INL/CON-24-78351-Revision-0

Jamming Detection for Low-Resolution SC-FDE Systems: A Machine Learning Approach

August 2024

Junghoon Kim, Miguel R. Castellanos, Robert Heath, Arupjyoti Bhuyan

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-24-78351-Revision-0

Jamming Detection for Low-Resolution SC-FDE Systems: A Machine Learning Approach

Junghoon Kim, Miguel R. Castellanos, Robert Heath, Arupjyoti Bhuyan

August 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Jamming Detection for Low-Resolution SC-FDE Systems: A Machine Learning Approach

Junghoon Kim*, Miguel R. Castellanos†, Arupjyoti Bhuyan‡, and Robert W. Heath Jr.§
*Motorola Mobility, Chicago, IL, USA (email: junghoon@motorola.com)
†Electrical and Computer Engineering, North Carolina State University, NC, USA (email: mrcastel@ncsu.edu)
‡Idaho National Laboratory, ID, USA (email: arupjyoti.bhuyan@inl.gov)
§Electrical and Computer Engineering, University of California, San Diego, CA, USA (email: rwheathjr@ucsd.edu)

***Abstract*—Jammers interfere with communication between base stations (BSs) and legitimate users, leading to degradation of wireless system performance. Our study focuses on jamming detection for wideband single-carrier frequency domain equalization (SC-FDE) systems with low-resolution analog-to-digital converters (ADCs). In such systems, jamming detection is challenging because traditional analytical approaches cannot be directly applied due to the delay dispersion in wideband channels and the non-linearity induced by low-resolution ADCs. We propose a machine learning (ML)-based jamming detection method that directly uses the quantized receive signals. Significantly, our ML-based detector can be integrated into existing standard frameworks, such as unique word (UW)-based SC-FDE systems, as it uses existing pilots without requiring additional pilots for jamming detection. Through numerical simulations, we show that two or more bits provide satisfactory performance compared to unquantized scenarios. Additionally, we demonstrate that using more and well-separated pilot symbols improves performance.**

I. INTRODUCTION

Wireless networks are vulnerable to jamming attacks due to the exposed nature of wireless links. Jamming signals disrupt communication between BSs and legitimate users by introducing errors in synchronization, channel estimation, and signal detection. This disruption ultimately leads to a decrease in data rate performance [1]. To counteract jamming, it is crucial for communication systems to detect the presence of jamming signals and develop effective jamming detection strategies, as it precedes any subsequent mitigation efforts.

For large bandwidth systems, communication systems experience wideband channels and prefer using low-resolution ADCs to reduce implementation and processing costs [2]. In wideband channels, jamming detection is further complicated by the multiple taps of channel delays. Furthermore, in low-resolution systems, jamming detection becomes more challenging due to the non-linearity introduced by low-resolution ADCs [2]. This makes the application of linear communication processing techniques impractical. In this paper, we study both low-resolution and wideband aspects for jamming detection. We focus on SC-FDE systems for wideband models, which are adopted for uplink in wireless standards, e.g., long-term evolution (LTE) [3] and IEEE 802.11ad [4]. These systems offer the advantage of a low peak-to-average power ratio, compared to orthogonal frequency division multiplexing (OFDM) systems.

Prior work on jamming detection mostly focused on narrowband channels [5]–[7], while some work discussed either low-resolution systems [8] or wideband channels [9]–[11]. For narrowband channels, several analytical methods were developed, such as hypothesis testing [5], random matrix theory-based approaches [6], and channel-specific detection methods [7]. Recently, jamming detection was studied for narrowband system with a one-bit comparator ADC [8]. For wideband channels, a self-contamination approach was proposed when the jammer uses the same pilot sequence as the transmitter [9]. For OFDM systems, a hypothesis testing-based method using pilot symbols in the frequency domain is proposed in [10]. In [11], a ML-based approach was proposed, using radiometric features, such as signal-to-noise ratio, energy threshold, and key OFDM parameters. The work [5]–[11], however, cannot be directly applied for SC-FDE systems with low-resolution ADCs, as the wideband and low-resolution components were not discussed jointly. Furthermore, the jamming detection methods tailored for OFDM systems [10], [11] cannot be directly transferred to SC-FDE systems.

