ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

DOTTORATO DI RICERCA IN

INGEGNERIA ELETTRONICA, TELECOMUNICAZIONI E TECNOLOGIE DELL'INFORMAZIONE

Ciclo 37

Settore Concorsuale: 09/F2 - TELECOMUNICAZIONI

Settore Scientifico Disciplinare: ING-INF/03 - TELECOMUNICAZIONI

TOWARDS INTELLIGENT SPECTRUM AWARENESS IN WIRELESS NETWORKS

Presentata da: Luca Arcangeloni

Coordinatore Dottorato

Davide Dardari

Supervisore

Andrea Giorgetti

Co-supervisore

Enrico Paolini

Esame finale anno 2025

ALMA MATER STUDIORUM
UNIVERSITY OF BOLOGNA

PH.D. PROGRAMME
ELECTRONICS, TELECOMMUNICATIONS, AND
INFORMATION TECHNOLOGIES ENGINEERING
(ETIT)

SSD ING/INF 03
SC 09/F2 Telecomunicazioni

TOWARDS INTELLIGENT SPECTRUM AWARENESS IN WIRELESS NETWORKS

Ph.D. Thesis

Ph.D. candidate
LUCA ARCANGELONI

Ph.D. coordinator
Prof. Ing.
DAVIDE DARDARI

Supervisor
Prof. Ing.
ANDREA GIORGETTI

XXXVII CYCLE

KEYWORDS

Spectrum Awareness

Spectrum Sensing

Jamming Detection

Latent Variable Models

Statistical Signal Processing

"So far, so good."
Vinz, La Haine, 1995

Acknowledgments

This work was partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, Mission 4, Component 2, Investment 1.3, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

Abstract

In the era of 6G communication, the demand for efficient radio spectrum utilization is rapidly increasing due to the proliferation of wireless devices like sensors, connected vehicles, and smart infrastructure. Future 6G networks will need to manage a highly congested spectrum, requiring novel strategies that go beyond the advancements of 5G. Among the key developments in 6G are integrated sensing and communication (ISAC) systems, which simultaneously enable data transmission and environmental sensing. This innovation is critical for applications such as traffic monitoring, autonomous driving, and urban safety. However, the complexity and intelligence of these systems introduce security vulnerabilities, particularly in the form of radar-related threats like deceptive jamming, which can compromise sensing functions.

Artificial intelligence (AI) will also be embedded into 6G networks, playing a crucial role in network orchestration, spectrum management, and system optimization. While AI offers great potential for enhancing efficiency, it also opens the door to new threats, such as unauthorized spectrum use, signal jamming, and denial-of-service attacks. These risks are amplified by AI-enabled attackers who can adapt their strategies dynamically, making detection more challenging. Hence, safeguarding 6G networks requires robust monitoring mechanisms for spectrum usage to detect anomalies and prevent improper use.

This thesis introduces a novel spectrum patrolling framework designed to secure wireless networks by monitoring radio-frequency (RF) environments through distributed sensors. The framework collects RF data and employs advanced signal processing techniques to extract meaningful analytics. These insights help in identifying and mitigating potential threats such as jammers

and unauthorized spectrum users.

The framework's key contributions include a blind source separation (BSS) technique designed to separate malicious signals from legitimate traffic. In addition, jamming attacks are identified through the application of causal inference using the transfer entropy (TE). Jamming detection is further addressed within an ISAC context, where a variational autoencoder (VAE)-based approach harnesses the capabilities of deep latent variable models. Moreover, the thesis investigates cooperative wideband spectrum sensing (WSS) through the use of factor analysis and variational inference, allowing for a detailed assessment of spectrum occupancy, aiding in user count estimation and noise power measurement. In the domain of cooperative WSS, a statistical meta-analysis approach is also introduced to improve the synthesis of multiple independent tests.

The adoption of spectrum patrol for jamming detection was validated in an ad hoc wireless network, considering key factors such as the medium access protocol (MAC) protocol, packet collisions, sensor spatial density, and channel impairments like path loss and shadowing. For identifying deceptive jammers in an ISAC context, a monostatic multiple-input multiple-output (MIMO)-orthogonal frequency-division multiplexing (OFDM) system was employed. Lastly, the cooperative WSS approach was developed with a focus on the presence of multiple primary users (PUs), a network of secondary user (SU) sensors, and the impact of shadowing and multipath propagation. The numerical results obtained through extensive and exhaustive simulations demonstrate that the proposed framework is consistent and can achieve the required performance.

Contents

List of Tables

List of Figures

Acronyms

ACK acknowledgment
AD anomaly detection
ADC analog to digital converter
AE autoencoder
AI artificial intelligence
AoA angle of arrival
AoD angle of departure
AP access point
AR auto-regressive
AvOCC all-versus-one cross correlation
AvOTE all-versus-one transfer entropy
AWGN additive white Gaussian noise
BMA basic mass assignment
BPR bad packet ratio
BS base station
BSS blind source separation
CAVI coordinate ascent variational inference
c.d.f. cumulative distribution function
CNN convolutional neural network
CR cognitive radio
CS compressed sensing
DBSS determined blind source separation
DFT discrete Fourier transform
DNN deep neural network
d.o.f. degrees of freedom

DoS denial-of-service
DRFM digital radio frequency memory
DSSS direct sequence spread spectrum
EIRP effective isotropic radiated power
ECCM electronic counter-countermeasures
ECM electronic countermeasure
ED energy detector
ELBO evidence lower bound
EPA extended pedestrian A
ETU extended typical urban
EVA extended vehicular A
FC fusion centre
FFT fast Fourier transform
FL federated learning
FPGA field-programmable gate array
GC Granger causality
GLRT generalized likelihood ratio test
GMM Gaussian mixture model
GNSS Global Navigation Satellite System
ICA independent component analysis
IoT internet of things
IRS intelligent reflecting surface
ISAC integrated sensing and communication
ITU International Telecommunication Union
i.i.d. independent, identically distributed
KL Kullback–Leibler
LoRa Long Range
LoRaWAN Long Range Wide Area Network
LOS line-of-sight
LRT likelihood ratio test
LS least squares
LTI linear time-invariant
MAC medium access protocol

MC Monte Carlo
MIMO multiple-input multiple-output
ML machine learning
MLE maximum likelihood estimation
MSE mean-square error
NN neural network
NLOS non-line-of-sight
NR new radio
NRMSE normalized root mean square error
OFDM orthogonal frequency-division multiplexing
OMP orthogonal matching pursuit
PCA principal component analysis
p.d.f. probability density function
PDR packet delivery ratio
PDSCH-DMRS physical downlink shared channel-demodulation reference signal
PU primary user
QPSK quadrature phase shift keying
RCS radar cross-section
RE resource element
ReLU rectified linear unit
RF radio-frequency
ROC receiver operating characteristic
RMSE root mean squared error
RSS received signal strength
r.v. random variable
SAE sparse autoencoder
SF spreading factor
SINR signal-to-interference plus noise ratio
SJR signal-to-jammer ratio
SNR signal-to-noise ratio
SSIR signal-to-self interference ratio
SU secondary user

SVD singular value decomposition
TDMA time division multiple access
TE transfer entropy
UAV unmanned aerial vehicle
UBSS underdetermined blind source separation
UE user equipment
ULA uniform linear array
WSS wideband spectrum sensing
VAE variational autoencoder
VBFA variational Bayes factor analysis
VI variational inference

Mathematical Notation

Throughout the thesis, capital boldface letters denote matrices, lowercase bold letters denote vectors, $(\cdot)^{-1}$ indicates the inverse operator, $||\cdot||_p$ is the l_p-norm, $|\cdot|$ is the module operator, $\odot$ stands for the element-wise product, and $\otimes$ stands for Kronecker product. $(\cdot)^{\mathsf{T}}$ and $(\cdot)^{\mathsf{H}}$ denote, respectively, simple and Hermitian transposition, while $(\cdot)^*$ denotes the conjugate operations. With $v_{i,j}$, $\mathbf{v}_{i,:}$, and $\mathbf{v}_{:,j}$, we represent, respectively, the element, the ith row, and the jth column of the matrix $\mathbf{V}$, and with $\mathbf{v}_{i,j:k}$ we select the elements between the jth and the kth entry of the ith row of $\mathbf{V}$, extremes included. $\mathbf{I}_N$ indicates the $N \times N$ identity matrix. $\mathbb{1}_{\{\mathcal{A}\}}$ is the indicator function equal to one when $\mathcal{A}$ is true and zero otherwise. $\det(\mathbf{V})$ and $\mathrm{tr}(\mathbf{V})$ stand, respectively, for the determinant and the trace of the matrix $\mathbf{V}$. $\mathrm{diag}(\mathbf{V})$ represents the vector containing the diagonal elements of the matrix $\mathbf{V}$, while $\mathrm{diag}(\mathbf{v})$ denotes the diagonal matrix with the elements of the vector $\mathbf{v}$ on its diagonal. $\mathbb{E}[\cdot]$ denotes the expectation operator, $\langle\cdot\rangle$ indicates the sample mean operator. We use $\mathcal{N}(\mu, \sigma^2)$ to denote a real Gaussian distribution with mean μ and variance σ^2, $\mathcal{CN}(0, \sigma^2)$ to denote a zero-mean circularly symmetric complex Gaussian distribution with variance σ^2, χ^2_m to denote a central chi squared distribution with m degrees of freedom (d.o.f.), and $\mathcal{U}(a, b)$ to denote a uniform distribution between a and b. To streamline the presentation and in keeping with common convention, we extend the notation for statistical distributions to denote their probability density functions (p.d.f.s) as well; for instance, $p(x) = \mathcal{N}(\mu, \sigma^2)$ indicates that $p(x)$ represents the p.d.f. of a normal distribution with respect to the variable x, where μ and σ^2 are the mean and variance, respectively. We use $Q(x)$ for the Q-function value in x. Finally, we use the big O notation, $\mathcal{O}(\cdot)$, to denote the computational complexity of algorithms.

Symbol	Description
$\mathbf{V}$	Matrix (capital boldface letter)
$\mathbf{v}$	Vector (lowercase boldface letter)
$v_{i,j}$	Element at row i and column j of matrix $\mathbf{V}$
$\mathbf{v}_{i,:}$	ith row of matrix $\mathbf{V}$
$\mathbf{v}_{:,j}$	jth column of matrix $\mathbf{V}$
$\mathbf{v}_{i,j:k}$	Elements between jth and kth entry of ith row of $\mathbf{V}$
$(\cdot)^{\mathsf{T}}$	Simple transposition
$(\cdot)^{\mathsf{H}}$	Hermitian transposition
$(\cdot)^{*}$	Conjugate operator
$(\cdot)^{-1}$	Inverse operator
$\|\| \cdot \|\|_p$	l_p-norm
$\| \cdot \|$	Module operator
$\odot$	Element-wise product
$\otimes$	Kronecker product
$\mathbf{I}_N$	$N \times N$ identity matrix
$\mathbb{1}_{\{\mathcal{A}\}}$	Indicator function (1 if $\mathcal{A}$ is true, 0 otherwise)
$\det(\mathbf{V})$	Determinant of matrix $\mathbf{V}$
$\mathrm{tr}(\mathbf{V})$	Trace of matrix $\mathbf{V}$
$\mathrm{diag}(\mathbf{V})$	Vector of diagonal elements of matrix $\mathbf{V}$
$\mathrm{diag}(\mathbf{v})$	Diagonal matrix with elements of vector $\mathbf{v}$ on the diagonal
$\mathbb{E}[\cdot]$	Expectation operator
$\langle \cdot \rangle$	Sample mean operator
$\mathcal{N}(\mu, \sigma^2)$	Real Gaussian distribution with mean μ and variance σ^2
$\mathcal{CN}(0, \sigma^2)$	Zero-mean circularly symmetric complex Gaussian distribution
χ^2_m	Central chi-squared distribution with m degrees of freedom
$\mathcal{U}(a, b)$	Uniform distribution between a and b
$Q(x)$	Q-function value at x
$\mathcal{O}(\cdot)$	Big O notation (computational complexity)

Table 1: List of symbols and their descriptions.

Chapter 1

Introduction

In the coming era of 6G communication systems, the demand for radio spectrum resources is expected to skyrocket, driven by billions of wireless devices such as sensors, connected vehicles, and smart infrastructures. To accommodate this massive increase in connectivity, a fundamental shift in wireless technology will be required. While 6G will likely build upon the advancements made in 5G, entirely new strategies will be necessary to achieve the next leap in network performance. Researchers are already pushing the boundaries of technology to create denser networks, increase bandwidth, reduce latency, and improve reliability. To meet these ambitious goals, intelligent devices with adaptive learning and decision-making capabilities will play a central role. These future 6G devices will employ advanced spectrum awareness tools, leveraging learning and inference techniques to optimize the use of available resources [2].

One of the emerging innovations within 6G is the concept of integrated sensing and communication (ISAC) systems, which promise to revolutionize applications like traffic monitoring, autonomous driving, and urban safety. ISAC systems enable the simultaneous use of wireless signals for both communication and environmental sensing, leading to enhanced situational awareness and optimized resource use. However, despite these promising advancements, the increasing complexity and intelligence of 6G networks introduce significant vulnerabilities. Specifically, ISAC systems are vulnerable to radar-

related security threats, such as deceptive jamming, which can impair their sensing functions.

Furthermore, artificial intelligence (AI), widely recognized as a fundamental driver of autonomous decision-making, is expected to be fully embedded in heterogeneous mobile radio systems, enhancing network orchestration, spectrum management, localization, and overall system optimization. While AI will enhance efficiency and connectivity, it will also expose networks to new risks, such as unauthorized spectrum use, signal jamming, and denial-of-service attacks. For instance, AI-enabled attackers could dynamically adapt their strategies in response to network conditions, making their activities harder to detect and mitigate. These challenges highlight the urgent need to ensure the resilience and security of future communication infrastructures.

In this context, real-time monitoring of radio spectrum usage becomes paramount for regulatory compliance and the prevention of improper use. As communication technology becomes more deeply integrated into society, large-scale spectrum patrolling will be crucial in safeguarding wireless networks. Understanding how networks interact with the wireless medium will be essential for developing effective strategies for spectrum monitoring and maintaining the integrity of next-generation communication systems.

1.1 Spectrum Patrolling

A spectrum patrolling mechanism can be employed to enhance the security of next-generation wireless networks. Fig. 1.1 illustrates a scenario where UAVs serve as spectrum patrol units, collecting data on the radio-frequency (RF) environment. This information is then transmitted to an authority, acting as a fusion center, which extracts wireless network analytics. These analytics are subsequently used to identify anomalies and detect malicious actors, such as jammers, that may be interfering with the network.

The patrol system may consist of a dedicated device, a network provided by the authority, or a crowdsourced platform. In the latter case, users periodically sense the spectrum and relay refined data to operators or regulatory bodies [3]. This information is analyzed to generate comprehensive network

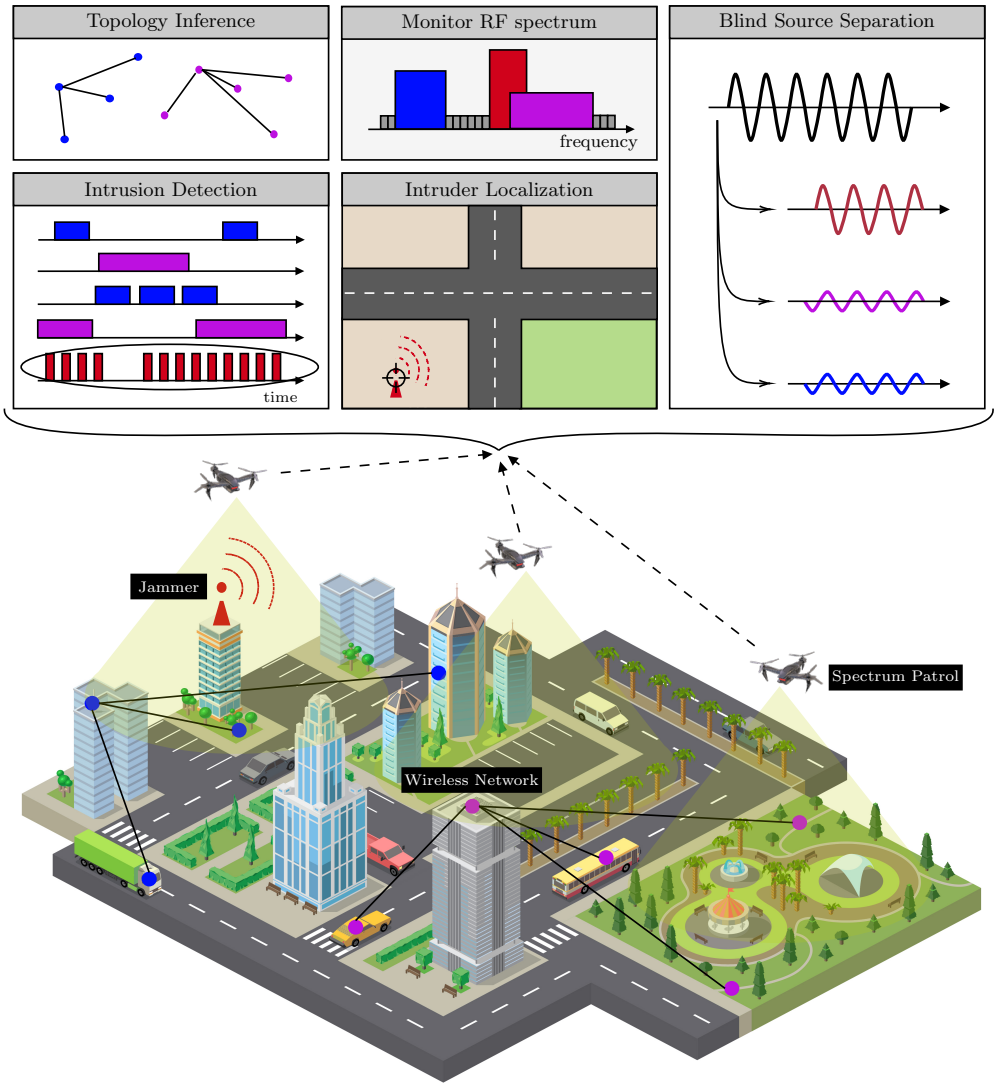

Figure 1.1: An illustration of wireless networks that has been disrupted by an intelligent jamming device. Unmanned aerial vehicles (UAVs), which are monitoring the RF environment as part of a spectrum patrol, apply advanced analytics extraction techniques to gain valuable insights from the data. The aim is to obtain as much information as possible about the situation and eventually identify the jammer. The extracted analytics are then forwarded to the authority in charge so that it can secure the environment. Urban image designed by *vectorpocket* in *http://www.freepik.com*.

analytics, providing the regulator with a detailed overview of the RF environment. Such insights enable the timely detection of anomalies or unauthorized users, allowing for effective measures to secure the network.

The ability to extract and analyze complex features of the wireless network, from the physical layer to the application layer, will be essential for identifying threats such as jammers and unauthorized spectrum users. Moreover, this capability will play a pivotal role in optimizing communication processes and facilitating spectrum reuse [4, 5]. In this section, we propose a set of key characteristics that can enable spectrum patrolling to effectively orchestrate and protect next-generation wireless networks and their users.

Monitor the RF Spectrum. Although reliable communication is essential, the current method of spectrum monitoring still heavily relies on regulators using expensive, power-hungry laboratory-grade spectrum analyzers [2]. This traditional approach is both inefficient and not scalable. In contrast, future wireless networks require a continuous and thorough spectrum monitoring strategy to promptly address security issues, ensuring complete coverage across the temporal, frequency, and spatial domains [6]. Utilizing data-driven spectrum sensing algorithms transforms spectrum monitoring into a dynamic process, offering a real-time overview of the RF spectrum usage. This technique enables the identification of active and inactive frequency bands, supporting the detection of unauthorized activities within regulated frequency ranges.

Topology Inference. The ability to reconstruct the network's topology from limited observations at certain nodes or edges, with minimal or no prior information, would greatly enhance the effectiveness of spectrum patrolling [2, 7]. While this task is already complex in wired networks, it becomes even more difficult in wireless environments due to interference, path loss, shadowing, fading, and the hidden terminal problem. Although node connectivity can sometimes be inferred from physical proximity, determining which nodes are actively communicating often requires analyzing their activity patterns, as many nodes may be within range of one another.

Blind Source Separation. Being external to legitimate wireless networks, a patrol system can leverage blind source separation (BSS) techniques to

distinguish signals from different transmitters. These methods enable the isolation of illegitimate signals from legitimate ones. For instance, as shown in Fig. 1.1, the jammer's red signal can be further analyzed to classify its type or modulation. While BSS is commonly applied in scenarios where the number of sensors exceeds the number of network nodes, in the context of wireless security, the number of patrol sensors is typically lower than the number of transmitters, making the underdetermined blind source separation (UBSS) problem more challenging to address.

Intrusion Detection. Utilizing signal processing techniques such as UBSS and spectrum sensing algorithms, one of the primary objectives of the patrol is to detect intruders within a specified area. As illustrated in Fig. 1.1, UAVs, functioning as patrol sensors, are tasked with identifying the presence of a jammer interfering with legitimate communications of two wireless networks. This task is particularly challenging due to the lack of prior knowledge regarding the transmitted signals in the RF medium, yet the system must still be able to distinguish the illegitimate user.

Intruder Localization. Following the detection of an intrusion, a patroller can ascertain the spatial position of the source. This information allows the authority to identify potential sources of interference. By combining location data with other insights extracted from the data set, the authority gains a comprehensive view that aids in effective interference mitigation and network security. As the malicious user has an interest in remaining undetected, the patrol must manage both collaborative and non-collaborative localisation techniques to form a comprehensive picture of the RF scene [8].

1.2 Aims of this Work

This thesis presents a novel framework for monitoring the RF spectrum and detecting smart jammers by analyzing spectrum usage through RF sensors, referred to as the spectrum patrol. The proposed methodology is blind, enabling the analysis of wireless networks with unknown characteristics, such

as the number of nodes, physical layer signals, and medium access protocol (MAC) and routing protocols. Fig. 1.2 illustrates the complete logical structure of the framework. Due to the wireless nature of the medium, the over-the-air signals captured by the sensors are mixed. To address this, BSS is employed to separate traffic patterns. The extracted traffic profiles are then analyzed using a causal inference approach to identify the presence of a jammer. Simultaneously, the patrol system monitors spectrum usage through frequency-domain representations of the received signals, detecting occupied portions of the band and counting the number of signals within those sections.

The following section provides a brief overview of the key research stages conducted during the Ph.D. period.

1.2.1 Blind Source Separation

Each RF sensor that constitutes the patrol collects a mixture of over-the-air received powers from all nodes of the observed network, including the jammer. The collected mixtures are then transmitted to a fusion centre (FC), which may be either a component of the patrol or the authority responsible for overseeing the area. The acquired mixtures are subsequently processed to differentiate between the traffic profiles generated by each actors. The research on BSS tackles the following research points:

- *P1 - It is reasonable to consider a number of sensors that is lower than the number of wireless nodes in a given area. Therefore, approaches based on UBSS must be considered.*
- *P2 - The efficacy of UBSS methods is contingent upon the veracity of the sparsity assumption; thus, it is necessary to evaluate this assumption in a wireless scenario.*
- *P3 - In order to obtain a UBSS solution, it is necessary to adopt a two-step approach. The first step involves estimating the mixing matrix, while the second step is concerned with the reconstruction of the source matrix.*

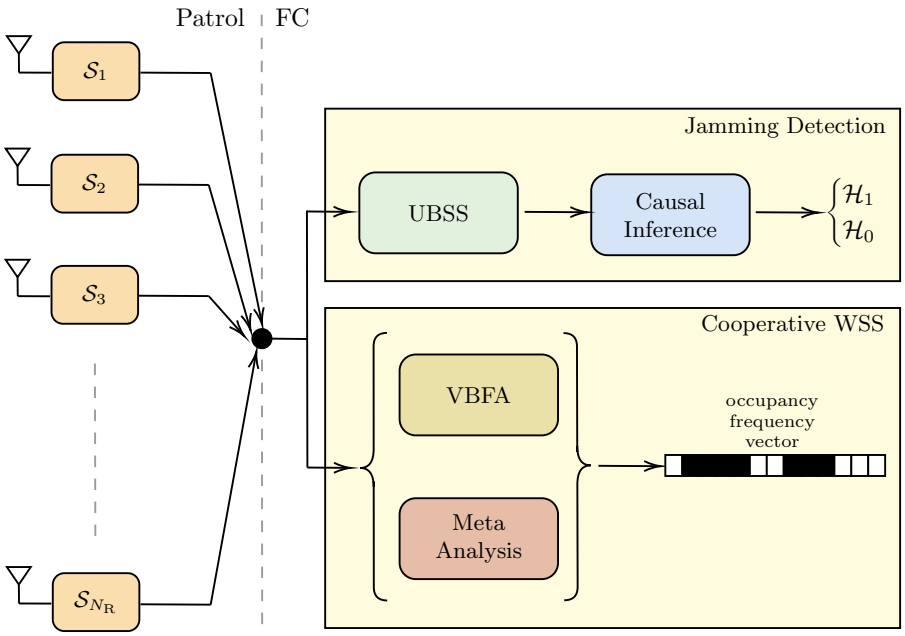

Figure 1.2: A logical block representation of the proposed framework. The spectrum patrol collects the over-the-air traffic profiles generated by the wireless network nodes. Subsequently, for jamming detection, a BSS is performed to unmix the received signals, and a causal inference technique is used for the detection. For spectrum sensing, two different solutions are proposed. The first is based on a factor analysis model, and the second is based on a meta-analysis approach.

