Experimental Analysis of Cross-Layer Sensing for Protocol-Agnostic Packet Boundary Recognition

Maxwell McManus[1], Zhangyu Guan[1], Elizabeth Serena Bentley[2], and Scott Pudlewski[3]
[1]Dept. of Electrical Engineering, State University of New York (SUNY) at Buffalo, Buffalo, NY 14260, USA
[2]Air Force Research Laboratory (AFRL), Rome, NY 13440, USA
[3]Georgia Tech Research Institute (GTRI), Atlanta, GA 30332, USA
Email: {memcmanu, guan}@buffalo.edu, elizabeth.bentley.3@us.af.mil, scott.pudlewski@gtri.gatech.edu

***Abstract*—Radio-frequency (RF) sensing is a key technology for designing intelligent and secure wireless networks with high spectral efficiency and environment-aware adaptation capabilities. However, existing sensing techniques can extract only limited information from RF signals or assume that the RF signals are generated by certain known protocols. As a result, their applications are limited if proprietary protocols or encryption methods are adopted, or in environments subject to errors such as unintended interference. To address this challenge, we study *protocol-agnostic cross-layer sensing* to extract high-layer protocol information from raw RF samples *without* any a priori knowledge of the protocols. First, we present a framework for protocol-agnostic sensing for over-the-air (OTA) RF signals, by taking packet boundary recognition (PBR) as an example. The framework consists of three major components: *OTA Signal Generator*, *Agnostic RF Sink*, and *Ground Truth Generator*. Then, we develop a software-defined testbed using USRP SDRs, with eleven benchmark statistical algorithms implemented in the *Agnostic RF Sink*, including Kullback-Leibler divergence and cross-power spectral density, among others. Finally, we test the effectiveness of these statistical algorithms in PBR on OTA RF samples, considering a wide variety of transmission parameters, including modulation type, transmission distance, and packet length. It is found that *none* of these benchmark statistical algorithms can achieve consistently high PBR rate, and new algorithms are required particularly in next-generation low-latency wireless systems.**

I. Introduction

Radio-frequency (RF) sensing is a key technology to design the next-generation intelligent and secure wireless networks with higher spectral efficiency and better resilience against adversarial attacks. In the past decades, RF sensing has attracted significant research interest, focusing on cognitive radio [1], spectrum coexistence [2], localization and tracking [3], and detection of adversarial interference [4], among others. This article studies a new application of RF sensing, which we call *protocol-agnostic cross-layer sensing*, in non-cooperative environments with *limited or no* a priori knowledge of the protocols adopted by the wireless networks.

Why Protocol-Agnostic Cross-Layer Sensing? Different from the RF sensing at physical layer, where the primary objective is to detect the presence and strength of radio signals [5], [6], cross-layer RF sensing aims to discover a richer set of signal features at higher protocol layers, and hence to unveil the hidden traffic pattern and enable more sophisticated adaptation to the dynamic spectrum environments or launch more effective denial of service (DoS) efforts. For example, it is discussed in [4] that, compared to traditional continuous-noise interference, significantly more effective interference attempts can be launched against a network if adequate knowledge of the network's transmission protocols can be obtained. Towards this end, the low-level time-domain information of the control packets of a known protocol such as timing and length can be used to implement protocol-aware interference to target those control packets [4].

While existing research has shown great potential of cross-layer sensing, there are still several challenges to address. First, the quality of the received RF signals, in terms of signal strength and signal-to-noise ratio (SNR), is highly affected by path loss, fading, shadowing, noise, and other factors. As a result, it is difficult to extract any useful high-layer protocol information without successful decoding of the packets because of the poor-quality RF signals. Moreover, it is also challenging to perform cross-layer sensing in those low-power IoT systems [7], [8] such as Bluetooth, LoRaWAN and SigFox, where spread-spectrum and frequency hopping techniques have been utilized for interference avoidance in high-density RF environments [7].

Second, as more spectrum resources are made open for unlicensed use, different wireless systems may need to co-locate on the same frequency band while operating different, possibly proprietary protocols. For example, the ISM bands (USA: 915 MHz, Europe: 868 MHz) are home to many low-power, wide area network (LPWAN) technologies such as SigFox and LoRaWAN [9]. SigFox is an Ultra-Narrowband (UNB) communication scheme based on proprietary MAC-layer protocol, which ensures a high degree of network security by limiting the over-the-air (OTA) activity of devices within a network in addition to non-OTA activation of end devices [10]. In such scenarios, higher-layer protocol information cannot be sensed by decoding the packet header information because of the proprietary protocols.