In this paper, we establish a comprehensive jamming detection framework that uses as input the quantized receive signals. We then propose a ML-based jamming detector to extract underlying features from the quantized receive signals. We train the ML-based detector across an expected range of jamming powers, ensuring its robustness against unknown/various jamming environments. Furthermore, we employ a weighted binary cross-entropy loss function for training, and thus the detector offers flexibility in obtaining diverse trade-offs between detection and false alarm rates. Through simulations, we show that using two or more bits yields satisfactory performance. Furthermore, performance improves when the pilots are well-separated, emphasizing the importance of pilot configuration for jamming detection.

II. SC-FDE SYSTEM WITH LOW-RESOLUTION ADCS

We first discuss the model for a SC-FDE system equipped with low-resolution ADCs in Sec. II-A. We then formulate an optimization problem for jamming detection in Sec. II-B.

A. SC-FDE system model

We consider a communication system where a transmitter with a single antenna communicates with a receiver with $N_{\rm rx}$ antennas. The system uses SC-FDE with $N_{\rm sc}$ sub-carriers. We define $\mathcal{S}$ as a set of symbols supported by specific modulation, e.g., quadrature phase-shift keying (QPSK). We denote the transmit symbol at time n during one block as $s[n] \in \mathcal{S}$, $n = 0, ..., N_{\text{sc}} - 1$. The transmit signal in the time domain is

$$\boldsymbol{s} = [s[0], ..., s[N_{\text{sc}} - 1]]^{\mathsf{T}} \in \mathbb{C}^{N_{\text{sc}} \times 1}. \tag{1}$$

We assume that N_{p} symbols are allocated as a pilot sequence at the beginning of the transmit signal, where $N_{\text{p}} < N_{\text{sc}}$. These pilot symbols, $\{s[n]\}_{n=0}^{N_{\text{p}}-1}$, are mutually known to both the transmitter and receiver and can be used for jamming detection at the receiver. Pilot symbols, known as UWs, are inserted at the beginning of each data block in SC-FDE systems according to IEEE 802.11ad [4]. These UWs replace the cyclic prefix (CP) to mitigate inter-symbol interference (ISI) across blocks. With the same overhead required as CP, the UWs can serve additional purposes including time/frequency synchronization, channel estimation, and phase tracking. In this paper, we propose that the receiver performs jamming detection using these pilot symbols.

We consider a scenario where a single-antenna jammer interferes with the communication between the transmitter and receiver. We denote the jamming symbol at time n as $q[n] \in \mathbb{C}$. The jamming signal in the time domain is then

$$\boldsymbol{q} = [q[0], ..., q[N_{\text{sc}} - 1]]^{\mathsf{T}} \in \mathbb{C}^{N_{\text{sc}} \times 1}. \tag{2}$$

Modern jammers use a variety of techniques to interfere with communication links [1]. We assume that the jammer has access to the transmit symbol set $\mathcal{S}$. This is reasonable given the wide availability of transmit protocols, e.g., long-term evolution (LTE) [3] or Wi-Fi [4]. In this paper, we focus on the feature of constant jamming. The jammer selects a symbol from $\mathcal{S}$ and uses it to interfere with the system as in [7]. We assume that jamming occurs at least in a block-by-block period, not symbol-by-symbol. The receiver then aims to detect jamming for the data block period of length N_{sc}, where the jamming signal is constant over the data block period, i.e., $q[n] = q \in \mathcal{S}$, $n = 0, ..., N_{\text{sc}} - 1$. We assume that the jammer uses the same carrier frequency as the transmitter to deliver a maximum jamming power to the system.