1.2.2 Jamming Detection

Jamming attacks to hinder communication capabilities are becoming a critical aspect of wireless networks. A challenging issue is the detection of reactive jammers that perform spectrum sensing and attack the network only when legitimate communication is in progress. In this scenario, we introduce a novel framework for reactive jamming detection using a patrol of RF sensors external to the network to be protected. The solution relies on the UBSS method and a new jamming detection based on causal inference. The jamming detection part tackles the following research points:

- *P4 - The possibility to exploit the causal relationship between the jammer and the legitimate nodes.*

- *P5 - The development of an algorithm capable of quantifying the causal*

strength between the received signals.

- *P6 - A statistical test that determines the significance of a causal link.*

The detection of a jammer in a ISAC system is approached from a different point of view in Chapter 5. In such a scenario, the objective is to detect the presence of a deceptive jammer that is capable of modifying the perceived location of actual targets. Starting from the echo signals acquired by the base station (BS) and leveraging the latent space identification capability of variational autoencoders (VAEs), the BS is able to detect the presence of an intruder in a multiple-input multiple-output (MIMO)-orthogonal frequency-division multiplexing (OFDM) system. In this context, the following research points are addresses:

- *P7 - Detection must be carried out without prior knowledge of the jammer. Therefore, the problem is reformulated as an anomaly detection task, where only target observations are available during the training phase.*
- *P8 - Leveraging the maximized evidence lower bound (ELBO), obtained after the training, to detect the presence of a deceptive jammer.*

While the primary focus of this thesis is spectrum patrol for jamming detection, Chapter 5 explores a complementary yet related topic: jamming detection in a monostatic ISAC system. This investigation, though not involving spectrum patrol directly, aligns with the broader scope of detecting jamming threats.

1.2.3 Cooperative Wideband Spectrum Sensing

Sensors observe the same frequency band and convey the frequency domain representations of the received signals to a FC. The FC then estimates the occupancy state of multiple portions of a large bandwidth, which are termed frequency bins. In particular, we introduce a novel wideband spectrum sensing (WSS) algorithm based on factor analysis solved by a variational inference (VI) method that provides deeper insights into the RF environment being analyzed. The cooperative WSS addresses the following research points:

- *P9 - It is possible to recast the WSS problem as a generative latent model through the application of factor analysis.*
- *P10 - The selection of the metric that is capable of differentiating between an occupied frequency bin and a free frequency bin.*
- *P11 - An investigation of the latent model is required in order to obtain further insights from the RF environment under analysis, specifically in relation to noise power estimation and user counting.*

The cooperative WSS is approached from a different point of view in Chapter 7. In that case, a meta-analysis solution is developed to detect the presence of a signal in a frequency components. The proposed method markedly diminishes the overhead on the backhaul link between sensors and the FC. However, it is constrained to a spectrum sensing objective, thereby precluding a more comprehensive understanding of the RF environment. In this context, the following research points are addresses:

- *P12 - The rule of meta-analysis for sensor fusion in order to lighten the transmissions towards the FC.*
- *P13 - An approximation of the test statistic in each sensor that is required for the computation of the mixture detector.*

1.3 Document Organization

This document is organized as follows. Chapter 2 introduces the scenarios and the system models. In particular, the propagation characteristics and channel impairments of a realistic scenario are modeled. Chapter 3 provides an overview of the underdetermined blind source separation problem and describes the proposed solutions. In Chapter 4, the problem of reactive jammer detection is addressed, introducing the key concept of causality as a basis for the proposed approach. Chapter 5 details a deceptive jammer detection method for MIMO-OFDM ISAC systems, leveraging the latent space identification capabilities of the VAE. The cooperative WSS is investigated in

Table 1.1: Summary of chapters and their connections.

Topic	**System Model** (*Ch. 2*)	**Numerical Result** (*Ch. 8*)
Blind Source Separation (*Ch. 3*)	Section 2.2	Section 8.1
Jammer Detection through Spectrum Patrol (*Ch. 4*)	Section 2.2	Section 8.1
Jammer Detection through Latent Model (*Ch. 5*)	Section 2.4	Section 8.2
Cooperative Wideband Spectrum Sensing (*Ch. 6*)	Section 2.3	Section 8.3
Meta-Analysis for WSS (*Ch. 7*)	Section 2.3	Section 8.3

Chapter 6 and Chapter 7, employing two distinct methodologies: variational Bayes factor analysis (VBFA) and meta-analysis. Chapter 8 provides the validation of the proposed framework through extensive numerical results. Finally, conclusions are drawn in Chapter 9, followed by the list of papers published and submitted during this Ph.D., and the references.

Given that Chapters 3 to 7 build upon the system models introduced in Chapter 2 and the numerical results discussed in Chapter 8, a summary outlining the structure and flow of the thesis is presented in Tab. 1.1.

Chapter 2

Scenarios of Interest and System Model

This chapter explores three critical scenarios that underscore the significance of spectrum awareness. Specifically, we outline how a profound understanding of the spectrum can significantly enhance network security in each scenario. Detailed system models for each case are also provided.

2.1 Received Signal and Channel Model

The foundation of each system model begins with the equivalent low-pass representation of the signal received by the jth sensor, expressed as

$$r_j(t) = \int_{-\infty}^{+\infty} \tilde{x}_l(t-\tau)\tilde{h}_{j,l}(t,\tau)d\tau + \nu_j(t) \tag{2.1}$$

where $\tilde{x}_l(t)$ represents the signal transmitted by node l, $\tilde{h}_{j,l}(t,\tau)$ denotes the channel impulse response between node l and receiver j, and $\nu_j(t)$ is the additive white Gaussian noise (AWGN) with independent, identically distributed (i.i.d.) real and imaginary components.

In this work, we assume a linear time-invariant (LTI) channel, such that

$$\tilde{h}_{j,l}(t,\tau) = \tilde{h}_{j,l}(\tau) = \sum_{i=1}^{L} c_i \delta(\tau - \tau_i) \tag{2.2}$$

where L indicates the number of paths, while c_i and τ_i represent the complex amplitude and delay associated with the ith path, respectively. It is possible to define the delay spread as

$$\tau_{\text{rms}} = \sqrt{\frac{\sum_{i=1}^{L}(\tau_i - \bar{\tau})^2 |c_i|^2}{\sum_{i=1}^{L} |c_i|^2}} \tag{2.3}$$

where $\bar{\tau}$ is the average delay that can be written as

$$\bar{\tau} = \frac{\sum_{i=1}^{L} \tau_i |c_i|^2}{\sum_{i=1}^{L} |c_i|^2}. \tag{2.4}$$

In this thesis, in some scenarios we consider flat fading, while in others is more appropriate to consider frequency selective channel. For this reason, the following two subsections present the structure of the received signals in both cases.

2.1.1 Narrowband Signal Scenario

Consider a channel with coherence bandwidth B_{ch}. When the signal bandwidth W satisfies $W \ll B_{\text{ch}}$, all echoes arrive within the symbol duration ($\tau_{\text{rms}} \ll 1/W$). Consequently, the individual echoes can be treated as a single composite echo and the channel can be written as

$$\tilde{h}_{j,l}(\tau) = \sum_{i=1}^{L} c_i \delta(\tau - \bar{\tau}). \tag{2.5}$$

In this scenario, the channel exhibits flat fading since its transfer function remains constant across the bandwidth W:[1]

$$H_{j,l}(f) = \mathcal{F}\{\tilde{h}_{j,l}(\tau)\} = \sum_{i=1}^{L} c_i \tag{2.6}$$

with $\mathcal{F}\{\cdot\}$ representing the Fourier transform.

The received signal can thus be expressed as

$$r_j(t) = \sum_{i=1}^{L} c_i \tilde{x}_l(t) + \nu_j(t) \tag{2.7}$$

where, for simplicity, the transmission delay $\bar{\tau}$ is omitted. After sampling, the nth sample of the received signal, between transmitter l and sensor j, is described as a flat fading channel model as follows

$$r_{j,n} = \tilde{h}_{j,l} \tilde{x}_{l,n} + \nu_{j,n} \tag{2.8}$$

where $\tilde{h}_{j,l} = \sum_{i=1}^{L} c_i$ is the resulting complex channel gain. Given a large L, for the central limit theorem, the channel gain follows a Gaussian distribution which leads to the Rayleigh and Ricean channel model.

2.1.2 Wideband Signal Scenario

In cases where the band W is not significantly smaller than B_{ch}, the channel exhibits frequency selective, given that the channel transfer function is subject to change within W. An illustrative example of this scenario can be found in the context of WSS, in which the presence of frequency-selective multipath channels between the primary users (PUs) and sensors necessitates such consideration. In this thesis, three International Telecommunication Union (ITU) channel models proposed in [9] are considered:

- extended pedestrian A (EPA), useful for planning indoor or pedestrian environments, such as shopping malls, airports, or train stations;

[1] Given $f \in [0, W]$, if $W\tau_{\text{rms}} \ll 1$, then it is possible to approximate $e^{-j2\pi f \tau_i} \simeq 1$ for each $i = 1, \ldots, L$.

Table 2.1: ITU channel models.

Channel Model	**path delays [ns]**								
EPA	0	30	70	80	110	190	410		
EVA	0	30	150	310	370	710	1090	1730	2510
ETU	0	50	120	200	230	500	1600	2300	5000
Channel Model	**average power gains [dB]**								
EPA	0	-1	-2	-3	-8	-17.2	-20.8		
EVA	0	-1.5	-1.4	-3.6	-0.6	-9.1	-7	-12	-16.9
ETU	-1	-1	-1	0	0	0	-3	-5	-7

- extended vehicular A (EVA), which describes vehicular scenarios, such as highways or urban roads;
- extended typical urban (ETU), which represents dense urban areas with high-rise buildings.

The path delays and average power gains of each model are shown in Tab. 2.1.

In this context, we adopt a frequency-domain representation, assuming that users transmit an OFDM signal. After applying the discrete Fourier transform (DFT) at the receiver, the received signal can be described as

$$\mathbf{y}_{:,k}^{(i)} = \mathbf{H}_{k}^{(i)} \mathbf{x}_{:,k}^{(i)} + \mathbf{n}_{:,k}^{(i)} \tag{2.9}$$

where $\mathbf{H}_{k}^{(i)}$ denotes the channel matrix, $\mathbf{x}_{:,k}^{(i)}$ represents the transmitted data at the kth subcarrier for the ith observation, and $\mathbf{n}_{:,k}^{(i)}$ is the AWGN component. Within this formulation, two distinct scenarios are analyzed.

MIMO system

In this case, we examine a MIMO link between a transmitter and a receiver equipped with antenna arrays comprising N_{A} elements. Therefore $\mathbf{x}_{:,k}^{(i)} = \mathbf{w}_{\mathrm{T}}^{(i)} x_{k}^{(i)}$ is the discrete-time signal transmitted in the kth subcarrier of at

time i, where $\mathbf{w}_{\mathrm{T}}^{(i)} \in \mathbb{C}^{N_{\mathrm{A}} \times 1}$ is the sensing beamforming vector used to map each modulation symbol, $x_k^{(i)}$, to the transmitting antennas. $\mathbf{y}_{:,k}^{(i)} \in \mathbb{C}^{N_{\mathrm{A}} \times 1}$ is the received modulation symbols at each antenna after the DFT block and $\mathbf{H}_k^{(i)} \in \mathbb{C}^{N_{\mathrm{A}} \times N_{\mathrm{A}}}$ is the channel matrix between two devices for the kth subcarrier in the ith observation.

Distributed system

In this context, we analyse a network comprising N_{T} single-antenna transmitters and a set N_{R} of single-antenna sensors deployed within a specified area. Thus, $\mathbf{x}_{:,k}^{(i)} \in \mathbb{C}^{N_{\mathrm{T},k} \times 1}$ is the vector of frequency samples transmitted by the users in the kth frequency bin at the ith observation, $N_{\mathrm{T},k}$ is the number of transmitters in the kth frequency bin, $\mathbf{y}_{:,k}^{(i)} \in \mathbb{C}^{N_{\mathrm{R}} \times 1}$ is the received modulation symbols at each sensor after the DFT block and $\mathbf{H}_k^{(i)} \in \mathbb{C}^{N_{\mathrm{R}} \times N_{\mathrm{T},k}}$ is the matrix of channel coefficients in frequency domain.

2.1.3 ISAC Channel Model

In this work, an ISAC system under a jamming attack is also analyzed, necessitating the characterization of the wireless channel for the sensing link between the BS and the target (i.e., BS-target-BS). Specifically, a line-of-sight (LOS) channel without Doppler effect is assumed. The channel matrix $\mathbf{H}_k^{(i)} \in \mathbb{C}^{N_{\mathrm{A}} \times N_{\mathrm{A}}}$ is given by

$$\mathbf{H}_k^{(i)} = \alpha_{\mathrm{t}}^{(i)} e^{j\phi_{\mathrm{t}}^{(i)}} e^{-j2\pi k \Delta f \tau_{\mathrm{t}}^{(i)}} \mathbf{a}_{\mathrm{R}}(\theta_{\mathrm{t}}^{(i)}) \mathbf{a}_{\mathrm{T}}^{\mathsf{T}}(\theta_{\mathrm{t}}^{(i)}) \tag{2.10}$$

where $\alpha_{\mathrm{t}}^{(i)}$, $\phi_{\mathrm{t}}^{(i)}$, $\tau_{\mathrm{t}}^{(i)}$, $\theta_{\mathrm{t}}^{(i)}$ are the attenuation, phase, delay, and angle of arrival (AoA)/angle of departure (AoD) of the target for the ith observation, respectively, and Δf is the subcarrier spacing.

The gain $\alpha_{\mathrm{t}}^{(i)}$ includes the attenuation along the BS-target-BS path, that is calculated as

$$\alpha_{\mathrm{t}}^{(i)} = \sqrt{\frac{c^2 \sigma_{\mathrm{RCS}}^{(i)}}{(4\pi)^3 f_{\mathrm{c}}^2 \left(r_{\mathrm{t}}^{(i)}\right)^4}} \tag{2.11}$$

where $r_{\mathrm{t}}^{(i)}$ is the distance between the target and the BS in the ith observation,

and $\sigma_{\text{RCS}}^{(i)}$ is its radar cross-section (RCS).

The jammer-BS channel matrix $\tilde{\mathbf{H}}_k^{(i)} \in \mathbb{C}^{N_\text{A} \times N_\text{J}}$, instead, can be written as

$$\tilde{\mathbf{H}}_k^{(i)} = \alpha_\text{J}^{(i)} e^{j\phi_\text{J}^{(i)}} e^{-j2\pi k \Delta f \tau_\text{J}^{(i)}} \mathbf{a}_\text{R}(\theta_{\text{BS,J}}^{(i)}) \mathbf{a}_\text{J}^\text{T}(\theta_{\text{J,BS}}^{(i)}) \tag{2.12}$$

where N_J is the number of jammer antenna elements, $\alpha_\text{J}^{(i)}$ is the channel attenuation given by the path-loss equation, $\phi_\text{J}^{(i)}$ is the phase shift, and $\tau_\text{J}^{(i)}$ is the delay of the direct path. Furthermore, $\theta_{\text{BS,J}}^{(i)}$ and $\theta_{\text{J,BS}}^{(i)}$ are the AoA and AoD of the LOS path.

2.2 Wireless Network Security

Private information and sensitive data rely heavily on the network infrastructure's security [10]. This aspect is becoming of paramount importance in several applications such as industrial internet of things (IoT), remote e-health, and V2X communications, where the wireless medium conveys critical data. To further exacerbate the problem, the upcoming AI revolution, while making intelligent and efficient devices on one side, may lead to a much more vulnerable technology on the other [7, 11, 12].

Considering the different security threats of wireless networks, we distinguish between passive (i.e., eavesdropping [13]) and active attacks [14]. Among the latter, the most common threat is denial-of-service (DoS), in which a malicious transmitter (i.e., jammer) generates interference attempting to prevent legitimate users from accessing the network. A wide variety of jammers have been investigated in the last two decades: the continuous jammer that emits a persistent radio signal, the random jammer that mimics a random behavior, and the reactive (smart) jammer capable of detecting ongoing communications via spectrum sensing and opportunistically interfere them [15, 16]. However, this last type of jammer can hide by inactivating the interference when the legitimate user is not communicating, thus making its detection remarkably hard. Moreover, considering that building a reactive jammer is becoming more accessible thanks to technological advances in

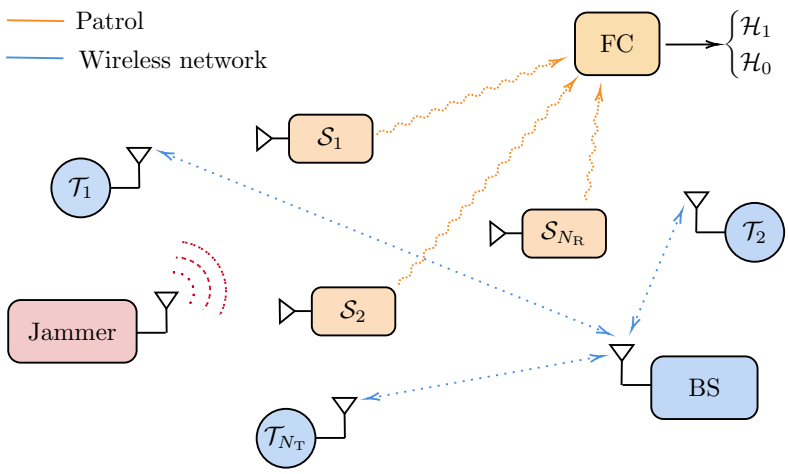

Figure 2.1: A wireless network under attack by a jammer. A patrol composed of RF sensors monitors the spectrum by sharing information with a fusion centre (FC) that performs jamming detection. Hypothesis $\mathcal{H}_1$ is the detection of a jammer, while $\mathcal{H}_0$ is the null hypothesis.

software-defined radio, developing new techniques to counteract such attackers is now of paramount importance [17, 18].

In this scenario, a solution that recently has been proposed makes use of a spectrum patrol to enforce security of a wireless network [3, 7, 19, 20]. The patrol can be composed by one or many devices that cooperate to monitor a region, sensing the RF spectrum and detecting the presence of anomalies (i.e., malicious users). An illustration of the aforementioned scenario is shown in Fig. 2.1. The patrollers can pair the information received by the legitimate users and e.g., the access points (APs) or the BSs when available, with the ones extracted from the spectrum analysis to detect the presence of a jammer.

2.2.1 System Model

Let us consider a scenario with a packet-based wireless network, a reactive jammer, and a patrol. In particular, the wireless network is composed by a set $\mathcal{T}$ of nodes (or users) and the patrol is formed by a set $\mathcal{S}$ of radio-frequency sensors, with cardinalities N_{T} and N_{R}, respectively. All the actors, namely the nodes, the sensors and the jammer are randomly deployed on a two-dimensional area.

Each RF sensor performs energy detection, collect the received energy samples for a period T_{ob} and forward the data to a FC. Information as number of transmitting nodes, their positions, and physical and MAC layer configurations of the legitimate network are unknown to the FC. In the presence of frequency flat channel, the nth sample of the equivalent low-pass signal received by the jth sensor is

$$r_{j,n} = \sum_{l=1}^{N_{\text{T}}+1} \tilde{h}_{j,l}\tilde{x}_{l,n} + \nu_{j,n} \tag{2.13}$$

where $\tilde{x}_{l,n}$ for $l = 1, \ldots, N_{\text{T}}$ is the nth sample of the signal transmitted by node l, $\tilde{x}_{N_{\text{T}}+1,n}$ is the signal emitted by the jammer, $\tilde{h}_{j,l}$ for $l = 1, \ldots, N_{\text{T}}$ is the channel gain between node l and sensor j, while $\tilde{h}_{j,N_{\text{T}}+1}$ is the jammer-sensor channel gain. The term $\nu_{j,n} \sim \mathcal{CN}(0, \tilde{\sigma}_j^2)$ is the AWGN at the jth sensor with i.i.d. real and imaginary parts, noise power $\tilde{\sigma}_j^2 = 2N_0^{\text{S}}W$ where W is the bandwidth and N_0^{S} is the two-sided power spectral density.

To reduce the number of collected samples and, consequently, the computational burden for jammer detection, each sensor extracts the energy of the received signal calculated over short time bins of duration T_{e} such that $T_{\text{ob}} = N_{\text{e}}T_{\text{e}}$, where N_{e} is the number of energy samples. Thus, we obtain the matrix $\mathbf{Y} \in \mathbb{R}^{N_{\text{R}} \times N_{\text{e}}}$, whose entries $y_{j,i}$ are the energy samples

$$y_{j,i} = \frac{1}{W} \sum_{d=1}^{N_{\text{d}}} |r_{j,(i-1)N_{\text{d}}+d}|^2 \tag{2.14}$$

where $N_{\text{d}} = T_{\text{e}}W$ is the number of signal samples used to compute the energy. This form of subsampling, while removing details (modulation, phase, etc.) of the signals emitted by the jammer and the nodes, it retains all the necessary information about the traffic profiles of the actors necessary to perform jamming detection.

Under the assumptions of signals emitted by the nodes mutually uncor-

related and uncorrelated with the noise, we can express $\mathbf{Y}$ as[2]

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{\Omega} \tag{2.15}$$

where the lth row of $\mathbf{X} \in \mathbb{R}^{(N_\mathrm{T}+1)\times N_\mathrm{e}}$ is the corresponding transmitter's energy profile and the last row contains the energy profile of the jammer. The entries $\omega_{j,i} = \frac{1}{W}\sum_{d=1}^{N_\mathrm{d}} |\nu_{j,(i-1)N_\mathrm{d}+d}|^2$ of $\mathbf{\Omega} \in \mathbb{R}^{N_\mathrm{R}\times N_\mathrm{e}}$ are the noise energy samples and $\mathbf{H} \in \mathbb{R}^{N_\mathrm{R}\times(N_\mathrm{T}+1)}$ is the matrix of the channel power gains $h_{j,l} = |\tilde{h}_{j,l}|^2$. The energy profiles are sent to a FC that performs the jammer detection.

2.3 Dynamic Spectrum Sharing

In recent years, the ever-increasing demand for higher data rates has pushed wireless technologies to their limits. The congestion observed in the sub-6 GHz spectrum has led researchers to explore millimeter-wave solutions [21], underscoring the finite nature of the radio spectrum and highlighting the need for its careful management and utilization. In response to the escalating demand for wireless connectivity and the scarcity of RF spectrum resources, spectrum sharing has emerged as a pivotal strategy to enhance spectrum efficiency in next-generation wireless systems [22]. Interestingly, despite the recognized scarcity of the spectrum, both unlicensed and licensed bands are typically only partially utilized, exhibiting gaps of significantly varying sizes [23]. Despite its potential, the widespread adoption of dynamic spectrum sharing faces numerous technical challenges [24]. These challenges include intelligent sensing and RF spectrum awareness, ensuring the protection of incumbent users, equitable distribution of spectrum resources, and managing the coexistence of active and passive RF systems [7,25]. A critical aspect of spectrum sharing is the ability to identify unused spectrum bands, often encapsulated within the spectrum sensing framework [6,26]. Wideband sensing typically relies on adopting a frequency domain representation of the received signal and computing metrics to assess the occupancy state of each

[2]Equation (2.15) holds for sufficiently large sample size $N_\mathrm{d} = T_\mathrm{e}W$.

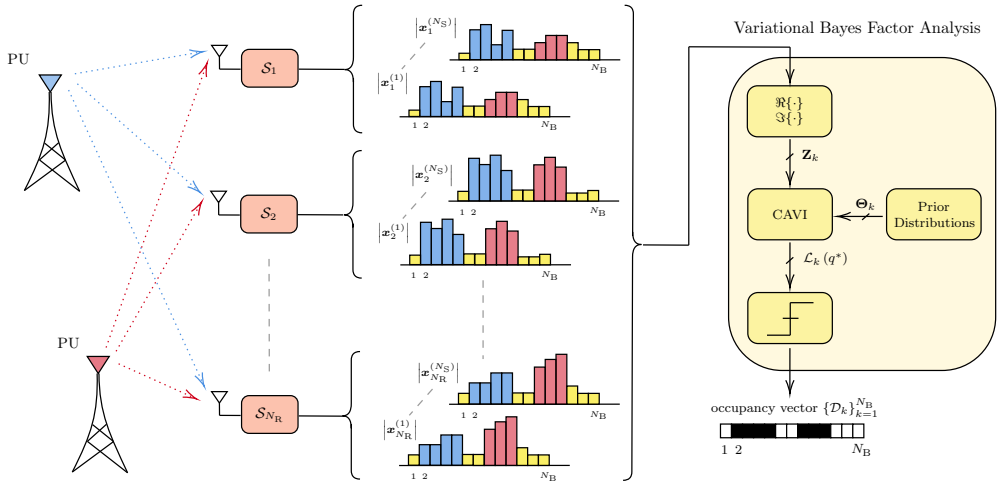

Figure 2.2: Wideband spectrum sensing scheme: an illustration of the data gathering process and decision-making. The blue PU transmits in the blue bandwidth, while the red PU transmits in the red bandwidth. Either both could be legitimate users, or one could be an intruder exploiting unused portions of the bandwidth. Spectrum holes are represented by yellow bars. The N_R sensors could be SUs or wireless patrols that monitor the spectrum in a specific area.

sub-band [27,28]. The core objectives of WSS can be summarized in two key scenarios. First, maximizing spectrum utilization while minimizing interference between PUs and secondary users (SUs). In this scenario, SUs utilize WSS to detect available spectrum holes for communication purposes. Alternatively, WSS algorithms can be employed by a spectrum patrol to detect unauthorized use of the spectrum. The wireless sensor patrol can schedule periodic sensing phases to monitor the RF medium. Then, the occupancy state of the spectrum can be forwarded to the authority that verifies the presence of intruders. In this context, the capability to count the number of transmissions within a bandwidth together with spectrum sensing can enhance the available information.