To address the above challenges, a key step is to understand through rigorous experiments the limitations of existing approaches for protocol-agnostic RF sensing. In this work

ACKNOWLEDGMENT OF SUPPORT AND DISCLAIMER: (a) Contractor acknowledges Government's support in the publication of this paper. This material is based upon work funded by AFRL, under AFRL Contract No. # FA8750-20-1-0501. (b) Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of AFRL.

Distribution A. Approved for public release: Distribution unlimited AFRL-2020-0313 on November 18, 2020.

we make an initial step towards this direction, taking packet boundary recognition (PBR) at the link layer based on raw RF samples at the physical layer as an example. We consider PBR because it is an enabling technique for collecting various upper-layer protocol characteristics of wireless networks, e.g., packet duration, timing, periodicity as well as type (e.g., control vs data). A wide set of new sensing-based applications can be enabled by our work, including intelligent spectrum access, wireless network traffic and non-cooperative interference detection, among others, through enhanced environmental awareness and protocol identification.

We claim the following two main contributions:

- We first present a framework for protocol-agnostic sensing for OTA RF signals. The framework consists of three components: *OTA Signal Generator*, *Agnostic RF Sink*, and *Ground Truth Generator*. We further develop a software-defined testbed based on USRP software radios, considering PBR as an example. Eleven statistical algorithms are implemented in the *Agnostic RF Sink* for PBR analysis of the received OTA signals.
- We conduct a rigorous performance evaluation of each of the PBR algorithms using OTA RF samples, and compare their performance with ground truths generated within the *Ground Truth Generator*. Time-domain analysis of low-level signal features provides necessary information for higher-level inference. Results indicate that *none* of these benchmark statistical methods can achieve consistently high PBR accuracy in all the tested scenarios, and new algorithms are required particularly in next-generation low-latency wireless systems.

II. Related Work

RF sensing has attracted significant research attention with a sizable and growing body of literature [1]–[3], [6], [11]–[14]. For example, the authors of [11] prove the ability to classify traffic by protocol according to only a fraction of packets within a stream, assuming packet size, timing, and received power levels to be known. Similarly, in [12] Dempsey et al. sense and classify different types of packets generated by a known set of network and transport layer protocols, assuming packet size, timing and other lower-layer packet information to be known. A wideband compressive sampling method is introduced in [15] to detect wireless signals in frequency hopping networks. The authors of [16] propose a simplified iterative compressive sensing approach to detect spectrum holes in ultra-wideband wireless UAV networks. Datta et al. compare in [17] the efficiency of cooperative sensing methods for spectrum detection by considering different fading models. In [18], the authors use spectral correlation function to extract second-order statistic information of the RF samples to detect spectrum occupants. Please refer to [6], [19] and references therein for a good survey of the main results in this field. Different from these work, where the physical layer information is usually assumed to be known, in this paper we focus on protocol-agnostic RF sensing with *limited or no* a priori knowledge of the signals.

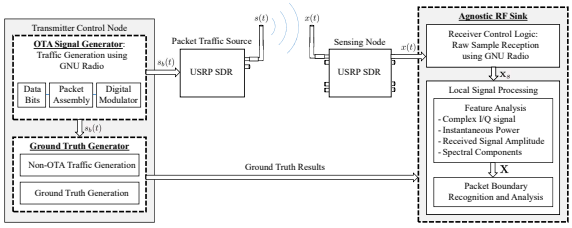


Fig. 1: Software-defined packet recognition framework.

The use of physical layer characteristics in protocol-agnostic applications has been most explored in the context of modulation recognition (MR) [20]–[24]. For example, a discrete wavelet two-stage neural network group is introduced in [20] to use time-frequency features for automatic MR. In [21], [22], O'Shea et al. show that convolutional neural networks (CNNs) trained on OTA radio signals can be an effective alternative to traditional feature-based MR. Zhang et al. propose in [23] to utilize frequency-domain information of the radio signals as input to a CNN for MR. Readers are referred to [24] and references therein for a good survey in this area. Different from MR, in this work we focus on a new application of protocol-agnostic sensing for packet boundary recognition.

III. Packet Boundary Recognition Framework

A. Overall Framework

The framework of the packet recognition system is illustrated in Fig. 1, where there are three major components: *OTA Signal Generator*, *Agnostic RF Sink*, and *Ground Truth Generator*. In the *OTA Signal Generator*, the passband source signal $s(t)$ is first generated by modulating baseband signal $s_b(t)$ to a carrier frequency f_c, i.e., $s(t) = \Re\{s_b(t)e^{j2\pi f_c t}\}$ and then sent to the SDR front-end of the *OTA Signal Generator* for over-the-air transmissions. At the same time, the baseband signal $s_b(t)$ is also recorded as a non-OTA traffic sequence in the *Ground Truth Generator* to extract ground truth packet boundary information.