For wideband channels, we define the delay-d transmitter-receiver channel [12] as $\boldsymbol{h}[d] \in \mathbb{C}^{N_{\text{rx}} \times 1}$. Similarly, we define the jammer-receiver channel as $\boldsymbol{g}[d] \in \mathbb{C}^{N_{\text{rx}} \times 1}$. We denote the maximum delay spread of the channel in symbol intervals as D, which leads to $d = 0, ..., D$. To represent a comprehensive signal model incorporating the jammer, we define the variable $\psi \in \{0, 1\}$ to indicate the presence of jamming, where $\psi = 1$ means that jamming exists, while $\psi = 0$ means that jamming does not exist. Let $p_{\text{tx}} \in \mathbb{R}$ denote the transmit power, $p_{\text{jam}} \in \mathbb{R}$ denote the jamming power, and $\boldsymbol{w}[n] \in \mathbb{C}^{N_{\text{rx}} \times 1}$ denote the noise vector with a complex Gaussian distribution $\mathcal{N}_{\mathbb{C}}(\boldsymbol{0}, \sigma^2 \boldsymbol{I})$. The receive symbol at time n is

$$\begin{aligned} \boldsymbol{y}[n] &= \sum_{d=0}^{D} \boldsymbol{h}[d] \sqrt{p_{\text{tx}}} s[n-d] \\ &+ \psi \sum_{d=0}^{D} \boldsymbol{g}[d] \sqrt{p_{\text{jam}}} q[n-d] + \boldsymbol{w}[n] \in \mathbb{C}^{N_{\text{rx}} \times 1}. \end{aligned} \tag{3}$$

If $\psi = 0$, the received signal is not jammed while, when $\psi = 1$, the receiver observes jamming interference over the frequency selective channel. We note that the D symbols from the previous data block, $s[-D], ..., s[-1]$, introduce ISI to the symbols in the current block. To prevent ISI to the data symbols, we assume that the number of pilot symbols or UWs, N_{p}, is not smaller than the channel delay D, i.e., $N_{\text{p}} \geq D$.

We consider a fully-digital receiver with b-bit ADCs that quantize the real and imaginary parts of the receive signal separately for each antenna. We represent the b-bit quantization effect as the function $\mathcal{Q}_b(\cdot)$, which is applied component-wise and separately to the real and imaginary parts. The quantized received signal at time n is

$$\boldsymbol{z}[n] = \mathcal{Q}_b(\boldsymbol{y}[n]). \tag{4}$$

In this paper, we employ uniform mid-rise quantization. Similar to previous work, e.g., [2], we assume that the average receive power at each antenna can be estimated before the ADC by automatic gain control (AGC), and that the quantization stepsize in $\mathcal{Q}_b(\cdot)$ can be calculated accordingly. Since the receive signal in (3) may contain jamming signals, the average powers will be affected by the jamming power and the frequency of jamming occurrence. We consider these factors to determine the stepsize for simulations in Sec. IV.

B. Problem formulation for jamming detection

The objective of the receiver is to determine the presence of jamming given $\{\boldsymbol{z}[n]\}_{n=0}^{N_{\text{sc}}-1}$. We denote the number of time steps used for jamming detection as $N_{\text{det}} \in \{1, ..., N_{\text{sc}}\}$, and the receiver uses $\{\boldsymbol{z}[n]\}_{n=0}^{N_{\text{det}}-1}$ for this purpose. The receiver may use all the receive signals ($N_{\text{det}} = N_{\text{sc}}$) or a subset of them ($N_{\text{det}} < N_{\text{sc}}$). We discuss the impact of choosing N_{det} in the simulation section, Sec. IV. We denote the receiver's inference of ψ as $\hat{\psi} \in \{0, 1\}$, where $\hat{\psi} = 1$ (0) means that the receiver declares that (no) jamming exists. Defining the functional form of a detection algorithm as $f(\cdot)$, we express the input-output relationship for jamming detection as $\hat{\psi} = f(\{\boldsymbol{z}[n]\}_{n=0}^{N_{\text{det}}-1})$.

We quantify two different error rates in jamming detection: (i) missed detection rate, $P_{\text{MD}} = \Pr[\hat{\psi} = 0 | \psi = 1]$, and false alarm rate, $P_{\text{FA}} = \Pr[\hat{\psi} = 1 | \psi = 0]$. Missed detection occurs when the detector incorrectly declares that no jamming exists ($\hat{\psi} = 0$) when jamming is present ($\psi = 1$). On the other hand, false alarm occurs when the detector incorrectly declares that jamming exists ($\hat{\psi} = 1$) when there is no actual jamming ($\psi = 0$). Note that there exists a trade-off between minimizing P_{MD} and P_{FA}. This implies that it is not possible to simultaneously minimize both rates; an adjustment made to reduce one tends to increase the other.

