Fourier Meets Gardner: Robust Blind Waveform Characterization

Radhika Mathuria
ECE, UC San Diego
rmathuria@ucsd.edu

Srivatsan Rajgopal
ECE, UC San Diego
srajagopal@ucsd.edu

Dinesh Bharadia
ECE, UC San Diego
dineshb@ucsd.edu

***Abstract*—Waveform Characterization is crucial for various spectrum sensing applications such as anomaly detection and measuring spectrum utilization. It consists of detecting the waveform type (single carrier or spread spectrum), modulation form (QAM, PSK, FSK, GMSK, GFSK etc) and corresponding parameters such as symbol rate and chip rate. In this paper, we propose a blind characterization algorithm suited for these applications using second-order cyclostationary and fourier domain features of signals. To test the proposed method's robustness, a comprehensive evaluation is conducted using both simulated and over-the-air (OTA) experiments with appropriate signal detection pre-processing steps. An overall modulation classification accuracy of 86.25% is attained for OTA testing with a modulation set consisting of QAM, PSK, FSK, GFSK, MSK, GMSK, DSSS and OOK.**

***Index Terms*—waveform characterization, cyclostationarity, anomaly detection, spectrum utilization**

I. Introduction

The Radio Frequency (RF) spectrum is a sparse and complex environment that poses a challenge for blind spectrum sensing applications such as anomaly detection and spectrum utilization measurement. With the proliferation of IoT devices, there arises a need to monitor the spectrum to identify unintended transmissions and potential security threats such as data ex-filtration or eavesdropping. In order to identify these activities, it is necessary to properly characterize a detected waveform. An effective approach to do this is to determine the waveform's modulation and protocol category. Moreover, it can also be valuable to determine the associated signal parameters, such as the data rate and modulation-specific parameters. Depending on the modulation technique used, these may include frequency deviation (frequency shift keying type), chip rate (spread spectrum type), symbol rate, and others. By estimating these, one can gain a more comprehensive understanding of the anomalous waveform. For example, an unexpected deviation in a standard protocol signal's symbol or chip rate may point towards an anomalous transmission that should be further investigated. Similarly, measuring spectrum utilization would require an understanding of the type of waveform (single carrier or spread spectrum), modulation and modulation order along with its data rate.

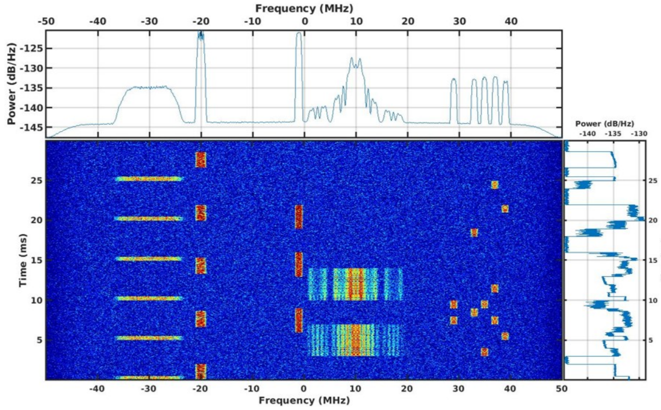


Fig. 1: The RF Spectrum is a complex environment that consists of multiple signals overlapping in time-frequency.

Blind Waveform Characterization is a challenging problem mainly due to the ambiguity involved in multiple factors, which range from the signal's characteristics to the radio parameters. In this work, the problem studied is one step ahead of the modulation classification problem as it also makes an attempt to extract signal parameters and identify protocols.

The following points describe some fundamental requirements of a robust waveform characterization system to operate for multiple spectrum sensing applications:

1) Function without apriori knowledge of the precise time-frequency bounds of signals: To effectively characterize signals from the spectrum, we must first detect and isolate them in time and frequency. This is because the receiver would collect a portion of the spectrum for a finite time period, encompassing of multiple transmissions as shown in Fig. 1.

Hence, for spectrum sensing scenarios when precise time-frequency boundaries of the signals are unknown, signal detection and isolation serve as a crucial pre-processing step. This is also established in [1], where the authors apply a channelizer followed by energy detection and higher-order statistics detection before passing the data through a modulation classifier. For this work also, we apply a recently proposed detection system, Searchlight [2], which is a robust energy detector specifically designed for blind spectrum sensing scenarios. Fig. 2 shows the high-level diagram of a spectrum sensing system containing the proposed waveform characterization block, which is preceded by a detector in order to provide it with the signal's time domain samples.

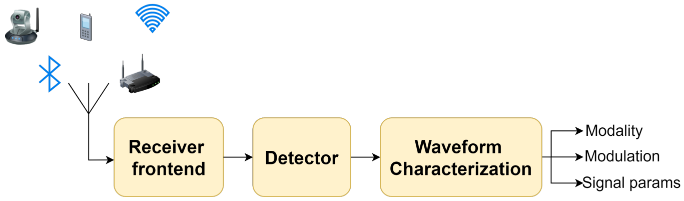


Fig. 2: A typical spectrum sensing system deployed with our proposed Waveform Characterization to provide detailed insights on the spectrum.

2) Use features that generalize over common signal characteristics: Signals have varying ranges of bandwidth, signal-to-noise ratio (SNR), symbol rates, pulse shaping filter characteristics, and other modulation-specific parameters such as frequency deviation (for frequency-shift keying type modulations) and chip rate (for direct sequence spread spectrum type modulations). This parameter diversity can majorly influence different features of signals such as power spectral density, and hence, they should be considered while designing a feature for a classifier. For this work, the datasets used to evaluate the algorithm are representative and comprehensive of the signal's characteristics.

3) Robust to RF Effects: Apart from signal-controlled parameters, the signals are affected by RF effects, such as the wireless channel, hardware effects like IQ imbalance, carrier frequency offset, and local oscillator leakage which could result in large deviations in the extracted features. For example, if a classifier is only trained using power spectral density (PSD) signatures of signals, then in the presence of a deep channel fade, the shape of the PSD would appear different and may lead to misclassification.