The signals received by the *Agnostic RF Sink*, denoted as $x(t)$, can be given as $x(t) = s(t) * h(t) + \eta(t)$, where $*$ is the convolution operation, $h(t)$ is the channel gain, and $\eta(t)$ represents noise introduced by the channel. The continuous signal $x(t)$ is first quantized by the *Receiver Control Logic* in the *RF Agnostic Sink* into a stream of discrete samples represented as a vector $\mathbf{x} = [x_1, x_2, ..., x_S]$, where S is the length of the quantized stream in samples. The resulting sample stream is then further divided into a set of consecutive bins each of size B in the *Local Signal Processing* block.

Denote the resulting set of bins as $\mathbf{X} = \{X_1, X_2, ..., X_\beta\}$, in which $\beta = \lfloor \frac{S}{B} \rfloor$ and $\lfloor \bullet \rfloor$ is the integer floor operation. The obtained bins $\mathbf{X}$ are finally used by the *Agnostic RF Sink* for feature extraction and PBR analysis. The analysis results are then evaluated by comparison with the ground truths captured by the *Ground Truth Generator*. This will be further discussed later in this section.

B. PBR Analysis

Recall in Section I that our objective is to understand the limitations of existing statistical methods for protocol-agnostic

sensing. To this end, eleven statistical PBR approaches have been implemented in the *Local Signal Processing* block of the *Agnostic RF Sink*. These approaches include cross-correlation, variance, covariance, entropy, cross-entropy, Pearson's correlation, Fisher's method, Kullback-Leibler Divergence (KLD), distance correlation, Welch's method, and cross-spectral density (CSD). These approaches have been selected to test, in a comparative manner, their potential for discovering the target patterns of the test data by considering a wide range of experimental configurations. Next, we discuss two representative categories of PBR analysis approaches to illustrate the experimental process.

Entropy, Cross-Entropy, and Relative Entropy Approaches. Entropy is a notion from information theory, taken as a measure of information, and has been applied to pattern recognition problems [25]. For PBR, sample bins containing inter-packet gaps are expected to exhibit different levels of entropy than bins without any gaps. In this work, Shannon entropy is considered. Given a single sample bin $X_m \in \mathbf{X}$, the corresponding entropy, denoted $H(X_m)$, can be calculated as

$$H(X_m) = -\sum_{i=1}^{B} P(x_{m,i}) \log_2 P(x_{m,i}), \tag{1}$$

where $P(x_{m,i})$ is the probability of sample $x_{m,i}$ in bin X_m.

Cross-entropy can be calculated similarly. For adjacent sequential bins $X_m, X_n \in \mathbf{X}$, their cross-entropy, denoted $H(X_m, X_n)$, can be calculated as

$$H(X_m, X_n) = -\sum_{i=1}^{B} P(x_{m,i}) \log_2 P(x_{n,i}). \tag{2}$$

Kullback-Leibler Divergence (KLD), or relative entropy, can be used to find the change in entropy based on statistical similarity of the two bins [26]. For sample bins $X_m, X_n \in \mathbf{X}$, the KLD, denoted $KL_{m,n}$ can be computed as

$$KL_{m,n} = H(X_m, X_n) - H(X_m) \tag{3}$$

where $H(X_m)$ and $H(X_m, X_n)$ represent the entropy and cross-entropy defined in (1) and (2), respectively. In this work, entropy and cross-entropy are used in feature extraction from RF data to exploit the difference in the distribution of in-packet samples from samples containing the inter-packet gap. For two identical sample bins, the computed KLD will be zero as there is no relative change in entropy.

Welch's (Periodogram) Method. This method is based on short-time spectral density estimation to show frequency domain information for each sample bin. These periodograms generated from overlapping windows within each sample bin using the discrete Fourier transform (DFT). The n-th sample in the m-th window of a sample bin, denoted as $x_m(n)$, can be expressed as

$$x_m(n) \triangleq w(n)x(n + mR), \tag{4}$$

where $m = 0, 1, ..., M-1, n = 0, 1, ..., N-1$ with M being the number of windows per bin and N the number of samples per window; $x(n + mR)$ is the $(n + mR)$-th sample of the bin, with R representing the window hop size (e.g., $R = 0.5$ allows 50% window overlap) and w is the windowing function. In this work, a Hann (raised cosine) window function has been used to prevent window edge discontinuities.

