Journal of Electrical Engineering, Vol. 76, No. 6, 2025, pp. 524-532
https://reference-global.com/journal/JEE

OFDM receiver design with detection of jamming or interference in LDPC-coded transmission

Tomáš Páleník, Viktor Szitkey, Martin Rakús

In this paper we present the design of our modified OFDM receiver design, which introduces a simple OFDM jamming detection method, usable for detecting several jamming attacks, including repeat-back-jamming style designs, previously deemed undetectable. This method depends on the presence of a compatible ECC, such as an LDPC, as it uses its iterative soft-decoder statistics as the basis for jamming or interference detection. The method is evaluated using our free and open source MATLAB OFDM+LDPC toolkit. Furthermore, the feasibility of the repeat-back jamming method is evaluated by measurements in a real, over-the-air radio transmission scenario with a Software-Defined Radio transmitter, receiver, and jammer implementation using USRP frontends. Measurements of the jammer latency, detrimental to the success of this attack, are presented.

Keywords: OFDM, radio transmission, jamming detection, software-defined radio

1 Introduction

Orthogonal Frequency Division Multiplexing (OFDM) has been the modulation of choice in wireless networks since the IEEE 802.11a and 3GPP Release 8 and is currently the backbone of the latest standards, such as IEEE205.11be [1] and 5G-Advanced, defined in the recent Release 18 [2]. Because of its natural resistance to multipath propagation within the context of Rayleigh and Rician fading channels, recent publiccations suggest it will likely continue to be the modulation of choice also in future 6G systems [3].

There have been many attacks on the PHY layer described in the past, focusing on various aspects of the OFDM transmission. One of the primary targets for jamming are the pilot signals, necessarily present in order for the receiver to estimate the channel state and perform Frequency Domain Equalization (FDE). The drawback of these is that the jammer must synchronize to the transmission to be able to target specific subcarriers within specific OFDM symbols in the time-frequency lattice. Other methods focus on the frame synchronization preamble or jamming a selected sub channel, such as the Physical Downlink Control Channel (PDCCH). An overview of jamming methods can be found in [4].

One of the more subtle methods of jamming, general to all OFDM transmissions, was described in [5] and is similar to the Repeat-Back-Jamming (RBJ) introduced earlier for the spread-spectrum systems. The basic principle of such a method is to exploit the known vulnerability of an OFDM transmission, where the Cyclic Prefix (CP) is inserted in the transmitter (TX), and then discarded in the receiver (RX), in order to convert the linear channel convolution to appear as a cyclic convolution. The crucial condition for this procedure to work is that the length of the CP must be greater than the length of the impulse response of the channel. Practically, this requires the CP design to accommodate the RMS value of the channel delay spread σ_τ. In [5], the jammer, if able to receive the transmitted OFDM symbol, exploits this condition and artificially constructs an extra delayed signal copy. If successful, the resulting interfering signals appear to the receiver as a multipath propagation where the delay of the last path breaks the required condition of fitting into the CP duration time, resulting in an Inter-Carrier Interference (ICI) within the received OFDM symbol. Since nothing but a copy of a transmitted symbol was used for the jamming, this attack may be considered undetectable [5]. In this paper, we describe a method able, to some extent, detect even this kind of attack,

Faculty of Electrical Engineering and Information Technology
Slovak University of Technology in Bratislava, Slovakia
martin.rakus@stuba.sk

https://doi.org/10.2478/jee-2025-0054, Print (till 2015) ISSN 1335-3632, On-line ISSN 1339-309X

provided the transmission is equipped with an iteratively decoded ECC (Error Control Code). This condition is met for most of the recent OFDM-based communications standard, since the Low-Density Parity-Check (LDPC) codes are defined for Wi-Fi since IEEE802.11-2020 [6]. Together with the polar codes, LDPC are the primary ECC also defined for the 5G New Radio specifications [2].

The paper is organized as follows: A brief summary of basic OFDM principles, fading channel transmission, and LDPC is given in the following section. A more detailed description is out of scope of this paper and can be found in [7, 8]. The third section introduces the jamming context, and its basic mathematical description. The fourth section describes our simple jammer detection method and the modified OFDM receiver design and provides MATLAB simulation results. The fifth section presents a practical methodology for evaluating the feasibility of the RBJ implementation using affordable commercially available Software-Defined Radio (SDR) hardware Universal Software Radio Peripherals (USRP) and provides the necessary latency measurement results. The last section then concludes the paper.

2 OFDM and multipath fading

2.1 Basic OFDM principles

The principle of OFDM is the conceptual demultiplexing of the data stream to many low-rate streams in the transmitter (TX), each mapped to a subcarrier, and further modulated in the digital domain, then placed on a separate frequency. The N subcarriers are spaced in the frequency domain with distance $\Delta f = 1/T$, where T is the OFDM symbol duration. This subcarrier spacing implements the orthogonality of the subcarriers, illustrated in Fig. 1. The center of each subcarrier is placed at the zero of the frequency responses of other subcarriers. This makes the set of discrete frequencies $f_i \in \{k\Delta f + f_0\}$, $k=\{0, 1, \dots N-1\}$ interference-free. The N orthogonal subchannels are then multiplexed to form the OFDM prototype. Conversion to time domain is implemented using the Inverse Discreet Fourier Transform (IDFT). This operation also implements the multiplexing of the low-rate substreams to create the OFDM prototype samples out of the frequency-domain (signal space) complex amplitudes.