4) Awareness of interference in the spectrum: In practice, one may not always receive clean captures of signals from the spectrum, due to the presence of interfering signals. Hence, the classifier should be capable of distinguishing these cases from those when it receives a capture containing only one modulation. In this case, it can flag it off as either an unknown signal, or detect the presence of both modulated signals.

With these points into consideration, this paper proposes a methodology for waveform characterization that distinguishes commonly employed modulation categories using cyclostationarity and frequency domain features extracted from the time domain samples of the signal. It also extracts signal parameters such as symbol rate, chip rate and carrier frequency along with classifying some standard protocols and lays out a blueprint for adding other signals of interest for classification.

II. Cyclostationarity-based Waveform Characterization

A. A primer on cyclostationarity

Cyclostationary processes are a special subset of random processes where the statistical properties of the signals, such as the autocorrelation function vary periodically with respect to time as proposed by Gardner [3]. A commonly employed measure of cyclostationarity is the Spectral Correlation Density (SCD). Mathematically, the SCD is defined as the Fourier transform of the cyclic autocorrelation function, and thus measures the cyclic spectral redundancy. This is defined as:

$$S_x(f,\alpha) = \lim_{T\to\infty} \lim_{\Delta\to\infty} \int_{-\frac{\Delta t}{2}}^{\frac{\Delta t}{2}} \frac{1}{\sqrt{T}} X_T(t, f{+}\frac{\alpha}{2}) \frac{1}{\sqrt{T}} X_T^*(t, f{-}\frac{\alpha}{2}) dt \tag{1}$$

where $X_{T,u}$ is the finite Fourier transform of the signal $x(t)$ evaluated at the frequency u [4]. The SCD can be visualized as a two-dimensional function of spectral frequencies and cycle frequencies (f,α) wherein the regions of high magnitude correspond to high spectral correlation. Since wireless signals are complex in nature, it can be useful to analyze different configurations of $X_{T,u}$. The non-conjugate SCD is thus as defined in Equation (1), while the conjugate SCD is formed by the lag product of $X_{T,u}$ with no conjugation in the second term. Both these quantities may reveal different information about the cyclostationarity of a signal.

B. Related work

In literature, modulation classification is studied using feature-based methods such as the Fourier transform [5] and Wavelet transform [6], [7]. Another category of methods include likelihood-based techniques [8], [9], which are not practical for blind classification as they require estimation of various parameter distributions apriori. More recently, machine learning algorithms such as convolutional neural networks [10] are also deployed to train neural networks using I/Q samples and derived features. Since wireless signals exhibit cyclostationarity due to various factors that induce periodicity in them, such as symbol rate, chip rate etc. these signatures have emerged as a popular choice for blind detection [11] as well as modulation classification tasks [1], [12]. As shown in [13], cyclostationary features form a good choice to provide robustness against these RF non-linearities. However, there is a need to view the waveform characterization problem in a unified manner, from the point of view of a practical spectrum sensing system - analyzing effects of varying sample rates, SNRs, detection errors, and intricacies of blind cyclic features which this work aims to cover.

C. Goals of the proposed work

To address these requirements, this paper proposes a technique for blind waveform characterization designed to specifically tackle the complexities of a practical spectrum sensing system with the following key aspects:

1) Representative dataset generation using synthetic and over the air datasets consisting of different modulations and protocol-based signals that are pre-processed with a detection system
2) Decision-tree based classifier that takes insight from multiple signal processing features analyzed to develop a flow-chart based approach to return modulation, protocol and signal parameters

3) Extensive evaluation under different scenarios by comparing the classification accuracy with metrics such as SNR and Energy to Noise Ratio (ENR)

III. Algorithm Design

Waveform Characterization is an integral step to provide context to the detected transmissions in the RF spectrum. It operates on the I/Q samples of the detected signal in order to identify the modality, modulation, protocol (if present), and estimate signal parameters. Cyclostationary and frequency domain features are extracted and passed through a decision-tree-based classifier to predict these quantities. A high-level overview of this process is shown in Fig. 3 and described step-by-step in the next section.

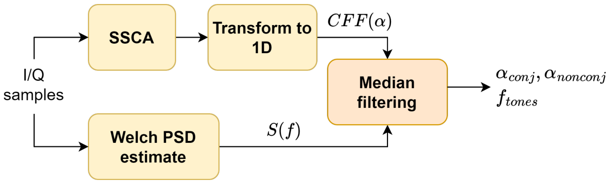


Fig. 3: A combination of cyclostationary and frequency domain features are used for classification.

A. Exploiting cyclostationary features

Cyclostationary patterns provide a unique way to represent various modulated signals in the spectrum. This is because wireless signals exhibit periodicities due to different factors such as chip sequence, symbol rate etc. leading to cyclostationary properties. To develop logic around processing the cyclostationary features, it is necessary to extract the prominent cycle frequencies of the signal, and most importantly map the patterns to the broad modulation family.

Signal detection systems such as [2] are prone to errors in isolating the signal in time/frequency. As proven in [14], even in these cases, the cyclostationary signatures can be retained by processing narrow subbands of the signal. This makes cyclostationary features a very robust choice for blind detection and classification applications.

1) Using the Strip Spectral Correlation Analyzer: In order to extract the cyclostationary features, the Strip Spectral Correlation Analyzer (SSCA) is used. This provides a blind estimation of the SCD, since conventional techniques such as the frequency smoothing method and time smoothing method are extremely sensitive to the cycle frequency resolution making them impractical to use for blind characterization scenarios. The SSCA point estimates are computed as follows [15]:

$$S_{xy}^{f_k+q\Delta\alpha}(n, \frac{f_k}{2} - q\frac{\Delta\alpha}{2})_{\Delta t} = \sum_{r} X_T(r, f_k) y^*(r) g(n-r) e^{-j2\pi q \frac{r}{N}} \tag{2}$$

where X_T is the complex demodulate of the signal, $\alpha = f_k + q\Delta\alpha$ and $f = 0.5 * (f_k - q\Delta\alpha)$. $y(r)$ is the unfiltered version of the signal, and this product is multiplied by a suitable window $g(n)$. The two governing parameters of the algorithm are the resolution in spectral and cycle frequency, (N, N_p). The two-dimensional output of the SSCA is transformed into a one-dimension cyclic feature function (CFF) following the steps described in [15]. The dominant cycle frequencies (CFs) appear as sharp peaks in the CFF if (N, N_p) are properly set, making it relatively simpler to extract them using signal processing techniques.