To account for the balance between these two distinct errors, we aim to minimize the missed detection rate (i.e., maximizing the detection rate, $P_{\text{D}} = 1 - P_{\text{MD}}$) given a constraint on false alarm rate. We denote the acceptable false alarm threshold for our communication system as $\epsilon \in [0, 1]$. Then, we can formulate the optimization problem as

$$\underset{f(\cdot)}{\text{Maximize}}\ P_{\text{D}} \quad \text{subject to } P_{\text{FA}} \leq \epsilon. \tag{5}$$

Our primary objective is to develop detectors that yield high detection rates for every false alarm rate. Designing the jamming detector $f(\cdot)$ in (5) presents challenges because existing techniques, such as hypothesis testing, cannot be directly applied. This is because analyzing the receive signal model is challenging due to the non-linearity introduced by low-resolution ADCs and the multiple channel taps in wideband channels. In this paper, we propose a ML framework for jamming detection in low-resolution SC-FDE systems in Sec. III.

III. Jamming detection with machine learning

We propose to exploit deep neural networks (DNNs) to effectively extract latent features from quantized receive signals for jamming detection. In Sec. III-A, we first discuss the input-output model for the DNN-based detector. We then discuss two distinct phases: (i) the training phase in Sec. III-B, during which the DNN is trained using training data, and (ii) the inference phase in Sec. III-C, during which the trained DNN is utilized for inference for jamming detection.

A. Input-output model

We adopt a fully-connected neural network with two hidden layers. The first hidden layer consists of L_1 neurons and the second layer has L_2 neurons. The input of the DNN is the quantized signals, i.e., $\{\boldsymbol{z}[n]\}_{n=0}^{N_{\text{det}}-1}$. We use the real and imaginary parts separately, and thus the input size is $2N_{\text{rx}}N_{\text{det}}$. Note that the pilot symbols are not inputs to the DNN, and thus the receiver does not need prior knowledge of them. However, the characteristics of the pilot symbols are implicitly captured in the receive signals. At the output layer, we use the sigmoid activation function to capture the jamming detection problem as a binary classification problem [13], resulting in an output range between 0 and 1. By denoting the jamming detector with learnable parameters $\boldsymbol{\theta}$ as $f_{\boldsymbol{\theta}}(\cdot)$, we can represent the input-output relationship as $\tilde{\psi} = f_{\boldsymbol{\theta}}(\{\boldsymbol{z}[n]\}_{n=0}^{N_{\text{det}}-1}) \in (0,1)$. In the following subsections, we will discuss how to train the detector $f_{\boldsymbol{\theta}}(\cdot)$ and how to conduct jamming detection.

B. Training stage

We first denote the number of data blocks for training as N_{tr}. The k-th data block is denoted by $\mathcal{T}^{(k)} = \{\{\boldsymbol{z}^{(k)}[n]\}_{n=0}^{N_{\text{det}}-1}, \psi^{(k)}\}$, for $k = 0, ..., N_{\text{tr}}-1$. Here, $\psi^{(k)} \in \{0,1\}$ denotes the label of the k-th data block, where $\psi^{(k)} = 1$ when jamming exists while $\psi^{(k)} = 0$ when no jamming exists. The input $\{\boldsymbol{z}^{(k)}[n]\}_{n=0}^{N_{\text{det}}-1}$ denotes the quantized receive signals of the k-th data block. The set of entire data blocks for training is then denoted by $\mathcal{T} = \{\mathcal{T}^{(k)}\}_{k=0}^{N_{\text{tr}}-1}$. We consider two types of data blocks: (i) non-jamming data blocks with size $N_{\text{tr},0}$ and (ii) jamming data blocks with size $N_{\text{tr},1}$, where $N_{\text{tr}} = N_{\text{tr},0} + N_{\text{tr},1}$. For the non-jamming case, the quantized receive signals, $\{\boldsymbol{z}^{(k)}[n]\}_{n=0}^{N_{\text{det}}-1}$, are generated by setting $\psi^{(k)} = 0$ in (3)-(4) for $k = 0, ..., N_{\text{tr},0}-1$. For the jamming case, the quantized receive signals are generated by setting $\psi^{(k)} = 1$ in (3)-(4) for $k = N_{\text{tr},0}, ..., N_{\text{tr}}-1$.