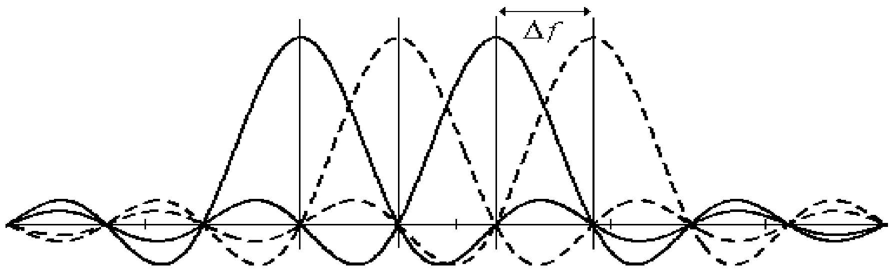

Fig. 1. Orthogonal subcarrier spacing in frequency domain [9]

A unitary IDFT definition is given by (1), useful to preserve the signal energy between the time and frequency domains.

$$x_n = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} X_k \cdot e^{\frac{j2\pi}{N}nk} \quad (1)$$

where $n, k = 0, \cdots, N-1$

After time-domain conversion, the block of OFDM symbol samples is prefixed by its own subblock, which contains some fraction of its samples (Typical values range from 1/32 to 1/4) [1, 2]. The repetition is denoted the Cyclic Prefix Insertion (CPI) and is paired together with an inverse operation in the receiver – the Cyclic Prefix Removal (CPR). Both operations together enable a computationally feasible equalization of the multipath-channel distortion. The operation of the Cyclic Prefix (CP) insertion is shown in Fig. 2, with the CP length denoted as T_g. The useful symbol time is denoted T, and the transmitted OFDM symbol duration $T_{OFDM} = T_g + T$.

These values also define the number of samples for discrete-time processing: the number of data samples is equal to the Fourier Transform size N. We denote N_{CP} as the number of the samples of the cyclic prefix.

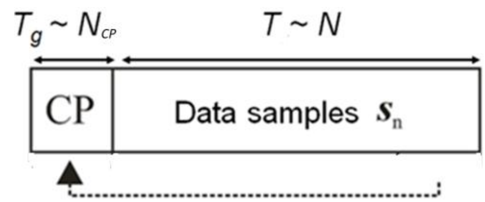

Fig. 2. The OFDM symbol (block of samples) prolonged by cyclic prefix insertion [9]

2.2 Multipath fading channel

In cellular network transmission, the distortion of the transmitted signal can be divided into three primary effects: reflection, refraction and scattering [7]. As illustrated in Fig. 3, several differently delayed and variously attenuated copies of the transmitted OFDM prototype arrive at the receiver antenna. The receiver observes a resulting superposition of these interfering copies. Such a channel characteristic can be described by a Finite Impulse Response (FIR) filter. In discrete-time and discrete-frequency domains the filter is defined by impulse response $h(n)$, and frequency characteristics $H(k)$ (further denoted as h_n, H_k or $\boldsymbol{h}$, $\boldsymbol{H}$). The transmission in a multipath fading channel is then modelled by a convolution of the transmitted OFDM prototype – vector $\boldsymbol{t}$ with the channel impulse response $\boldsymbol{h}$ given by Eqn. (2):

$$r_n = \sum_{m=1}^{\nu} h_m t_{n-m+1}, \qquad n = 1, \cdots, N + \nu - 1 \quad (2)$$

As in the simpler AWGN model, a random white Gaussian noise with power σ^2 is then superimposed on the received vector $\boldsymbol{r}$.

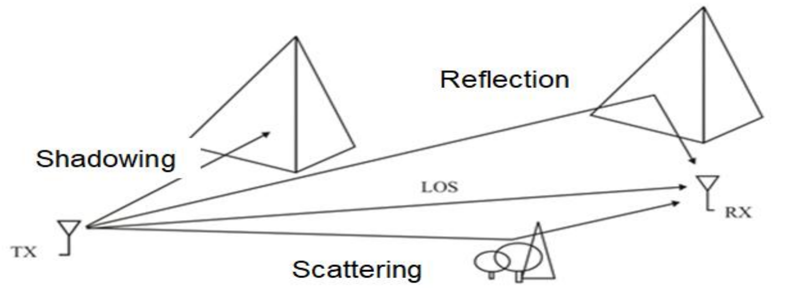

Fig. 3. Multipath propagation of a wireless signal in a terrestrial channel [9]

Figure 4 illustrates a simplified OFDM system alongside the multipath channel model. Although Analog-to-Digital (A/D) and Digital-to-Analog (D/A) converter circuits are essential, the majority of signal processing occurs in the digital domain. The ECC block implements redundancy to safeguard data against channel-induced errors. The receiver's corresponding A-Posteriori Probability (APP) block serves as a soft-input decoder relying on posterior probabilities.