2.3.1 System Model

The WSS performance can be significantly improved through the implementation of cooperative strategies where N_R sensors observe the same frequency band and share the frequency domain representations of the received signals

to a FC [29–33]. The FC performs the WSS algorithm with the goal to understand which frequency band segments are currently occupied and to identify those that can be classified as spectrum holes.

To perform a spectrum sensing, sensors collect N_{S} independent frequency domain vectors by repeated measurements;[3] we will call them observations or snapshots, each with N_{B} frequency components, $\mathbf{y}_{j,:}^{(i)} = (y_{j,1}^{(i)}, \ldots, y_{j,N_{\mathrm{B}}}^{(i)})^{\mathsf{T}}$ with $i = 1, \ldots, N_{\mathrm{S}}$ and $j = 1, \ldots, N_{\mathrm{R}}$. The WSS strategy can be applied using any frequency representation of data. Note that the vector $\mathbf{y}_{j,:}^{(i)}$ can be any kind of frequency domain representation obtained with a Nyquist sampling rate, such as a power spectral density estimate, the output of a filter bank or, as assumed here, the output of a N_{B}-points DFT [34]. We generally refer to the elements of $\mathbf{y}_{j,:}^{(i)}$ as frequency bins.

The received signal at the ith observation in the jth sensor is denoted as the N_{B} length vector

$$\mathbf{r}_{j,:}^{(i)} = \boldsymbol{\xi}_{j,:}^{(i)} + \boldsymbol{\nu}_{j,:}^{(i)} \tag{2.16}$$

where $\boldsymbol{\xi}_{j,:}^{(i)}$ and $\boldsymbol{\nu}_{j,:}^{(i)}$ are the aggregation of unknown PUs signals and AWGN with power $\tilde{\sigma}_j^2$, collected by the jth sensor in the ith measurement, in time-domain, respectively. The output of the DFT at the ith observation in the jth sensor is denoted as the N_{B} length vector

$$\mathbf{y}_{j,:}^{(i)} = \mathbf{s}_{j,:}^{(i)} + \mathbf{n}_{j,:}^{(i)} \tag{2.17}$$

where $\mathbf{s}_{j,:}^{(i)} = \mathsf{DFT}[\boldsymbol{\xi}_{j,:}^{(i)}]$ and $\mathbf{n}_{j,:}^{(i)} = \mathsf{DFT}[\boldsymbol{\nu}_{j,:}^{(i)}]$. The signal-to-noise ratio (SNR), at the jth sensor, is defined as

$$\mathsf{SNR}_j = \frac{\mathbb{E}\left[\boldsymbol{\xi}_{j,:}^{(i)}\left(\boldsymbol{\xi}_{j,:}^{(i)}\right)^{\mathsf{H}}\right]}{\mathbb{E}\left[\boldsymbol{\nu}_{j,:}^{(i)}\left(\boldsymbol{\nu}_{j,:}^{(i)}\right)^{\mathsf{H}}\right]} = \frac{\mathbb{E}\left[\mathbf{s}_{j,:}^{(i)}\left(\mathbf{s}_{j,:}^{(i)}\right)^{\mathsf{H}}\right]}{\sigma_j^2} \tag{2.18}$$

where the second term is derived by the Parseval's identity applied to DFT and express the SNR in the frequency domain with $\sigma_j^2 = N_{\mathrm{B}}\,\tilde{\sigma}_j^2$ denoting the

[3] We assume that frequency occupancy does not change during the N_{S} observations.

noise power per frequency bin.

An overview of the data-gathering process and decision making, performed by the FC, is presented in Fig. 2.2, where PU signals (red and blue bars) occupy k^* bins overall, while the remaining $N_\mathrm{B} - k^*$ contain only noise (yellow bars). The goal of cooperative WSS is to identify the k^* occupied bins.

2.4 Integrated Sensing and Communication

As detailed in the previous Section 2.2, jamming attacks can jeopardize wireless communication networks. However, jamming poses a significant threat to sensing infrastructures as well, particularly those aimed at locating passive targets through wireless signals. The vulnerability of backscatter signals received by radar in sensing applications represents a significant risk. These signals are typically weak, rendering them susceptible to disruption by jamming. This issue is especially concerning in the context of 6G, where the emerging paradigm of ISAC systems is expected to revolutionize applications such as traffic monitoring and autonomous driving. ISAC systems are sensitive to a range of traditional radar security threats (e.g., advanced radar electronic countermeasure (ECM)), which are designed to deceive the sensing systems [35]. Among those attacks, the deceptive jamming technique known as digital radio frequency memory (DRFM) is particularly significant, as it enables precise scaling and delaying of intercepted radar waveforms by the jammer. Moreover, the global DRFM market is projected to experience substantial growth due to the widespread adoption of AI. A deceptive jammer can exploit information about signals transmitted by the BS to mimic the behavior of a typical network user equipment (UE). For example, common pilot/reference signals proposed for integrating sensing capabilities into communication networks [36–38] might already be known to intruders, potentially jeopardizing network security. An illustration of the aforementioned scenario is shown in Fig. 2.3. The deceptive jammer is able to falsify the BS's estimation of the target position. In this case we do not consider a patrol, the BS itself is responsible to detect the presence of a jammer analyzing the backscatter signal.

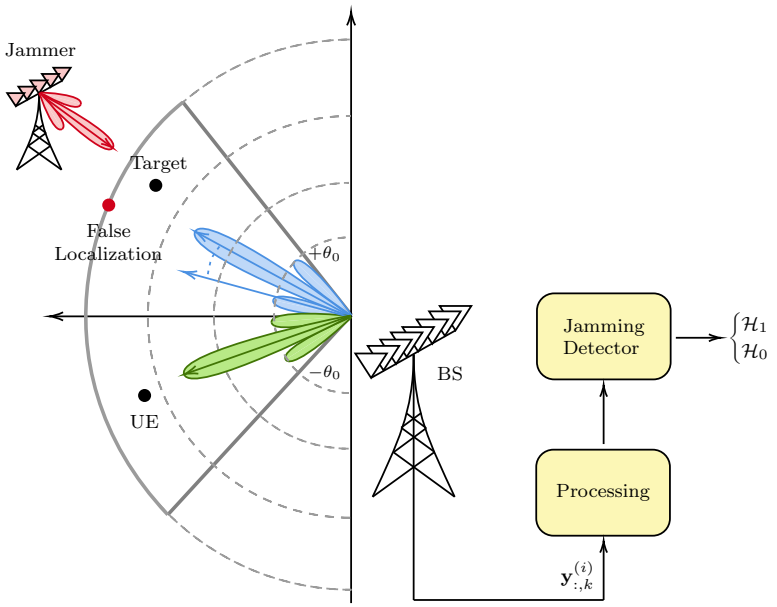

Figure 2.3: The monostatic OFDM ISAC scheme in presence of a deceptive jammer. Hypothesis $\mathcal{H}_1$ is the detection of a jammer, while $\mathcal{H}_0$ is the null hypothesis.

2.4.1 System Model

Transmitted Signal at the BS

Let us consider the monostatic MIMO OFDM system depicted in Fig. 2.3, which consists of transmitter and receiver antenna arrays with both N_A elements, used for communication and sensing. We assume that uniform linear arrays (ULAs) with half-wavelength separation, i.e., $d = \lambda/2$, where $\lambda = c/f_\mathrm{c}$, c is the speed of light, and f_c is the carrier frequency, are employed for both transmission and reception. According to [39], we assume that sensing is performed using repeated time-frequency slots composed of N_B subcarriers and M OFDM symbols each. Within such slots, a sensing beam is activated beside a communication beam (for downlink communication towards a user) [40]. However, for jamming detection, we pick one "observation" within each slot, which refers to a vector containing the received OFDM symbols (right after the fast Fourier transform (FFT) processing at the sensing receiver) across the N_B subcarriers at time i.

With such a multibeam ISAC approach only a fraction of total power

of the OFDM signal is designated to sensing purposes. The discrete-time transmitted signal in the kth subcarrier of at time i, can be written as [40]

$$\mathbf{x}_{:,k}^{(i)} = \mathbf{w}_{\mathrm{T}}^{(i)}\, x_k^{(i)} \tag{2.19}$$

where $k = 1, \ldots, N_{\mathrm{B}}$, $i = 1, \ldots, N_{\mathrm{S}}$ with N_{S} the number of observations, and $\mathbf{w}_{\mathrm{T}}^{(i)} \in \mathbb{C}^{N_{\mathrm{A}} \times 1}$ is the sensing beamforming vector used to map each modulation symbol, $x_k^{(i)}$, to the transmitting antennas. By considering a beam steering approach and performing a normalization with respect to the effective isotropic radiated power (EIRP) $P_{\mathrm{T}}G_{\mathrm{T}}$, we express the beamforming vector as

$$\mathbf{w}_{\mathrm{T}}^{(i)} = \frac{\sqrt{\rho P_{\mathrm{T}} G_{\mathrm{T}}}}{N_{\mathrm{A}}} \mathbf{a}_{\mathrm{T}}^{*}(\theta_{\mathrm{T}}^{(i)}) \tag{2.20}$$

where $\rho \in [0, 1]$ is the parameter used to control the fraction of the total power apportioned to the sensing direction, P_{T} is the transmit power, G_{T} is the transmit array gain along the beam steering direction, and $\mathbf{a}_{\mathrm{T}}(\theta_{\mathrm{T}}^{(i)}) \in \mathbb{C}^{N_{\mathrm{A}} \times 1}$ is the steering vector along the sensing directions $\theta_{\mathrm{T}}^{(i)}$. In particular, the steering vector for the considered ULA can be expressed as

$$\mathbf{a}_{\mathrm{T}}(\theta_{\mathrm{T}}^{(i)}) = \left[1, e^{j\pi \sin(\theta_{\mathrm{T}}^{(i)})}, \ldots, e^{j\pi(N_{\mathrm{A}}-1)\sin(\theta_{\mathrm{T}}^{(i)})}\right]^{\mathsf{T}}. \tag{2.21}$$

For generality and to facilitate jamming detection in an unknown environment, we assume the interval between two consecutive observations exceeds the channel's coherence time. This results in different channel realizations for the sensing receiver with each observation. Additionally, the characteristics of both the target and jammer may vary across observations; for instance, their positions relative to the BS may change.

Received Signal at the BS

Let us assume the presence of a point-like target within the sensing beam. The received signal is processed by a typical OFDM receiver [40], such that the vector $\mathbf{y}_{:,k}^{(i)} \in \mathbb{C}^{N_{\mathrm{A}} \times 1}$ of the received modulation symbols at each antenna

after the FFT block is

$$\mathbf{y}_{:,k}^{(i)} = \mathbf{H}_k^{(i)}\mathbf{x}_{:,k}^{(i)} + \tilde{\mathbf{H}}_k^{(i)}\tilde{\mathbf{x}}_{:,k}^{(i)} + \boldsymbol{\zeta}_{:,k}^{(i)} + \mathbf{n}_{:,k}^{(i)} \tag{2.22}$$

where $\mathbf{H}_k^{(i)} \in \mathbb{C}^{N_\mathrm{A}\times N_\mathrm{A}}$ is the channel matrix between the target and the BS for the kth subcarrier in the ith observation, $\tilde{\mathbf{H}}_k^{(i)} \in \mathbb{C}^{N_\mathrm{A}\times N_\mathrm{J}}$ is the channel matrix between the BS and the jammer, $\tilde{\mathbf{x}}_{:,k}^{(i)} \in \mathbb{C}^{N_\mathrm{J}\times 1}$ is the jammer signal, N_J is the number of jammer antenna elements, $\boldsymbol{\zeta}_{:,k}^{(i)} \in \mathbb{C}^{N_\mathrm{A}\times 1}$ is the vector whose elements represent the self-interference due to imperfect Tx–Rx isolation at each receiving antenna, and $\mathbf{n}_{:,k}^{(i)} \sim \mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I}_{N_\mathrm{A}})$ is the noise power at the sensing receiver. Let us remark that, in absence of the jammer, the second term in (2.22) is zero.

Regarding the self-interference term in (2.22), each element of vector $\boldsymbol{\zeta}_{:,k}^{(i)}$ can be interpreted as the signal scattered by a static target located very close to the receiver [40]. Hence,

$$\boldsymbol{\zeta}_{:,k}^{(i)} = \alpha_\mathrm{SI}^{(i)} x_k^{(i)} [e^{j\phi_{\mathrm{SI},1}^{(i)}}, \ldots, e^{j\phi_{\mathrm{SI},N_\mathrm{A}}^{(i)}}]^\mathsf{T} \tag{2.23}$$

where $\alpha_\mathrm{SI}^{(i)}$ is the self-interference attenuation and is the same for all receiving antennas, and $[\phi_{\mathrm{SI},1}^{(i)}, \ldots, \phi_{\mathrm{SI},N_\mathrm{A}}^{(i)}]$ are the phase shifts at the antennas.

2.5 Jammer Model

A significant portion of this thesis is dedicated to the analysis of jamming detection techniques. In this section, the various jammer models that have been employed in this study are presented. In particular, two distinct models are considered: one designed to disrupt communication networks, and another aimed at deceiving radar systems.

2.5.1 Reactive Jammer

A reactive jammer is an advanced ECM device designed to disrupt communication signals. Unlike traditional jammers that continuously emit interference, reactive jammers detect and target specific transmissions only when

they are active, making them more efficient and harder to detect.

The jammer is modeled by the 4-states machine shown in Fig. 2.4(a), where two sensing states, S_1 and S_2, alternate with idle and jamming states, I and J, respectively. In the idle state, the jammer remains silent for a time T_I and then it jumps into state S_1. In state S_1, the jammer senses the channel for a time T_1 to detect the transmission of a user; if no transmission is detected (hypothesis $\mathcal{H}_0$), the jammer returns to the idle state. When a signal is detected (hypothesis $\mathcal{H}_1$) the attacker goes into state J and interferes the communication for a time T_J. During T_J, the jamming signal with power P_J is transmitted. This jamming signal can assume several forms, e.g., white noise, a sinusoid or a signal with the same modulation of the victim communications. Then, the attacker alternates between states J and S_2, in which it performs detection with sensing time T_2.[4] Fig. 2.4(b) shows an example of a jammer attack.

During S_1 and S_2, the jammer senses the channel in a bandwidth W with sampling time $1/W$. In the presence of frequency flat channel, the nth sample of the equivalent low-pass signal received by the jammer is[5]

$$r_n^{\mathrm{J}} = \sum_{l=1}^{N_{\mathrm{T}}} \tilde{h}_l^{\mathrm{J}} \tilde{x}_{l,n} + \nu_n^{\mathrm{J}} \tag{2.24}$$

where $\tilde{x}_{l,n}$ for $l = 1, \ldots, N_{\mathrm{T}}$ is the nth sample of the signal transmitted by node l, $\tilde{h}_l^{\mathrm{J}}$ for $l = 1, \ldots, N_{\mathrm{T}}$ is the channel gain between node l and the jammer, and $\nu_n^{\mathrm{J}} \sim \mathcal{CN}(0, \sigma_{\mathrm{J}}^2)$ is the AWGN with i.i.d. real and imaginary parts, with noise power $\sigma_{\mathrm{J}}^2 = 2N_0^{\mathrm{J}}W$, where N_0^{J} is the two-sided power spectral density.[6]

The detection of a transmission is performed with an energy detector

[4] Note that the sensing time T_2 is usually shorter than T_1 to allow a more effective sensing [41], [42].

[5] We also consider that the coherence time of the channel is larger than the sensing times, T_1 and T_2.

[6] We consider $\tilde{x}_{l,n} = 0$ if node t is not transmitting at time instant n.

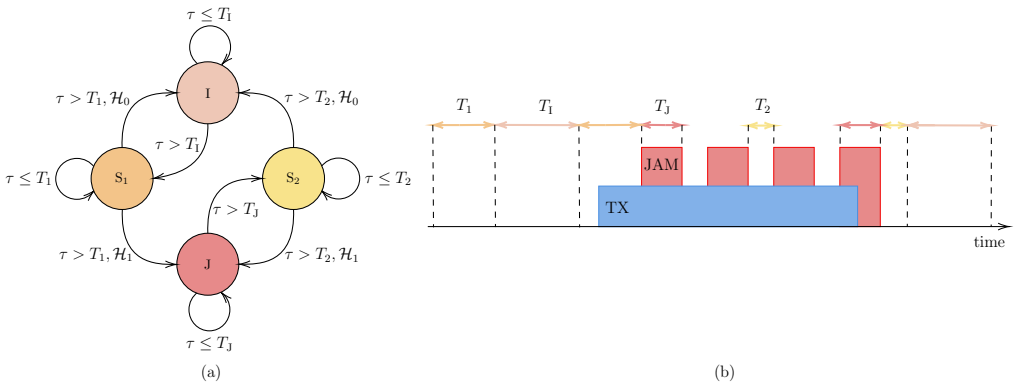

Figure 2.4: (a) Finite-state machine model for the reactive jammer. Hypothesis $\mathcal{H}_1$ is the detection of a transmission, while $\mathcal{H}_0$ is the null hypothesis; S_1 and S_2 are the sensing states; I and J are the idle and jamming states, respectively; τ is the sojourn time in a given state. (b) An example of reactive jamming. The jammer senses the spectrum for a period T_1 and detects the transmission of a user (in blue). Then, it alternates jamming (in red) and short sensing phases to make the jamming operation more effective.

(ED) [41] represented by

$$\frac{2}{\sigma_\mathrm{J}^2} \sum_{n=1}^{N_\mathrm{p}} |r_n^\mathrm{J}|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \xi \tag{2.25}$$

where ξ is the detection threshold obtained fixing the false alarm probability to 0.01. The time-bandwidth product of the ED is thus $N_\mathrm{p} \in \{WT_1, WT_2\}$ depending on the current jammer state.

2.5.2 Deceptive Jammer

A deceptive jammer in radar systems is a sophisticated ECM designed to mislead radar operators by transmitting false signals. These jammers create fake targets or alter the perceived location and speed of real targets, confusing the radar's tracking and detection capabilities. The most efficient way to implement a deceptive jammer consists to use a DRFM. It is a high speed, analog-to-digital converter and storage system which provides the capability to sample, process, and play back RF signals with minimum loss of fidelity.

In the event that the jammer is integrated into the cellular network, it is able to rapidly obtain pertinent data and formulate an effective strategy. For instance, in a hypothetical 5G NR network where ISAC is per-

formed using the physical downlink shared channel-demodulation reference signal (PDSCH-DMRS), also designated as the pilot, the jammer may be able to access the primary and secondary synchronization signals in order to obtain the physical cell identity. The cell ID comprises data regarding the initialization of the PDSCH-DMRS. Consequently, the jammer is aware of the resource elements (REs) where the PDSCH-DMRS is transmitted and what symbols it is composed of, thus facilitating the transmission of a delayed version of the pilot towards the BS.

Let us consider a deceptive jammer capable of mimicking the signal transmitted by the BS and injecting a false delay into the received signal with the aim of falsifying the BS's estimated location of the target. Specifically, this study assumes that the jamming attack occurs in the ith observation and kth subcarrier, using the same symbols $x_k^{(i)}$ transmitted by the BS. This represents a worst-case scenario where the radar receiver is completely misled.

The jammer comprises a transmitter antenna array with N_{J} elements arranged in an ULA with half-wavelength separation and adopts OFDM modulation with K subcarriers. Therefore, its signal can be written as

$$\tilde{\mathbf{x}}_{:,k}^{(i)} = \mathbf{w}_{\text{J}}^{(i)} x_k^{(i)} e^{-j2\pi k \Delta f \tau_{\text{f}}^{(i)}} \tag{2.26}$$

where $\mathbf{w}_{\text{J}}^{(i)} \in \mathbb{C}^{N_{\text{J}} \times 1}$ is the jammer beamforming vector and $\tau_{\text{f}}^{(i)}$ is the false delay introduced by the jammer. The beamforming vector can be expressed as

$$\mathbf{w}_{\text{J}}^{(i)} = \frac{\sqrt{P_{\text{J}} G_{\text{J}}}}{N_{\text{J}}} \mathbf{a}_{\text{J}}^{*}(\theta_{\text{J}}^{(i)}) \tag{2.27}$$

where P_{J} is the jammer signal power, G_{J} is the array gain along the beam steering direction, and $\mathbf{a}_{\text{J}}(\theta_{\text{J}}^{(i)}) \in \mathbb{C}^{N_{\text{J}} \times 1}$ is the steering vector.

Chapter 3

Blind Source Separation

The spectrum patrol captures mixtures of signals transmitted by network nodes and extracts the energy profiles shown in (2.14). These profiles retain information on the nodes' temporal behavior without the need for demodulation. To detect the presence of a jammer through causal inference, the first step is to characterize the temporal transmission patterns of each node in the wireless network. This necessitates reconstructing the temporal traffic profiles, $\mathbf{X}$, as if they were directly measured at each node. However, due to the wireless medium, the sensors capture a mixture of signals from the nodes, as shown in (2.15), necessitating an unmixing process to isolate $\mathbf{X}$ [43, 44]. In literature, the solutions put forth to accomplish this unmixing process are collectively referred to as BSS.

3.1 Existing Works

The BSS aims at recovering the source matrix $\mathbf{X}$ starting from the observations, $\mathbf{Y}$, without any prior knowledge of the channel matrix $\mathbf{H}$. This technique has wide applications in areas such as telecommunications, audio processing, and medical signal analysis. The fundamental goal of BSS is to recover the original source signals from observed mixtures, relying on the assumption that the sources are statistically independent or uncorrelated. In the field of audio processing, the source separation problem is analogous to

the cocktail party scenario, wherein multiple individuals engage in simultaneous discourse within a confined space, and the listener attempts to discern one particular conversation. [45]. There are two main approaches to BSS: determined blind source separation (DBSS) and UBSS.

In the DBSS approach, the number of observed mixed signals $N_{\mathrm{T}} + 1$ is equal to or greater than the number of source signals N_{R}. In literature, various methods for DBSS have been proposed, e.g., matrix factorization [46] and tensor decomposition [47,48], to name a few. However, the most popular technique is the independent component analysis (ICA). It exploits the statistical independence of the source signals to separate them. By maximizing the non-Gaussianity of the signals or minimizing mutual information, ICA effectively unmixes the observed signals [7].

In the UBSS approach, the number of observed mixed signals is less than the number of source signals. This scenario is more challenging because the system of equations is underdetermined, leading to an infinite number of possible solutions. Techniques for UBSS often involve additional assumptions or constraints, such as sparsity of the source signals [1]. They presumes that the source signals exhibit sparsity in a specific domain, such as time or frequency, implying that only a few sources are active at any given moment in these domains. To achieve sparsity, UBSS is typically applied following a linear transformation into the time-frequency domain. Rickard et al. introduced a method known as Degenerate Unmixing Estimation Technique (DUET) in [49], employing a windowed Fourier transform. A comparable approach is discussed in [50], where the short-time Fourier transform is utilized.

3.2 Problem Statement

We consider the worst-case scenario in which the number of RF sensors is less than the number of transmitters, i.e., we solve an underdetermined blind source separation (UBSS) problem. This implies that the mixing matrix $\mathbf{H}$ is not invertible, making the classical overdetermined BSS techniques inappropriate. Therefore, as in [1], we tackle the UBSS problem by first estimating the mixing matrix and then the source matrix, leveraging on its sparse na-

ture, i.e., assuming that each column of $\mathbf{X}$ has few non-zero entries. This assumption means that few nodes are transmitting simultaneously. If the MAC layer is based on scheduled access protocol, then at most two actors will transmit simultaneously: a network node and the jammer. Instead, if the network adopts a random access protocol, multiple nodes might concur in the transmission and collide. However, in a well-designed random access protocol the network is not overloaded and the source matrix, $\mathbf{X}$, is likely to be highly sparse. In the following, we propose a novel UBSS algorithm based on [1] that exploits such sparsity. Unlike most of the literature regarding UBSS, in which the sources that have to be separated are audio signals, we tailor our solution to deal with energy profiles transmitted by wireless nodes. In this sense, we did not use operations such as transformations to the time-frequency domain, that are common in the UBSS methods to increase the sparsity. For this reason, we propose a modified version of the algorithm in [1].