Then, the periodogram, denoted as $P_m(\omega)$ for the m-th window of a sample bin at frequency ω, can be written as

$$P_m(\omega) = \frac{1}{N} \left| \sum_{n=0}^{N-1} x_m(n) e^{-j2\pi n/N} \right|^2 \tag{5}$$

where $\mathbf{x}_m = (x_m(n))_{n=0}^{N}$ is the sample vector of the m-th window with $x_m(n)$ defined in (4). For each sample bin, let $S(\omega)$ represent the average of the resulting periodograms, then $S(\omega) \triangleq \frac{1}{M} \sum_{m=0}^{M-1} P_m(\omega)$, where $P_m(\omega)$ is the periodogram calculated in (5). Since this method takes a single sample bin as input, the target feature is defined as the magnitude of the peak frequency component of each sample bin.

C. Ground Truth Analysis

The PBR results obtained by the statistical approaches discussed in Sec. III-B will be compared against two types of ground truth information: the number of packets in each transmission denoted as G and the sample index of g-th packet boundary denoted as g_{smp}.

The number of packets in each transmission, i.e., G, is known from the time of transmission and will be used to determine the overall PBR rate for each of methods discussed above. Denote the PBR rate as $\Gamma = \frac{G_{prd}}{G}$, where G_{prd} is the predicted number of packets in the stream, determined using the approaches discussed in Section III-B.

To verify individual packet boundary locations, we first determine the sample index g_{smp} and bin index g_{bin} of the g-th calculated boundary and then compare them to the ground truth boundary locations. With a fixed transmission bit rate R_{bit}^{TX} and receive sample rate R_{smp}^{RX}, the expected location of the g-th packet boundary can be predicted as, in the case of uniform packet length L_{byte}, $g_{smp} = \hat{g}_{smp} + 8gL_{byte} * \frac{R_{smp}^{RX}}{R_{bit}^{TX}}$, where $\hat{g}_{smp}$ represents the index of the starting sample of the first packet within the collected RF data.

IV. Data Collection

Based on the PBR framework discussed in Section III, a testbed has been developed using USRP software defined radios. Figure 2 shows a snapshot of the testbed, where the transmitter and receiver are implemented using USRP N210 and B210, respectively. The control host is a Dell Latitude 5491 laptop, which implements the *OTA Signal Generator* and *Agnostic RF Sink* as customized implementations in GNU Radio, and *Ground Truth Generator* as functions in Python.

Two categories of data have been generated, based on the length of the modulated packets: fixed-length packet streams, to investigate how different packet sizes are detected, and

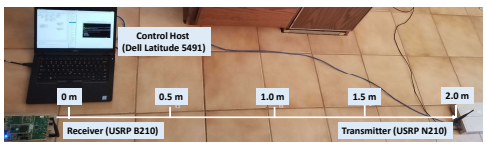


Fig. 2: A snapshot of the software-defined PBR testbed.

Modulation	Stream Type	Packet Sizes (Bytes)
BPSK	OTA (Streams 1-20)	1500 (Streams 1-5)
		2000 (Streams 6-10)
		4000 (Streams 11-15)
		Random (Streams 16-20)
	Non-OTA (Streams 101-104)	1500
		2000
		4000
		Random
GMSK	OTA (Streams 21-40)	1500 (Streams 21-25)
		2000 (Streams 26-30)
		4000 (Streams 31-35)
		Random (Streams 36-40)
	Non-OTA (Streams 105-108)	1500
		2000
		4000
		Random
8-PSK	OTA (Streams 41-60)	1500 (Streams 41-45)
		2000 (Streams 46-50)
		4000 (Streams 51-55)
		Random (Streams 56-60)
	Non-OTA (Streams 109-112)	1500
		2000
		4000
		Random
16-QAM	OTA (Streams 61-80)	1500 (Streams 61-65)
		2000 (Streams 66-70)
		4000 (Streams 71-75)
		Random (Streams 76-80)
	Non-OTA (Streams 113-116)	1500
		2000
		4000
		Random
QPSK	OTA (Streams 81-100)	1500 (Streams 81-85)
		2000 (Streams 86-90)
		4000 (Streams 91-95)
		Random (Streams 96-100)
	Non-OTA (Streams 117-120)	1500
		2000
		4000
		Random

TABLE I: Summary of generated datasets.

random packet streams, to model more realistic network behaviors. The former consists of uniform packets of lengths of 1500, 2000, or 4000 bytes. The latter consists of packets with lengths determined by a known pseudorandom sequence, with a minimum length of 48 bytes and a maximum length of 4080 bytes. For each type of stream, five of the most widely-used digital modulations have been considered, including BPSK, QPSK, GMSK, 8-PSK, and 16-QAM. The generated samples are first saved as arrays of complex *Non-OTA* data and sent to the *Ground Truth Generator* prior to OTA transmission.