2) Cyclic analysis of modulated signals: Using the SSCA, we extensively analyzed the cyclostationary features of some common modulation families considering all the effects discussed for a practical modulation classifier. These are also theoretically established in [3], [16]. Fig. 4 shows the non-conjugate and conjugate cyclostationary features using SSCA of a Bluetooth packet collected from the 2.45 GHz band. The peaks in the non-conjugate and conjugate CFF appear at the symbol rate, which in this case is 1 MHz.

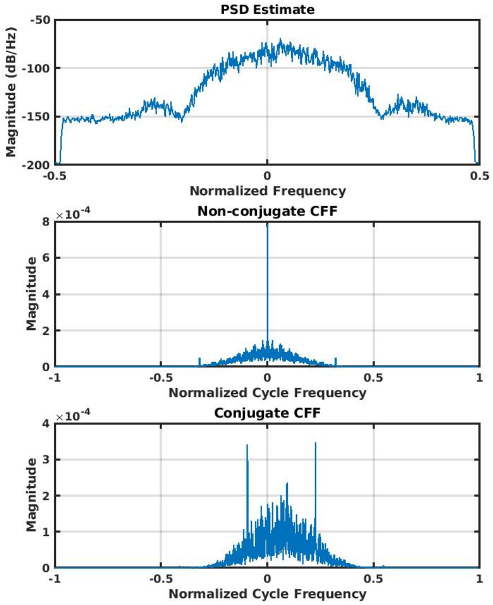


Fig. 4: PSD and Cyclostationary signatures of a captured BLE packet

Table I shows the signal categories divided into various groups based on their second-order cyclostationary features. It can be seen that second-order features are not sufficient to distinguish some modulations such as QAM/PSK, MSK/GMSK etc.

B. Using Frequency Domain features as a support

Frequency domain features such as the power spectral density (PSD) estimate of a signal can also serve as a distinguishing factor for many common modulations. Additionally, they are efficient to compute by leveraging the low computational complexity of the Fourier transform. In this work, we leverage the fact that each tone in a signal's PSD gives rise to a conjugate cycle frequency at twice the tone frequency. Hence,

TABLE I: Signal families divided based on common cyclostationary signatures

Signal family	**Non-conjugate CFs**	**Conjugate CFs**
BPSK, OOK	f_{sym}	$2f_{\text{c}}$, $2f_{\text{c}} \pm f_{\text{sym}}$
QAM, PSK	f_{sym}	-
FSK, GFSK	f_{sym}, $2f_{\text{tones}}$	$2f_{\text{c}}$, $2f_{\text{c}}\pm 2f_{\text{tones}}$, $2f_{\text{c}}\pm f_{\text{sym}}$
MSK, GMSK	f_{sym}	$2f_{\text{c}} \pm 0.5f_{\text{sym}}$
DSSS BPSK	f_{sym}, f_{chip}	$2f_{\text{c}}$, $2f_{\text{c}} \pm f_{\text{sym}}$
DSSS QAM, PSK	f_{sym}, f_{chip}	-

TABLE II: Feature look-up table for different modulations

Modulation	**Rule**
BPSK	- Conjugate CFs at $2f_c$, $2f_c \pm f_{sym}$ - No tone in the PSD
OOK	- Conjugate CFs at $2f_c$, $2f_c \pm f_{sym}$ - Tone present in PSD at f_c
DSSS	- Non-conjugate CFs at harmonics of f_{sym} - Non-conjugate CFs do not have strictly decreasing heights
FSK	- Tones present in PSD separated by f_{dev} - Most dominant peaks in conjugate PSD should correspond to $2f_{tone}$ - If so, modulation order of FSK = number of detected tone frequencies
MSK/GMSK	- No tone in PSD - Conjugate CFs separated by f_{sym} - No conjugate CFs at $2f_c$
QAM/PSK	- No conjugate CFs

if a tone is detected at frequency f_0, there should be a corresponding conjugate cycle frequency detected at $\frac{f_0}{2}$.

By adding this linkage between the cycle and tone frequencies, we try to avoid any false positives that could be encountered due to incorrect thresholding. A tone is said to be detected if $\alpha_{conjugate} - 2f_{tone} < \delta$, where δ is a tolerance factor to factor in the change in resolution between the two frequencies.

C. Extraction of cyclostationary and frequency domain features - Median filtering

To extract the frequencies from the CFF as well as PSD, an adaptive thresholding mechanism is required that is robust to the noise variance. We borrow an idea from image processing applications, where median filters are known to denoise an image while preserving the sharp edges [17]. Similarly, a median filter could preserve the dominant peaks in the CFF and PSD for this use case. If $f(x)$ is the feature function and $\tilde{f}(x)$ is the median filtered version of it, a frequency crosses the threshold if $f(x) > \beta\tilde{f}(x)$, where β is the scale factor set to raise $\tilde{f}(x)$ to form a threshold. This is heuristically set based on experimental data. The median filter can adapt itself to the shape of the CFF while preserving the peaks. In cases when the features are absent, no cycle frequencies should be detected.

D. Forming a decision tree

With the look-up tables for the cyclostationary as well as frequency domain features, a set of rules can be laid out for each modulation category. These rules can then be converted into some logic using the extracted features which can be organized as a decision tree. A summary of these rules is given in Table II.

It is to be noted that using this set of features, it is not possible to further resolve some modulations, such as QAM/PSK and MSK/GMSK due to similar features. However, if one extends to using higher-order cyclostationary features using a similar approach, these modulations can be separately resolved too.