We incorporate two distinct features into training to improve robustness and flexibility for jamming detection. First, we train our ML-based detector to be robust to unknown jamming-related parameters. To this end, we consider an expected range of jamming power, $[p_{\text{jam}}^{\min}, p_{\text{jam}}^{\max}]$, and generate the data blocks for training within this range using a specific distribution. Consequently, it does not require any modifications when faced with various jamming conditions. Setting the range of jamming power is reasonable since very low jamming power has minimal impact on the system, while very high jamming power can be easily detected, for example, using energy detection, without a sophisticated jamming detection method. The trained ML-based detector is then expected to perform well under various jamming powers and channels in the low-resolution wideband SC-FDE system.

We next discuss flexibility for jamming detection. To facilitate supervised learning, we reformulate (5) to the problem with a single objective function and no constraint. This is expressed as $\underset{f_{\boldsymbol{\theta}}(\cdot)}{\text{Minimize}}\ \alpha P_{\text{MD}} + (1-\alpha)P_{\text{FA}}$, where $\alpha \in [0,1]$ is the weight coefficient that can be chosen based on the threshold ϵ in (5). To train the detector that minimizes $\alpha P_{\text{MD}} + (1-\alpha)P_{\text{FA}}$, we adopt the weighted binary cross entropy (BCE) loss function [14]. We denote the inference output of the k-th data by the ML-based detector as $\tilde{\psi}^{(k)}$. The weighted BCE loss is then expressed as

$$L = -\sum_{k=0}^{N_{\text{tr}}-1} \left(\alpha\psi^{(k)} \log\tilde{\psi}^{(k)} + (1-\alpha)(1-\psi^{(k)})\log(1-\tilde{\psi}^{(k)})\right). \tag{6}$$

The weighted BCE loss is commonly employed for training with unbalanced data, ensuring a balanced classification outcome for various inference data [14]. In our case, we use the weighted BCE loss to obtain different trade-offs between P_{MD} and P_{FA}. A large weight coefficient encourages the detector to prioritize improving detection over reducing false alarms, while a small weight encourages the opposite behavior. The choice of α that yields a desirable value of P_{FA} (or ϵ) is challenging due to the complexity of explicitly analyzing neural networks. The practical approach is to train with different α values, resulting in various models, each satisfying a distinct P_{FA}. Therefore, by adopting the weighted BCE loss, we obtain the flexibility to train models with different trade-offs between detection rates and false alarm rates.

C. Inference stage

For inference, the receiver converts the sigmoid function output $\tilde{\psi} \in (0,1)$ to the final inference variable $\hat{\psi} \in \{0,1\}$ by setting $\hat{\psi} = 1$ when $\tilde{\psi} \geq 0.5$, and $\hat{\psi} = 0$ when $\tilde{\psi} < 0.5$, following classical binary classification [13]. We note that the false alarm rate P_{FA} is independent of the jamming signal or its characteristics, since this rate is a metric for the non-jamming scenario. Selecting a detector with a predefined P_{FA} does not require any knowledge of the jamming details. By using the weighted BCE loss with different weight coefficients for training, the receiver can develop and store multiple detectors each with distinct value of P_{FA}. To decide which detector to use during the inference stage, the receiver can assess their performance in terms of P_{FA} using non-jamming validation data. Then, the receiver can choose the detector that aligns with a desired value of P_{FA}. To reduce the storage overhead, the receiver can be selective and store only those detectors falling within a specified range of P_{FA}, for instance, excluding detectors with a high P_{FA} exceeding 20%.

Using ML offers a significant advantage in terms of parameter knowledge compared to existing analytical approaches, such as hypothesis testing. Hypothesis testing typically requires knowledge of specific parameters including jamming powers, jammer-receiver channel characteristics, and quantization effects to formulate a testing formula. In contrast, our ML approach does not require any of these parameters specifically.

IV. Numerical experiments

In this section, we first describe the parameter setup and wideband channel models for simulations in Sec. IV-A. We then evaluate the performance of our ML-based jamming detector for low-resolution SC-FDE systems in Sec. IV-B.