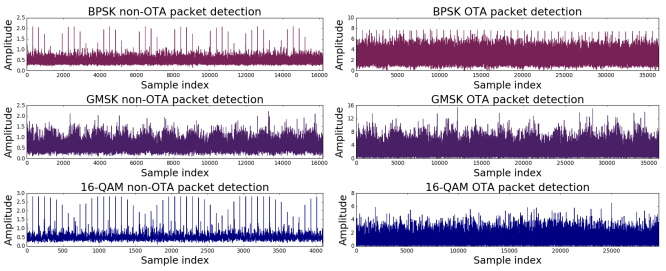
On the receiver side, the OTA data is collected and preprocessed for PBR analysis. The data is preprocessed as described in Section III, including quantization and binning of radio signals into vectors of sizes 50 and 100 samples. Each of the preprocessed datasets is then used to further generate three feature sets consisting of complex I/Q data, received signal amplitude, and short-time frequency spectrum.

In total 100 datasets of OTA radio signals have been collected, each consisting of around 3,000,000 samples, as well as 20 sets of non-OTA data each containing between 400,000 and 1,600,000 samples. The collected datasets are summarized in Table I.

V. Performance Analysis

In this section, we evaluate the PBR approaches discussed in Section III, by comparing them against ground truths in terms of PBR rate and accuracy in a variety of conditions. The PBR rate refers to the percentage of packets detected successfully, while the PBR accuracy is defined as the distance between the predicted and the ground truth packet boundaries. Next, we study two PBR examples for non-OTA and OTA data in Figs. 3(a) and 3(b), respectively.

Figure 3(a) shows an example of the PBR results for Welch's method on non-OTA data with packet size of 2000 bytes and modulation types of BPSK (top), GMSK (middle) and 16-QAM (bottom). The output values of Welch's Method



(a) (b)

Fig. 3: Example PBR output using sensed signals (Welch's method). (a) Example of non-OTA data; (b) Example of sensed OTA data.

is proportional to the frequency content of the baseband signal. In Fig. 3(a), it can be found that the output values of Welch's Method range from 0 to 3. By comparing with the ground truth obtained in Section III, we found that each of the major peaks in the three plots corresponds to a packet boundary, which verifies the effectiveness of Welch's Method in PBR.

The corresponding results for OTA data is reported in Fig. 3(b). In the test cases, the output values of Welch's method range from 0 to 16. Compared to non-OTA results in Fig. 3(a), the clarity of the peak values has been somewhat degraded by channel effects inherent to OTA transmissions.

PBR Rate Analysis. In the following three experiments, we study the PBR rate of the 11 approaches discussed in Section III. The results are reported in Figs. 4, 5, and 6.

In Fig. 4, we plot the PBR rate for QPSK modulated packets of size 1500, 2000, 4000 bytes as well as random size. The bin size has been set to 100 samples. The results are obtained by averaging over 5 transmission ranges as shown in Fig. 2. It can be seen that the PBR rate ranges from 30% to 99% with different parameters, and that in general, a higher PBR rate can be achieved with longer packets. For example, with packet size of 1500 bytes, as shown in Fig. 4, the most accurate method is KLD, which can detect 76% of packets. The corresponding PBR rate is 99% for packet sizes of both 2000 and 4000 bytes. Similarly, a very good PBR performance can also be achieved by the distance correlation approach and variance approach, with a PBR rate of 97% for both approaches with packet size of 4000 bytes.

From Fig. 4, it can also be found that the PBR rate is significantly degraded for all 11 approaches when the packets are generated with random length. For example, the PBR rate is only 30%, 35%, 36%, 38% and 40% for the KLD, cross-correlation, variance, covariance, and distance correla-

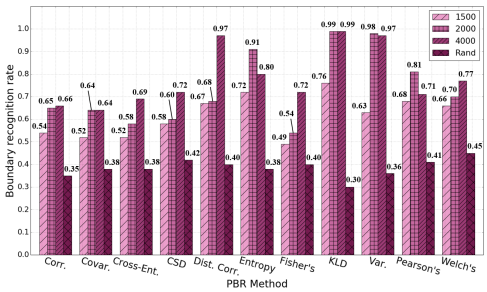


Fig. 4: PBR rate for QPSK-modulated data streams with packet size of 1500, 2000, 4000 bytes and random size.

tion approaches, respectively. The most accurate method for random-sized packets is Welch's method, which can detect 45% of packet boundaries. This experiment implies that i) with the tested existing statistical approaches, we can expect PBR rates between 30% and 100% in real wireless networks, where packets are usually generated according to a fixed set of packet lengths; and ii) in the presence of unintended interference, it can be an effective security measure to randomize packet lengths in order to reduce the probability of detection.

