electronics

MDPI

Article

Securing the Future: A Resourceful Jamming Detection Method Utilizing the EVM Metric for Next-Generation Communication Systems

Cem Örnek [1,2,*] and Mesut Kartal [2]

[1] Radar and Electronic Warfare Systems Business Sector, Aselsan Inc., Ankara 06830, Turkey
[2] Electronics and Communication Engineering, Istanbul Technical University, Istanbul 34469, Turkey; kartalme@itu.edu.tr
* Correspondence: ornek19@itu.edu.tr; Tel.: +90-536-976-5667

Abstract: This paper addresses the escalating threat of malicious jamming in next-generation communication systems, propelled by their continuous advancement in speed, latency, and connectivity. Recognizing the imperative for communication security, we propose an efficient jamming detection method with distinct innovations and contributions. Motivated by the growing sophistication of jamming techniques, we advocate the adoption of the error vector magnitude (EVM) metric, measured in IQ symbols, deviating from traditional received signal strength and bit error rate-based measurements. Our method achieves enhanced jamming detection sensitivity, surpassing existing approaches. Furthermore, it introduces low complexity, ensuring resource-effective detection. Crucially, our approach provides vital jammer frequency information, enhancing counteraction capabilities against jamming attacks. It demonstrates stable results against varying system parameters, such as modulation type and code rate, thereby contributing to adaptability. Emphasizing practicality, the method seamlessly integrates into 5G and LTE systems without imposing additional overhead. Versatility is demonstrated through successful operations in diverse scenarios that are run by extended simulation conditions. Theoretical analysis substantiates these advantages, reinforcing the validity of our methodology. The study's success is further validated through laboratory experiments, providing empirical evidence of its effectiveness. The proposed method represents a significant step toward fortifying next-generation communication systems against evolving jamming threats.

Keywords: jamming detection; EVM; 5G; resource block

check for updates

Citation: Örnek, C.; Kartal, M. Securing the Future: A Resourceful Jamming Detection Method Utilizing the EVM Metric for Next-Generation Communication Systems. *Electronics* **2023**, *12*, 4948. https://doi.org/10.3390/electronics12244948

Academic Editors: Dariusz Rzońca and Tomasz Rak

Received: 1 November 2023
Revised: 30 November 2023
Accepted: 4 December 2023
Published: 9 December 2023

1. Introduction

5G and beyond communication systems are revolutionizing communication in today's rapidly evolving technological landscape. These systems provide a significant increase in access to Internet-based services with high speeds, low latency, and wide bandwidth. They offer users a seamless experience across multiple devices, facilitating integration between mobile devices, desktops, and other platforms. They also support innovative features and applications, enabling technologies such as augmented reality, remote interventions, and the Internet of things. Owing to their flexibility and future-proof adaptability, these systems play a key role in digital transformation, bringing a more efficient, secure, and rich experience to the world of communications. However, all of these features also open up the possibility for malicious jammers to attack more targets and corrupt more data. Therefore, fast, accurate, and effective detection of jamming attacks is vital for increasing the defense capabilities of systems.

Several jamming detection methods are proposed for wireless networks [1,2]. A significant number of these utilize received signal strength (RSS) measurements. The authors of [3–7] obtain the RSS by estimating the spectrum of the received signal and observe the effect of jamming signals on the RSS. In other studies, the optimal RSS thresholds for

jamming detection are determined with likelihood tests performed by considering the jamming presence and absence hypotheses. This method is widely proposed for massive SIMO [8], massive MIMO [9], LTE [10], direct-sequence spread-spectrum (DSSS) [11], wireless sensor networks [12], ad hoc networks [13], cognitive radio networks [14] and satellite communication [15] systems.

In addition, many studies propose the use of RSS-based metrics in combination with bit error rate (BER)-based metrics such as throughput, packet error rate, packet delivery ratio, packet sent ratio, packet loss rate, and bad packet ratio. Accordingly, the effects of jamming are observed jointly on the RSS- and BER-based metrics, and jamming detection threshold levels are set on these metrics. The jamming detection performance of such methods is demonstrated with simulations in [16–20], and with experimental studies as well as simulations in [21–23]. On the other hand, in [24–27], these metrics are used to train machine learning algorithms such as support vector machines, neural networks, and random forests for jamming detection. In addition to the aforementioned metrics, the chip error rate [28] and inter-arrival time [29] are other metrics examined for jamming detection.

Machine learning algorithms are also trained using spectrogram images [30], IQ samples [31], time-domain signal samples [32], and FFT samples [33,34] for jamming detection. Although machine learning algorithms are becoming increasingly popular, the issues of training these algorithms, collecting sufficient data for training, adapting to varying jamming strategies, and integrating them into the system architecture with minimal overhead must be considered.

Subspace analysis methods are the other methods used in jamming detection. Such methods use eigenvalue [35] or singular-value [36] analyses to identify the subspaces formed by the signal and jamming. However, the jamming detection success of such methods requires the jamming level to be sufficiently higher than the legitimate signal level.

In our previous study [37], the EVM vs. RB metric was proposed to detect jamming attacks in 5G networks. The error vector magnitude (EVM) is measured for each resource block (RB) in the received signal and jamming signals are then detected at RBs where the EVM upper threshold is not met. The success of EVM vs. RB in terms of sensitivity compared to classical BER-based methods was verified with simulations containing only a limited number of scenarios. The EVM metric is also used in studies [38,39] to study jamming effects in OFDM systems. However, these studies have aimed to identify the jamming strategies that cause the greatest damage to the system.

In this paper, we extend the work for the EVM vs. RB measurement and list below all the innovations and contributions achieved:

1. EVM metric utilization: The paper advocates for the utilization of the EVM metric measured in IQ symbols, a departure from the commonly used classical RSS and BER based metrics in the literature.
2. Enhanced sensitivity: The proposed method demonstrates a significant improvement in jamming detection sensitivity compared to existing approaches. Although low-power hidden jamming signals that cannot be detected using conventional metrics do not cause denial of service, they can limit the data transmission rate. Due to the EVM's ability to detect small variations in jamming level, jamming signals hidden in an extreme form 20 dB below the legal signal are also successfully detected.
3. Low complexity: For next-generation networks with low latency requirements, it is advantageous that the proposed method has a low complexity of $O(N)$. This advantage also contributes to the fast response of the system for anti-jamming measures.
4. Jammer frequency information: The proposed method calculates the EVM metric for each RB in the received signal. Since RBs represent the frequency domain, the frequency bands in which jamming attacks occur are also revealed. This important information, which is not provided by most methods, offers an important background for countermeasure steps such as jammer localization [40] and antijamming frequency planning. In addition, the concepts of ambient backscattering and RF energy harvesting [41,42] are recently proposed as solutions to the battery problems of IoT devices.

By using the jamming frequency information provided by our method, these devices can be tuned to the correct jamming frequencies and, as a result, jamming energy, which is usually emitted at high RF powers, can be utilized.

5. Reliability: The EVM vs. RB measurement provides a stable jamming detection performance against varying system parameters such as modulation degree and code rate. However, BER-based methods are affected by the variations of these parameters and provide unreliable results.
6. Usability and compatibility: In LTE and 5G systems, it is known that reference IQ symbols are also sent in the transmitted data packet to enable the UE to estimate the channel. The EVM metric used by the proposed method is calculated using these reference symbols that are already in the system architecture. Thus, the proposed method can be easily integrated into the system without the need for changes in system operation or hardware. Moreover, since jamming detection can be performed using a single threshold level for the EVM metric, there is no need for any pre-operational training and validation phases. As a result, the proposed method is suitable for LTE, 5G, and beyond communication systems, which include IQ modulation and resource block (RB) architectures.
7. Theoretical analysis support: All presented advantages are substantiated with thorough theoretical analysis, reinforcing the validity and efficacy of the proposed jamming detection methodology.
8. Versatility in system scenarios: The proposed method's successful operation in different system scenarios is underscored by extending the simulation conditions to cover the sub-6 GHz frequency region usage, different numerology (OFDM subcarrier spacing) usage, line-of-sight (LOS) and non-line-of-sight (NLOS) channel cases, MIMO structures, and millimeter-wave (mmWave) band usage scenarios.
9. Laboratory experiment validation: The study's success is conclusively demonstrated through experiments conducted in a laboratory environment, providing empirical evidence of the method's effectiveness.

2. System Model

The effectiveness of the proposed method is demonstrated on a 5G downlink data-transmission infrastructure. For this purpose, the process steps shown in Figure 1 are implemented in MATLAB [43] by considering the 3GPP standards [44–48].

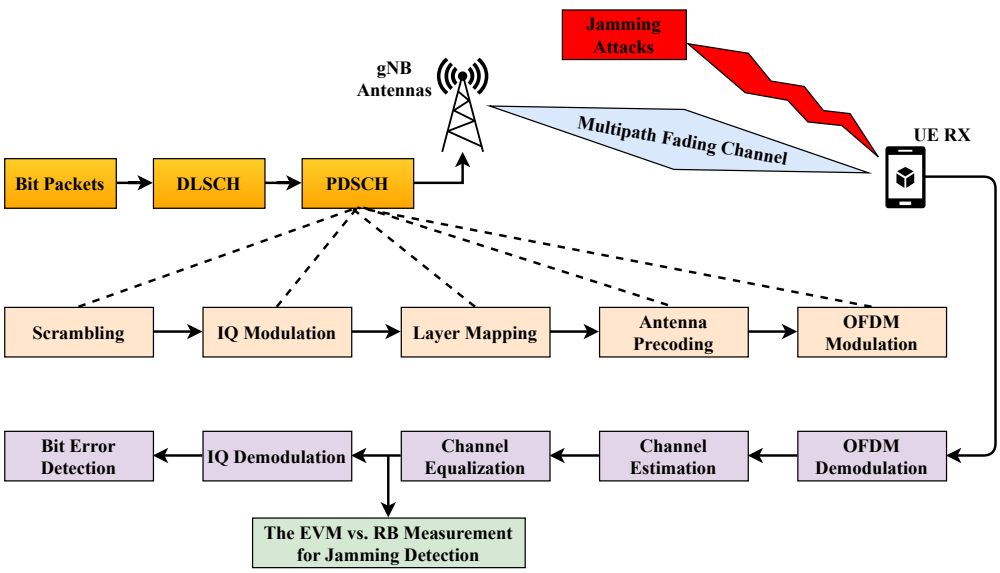


Figure 1. 5G Downlink Data Transmission.

First, the data bits are generated at the gNB (base station); they are then subjected to "cyclic redundancy check" insertion and "low-density parity-check" coding [44] at the downlink shared channel (DLSCH) step [45]. This permits the UE to detect and correct bit errors. The obtained code words are then transferred to the physical downlink shared channel (PDSCH) stage.

In the PDSCH stage [46], the code words are first scrambled so that the broadcast cannot be decoded by unautorized devices. IQ modulation is then performed, providing one of the QPSK, 16-QAM, 64-QAM or 256-QAM options [47].

The obtained IQ symbols are mapped to the MIMO transmitter antennas in the layer-mapping phase. In addition, demodulation reference signals (DM-RS) [47], which are reference IQ symbols required for channel estimation in the UE side, are also included in the data symbols.