The Constellation Mapping (CM) block executes the signal space mapping, such as BPSK, QPSK, or QAM and the receiver's Discrete Fourier Transform (DFT) block converts the received OFDM block back into the frequency (signal space) domain. The resulting noisy samples are then fed into the Frequency Domain Equalization (FDE) stage. The equalized, but still noisy samples (signal space projections) provide input to the ECC decoder.

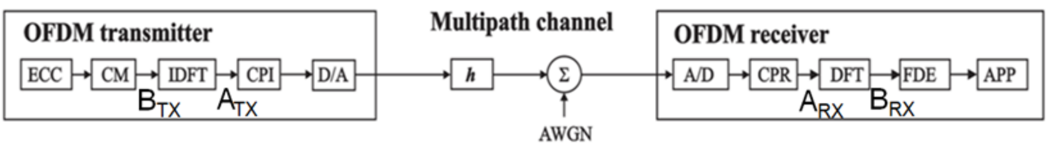

Fig. 4. OFDM transmission model with multipath channel [9]

2.3 LDPC and iterative decoding

The posterior-probability based Soft-Input Soft Output (SISO) LDPC decoder usually implements a variant of the Message Passing (MP) algorithm, origins of which can be traced back to the original LDPC definition by Gallager [10]. All such algorithms are best described as graph algorithms using the Tanner graph [11] representation of the parity check matrix **H**. The parity equations-rows of **H** are denoted as check nodes (CN), and codeword positions-columns of **H** are denoted variable nodes (VN). A practical and numerically stable version of the decoder called the Min-Sum Algorithm (MSA) [12] is based on the Log-Likelihood Ratio (LLR) metrics Z defined as:

$$Z_n^{(0)} = \ln \frac{p(x_n = 0/y_n)}{p(x_n = 1/y_n)} = 2y_n/\sigma^2 \quad (3)$$

where y_n is a noisy sample (signal space projection) of the received and equalized OFDM prototype.

The iterations of the MSA can be further divided into four steps, using the definitions of $N(m)$ as the set of all VNs incident with CN m, and $M(n)$ as the set of all CNs incident with VN n [13]:

A. The horizontal scan – the check node message:

For each m and each $N(m)$ compute the CN message L_{mn}, out of the variable node messages Z_{mn} coming from all incident VNs except for the output one.

$$L_{mn}{}^{(k)} = \min_{n' \in N(m) \backslash n} |Z_{mn'}{}^{(k)}| \cdot \prod_{n' \in N(m) \backslash n} \operatorname{sgn}(Z_{mn'}{}^{(k)}) \tag{4}$$

B. The vertical scan - the variable node message:

For each n and each $M(n)$ calculate the variable node message Z_{mn} coming from all incident CNs, except for the output one.

C. The posterior probability estimate:

For each n and each $M(n)$ calculate the posterior LLR estimate $Z_n{}^{(k)}$:

$$Z_{mn}{}^{(k)} = Z_n{}^{(0)} + \sum_{m' \in M(n) \backslash m} L_{m'n}{}^{(k)} \tag{5}$$

D. Hard decision and stopping condition:

For each n compute the bit estimate $\hat{x}_n$:

$$\hat{x}_n{}^{(k)} = \begin{cases} 0, & \text{if } Z_n{}^{(k)} > 0; \\ 1, & \text{otherwise} \end{cases} \tag{6}$$

and check orthogonality with the **H** matrix:

$$\mathbf{H}\hat{\mathbf{x}} = \mathbf{0}, \quad \text{over GF(2)} \tag{7}$$

If condition (7) is satisfied, terminate the decoding.

The Min-Sum Algorithm is typically started with a predefined maximum number of iterations and may terminate early, based on condition (7). The analysis of the number of iterations serves as a basis for the method suggested in later sections.

3 The jammed channel model

The situation of interest is depicted in Fig. 5 where the TX sends the OFDM-modulated signal to the intended RX Over-The-Air (OTA) through a multipath-propagation channel. This is a practical setting in terrestrial OFDM-based networks. The jammer (JAM) is assumed to be able to receive the signal, and retransmit its copy with a controlled delay towards the receiver. The transmitted OFDM signal is defined as a series of OFDM symbols $\boldsymbol{t}^o$, where the superscript index o denotes the index of the OFDM symbol and $\boldsymbol{t}$ may be represented in the discrete-time domain as a vector of samples t_n:

$$\boldsymbol{t} = [t_0, t_1, \cdots, t_{N+L_{CP}-1}] \equiv [s_{N-L_{CP}}, \cdots, s_{N-1}, s_0, s_1, \cdots, s_{N-1}] \tag{8}$$

with N being the Fourier transform size and L_{CP} the size of the Cyclic Prefix. The CP samples are redundant copies of the last L_{CP} samples and are discarded in the RX.