In Fig. 5, we plot the PBR rate of the KLD approach considering 5 modulations and packets of sizes of 1500, 2000, and 4000 bytes as well as random size. The bin size has been set to 100 samples. We consider the KLD approach in this experiment because it achieves the highest PBR rate in most of the tested cases. It can be seen that it can achieve a PBR rate of 87%, 87%, 70%, and 99% with fixed packet lengths for BPSK, 8-PSK, 16-QAM, and QPSK modulations, respectively. The corresponding PBR rate with random packet lengths is 41%, 43%, 45%, and 30%. The exception is GMSK, for which a PBR rate of less than 50% can be achieved even with fixed packet lengths; for this modulation, according to our experiments the most effective PBR approaches are Welch's Method and the CSD approach, which can achieve a PBR rate of at least 60%. From this experiment we can see that there is no "one-size-fits-all" approach for PBR in wireless networks with time-varying or unknown modulation types.

In Fig. 6(a), we further plot the PBR rate of the KLD approach with different transmission distances, considering the same modulation and packet size as in Fig. 5. It can be seen that the KLD approach can achieve a consistent PBR rate for most modulations. For example, a PBR rate of 82%, 80%, 82%, 82%, and 82% can be achieved for QPSK modulation at 50 samples per bin as the transmission distance increases from 0.5 meters to 2.5 meters. Similarly, almost a 100% PBR rate can be achieved at 100 samples per bin. The same trend can also be observed for other modulations, except 16-QAM. As shown in the right figure, the PBR rate of 16-QAM decreases from 92% to 50% as transmission distance increases from 0.5 meters to 2.5 meters. This is because high-order modulations can result in increased sensitivity to channel effects such as noise, fading, etc. We also notice that this sensitivity is accentuated with larger sample bins. As shown in the left-hand side plot, a more consistent PBR rate can be achieved for 16-QAM with smaller bin sizes. Therefore, smaller bin sizes should be used for high-order modulations at long transmission ranges for more consistent PBR performance.

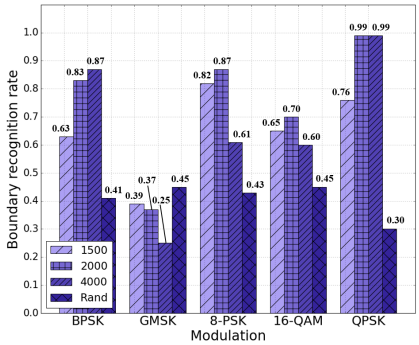
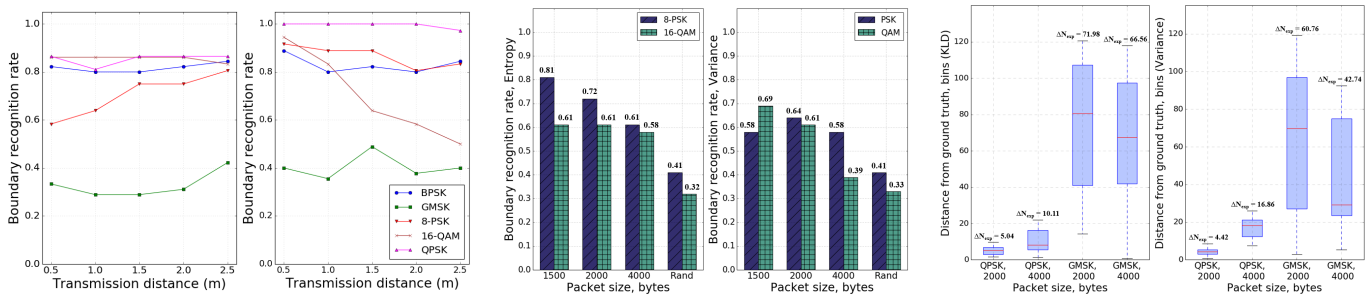


Fig. 5: Analysis of modulation for KLD, 2000-byte packets.