The IQ symbols are modulated into the RF band using OFDM. The smallest frequency grid required for downlink transmission is called a resource element, which corresponds to one OFDM subcarrier frequency. A group of 12 consecutive subcarriers (resource elements) in the frequency domain form a resource block (RB). The total bandwidth allocated to a UE is expressed in the number of RBs, and the concept of RB is used throughout the rest of the paper.

Finally, the obtained RF signal is transmitted via MIMO antennas. The mentioned MIMO-OFDM system is detailed in Figure 2. There are N_T transmitter and N_R receiver antennas in the system.

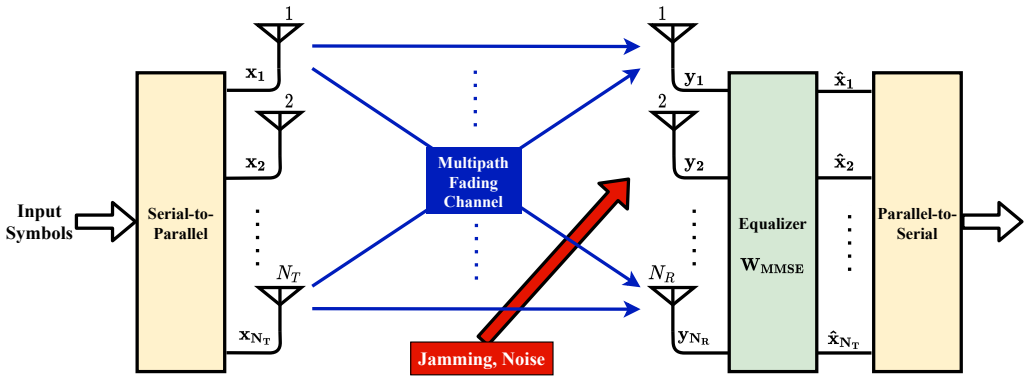


Figure 2. MIMO-OFDM Transmit–Receive Model.

The CDL (Clustered Delay Line) channel model, specified by 3GPP [48] for 5G and beyond communication systems, represents a realistic channel structure with clustered multipath components, each exhibiting Rayleigh fading characteristics. This model aligns with industry standards and is well-suited for the simulation of wireless communication systems, allowing us realistic capture of the effects of multipath propagation and fading in our study. Hence, the overall multipath channel can be expressed by an **H** matrix with each element following a Rayleigh distribution.

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_{1,1} & \dots & \mathbf{h}_{1,N_T} \\ \vdots & \ddots & \vdots \\ \mathbf{h}_{N_R,1} & \dots & \mathbf{h}_{N_R,N_T} \end{bmatrix}, \tag{1}$$

where $\mathbf{h}_{i,j} = \left[h_{i,j}[L-1] \dots h_{i,j}[0]\right]$ is the channel between the ith receiver and jth transmitter antennas, and L is the maximum channel length of all $N_R \times N_T$ links. The statistical properties of $h_{i,j}[l] (l = 0, \dots, L-1)$ and $\mathbf{h}_{i,j}$ can be summarized as follows:

$$\mathbb{E}\{h_{i,j}[l]\} = 0, \tag{2}$$

$$\mathbb{E}\{|h_{i,j}[l]|^2\} = 1, \tag{3}$$

$$\mathbb{E}\{h_{i,j}[l]h^*_{m,n}[l]\} = 0 \text{ if } i \neq m \text{ or } j \neq n, \text{ and so} \tag{4}$$

$$\mathbb{E}\{\mathbf{h}_{i,j}\mathbf{h}^H_{i,j}\} = L. \tag{5}$$

The received signal samples at time instant k are expressed as follows:

$$\mathbf{y}[k] = \sqrt{\frac{P_T}{N_T}} \begin{bmatrix} \mathbf{h}_{1,1} & \dots & \mathbf{h}_{1,N_T} \\ \vdots & \vdots & \vdots \\ \mathbf{h}_{N_R,1} & \dots & \mathbf{h}_{N_R,N_T} \end{bmatrix} \begin{bmatrix} \mathbf{x}_1[k] \\ \vdots \\ \mathbf{x}_{N_T}[k] \end{bmatrix} + \mathbf{v}[k], \tag{6}$$

where P_T represents the average transmitted symbol power, $\mathbf{v}[k] = \mathbf{j}[k] + \mathbf{n}[k]$ represents the sum of the received jamming and noise vectors, and

$$\mathbf{x}_j[k] = \begin{bmatrix} x_j[k-L+1] \\ \vdots \\ x_j[k] \end{bmatrix} \tag{7}$$

is the vector of the transmitted symbols, each with an average power of one unit, that is, $\sigma_x^2 = 1$.

T received vector samples can be combined into a single matrix as

$$\begin{aligned} \mathbf{Y} = [\mathbf{y}[k] \dots \mathbf{y}[k+T-1]] &= \sqrt{\frac{P_T}{N_T}} \begin{bmatrix} \mathbf{h}_{1,1} & \dots & \mathbf{h}_{1,N_T} \\ \vdots & \vdots & \vdots \\ \mathbf{h}_{N_R,1} & \dots & \mathbf{h}_{N_R,N_T} \end{bmatrix} \begin{bmatrix} \mathbf{X}_1 \\ \vdots \\ \mathbf{X}_{N_T} \end{bmatrix} + \mathbf{V} \\ &= \sqrt{\frac{P_T}{N_T}} \mathbf{H}\mathbf{X} + \mathbf{V}, \end{aligned} \tag{8}$$

where $\mathbf{X}_j$ and $\mathbf{V}$ are written as

$$\mathbf{X}_j = \begin{bmatrix} x_j[k-L+1] & x_j[k-L+2] & \dots & x_j[k-L+T] \\ \vdots & \vdots & \dots & \vdots \\ x_j[k-1] & x_j[k] & \dots & x_j[k+T-2] \\ x_j[k] & x_j[k+1] & \dots & x_j[k+T-1] \end{bmatrix} \text{ and} \tag{9}$$

$$\mathbf{V} = \begin{bmatrix} v_1[k] & v_1[k+1] & \dots & v_1[k+T-1] \\ v_2[k] & v_2[k+1] & \dots & v_2[k+T-1] \\ \vdots & \vdots & \dots & \vdots \\ v_{N_R}[k] & v_{N_R}[k+1] & \dots & v_{N_R}[k+T-1] \end{bmatrix}. \tag{10}$$

After receiving $\mathbf{Y}$, the Minimum Mean Squared Error (MMSE) equalizer is used to mitigate the negative effects caused by the channel, such as fading. The MMSE equalization matrix, $\mathbf{W}_{MMSE}$ [49], is calculated as

$$\begin{aligned} \mathbf{W}_{MMSE} &= \sqrt{\frac{N_T}{P_T}} \left(\mathbf{H}^H\mathbf{H} + \frac{P_V N_T}{P_T} \mathbf{I}_{N_T} \right)^{-1} \mathbf{H}^H \\ &= \sqrt{\frac{N_T}{P_T}} \mathbf{B}\mathbf{H}^H, \end{aligned} \tag{11}$$

where $P_V = P_J + P_N$ is the sum of jamming (P_J) and noise (P_N) powers and

$$\mathbf{B} = \left(\mathbf{H}^H\mathbf{H} + \frac{P_V N_T}{P_T}\mathbf{I}_{N_T}\right)^{-1}. \tag{12}$$

To estimate the transmitted IQ symbols, the equalizer is applied as follows:

$$\begin{aligned}\hat{\mathbf{X}} = \mathbf{W}_{MMSE}\mathbf{Y} &= \sqrt{\frac{N_T}{P_T}}\mathbf{B}\mathbf{H}^H\mathbf{Y} \\ &= \mathbf{B}\mathbf{H}^H\mathbf{H}\mathbf{X} + \sqrt{\frac{N_T}{P_T}}\mathbf{B}\mathbf{H}^H\mathbf{V} \\ &= \mathbf{B}\mathbf{C}\mathbf{X} + \sqrt{\frac{N_T}{P_T}}\mathbf{B}\mathbf{H}^H\mathbf{V},\end{aligned} \tag{13}$$

where $\mathbf{C} = \mathbf{H}^H\mathbf{H}$.

At this point, the proposed error vector magnitude (EVM) metric for jamming detection is calculated using the reference and estimated IQ symbols as follows:

$$EVM_n = \sqrt{\frac{e_n^2}{\frac{1}{N}\sum_{n=1}^{N}(i_n^2 + q_n^2)}}, \tag{14}$$

where

- n denotes the index of the IQ symbol,
- N is the total number of symbols used for calculation,
- $e_n^2 = (i_n - \hat{i_n})^2 + (q_n - \hat{q_n})^2$ is the power of the error caused by the jamming and noise,
- i_n and q_n are the reference in-phase and quadrature values of the nth symbol ($x_n = i_n + jq_n$),
- $\hat{i_n}$ and $\hat{q_n}$ are the estimated in-phase and quadrature values of the nth symbol ($\hat{x_n} = \hat{i_n} + j\hat{q_n}$),
- $\frac{1}{N}\sum_{n=1}^{N}(i_n^2 + q_n^2)$ represents the average power of the reference symbols.

As shown in Equation (14), each of the N symbols is used once for vectoral difference calculation. Therefore, the computational complexity of the EVM is in terms of the first power of N, that is, $O(N)$. Consequently, the computational complexity of our jamming detection method using the EVM metric has a low value of $O(N)$.

For EVM calculation, both reference and estimated symbols are required. The natural flow of next-generation communication systems, such as LTE and 5G, includes the transmission of reference symbols. In this manner, without any pre-training and without changing the system architecture, we calculate the EVM metric and detect the presence of a jamming signal by checking whether the EVM exceeds a single threshold level. This makes the proposed method very advantageous in terms of integrability into real-world scenarios.

In addition, Equation (14) indicates that EVM is proportional to the square root of the jamming plus noise-to-signal ratio ($JNSR_{\hat{x}}$). Therefore, to perform EVM analysis, it is necessary to extract the signal, jamming, and noise power components from $\hat{\mathbf{X}}$. For this purpose, it is convenient to calculate the covariance matrix of $\hat{\mathbf{X}}$. Using the statistical independence property [49] and Equation (5), the covariance matrix is calculated as follows:

$$\begin{aligned}\mathbf{\Sigma}_{\hat{X}\hat{X}} &= \mathbf{\Sigma}_{BB}\mathbf{\Sigma}_{CC}\mathbf{\Sigma}_{XX} + \frac{N_T}{P_T}\mathbf{\Sigma}_{BB}\mathbf{\Sigma}_{HH}\mathbf{\Sigma}_{VV} \\ &= \left(\sigma_b^2 L^2 \sigma_x^2 + \frac{N_T}{P_T}\sigma_b^2 L \sigma_v^2\right)\mathbf{I}_{\mathbf{N_T}},\end{aligned} \tag{15}$$

where $\sigma_x^2 = 1$ as expressed in Equation (7), and σ_v^2 is $P_V = P_J + P_N$. The diagonals of $\mathbf{\Sigma}_{\hat{X}\hat{X}}$ indicate the total power of each $\hat{x}_n$. Thus, $JNSR_{\hat{x}}$ can be obtained as follows:

$$JNSR_{\hat{x}} = \frac{N_T}{P_T}\frac{\sigma_b^2 L \sigma_v^2}{\sigma_b^2 L^2 \sigma_x^2} = \frac{P_V N_T}{P_T L}. \tag{16}$$

Consequently, it is revealed that the EVM is related to the parameters given in Equation (17).

$$EVM_n \propto \sqrt{JNSR_{\hat{x}}} = \sqrt{\frac{P_V N_T}{P_T L}} = \sqrt{\frac{P_J + P_N}{(P_T/N_T)L}}. \tag{17}$$

As shown in Equation (17), EVM depends directly on the jamming power represented by P_J. Thus, the EVM metric can sense even small changes in the jamming level. However, for BER-based metrics, such as throughput and packet delivery ratio, to detect jamming signals, the jamming power must be strong enough to divert the received IQ symbols to the wrong regions in the constellation diagram, that is, to create a bit error. Because jamming signals below this jamming power do not create any bit errors, jamming is not sensed by BER-based metrics. Although such weak jamming signals do not cause denial of service, they may limit the data rate performance. Owing to the aforementioned ability of the EVM, these jamming signals can also be successfully detected.