Fig. 5 shows the entire flow diagram of the classifier created using the rules in Table II where each endpoint represents a decision. Each stage is like a binary classification problem which outputs whether that particular modulation category is detected or not. If it is not detected, the features are passed to the next stage, and so on. If no modulation category matches, the signal is classified as an unknown category. Also, in some cases the classification is two-stage, for example, once a signal is classified as DSSS, it goes through another set of classifiers to check if it belongs to a protocol-based DSSS (WiFi, Zigbee) or it is vanilla DSSS (no protocol, can be possibly an LPI signal). Once a modulation is detected, all relevant parameters based on Table I are extracted for that category.

E. Sub-classifiers

1) DSSS Classifier: DSSS (QAM and PSK) exhibit non-conjugate cyclostationarity at harmonics of symbol rate and chip rate due to the spreading sequence. This leads to a unique cyclic signature unlike other single carrier modulations making it easy to filter out first. Given that the chip rate of DSSS is an integral multiple of the symbol rate, the first harmonic non-conjugate CF corresponds to the symbol rate, the non-conjugate CFs typically occur as $f_{sym}, 2f_{sym}, 3f_{sym}$ and so on. Since one of these harmonics would be the cycle frequency corresponding to the chip rate, the magnitude of spectral correlation would be greater (leading to uneven prominence). Single carrier signals may also have CFs at harmonics of f_{sym}, depending on pulse shaping, but with steadily decreasing/constant prominences. Hence, after detecting harmonic CFs, it is important to also check the prominences of the detected CFs. For a modulation to be classified as DSSS, the prominence should not steadily increase or decrease, i.e. it should exhibit a variable nature as shown in Fig. 6.

2) Real modulations classifier: Real modulations refer to those that only contain an in-phase component, and this leads to similar conjugate and non-conjugate CFs:

$$\alpha_{nonconj} = \pm f_{sym} \qquad \alpha_{conj} = 2f_c, 2f_c \pm f_{sym} \tag{3}$$

If the detected conjugate CFs are $[\alpha_1, \alpha_2, \alpha_3]$ then,

$$||\alpha_2 - \alpha_1| - \alpha_{sym}| < \delta \;\; , \;\; ||\alpha_3 - \alpha_2| - \alpha_{sym}| < \delta \tag{4}$$

where δ is a small tolerance factor. If this test is successful, the tone frequency check is employed to distinguish between OOK and BPSK.

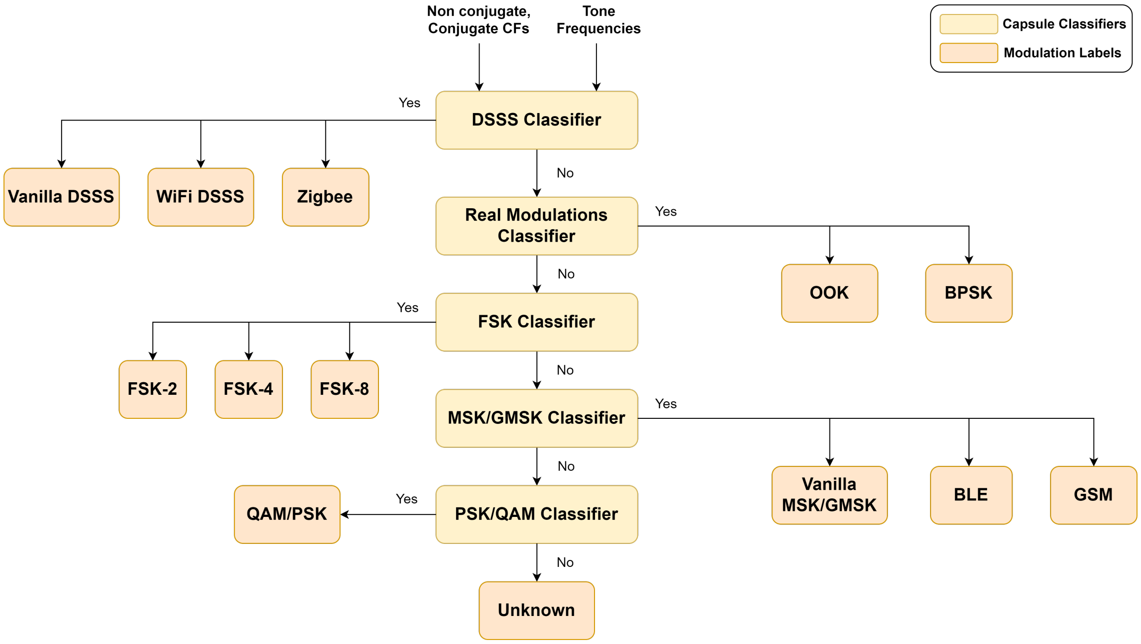


Fig. 5: Hierarchical decision tree-based classifier

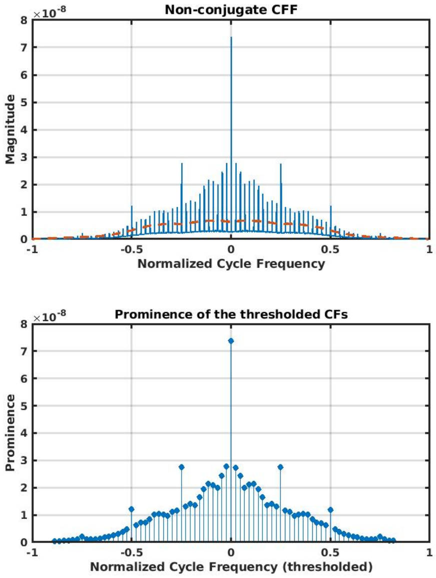


Fig. 6: Non-conjugate CFF and the corresponding peak prominences of the thresholded CFs

3) FSK classifier: With the assumption that the FSK signals are discontinuous-phase type, the presence of tones and their corresponding conjugate CFs is used as a test for FSK modulations. Additionally, the symbol rate and frequency deviation can also be extracted.