In Fig. 6(b), we further study the PBR rate achievable with different packet sizes by considering 8-PSK and 16-QAM as example modulations for entropy and variance approaches. In general, a higher PBR rate can be achieved with 8-PSK modulation than with 16-QAM modulation in almost all the tested cases. For example, a PBR rate of 81% can be achieved for 8-PSK using the entropy method and packet size of 1500 bytes, which is 61% for 16-QAM. This implies that in the context of protocol-agnostic sensing, higher-order modulation schemes can be used to reduce the probability of detection. It is also found from the left-hand side of the figure that for the entropy approach, a consistent PBR rate can be achieved for 16-QAM with different static packet sizes; in contrast, the right-hand side of the figure shows that a consistent PBR rate can be achieved for 8-PSK modulation using the variance approach. Due to the prevalence of packets smaller than 1500 bytes within each random-length set (∼40%), poor performance on traffic with randomized packet length is expected given the performance degradation observed with smaller packet sizes for most observed methods. From these results, it is further verified that no single statistical approach to PBR will perform well across all the tested variables.

PBR Accuracy Analysis. In this experiment, we study the PBR accuracy performance, taking KLD and variance approaches as an example. As discussed in the beginning of this section, PBR accuracy is defined as the relative difference between the predicted and ground truth packet boundaries. This accuracy measure is determined by comparing the ground truth boundaries to each predicted boundary, and is defined as $\Delta G_{prd} = \frac{1}{G_{prd}} \sum_{n=1}^{G_{prd}} \mid g_{bin}(n) - g_{bin,prd}(n) \mid$, where G_{prd} is the predicted number of packets in a sample stream, $g_{bin}(n)$ is the ground truth bin location of the n-th boundary, and $g_{bin,prd}(n)$ is the corresponding predicted bin location.

The results are reported in Fig. 6(c), where QPSK and GMSK modulations are considered using KLD and variance methods for packet sizes of 2000 and 4000 bytes. It can be seen from the left-hand side figure that the KLD-based method accurately predicts QPSK packets, while the achievable prediction accuracy is significantly lower for GMSK-modulated packets. For example, we observe a ΔG_{prd} of 5.04 bins (each of 50 samples) for KLD method on QPSK-modulated packets of size 2000 bytes, which is 71.98 bins for GMSK-modulated packets. Similar results can be observed in the right-hand side of Fig. 6(c) for the variance approach. The sampling rate was configured in the receiver USRP to be 1,000,000 samples per second. Therefore, an offset of 5.04 bins corresponds to 252 μs, and 3.6 ms for 71.98 bins offset. While these ground truths are not attainable in a protocol-agnostic context, this is an important metric by which to validate PBR algorithms. This implies that existing statistical approaches are more suitable for PBR detection in low data rate wireless systems with long packets, for example LoRaWAN and LTE networks.



(a) (b) (c)

Fig. 6: Performance metrics of various test configurations. (a) PBR rate against transmission distance with bin size of 50 (left) and 100 (right) samples; (b) PBR rates with different packet sizes for entropy (left) and variance (right) approaches; and (c) PBR accuracy of KLD (left) and variance (right) approaches.

VI. Conclusions and Future Work

In this work, we have established benchmarks for a new RF sensing technique called *protocol-agnostic cross-layer sensing*, taking link-layer time-domain PBR based on physical-layer raw RF samples as an example. We analyzed experimentally the effectiveness of eleven statistical sensing approaches in terms of PBR rate and accuracy by generating a dataset of RF samples, considering a wide set of modulation types and packet lengths. It is found that *none* of these statistical approaches can achieve consistent good PBR results in all scenarios. The dataset collected in this work and the performance analysis can provide a benchmark for research in protocol-agnostic sensing. In future work we will study protocol-agnostic sensing in scenarios with time-varying packet lengths and in the presence of interference, by jointly considering packet boundary and other features such as frequency and modulation type.

References

[1] F. Jin and T. Qiu, "Low Complexity Compressive Wideband Spectrum Sensing in Cognitive Radio," in *Proc. of CITS*, Colmar, France, August 2018.

[2] L. Zhang and Y. Liang, "Joint Spectrum Sensing and Packet Error Rate Optimization in Cognitive IoT," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7816–7827, October 2019.

[3] L. Chen, "Security and privacy on physical layer for wireless sensing: A survey," *Security and Privacy*, vol. 1, no. 5, pp. 1–10, April 2018.

[4] Y. Zou, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, May 2016.