EVM also depends on the transmitted symbol power, which is denoted as P_T. After equalization, P_T is normalized by N_T. Parameter L, on the other hand, is the expected improvement brought by the equalizer. This improvement is also mentioned in simulation results in Section 3.1.

Another conclusion is that the EVM metric is not affected by varying system parameters, such as modulation type and code rate, and as a result, jamming signals are stably detected. However, as shown in the results in Sections 3.2 and 3.3, BER-based metrics are affected by these system parameters and exhibit unreliable results.

The final EVM is expressed in both the RMS (18) and MAX (19). Because the maximum EVM can sense instantaneous distortions in the received signal, it can also detect more sophisticated jamming attacks that target a short-timed fragment of the legitimate signal. Such jammers are also called reactive or responsive jammers [50] and may adopt such short-time operating styles to minimize both their detectability and battery usage. Therefore, the maximum EVM is used in this study.

$$EVM_{RMS} = \sqrt{\frac{\sum_{n=1}^{N} EVM_n^2}{N}}, \tag{18}$$

$$EVM_{MAX} = \max_{n \in [1,\ldots,N]} EVM_n. \tag{19}$$

The maximum EVM is measured for each RB in the received signal. Thus, the EVM vs. RB data are obtained. Because the RBs represent the frequency domain, the EVM vs. RB data reveal the frequency bands attacked by the jammer. After this stage, the operations in the receiver side are completed with IQ demodulation and decoding, and the data bits are obtained. The BER and throughput are measured using the data bits, and these measurements are also observed for jamming detection, whereas the EVM vs. RB detects the jamming attack at an earlier stage. This capability brings extra speed along with low computational complexity.

3. Simulation Results

3.1. Base Scenario

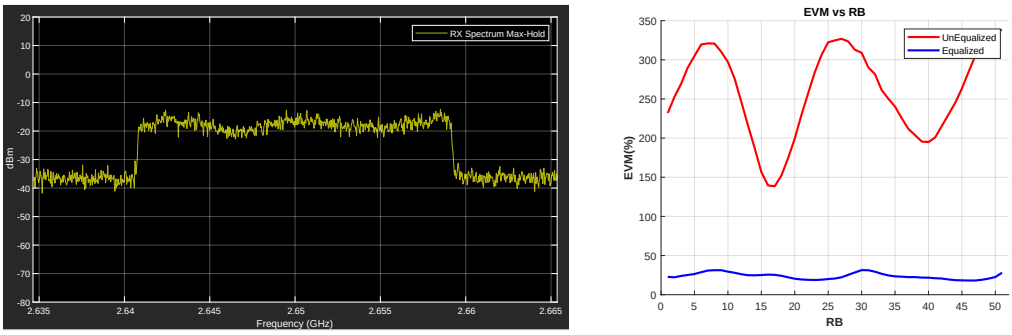
The processing steps required for 5G downlink data transmission are explained in Section 2. The system parameters used in the processing steps are listed in Table 1.

Jammers may concentrate their RF energy into certain frequency bands using tone-type signals, or occupy a broader spectrum using chirp-type signals. Therefore, it is considered sufficient to examine the tone and chirp jammers in this study.

Table 1. Selected Data Transmission Parameters for the Base Scenario.

Parameter Name	Value	Explanation
Carrier Frequency	2.65 GHz	Frequency Range-1 for 5G
MIMO Structure	8×2	
MIMO Transmission Layers	2	
Fading Channel Model	CDL-C	Urban Macrocell Model, NLOS
OFDM Subcarrier Spacing (SCS)	30 kHz	$\mu = 1$ (numerology)
Assigned RBs	51	Transmission bandwidth close to 20 MHz with the 30 kHz SCS
IQ Modulation	16QAM	
Code Rate	490/1024	

First, in the no-jammer case, the RF power spectrum and EVM vs. RB are measured for the received signal, and the measurement results are shown in Figure 3. The observed fluctuations in the spectrum is caused by multipath fading. As explained in Section 2, an equalizer is used to minimize the fading effect on the received IQ symbols. To observe the effect of equalizer on the EVM data, EVM vs. RB is measured for both the unequalized and equalized IQ symbols, as shown in Figure 3b. The EVM vs. RB measurement obtained using unequalized IQ symbols directly reflects the fluctuation characteristics of the RF spectrum (red line in Figure 3b). On the other hand, the improvement brought about by the equalizer shows a decrease in the EVM data (blue line in Figure 3b). As shown in Equation (17), this improvement is expected.

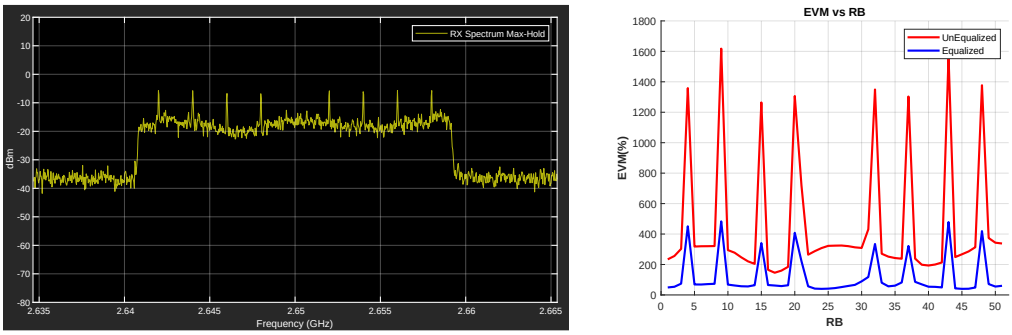


(**a**) (**b**)

Figure 3. No-Jammer Case, Obtained Throughput = %100 (BER = 0). (**a**) The Rx signal spectrum and (**b**) EVM vs. RB.

The same measurements are performed for different jamming cases, that is, tone and chirp jammers. Reviews related to tone jamming are given below, whereas repeated reviews for chirp jamming are provided in the Appendix A. The SJR parameter is selected as -5 dB for both jamming conditions. The observed changes in the RF power spectrum and EVM after the application of these jamming signals are shown in Figures 4 and A1, respectively. In the EVM vs. RB data obtained using unequalized symbols, jamming effects are observed in addition to fluctuations owing to the fading (red lines in Figures 4b and A1b). On the other

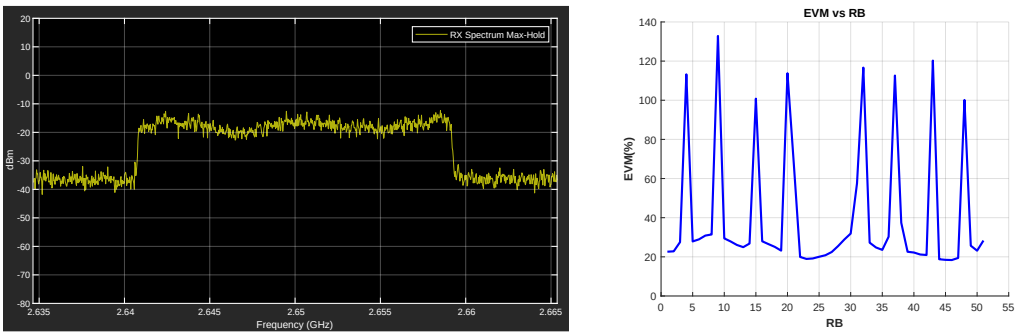
hand, in the EVM vs. RB measurement taken with equalized symbols, the fluctuation is minimized owing to the equalizer, but jamming effects are still clearly observed (blue lines in Figures 4b and A1b)). Thus, in the EVM vs. RB data obtained with equalized symbols, jamming signals can be easily detected using a single threshold level, without considering any fluctuation effect in the data. Therefore, to avoid dealing with the fluctuation effect due to fading, EVM vs. RB measurement using equalized IQ symbols is proposed for jamming detection.



(**a**) (**b**)

Figure 4. Tone Jammer Case, SJR = −5 dB, Obtained Throughput = %0 (BER = 0.343). (**a**) shows the Rx signal spectrum and (**b**) shows the EVM vs. RB.

In the next simulation, where the SJR is increased to 10 dB, the received signal is contaminated with jammers of the same tone and chirp type. The RF spectrum and EVM vs. RB measurements are shown in Figures 5 and A2, respectively. In this SJR case, the jamming signals cannot be detected using the RF power spectrum, which provides RSS information, as shown in Figures 5a and A2a. In addition, the throughput measurement for both the jamming cases is 100%, which means that the jamming effect cannot be sensed using this BER-based metric. However, the EVM vs. RB measurements successfully detect these small jamming signals, as shown in Figures 5b and A2b. This reveals the success of the proposed method in terms of sensitivity compared with RSS- and BER-based methods.



(**a**) (**b**)

Figure 5. Tone Jammer Case, SJR = 10 dB, Obtained Throughput = 100% (BER = 0), (**a**) the Rx signal spectrum and (**b**) EVM vs. RB.

EVM vs. RB, throughput, and BER are measured for various SJR values to examine the dependencies of the jamming detection metrics on SJR. According to the results shown in Figure 6d, jamming cannot be sensed using the throughput and BER observations when SJR exceeds 10 dB. However, using the EVM vs. RB measurement, jamming signals are successfully detected, even under extreme SJR conditions, such as 20 dB (Figure 6b). To demonstrate the performance of EVM vs. RB under other SJR conditions, the peak value of EVM vs. RB for each SJR is calculated and the results are shown in Figure 6c. It is

concluded that jamming signals with an SJR of 25 dB can also be detected using EVM vs. RB. However, beyond 25 dB, EVM vs. RB also becomes unsuccessful in jamming detection.