4) MSK/GMSK classifier: MSK/GMSK do not possess a cycle frequency corresponding to the carrier frequency due to their continuous phase nature. The two most prominent conjugate CFs differ by the symbol rate, i.e.:

$$||\alpha_2 - \alpha_1| - \alpha_{sym}| < \gamma \tag{5}$$

where γ is a tolerance factor and$[\alpha_1, \alpha_2]$ are the two conjugate CFs. It is to be noted that this condition could be even true for BPSK/OOK but since they would already be detected at an earlier stage, there would not be an ambiguity. Therefore, the placement of each sub-classifier in the main decision tree is crucial.

5) QAM/PSK classifier: QAM/PSK are the only class in the above modulations that do not possess any conjugate cyclic features or tones. Hence, at the end of the entire decision tree if there is a signal such that two symmetric non-conjugate CFs are detected but no conjugate CF is present, then this is classified as QAM/PSK. If a signal does not meet this criterion, then it is classified as ”unknown”.

IV. Evaluation

A. Dataset Generation

Due to the varied parameterizations possible for anomalous signals, a broad spectrum of parameter sweeps were incorporated into the datasets. Tables III, IV, V, VI show the parameter sweeps in the datasets for various categories. The $\frac{E_s}{N_o}$ for spread spectrum signals is set as low as -10 dB as these are common below-noise floor signals due to their spreading properties for recovery. Also, different chip sequence lengths are included in the dataset as this parameter also plays a significant role in changing the power spectral density of the signal.

A large dataset containing data points with each of these parameter combinations was used for analysis and testing. Two kinds of datasets with the same parameterizations were

TABLE III: Dataset parameter ranges for single carrier signals

Parameter	Range
Es/No	-5 to 25 dB
Symbol Rate	250 KHz to 10 MHz
RRC roll-off factor	0.25 to 0.4
RRC filter spans	4 to 10
Signal durations	2 to 8 ms
Samples Per Symbol	2 to 8

TABLE IV: Dataset parameter ranges for spread spectrum signals

Parameter	Range
Es/No	-10 to 25 dB
Symbol Rate	250 KHz to 5 MHz
RRC roll-off factor	0.25 to 0.4
RRC filter spans	4 to 10
Signal durations	2 to 5 ms
Chips per Symbol	3, 7, 11, 15, 31, 63, 127
Samples Per Chip	2 to 10

generated - one with simulated AWGN noise and wireless channel models such as heuristic (multipath) and rician, and the other was passed over the air using USRP N320s as shown in Fig. 7. In the synthetic dataset, all signals were resampled to 100 Msps, while in the OTA datasets, the signals were resampled based on the radio's settings.

Fig. 7: Hardware setup that consisted of USRP N320s

TABLE V: Modulation order sweeps in the dataset

Modulation	Orders
FSK	2, 4, 8
PSK	2, 4, 8, 16, 32
QAM	16, 64, 256
DSSS PSK	2, 4, 8, 16, 32
DSSS QAM	16, 64, 256

Apart from the vanilla modulations, the protocol signals (BLE, WiFi, Zigbee, GSM) consist of a mix of synthetically generated signals, and real-world captures from their respective frequency bands using SDRs.

B. Data pre-processing

The signals are resampled from their original sample rate and are confined only within a certain time-frequency range in the collected data. The goal of a detector would be to hence identify these bounds, and extract the I/Q samples corresponding to this. However, the detector may introduce some error into the system, in terms of time and/or frequency bounds and hence the effect of this should be incorporated into the testing of the classifier. Two types of detectors are used- one is a perfect energy detector that knows in prior the location of the signal to help establish a baseline, and the other is Searchlight [2], as described in an earlier section.

TABLE VI: Modulation-specific parameter sweeps in the dataset

Modulation	Parameter	Value
FSK	Frequency deviation	0.05 to 0.6
GFSK, GMSK	Bandwidth-time product	0.2 to 1
DSSS	Samples per chip	2 to 10
DSSS	Spreading codes	Random PN Sequence Barker codes

Fig. 8 shows this entire pre-processing flow. Finally, after each pre-processed data point is obtained, it is passed through the feature extraction block where the relevant features are extracted.

C. Evaluation metrics

We use $\frac{Es}{N_o}$ and the Energy to Noise ratio (ENR) as the key metrics for evaluating the classification accuracies. While both $\frac{E_s}{N_o}$ and SNR measure signal power relative to noise power these two metrics are only equal for a signal that is not oversampled. $\frac{E_s}{N_o}$ is actually the in-band SNR of a signal and hence for resampled signals, the following relation exists [18]:

$$SNR = \frac{E_s}{N_o}\frac{B/W}{f_s} \tag{6}$$

If a low SNR signal is collected for a sufficiently long time, its energy would be more than the same SNR signal collected for a shorter duration. Hence, Energy to Noise Ratio [18], which measures the energy of the signal is a more appropriate technique as compared to SNR for evaluation. To the best of our knowledge, this is the first work that studies the modulation classification performance with respect to ENR. Mathematically ENR (in dB) is defined as:

$$ENR = SNR + 10\log_{10}(bt) \tag{7}$$

Here, bt is the time-bandwidth product of the energy box and is a dimensionless quantity. For example, if a signal spans 5 ms and is 1 MHz wide, this product would be 500. Hence, the classification accuracy is compared against ENR and $\frac{E_s}{N_o}$.

V. Results

The results of the classifier are evaluated under multiple combinations of dataset and pre-processing techniques to allow extensive testing.

A. Vanilla modulations

Figs. 9, 10 and 11 show the per-category accuracies for different datasets. As expected, a perfect energy detector leads to a better overall classification accuracy of 92.5% and 74.125% for OTA and synthetic datasets respectively. The synthetic dataset contains a much lower range of SNR for the signals since it can be controlled while for OTA data, this is difficult to control and hence causing the difference in accuracies. Using searchlight with OTA data, we obtain a classification accuracy of 86.25%, which is slightly lesser than a perfect energy detector with the same dataset.