3.3 Estimate of the Mixing Matrix

We now aim to estimate $\mathbf{H}$ starting from the observations, $\mathbf{Y}$, relying on the sparsity of $\mathbf{X}$. For the sake of clarity, we first introduce the general estimation methodology and then remark two different situations: with or without jammer.

3.3.1 Transmission detection

Given the matrix of energy profiles, $\mathbf{Y}$, to reduce the number of samples and lighten the channel matrix estimation, the FC performs transmission detection. In particular, it aims to identify the samples corresponding to the occurrence of a transmission. The transmission detection algorithm is detailed in Algorithm 1 where, given $\mathbf{Y}$ as input, we analyze one column at a time. When a detection arises (line 5 of the algorithm) we start saving the columns until positive detection continues to occur. The output is a set of matrices $\mathbf{Y}^k$, with $k = 1, \ldots, K$, such that $\mathbf{Y}^k = \mathbf{Y}_{:,i_k:i_k+N_k}$ is a sub-matrix of

Algorithm 1: Transmission detection

Input : $\mathbf{Y} \in \mathbb{R}^{N_\mathrm{R} \times N_\mathrm{e}}$, $\epsilon^\dagger$
Output: $\mathbf{Y}^1, \ldots, \mathbf{Y}^\mathrm{K}$

$k \leftarrow 1$
Initialize $\mathbf{Y}^k \leftarrow \mathbf{0}$
for i **from** 1 **to** N_e **do**
  $\mathrm{TX}_i = \mathit{false}$
  $v_s \leftarrow \frac{2}{\sigma_\mathrm{S}^2} y_{s,i} > \epsilon,\ \forall s = 1, \ldots, N_\mathrm{R}$
  if at least one v_s is *true* **then**
    $\mathbf{Y}^k = \left[\mathbf{Y}^k\ \mathbf{y}_{:,i}\right]$
    $\mathrm{TX}_i = \mathit{true}$
  else
    if $\mathrm{TX}_{i-1} = \mathit{true}$ **and** $2 \leq i < N_\mathrm{e}$ **then**
      $k \leftarrow k+1$
      Initialize $\mathbf{Y}^k \leftarrow \mathbf{0}$
    end
  end
end

† ϵ is the detection threshold obtained fixing the false alarm probability to 0.01.

$\mathbf{Y}$ composed by its N_k consecutive columns in which the kth transmission has been detected. The transmission starting index is denoted as i_k. Each matrix $\mathbf{Y}^k$ can contain the superposition of the energy profiles transmitted by the nodes, the jammer, and the thermal noise. Fig. 3.1 depicts an example of the jth row of $\mathbf{Y}^k$. If the transmission detection is successful, the remaining rows of $\mathbf{Y}^k$ should have the same structure as the jth. However, since each row of $\mathbf{Y}^k$ corresponds to the measurement carried out by a different RF sensor, the signals of the transmitters will be mixed in different ways depending on the propagation scenario. Let us now reformulate eq. (2.15) as

$$\mathbf{Y}^k = \mathbf{H}\mathbf{X}^k + \mathbf{\Omega}^k \tag{3.1}$$

where $\mathbf{X}^k = \mathbf{X}_{:,i_k:i_k+N_k}$ and $\mathbf{\Omega}^k = \mathbf{\Omega}_{:,i_k:i_k+N_k}$.

3.3.2 Pseudo channel matrix estimation

In this phase we estimate a raw oversized version of the channel matrix, called pseudo channel matrix. We now feed matrix $\mathbf{Y}^k$ as input to the algorithm in [1], that is further described in the following. Initially, we divide element-wise each row of $\mathbf{Y}^k$ by its qth row, to obtain the ratio matrix

$$\mathbf{R} = \mathbf{Y}^k / \mathbf{y}^k_{q,:}. \tag{3.2}$$

Fig. 3.1 depicts an example of the jth row of $\mathbf{R}$ in which the transmission of a smart jammer is partially overlapped with the one of a legitimate user. This row is the result of the division between the jth and the qth rows of $\mathbf{Y}^k$ with $j \neq q$.

Then, $\mathbf{R}$ is divided into the sub-matrices $\mathbf{R}^i$, $i = 1, \ldots, I$ using the quantization-based clustering algorithm proposed in [1]. Fig. 3.1 offers a graphical illustration of this operation: looking at the jth row of $\mathbf{R}$, $\mathbf{r}_{j,:}$, it is possible to observe $I_j = 3$ clusters of samples. Each cluster is the set of samples whose energy values are all similar and are depicted in blue, red, and purple, respectively. As an example, let us imagine that the blue cluster is labeled as cluster 1. If we select all the columns of $\mathbf{R}$ identified by the same column indexes of cluster 1, we obtain the sub-matrix $\mathbf{R}^1$. The same operation can be repeated for all the clusters identified by each row of $\mathbf{R}$, overall generating $I = \sum_{j=1}^{N_\mathrm{R}} I_j$ sub-matrices. For more details about the clustering algorithm please refer to [1, Section II].

Considering the generic sub-matrix $\mathbf{R}^i$, we now estimate the corresponding column of the pseudo channel matrix as [1]

$$\widehat{\mathbf{h}}_{:,i} = \frac{[\langle \mathbf{r}^i_{1,:} \rangle, \ldots, \langle \mathbf{r}^i_{N_\mathrm{R},:} \rangle]^\mathsf{T}}{\| [\langle \mathbf{r}^i_{1,:} \rangle, \ldots, \langle \mathbf{r}^i_{N_\mathrm{R},:} \rangle]^\mathsf{T} \|_2} \qquad i = 1, \ldots, I \tag{3.3}$$

As detailed in Algorithm 2, which summarizes the complete mixing matrix estimation procedure, the steps between lines 4 and 8 are repeated for $q = 1, \ldots, N_\mathrm{R}$ to estimate a pseudo channel matrix $\hat{\mathbf{H}}^k \in \mathbb{R}^{N_\mathrm{R} \times N_h}$. Note that due to the concatenation procedure on step 8 of Algorithm 2 the final number of

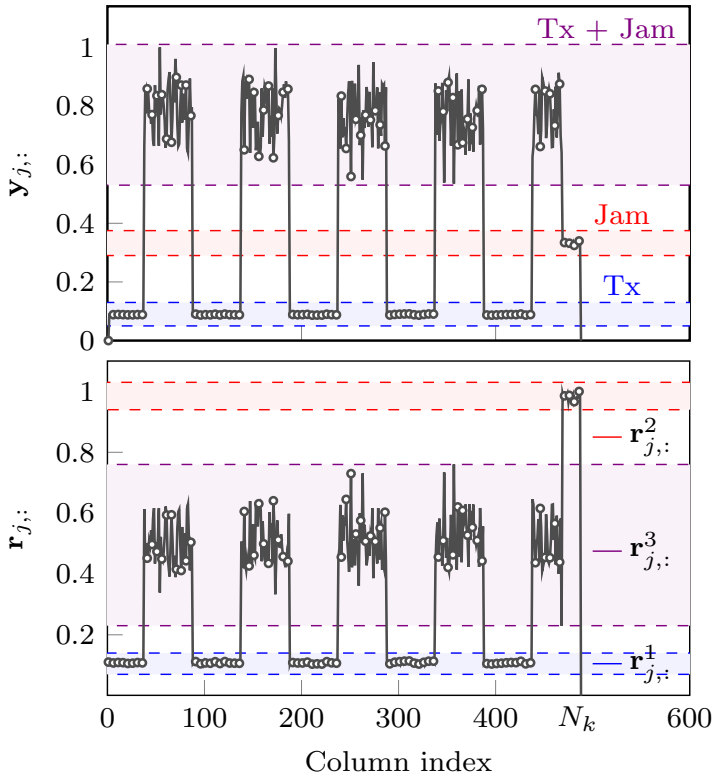

Figure 3.1: Above, example of the jth row of $\mathbf{Y}^k$ in a scenario with a transmitter and the jammer. Below, the corresponding jth row of $\mathbf{R}$ where we note the presence of three clusters. $\mathbf{R}^1$, $\mathbf{R}^2$, and $\mathbf{R}^3$ are the sub-matrices obtained after the clustering operation and corresponding to the samples associated to the user transmission, the jammer, and the overlap of the two, respectively.

columns of $\hat{\mathbf{H}}^k$ is now indicated with N_h.

3.3.3 Dimensionality reduction

Due to the estimation procedure, the pseudo channel matrices are likely to have a larger number of columns than $\mathbf{H}$. For this reason, we reduce the dimensionality of $\hat{\mathbf{H}}^k$ as follows. By performing singular value decomposition (SVD) of $\hat{\mathbf{H}}^k = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^\mathsf{T}$, the matrices of the singular vectors $\mathbf{U}$, $\mathbf{V}$, and the diagonal matrix of the singular values $\mathbf{\Lambda}$ are obtained. The singular values Λ_n, with $n = 1, 2, \ldots, N_h$, are thus sorted in descending order along with the

Algorithm 2: Estimate of the mixing matrix

Input : $\mathbf{Y}^k \in \mathbb{R}^{N_\mathrm{R} \times N_k}$, $k = 1, \ldots, \mathrm{K}$
Output: $\mathbf{W}$

for k **from** 1 **to** K **do**
  $\hat{\mathbf{H}}^k \leftarrow [\,]$
  for q **from** 1 **to** N_R **do**
    $\mathbf{R} \leftarrow \mathbf{Y}^k / \mathbf{y}^k_{q,:}$
    $\mathbf{R}^1, \ldots, \mathbf{R}^I \leftarrow$ FindSubMatrices($\mathbf{R}$)
    for i **from** 1 **to** I **do**
      $\hat{\mathbf{h}}_{:,i} \leftarrow \frac{[\langle \mathbf{r}^i_{1,:} \rangle, \ldots, \langle \mathbf{r}^i_{N_\mathrm{R},:} \rangle]^\mathsf{T}}{\| [\langle \mathbf{r}^i_{1,:} \rangle, \ldots, \langle \mathbf{r}^i_{N_\mathrm{R},:} \rangle]^\mathsf{T} \|_2}$
      $\hat{\mathbf{H}}^k \leftarrow \left[\hat{\mathbf{H}}^k \; \hat{\mathbf{h}}_{:,1} \ldots \hat{\mathbf{h}}_{:,I}\right]$
    end
  end
  Step 2: Pseudo Channel Matrix Estimation
  $\mathbf{W}^k \leftarrow$ Step 3: DimensionalityReduction($\hat{\mathbf{H}}^k$)
end
$\mathbf{W} \leftarrow$ Step 4: DuplicateElimination($\mathbf{W}^1, \ldots, \mathbf{W}^\mathrm{K}$)

corresponding singular vectors. The number of independent columns N_w of $\hat{\mathbf{H}}^k$ is given by the number of significant singular values, i.e.,

$$N_w = \sum_{n=1}^{N_h} \mathbb{1}_{\{\Lambda_n > \Lambda_1 \bar{\Lambda}\}} \tag{3.4}$$

where $\bar{\Lambda}$ is the singular value selection parameter chosen, e.g., according to the scree plot approach [51]. The decision on the singular value Λ_n is taken comparing the ratio Λ_n/Λ_1 with the threshold $\bar{\Lambda} = 0.01$. Such value means that Λ_n is two orders of magnitude smaller than the maximum singular value Λ_1. To accomplish the dimensionality reduction, a linear transformation is performed using a projection matrix $\tilde{\mathbf{V}} \in \mathbb{R}^{N_h \times N_w}$ obtained retaining only the N_w singular vectors of $\mathbf{V}$ corresponding to the most significant singular values. Therefore, $\hat{\mathbf{H}}^k$ can be projected onto a subspace whose dimensionality

is reduced from N_h to N_w by

$$\mathbf{W}^k = \hat{\mathbf{H}}^k \tilde{\mathbf{V}} \tag{3.5}$$

where $\mathbf{W}^k \in \mathbb{R}^{N_\mathrm{R} \times N_w}$ is the kth reduced pseudo channel matrix.[1] Iterating the procedure for each pseudo channel matrix $\hat{\mathbf{H}}^k$, we estimate a set of reduced pseudo channel matrices $\mathbf{W}^k$, with $k = 1, \ldots, K$ and concatenate them such that $\tilde{\mathbf{W}} = [\mathbf{W}^1, \mathbf{W}^2, \ldots, \mathbf{W}^K]$.

3.3.4 Duplicate elimination

After the complex procedure described above, it is possible that $\tilde{\mathbf{W}}$ contains multiple estimations of the same column of $\mathbf{H}$. In this case, an additional operation is performed to remove the duplicates from $\tilde{\mathbf{W}}$. Given a column $\tilde{\mathbf{w}}_{:,i}$, we recognise that $\tilde{\mathbf{w}}_{:,j}$ is a duplicate if

$$\|\tilde{\mathbf{w}}_{:,j} - \tilde{\mathbf{w}}_{:,i}\|_2 < \beta \tag{3.6}$$

where β is the elimination threshold. In the end, we obtain the estimated channel matrix $\mathbf{W} \in \mathbb{R}^{N_\mathrm{R} \times N_\mathrm{W}}$, where N_W is the number of estimated columns. In the numerical results section, a conservative threshold can reasonably be chosen, i.e., $\beta = 0.05$.

3.3.5 UBSS without Jammer

Note that considering the absence of the jammer, collisions, and thermal noise a graphical illustration of the matrix $\mathbf{X}^k$ is shown in Fig. 3.2, where $\mathbf{p}_k = [x_{k,i_k} \ldots x_{k,i_k+N_k}]$ is the vector of N_k energy samples of the packet transmitted by node k, and i_k is the index that identifies the packet transmission starting time.[2] Here we have $K = N_\mathrm{T}$ matrices, and $\mathbf{Y}^k$ corresponds to the packet transmitted by the kth node, $\mathbf{p}_k$. Therefore, (3.1) becomes $\mathbf{Y}^k = \mathbf{h}_{:,k} \otimes \mathbf{p}_k$

[1] It is important to note that, as a consequence of the dimensionality reduction, the entries of $\mathbf{W}^k$ may not be equal to the channel gains, and they can also be negative.

[2] To simplify the algorithm explanation, without loss of generality, the example in Fig. 3.2 considers one transmitted packet per node.

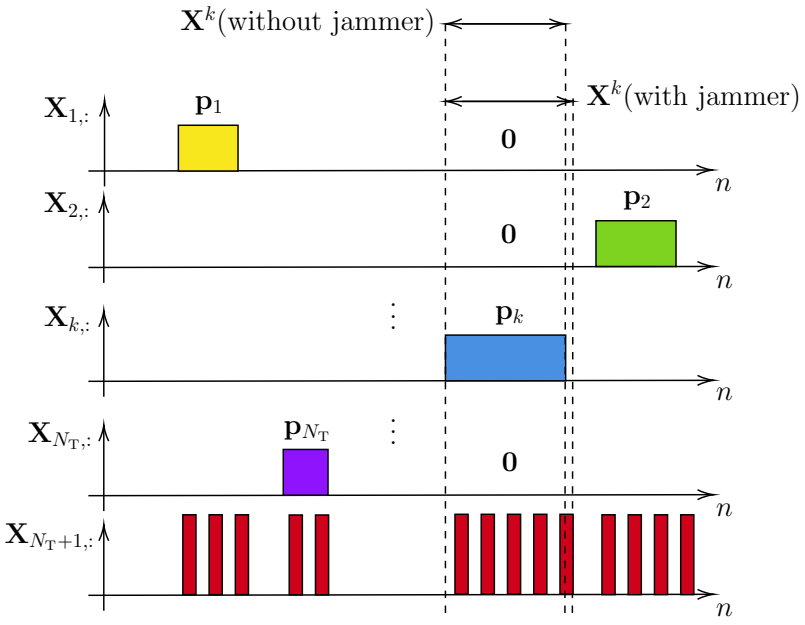

Figure 3.2: An illustration of the rows of $\mathbf{X}$. Row $\mathbf{X}_{N_\mathrm{T}+1}$ contains the energy profile of the signal emitted by the jammer. If the jammer is absent it is a row of zeros.

and the entries of $\mathbf{R}$ are $r_{i,j} = h_{i,k}/h_{q,k}$. Hence, the estimator (3.3) reduces to

$$\widehat{\mathbf{h}}_{:,k} = \frac{\mathbf{h}_{:,k}}{\|\mathbf{h}_{:,k}\|_2} \tag{3.7}$$

providing a perfect estimation of the channel matrix coefficient except for a normalization factor. Such normalization does not affect the reconstruction of the temporal profiles of the activities of the nodes. In this ideal scenario, the clustering operation in $\mathbf{R}$ returns the same whole matrix, from which it is possible to estimate the kth column of $\mathbf{H}$.

3.3.6 UBSS with Jammer

The problem becomes more challenging in the presence of a jammer because each transmitted packet could experience at least one collision with the jamming signal.[3] In this case, a graphical illustration of the matrix $\mathbf{X}^k$ is shown

[3]In the case of random access protocol, collisions can also occur between the packets transmitted by legitimate users. However, the algorithm does not need to distinguish between different types of collisions.

in Fig. 3.2, where the jamming packets in row $N_{\mathrm{T}}+1$ are highlighted in red. Here, due to the presence of the jammer packets, $\mathbf{Y}^k$ is the superposition of the transmissions of the jammer and the kth legitimate node. Evaluating the corresponding matrix $\mathbf{R}$ and performing the clustering operation, we obtain the three submatrices whose jth rows are depicted in Fig. 3.1. The first, in blue, is composed of the columns of $\mathbf{R}$ corresponding only to the transmission of the kth node, the second, in red, is obtained by the columns corresponding only to the transmission of the jammer, while the third, in purple, is composed by the columns corresponding to the superposition of the transmissions of the node and the jammer. The estimation in (3.3) is performed for the three sub-matrices, obtaining three estimated pseudo channel matrix columns. Considering the sub-matrix $\mathbf{R}^3$, the corresponding estimated column $\hat{\mathbf{h}}_{:,3}$ is wrong because of the superposition of the two signals. However, it is dependent of $\hat{\mathbf{h}}_{:,1}$ and $\hat{\mathbf{h}}_{:,2}$, and, thus, deleted through dimensionality reduction.

3.4 Unmixing by OMP

Once the mixing matrix $\mathbf{W}$ is estimated, the reconstruction of the transmitted energy profiles is performed. More precisely, we aim to estimate $\mathbf{X}$ starting from the observations $\mathbf{Y}$ and the estimated mixing matrix $\mathbf{W}$. There are three possible approaches:

- Determined, i.e., $N_{\mathrm{R}} = N_{\mathrm{W}}$, if $\mathbf{W}$ has full rank, then $\mathbf{X} = \mathbf{W}^{-1}\mathbf{Y}$.

- Overdetermined, i.e., $N_{\mathrm{R}} > N_{\mathrm{W}}$, it is possible to find an approximate solution $\mathbf{X} = \mathbf{W}^{\dagger}\mathbf{Y}$, where $\mathbf{W}^{\dagger}$ is the pseudo-inverse of $\mathbf{W}$.

- Underdetermined, i.e., $N_{\mathrm{R}} < N_{\mathrm{W}}$, where we generally have an infinite number of solutions and the problem is solved through an optimization algorithm. Hence the objective here is to maximize/minimize an objective function under a set of constraints.

As previously outlined, our analysis is based on an underdetermined scenario with a sparsity constraint. The problem is thus formulated as follows

$$\begin{aligned} &\min_{\mathbf{x}_{:,i}} \|\mathbf{x}_{:,i}\|_0 \\ &\text{s.t. } \mathbf{W}\mathbf{x}_{:,i} = \mathbf{y}_{:,i} \end{aligned} \tag{3.8}$$

for $i = 1, \ldots, N_\text{e}$. This problem is recognized as NP-hard and can be addressed using two primary methods. The first method is *basis pursuit*, a sophisticated numerical technique that, in some instances, achieves an exact solution by substituting the l_0 norm with the l_1 norm [52]. The second approach, which we employ in our solution, is *matching pursuit*. This method seeks a sequential, sub-optimal representation through a greedy algorithm [53]. Specifically, in this study, we reformulate equation (3.8) to be solved using the orthogonal matching pursuit (OMP) algorithm [54], i.e.,

$$\begin{aligned} &\min_{\mathbf{x}_{:,i}} \|\mathbf{y}_{:,i} - \mathbf{W}\mathbf{x}_{:,i}\|_2 \\ &\text{s.t. } \|\mathbf{x}_{:,i}\|_0 \leq \gamma \end{aligned} \tag{3.9}$$

where γ is the sparsity constraint.

The output of the OMP is a matrix $\hat{\mathbf{X}} \in \mathbb{R}^{N_\text{W} \times N_\text{e}}$ where, due to the dimensionality reduction adopted, some entries could get a sign flip; hence, the absolute value of the elements of $\hat{\mathbf{X}}$ is taken. Given that the number of columns of the estimated mixing matrix $\mathbf{W}$ might be different from the real one, even after OMP, the matrix $\hat{\mathbf{X}}$ might have a different number N_W of rows than $\mathbf{X}$. Usually, in these cases, part of the estimated sources contains only residual crosstalk due to the separation. For this reason, we perform a skimming operation that deletes all the negligible rows. This operation is performed deleting all the rows $\hat{\mathbf{x}}_{i,:}$ that satisfy

$$\frac{\max \hat{\mathbf{x}}_{i,:}}{\max \hat{\mathbf{X}}} < \Gamma \tag{3.10}$$

where $\max \hat{\mathbf{X}}$ is the maximum value in $\hat{\mathbf{X}}$, and $\Gamma \in [0, 1]$ is the skimming

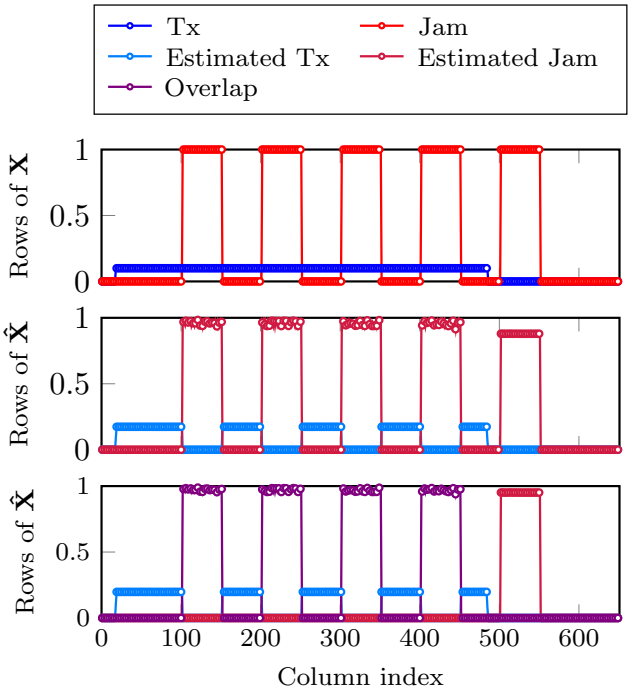

Figure 3.3: Above are the true energy profiles of a single transmitter and the jammer. In the middle, the energy profiles recovered with the algorithm proposed in this chapter. Below is the result with the algorithm in [1]. For both algorithms, $N_{\mathrm{R}} = 5$, and OMP is used in the second step. Notice that three sources are reconstructed instead of two in the image below. The phantom source is represented in purple and corresponds to the overlap between transmitter and jammer packets. On the contrary, the proposed solution correctly recovers only two sources with appreciable fidelity of the jammer profile.

threshold. A threshold $\Gamma = 0.001$ is reasonable, because the residual crosstalk is notably smaller than the correctly estimated sources. In conclusion, at the end of the UBSS we obtain a matrix $\mathbf{Z} \in \mathbb{R}^{L \times N_{\mathrm{e}}}$ where L is the final number of estimated sources.

3.4.1 Sparsity

Given the fixed sparsity in (3.9), how do we determine the appropriate value for γ? In other words, under what conditions can we assert the uniqueness of the sparsest solution? The answer to these questions lies in the concept

of the spark. The spark of a matrix $\mathbf{W} \in \mathbb{R}^{N_\mathrm{R} \times N_\mathrm{W}}$ is defined as the smallest number of columns of $\mathbf{W}$ that are linearly dependent. According to the uniqueness theorem, if the equation $\mathbf{W}\mathbf{x}_{:,i} = \mathbf{y}_{:,i}$ has a solution $\mathbf{x}_{:,i}$ such that $\|\mathbf{x}_{:,i}\|_0 < \mathrm{spark}(\mathbf{W})/2$, then this solution is guaranteed to be the sparsest possible.