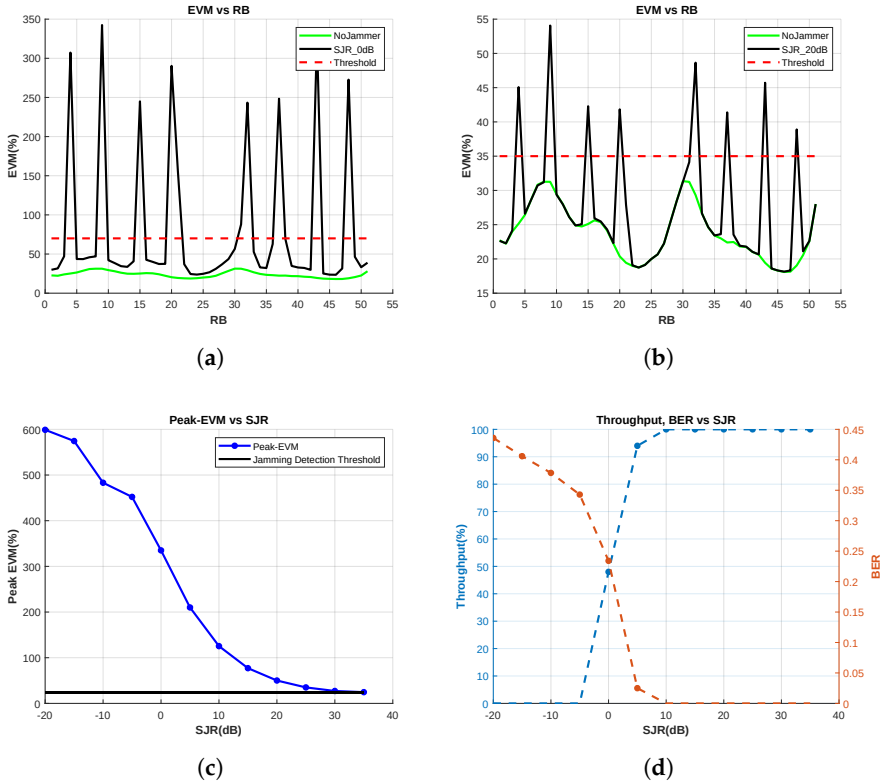


Figure 6. EVM vs. RB, BER and Throughput Measurements for Multitone Jammer. (**a**) EVM vs. RB for SJR = 0 dB, (**b**) EVM vs. RB for SJR = 20 dB, (**c**) Peak-EVM vs. SJR, and (**d**) throughput and BER vs. SJR.

The sensitivity performance of the proposed method for tone jamming is also valid for chirp jamming, as shown in Figure A3. In the following sections, the BER results are not presented alongside the throughput results, because, as shown in the figures, the BER is inversely proportional to the throughput and does not provide any additional information.

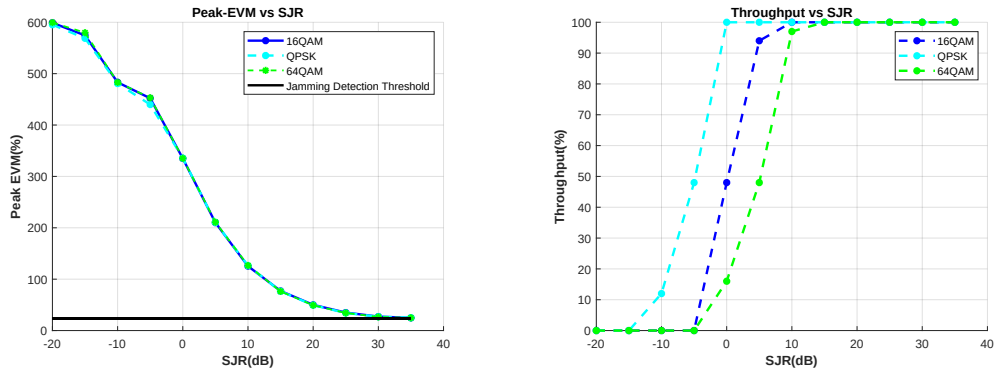
3.2. Reliability of the Proposed Method against Modulation Type Change

5G systems choose the appropriate M-PSK or M-QAM modulation types according to the data rates required by the UEs and channel availability. 16-QAM modulation is considered in the base scenario (Section 3.1). In this section, along with 16-QAM, QPSK and 64-QAM modulations are considered. Thus, jamming detection performances of EVM vs. RB and throughput metrics are examined against changes in the modulation type.

For the QPSK, 16-QAM, and 64-QAM modulation-type use cases, the peaks of EVM vs. RB are calculated for each SJR, and the results are presented in Figure 7a. Because the EVM measurement shows consistent results across modulation types, the proposed method can be safely used for jamming detection in system scenarios in which the modulation type changes.

On the other hand, Figure 7b shows the throghput results versus SJR for the use cases of the aforementioned modulation types. When SJR is 0 dB, the throughput for the QPSK case is 100%; therefore, no jamming signal is detected. If the system decides that there is no jamming threat by looking at this throughput result and then increases the modulation degree to 16-QAM or 64-QAM, it experiences a dramatic decrease in throughput. In other words, the jamming effect is sensed differently by using the throughput metric under different modulation-type usage conditions. However, the proposed measurement consistently

detects jamming threats independently of the chosen modulation type, thereby possessing the capability to provide reliable guidance to the system.



(**a**) (**b**)

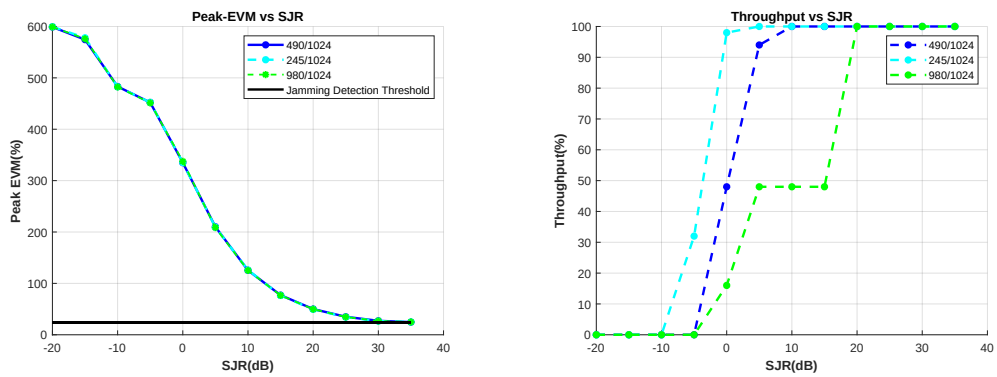
Figure 7. Effect of the Modulation Type Change, Tone Jammer. (**a**) Peak-EVM vs. SJR, and (**b**) throughput vs. SJR.

The results in Figure A4 show that this reliability of the proposed method against changes in the modulation type is also achieved for the chirp jamming case.

3.3. Reliability of the Proposed Method against Code Rate Change

In 5G systems, the code rate parameter can also be changed depending on the requirements. A code rate of 490/1024 is considered for the base scenario. In this section, code rates of 245/1024 and 980/1024 are also considered.

For the aforementioned code rate use cases, the peaks of EVM vs. RB are calculated for each SJR, and the results are shown in Figure 8a. The proposed method provides stable results without being affected by the code rate parameter; therefore, it can be safely used for jamming detection in system scenarios in which the code rate changes.



(**a**) (**b**)

Figure 8. Effect of the Code Rate Change, Tone Jammer. (**a**) Peak-EVM vs. SJR, and (**b**) Throughput vs. SJR.

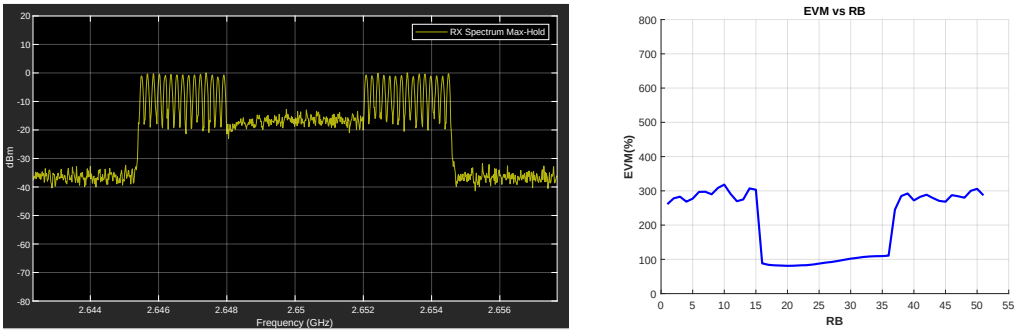
However, Figure 8b shows that different throughput results are obtained for different code rate conditions for a fixed SJR case. For example, when the SJR is 0 dB and a code rate of 245/1024 is used, the throughput approaches 100%. Therefore, the jamming effect cannot be clearly observed. If the system relies on this and decides to increase the code rate to 490/1024 or 980/1024, the throughput decreases significantly. Meanwhile, the proposed measurement can prevent such incorrect decisions, because it detects jamming threats without being affected by code rate changes.

This achievement of the proposed method for the tone-jamming scenario is also valid under chirp-jamming, as shown in Figure A5.

3.4. Change in the OFDM Subcarrier Space (SCS)

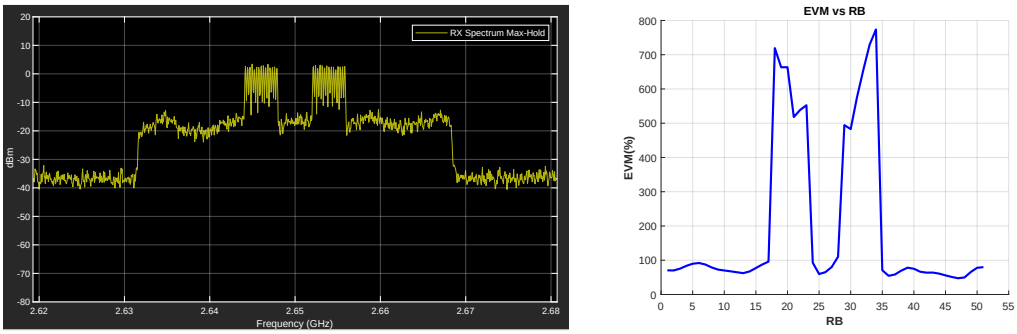
In the previous sections, simulations are performed for 30 kHz OFDM SCS use; however, 5G networks can also use OFDM SCSs of 15, 60, 120, and 240 kHz to serve other applications with different bandwidth requirements. This flexible use of different OFDM SCS corresponds to the numerology term. However, only the 15 kHz SCS option is available for LTE networks. In this section, we demonstrate that the EVM vs. RB measurement successfully detects jamming attacks for different SCS use cases. For this purpose, simulations are performed for 15 and 60 kHz SCS selections.

The jamming signal types and jamming frequencies are the same as those described in the previous sections. When the SCS is reduced from 30 to 15 kHz, the transmission bandwidth is halved, resulting in half of the jamming frequencies occupying the spectrum (Figures 9a and A6a). Conversely, when the SCS is increased to 60 kHz, all jamming frequencies are observed in the transmission bandwidth (Figures 10a and A7a). Figures 9b, 10b, A6b and A7b show that the EVM vs. RB measurement successfully detects all jamming attacks included in the transmission bandwidth regardless of the OFDM SCS applied.