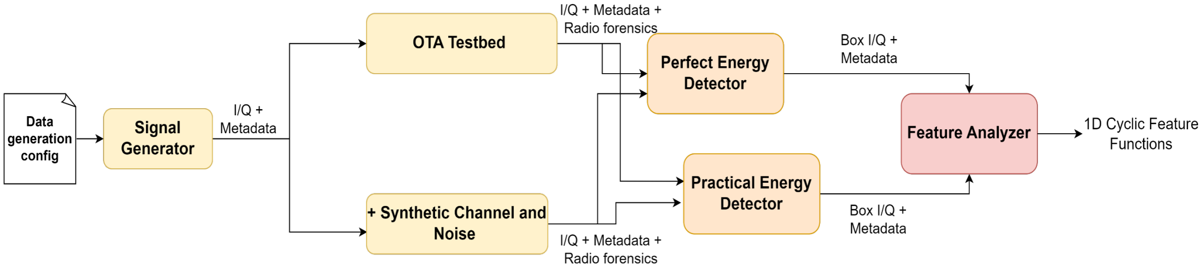

Data generation config
Signal Generator
I/Q + Metadata
OTA Testbed
+ Synthetic Channel and Noise
I/Q + Metadata + Radio forensics
I/Q + Metadata + Radio forensics
Perfect Energy Detector
Practical Energy Detector
Box I/Q + Metadata
Box I/Q + Metadata
Feature Analyzer
1D Cyclic Feature Functions

Fig. 8: The feature analysis procedure consists of signal generation and transmission, followed by detection.

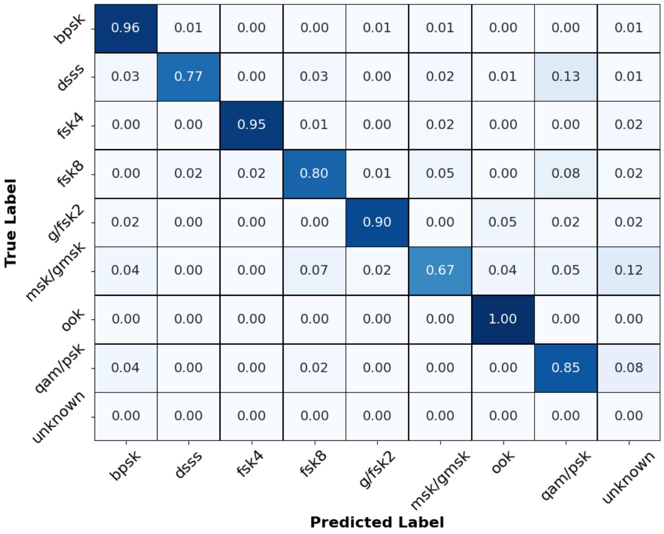


Fig. 9: Confusion Matrix of the OTA dataset passed through the practical energy detector (Searchight [2])

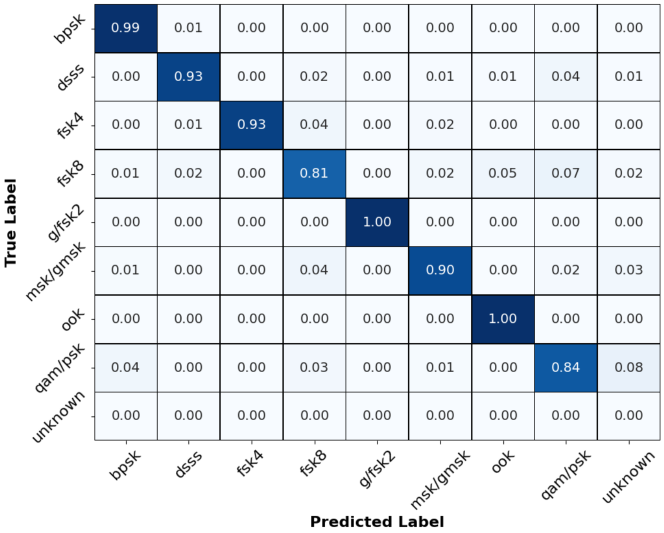


Fig. 10: Confusion Matrix of the OTA dataset passed through a perfect energy detector

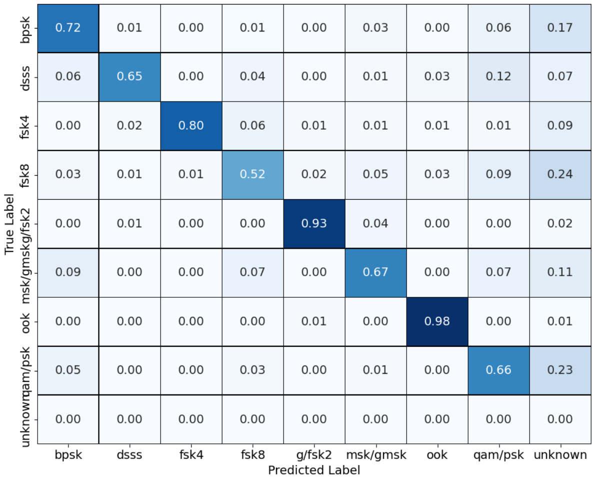


Fig. 11: Confusion Matrix of the synthetic dataset passed through a perfect energy detector

There is a significant decrease in the accuracy of DSSS from 93% to 77% from the perfect to practical energy detector case. This can be attributed to the fact that DSSS has many discontinuities in energy and hence is especially more prone to errors in isolating its time-frequency bounds. If a narrow subband of DSSS is detected as a separate signal, then this would resemble its single carrier counterpart, and hence 13% of the DSSS QAM/PSK was classified as single carrier QAM/PSK. In this manner, testing the algorithm with different flavors of data aids in forming a better understanding of the specific issues. Fig. 12 shows the per-category classification accuracy as a function of the ENR. The general trend observed is an increase in accuracy with an increase in ENR, however we can observe that some modulations such as MSK/GMSK require a higher ENR to achieve 80% accuracy. This is because they are continuous-phase modulations, which lead to weaker non-conjugate cyclic features. Hence in low ENR scenarios, it is challenging to extract their cycle frequencies, causing low accuracy.