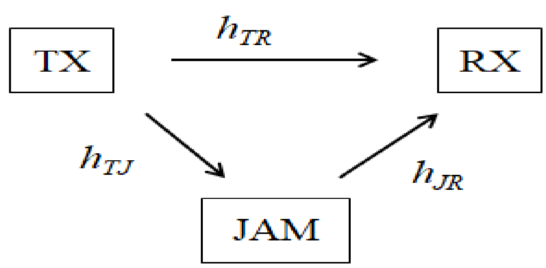

Fig. 5. The multipath-propagation jammed channel model

The discrete-time OFDM symbol (vector) without the redundant CP is denoted $\boldsymbol{s}$ and defined by Eqn. (1). It is constructed using IDFT in the TX from a vector of frequency domain samples S_k , which represent the complex amplitudes of OFDM subcarriers, selected from a given constellation. The multipath channel introduces convolution of the transmitted vector $\boldsymbol{t}$, with channel impulse response $\boldsymbol{h}$, in discrete time defined by Eqn. (2). This defines a linear convolution, with the effect of prolonging the transmitted symbol by ν–1 samples. As shown in Fig. 5, between TX and RX, the signal is affected by the multipath propagation defined by the channel impulse response $\boldsymbol{h}_{TR}$, while the channel between TX and JAM is described by $\boldsymbol{h}_{TJ}$, and the channel between JAM and RX by $\boldsymbol{h}_{JR}$. Furthermore, all three propagations are also affected by the AWGN noise, further denoted by vectors $\boldsymbol{n}_{RT}$, $\boldsymbol{n}_{RJ}$, $\boldsymbol{n}_{JR}$.

As shown in [5], by relaying the intentionally delayed copy of the OFDM signal by the jammer, the reception of the original signal along with the delayed jamming signal, may be described as:

$$\boldsymbol{r} = \boldsymbol{h}_{TR} * \boldsymbol{t} + \boldsymbol{h}_{JR} * \boldsymbol{h}_{TJ} * \boldsymbol{t}' + \boldsymbol{h}_{JR} * \boldsymbol{n}_{TJ} + \boldsymbol{n}_{TR} \tag{9}$$

where $\boldsymbol{t}'$ consists of samples of two successive OFDM symbols, $\boldsymbol{s}^o$ and $\boldsymbol{s}^{o-1}$, as defined in [5]. This can further be simplified and viewed from the RX perspective as Inter-Symbol Interference (ISI) caused by a time-varying virtual $\boldsymbol{h}$ that breaks the assumption necessary for ISI-free transmission:

$$\nu_{max} \leq L_{CP} \tag{10}$$

where ν_{max} is the maximum length of the channel impulse response and L_{CP} the length of the CP. Putting emphasis on the discrete-time processing, the OFDM symbol is a vector, or block of samples, and the ISI is denoted as Inter-Block Interference (IBI). The IBI is present even if condition (10) is met, but it only affects the redundant samples of the CP, which are discarded in the RX. If condition (10) is not met, the extra IBI also affects the useful data samples. This extra interference can be quantified by:

$$\hat{r}_{IBI}(l) = \sum_{l=0}^{\Delta-1} h_{l+L_{CP}+1} s_{N-(l+1)}^{o-1} \tag{11}$$

where Δ is the length of $\boldsymbol{h}$ exceeding L_{CP}. This introduces errors in the sensitive FDE equalization process, bringing about a catastrophic effect on the system Bit Error Rate (BER). The effect of the artificially prolonged $\boldsymbol{h}$ is demonstrated in Fig. 6, where the channel convolution matrix is depicted for $N = 5$, $L_{CP} = 2$, $\nu_{max} = 3$ and $\Delta = 2$:

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \equiv \hat{r}_0 \\ r_3 \equiv \hat{r}_1 \\ r_4 \equiv \hat{r}_2 \\ r_5 \equiv \hat{r}_3 \\ r_6 \equiv \hat{r}_4 \\ r_7 \\ r_8 \\ r_9 \\ r_{10} \end{bmatrix} = \begin{bmatrix} h_0 & 0 & 0 & 0 & 0 & 0 & 0 \\ h_1 & h_0 & 0 & 0 & 0 & 0 & 0 \\ \hline h_2 & h_1 & h_0 & 0 & 0 & 0 & 0 \\ \boldsymbol{h_3} & h_2 & h_1 & h_0 & 0 & 0 & 0 \\ \boldsymbol{h_4} & \boldsymbol{h_3} & h_2 & h_1 & h_0 & 0 & 0 \\ 0 & \boldsymbol{h_4} & \boldsymbol{h_3} & h_2 & h_1 & h_0 & 0 \\ 0 & 0 & \boldsymbol{h_4} & \boldsymbol{h_3} & h_2 & h_1 & h_0 \\ \hdashline 0 & 0 & 0 & \boldsymbol{h_4} & \boldsymbol{h_3} & h_2 & h_1 \\ 0 & 0 & 0 & 0 & \boldsymbol{h_4} & \boldsymbol{h_3} & h_2 \\ \hdashline 0 & 0 & 0 & 0 & 0 & \boldsymbol{h_4} & \boldsymbol{h_3} \\ 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{h_4} \end{bmatrix} \cdot \begin{bmatrix} s_3 \\ s_4 \\ s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix}$$

Fig. 6. Example channel convolution matrix, bold h_i coefficients denote IBI from the previous OFDM symbol.