(**a**) (**b**)

Figure 9. Chirp Jammer Case, SJR = −10 dB, SCS = 15 kHz. (**a**) the Rx signal spectrum and (**b**) EVM vs. RB.



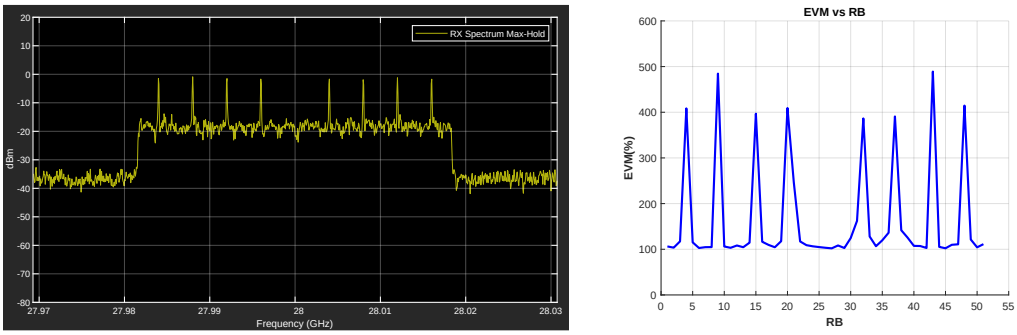
(**a**) (**b**)

Figure 10. Chirp Jammer Case, SJR = −10 dB, SCS = 60 kHz. (**a**) the Rx signal spectrum and (**b**) EVM vs. RB.

3.5. Jamming Detection for mmWave Conditions

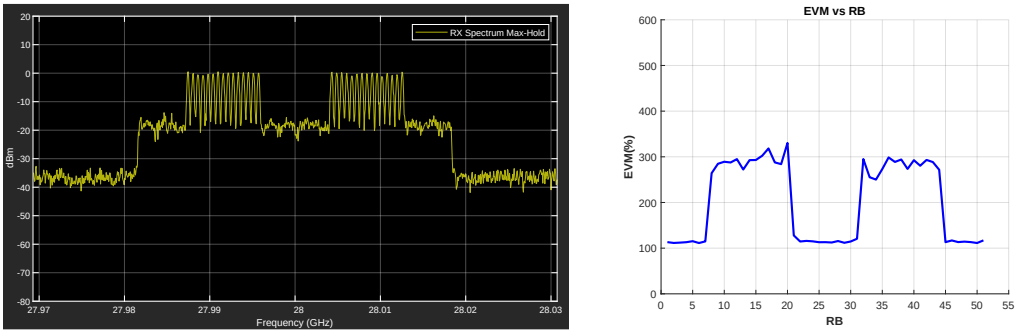
Millimeter waves encompass frequencies of 24 GHz and above. Millimeter-wave (mmWave) bands offer increased bandwidth and data transfer rates, although they have a limited coverage range. Consequently, mmWave signals rely significantly on line-of-sight (LOS) propagation to ensure effective coverage.

In the previous sections, experiments are conducted on the utilization of 5G in the sub-6 GHz frequency range. In this section, on the other hand, the channel conditions are changed, taking into consideration the deployment of 5G in the mmWave frequency band, along with the corresponding channel conditions. In this context, the carrier frequency is adjusted to 28 GHz, the transmission channel type is set to CDL-D (LOS), and OFDM SCS is configured at 60 kHz. Figures 11 and 12 show that the EVM vs. RB metric can be successfully used to detect jamming attacks under mmWave data transmission conditions.



(**a**) (**b**)

Figure 11. Tone Jammer Case, MmWave Conditions, SJR = −10 dB. (**a**) the Rx signal spectrum and (**b**) EVM vs. RB.



(**a**) (**b**)

Figure 12. Chirp Jammer Case, MmWave Conditions, SJR = −10 dB. (**a**) the Rx signal spectrum and (**b**) EVM vs. RB.

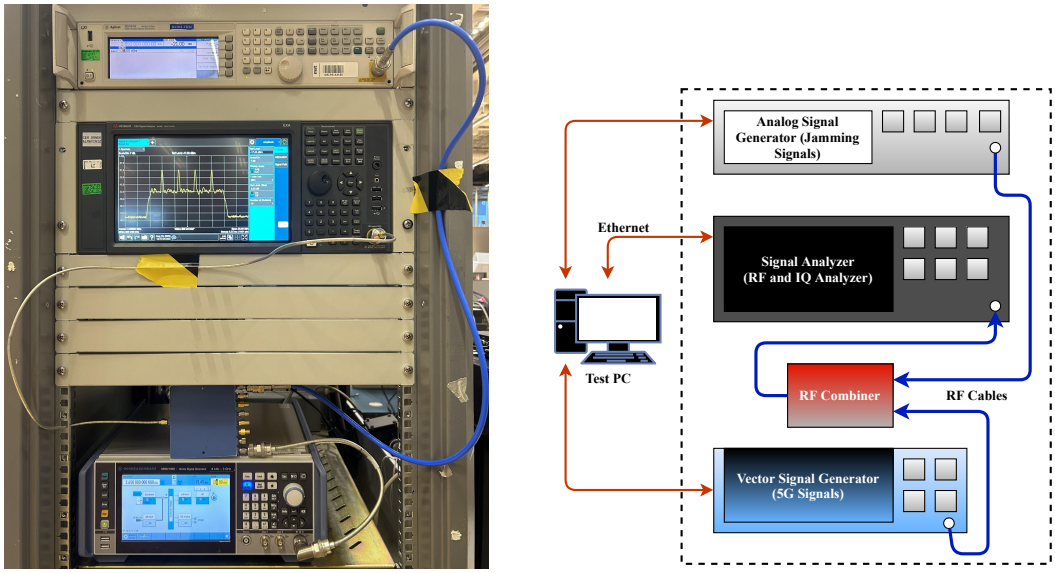
4. In-Lab Validation

In this section, the jamming detection performance of the EVM vs. RB measurement is demonstrated through experiments performed in a laboratory environment in addition to theoretical analysis and simulations. Because broadcasting interfering (jamming) signals alongside legitimate communication is illegal, experiments are performed in a closed-loop manner by adopting the following procedure to overcome this legal limitation:

First, the vector signal generator shown in Figure 13 generates a 5G signal by modulating the IQ symbols in the baseband to the RF band with OFDM. The IQ modulation, OFDM subcarrier spacing and number of OFDM subcarriers are set to 16-QAM, 30 kHz and 612, respectively, to make the generated signal similar to that in the base scenario (Section 3.1). The jamming signal, on the other hand, is generated in the RF band using the analog signal generator. The 5G signal is then contaminated with the jamming signal using the RF combiner module, and the resulting signal is transferred to the spectrum analyzer, which represents the receiver.

The spectrum analyzer calculates the RF power spectrum that provides the RSS information and performs RF demodulation to obtain IQ symbols. To calculate the EVM vs. RB data, the correct (reference) IQ symbols transmitted by the vector signal generator

and jammed IQ symbols obtained by the spectrum analyzer are transferred to the test PC. EVM vs. RB data are then obtained by calculating the EVM metric using Equation (14) for each RB.

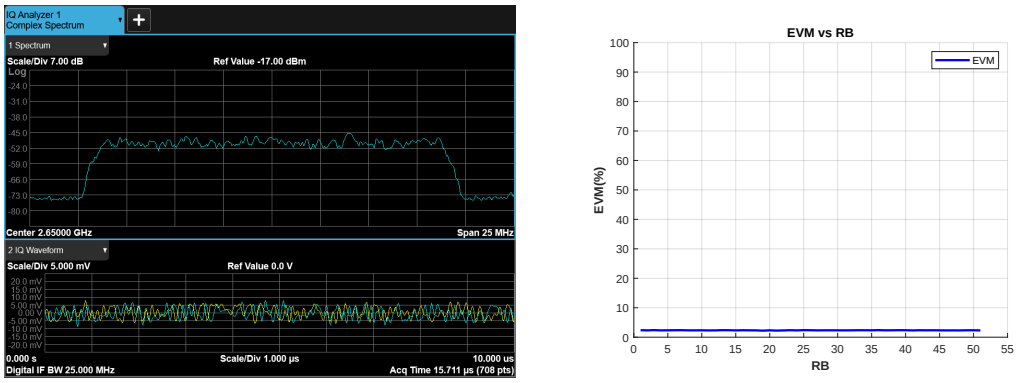


(**a**) (**b**)

Figure 13. (**a**) The hardware setup and (**b**) the block diagram of the setup.

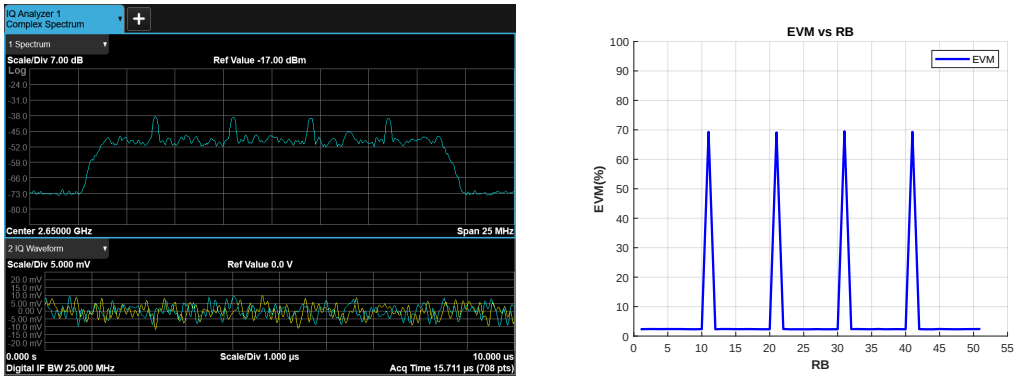
The first experiment is conducted for a no-jammer scenario. Figure 14a shows the power spectrum of the received RF signal and Figure 14b shows EVM vs. RB results. It is observed that there is no jamming signal in the spectrum other than the 5G signal, and on the other hand, the EVM values are low as expected.

Figures 15 and 16 show the results for the tone and chirp jamming cases, respectively, where SJR is −10 dB. The effects of the jamming signals on the spectrum are clearly visible in Figures 15a and 16a. In parallel, the EVM vs. RB measurement successfully reveals jamming attacks for RBs corresponding to the frequency bands exposed to the jamming signals (Figures 15b and 16b).



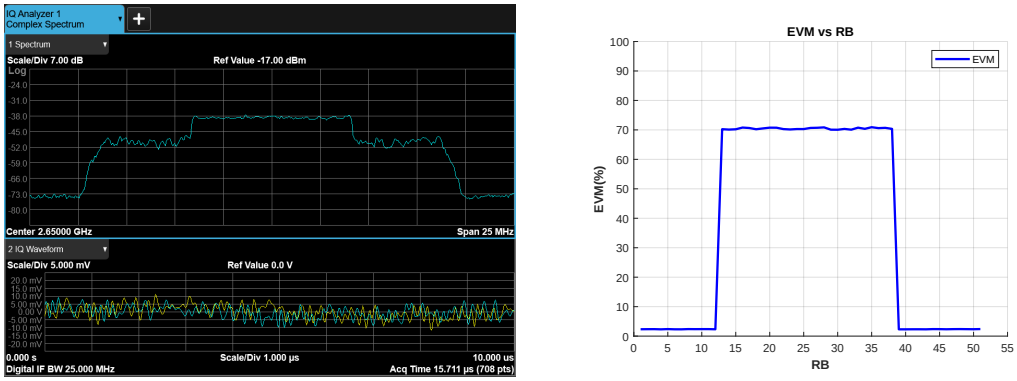
(**a**) (**b**)

Figure 14. No-Jammer Case, (**a**) the Rx signal spectrum and time-domain IQ waveform obtained after RF demodulation and (**b**) EVM vs. RB.