As shown in Fig. 13, the average ENR across the dataset to achieve 80% accuracy is approximately 53 dB, but in terms of SNR it is only 7 dB. This is a reasonable limit for conventional communication signals. It is to be noted that even at low SNRs

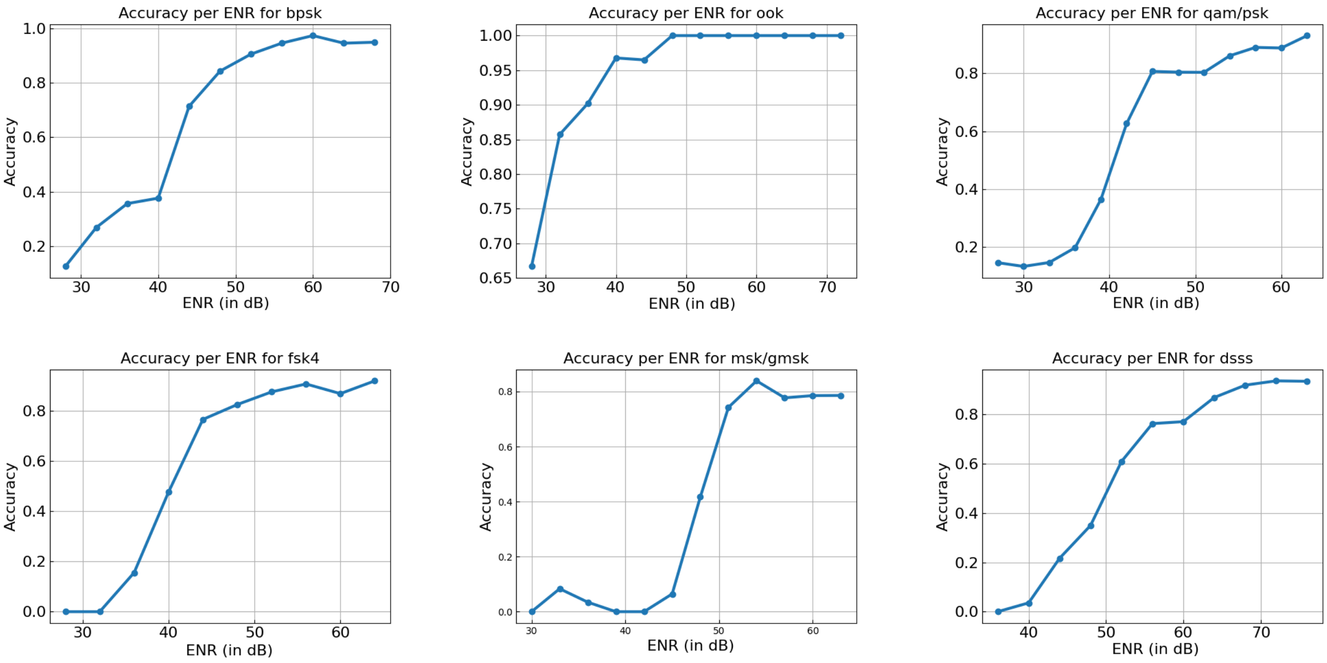


Fig. 12: Accuracy vs ENR of classifier results with simulated data

0 dB, the classification accuracy is still above 50%. Also, the application of different wireless channel models as compared to an identity channel causes a dip in accuracy.

B. *Protocol-based signals*

As shown in the decision tree in Fig. 5, some modulations are also classified up to a protocol level. We take up an example for the MSK/GMSK family of modulations, consisting of vanilla MSK/GMSK, BLE and GSM signals. Once the symbol rate is estimated, a look-up table is used to compare the extracted and expected symbol rates. Additionally, knowledge of center frequency would also help, but is not used in this test. Table VII shows the required non-conjugate cycle frequency for the protocols. A similar look-up table can be created for any protocol signal, once its dominant cycle frequencies are characterized depending on the system use case.

TABLE VII: Cycle frequencies look-up table for the MSK/GMSK classification

Waveform	**Non-conjugate cycle frequency**
BLE	1 MHz or 2 MHz
GSM DL	67.7 KHz
Vanilla MSK/GMSK	Any

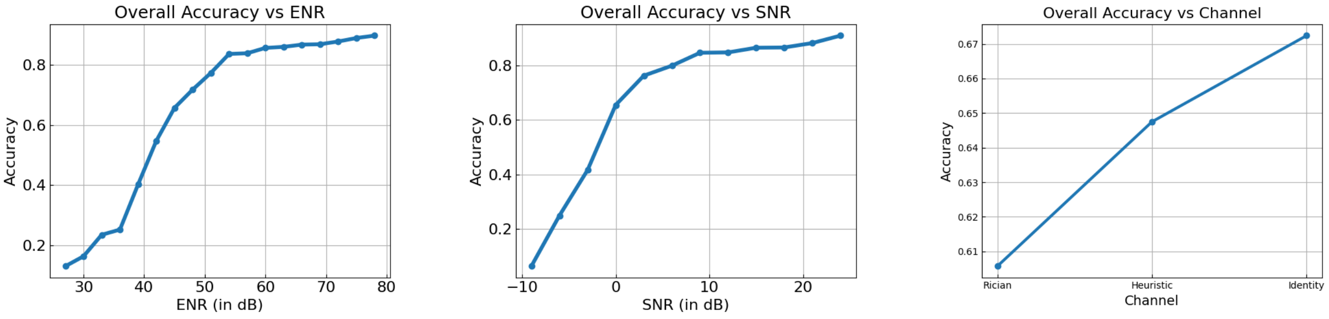
This was tested using simulated BLE and GSM DL packets, and an accuracy of 87% was achieved for BLE, while an accuracy of 91% was achieved for GSM DL. While this was done only with GSM DL packets, it can also be extended to other variants of GSM by analyzing their cycle frequencies and adding them to the LUT. Additionally, the symbol rate of BLE was also estimated (1 MHz or 2 MHz) using the extracted non-conjugate cycle frequencies. Similar to this, based on a particular spectrum sensing application, or frequency band of interest, the different protocol waveforms can be characterized in terms of their dominant cycle frequencies. Additionally, the decision tree structure allows for easy addition of classifiers for other modulations that are not currently included by following the established blueprint for building the classifier submodules.