A. Simulation setup

We consider $D = 4$ and the set of QPSK symbols $\mathcal{S} = \{e^{j\pi/4}, e^{j3\pi/4}, e^{j5\pi/4}, e^{j7\pi/4}\}$. These choices align with the IEEE 802.11 standard [4]. We consider $p_{\text{tx}} = 100$mW and $q = e^{j\pi/4}$. The noise power is set to $\sigma^2 = -90$dBm, which is valid when a 20MHz bandwidth is used for the system. The range of the jamming power is set to $[p_{\text{jam}}^{\min}, p_{\text{jam}}^{\max}] = [10,\ 300]$mW. For the DNN, we use $L_1 = 300$ and $L_2 = 100$. Each hidden layer consists of linear layer followed by the rectified linear unit (ReLu) activation function at each neuron. For training, we consider the Adam optimizer and $N_{\text{epoch}} = 100$ epochs. The number of data blocks for training is $N_{\text{tr}} = 3 \times 10^6$, where $N_{\text{tr},0} = 1.5 \times 10^6$ and $N_{\text{tr},1} = 1.5 \times 10^6$. For the jamming data, we consider the jamming power from the finite set $\mathcal{P}_{\text{J}} = \{10,\ 50,\ 100,\ 200,\ 300\}$ in mW and generate $N_{\text{tr},1}/|\mathcal{P}_{\text{J}}| = 3 \times 10^5$ data blocks for each power case. The data blocks for validation comprises 5% of the data blocks for training. The total number of data blocks for testing is $N_{\text{test}} = 3 \times 10^4$ that consists of the non-jamming and jamming cases equally. For realistic choice of stepsizes of ADCs in jammed systems, we consider a scenario where jamming occurs with a probability of 30% in the system with power randomly chosen from the uniform distribution $\mathcal{U}[p_{\text{jam}}^{\min}, p_{\text{jam}}^{\max}]$.

We adopt a geometric wideband mmWave channel model [15], both for the transmitter-receiver and jammer-receiver channels. We consider the same pulse shaping filter for the transmitter and jammer as the root raised cosine filter, and set the roll-off coefficient to $\beta_{\text{roll-off}} = 1$ as in [12]. The number of signal path clusters, L, is following Poisson distribution with a mean of 5. The center AoAs of the L clusters are assumed to be uniformly distributed in $[0, 2\pi)$. Each cluster has 10 rays with Laplacian distributed AoAs and angle delay 5^o. We assume all rays within each cluster have the same time delays, and the time delays are generated by the uniform distribution $\mathcal{U}[0, DT_s]$, where T_s is the sampling period. The path loss of rays is generated by the large/small-scale fading factors according to the channel characteristics of frequency 2.5GHz. We consider the same parameter settings for the jammer-receiver channel, $\{\boldsymbol{g}[d]\}_{d=0}^{D}$, as the transmit-receiver channel, $\{\boldsymbol{h}[d]\}_{d=0}^{D}$, given that both the jammer and transmitter are within the receiver's range of interest. We assume that jamming exists at the synchronized timing (at the receiver based on the transmitter) and continues within the data block. We thus consider the cluster time delays of the jammer-receiver channel to follow $\mathcal{U}[0, DT_s]$. We assume no frequency offsets between the transmitter and receiver and between the jammer and receiver.

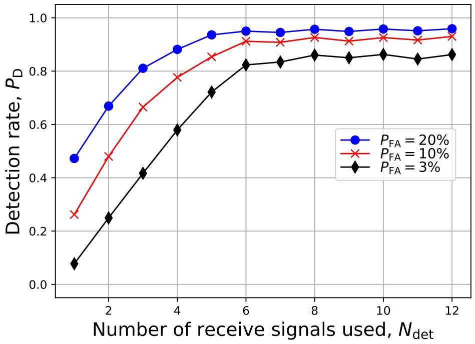

Fig. 1: Detection rate along the number of receive signals used for jamming detection when $p_{\text{jam}}/p_{\text{tx}} = 1/2$, $N_{\text{p}} = 4$, and $b = 3$. The performance improves up to using the $N_{\text{det}} = N_{\text{p}} + D = 8$ receive signals because the N_{p} pilots are contained in these signals in wideband channels with a maximum delay of D. This implies that the ML-based detector fully exploits the pilot information.