However, the spark of a matrix is NP-hard to compute [55]. Therefore, to avoid this problem, a possible solution is based on the definition of the mutual coherence. The value of γ is chosen according to the mutual coherence, the largest normalized inner product between distinct columns of $\mathbf{W}$, i.e.,

$$\mu(\mathbf{W}) = \max_{1 \leq i,j \leq N_\mathrm{W}, i \neq j} \frac{|\mathbf{w}_{:,i}^\mathsf{T} \mathbf{w}_{:,j}|}{\|\mathbf{w}_{:,i}\|_2 \|\mathbf{w}_{:,j}\|_2}. \tag{3.11}$$

A large $\mu(\mathbf{W})$ means that the columns of $\mathbf{W}$ are highly correlated and, thus, the signal reconstruction is hard. It has been proved that [56]

$$\mathrm{spark}(\mathbf{W}) \geq 1 + \frac{1}{\mu(\mathbf{W})}. \tag{3.12}$$

Thus, a stricter version of the uniqueness theorem can be applied: if the problem (3.9) admits a solution $\mathbf{x}_{:,i}$ with $\|\mathbf{x}_{:,i}\|_0 < \frac{1}{2}\big(1 + \frac{1}{\mu(\mathbf{W})}\big)$, then it is the sparsest possible. Hence, the sparsity constraint is set to

$$\gamma = \frac{1}{2}\left(1 + \frac{1}{\mu(\mathbf{W})}\right). \tag{3.13}$$

Since the estimated channel matrix, $\mathbf{W}$, might have duplicated columns, then $\mu(\mathbf{W}) \simeq 1$ and $\gamma = 1$. Setting the sparsity constraint to 1 has a direct consequence in the estimation of the sources, clearly portrayed in Fig. 3.3, in which a scenario with $N_\mathrm{R} = 5$ sensors, a single transmitter, and the jammer is considered. In fig. 3.3, the image above shows the transmitted signals, while in the middle and below the reconstructed sources with and without the dimensionality reduction procedure are depicted, respectively. It is possible to notice how in both cases, the reconstructed signal in blue is fragmented because of the sparsity constraint that imposes that in each column $\mathbf{x}_{:,i}$ only one entry has to be nonzero. Hence, in case of a collision, only one of the

colliding signals will be correctly estimated in each energy sample. This approach leads to a non-perfect signal reconstruction when collisions arise, but it is tolerable since its impact on the jamming detection is low, as shown in the simulations in Chapter 8. Moreover, Fig. 3.3 shows how dimensionality reduction allows a more accurate reconstruction of the sources.

Chapter 4

Jammer Detection through Spectrum Patrol

A reactive jammer poses a significant threat to the physical layer security of communication networks. Unlike other types of jammers, its behavior is uniquely dependent on the actions of legitimate users, initiating an attack only when the user transmits. This creates a causal relationship where the user's transmission triggers the jammer's interference. In this chapter, we leverage this characteristic to develop a method for detecting reactive jamming. Specifically, we consider a spectrum patrol that is presumed to lack prior awareness of legitimate networks and is tasked with discerning the presence of a reactive jammer.

4.1 Existing Works

Historically, jamming has been primarily studied within the context of spread spectrum communications for military applications. However, over the past decade, its scope has expanded to civilian domains, prompting numerous studies on its impact on wireless networks [57, 58]. In [59], the authors study the detection of reactive jamming in direct sequence spread spectrum (DSSS) wireless communications systems. The detection is carried out using two metrics based on the packet delivery ratio (PDR), namely, an observed PDR_o and

an estimated PDR_e. The first is the ratio of correctly received packets over the total number of transmitted ones, while the second PDR is predicted through the chip error rate of the packet preamble. The rationale behind this detection strategy is that the jammer cannot interfere the first preamble symbols of a packet because of the non-negligible sensing time. In [60], a scheme for detecting a jammer exploiting the received signal strength (RSS) and the errors of the received bits sequence is proposed. If a bit is received with an error and the corresponding RSS value is high, then there should be an external interferer (i.e., the jammer); instead, if the corresponding RSS is low, errors are likely caused by the weak signal, e.g., due to multipath or shadowing. Since jamming can severely affect the performance of Global Navigation Satellite Systems (GNSSs), characterized by remarkably low received powers, several works tackle this problem. For example, in [61], the authors exploit the carrier-to-noise density power ratio to detect the attacker. The rationale behind this is that the victim perceives a significant increase in the noise power in the presence of jamming. In [62], the authors study the physical layer security of a pilot-based massive MIMO system proposing a generalized likelihood ratio test (GLRT). In [63], the authors present an algorithm for jammer detection in wide-band cognitive radio networks based on compressed sensing (CS) and ED. They first sample the wide-band signal through CS and identify a set of sub-bands occupied by legitimate users and the jammer. Then, the power spectral density is used to detect the jammer based on the information about licit transmitters and the jammer stored on a database. The proposed method is computationally inexpensive but exhibits a high missed detection rate and relies on a database that contains information about all the legitimate users and the jammer, which might not always be feasible. In [64], the authors propose three classifiers, namely K-nearest neighbors, random forest, and Bayesian classifier to detect a proactive jammer. In [65], a framework to guide the receiver in selecting the most suitable between many conventional anti-jamming schemes is proposed.

Recently, the introduction of AI techniques in the field of wireless communications gave impetus to developing machine learning (ML)-based jamming detectors. In [66], two neural networks (NNs) are proposed to detect and

classify a jammer in OFDM transmissions. The authors suggest the introduction of a pre-processing stage in which a time-frequency transform is performed to improve the NNs performance. A similar method is applied in [67] to an OFDM-based satellite communication system. Both detection and classification are also performed in [68] where the authors propose an ML-based approach that exploits only the PDR and the RSS, retrievable at the GW side without demodulating the signals received from the network nodes. In [69], a large dataset with signal features that identify jamming signals is generated. Then, random forest, support vector machine and a NN are tested in a wireless communication network using this dataset for training. In [70], a multi-layer perceptron NN is used to classify and detect a jammer attempting to interfere DVB-S2 signals. In [71], the authors suggest combining cyclic spectral analysis and NNs for jamming detection in wide-band cognitive radios. All the proposed ML-based jamming detectors have the same general operating scheme, composed of features extraction and selection followed by training and testing of a specific algorithm.

The detection schemes mentioned above need to be performed on the receiver side, i.e., within the network, as they require almost complete knowledge of the details of the communication protocols and the transmitted signals. For example, in [59], the prior knowledge of the first few jamming-free bits in the preamble is assumed, while in [60] the capability of detecting bit errors is mandatory for the detection, thus requiring the demodulation of the received packets. Instead, the AI-based solutions are sensitive to generalization errors because if the training is performed using specific signal formats (e.g., OFDM in [66, 67]), then a change in the format will require a brand new training procedure.

The main problem of the listed approaches is that all the computational burden is carried by only one device, which is usually part of the network infrastructure, and this limits the overall performance of both the network and the jamming detection. From this perspective, the idea of adopting a set of crowdsourced spectrum sensors (or patrollers) that cooperate to detect violations of the spectrum usage policies appears attractive [3,19]. In [3], the authors address a collaborative signal detection problem in which they aim

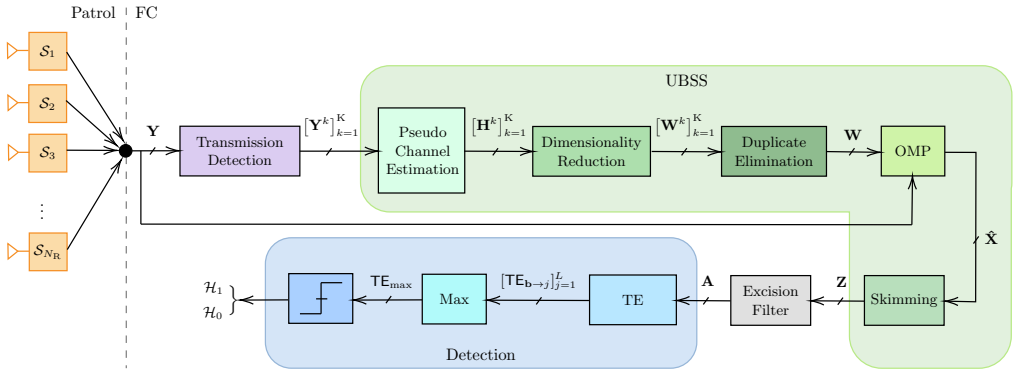

Figure 4.1: Block diagram of the patrol system with N_{R} sensors. In the FC, after a transmission detection, UBSS is performed, then separated energy profiles are transformed into binary series analyzed by transfer entropy (TE) to detect the presence of a jamming attack.

to identify the optimal subset of sensors and their configurations to maximize the detection performance given certain resource limitations. In [19], mobile users cooperate through a crowdsourced enforcement architecture to detect and localize an infraction effectively. Both the presented methods rely on the spectrum patrollers receiving only the signal emitted by the intruder (i.e., a jammer). However, in a more general scenario, the transmission of the jammer concurs with the ones of the legitimate users, causing the sensors to receive a mixture of superposed signals.

4.2 Problem Statement

We propose a novel framework for detecting reactive jammers that exploit the mixed signals received by the spectrum patrollers and an original methodology based on causal inference. The detection strategy is quite general, including situations where legitimate users belong to different networks sharing the same spectrum. For this reason, the spectrum patrollers observe mixtures of signals transmitted over the air by the network nodes and extract energy profiles collected in the matrix $\mathbf{Y}$ in (2.15). Such profiles retain information on the temporal behavior of the nodes without requiring demodulation.

Following this pre-processing stage, the solution applies the UBSS algorithm presented in Chapter 3, resulting in the matrix $\mathbf{Z}$, which provides an estimation of the energy profiles transmitted by each network node and the jammer.

After signal separation, we analyze the temporal relationship between the signals emitted by the nodes to detect the presence of an intruder. If the jammer is reactive, it only transmits after sensing a legitimate user's transmission. This behavior can be modeled as a causal relationship, where the legitimate user's transmission is the cause, and the jammer's attack is the effect. Therefore, our objective is to detect the presence of the jammer by identifying this causal relationship using causal inference tools [72]. To achieve this, we propose a novel jamming detection methodology based on *directed information*, a metric that quantifies causal relationships between time series, originally introduced in [73] and later reinterpreted in [74] under the name transfer entropy (TE). The complete processing chain is depicted in Fig. 4.1. The green blocks correspond to the UBSS step, while the excision filter and blue blocks are discussed in detail in this chapter.

4.3 Excision Filter

The jamming detection algorithm presented in Section 4.5 is based on the temporal dynamics of the packet flows generated by the nodes and the jammer. To lighten the causality inference procedure, we process the time series in $\mathbf{Z}$ to obtain sequences of 0s and 1s; this is performed by an excision filter which zeroes out the energy samples due to crosstalk [75]. The output is matrix $\mathbf{A} \in \mathbb{R}^{L \times N_e}$ with entries

$$a_{l,n} = \begin{cases} 1 & \text{if } z_{l,n} \geq \lambda_l \\ 0 & \text{otherwise} \end{cases} \tag{4.1}$$

where the threshold λ_l is set as a fraction $q \in [0, 1]$ of the maximum of $\mathbf{z}_{l,:}$, i.e.,

$$\lambda_l = q \cdot \max_n z_{l,n}, \quad l = 1, \ldots, L. \tag{4.2}$$

In the numerical results section, the threshold q is set to 0.01.

4.4 Causality

In statistics, given two random variables B and C, the focus is often on prediction. For instance, one might be interested in determining the likely value of B given that $C = c$, or in calculating the probability that $B = b$ conditioned on $C = c$. Causality, however, introduces a different inquiry, aiming to understand the consequences of directly intervening in the system [76]. Specifically, one might ask: What effect does an intervention on C have on B? [1]

Answering this question requires knowledge of the system's causal structure. In the context of time series analysis, a widely accepted definition of causality is provided by *Granger Causality*, which asserts that: a time series $\mathbf{a}_i$ is said to Granger-cause another time series $\mathbf{a}_j$ if past values of $\mathbf{a}_i$ contain information that helps predict $\mathbf{a}_j$ beyond what is contained in past values of $\mathbf{a}_j$ alone [77].

There are two primary approaches to evaluating Granger Causality:

- Model-based: this approach involves the use of a specific model, with the most common being the autoregressive model, where the current sample is expressed as a linear combination of past samples.

- Model-free: this approach is employed when selecting an appropriate model is challenging, such as in cases of non-linearity between the

[1] It is important to distinguish between the concepts of intervention and observation. If we observe that $C = c$, it can be concluded that the condition of the system has caused C to be worth c. However, if we intervene and set $C = c$, we are effectively removing all causal links that may exist between C and other variables. For further investigation, please refer to [76].

present and past. A commonly used tool in this context is TE.

4.4.1 Transfer Entropy

The smart jammer transmits solely after the detection of the transmission of a legitimate user. Hence, we expect to find an underlying causal relationship between the energy profiles transmitted by the users and the jammer, in which the latter is the *effect* and the others are the *causes*. A state-of-the-art tool for causal inference in time series is TE [74], [73]. Considering two rows $\mathbf{a}_{i,:}$ and $\mathbf{a}_{j,:}$ of $\mathbf{A}$, the TE from $\mathbf{a}_{i,:}$ to $\mathbf{a}_{j,:}$ is a conditional mutual information defined as

$$\begin{aligned}
&\mathsf{TE}_{i\to j}(k,r) = \mathcal{I}\left(a_{j,n}; \mathbf{a}_{i,n-1:n-r} | \mathbf{a}_{j,n-1:n-k}\right) \\
&= \sum_{\substack{\mathbf{a}_{j,n-1:n-k},\\ \mathbf{a}_{i,n-1:n-r},\\ a_{j,n}}} p\left(a_{j,n}, \mathbf{a}_{i,n-1:n-r}, \mathbf{a}_{j,n-1:n-k}\right) \log_2 \frac{p\left(a_{j,n} | \mathbf{a}_{i,n-1:n-r}, \mathbf{a}_{j,n-1:n-k}\right)}{p\left(a_{j,n} | \mathbf{a}_{j,n-1:n-k}\right)} \\
&= \mathbb{E}\left[\log_2 \frac{p\left(a_{j,n} | \mathbf{a}_{i,n-1:n-r}, \mathbf{a}_{j,n-1:n-k}\right)}{p\left(a_{j,n} | \mathbf{a}_{j,n-1:n-k}\right)}\right]
\end{aligned} \tag{4.3}$$

where $p(\cdot|\cdot)$ is a conditional probability mass function, $\mathcal{I}(\cdot)$ indicates the mutual information, and k and r are time lags. As in [72], histogram based estimates are computed for the probability mass functions $p(\cdot|\cdot)$, for each possible configurations of $a_{j,n}$, $\mathbf{a}_{j,n-1:n-k}$, and $\mathbf{a}_{i,n-1:n-r}$. TE can be interpreted as the amount of information in the current values of $\mathbf{a}_{j,:}$ that is contained in the past values of $\mathbf{a}_{i,:}$, given the past values of $\mathbf{a}_{j,:}$. If $\mathbf{a}_{i,:}$ has no influence on $\mathbf{a}_{j,:}$, then the two probabilities in the fraction are equal and $\mathsf{TE}_{i\to j}(k,r) = 0$. Otherwise, if some information flows from $\mathbf{a}_{i,:}$ to $\mathbf{a}_{j,:}$, then $\mathsf{TE}_{i\to j}(k,r) > 0$. TE, unlike mutual information and cross-correlation, is asymmetrical and, thus, it allows identifying the direction of the information flow between the time series.

Algorithm 3: All-versus-one transfer entropy (AvOTE) for jammer attack detection

Input : $\mathbf{A} \in \mathbb{R}^{L \times N_e}$, $k_{\max}$, $r_{\max}$, θ
Output: Decision $\mathcal{H} \in \{\mathcal{H}_0, \mathcal{H}_1\}$

$\mathbf{v} \leftarrow \mathbf{0}$
for j **from** 1 **to** L **do**
  $\mathbf{b} \leftarrow \sum_{i=1, i \neq j}^{L} \mathbf{a}_{i,:}$
  Perform grid search to set k and r:
  $k_{\text{sel}} \leftarrow 0$
  $r_{\text{sel}} \leftarrow 0$
  for k **from** 1 **to** $k_{\max}$ **do**
    for r **from** 1 **to** $r_{\max}$ **do**
      if $\mathsf{TE}_{\mathbf{b} \to j}(k, r) > \mathsf{TE}_{\mathbf{b} \to j}(k_{\text{sel}}, r_{\text{sel}})$ **then**
        $k_{\text{sel}} \leftarrow k$
        $r_{\text{sel}} \leftarrow r$
      end
    end
  end
  $v_j \leftarrow \mathsf{TE}_{\mathbf{b} \to j}(k_{\text{sel}}, r_{\text{sel}})$
end
$\mathsf{TE}_{\max} \leftarrow \max_j \{v_j\}$
$\mathcal{H} \leftarrow \mathsf{TE}_{\max} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta$

4.5 Jammer Detection via Causal Inference

Let us consider a wireless network with a star topology, in which the nodes communicate with the gateway or AP so that the energy profiles transmitted are not causally related. We now seek to detect the information flow from the signals emitted by the legitimate nodes toward the jammer. Hence, we evaluate $\mathsf{TE}_{i \to j}(k, r)$ for each possible pair of transmitters (i, j), expecting that the measure of causality will be more significant when the ith transmitter is a legitimate node and the jth is the jammer. On the contrary, TE will be negligible when both transmitters are legitimate. This procedure implies calculating $L(L-1)$ values of TE, where L is the number of estimated

transmitters. To reduce the number of TE computations, we propose a novel approach named all-versus-one transfer entropy (AvOTE). Considering that during its sensing phase, the jammer collects energy samples corresponding to the superposition of the signals emitted by all the legitimate nodes, we expect to find a causal relationship in which the sum of the signals emitted by the nodes is the *cause* and the jamming signal is the *effect*. Therefore, let us introduce the sum vector $\mathbf{b} \in \mathbb{R}^{1\times N_\mathrm{e}}$, defined as $\mathbf{b} = \sum_{i=1}^{L} \mathbf{a}_{i,:}$ with $i \neq j$. Hence, we evaluate $\mathsf{TE}_{\mathbf{b}\to j}(k, r)$ for each transmitter $j = 1, \ldots, L$, namely the TE from the sum of all the other signals towards the jth signal. We expect that only when the jth transmitter is the jammer the corresponding TE will be significant and the highest among all. This procedure is computationally lighter than the previous one because it only requires the computation of L TEs. Then, given that we aim to detect the presence of one jammer, we find the maximum of the TEs evaluated, $\mathsf{TE}_{\max}$.

A high $\mathsf{TE}_{\max}$ value indicates that a jammer is likely to be present, while a small value denotes its absence. Thus, $\mathsf{TE}_{\max}$ can be interpreted as a test statistic, hence

$$\mathsf{TE}_{\max} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta. \tag{4.4}$$

The null hypothesis, $\mathcal{H}_0$, stands for the case when no jamming is present, while the alternate hypothesis, $\mathcal{H}_1$, corresponds to its presence. The threshold θ is given by setting the false alarm probability $p_{\mathrm{FA}} = \mathbb{P}(\mathsf{TE}_{\max} > \theta \,|\, \mathcal{H}_0)$, where the null distribution, is calculated via histogram based probability density function estimation.[2] The correct time lags for calculating TE are set by performing a grid search and finding the combination that outputs the highest value of TE. The complete AvOTE method is detailed in Algorithm 3. In the numerical results section, the maximum time lags for TE are set to $k_{\max} = r_{\max} = 8$ samples.

[2]We collect a large number of $\mathsf{TE}_{\max}$ values while ensuring that no jammer is present (i.e., under $\mathcal{H}_0$). These values are then used to construct a histogram, which serves as an empirical approximation of the null distribution of $\mathsf{TE}_{\max}$. By analyzing this histogram, we can determine the threshold θ such that the probability $\mathbb{P}(\mathsf{TE}_{\max} > \theta \,|\, \mathcal{H}_0)$ matches the desired false alarm probability p_{FA}. This approach allows us to accurately set θ, ensuring that the test maintains the specified level of false alarms.

Algorithm 4: All-versus-one cross correlation (AvOCC) for jammer attack detection

Input : $\mathbf{A} \in \mathbb{R}^{L \times N_\mathrm{e}}$, θ
Output: Decision $\mathcal{H} \in \{\mathcal{H}_0, \mathcal{H}_1\}$

$\mathbf{v} \leftarrow \mathbf{0}$
for j **from** 1 **to** L **do**
  $\mathbf{b} \leftarrow \sum_{i=1, i\neq j}^{L} \mathbf{a}_{i,:}$
  $v_j \leftarrow \max_m |\mathbf{c}_{\mathbf{b}\leftrightarrow j}(m)|$
end
$\mathsf{CC}_{\max} \leftarrow \max_j \{v_j\}$
$\mathsf{CC}_{\max} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta$

4.6 Cross Correlation

Despite cross-correlation cannot determine causality, we include a comparison between our causality-based solution, AvOTE, and a cross-correlation-based method, AvOCC, in the numerical results section to further validate our approach. Given two reconstructed energy profiles $\mathbf{a}_{i,:}$ and $\mathbf{a}_{j,:}$, the cross-correlation is

$$\mathbf{c}_{i\leftrightarrow j}(m) = \sum_{n=1}^{N_\mathrm{e}-m} a_{i,n} a_{j,n+m} \tag{4.5}$$

where n indicates the time samples and m is the time lag. The AvOCC algorithm is detailed in Algorithm 4. Since, in this case, the grid search is not necessary, and the computation of cross-correlation is much easier than TE, AvOCC is computationally lighter than AvOTE.

Chapter 5

Jammer Detection through Latent Model

In radar applications, deceptive jammers pose a significant threat by obscuring the true target position and misleading the receiver with false location information. Consequently, developing effective strategies for intruder detection within sensing networks is crucial, particularly for the next generation of wireless systems, where dual-functional networks will be deployed [78].

The integration of AI techniques into wireless communications has accelerated the development of neural network-based jamming detectors. In this chapter, we focus on the application of VAEs for deceptive jamming detection, as these generative latent variable models excel at learning latent data representations, making them well-suited for this task.

5.1 Existing Works

With the rapid proliferation of ISAC techniques as a cornerstone of the upcoming 6G wireless generations, a new threat emerges for wireless networks. If jamming attacks are feasible in communication, they become even easier for sensing due to the significantly weaker echo signals at the BS receiver. Furthermore, the threat is heightened by the presence of increasingly intelligent jammers that not only disrupt communications but also aim to deceive

legitimate users. For example, in [79,80] they propose an illegitimate use of a intelligent reflecting surface (IRS) with the goal to degrade sensing and communication performance. The idea is to quickly change the wireless channel within the coherence time, as ISAC performance depends on maintaining a consistent coherence time. In [81], instead, the IRS is used to flexibly configure the propagation environment of ISAC in order to mitigate jamming attack.

Further exploring ISAC's physical layer security, in [82] they investigate the possibility that a malicious target exploits the sensing signal capturing information reserved for the UE. At the first stage, through a omnidirectional waveform, assuming to know the position of the UE, they obtain an angle estimation of Eve. However, they do not consider the possibility that Eve cooperates with a deceptive jamming which is able to falsify his position. To the best of our knowledge, the presence of a deceptive jammer in an ISAC scenario has not been addressed in the existing literature. However, in comparison to a traditional radar application, the likelihood of a jammer being able to deceive the BS is significantly higher in an ISAC network.

In Section 4.1, a comprehensive review of the literature on jammer detection techniques in communication networks was provided. Accordingly, this section shifts focus to a detailed examination of jammer detection schemes within radar systems. Classic methods exploit likelihood-based algorithms that model the echo signals and adopting the GLRT, as in [83, 84]. They employee a two-block approach to resolve a multiple hypothesis test. Initially, the presence of a target and only noise is distinguished. Subsequently, a second test is conducted to differentiate between a radar target and a false target. While these likelihood-based methods rely on some prior information as the statistical distribution of the channel and the clutter, in [85], they perform jamming recognition and classification basing on feature extraction. In particular, two classifiers, decision tree and support vector machine, are fed with featured extracted by the received signals. In [86], the authors propose electronic counter-countermeasures (ECCM) schemes for OFDM radar that improve local signal-to-interference plus noise ratio (SINR), optimize initial phases to resist deception jamming, and develop waveform optimiza-

tion methods to minimize jamming energy. In [87], the authors propose a power optimization strategy for multiple radar systems to counteract deception jamming in multi-target tracking tasks. They derive the posterior Cramer-Rao lower bound for deception range, which is crucial for distinguishing between physical and false targets. Using this metric, they introduce a method for false target discrimination and formulate a power optimization problem aimed at optimizing both tracking accuracy and discrimination performance.

5.2 Problem Statement

We propose a jamming detection framework that, starting from the echo signals acquired by the BS and leveraging the latent space identification capability of VAEs is able to detect the presence of an intruder in a MIMO-OFDM system. The detector is trained on a dataset consisting of received echoes from a real target in the absence of jamming, allowing the VAE to learn the optimal latent representation of the data. During testing, when the jammer is present, the detector identifies the anomalous signal by its incompatibility with the learned latent space. To evaluate the performance of the proposed solution, we investigate a case study consisting of a 5G wireless network employing an ISAC system in presence of a deceptive jammer, already detailed in Section 2.4.

In Fig. 5.1, the decision-making process is illustrated. Initially, the BS performs pre-processing, after which the processed backscatter vector $\mathbf{g}_{:,i}$ is fed into the VAE. The output of the VAE is the ELBO, which serves as the test statistic for detecting the presence of the jammer. The following sections will examine each block of the scheme in turn.