[5] J. Du, H. Huang, X. J. Jing, and X. Chen, "Cyclostationary feature based spectrum sensing via low-rank and sparse decomposition in cognitive radio network," in *Proc. of ISCIT*, Qingdao, China, September 2016.

[6] A. Ali and W. Hamouda, "Advances on Spectrum Sensing for Cognitive Radio Networks: Theory and Applications," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1277–1304, November 2017.

[7] L. Zhang, Y. Liang, and M. Xiao, "Spectrum Sharing for Internet of Things: A Survey," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 132–139, June 2019.

[8] M. K. Hanawal, Y. Hayel, and Q. Zhu, "Effective Utilization of Licensed and Unlicensed Spectrum in Large Scale Ad Hoc Networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 618–630, June 2020.

[9] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist, and Z. Zhang, "Low Power Wide Area Networks: A Survey of Enabling Technologies, Applications and Interoperability Needs," *IEEE Access*, vol. 6, pp. 77 454–77 473, November 2018.

[10] S. Chacko, M. D. Job *et al.*, "Security mechanisms and Vulnerabilities in LPWAN," in *Proc. of IOP Conference Series: Materials Science and Engineering*, Kerala State, India, April 2018.

[11] S. Maru and T. X. Brown, "Packet classification in co-mingled traffic streams," in *Proc. of IEEE Workshop on Secure Network Protocols*, Princeton, New Jersey, USA, December 2009.

[12] T. Dempsey, G. Sahin, Y. T. Morton, and C. M. Hopper, "Intelligent sensing and classification in ad hoc networks: a case study," *IEEE Aerospace and Electronic Systems Magazine*, vol. 24, no. 8, pp. 23–30, August 2009.

[13] S. Wang, W. Guo, and M. D. McDonnell, "Downlink interference estimation without feedback for heterogeneous network interference avoidance," in *Proc. of ICT*, Lisbon, Portugal, June 2014.

[14] V. Bhardwaj, T. Goel, and G. Mahendru, "A Novel Wavelet Packet Based Direction of Arrival Estimation for Spectrum Sensing in Cognitive Radio Networks," in *Proc. of SPIN*, Noida, India, September 2018.

[15] F. Liu, M. W. Marcellin, N. A. Goodman, and A. Bilgin, "Compressive Sampling for Detection of Frequency-Hopping Spread Spectrum Signals," *IEEE Transactions on Signal Processing*, vol. 64, no. 21, pp. 5513–5524, August 2016.

[16] W. Xu, S. Wang, S. Yan, and J. He, "An efficient wideband spectrum sensing algorithm for unmanned aerial vehicle communication networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1768–1780, November 2018.

[17] T. Datta, S. T. Anindo, and S. S. Alam, "Detection Performance Analysis for Wideband Cognitive Radio Network: A Compressive Sensing Approach," in *Proc. of IC4ME2*, Rajshahi, Bangladesh, July 2019.

[18] K. Sherbin and V. Sindhu, "Cyclostationary Feature Detection for Spectrum Sensing in Cognitive Radio Network," in *Proc. of ICCS*, Madurai, India, May 2019.

[19] B. Paul, A. R. Chiriyath, and D. W. Bliss, "Survey of RF communications and sensing convergence research," *IEEE Access*, vol. 5, pp. 252–270, December 2016.

[20] C. Zhang, L. Yang, and X. Wang, "Discrete wavelet neural network group system for digital modulation recognition," in *Proc. of IEEE ICCSN*, Xi'an, China, September 2011.

[21] T. O'Shea, J. Corgan, and T. Clancy, "Convolutional Radio Modulation Recognition Networks," in *Proc. of International conference on engineering applications of neural networks*, Aberdeen, United Kingdom, September 2016.

[22] T. J. O'Shea, T. Roy, and T. C. Clancy, "Over-the-Air Deep Learning Based Radio Signal Classification," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 168–179, January 2018.

[23] Q. Zhang, Z. Xu, and P. Zhang, "Modulation recognition using wavelet-assisted convolutional neural network," in *Proc. of ATC*, Ho Chi Minh City, Vietnam, December 2018.

[24] X. Li, F. Dong, S. Zhang, and W. Guo, "A survey on deep learning techniques in wireless signal recognition," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[25] A. K. C. Wong and M. You, "Entropy and Distance of Random Graphs with Application to Structural Pattern Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. PAMI-7, no. 5, pp. 599–609, September 1985.

[26] A.-K. Seghouane, "A Kullback–Leibler divergence approach to blind image restoration," *IEEE Transactions on Image Processing*, vol. 20, no. 7, pp. 2078–2083, January 2011.