(**a**) (**b**)

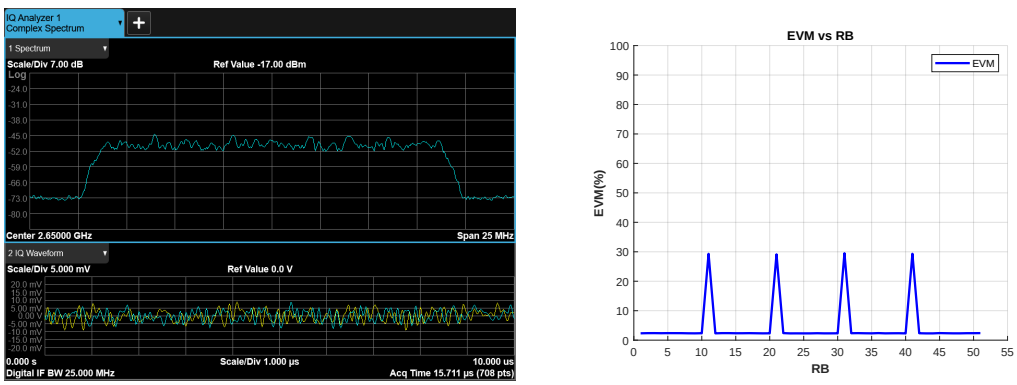
Figure 15. Tone Jammer Case, SJR = −10 dB, (**a**) the Rx signal spectrum and time-domain IQ waveform obtained after RF demodulation and (**b**) EVM vs. RB.



(**a**) (**b**)

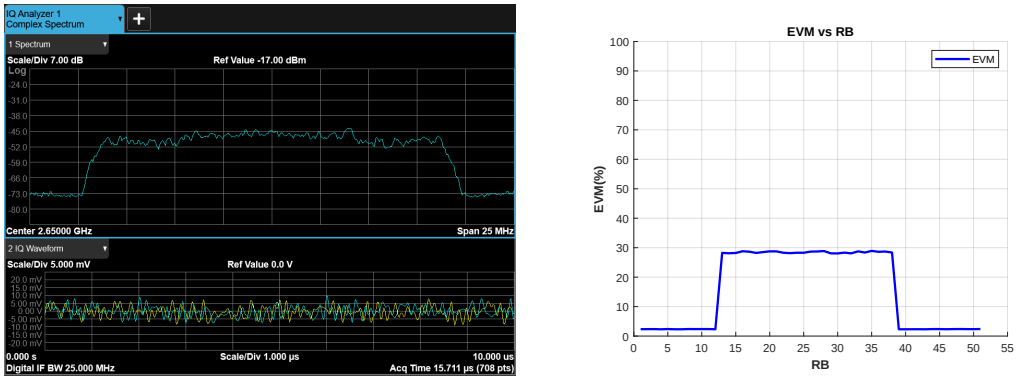
Figure 16. Chirp Jammer Case, SJR = −10 dB, (**a**) the Rx signal spectrum and time-domain IQ waveform obtained after RF demodulation and (**b**) EVM vs. RB.

In the next experiment, to test the jamming detection sensitivity of both the RF power spectrum and the EVM-vs-RB metric, the SJR parameter is set to 0 dB by reducing the power of the jamming signals by 10 dB. The results obtained for the tone and chirp jamming cases are shown in Figures 17 and 18, respectively. As shown in Figures 17a and 18a, the jamming signals become no longer detectable in the RF power spectrum. However, the EVM-vs-RB metric (Figures 17b and 18b) can still clearly detect jamming threats hidden in the spectrum.



(**a**) (**b**)

Figure 17. Tone Jammer Case, SJR = 0 dB, (**a**) the Rx signal spectrum and time-domain IQ waveform obtained after RF demodulation and (**b**) EVM vs. RB.



(**a**) (**b**)

Figure 18. Chirp Jammer Case, SJR = 0 dB, (**a**) the Rx signal spectrum and time-domain IQ waveform obtained after RF demodulation and (**b**) EVM vs. RB.

5. Discussion

The presented paper introduces a novel and efficient jamming detection method, EVM vs. RB, designed to enhance the security of next-generation communication systems against jamming attacks. The method is characterized by its ability to measure the EVM in the system, offering a direct perception of changes in jamming levels. The sensitivity success of the proposed method is a significant contribution to the field, as it enables robust detection even in the presence of small jamming signals that may remain unnoticed by other metrics.

A crucial aspect of the proposed method is its low complexity, operating at $O(N)$, and its independence from variable system parameters such as modulation degree and code rate. This independence ensures the method's adaptability to diverse communication scenarios, adding to its practicality and versatility in real-world applications.

The theoretical analysis of the proposed method begins with the construction of a 5G data transmission infrastructure based on international 3GPP standards. By incorporating a jamming attack into the system model, analytical expressions for received IQ symbols are calculated, leading to the derivation of the EVM expression. This analytical foundation establishes the groundwork for understanding the method's inner workings, particularly its capability to perceive changes in jamming levels directly.

Simulation results using MATLAB software [43] showcase the effectiveness of EVM vs. RB in providing the jammer's spectrum information. Comparative metrics, including power spectrum for Received Signal Strength (RSS), Bit Error Rate (BER), and BER-dependent throughput, are evaluated. The results demonstrate that EVM vs. RB outperforms these metrics in detecting jamming signals, even at an extreme Signal Jamming Ratio (SJR) of 25 dB. This robust performance underscores the method's resilience against varying jamming levels, reinforcing its potential as a reliable jamming detection solution.

Furthermore, the simulations reveal the stability of EVM vs. RB against changes in system parameters such as modulation degree and code rate. In contrast, metrics like throughput exhibit unreliability under such variations. This highlights the method's ability to maintain consistent performance across different communication scenarios, a critical factor for its widespread applicability.

The study extends its scope to various applications, including 5G's mmWave technology, demonstrating the versatility of EVM vs. RB across different communication technologies. The method's success is further validated through experimental studies conducted in a laboratory environment, providing empirical evidence of its effectiveness in real-world settings.

In conclusion, the proposed EVM vs. RB jamming detection method presents a compelling solution to enhance the security of next-generation communication systems. Its direct perception of jamming level changes, low complexity, and independence from variable system parameters contribute to its robustness and adaptability. The extensive theoretical analysis, simulations, and experimental studies collectively establish the method

as a promising and practical tool in the ongoing efforts to safeguard communication systems against jamming attacks.

6. Conclusions

This paper introduces a capable jamming detection method to secure LTE, 5G, and next-generation communication systems. Through the utilization of the EVM metric measured in IQ symbols, the proposed approach diverges from traditional methods based on RSS- and BER-based measurements, thereby contributing to the advancement of jamming detection methodologies.

The achieved contributions of this research are multi-faceted. First, the utilization of the EVM metric demonstrates its effectiveness in enhancing jamming detection sensitivity, surpassing existing approaches and providing a more reliable solution. Moreover, the method introduces low computational complexity. On the other hand, the provision of jammer frequency information by measuring the EVM for each RB in the received signal, a critical aspect often lacking in other methods, further fortifies the system's capabilities in understanding and counteracting jamming attacks.

A notable strength of the proposed methodology is that it provides stable results against changes in system parameters such as modulation type and code rate. This stability contributes to the reliability of the results.

The verification methods employed in this study serve to reinforce the credibility of the proposed approach. The method's successful operation in diverse system scenarios, as highlighted through extended simulation conditions, underscores its versatility and applicability in real-world situations. Theoretical analyses provide a solid foundation for the presented advantages, establishing the validity and efficacy of the jamming detection methodology. Furthermore, the conclusive demonstration of the method's success in laboratory experiments offers empirical evidence, validating its effectiveness in practical settings.

Looking ahead, the future direction of this research aims to leverage the jammer frequency information provided by the proposed method. The intention is to develop an intelligent frequency assignment strategy for anti-jamming purposes. This forward-looking approach underscores the continuous evolution of the proposed methodology, with potential applications in optimizing communication systems against sophisticated jamming attacks.

In summary, this study not only introduces a novel jamming detection method, but also substantiates its effectiveness through theoretical analysis and empirical validation. The method's low computational complexity, adaptability to varying system parameters, and seamless integration into existing communication systems position it as a promising solution for securing LTE, 5G, and future communication networks against jamming attacks. The envisioned future direction further emphasizes the potential of this methodology to contribute to intelligent anti-jamming strategies.

Author Contributions: Conceptualization, C.Ö. and M.K.; Methodology, C.Ö. and M.K.; Software, C.Ö.; Validation, C.Ö. and M.K.; Formal analysis, C.Ö.; Investigation, M.K.; Resources, C.Ö.; Data curation, C.Ö.; Writing—original draft, C.Ö.; Writing—review & editing, C.Ö. and M.K.; Supervision, M.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Most data are included in the article. All data are available upon request from the corresponding author.