5.3 Pre-Processing at the Base Station

Let us consider the vector of received symbols obtained from (2.22), $\mathbf{y}_{:,k}^{(i)}$, and let us assume a specific sensing direction such that $\theta_{\mathrm{R}}^{(i)} = \theta_{\mathrm{T}}^{(i)}$. Spatial

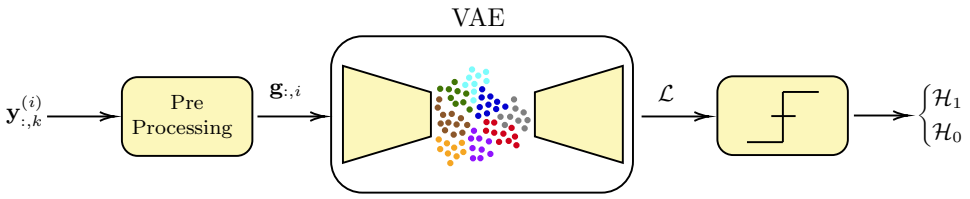

Figure 5.1: Jamming detection scheme with VAE: an illustration of the decision-making.

combining is then performed using the receiving beamforming vector as

$$\mathbf{w}_{\mathrm{R}}^{(i)} = \mathbf{a}_{\mathrm{R}}^{\mathsf{H}}(\theta_{\mathrm{R}}^{(i)}) = \left[1, e^{-j\pi \sin(\theta_{\mathrm{R}}^{(i)})}, \ldots, e^{-j\pi(N_{\mathrm{R}}-1)\sin(\theta_{\mathrm{R}}^{(i)})}\right].$$

This results in the formation of a grid of received symbols, where each element $y_k^{(i)}$ is obtained by taking the inner product between the receiving beamforming vector $\mathbf{w}_{\mathrm{R}}^{(i)}$ and the vector of the symbols received at each antenna $\mathbf{y}_{:,k}^{(i)}$, i.e., $y_k^{(i)} = \mathbf{w}_{\mathrm{R}}^{(i)}\mathbf{y}_{:,k}^{(i)}$. Then, reciprocal filtering is performed, which consists of an element-wise division between the received and the transmitted grids to remove the dependence on the transmitted symbols, yielding $g_k^{(i)} = y_k^{(i)}/x_k^{(i)}$. Considering the ith observation, we have

$$g_k^{(i)} = \mathbf{w}_{\mathrm{R}}^{(i)}\mathbf{H}_k^{(i)}\mathbf{w}_{\mathrm{T}}^{(i)} + \mathbf{w}_{\mathrm{R}}^{(i)}\tilde{\mathbf{H}}_k^{(i)}\mathbf{w}_{\mathrm{J}}^{(i)} e^{-j2\pi k\Delta f \tau_{\mathrm{f}}^{(i)}} + \frac{\mathbf{w}_{\mathrm{R}}^{(i)}\boldsymbol{\zeta}_{:,k}^{(i)}}{x_k^{(i)}} + \frac{\mathbf{w}_{\mathrm{R}}^{(i)}\mathbf{n}_{:,k}^{(i)}}{x_k^{(i)}} \quad (5.1)$$

where the second term is the signal injected by the jammer into the BS receiver to deceive sensing. Although the jammer is capable of reproducing the BS sensing signal, there are notable differences between the first and second term in (5.1). Firstly, distinct power levels are evident as the jammer transmits signals with an EIRP $P_{\mathrm{J}}G_{\mathrm{J}}$, which is absent in the echo signal from the target. Additionally, the channel between the BS and the jammer does not include a convolution of two channel impulse responses due to the absence of backscatter. Finally, for the sake of jamming detection, the real and imaginary parts of $g_k^{(i)}$ are split and arranged in a matrix $\mathbf{G} \in \mathbb{C}^{2N_{\mathrm{B}} \times N_{\mathrm{S}}}$,

whose ith column is

$$\mathbf{g}_{:,i} = \left[\Re\{g_0^{(i)}\}, \ldots, \Re\{g_{N_\mathrm{B}}^{(i)}\}, \Im\{g_0^{(i)}\}, \ldots, \Im\{g_{N_\mathrm{B}}^{(i)}\}\right]^\mathsf{T}.$$

5.4 Variational Autoencoder

5.4.1 VAE for Anomaly Detection

VAEs represent a class of generative latent variable models that encode input data into a latent space and subsequently decode it back to the original space. A key characteristic of VAEs is their imposition of a specific distribution, typically Gaussian, on the latent space, as introduced in the foundational work by Kingma and Welling [88]. VAEs fall within the domain of stochastic VI methods, utilizing gradient-based optimization to maximize the ELBO. The reparameterization trick proposed in [88] facilitates the integration of VI into an autoencoder framework, enabling the ELBO maximization through conventional back-propagation techniques.

VAEs have demonstrated particular efficacy in anomaly detection (AD) due to their capacity to learn the underlying distribution of normal data. During the AD process, VAEs are trained exclusively on normal data, developing a robust ability to accurately reconstruct these data points. When presented with an anomalous data point, the VAE's decoder produces an output that diverges significantly from the expected, as the anomalous data fails to align with the learned distribution. By defining an appropriate threshold, VAEs can effectively identify and flag outliers, making them a powerful tool for anomaly detection.

AD methods leveraging VAEs have been explored in various studies. For instance, [89] introduces an AD approach based on the reconstruction probability derived from a VAE. It is crucial to distinguish between the reconstruction error in traditional autoencoder architectures and the reconstruction probability in VAEs. As depicted in Fig. 5.2, the VAE decoder generates a probability density function that represents the likelihood of the input data, conditioned on the latent space under the trained generative model,

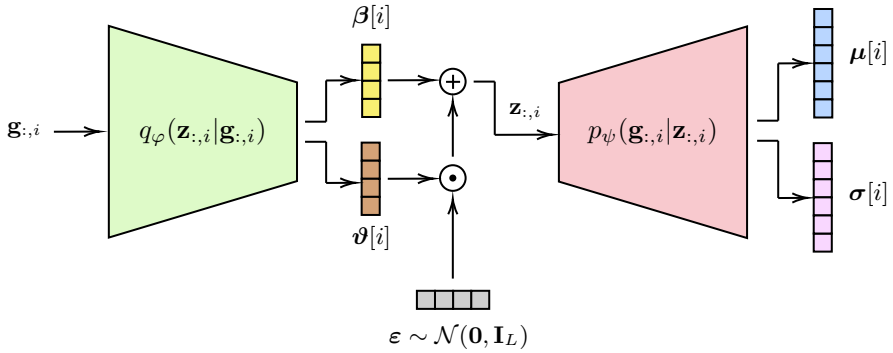

Figure 5.2: Schematic illustration of the VAE. The latent variable is obtained using the reparameterization trick $\mathbf{z}_{:,i} = \boldsymbol{\beta}[i] + \boldsymbol{\vartheta}[i] \odot \boldsymbol{\varepsilon}$.

contrasting with the deterministic mappings found in conventional autoencoders. The superiority of VAEs over autoencoder-based AD algorithms is demonstrated in [89].

Further applications of VAEs in AD are seen in various contexts. In [90], an unsupervised AD algorithm based on VAEs is employed to monitor key performance indicators in web applications. A novel combination of context encoders (a specialized form of denoising autoencoder) and VAEs for anomaly detection in medical images is presented in [91]. Additionally, [92] demonstrates the use of VAEs as feature extractors, capitalizing on the latent space's ability to encapsulate essential information from the input dataset, which is then utilized by traditional algorithms to perform AD on the extracted features.

5.4.2 Definition

We begin our analysis by observing that the system model in (5.1), in the absence of a jammer (i.e., when the second term is zero), can be interpreted as a latent model for the generation of $g_k^{(i)}$. Our initial objective is to learn the latent space generated by the system under no-jammer conditions by means of a variational autoencoder. The goal of VAE is to provide a good approximation for the posterior distribution $p_{\boldsymbol{\psi}}(\mathbf{Z}|\mathbf{G})$ of the latent variables $\mathbf{Z} = \{\mathbf{z}_{:,i}\}_{i=1}^{N_S}$ given the observed data $\mathbf{G}$ and with parameters $\boldsymbol{\psi}$ [93]. Let

us define L as the dimension of the latent variable $\mathbf{z}_{:,i} \in \mathbb{R}^{L\times 1}$. Considering the independence between the observations in $\mathbf{G}$, such distribution can be expressed as $p_{\boldsymbol{\psi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})$. Since the posterior distribution cannot be directly computed due to the intractability of the marginal likelihood

$$p_{\boldsymbol{\psi}}(\mathbf{g}_{:,i}) = \int_{\mathbf{z}_{:,i}} p_{\boldsymbol{\psi}}(\mathbf{g}_{:,i}, \mathbf{z}_{:,i}) d\mathbf{z}_{:,i}, \tag{5.2}$$

VI provides an approximate distribution $q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})$ with parameters $\boldsymbol{\varphi}$. In particular, the best approximation can be computed by minimizing the following Kullback-Leibler divergence

$$D_{\mathrm{KL}}(q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})||p_{\boldsymbol{\psi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})) = -\mathbb{E}_{q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})}\left[\ln \frac{p_{\boldsymbol{\psi}}(\mathbf{g}_{:,i}, \mathbf{z}_{:,i})}{q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})}\right] + \ln p_{\boldsymbol{\psi}}(\mathbf{g}_{:,i}) \tag{5.3}$$

or, equivalently, by maximizing the ELBO

$$\mathcal{L}(\boldsymbol{\psi}, \boldsymbol{\varphi}, \mathbf{g}_{:,i}) = \mathbb{E}_{q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})}\left[\ln \frac{p_{\boldsymbol{\psi}}(\mathbf{g}_{:,i}, \mathbf{z}_{:,i})}{q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})}\right]. \tag{5.4}$$

Traditional mean-field VI methods factorize $q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})$ to derive a closed-form solution for the ELBO [94]. However, these methods suffer from computational inefficiency as they require iteration through the entire dataset at each algorithmic step [95]. For this reason, VAE provides a stochastic VI solution aiming to maximize the $\mathcal{L}(\boldsymbol{\psi}, \boldsymbol{\varphi}, \mathbf{g}_{:,i})$ using gradient-based optimization techniques.

Let us now assume the following prior distributions

$$p_{\boldsymbol{\psi}}(\mathbf{g}_{:,i}|\mathbf{z}_{:,i}) = \mathcal{N}(\boldsymbol{\mu}[i], \boldsymbol{\sigma}^2[i]\mathbf{I}_{2K}), \tag{5.5}$$

$$p(\mathbf{z}_{:,i}) = \mathcal{N}(\mathbf{0}, \mathbf{I}_L), \tag{5.6}$$

$$q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i}) = \mathcal{N}(\boldsymbol{\beta}[i], \boldsymbol{\vartheta}^2[i]\mathbf{I}_L). \tag{5.7}$$

The choice of Gaussian priors for the latent space has many benefits: (i) the Gaussian distribution is mathematically convenient due to its properties, such as admitting a closed-form expression for the Kullback-Leibler diver-

gence, which is essential for the VAE's optimization process; (ii) thanks to the central limit theorem, Gaussian priors are a natural and generalizable choice for modeling the latent space of diverse datasets; (iii) empirically, Gaussian priors have been shown to produce smooth and continuous latent spaces, which are desirable for generative tasks [88]. After proper manipulations, the ELBO can be written as

$$\mathcal{L}(\boldsymbol{\psi}, \boldsymbol{\varphi}, \mathbf{g}_{:,i}) = -D_{\mathrm{KL}}\left(q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})||p(\mathbf{z}_{:,i})\right) + \mathbb{E}_{q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})}\left[\ln p_{\boldsymbol{\psi}}(\mathbf{g}_{:,i}|\mathbf{z}_{:,i})\right]. \tag{5.8}$$

Adopting the reparameterization trick proposed in [88], considering the prior distributions in (5.5), (5.6), and (5.7), it is possible to obtain a differentiable formulation for the ELBO, i.e.,

$$\begin{aligned}\mathcal{L}(\boldsymbol{\psi}, \boldsymbol{\varphi}, \mathbf{g}_{:,i}) = \frac{1}{2}\sum_{l=1}^{L}\left(1 + \ln \vartheta_l^2[i] - \beta_l^2[i] - \vartheta_l^2[i]\right) \\ \underbrace{-\frac{1}{2}\sum_{k=1}^{2N_{\mathrm{B}}}\left(\ln 2\pi + \ln \sigma_k^2[i] + \frac{(g_{k,i} - \mu_k[i])^2}{\sigma_k^2[i]}\right)}_{V}\end{aligned} \tag{5.9}$$

where $V = -\mathbb{E}_{q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})}\left[\ln p_{\boldsymbol{\psi}}(\mathbf{g}_{:,i}|\mathbf{z}_{:,i})\right]$ is the reconstruction probability that will be used for jamming detection [89].

Fig. 5.2 encloses a schematic representation of a VAE. The function $q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})$ serves as a probabilistic encoder that, given an input $\mathbf{g}_{:,i}$, generates a distribution over the possible values of $\mathbf{z}_{:,i}$ from which $\mathbf{g}_{:,i}$ could have been produced. Similarly, $p_{\boldsymbol{\psi}}(\mathbf{g}_{:,i}|\mathbf{z}_{:,i})$ functions as a probabilistic decoder, producing a distribution over the possible values of $\mathbf{g}_{:,i}$ given $\mathbf{z}_{:,i}$. Thus, $\boldsymbol{\mu}[i]$, $\boldsymbol{\sigma}[i]$, $\boldsymbol{\beta}[i]$, and $\boldsymbol{\vartheta}[i]$ are the outputs of the encoder and decoder neural networks, whose weights are denoted by $\boldsymbol{\psi}$ and $\boldsymbol{\varphi}$, respectively.

5.4.3 Detector

The VAE, trained on echoes captured in absence of a jammer, seeks to learn the latent variables that better represent the channel in presence of a target.

Thus, after the training, if the VAE is fed with a vector $\mathbf{g}_{:,i}$ corresponding to the manipulated received signal in presence of a jammer, it provides an anomalous value for $\mathcal{L}(\boldsymbol{\psi}, \boldsymbol{\varphi}, \mathbf{g}_{:,i})$. Specifically, when the jammer is present results in significantly high values of the reconstruction probability V. Therefore, based on such considerations, we propose an anomaly detector that employs as metric the reconstruction probability, i.e.,

$$V \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \xi. \tag{5.10}$$

Hypothesis $\mathcal{H}_1$ corresponds to the presence of a jammer, while the null hypothesis, $\mathcal{H}_0$, corresponds to its absence. The thresholds ξ is obtained by setting the false alarm probability $p_{\text{FA}} = (V > \xi | \mathcal{H}_0)$, where the null distribution is calculated via histogram-based probability density function estimation.

Chapter 6

Cooperative Wideband Spectrum Sensing

Cooperative WSS represents a technique employed in cognitive radio networks for the purpose of detecting and identifying available frequency bands across a wide range of the spectrum. In this approach, SUs, also referred to as sensors in this thesis, collaborate to scan the spectrum, sharing their local sensing information to enhance the accuracy and reliability of detecting unoccupied bands. WSS serves as a facilitator for spectrum sharing, enabling more efficient utilisation of the radio frequency spectrum by allowing SUs to dynamically access underutilised bands without causing interference to licensed users.

6.1 Existing Works

In the last decade, extensive research has been conducted on the problem of spectrum sensing [96–98]. Early works, such as [99], proposed several classical machine learning-based methods for cooperative narrowband spectrum sensing, including K-means clustering and Gaussian mixture models (GMMs). A significant development in cooperative strategies was presented in [100], where a cooperative energy detection leveraging heterogeneous sensors was proposed. The proposed method evaluates basic mass assignment (BMA)

values for each SU based on the likelihood functions of the received signal's energy. Each SU sends its BMA values to the FC, which combines them using the Dempster fusion rule. It is shown that the method reduces to the optimal likelihood ratio fusion rule in the absence of noise. While the method accounts for noise uncertainty in each sensor, it assumes knowledge of the nominal SNR for each sensor to determine the discount rate. Furthermore, numerical results reveal that even a small degree of noise uncertainty can significantly degrade detection performance.

Subsequent studies introduced high-complexity sub-Nyquist techniques for WSS, achieving satisfactory detection performance in high-SNR regimes, as shown in [101–105]. These techniques employ sophisticated signal reconstruction and spectrum analysis algorithms, which are computationally intensive and require advanced digital signal processing, leading to increased system complexity and higher power consumption. Among these sub-Nyquist approaches, compressive sensing stands out by leveraging signal sparsity to accurately reconstruct signals from fewer samples. Here, signal sparsity is intended as a wideband signal with only a few non-zero samples, whether in frequency or time-frequency domain. For instance, compressive sensing over MIMO channels, as explored in [106], used delay embeddings of received signals sampled by a low-rate analog to digital converter (ADC) and Candecomp/Parafac decomposition to extract carrier frequencies and power spectra. However, this approach needed many samples and was only effective in high-SNR conditions.

Recent advancements have leveraged AI techniques to enhance spectrum sensing capabilities. In [107], a computationally lightweight detector based on deep convolution separable methods was adopted, employing convolutional neural network (CNN) to process spectrograms and merge outcomes using non-maximum suppression fusion rules. Additionally, [108] introduced a federated learning (FL)-based centralized spectrum sensing algorithm, where sensors update a local ML model and share model coefficients with a central node for integration. Although federated learning reduces the amount of raw data exchanged between sensors by sharing model parameters, the overall communication overhead can still be substantial. This overhead is

particularly significant in large-scale networks with many sensors. Parallel processing techniques using CNNs were discussed in [109] and [110], where received I/Q samples were processed concurrently, and spectrum sensing was approached as a classification problem. Despite improvements, implementing Parallel CNNs still involves considerable computational complexity due to processing I/Q samples by two parallel networks. Similarly, [23] introduced DeepSense, a deep neural network (DNN)-based solution implemented on an field-programmable gate array (FPGA) to perform fast WSS using CNN for multi-label classification tasks. In contrast, an unsupervised approach utilizing deep clustering for cooperative narrowband spectrum sensing was proposed in [111]. This method employed a sparse autoencoder to learn hidden features from locally computed energy levels. However, it did not account for noise power variability among SUs and required prior identification of clusters corresponding to noise and PU signals.

6.2 Problem Statement

We propose a cooperative WSS framework that utilizes a frequency domain description of signals received by sensors to estimate the occupancy state of multiple portions of a large bandwidth, termed frequency bins. This framework operates independently of the sparsity of the received signals and does not require prior knowledge of the sensors' noise power. In particular, we recast the cooperative WSS problem within a Bayesian factor analysis framework and introduce a VI strategy to approximate its posterior distribution. The occupancy state of each frequency bin is then estimated through binary hypothesis testing, employing the ELBO from the variational Bayes factor analysis (VBFA) as the test statistic.

The full processing pipeline of the VBFA is illustrated in Fig. 6.1. Initially, during the pre-processing stage, the vector of frequency bins $\mathbf{y}_{j,:}^{(i)}$ is separated into its real and imaginary components. Subsequently, the coordinate ascent variational inference (CAVI) algorithm is employed to identify the optimal approximate posterior distribution by maximizing the ELBO. The ELBO is then utilized as the test statistic for spectrum hole detection. The

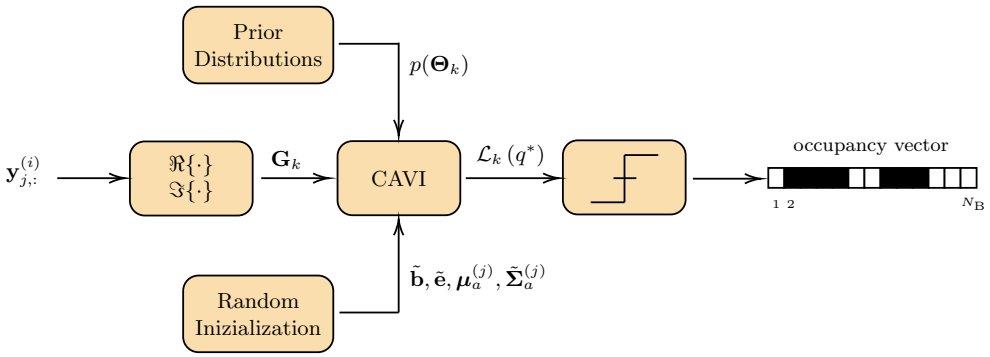

Figure 6.1: VBFA scheme for cooperative WSS.

subsequent sections will provide a detailed examination of each component of this process.

6.3 Variational Bayes Factor Analysis

6.3.1 Pre-Processing

Let us define $\mathbf{x}_{:,k}^{(i)} \in \mathbb{C}^{N_{\mathrm{T},k}\times 1}$ as the vector of frequency samples transmitted by the PUs in the kth frequency bin at the ith observation, $N_{\mathrm{T},k}$ is the number of PUs transmitters in the kth frequency bin, and $\mathbf{H}_k \in \mathbb{C}^{N_\mathrm{R}\times N_{\mathrm{T},k}}$ is the matrix of channel coefficients in frequency domain. The entries of $\mathbf{H}_k$ take into account frequency-selective multipath fading, which we assume flat within a single frequency bin and constant along the observations.[1] We then express $\mathbf{s}_{:,k}^{(i)}$ as

$$\mathbf{s}_{:,k}^{(i)} = \mathbf{H}_k \mathbf{x}_{:,k}^{(i)} \tag{6.1}$$

and the received signals at the ith observation in the k frequency bin as

$$\mathbf{y}_{:,k}^{(i)} = \mathbf{s}_{:,k}^{(i)} + \mathbf{n}_{:,k}^{(i)}. \tag{6.2}$$

[1]It is assumed that the time to collect all N_S observations is less than the channel coherence time.

Let us now split real and imaginary parts of $\mathbf{y}_{:,k}^{(i)}$ as

$$\tilde{\mathbf{g}}_{:,k}^{(i)} = \begin{bmatrix} \Re\{\mathbf{y}_{:,k}^{(i)}\} \\ \Im\{\mathbf{y}_{:,k}^{(i)}\} \end{bmatrix} = \mathbf{A}_k \mathbf{z}_{:,k}^{(i)} + \mathbf{w}_{:,k}^{(i)} \tag{6.3}$$

where $\tilde{\mathbf{g}}_{:,k}^{(i)} \in \mathbb{R}^{2N_\mathrm{R}\times 1}$, $\mathbf{z}_{:,k}^{(i)} = \left[\Re\{\mathbf{x}_{:,k}^{(i)}\}, \Im\{\mathbf{x}_{:,k}^{(i)}\}\right]^\mathsf{T} \in \mathbb{R}^{2N_{\mathrm{T},k}\times 1}$, $\mathbf{w}_{:,k}^{(i)} = \left[\Re\{\mathbf{n}_{:,k}^{(i)}\}, \Im\{\mathbf{n}_{:,k}^{(i)}\}\right]^\mathsf{T} \in \mathbb{R}^{2N_\mathrm{R}\times 1}$, $\mathbf{A}_k \in \mathbb{R}^{2N_\mathrm{R}\times 2N_{\mathrm{T},k}}$ is the matrix consisting of the real and imaginary parts of the entries of $\mathbf{H}_k$, and $\mathbf{w}_{:,k}^{(i)} \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_w)$ where $\mathbf{\Sigma}_w = \frac{1}{2}\mathrm{diag}(\sigma_1^2, \ldots, \sigma_{N_\mathrm{R}}^2, \sigma_1^2, \ldots, \sigma_{N_\mathrm{R}}^2)$.

6.3.2 Bayesian Factor Analysis

Factor analysis is a statistical technique used to identify underlying relationships or patterns among a set of observed data. By analyzing the correlations between observed variables, it aims to reduce data dimensionality by grouping related variables into a smaller number of factors. These factors represent latent constructs that explain the observed correlations [112].

The received signal structure (6.3) can be interpreted as a factor analysis model where $\mathbf{z}_{:,k}^{(i)}$ is a $2N_{\mathrm{T},k}$-dimensional vector of latent variables, and $\tilde{\mathbf{g}}_{:,k}^{(i)}$ are the observations.[2] Let us define the observations matrix in the kth bin as $\mathbf{G}_k = [\mathbf{g}_{:,i}]_{i=1}^{N_\mathrm{S}}$, where $\mathbf{g}_{:,i} = \tilde{\mathbf{g}}_{:,k}^{(i)}$. In light of this interpretation, we aim to estimate the latent variable dimension in bin k, $2\hat{N}_{\mathrm{T},k}$, which tells us if a PU is transmitting, i.e., if $\hat{N}_{\mathrm{T},k} = 0$, no PU is transmitting in bin k, if $\hat{N}_{\mathrm{T},k} > 0$ then one or more PUs are occupying the frequency bin. We now introduce the Bayesian factor analysis and derive a binary hypothesis test that can be used to detect the presence of one or more PU signals in a frequency bin.

Prior Distributions

Bayesian factor analysis requires defining the prior distributions for all the parameters of the model. Let us define the set of unknown parameters as $\mathbf{\Theta}_k = \{\mathbf{Z}_k, \mathbf{\Psi}_k, \mathbf{A}_k, \boldsymbol{\alpha}_k\}$, where $\mathbf{Z}_k \in \mathbb{R}^{N_k \times N_\mathrm{S}}$ is the matrix of factors (i.e., the

[2] If all the sensors experience the same noise power, i.e., $\mathbf{\Sigma}_w = \sigma^2\mathbf{I}$, then (6.3) is a probabilistic principal component analysis (PCA) model [113].