The solid line in Fig. 6 delineates the CP. The dashed line marks the end of the useful OFDM symbol, which can be reindexed to $\hat{r}$ to be compatible with Eqn. (11). The first L_{CP} samples are discarded because they are corrupted by the overlapping samples from the previous block (r^{o-1}_7, r^{o-1}_8). Bold-faced samples of $\boldsymbol{h}$ denote the samples in excess of L_{CP}. The samples r_7 to r_{10} (under the dashed line) then corrupt the next OFDM block, and the dotted line indicates the samples that cause interference in excess of the CP. Samples r^o_9, r^o_{10} of OFDM symbol o will interfere with r^{o+1}_2, r^{o+1}_3 of the next symbol $o+1$.

4 Jammer detection method

4.1 LDPC decoding observations

Modern communications standards and systems use the Adaptive Coding and Modulation (ACM) to maintain a reasonably low resulting BER, usually under 10^{-6}. The modulation constellation and ECC code parameters are adaptively tuned on a per-frame basis, according to the detected channel conditions. The system works to maintain a proper point at the waterfall curve. Three observations are the basis of the proposed jammer detection method:

The first observation is that when an iteratively decoded code, such as an LDPC, is used, the decoding algorithm, such as the widely used Min-Sum Algorithm (MSA), provides an extra output: the number of iterations the decoding actually took. This may be further used for jammer detection.

The second observation is that the number of iterations at a desired E_b/N_0 point with BER approximately 10^{-6} is usually far lower than the maximum number of iterations I_{max} defined for the MSA. Figure 7 shows the histogram, obtained by MATLAB simulations, of the number of iterations, where I_{max} was set to 20 at a point E_b/N_0 near the target BER.

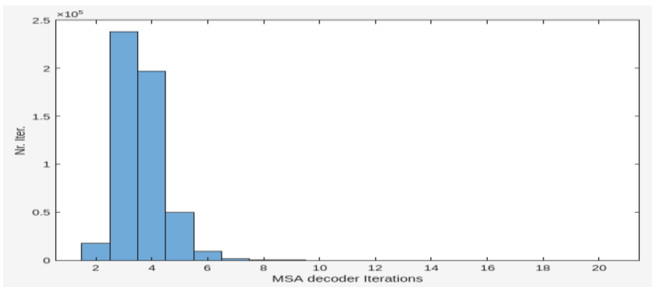

Fig. 7. Histogram of the number of iterations of an MSA decoding for a selected E_b/N_0 resulting in BER of approx. 10^{-6}

As shown in Fig. 7, even though the maximum number of MSA iterations was set to 20, at the practical point, the average actual number of iterations was less than four.

A third observation is the fact that, at a desired E_b/N_0 point, not only are the situations where the decoder reaches I_{max} very rare, they are almost always isolated. It is therefore reasonable to analyze the lengths of runs where decoder iteration count equals I_{max} and use this as a metric to detect anomalies, such as jamming. Table 1 shows the statistics for the MSA decoder iterations, with jammer (JAM) and without the jammer (NOJ) for I_{max}=20. The *Isolated* column indicates the total number of isolated instances, the columns *Nr. runs 2* and 3 indicate how many times a run of length 2 or 3 was observed (only one such instance per frame is counted). The MATLAB simulation was organized in 2680 frames by 192 OFDM symbols, each using N=1944 subcarriers. N_{it} in Tab. 1 denotes the number of iterations.

Table 1. MSA iterations statistics

	avg(N_{it})	var(N_{it})	Isolated	2 runs	3 runs
NOJ	3.6197	0.7097	21	0	0
JAM	19.1354	0.8134	2680	2680	2680

As shown in Tab. 1., the substantial rise in runs where I_{max} is reached is a good indicator of a jammer presence. A simple threshold comparison method is therefore highly tunable, effective, and requires almost no additional resources. The number of isolated incidents may also seem to be a predictor, but these may occur naturally in a Rayleigh fading channel and cause false positives.