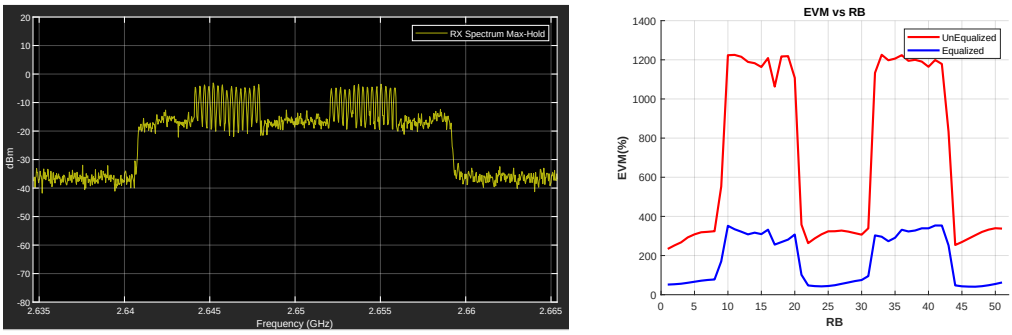
Conflicts of Interest: This work was supported by Aselsan Inc. The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

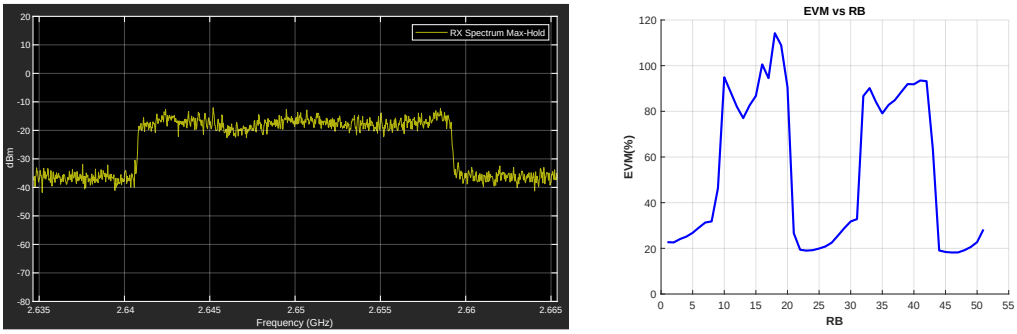
3GPP	3rd Generation Partnership Project
5G	5th Generation of Cellular Networks
BER	Bit Error Rate
CDL	Clustered Delay Line
DLSCH	Downlink Shared Channel
DM-RS	Demodulation Reference Signals
DSSS	Direct-Sequence Spread-Spectrum
EVM	Error Vector Magnitude
FFT	Fast Fourrier Transform
IQ	In-phase and Quadrature
JNSR	Jamming plus Noise-to-Signal Ratio
LOS	Line of Sight
LTE	Long-Term Evolution
MIMO	Multiple Input, Multiple Output
MMSE	Minimum Mean Squared Error
NLOS	Non-Line of Sight
OFDM	Orthogonal Frequency Division Multiplexing
PDSCH	Physical Downlink Shared Channel
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RB	Resource Block
RF	Radio Frequency
RSS	Received Signal Strength
Rx	Receive
SCS	Subcarrier Spacing
SIMO	Single Input, Multiple Output
SJR	Signal-to-Jamming Ratio
Tx	Transmit
UE	User Equipment

Appendix A



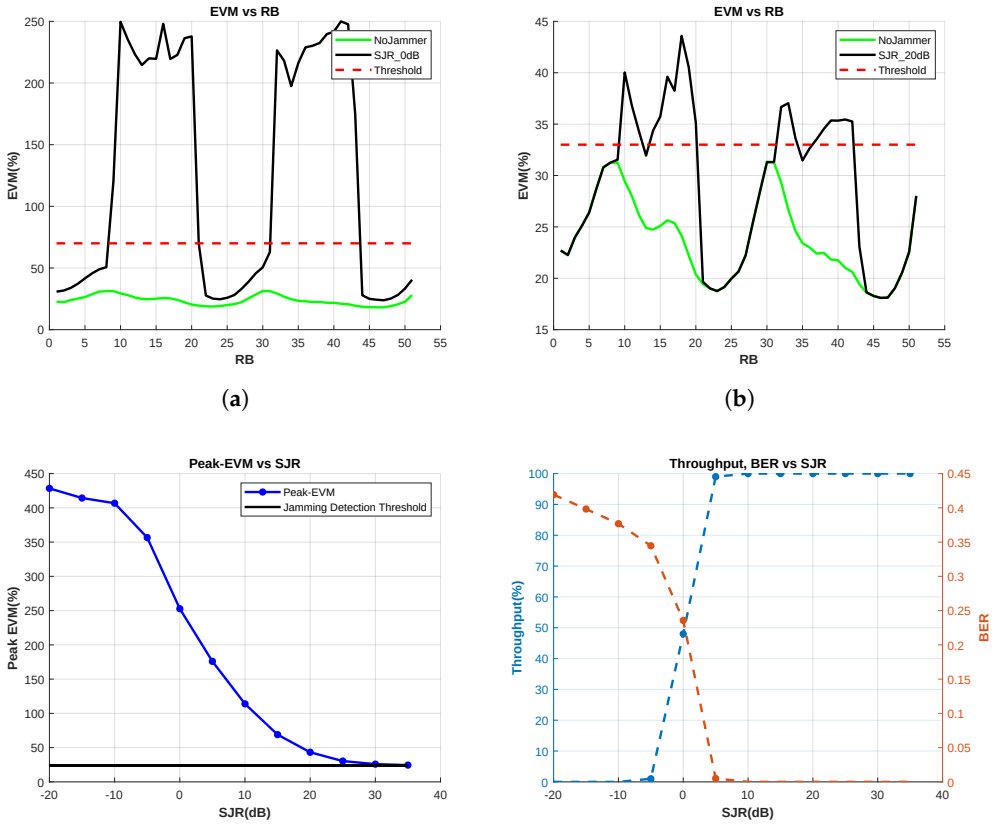
(**a**) (**b**)

Figure A1. Chirp Jammer Case, SJR = −5 dB, Obtained Throughput = %1 (BER = 0.344). (**a**) the Rx signal spectrum and (**b**) EVM vs. RB.



(**a**) (**b**)

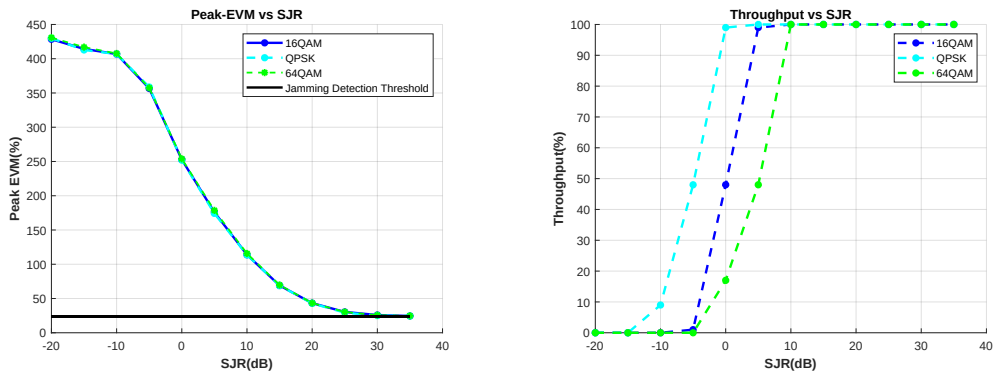
Figure A2. Chirp Jammer Case, SJR = 10 dB, Obtained Throughput = %100 (BER = 0), (**a**) the Rx signal spectrum and (**b**) EVM vs. RB.



(**a**) (**b**)

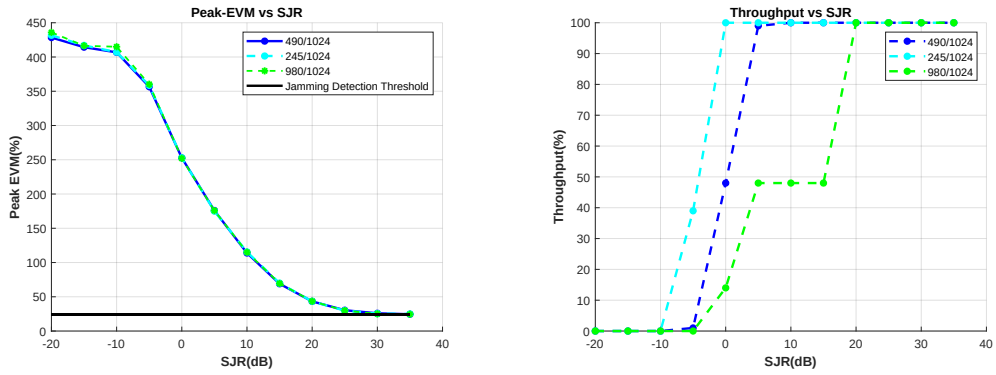
(**c**) (**d**)

Figure A3. EVM vs. RB , BER and Throughput Measurements for Chirp Jammer, (**a**) EVM vs. RB for SJR = 0 dB, (**b**) EVM vs. RB for SJR = 20 dB, (**c**) Peak-EVM vs. SJR, and (**d**) Throughput and BER vs. SJR.



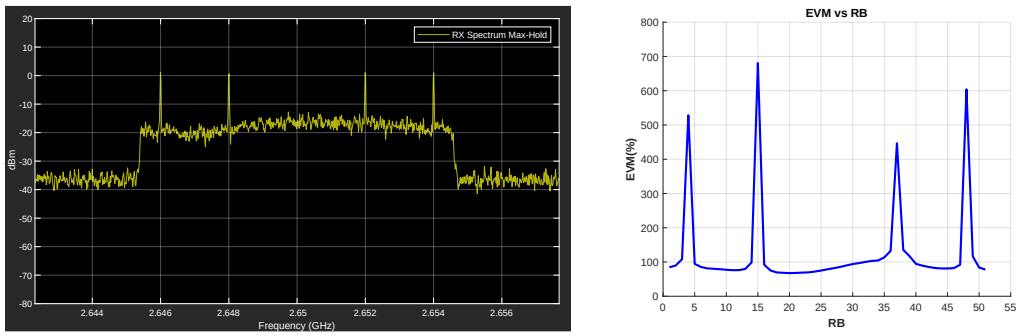
(**a**) (**b**)

Figure A4. Effect of the Modulation Type Change, Chirp Jammer. (**a**) Peak-EVM vs. SJR, and (**b**) Throughput vs. SJR.



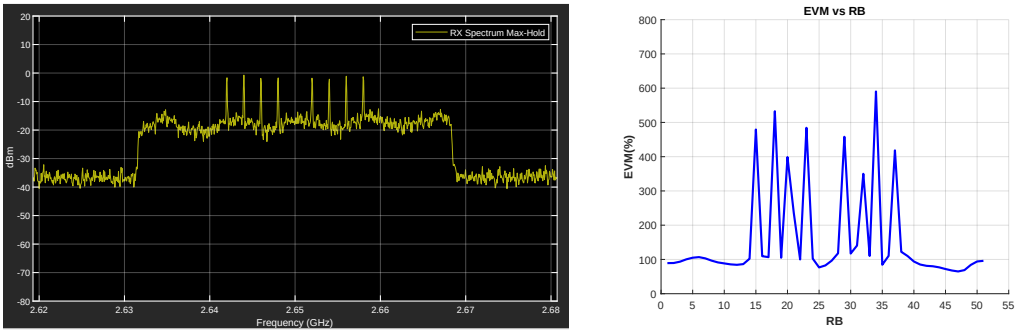
(**a**) (**b**)

Figure A5. Effect of the Code Rate Change, Chirp Jammer. (**a**) Peak-EVM vs. SJR, and (**b**) Throughput vs. SJR.



(**a**) (**b**)

Figure A6. Tone Jammer Case, SJR = −10 dB, SCS = 15 kHz. (**a**) the Rx signal spectrum and (**b**) EVM vs. RB.



(**a**) (**b**)

Figure A7. Tone Jammer Case, SJR = −10 dB, SCS = 60 kHz. (**a**) the Rx signal spectrum and (**b**) EVM vs. RB.