B. Wideband SC-FDE systems

Fig. 1 demonstrates the detection rate, P_{D}, across the number of receive signals used for jamming detection, N_{det}. We consider $p_{\text{jam}} = 50$mW, $N_{\text{p}} = 4$, and $b = 3$. From the plot, using more receive signals improves the detection rate rapidly up to $N_{\text{det}} = 6$, with slight increases up to $N_{\text{p}} + D = 8$. We note that the receive signal for $n < N_{\text{p}} + D$ contains pilot information since the maximum path delay is D, while the receive signal for $n \geq N_{\text{p}} + D$ does not contain any pilot information. The result in Fig. 1 confirms that using the receive signals containing known pilots yields good results up to $N_{\text{det}} = N_{\text{p}} + D = 8$. However, the performance does not improve when the receiver starts to use excessive receive signals that do not contain pilots, i.e., $N_{\text{det}} > 8$. This implies that the ML-based detector learns how to fully exploit the pilot information in delayed channels for jamming detection.

Fig. 2 demonstrates the detection rate, P_{D}, along the false alarm rate, P_{FA}, under various bit configurations when $p_{\text{jam}} = 50$mW, $N_{\text{p}} = 4$, and $N_{\text{det}} = 8$. Performance increases as the resolution of ADCs, b, increases. We observe a substantial performance loss for $b = 1$. This is because one-bit quantization cannot capture the signal intensity, which can be used as a feature for jamming detection. Overall, the detection performance is promising for the low resolution cases, $b \leq 3$. For $P_{\text{FA}} = 5\%$, the receiver achieves $P_{\text{D}} = 77\%$, 84%, 88%

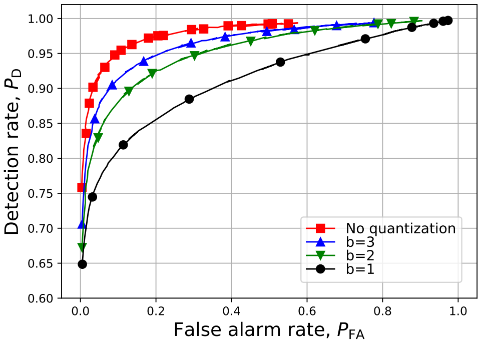

Fig. 2: Performance curve with $p_{\text{jam}}/p_{\text{tx}} = 1/2$, $N_{\text{p}} = 4$, and $N_{\text{det}} = 8$. The performance improves as the resolution of ADCs, b, increases. The overall performance of low-resolution ADCs is competitive with the non-quantization case, which shows our ML-based detector's capability to learn latent features from quantized signals for effective jamming detection.

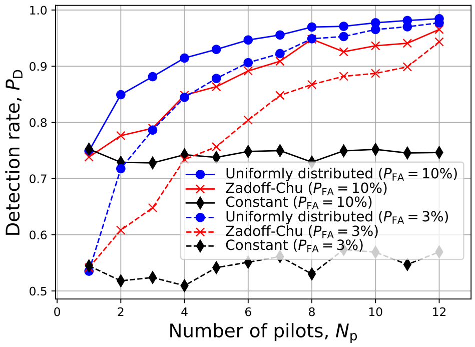

Fig. 3: Detection rate along the number of pilot symbols when $p_{\text{jam}}/p_{\text{tx}} = 1/2$, $b = 3$ and $N_{\text{det}} = N_{\text{p}} + D$. Uniformly distributed pilots yield the best performance, emphasizing the importance of using well-separated pilots. The Zadoff-Chu sequence still achieves good detection performance. This indicates that our ML-based detector can be integrated into current standard frameworks without allocating additional pilots for jamming detection.

with $b = 1, 2, 3$, and 92% for non-quantization (perfect resolution). This demonstrates our ML-based detector's ability to learn underlying features from quantized signals for jamming detection in low-resolution systems.