PU signals if present), N_k is the unknown latent dimension that is initialized by the algorithm, $\mathbf{\Psi}_k = \mathbf{\Sigma}_{\boldsymbol{w_k}}^{-1}$ is the noise precision matrix, and $\boldsymbol{\alpha}_k$ is the vector of hyperparameters that control the inverse variance of the columns of $\mathbf{A}_k$ [113]. Since factor analysis is applied independently to each frequency bin, we drop the subscripts $:, k$ and k from the observations and latent variable matrices in the rest of the chapter. We now list the priors adopted for each parameter according to [114, 115].

The prior of $\mathbf{Z}$ is

$$p(\mathbf{Z}) = \prod_{i=1}^{N_\mathrm{S}} p(\mathbf{z}_{:,i}) \tag{6.4}$$

where $p(\mathbf{z}_{:,i}) = \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$. The prior of $\mathbf{\Psi}$ is

$$p(\mathbf{\Psi}) = \prod_{j=1}^{2N_\mathrm{R}} p(\boldsymbol{\psi}_{j,j}) \tag{6.5}$$

where $p(\boldsymbol{\psi}_{j,j}) = \mathcal{G}(v, e_j)$, and $\mathcal{G}(v, e_j)$ is the gamma distribution with shape parameter v and inverse scale parameter e_j.

Since we are interested in the effective dimensionality of the latent space, we introduce a hierarchical prior $p(\mathbf{A}|\boldsymbol{\alpha})$ over the matrix $\mathbf{A}$, governed by a N-dimensional vector of hyperparameters $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_N]$. The prior $p(\mathbf{A}|\boldsymbol{\alpha})$ is

$$p(\mathbf{A}|\boldsymbol{\alpha}) = \prod_{d=1}^{N} p(\mathbf{a}_{:,d}|\alpha_d) \tag{6.6}$$

where $p(\mathbf{a}_{:,d}) = \mathcal{N}(\mathbf{0}, \frac{1}{\alpha_d}\mathbf{I}_{2N_\mathrm{R}})$. With the hierarchical prior, $\mathbf{a}_{:,d}$ will tend to be small if α_d has a posterior distribution concentrated at large values, thus that direction in latent space will be switched off. Finally, the prior for $\boldsymbol{\alpha}$ is

$$p(\boldsymbol{\alpha}) = \prod_{d=1}^{N} p(\alpha_d) \tag{6.7}$$

where $p(\alpha_d) = \mathcal{G}(a, b_d)$ with a and b_d representing the shape and inverse scale

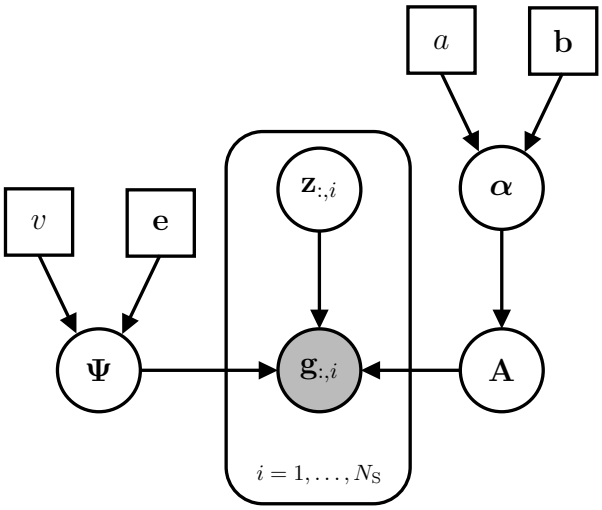

Figure 6.2: Graphical representation for Bayesian factor analysis. The node with a gray background represents sensors observations. The box is a compact notion to denote that we have N_{S} nodes for each variable inside it.

parameters, respectively. In Fig. 6.2, a representation of Bayesian factor analysis as a probabilistic graphical model is shown. Here, the estimation of the latent dimension is converted into a Bayesian inference problem, where the objective is the evaluation of the posterior distribution

$$p(\boldsymbol{\Theta}|\mathbf{G}) = \frac{p(\mathbf{G}, \boldsymbol{\Theta})}{p(\mathbf{G})}. \tag{6.8}$$

Knowing $p(\boldsymbol{\Theta}|\mathbf{G})$ means estimating the latent space dimension. However, the posterior cannot be directly computed due to the intractability of the marginal distribution

$$p(\mathbf{G}) = \int_{\boldsymbol{\Theta}} p(\mathbf{G}, \boldsymbol{\Theta}) d\boldsymbol{\Theta} \tag{6.9}$$

where

$$p(\mathbf{G}, \boldsymbol{\Theta}) = p(\mathbf{G}|\mathbf{Z}, \boldsymbol{\Psi}, \mathbf{A}, \boldsymbol{\alpha}) p(\mathbf{Z}) p(\boldsymbol{\Psi}) p(\mathbf{A}|\boldsymbol{\alpha}) p(\boldsymbol{\alpha}). \tag{6.10}$$

Based on the previous consideration, the following subsection approximates the true posterior distribution using a variational Bayes approach.

6.3.3 Mean-Field Variational Inference

In Chapter 5, a stochastic VI approach was employed to train a VAE with the objective of maximizing the ELBO. However, in the present scenario, the lack of a large dataset containing diverse channel realizations hinders the effective training of a DNN architecture. Instead, our focus here is on detecting spectrum holes given N_{S} independent observations of the received signals, assuming the channel $\mathbf{H}_k$ remains constant across these observations. Consequently, a mean-field VI approach is adopted for this task. The key idea of the mean-field approach is to simplify the problem by assuming that the posterior distribution can be factorized into independent distributions over subsets of the latent variables. This assumption reduces the complexity of the distribution, allowing for a tractable approximation [94].[3]

Let us consider a family of distributions, $q(\boldsymbol{\Theta})$, from which we seek the one that best approximates the posterior distribution $p(\boldsymbol{\Theta}|\mathbf{G})$. We now restrict the family of distributions by partitioning the elements of $\boldsymbol{\Theta}$ into disjoint groups and assuming that the q distribution factorizes with respect to these groups as

$$q(\boldsymbol{\Theta}) = \prod_{m=1}^{M} q_m(\boldsymbol{\theta}_m) = q(\mathbf{Z})q(\boldsymbol{\Psi})q(\mathbf{A})q(\boldsymbol{\alpha}) \tag{6.11}$$

where $q_m(\boldsymbol{\theta}_m)$ is the approximate distribution for the generic latent variable $\boldsymbol{\theta}_m$, and in our case $M = 4$.

Proposition 1. *Considering the sets of observations* $\mathbf{G}$ *and latent variables* $\boldsymbol{\Theta}$*, and a family of distributions* $q(\boldsymbol{\Theta})$ *that can be factorized as in* (6.11)*, the distribution that better approximates the posterior of* $\boldsymbol{\theta}_m$*,* $q_m^*(\boldsymbol{\theta}_m)$*, is*

$$\ln q_m^*(\boldsymbol{\theta}_m) = \mathbb{E}_{l\neq m}\left[\ln p(\mathbf{G}, \boldsymbol{\Theta})\right] + c_1 \tag{6.12}$$

where $\mathbb{E}_{l\neq m}[\cdot]$ *denotes the expectation with respect to the distributions* q *over all the variables* $\boldsymbol{\theta}_l$ *for* $l \neq m$*,* c_1 *is a constant, and* $\ln p(\mathbf{G}, \boldsymbol{\Theta})$ *is the natural logarithm of* (6.10)*, which is written as*

[3] This factorized form of variational inference corresponds to an approximation framework developed in physics called mean field theory [116].

$$\begin{aligned}\ln p(\mathbf{G},\boldsymbol{\Theta}) &= \sum_{i=1}^{N_\mathrm{S}} \ln p(\mathbf{g}_{:,i}|\mathbf{z}_{:,i},\boldsymbol{\Psi},\mathbf{A}) + \sum_{i=1}^{N_\mathrm{S}} \ln p(\mathbf{z}_{:,i}) + \sum_{j=1}^{2N_\mathrm{R}} p(\psi_{j,j}) \\ &\quad + \sum_{d=1}^{N} \ln p(\mathbf{a}_{:,d}) + \sum_{d=1}^{N} \ln p(\alpha_d) \\ &= \frac{N_\mathrm{S}}{2} \ln\det(\boldsymbol{\Psi}) - \frac{1}{2}\sum_{i=1}^{N_\mathrm{S}} (\mathbf{g}_{:,i} - \mathbf{A}\mathbf{z}_{:,i})^\mathsf{T} \boldsymbol{\Psi} (\mathbf{g}_{:,i} - \mathbf{A}\mathbf{z}_{:,i}) - \frac{1}{2}\sum_{i=1}^{N_\mathrm{S}} \mathbf{z}_{:,i}^\mathsf{T}\mathbf{z}_{:,i} \\ &\quad + \sum_{j=1}^{2N_\mathrm{R}} (v-1)\ln\psi_{j,j} - \sum_{j=1}^{2N_\mathrm{R}} e_j\psi_{j,j} + N_\mathrm{R}\sum_{d=1}^{N}\ln\alpha_d \\ &\quad - \frac{1}{2}\sum_{d=1}^{N}\alpha_d \mathbf{a}_{:,d}^\mathsf{T}\mathbf{a}_{:,d} + \sum_{d=1}^{N}(a-1)\ln\alpha_d - \sum_{d=1}^{N} b_d\alpha_d + c_2. \end{aligned} \tag{6.13}$$

with c_2 also being a constant.

Proof. It has been shown that the Kullback-Leibler divergence between $q(\boldsymbol{\Theta})$ and $p(\boldsymbol{\Theta}|\mathbf{G})$ can be expressed as

$$\begin{aligned} D_\mathrm{KL}(q(\boldsymbol{\Theta})||p(\boldsymbol{\Theta}|\mathbf{G})) &= -\mathbb{E}_q\left[\ln\frac{p(\mathbf{G},\boldsymbol{\Theta})}{q(\boldsymbol{\Theta})}\right] + \ln p(\mathbf{G}) \\ &= -\mathcal{L}(q) + \ln p(\mathbf{G}) \end{aligned} \tag{6.14}$$

where $\mathcal{L}(q)$ is the ELBO, and $\mathbb{E}_q[\cdot]$ is the expectation over the distribution $q(\boldsymbol{\Theta})$ [93, 95]. The optimal approximation for the posterior distribution is found by seeking for the distribution $q^*(\boldsymbol{\Theta})$ that minimizes the Kullback-Leibler divergence

$$q^*(\boldsymbol{\Theta}) = \arg\min_q D_\mathrm{KL}(q(\boldsymbol{\Theta})||p(\boldsymbol{\Theta}|\mathbf{G})). \tag{6.15}$$

From (6.14), minimizing $D_\mathrm{KL}(q(\boldsymbol{\Theta})||q(\boldsymbol{\Theta}|\mathbf{G}))$ translates into maximizing the ELBO, i.e.,

$$q^*(\boldsymbol{\Theta}) = \arg\max_q \mathcal{L}(q). \tag{6.16}$$

According to the CAVI method proposed in [94], the distribution that max-

imizes $\mathcal{L}(q)$ is given by (6.12). □

The set of equations given by (6.12) for $m = 1, ..., M$ represent a set of consistency conditions for the maximum of the ELBO subject to the factorization constraint. However, they do not represent an explicit solution because the expression on the right-hand side of (6.12) for the optimum $q_m^*(\boldsymbol{\theta}_m)$ depends on expectations computed with respect to the other factors $q_l^*(\boldsymbol{\theta}_l)$ for $l \neq m$. We will therefore seek a consistent solution by first initializing all of the factors $q_l^*(\boldsymbol{\theta}_l)$ appropriately and then cycling through the factors and replacing each in turn with a revised estimate given by the right-hand side of (6.12) evaluated using the current estimates for all of the other factors. In particular the equations given by (6.12) for $m = 1, \ldots, M$ are iterated until convergence of the ELBO. Convergence is guaranteed because bound is convex with respect to each of the factors [94].

The approximate distributions of the latent variables can be computed in closed-form by substituting (6.13) in (6.12). For the columns of $\mathbf{Z}$ we obtain

$$q^*(\mathbf{z}_{:,i}) = \mathcal{N}(\boldsymbol{\mu}_z^{(i)}, \tilde{\boldsymbol{\Sigma}}_z) \tag{6.17}$$

where

$$\begin{aligned} \boldsymbol{\mu}_z^{(i)} &= \tilde{\boldsymbol{\Sigma}}_z \mathbb{E}[\mathbf{A}^\mathsf{T}] \mathbb{E}[\boldsymbol{\Psi}] \mathbf{g}_{:,i} \\ \tilde{\boldsymbol{\Sigma}}_z &= \left(\mathbf{I}_N + \mathbb{E}[\mathbf{A}^\mathsf{T} \boldsymbol{\Psi} \mathbf{A}]\right)^{-1}. \end{aligned}$$

Then, for the diagonal elements of $\boldsymbol{\Psi}$ we have

$$q^*(\psi_{j,j}) = \mathcal{G}(\tilde{v}, \tilde{e}_j) \tag{6.18}$$

where

$$\tilde{v} = v + \frac{N_\mathrm{S}}{2} \tag{6.19}$$

$$\tilde{e}_j = e_j + \frac{1}{2} \sum_{i=1}^{N_\mathrm{S}} \mathbb{E}\left[(g_{j,i} - \mathbf{a}_{j,:} \mathbf{z}_{:,i})^2\right]. \tag{6.20}$$

The distribution of the rows of $\mathbf{A}$ is

$$q^*(\mathbf{a}_{j,:}) = \mathcal{N}(\boldsymbol{\mu}_a^{(j)}, \tilde{\boldsymbol{\Sigma}}_a^{(j)}) \tag{6.21}$$

where

$$\begin{aligned}
\boldsymbol{\mu}_a^{(j)} &= \tilde{\boldsymbol{\Sigma}}_a^{(j)} \mathbb{E}[\psi_{j,j}] \sum_{i=1}^{N_\mathrm{S}} g_{j,i} \mathbb{E}[\mathbf{z}_{:,i}] \\
\tilde{\boldsymbol{\Sigma}}_a^{(j)} &= \left(\mathbb{E}[\psi_{j,j}] \sum_{i=1}^{N_\mathrm{S}} \mathbb{E}[\mathbf{z}_{:,i} \mathbf{z}_{:,i}^\mathsf{T}] + \mathbb{E}[\mathrm{diag}(\boldsymbol{\alpha})] \right)^{-1}.
\end{aligned}$$

Finally, for the elements of $\boldsymbol{\alpha}$ we have

$$q^*(\alpha_d) = \mathcal{G}(\tilde{a}, \tilde{b}_d) \tag{6.22}$$

where

$$\tilde{a} = a + N_\mathrm{R} \tag{6.23}$$

$$\tilde{b}_d = b_d + \frac{\mathbb{E}[\mathbf{a}_{:,d}^\mathsf{T} \mathbf{a}_{:,d}]}{2}. \tag{6.24}$$

In the previous expressions, $i = 1, \ldots, N_\mathrm{S}$, $j = 1, \ldots, 2N_\mathrm{R}$, and $d = 1, \ldots, N$. The iteration steps performed by the CAVI are shown in Algorithm 5.

6.3.4 ELBO

We now derive a closed-form expression for the maximum ELBO, $\mathcal{L}(q^*)$, obtained using CAVI algorithm. The resulting expression is then used as a metric to perform spectrum sensing via binary hypothesis testing.

Proposition 2. *The maximum ELBO in* (6.16)*,* $\mathcal{L}(q^*)$*, admits the closed-form expression*

$$\mathcal{L}(q^*) = \underbrace{\frac{N_\mathrm{S}}{2}\ln\det\left(\tilde{\boldsymbol{\Sigma}}_z\right) + \frac{N_\mathrm{S}}{2}\mathrm{tr}\left(\mathbf{I}_N - \tilde{\boldsymbol{\Sigma}}_z\right) - \frac{1}{2}\sum_{i=1}^{N_\mathrm{S}}\mathrm{tr}\left(\boldsymbol{\mu}_z^{(i)}(\boldsymbol{\mu}_z^{(i)})^\mathsf{T}\right)}_{-D_\mathrm{KL}(q(\mathbf{Z})||p(\mathbf{Z}))} + \frac{1}{2}\sum_{j=1}^{2N_\mathrm{R}}\ln\det\left(\tilde{\boldsymbol{\Sigma}}_a^{(j)}\right) - \tilde{a}\sum_{d=1}^{N}\ln\tilde{b}_d - \tilde{v}\sum_{j=1}^{2N_\mathrm{R}}\ln\tilde{e}_j + c_3. \tag{6.25}$$

where c_3 is a constant.

Proof. Manipulating $\mathcal{L}(q)$ from (6.14) we obtain

$$\begin{aligned}\mathcal{L}(q) = {} & \mathbb{E}_{q(\mathbf{Z}),q(\boldsymbol{\Psi}),q(\mathbf{A}),q(\boldsymbol{\alpha})}\left[\ln p\left(\mathbf{G}|\mathbf{Z},\boldsymbol{\Psi},\mathbf{A},\boldsymbol{\alpha}\right)\right] \\ & - D_\mathrm{KL}\left(q(\mathbf{Z})||p(\mathbf{Z})\right) - D_\mathrm{KL}\left(q(\boldsymbol{\Psi})||p(\boldsymbol{\Psi})\right) \\ & - \mathbb{E}_{q(\boldsymbol{\alpha})}\left[D_\mathrm{KL}\left(q(\mathbf{A})||p(\mathbf{A}|\boldsymbol{\alpha})\right)\right] - D_\mathrm{KL}\left(q(\boldsymbol{\alpha})||p(\boldsymbol{\alpha})\right)\end{aligned} \tag{6.26}$$

where the superscript $.^*$ in the distribution $q(\cdot)$ is omitted to lighten the notation. We now compute all the terms in (6.26).

1. Compute $\mathbb{E}_{q(\mathbf{Z}),q(\boldsymbol{\Psi}),q(\mathbf{A}),q(\boldsymbol{\alpha})}\left[\ln p\left(\mathbf{G}|\mathbf{Z},\boldsymbol{\Psi},\mathbf{A},\boldsymbol{\alpha}\right)\right]$

It is easy to see that $p\left(\mathbf{G}|\mathbf{Z},\boldsymbol{\Psi},\mathbf{A},\boldsymbol{\alpha}\right) = \mathcal{N}\left(\mathbf{A}\mathbf{z}_{:,i},\boldsymbol{\Psi}^{-1}\right)$. Considering that

$$(\mathbf{g}_{:,i} - \mathbf{A}\mathbf{z}_{:,i})^\mathsf{T}\boldsymbol{\Psi}(\mathbf{g}_{:,i} - \mathbf{A}\mathbf{z}_{:,i}) = \sum_{j=1}^{2N_\mathrm{R}}(g_{j,i} - \mathbf{a}_{j,:}\mathbf{z}_{:,i})^2\psi_{j,j}$$

we have

$$\begin{aligned}&\mathbb{E}_{q(\mathbf{Z}),q(\boldsymbol{\Psi}),q(\mathbf{A}),q(\boldsymbol{\alpha})}\left[\ln p\left(\mathbf{G}|\mathbf{Z},\boldsymbol{\Psi},\mathbf{A},\boldsymbol{\alpha}\right)\right] = \\ &\frac{N_\mathrm{S}}{2}\sum_{j=1}^{2N_\mathrm{R}}\mathbb{E}[\ln\psi_{j,j}] - N_\mathrm{S}N_\mathrm{R}\ln(2\pi) - \frac{1}{2}\sum_{i=1}^{N_\mathrm{S}}\sum_{j=1}^{2N_\mathrm{R}}\mathbb{E}\left[(g_{j,i} - \mathbf{a}_{j,:}\mathbf{z}_{:,i})^2\right]\mathbb{E}[\psi_{j,j}].\end{aligned} \tag{6.27}$$

2. Compute $-D_\mathrm{KL}\left(q(\mathbf{Z})||p(\mathbf{Z})\right)$

The negative Kullback-Leibler divergence can be expressed as $\mathbb{E}_{q(\mathbf{Z})}[\ln p(\mathbf{Z})] - \mathbb{E}_{q(\mathbf{Z})}[\ln q(\mathbf{Z})]$ where $p(\mathbf{Z})$ is given in (6.4) and $q(\mathbf{Z})$ in (6.17). Then, recalling

that

$$\begin{aligned} \mathbb{E}\left[\mathbf{z}_{:,i}\mathbf{z}_{:,i}^{\mathsf{T}}\right] &= \tilde{\boldsymbol{\Sigma}}_z + \boldsymbol{\mu}_z^{(i)}(\boldsymbol{\mu}_z^{(i)})^{\mathsf{T}} \\ \mathbf{z}_{:,i}^{\mathsf{T}}\left(\mathbf{I}_N - (\tilde{\boldsymbol{\Sigma}}_z)^{-1}\right)\mathbf{z}_{:,i} &= \mathrm{tr}\Big(\mathbf{z}_{:,i}\mathbf{z}_{:,i}^{\mathsf{T}}\left(\mathbf{I}_N - (\tilde{\boldsymbol{\Sigma}}_z)^{-1}\right)\Big) \end{aligned} \tag{6.28}$$

we finally obtain

$$\begin{aligned} &- D_{\mathrm{KL}}\left(q(\mathbf{Z})||p(\mathbf{Z})\right) = \\ &\frac{N_{\mathrm{S}}}{2}\left(\ln\det\left(\tilde{\boldsymbol{\Sigma}}_z\right) + \mathrm{tr}\Big(\mathbf{I}_N - \tilde{\boldsymbol{\Sigma}}_z\Big)\right) - \frac{1}{2}\sum_{i=1}^{N_{\mathrm{S}}}\mathrm{tr}\Big(\boldsymbol{\mu}_z^{(i)}(\boldsymbol{\mu}_z^{(i)})^{\mathsf{T}}\Big)\,. \end{aligned} \tag{6.29}$$

3. Compute $-D_{\mathrm{KL}}\left(q(\boldsymbol{\Psi})||p(\boldsymbol{\Psi})\right)$

The negative Kullback-Leibler divergence is equal to $\mathbb{E}_{q(\boldsymbol{\Psi})}[\ln p(\boldsymbol{\Psi})] - \mathbb{E}_{q(\boldsymbol{\Psi})}[\ln q(\boldsymbol{\Psi})]$ where $p(\boldsymbol{\Psi})$ is given in (6.5) and $q(\boldsymbol{\Psi})$ in (6.18). Substituting (6.19) and (6.20) yields

$$\begin{aligned} &- D_{\mathrm{KL}}\left(q(\boldsymbol{\Psi})||p(\boldsymbol{\Psi})\right) = -\frac{N_{\mathrm{S}}}{2}\sum_{j=1}^{2N_{\mathrm{R}}}\mathbb{E}[\ln\psi_{j,j}] + v\sum_{j=1}^{2N_{\mathrm{R}}}\ln(e_j) \\ &+ \frac{1}{2}\sum_{i=1}^{N_{\mathrm{S}}}\sum_{j=1}^{2N_{\mathrm{R}}}\mathbb{E}\left[(g_{j,i} - \mathbf{a}_{j,:}\mathbf{z}_{:,i})^2\right]\mathbb{E}[\psi_{j,j}] - \tilde{v}\sum_{j=1}^{2N_{\mathrm{R}}}\ln(\tilde{e}_j) + 2N_{\mathrm{R}}\ln\frac{\Gamma(\tilde{v})}{\Gamma(v)}. \end{aligned} \tag{6.30}$$

4. Compute $-D_{\mathrm{KL}}\left(q(\boldsymbol{\alpha})||p(\boldsymbol{\alpha})\right)$

The negative Kullback-Leibler divergence is equal to $\mathbb{E}_{q(\boldsymbol{\alpha})}[\ln p(\boldsymbol{\alpha})] - \mathbb{E}_{q(\boldsymbol{\alpha})}[\ln q(\boldsymbol{\alpha})]$ where $p(\boldsymbol{\alpha})$ is given in (6.7) and $q(\boldsymbol{\alpha})$ in (6.22). Substituting (6.23) and (6.24) yields

$$\begin{aligned} &- D_{\mathrm{KL}}\left(q(\boldsymbol{\alpha})||p(\boldsymbol{\alpha})\right) = -N_{\mathrm{R}}\sum_{d=1}^{N}\mathbb{E}[\ln\alpha_d] + a\sum_{d=1}^{N}\ln(b_d) \\ &+ \frac{1}{2}\sum_{d=1}^{N}\mathbb{E}[\mathbf{a}_{:,d}^{\mathsf{T}}\mathbf{a}_{:,d}]\mathbb{E}[\alpha_d] - \tilde{a}\sum_{d=1}^{N}\ln(\tilde{b}_d) + N\ln\frac{\Gamma(\tilde{a})}{\Gamma(a)}. \end{aligned} \tag{6.31}$$

5. Compute $-\mathbb{E}_{q(\boldsymbol{\alpha})}\left[D_{\mathrm{KL}}\left(q(\mathbf{A})||p(\mathbf{A}|\boldsymbol{\alpha})\right)\right]$

We start from rewriting the Kullback-Leibler divergence as

$$-\mathbb{E}_{q(\boldsymbol{\alpha})}\left[D_{\mathrm{KL}}\left(q(\mathbf{A})||p(\mathbf{A}|\boldsymbol{\alpha})\right)\right] = \mathbb{E}_{q(\boldsymbol{\alpha}),q(\mathbf{A})}\left[\ln p(\mathbf{A}|\boldsymbol{\alpha})\right] - \mathbb{E}_{q(\boldsymbol{\alpha}),q(\mathbf{A})}\left[\ln q(\mathbf{A})\right]$$

where $p(\mathbf{A}|\boldsymbol{\alpha})$ is given in (6.6) and $q(\mathbf{A})$ in (6.21). Using the properties in (6.28) with $\mathbf{a}_{j,:}$, we obtain

$$\begin{aligned} &- \mathbb{E}_{q(\boldsymbol{\alpha})}\left[D_{\mathrm{KL}}\left(q(\mathbf{A})||p(\mathbf{A}|\boldsymbol{\alpha})\right)\right] = N_{\mathrm{R}}\sum_{d=1}^{N}\mathbb{E}[\ln\alpha_d] + N_{\mathrm{R}}N \\ &- \frac{1}{2}\sum_{d=1}^{N}\mathbb{E}[\mathbf{a}_{:,d}^{\mathsf{T}}\mathbf{a}_{:,d}]\mathbb{E}[\alpha_d] + \frac{1}{2}\sum_{j=1}^{2N_{\mathrm{R}}}\ln\det\left(\tilde{\boldsymbol{\Sigma}}_a^j\right). \end{aligned} \tag{6.32}$$

Incorporating (6.27), (6.29), (6.30), (6.31), and (6.32) into (6.26) yields (6.25), concluding the proof. □

Detector

The value of $\mathcal{L}(q^*)$ obtained using CAVI algorithm depends on whether one or more PUs are transmitting in the considered frequency bin. When $\mathbf{z}_{:,i} = \mathbf{0}$ for each $i = 1, \ldots, N_{\mathrm{S}}$, i.e., no PU is transmitting during the observation window, then $q^*(\mathbf{z}_{:,i}) = \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$. In other words, since the algorithm is unable to learn an approximate posterior distribution, it coincides with the chosen prior $p(\mathbf{z}_{:,i})$, and the first three terms in (6.25) are zero. Conversely, when a PU signal is observed these terms assume negative values. An example of the values of $\mathcal{L}(q^*)$ in the presence and absence of PU signals is shown in Fig. 6.3. Hence, we use $\mathcal{L}(q^*)$ as a test statistic to detect the presence of a PU in a frequency bin as

$$\mathcal{L}(q^*) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \varphi. \tag{6.33}$$

Hypothesis $\mathcal{H}_1$ corresponds to the presence of at least one PU signal, while the null hypothesis, $\mathcal{H}_0$, corresponds to its absence. The threshold φ is given by setting the false alarm probability $p_{\mathrm{FA}} = \mathbb{P}(\mathcal{L}(q^*) < \varphi \,|\, \mathcal{H}_0)$, where the null distribution is calculated via histogram based probability density function estimation.