References

1. Pirayesh, H.; Zeng, H. Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 767–809. [CrossRef]
2. Grover, K.; Lim, A.; Yang, Q. Jamming and anti-jamming techniques in wireless networks: A survey. *Int. J. Ad Hoc Ubiquitous Comput.* **2014**, *17*, 197. [CrossRef]
3. Xu, H.; Cheng, Y.; Wang, P. Jamming Detection in Broadband Frequency Hopping Systems Based on Multi-Segment Signals Spectrum Clustering. *IEEE Access* **2021**, *9*, 29980–29992. [CrossRef]
4. Liu, Z.; Liu, H.; Xu, W.; Chen, Y. An Error-Minimizing Framework for Localizing Jammers in Wireless Networks. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 508–517. [CrossRef]
5. Mughal, M.O.; Dabcevic, K.; Marcenaro, L.; Regazzoni, C.S. Compressed sensing based jammer detection algorithm for wide-band cognitive radio networks. In Proceedings of the 2015 3rd International Workshop on Compressed Sensing Theory and Its Applications to Radar, Sonar and Remote Sensing (CoSeRa), Pisa, Italy, 17–19 June 2015 ; pp. 119–123. [CrossRef]
6. Hamdy, A.; Digham, F.; Nasr, O.A.; Mourad, H.M. Automatic detection of jammer interference in GSM networks. In Proceedings of the 2018 International Conference on Innovative Trends in Computer Engineering (ITCE), Aswan, Egypt, 19–21 February 2018; pp. 248–252. [CrossRef]
7. Ferre, R.M.; Richter, P.; Fuente, A.D.L.; Lohan, E.S. In-lab validation of jammer detection and direction finding algorithms for GNSS. In Proceedings of the 2019 International Conference on Localization and GNSS (ICL-GNSS), Nuremberg, Germany, 4–6 June 2019; pp. 1–6. [CrossRef]
8. Xu, S.; Xu, W.; Pan, C.; Elkashlan, M. Detection of Jamming Attack in Non-Coherent Massive SIMO Systems. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2387–2399. [CrossRef]
9. Akhlaghpasand, H.; Razavizadeh, S.M.; Björnson, E.; Do, T.T. Jamming Detection in Massive MIMO Systems. *IEEE Wirel. Commun. Lett.* **2018**, *7*, 242–245. [CrossRef]
10. Eygi, M.; Kurt, G.K. Jamming Detection: A Multicarrier Approach. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018; pp. 1–4. [CrossRef]
11. Chen, X.; Yang, W. Detection of Jamming in DSSS Systems Using FRESH Filters. In Proceedings of the 2020 IEEE 3rd International Conference of Safe Production and Informatization (IICSPI), Chongqing, China, 28-30 November 2020; pp. 320–325. [CrossRef]
12. Choi, J.; Mughal, M.O.; Choi, Y.; Kim, D.; Lopez-Salcedo, J.A.; Kim, S. CUSUM-based Joint Jammer Detection and Localization. In Proceedings of the 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Republic of Korea, 22–25 October 2018; pp. 1–5. [CrossRef]
13. Eriksson, G.; Hansson, A. Derivation of detection times for a simple follower-jammer model used in mobile ad hoc-network simulations. In Proceedings of the 2019 International Conference on Military Communications and Information Systems (ICMCIS), Budva, Montenegro, 14–15 May 2019; pp. 1–5. [CrossRef]
14. Mohammadi, J.; Stańczak, S.; Zheng, M. Joint spectrum sensing and jamming detection with correlated channels in cognitive radio networks. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 889–894. [CrossRef]
15. Liu, M.; Jin, L.; Shang, B. LSTM-Based Jamming Detection for Satellite Communication with Alpha-Stable Noise. In Proceedings of the 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Nanjing, China, 29 March 2021; pp. 1–5. [CrossRef]
16. Malebary, S.; Xu, W.; Huang, C.-T. Jamming mobility in 802.11p networks: Modeling, evaluation, and detection. In Proceedings of the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9–11 December 2016; pp. 1–7. [CrossRef]
17. Manju, V.C.; Kumar, M.S. Detection of jamming style DoS attack in Wireless Sensor Network. In Proceedings of the 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, India, 6–8 December 2012; pp. 563–567. [CrossRef]

18. Bodkhe, A.A.; Raut, A.R. Identifying Jammers in Wireless Sensor Network with an Approach to Defend Reactive Jammer. In Proceedings of the 2014 Fourth International Conference on Communication Systems and Network Technologies, Bhopal, India, 7–9 April 2014; pp. 89–92. [CrossRef]
19. Yu, B.; Zhang, L.-Y. An improved detection method for different types of jamming attacks in wireless networks. In Proceedings of the 2014 2nd International Conference on Systems and Informatics (ICSAI 2014), Shanghai, China, 15–17 November 2014; pp. 553–558. [CrossRef]
20. Marttinen, A.; Wyglinski, A.M.; Jäntti, R. Statistics-Based Jamming Detection Algorithm for Jamming Attacks against Tactical MANETs. In Proceedings of the 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 6–8 October 2014; pp. 501–506. [CrossRef]
21. Sufyan, N.; Saqib, N.A.; Zia, M. Detection of jamming attacks in 802.11b wireless networks. *J. Wirel. Commun. Netw.* **2013**, *2013*, 208. [CrossRef]
22. Liu, G.; Liu, J.; Li, Y.; Xiao, L.; Tang, Y. Jamming Detection of Smartphones for WiFi Signals. In Proceedings of the 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015; pp. 1–3. [CrossRef]
23. Duan, B.; Yin, D.; Cong, Y.; Zhou, H.; Xiang, X.; Shen, L. Anti-Jamming Path Planning for Unmanned Aerial Vehicles with Imperfect Jammer Information. In Proceedings of the 2018 IEEE International Conference on Robotics and Biomimetics (ROBIO), Kuala Lumpur, Malaysia, 12–15 December 2018; pp. 729–735. [CrossRef]
24. Arjoune, Y.; Salahdine, F.; Islam, M.S.; Ghribi, E.; Kaabouch, N. A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication. In Proceedings of the 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 7–10 January 2020; pp. 459–464. [CrossRef]
25. Jahanshahi, J.A.; Ghorashi, S.A.; Eslami, M. A support vector machine based algorithm for jamming attacks detection in cellular networks. In Proceedings of the 2011 Wireless Advanced, London, UK, 20–22 June 2011; pp. 180–184. [CrossRef]
26. Puñal, O.; Aktaş, I.; Schnelke, C.-J.; Abidin, G.; Wehrle, K.; Gross, J. Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation. In Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, Sydney, NSW, Australia, 19 June 2014; pp. 1–10. [CrossRef]
27. Upadhyaya, B.; Sun, S.; Sikdar, B. Machine Learning-based Jamming Detection in Wireless IoT Networks. In Proceedings of the 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), Singapore, 28–30 August 2019; pp. 1–5. [CrossRef]
28. Spuhler, M.; Giustiniano, D.; Lenders, V.; Wilhelm, M.; Schmitt, J.B. Detection of Reactive Jamming in DSSS-based Wireless Communications. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1593–1603. [CrossRef]
29. Osanaiye, O.; Alfa, A.S.; Hancke, G.P. A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. *Sensors* **2018**, *18*, 1691. [CrossRef] [PubMed]
30. Morales Ferre, R.; de la Fuente, A.; Lohan, E.S. Jammer Classification in GNSS Bands Via Machine Learning Algorithms. *Sensors* **2019**, *19*, 4841. [CrossRef] [PubMed]
31. Shi, Y.; Davaslioglu, K.; Sagduyu, Y.E.; Headley, W.C.; Fowler, M.; Green, G. Deep Learning for RF Signal Classification in Unknown and Dynamic Spectrum Environments. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11–14 November 2019; pp. 1–10. [CrossRef]
32. Li, T.; Wang, M.; Peng, D.; Yang, X. Identification of Jamming Factors in Electronic Information System Based on Deep Learning. In Proceedings of the 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, China, 8–11 October 2018; pp. 1426–1430. [CrossRef]
33. Zhang, N.; Li, Y.; Shi, Y.; Shen, J. A CNN-Based Adaptive Federated Learning Approach for Communication Jamming Recognition. *Electronics* **2023**, *12*, 3425. [CrossRef]
34. Shen, J.; Li, Y.; Zhu, Y.; Wan, L. Cooperative Multi-Node Jamming Recognition Method Based on Deep Residual Network. *Electronics* **2022**, *11*, 3280. [CrossRef]
35. Vinogradova, J.; Björnson, E.; Larsson, E.G. Detection and mitigation of jamming attacks in massive MIMO systems using random matrix theory. In Proceedings of the 2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Edinburgh, UK, 3–6 July 2016; pp. 1–5. [CrossRef]
36. Yang, X.; Li, A.; Wei, M.; Zhang, X.; Lu, S.; Wang, W. Jamming Signal Detection Based on TSVD Method. In Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA), Dalian, China, 25–27 August 2020; pp. 558–562. [CrossRef]
37. Örnek, C.; Kartal, M. An Efficient EVM Based Jamming Detection in 5G Networks. In Proceedings of the 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Amman, Jordan, 6–8 December 2022; pp. 130–135. [CrossRef]
38. Alakoca, H.; Kurt, G.K.; Ayyıldız, C. PHY based Jamming attacks against OFDM systems: A measurement study. In Proceedings of the 2017 25th Telecommunication Forum (TELFOR), Belgrade, Serbia, 21–22 November 2017; pp. 1–4. [CrossRef]
39. Bilodeau-Robitaille, O.; Gagnon, F. Digital RF Memory Jamming on OFDM SISO. In Proceedings of the 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 6–8 October 2014; pp. 1542–1548. [CrossRef]
40. Örnek, C.; Kartal, M. Work-in-Progress: An Efficient EVM Based Hybrid Jammer Localization Method for 5G Networks. In Proceedings of the 2023 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Istanbul, Turkiye, 4–7 July 2023; pp. 408–413. [CrossRef]
41. Zheng, K.; Jia, X.; Chi, K.; Liu, X. DDPG-Based Joint Time and Energy Management in Ambient Backscatter-Assisted Hybrid Underlay CRNs. *IEEE Trans. Commun.* **2023**, *71*, 441–456. [CrossRef]

42. Zheng, K.; Luo, R.; Wang, Z.; Liu, X.; Yao, Y. Short-Term and Long-Term Throughput Maximization in Mobile Wireless-Powered Internet of Things. *IEEE Internet Things J.* **2023** . [CrossRef]
43. *MATLAB R2021a*; The MathWorks, Inc.: Natick, MA, USA, 2021.
44. *3GPP TS 38.212. NR*; Multiplexing and Channel Coding. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network: Sophia Antipolis Cedex, France, 2020.
45. *3GPP TS 38.202. NR*; Services Provided by the Physical Layer. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network: Sophia Antipolis Cedex, France, 2020.
46. *3GPP TS 38.214. NR*; Physical Layer Procedures for Data. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network: Sophia Antipolis Cedex, France, 2020.
47. *3GPP TS 38.211. NR*; Physical Channels and Modulation. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network: Sophia Antipolis Cedex, France, 2020.
48. *3GPP TR 38.901. 5G*; Study on Channel Model for Frequencies from 0.5 to 100 GHz. Technical Specification Group Radio Access Network: Sophia Antipolis Cedex, France, 2020.
49. Paulraj, A.; Nabar, R.; Gore, D. *Introduction to Space-Time Wireless Communications*; Cambridge University Press: Cambridge, UK, 2003; pp. 84–186.
50. Arjoune, Y.; Faruque, S. Smart Jamming Attacks in 5G New Radio: A Review. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 1010–1015. [CrossRef]