C. *Symbol-rate estimation*

Cyclostationary features offer the added benefit of estimation of various signal parameters such as symbol rate, chip rate etc. Based on the median-filter based feature extraction framework developed, once a modulation is classified, we can map the particular cycle frequency to a known parameter. For example, it is known that the most prominent non-conjugate CF for QAM/PSK type modulations corresponds to the symbol rate. Fig. 14 shows the accuracy in the symbol rate estimation for QAM/PSK, which has a higher variance at lower symbol rates, but is more consistent at higher rates. This is because a lower symbol rate leads to a lower ENR, and hence weaker cyclic features.

VI. Conclusion

This work proposes a blind waveform characterization system capable of classifying various modulation categories and protocol-based signals with an accuracy of 86.25% on over-the-air data. The SSCA algorithm is implemented and used for the blind estimation of cyclic features. It also provides estimates of the parameters of a signal corresponding to the dominant cycle frequencies. The decision tree-based classifier structure, based on a combination of cyclostationary and fourier features brings the benefit that it can be extended to add



(a)

(b)

(c)

Fig. 13: Overall classification accuracy with respect to (a) ENR (b) SNR and (c) Wireless Channel

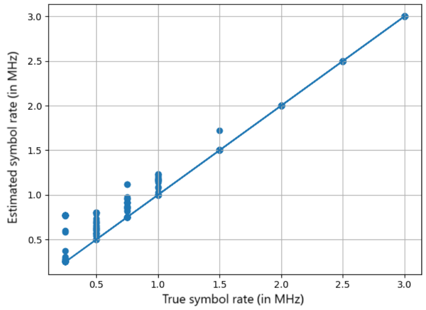


Fig. 14: Estimation of symbol rate for QAM/PSK using cycle frequencies

other modulations and protocols depending on the signal-of-interest for the given application. Additionally, new features can be incorporated for a finer classification level, such as higher-order-cyclic features.

VII. Acknowledgements

This section is based upon work supported in part by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via [2021-2106240007]. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.

References

[1] Chad M. Spooner, Apurva N. Mody, Jack Chuang, and Josh Petersen. Modulation recognition using second- and higher-order cyclostationarity. In *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–3, 2017.

[2] Richard Bell, Kyle Watson, Tianyi Hu, Isamu Poy, fred harris, and Dinesh Bharadia. Searchlight: An accurate, sensitive, and fast radio frequency energy detection system. In *MILCOM 2023-2023 IEEE Military Communications Conference (MILCOM)*. IEEE, 2023.

[3] W. Gardner and L. Franks. Characterization of cyclostationary random signal processes. *IEEE Transactions on Information Theory*, 21(1):4–14, 1975.

[4] W. Gardner. Measurement of spectral correlation. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 34(5):1111–1123, 1986.

[5] Z. Yu, Y.Q. Shi, and W. Su. M-ary frequency shift keying signal classification based-on discrete fourier transform. In *IEEE Military Communications Conference, 2003. MILCOM 2003.*, volume 2, pages 1167–1172 Vol.2, 2003.

[6] Kais Hassan, Iyad Dayoub, Walaa Hamouda, and Marion Berbineau. Automatic modulation recognition using wavelet transform and neural networks in wireless systems. *EURASIP Journal on Advances in Signal Processing*, 2010:42, 01 2010.

[7] K.C. Ho, W. Prokopiw, and Y.T. Chan. Modulation identification by the wavelet transform. In *Proceedings of MILCOM '95*, volume 2, pages 886–890 vol.2, 1995.

[8] Fahed Hameed, Octavia A. Dobre, and Dimitrie C. Popescu. On the likelihood-based approach to modulation classification. *IEEE Transactions on Wireless Communications*, 8(12):5884–5892, 2009.

[9] Ali Ramezani-Kebrya, Il-Min Kim, Dong In Kim, Francois Chan, and Robert Inkol. Likelihood-based modulation classification for multiple-antenna receiver. *IEEE Transactions on Communications*, 61(9):3816–3829, 2013.

[10] Timothy James O'Shea, Tamoghna Roy, and T. Charles Clancy. Over-the-air deep learning based radio signal classification. *IEEE Journal of Selected Topics in Signal Processing*, 12(1):168–179, 2018.

[11] Kyouwoong Kim, Ihsan A. Akbar, Kyung K. Bae, Jung-Sun Um, Chad M. Spooner, and Jeffrey H. Reed. Cyclostationary approaches to signal detection and classification in cognitive radio. In *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pages 212–215, 2007.

[12] Chad Spooner. *Chapter 18. Spectrum Sensing Based on Spectral Correlation*, page 593. 12 2009.

[13] Eric Rebeiz, Paulo Urriza, and Danijela Cabric. Optimizing wideband cyclostationary spectrum sensing under receiver impairments. *IEEE Transactions on Signal Processing*, 61(15):3931–3943, 2013.

[14] Chad M. Spooner, Apurva N. Mody, Jack Chuang, and Michael P. Anthony. Tunnelized cyclostationary signal processing: A novel approach to low-energy spectrum sensing. In *MILCOM 2013 - 2013 IEEE Military Communications Conference*, pages 811–816, 2013.

[15] Randy S. Roberts, William A. Brown, and Jr. Loomis, Herschel H. Computationally efficient algorithms for cyclic spectral analysis. *IEEE Signal Processing Magazine*, 8:38–49, April 1991.

[16] W. Gardner. Measurement of spectral correlation. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 34(5):1111–1123, 1986.

[17] Rafael C. Gonzalez and Richard E. Woods. *Digital Image Processing (3rd Edition)*. Prentice-Hall, Inc., USA, 2006.

[18] *Fundamentals of Statistical Signal Processing, Volume 1: Estimation Theory*. Pearson Education.