4.2 Novel OFDM receiver design

Based on the observations described above, a novel modified OFDM receiver design is proposed in Fig. 8, containing a jamming detection (JD) block based on the sliding window detecting the instantaneous runs of maximum LDPC decoder iterations. The JD block, upon detecting a jammer's presence, signals this event to the Radio Link Control (RLC), which may further decide how to handle the situation. The indication may be passed to upper layers to collect statistics and, assuming bidirectional transmission, the Adaptive Coding and Modulation (ACM) block may be instructed to fortify the transmission by setting a more powerful ECC code by decreasing the code rate, using a mode robust modulation, such as BPSK instead of the higher order QAM. Most importantly, a longer cyclic prefix may immediately be set. In order to inform the opposite side of the communication link, a special JAM bit could be introduced in the PHY-layer header to indicate the detection.

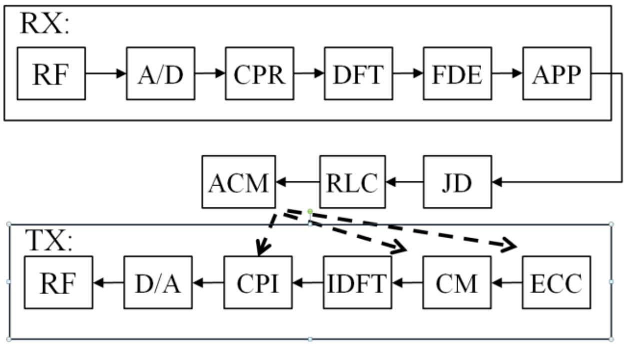

Fig. 8. Novel design of OFDM receiver

The effects of the jamming methods were evaluated using MATLAB simulations within the context of a Rayleigh fading multipath channel with 6 paths. Pedestrian speed receiver movements are shown in Fig. 9. The OFDM system uses N = 1944 subcarrier and L_{CP} = 122 samples which represents 1/16th of the OFDM symbol samples. The three dashed lines indicate: uncoded transmission,: unjammed (o marker), jammed with Δ=100 samples with jammer power –20dB lower than the TX (+ marker), and jammed with power equal to TX (x marker). The solid line then indicates the LDPC encoded transmission where detected jammed frames were discarded and only the residual BER was calculated after LDPC decoding. Simulation results were obtained by using our free and open source LDPC+OFDM MATLAB simulation toolkit available on GitHub [15, 16].

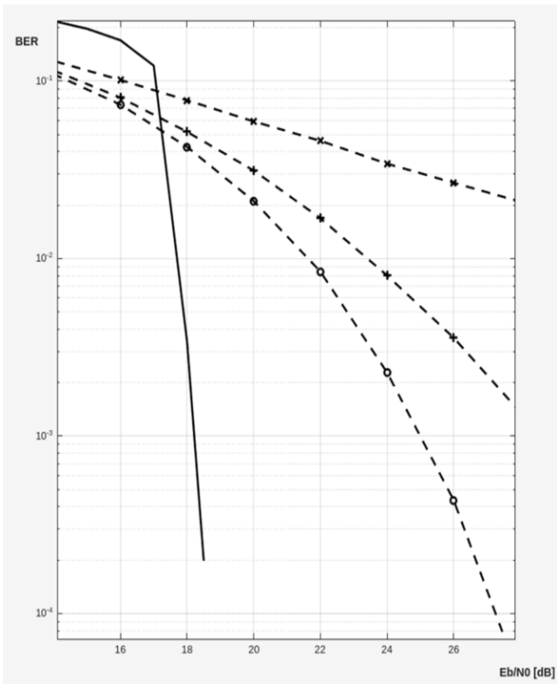

Fig. 9. Waterfall curves showing the jammer effect in Rayleigh channel. Solid: jammed-corrected. Dashed: no ECC: non-jammed (o), jammer –20dB (+), jammer 0 dB (x).

This design will work well in an AWGN channel as well as in a Rayleigh channel in a low-mobility scenario. However, in a higher mobility scenario, the deep fades can occur naturally and often, even if a jammer is not involved. The analysis of the statistical behavior of the deep fade occurrences is outside of the scope of this paper and is a topic for future research. What is clear at this point is that the design presented in Fig. 8 is also suitable for detection of deep fades.

5 Measurement evaluation of jamming feasibility

Our evaluation testbed is shown in Fig. 10. For measuring jammer latency as well as overall latency of Over-the-Air (OTA) transmission, our testbed consisted of 3 PCs with USRP and GNU Radio 3.10 running on Ubuntu 20.04. The PCs were equipped with mid-grade Intel Core i7 and AMD Ryzen CPUs. TX and RX used USRP N210 with UBX daughterboard. JAM used USRP B210, connected via USB3.0. All antennas were identical log periodic PCB antennas and operated in the 2.4-5 GHz ISM band. Since B210 simultaneously transmits and receives on the same frequency, self-interference had to be mitigated. B210 lacks hardware self-interference cancellation circuits and software solutions like time domain guard intervals or digital self-interference cancellation would require synchronization and/or filtering. A simple mitigation was achieved by physically separating antennas and by using a direct loopback cable connection between TX and JAM. (as shown in Fig. 10). Alternatively, a metal sheet could be used as a shield between the jammer antennas.