Fig. 3 shows the detection rate, P_{D}, along various numbers of pilot symbols, N_{p} with $p_{\text{jam}} = 50\text{mW}$, $b = 3$, and $N_{\text{det}} = N_{\text{p}} + D$. We consider three different pilot configurations: (i) uniformly distributed pilots over the unit circle in the complex domain, (ii) pilots generated by Zadoff-Chu sequence, and (iii) constant pilots as $e^{j\pi/4}$. Employing more pilots generally leads to improved performance except the constant pilot case. This indicates that using constant pilots is not effective for detecting constant jamming, and the separation of pilots is a key feature for jamming detection. Specifically, using uniformly distributed pilots yields the best detection rate among the three pilot configurations, emphasizing the importance of using well-separated pilots. Using pilots from the Zadoff-Chu sequence, commonly used in wireless standards, such as LTE [3], also provides good detection performance. This suggests that our ML-based detector can be integrated into current standard frameworks without requiring specific pilots or their configurations for jamming detection.

V. Conclusions

In this work, we proposed the ML-based jamming detector for low-resolution wideband SC-FDE systems. Through numerical simulations, we showed that our detector learns to fully exploit the pilot information in wideband channels and also learns underlying features from quantized signals for jamming detection. We also showed that performance improves when more pilots are used and these pilots are well separated. Importantly, our ML-based detector does not require additional pilots for jamming detection, making it suitable for integration into existing standard frameworks that already have pilots, such as UW-based SC-FDE systems.

References

[1] K. Grover, A. Lim, and Q. Yang, "Jamming and anti–jamming techniques in wireless networks: a survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, no. 4, pp. 197–215, Dec. 2014.

[2] J. Mo, P. Schniter, and R. W. Heath, "Channel estimation in broadband millimeter wave MIMO systems with few-bit ADCs," *IEEE Trans. Signal Process.*, vol. 66, no. 5, pp. 1141–1154, 2017.

[3] 3GPP TS 36.211, "LTE: Evolved universal terrestrial radio access (E-UTRA): Physical channels and modulation," vol. V14.2.0 Release 14, Mar. 2017.

[4] IEEE Computer Society, *IEEE 802.11 Standard for Information Technology*, pp. 1–4379, 2021.

[5] H. Akhlaghpasand, S. M. Razavizadeh, E. Björnson, and T. T. Do, "Jamming detection in massive MIMO systems," *IEEE Wirel. Commun. Lett.*, vol. 7, no. 2, pp. 242–245, Nov. 2017.

[6] J. Vinogradova, E. Björnson, and E. G. Larsson, "Detection and mitigation of jamming attacks in massive MIMO systems using random matrix theory," in *IEEE Sig. Process. Adv. Wirel. Commun. (SPAWC)*, Jul. 2016.

[7] S. Xu, W. Xu, C. Pan, and M. Elkashlan, "Detection of jamming attack in non-coherent massive SIMO systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 9, pp. 2387–2399, 2019.

[8] M. A. Teeti, "One-bit window comparator based jamming detection in massive MIMO system," in *IEEE Veh. Tech. Conference (VTC2021-Spring)*, 2021.

[9] J. K. Tugnait, "Detection of pilot spoofing attack over frequency selective channels," in *IEEE Stat. Signal Process. Workshop*, 2018, pp. 737–741.

[10] A. Ahmed, M. Zia, I. U. Haq, and H.-D. Han, "Detection of pilot contamination attack for frequency selective channels," *IEEE Access*, vol. 8, pp. 123 966–123 978, 2020.

[11] Y. Li, J. Pawlak, J. Price, K. Al Shamaileh, Q. Niyaz, S. Paheding, and V. Devabhaktuni, "Jamming detection and classification in OFDM-based UAVs via feature-and spectrogram-tailored machine learning," *IEEE Access*, vol. 10, pp. 16 859–16 870, Feb. 2022.

[12] A. Alkhateeb and R. W. Heath, "Frequency selective hybrid precoding for limited feedback millimeter wave systems," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1801–1818, 2016.

[13] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.

[14] X. Wu, D. Sahoo, and S. C. Hoi, "Recent advances in deep learning for object detection," *Neurocomputing*, vol. 396, pp. 39–64, 2020.

[15] M. R. Akdeniz, Y. Liu, M. K. Samimi, S. Sun, S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1164–1179, 2014.