The core idea of our method was to generate and transmit easily recognizable waveforms such as square or triangle, available in GNU Radio Companion. These waveforms were received by both RX and JAM. The jammer then immediately retransmitted the waveform via its second RF port. This relayed signal was received again on RX, introducing a measurable latency. Latency was determined in real-time using a combination of custom and native processing blocks and later calculated via post-processing in MATLAB. Among the available waveforms, the square was selected as GNU Radio's implementation includes a leading impulse, which aids in detection at the receiver.

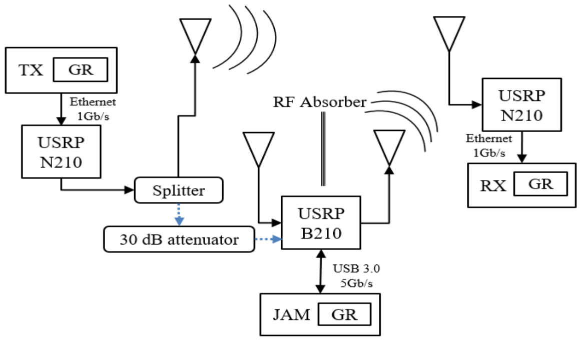

Fig. 10. Experimental testbed configuration of PCs and USRPs

Figure 11 illustrates an example of received signals, both directly from TX and those relayed by JAM, the latter appearing with reduced amplitude and a time delay.

The square waveform was configured to continuously repeat with a period of L_{Symbol} = 100 samples, which corresponds to 10 µs at a 10 MHz sampling rate. However, the continuous nature of the waveform made it difficult to determine which symbol instance was being observed due to overlap. To avoid this ambiguity, we introduced a zero-padding $L_{Padding}$ after each waveform repetition. This padding consisted of 10^6 samples (i.e., 100 ms of silence at 10 MHz sampling rate), ensuring clear separation between repeated signals. Since the expected delay introduced by JAM is at least an order of magnitude smaller, this structure guarantees that the correct waveform instance is isolated and compared at the receiver.

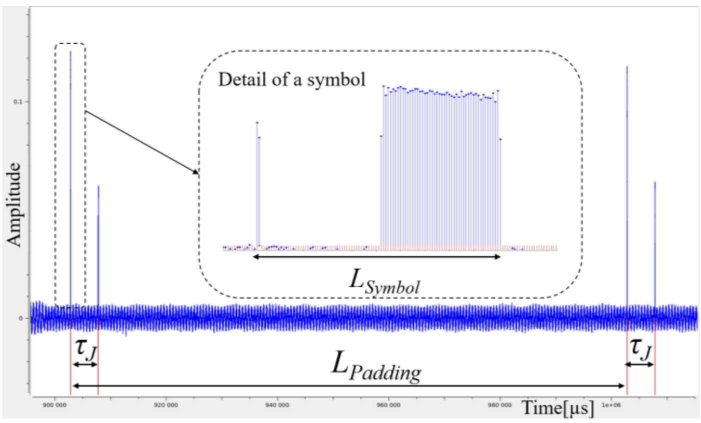

Fig. 11. Capture of received symbols from TX and relayed symbols from JAM on a GNU Radio Oscilloscope (Time Sink) with detail of symbol

Crucially, the observed delay τ_J corresponds to the latency between the original TX waveform and the JAM relayed copy and consistently repeats after $L_{Padding}$ interval.

Table 2 illustrates the impact of the jammer's sampling rate on measured latency. Among other factors, the sampling rate affects how quickly the USRP Hardware Driver (UHD) buffer fills, making it a significant contributor to overall system latency. Each data point in the figure represents an average of over 100 waveform repetitions, with a sampling rate at or below 20 MHz, which resulted in stable and consistent latency. However, when exceeding this threshold, the system experienced USRP underruns, leading to increased jitter and fluctuating latency measurements.

Table 2. Dependence of latency on sampling rate

Sampling rate (*MSPS*)	τ_J (μs)
1	22073
10	5418
20	2259
40	477

To evaluate whether an RBJ attack could effectively target the same OFDM symbol in real-world systems, it is essential to compare the observed jammer latency against the timing constraints defined in wireless standards. Table 3 summarizes the key timing parameters, including the cyclic prefix (guard interval) and symbol duration for several representative OFDM-based protocols. Even under controlled conditions with simplified waveform structures, the lowest observed latency with USRP B210 in our setup was consistently well above 68 μs. This aligns with the values reported in [17], which used a more optimized and dedicated latency-minimization setup, yet still could not reduce B210 latency below that threshold.

Table 3. Timing related parameters of different OFDM based standards

Standard	Preamble (μs)	Guard interval (μs)	Symbol interval (μs)	Min frame interval (μs)
802.11a [18]	16	0.8	4	~20
802.11ax [19]	20-32	0.8/1.6/3.2	12.8	~20
LTE DL [20]	160	0.8/1.6/3.2	66.7	1000
5G NR [21]	uses SSB	4.7 / 16.7	4.16 to 66.7	~125

This result has major implications for smart relay jamming feasibility. For instance, the cyclic prefix in 802.11a and Wi-Fi 6 is just 0.8 μs and even the shortest OFDM symbols in 5G NR are 4.16 μs long. Such tight windows are orders of magnitude smaller than what CPU-based SW processing at the can achieve. The focus of the jammer implementation must therefore shift to direct processing on the USRPs FPGA.

6 Conclusion

In this paper, we have presented a simple jamming detection method based on run-lengths of an iterative decoder of LDPC-encoded OFDM transmission reaching the maximum number of iterations. Furthermore, we presented the results of our measurements regarding the feasibility of an SDR implementation of a Repeat Back Jamming-like attack in the OFDM context. Based on the resulting jammer latencies, we conclude this attack to be infeasible when implemented in SW, and suggest a future focus on a direct FPGA-based implementation. Both our MATLAB simulation toolkit and GNU Radio flow graphs are freely available online.

Acknowledgement

This work was funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the contract No. 09I03-03-V04-00259.

References

[1] "IEEE Std 802.11be-2024", vol., no., pp.1-1020, 22 July 2025, doi: 10.1109/IEEESTD.2024.11090080..

[2] "3GPP Release 18 Specifications", https://www.3gpp.org/specifications-technologies/releases/release-18

[3] T-Mobile, AT&T, BT, Ericsson, et al., "6G Standardization - Principles, 3GPP 6G Workshop", *Incheon, Korea, March 2025,* ID: 6GWS-250234, https://www.3gpp.org/specifications-technologies/releases/release-19

[4] M. Lichtman, et al., "5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation", *2018 IEEE International Conference on Communications Workshops, Kansas City, MO, USA*, 2018, pp. 1-6, doi: 10.1109/ICCW.2018.8403769.

[5] L. Li, S. Tian, J. Huang and P. Zhang, "Efficient and unrecognizable OFDM jamming by failing the cyclic prefix functionality". *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 2017*, pp. 1-6, doi: 10.1109/WCSP.2017.8170905

[6] "IEEE Std 802.11-2020, Part 11: wireless lan MAC and PHY specifications - Annex F: HT LDPC matrix definitions", *IEEE New York (USA)*, 2021. p. 4130–4132. ISBN 978-1-5044-7283-8.

[7] B. Sklar and F. Harris, *Digital Communications: Fundamentals and Applications,* 3rd Edition. Pearson, 2020, ISBN: 978-0134588568.

[8] K.T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms 2nd*, Edition. Wiley, 2020, ISBN: 978-1119567479.

[9] T. Palenik, "Communication system design based on SDR platform: Exploiting the redundancy of an OFDM system", dissertation (in Slovak). Sep. 2010, Bratislava, Slovakia.

[10] R. G. Gallager, *Low-density parity-check codes*, MIT Press Cambridge (USA), 1963, doi: 10.7551/mitpress/4347.001.0001

[11] R. M. Tanner, D. Sridhara, A. Sridharan, et al., "LDPC block and convolutional codes based on circulant matrices", *IEEE Transactions on Information Theory*, 2004, vol. 50, no. 12, pp. 2966-2984, doi: 10.1109/TIT.2004.838370

[12] X. Huang, "Single-Scan Min-Sum Algorithms for Fast Decoding of LDPC Codes", *IEEE Information Theory Workshop ITW '06,* Chengdu, Oct. 2006, pp. 140 -143

[13] M. Rakus, T. Palenik, *Digital communications – collection of solved problems and examples*. 1st. ed. Camperdown, Emona Instruments, 2024. 246 p., ISBN 978-1-921903-15-1

[14] S. Liu, "Wi-Fi Energy Detection Testbed (12MTC)," 2023, https://github.com/liustone99/Wi-Fi-Energy-Detection-Testbed-I2MTC

[15] T. Palenik, "OFDM toolkit", https://github.com/talenik/OFDMtoolkit

[16] T. Palenik, "YALDPC toolkit", https://github.com/talenik/YALDPC

[17] S. Kumar and F. Kaltenberger, *Latency Measurements for USRP B210 and X300 for GPP based SDR Applications,* Eurecom, France, https://sumiteurecom.github.io/latency-measurements-usrp.pdf

[18] Keysight Technologies, "IEEE 802.11 OFDM Overview – WLAN OFDM Analysis", https://helpfiles.keysight.com/csg/89600B/ Webhelp/Subsystems/wlan-ofdm/content/ofdm_80211-overview.htm

[19] Cisco Meraki, "Wi-Fi 6 (802.11ax) Technical Guide", https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best Practices/Wi-Fi_6_(802.11ax)_ Technical_Guide

[20] ShareTechnote, "LTE Timing Advance – Understanding Timing Parameters in LTE", https://www.sharetechnote.com/html /Handbook_LTE_TimingAdvance.html

[21] ShareTechnote, "5G Frame Structure – NR Frame and Slot Timing", https://www.sharetechnote.com/html/5G/5G_FrameStructure.html

Received 20 August 2025