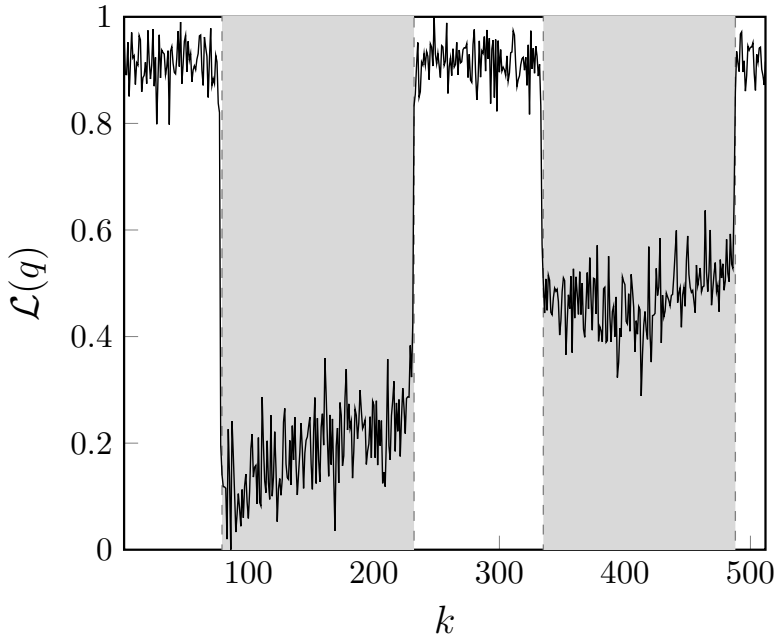

Figure 6.3: An example of values of $\mathcal{L}(q^*)$ after the CAVI algorithm has reached convergence, normalized between 0 and 1, for all the $N_{\mathrm{B}} = 512$ bins. The gray areas denote the bins in which a PU signal is present.

The complete detection method is detailed in Algorithm 5, where the latent dimension N is initialized to $2N_{\mathrm{R}} - 1$, i.e., the dimension of $\mathbf{g}_{:,i}$ minus one [94]. We remark that the test (6.33) is executed independently for each frequency bin.

6.3.5 Primary User Count Estimation

The primary purpose of a generative latent variable model is to determine the appropriate dimension of the latent space. From the perspective of the WSS, this ability is not essential since we only discriminate between dimension zero (i.e. only noise) or dimension greater than zero (i.e. the presence of at least one PU). However, in the broader context of spectrum awareness, knowledge of the number of PUs transmitting in a frequency bin can provide a complete understanding of spectrum usage, in addition to the discovery of spectrum holes [117]. This capability can be exploit in security applications where a deep knowledge of the spectrum is required to detect the presence

of a possible intruder.

The number of PUs in the kth bin can be estimated as the size of the latent space when the algorithm has reached convergence. In other words, an estimation $\hat{N}_{\mathrm{T,k}}$ of the number of PUs $N_{\mathrm{T},k}$ is given by

$$\hat{N}_{\mathrm{T,k}} = \frac{||\boldsymbol{\mu}_z^{(i)}||_0}{2} \tag{6.34}$$

where $i \in \{1, \ldots, N_{\mathrm{S}}\}$ and $||\cdot||_0$ is the ℓ_0-norm.[4]

6.4 Genie-aided Spectrum Sensing

In the numerical results Section 8.3, we validate the proposed VBFA-based algorithm by comparing its performance against a likelihood ratio test (LRT)-based genie-aided detector, which has complete knowledge of the covariance of the signals from PUs, the channel coefficients linking each PU to SU, and the noise covariance affecting each SU.

Let us formulate the per frequency bin spectrum sensing problem as a binary hypothesis test, i.e.,

$$\begin{cases} \mathcal{H}_0: & \mathbf{y}_{:,k}^{(i)} = \mathbf{n}_{:,k}^{(i)} \\ \mathcal{H}_1: & \mathbf{y}_{:,k}^{(i)} = \mathbf{s}_{:,k}^{(i)} + \mathbf{n}_{:,k}^{(i)} \end{cases} \tag{6.35}$$

where $i = 1, \ldots, N_{\mathrm{S}}$, $\mathbf{n}_{:,k}^{(i)} \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma}_n)$, and $\mathbf{s}_{:,k}^{(i)} \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma}_s)$. Let us aggregate the observations of all the SUs in the kth bin in matrix $\mathbf{Y} = \left(\mathbf{y}_{:,k}^{(1)}, \mathbf{y}_{:,k}^{(2)}, \ldots, \mathbf{y}_{:,k}^{(N_{\mathrm{S}})}\right)$. The log-likelihoods of the observations in the two hy-

[4]The result is independent on the considered column because the dimensionality of reduction is applied equally in all the N_{S} observations. Thus, $||\boldsymbol{\mu}_z^{(1)}||_0 = \cdots = ||\boldsymbol{\mu}_z^{(N_{\mathrm{S}})}||_0$.

potheses are

$$\ln f_{\mathbf{Y}|\mathcal{H}_0}(\mathbf{Y}|\mathcal{H}_0) = -\frac{1}{2}\sum_{i=1}^{N_\mathrm{S}} \left(\mathbf{y}_{:,k}^{(i)}\right)^{\mathsf{H}} \boldsymbol{\Sigma}_n^{-1}\mathbf{y}_{:,k}^{(i)} \tag{6.36}$$

$$\ln f_{\mathbf{Y}|\mathcal{H}_1}(\mathbf{Y}|\mathcal{H}_1) = -\frac{1}{2}\sum_{i=1}^{N_\mathrm{S}} \left(\mathbf{y}_{:,k}^{(i)}\right)^{\mathsf{H}} (\boldsymbol{\Sigma}_s + \boldsymbol{\Sigma}_n)^{-1}\mathbf{y}_{:,k}^{(i)} \tag{6.37}$$

where we omitted irrelevant constants. We now assume that the genie has full knowledge of $\boldsymbol{\Sigma}_n$ and $\boldsymbol{\Sigma}_s$, and performs spectrum sensing through the LRT

$$\Lambda\left(\mathbf{Y}\right) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta \tag{6.38}$$

with metric

$$\Lambda\left(\mathbf{Y}\right) = \sum_{i=1}^{N_\mathrm{S}} \left(\mathbf{y}_{:,k}^{(i)}\right)^{\mathsf{H}} \boldsymbol{\Sigma}_n^{-1}\mathbf{y}_{:,k}^{(i)} - \left(\mathbf{y}_{:,k}^{(i)}\right)^{\mathsf{H}} \left(\boldsymbol{\Sigma}_s + \boldsymbol{\Sigma}_n\right)^{-1} \mathbf{y}_{:,k}^{(i)}$$

obtained from (6.36) and (6.37) by some simple manipulation. We remark that the received signal covariance matrix $\boldsymbol{\Sigma}_s$ can be expressed as a function of the transmitted signals and the channel coefficients between the PUs and the SUs.

Algorithm 5: VBFA-based algorithm for WSS

Input : N_{S}, N_{R}, N_{B}, v, $\mathbf{e}$, a, $\mathbf{b}$, $\mathbf{g}_{:,k}^{(i)}$ for $k = 1, \ldots, N_{\mathrm{B}}$, $i = 1, \ldots, N_{\mathrm{S}}$
Output: Decision $\mathcal{D}_k \in \{\mathcal{H}_0, \mathcal{H}_1\}$ for $k = 1, \ldots, N_{\mathrm{B}}$

$N \leftarrow 2N_{\mathrm{R}} - 1$
$\tilde{v} \leftarrow v + \frac{N_{\mathrm{S}}}{2}$
$\tilde{a} \leftarrow a + N_{\mathrm{R}}$
for k **from** 1 **to** N_B **do**
  Initialize $\tilde{\mathbf{b}}$, $\tilde{\mathbf{e}}$, $\boldsymbol{\mu}_a^{(j)}$, $\tilde{\boldsymbol{\Sigma}}_a^{(j)}$ for $j = 1, \ldots, 2N_{\mathrm{R}}$
  $\mathbf{G} \leftarrow \{\mathbf{g}_{:,k}^{(i)}\}_{i=1}^{N_{\mathrm{S}}}$
  while $\mathcal{L}(q^*)$ *does not converge (see* (8.10)*)* **do**
    Compute $q^*(\mathbf{Z})$:
    $\tilde{\boldsymbol{\Sigma}}_z \leftarrow \left(\mathbf{I}_N + \mathbb{E}[\mathbf{A}^{\mathsf{T}}\boldsymbol{\Psi}\mathbf{A}]\right)^{-1}$
    for i **from** 1 **to** N_S **do**
      $\boldsymbol{\mu}_z^{(i)} \leftarrow \tilde{\boldsymbol{\Sigma}}_z \mathbb{E}[\mathbf{A}^{\mathsf{T}}]\mathbb{E}[\boldsymbol{\Psi}]\mathbf{g}_{:,i}$
    end
    Compute $q^*(\mathbf{A})$:
    for j **from** 1 **to** $2N_R$ **do**
      $\tilde{\boldsymbol{\Sigma}}_a^{(j)} \leftarrow \left(\mathbb{E}[\psi_{j,j}] \sum_{i=1}^{N_{\mathrm{S}}} \mathbb{E}[\mathbf{z}_{:,i}\mathbf{z}_{:,i}^{\mathsf{T}}] + \mathbb{E}[\mathrm{diag}(\boldsymbol{\alpha})]\right)^{-1}$
      $\boldsymbol{\mu}_a^{(j)} \leftarrow \tilde{\boldsymbol{\Sigma}}_a^{(j)} \mathbb{E}[\psi_{j,j}] \sum_{i=1}^{N_{\mathrm{S}}} g_{j,i}\mathbb{E}[\mathbf{z}_{:,i}]$
    end
    Compute $q^*(\boldsymbol{\alpha})$:
    for d **from** 1 **to** N **do**
      $\tilde{b}_d \leftarrow b_d + \frac{\mathbb{E}[\mathbf{a}_{:,d}^{\mathsf{T}}\mathbf{a}_{:,d}]}{2}$
    end
    Compute $q^*(\boldsymbol{\Psi})$:
    for j **from** 1 **to** $2N_R$ **do**
      $\tilde{e}_j \leftarrow e_j + \frac{1}{2}\sum_{i=1}^{N_{\mathrm{S}}} \mathbb{E}\left[(g_{j,i} - \mathbf{a}_{j,:}\mathbf{z}_{:,i})^2\right]$
    end
    Compute $\mathcal{L}(q^*)$ in (6.25)
  end
  $\mathcal{D}_k \leftarrow \mathcal{L}(q^*) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \varphi$
end

Chapter 7

Meta-Analysis for WSS

This chapter introduces a novel method for cooperative WSS, which is based on a very old but powerful framework called meta-analysis.

7.1 Problem Statement

Meta-analysis is a statistical approach that integrates and synthesizes the findings of multiple independent "studies" addressing a common research question. By aggregating data from various sources, it aims to provide a more accurate and reliable estimate of the overall effect size, thus enhancing the generalizability of the conclusions. This method is particularly valuable in situations where individual studies yield inconsistent results or are limited by small sample sizes [118].

In the context of cooperative WSS, a "study" is analogous to a sensor that monitors the specific band. While each sensor can independently perform spectrum sensing based on its own observations, variations in channel conditions and geographical locations may lead to differing detection outcomes. To address these discrepancies, a meta-analysis approach can be applied at the FC, combining the detection results from all sensors to produce a more accurate and reliable final outcome.

Fig. 7.1 illustrates the advantages of the meta-analysis approach compared to the previously proposed solution in Chapter 6. In the VBFA

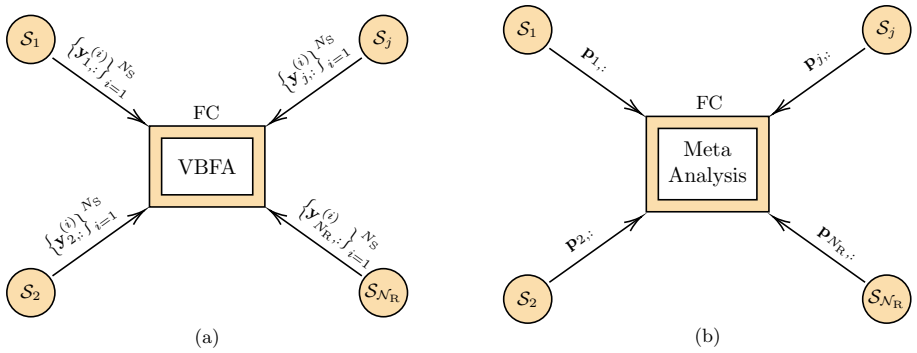

Figure 7.1: (a) VBFA approach, where the jth sensor transmits the N_{B} frequency components $\mathbf{y}_{j,:}^{(i)}$ to the FC for $i = 1, \ldots, N_{\mathrm{S}}$. (b) Meta-analysis approach, where the jth sensor shares the vector $\mathbf{p}_{j,:}$, containing the p-values for each frequency bin.

method, for the kth frequency bin, sensors transmit the N_{S} frequency domain representations of their received signals to the FC. In contrast, as will be discussed in the following section, the meta-analysis approach requires each sensor to share only a scalar value. This significantly reduces the overhead on the backhaul link.

7.2 Meta-Analysis

Meta-analysis refers to the synthesis of data from multiple independent tests. In this section, we combine the detection performed by each sensor in a mixture detector by using meta-analysis. In this scenario, each sensor performs a statistical hypothesis test based on the frequency domain observations of a single frequency bin; then, the outcomes of N_{R} binary hypotheses tests are combined to determine the presence or absence of a signal in that bin. The procedure is repeated for each frequency bin.

7.2.1 p-value

The meta-analysis relies on the evaluation of the p-values, which represents the probability of obtaining a test statistic at least as extreme as the one

observed, assuming that the null hypothesis $\mathcal{H}_0$ is true. It quantifies the strength of evidence against the null hypothesis: smaller p-values indicate stronger evidence, while larger p-values suggest weaker evidence. In mathematical terms, let V represent the test statistic and v be the observed value, then the p-value for test j at bin k is

$$p_{j,k} = \mathbb{P}(V \geq v|\mathcal{H}_0). \tag{7.1}$$

A p-value below a predetermined significance level (commonly denoted as false alarm probability p_{FA}) leads to the rejection of the null hypothesis, suggesting that the observed result is statistically significant. Conversely, if the p-value is greater than p_{FA}, the null hypothesis cannot be rejected.

7.2.2 Ordering Phase

A single statistic test performed by the jth sensor necessitates the estimation of noise power. To this end, a sorted version $\tilde{\mathbf{y}}_{j,:}^{(i)}$ of the observed vector $\mathbf{y}_{j,:}^{(i)}$ is considered. The sorting is executed according to the estimated power of each bin, $\widehat{\sigma}_{j,q}^2 = (1/N_{\mathrm{S}}) \sum_{i=1}^{N_{\mathrm{S}}} \left|y_{j,q}^{(i)}\right|^2$, so that $\left(\widehat{\sigma}_{j,1}^2, \widehat{\sigma}_{j,2}^2, \ldots, \widehat{\sigma}_{j,N_{\mathrm{B}}}^2\right)$ are arranged in ascending order. The ordering phase is depicted in Fig. 7.2. After this operation, it can be assumed that the first frequency bin $\tilde{y}_{j,1}^{(i)}$ is comprised solely of noise. Consequently, an estimated noise power can be derived from $\sum_{i=1}^{N_{\mathrm{S}}} |\tilde{y}_{j,1}^{(i)}|^2$.

7.2.3 Single Test

From (2.17), a binary hypotheses model for the jth sensor and the kth bin can be formulated

$$\begin{cases} \mathcal{H}_0: & y_{j,k}^{(i)} = n_{j,k}^{(i)} \\ \mathcal{H}_1: & y_{j,k}^{(i)} = s_{j,k}^{(i)} + n_{j,k}^{(i)}. \end{cases} \tag{7.2}$$

As already mentioned, for many communication signals (e.g., OFDM), the received samples can be modeled as zero-mean complex Gaussian random variables (r.v.s), such that $y_{j,k}^{(i)} \sim \mathcal{CN}(0, \sigma_j^2)$ for $\mathcal{H}_0$ and $y_{j,k}^{(i)} \sim \mathcal{CN}(0, \sigma_{j,k}^2 + \sigma_j^2)$ for $\mathcal{H}_1$. Let us assume that we are able to estimate the noise power, e.g., from

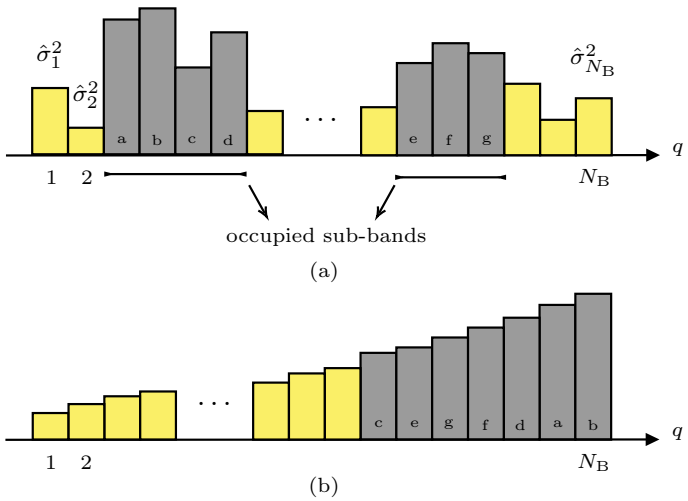

Figure 7.2: Ordering phase for the noise power estimation. Ordering is based on the average power of the elements of $\mathbf{y}_{j,:}^{(i)}$ (a), providing the vector $\tilde{\mathbf{y}}_{j,:}^{(i)}$ (b).

the first frequency bin obtained after ordering as described in the previous Subsection 7.2.2. Then, a test statistic is constructed

$$V_{j,k} = \frac{\sum_{i=1}^{N_S} |y_{j,k}^{(i)}|^2}{\sum_{i=1}^{N_S} |\tilde{y}_{j,1}^{(i)}|^2} \tag{7.3}$$

and the p-value is computed by the cumulative distribution function (c.d.f.) of $V_{j,k}$ as $p_{j,k} = 1 - F_{V_{j,k}}(v)$ for $j = 1, \ldots, N_R$ and $k = 1, \ldots, N_B$. The calculation of $F_{V_{j,k}}(v)$ is a challenging undertaking, and thus we provide an approximation thereof.

Approximate c.d.f.

Let us define the r.v.s $Y = \sum_{i=1}^{N_S} |y_{j,k}^{(i)}|^2$ and $Y_{(1)} = \sum_{i=1}^{N_S} |\tilde{y}_{j,1}^{(i)}|^2$ takes after a order operation where $Y_{(1)} < Y_{(2)} < \cdots < Y_{(N_B)}$. Although it is straightforward to demonstrate that $Y \sim \mathcal{X}_{2N_S}^2$, due to the ordering, it is not possible to draw the same conclusion for $Y_{(1)}$. In particular, the right probability density

function (p.d.f.) for $Y_{(1)}$ is given by [119]

$$f_{Y_{(1)}}(y) = N_{\mathrm{B}}(1 - F_Y(y))^{N_{\mathrm{B}}-1} f_Y(y) \tag{7.4}$$

where $F_Y(y)$ and $f_Y(y)$ are the c.d.f. and p.d.f. of Y, respectively. They can be written as

$$\begin{aligned} f_Y(y) &= \frac{1}{\Gamma(N_{\mathrm{S}})\sigma_j^{2N_{\mathrm{S}}}} y^{N_{\mathrm{S}}-1} e^{-\frac{y}{\sigma_j^2}} \\ F_Y(y) &= \frac{1}{\Gamma(N_{\mathrm{S}})} \int_0^{y/\sigma_j^2} z^{N_{\mathrm{S}}-1} e^{-z} dz = \Gamma_{\mathrm{inc}}\left(\frac{y}{\sigma_j^2}, N_{\mathrm{S}}\right) \end{aligned} \tag{7.5}$$

where $\Gamma(\cdot)$ is the gamma function and $\Gamma_{\mathrm{inc}}(\cdot,\cdot)$ is the incomplete gamma function.[1]

In order to compute the c.d.f. of $V_{j,k}$, we adopt the moments matching approach, whereby the parameters of a known distribution are set to match the first three moments of the true distribution of $V_{j,k}$. It is therefore necessary to have knowledge of the moments of the distribution of $V_{j,k}$. As evidenced in [34, Appendix], the moments of $V_{j,k}$ can be expressed as

$$\mathbb{E}[V_{j,k}^m] = \frac{\mathbb{E}[Y^m]}{\mathbb{E}[Y_{(1)}^m]} \tag{7.6}$$

where

$$\mathbb{E}[Y^m] = \sigma_j^{2m} \frac{\Gamma(N_{\mathrm{S}} + m)}{\Gamma(N_{\mathrm{S}})} \tag{7.7}$$

[1] It should be noted that the definition of the incomplete gamma function $\Gamma_{\mathrm{inc}}\left(y/\sigma_j^2, N_{\mathrm{S}}\right)$ includes the term $\frac{1}{\Gamma(N_{\mathrm{S}})}$, in accordance with the Matlab notation.

$$\begin{aligned}\mathbb{E}[Y_{(1)}^m] &= \int_{-\infty}^{+\infty} y^m f_{Y_{(1)}}(y)dy \\ &= \int_{-\infty}^{+\infty} y^m N_{\mathrm{B}}(1-F_Y(y))^{N_{\mathrm{B}}-1} f_Y(y)dy \\ &= N_{\mathrm{B}} \int_0^1 (F^{-1}(u))^m (1-u)^{N_{\mathrm{B}}-1} du\end{aligned} \tag{7.8}$$

with $u = F_Y(y)$ and $F^{-1}(u) = \sigma_j^2\, \Gamma_{\mathrm{inc}}^{-1}(u, N_{\mathrm{S}})$. Incorporating (7.7) and (7.8) into (7.6) yields

$$\mathbb{E}[V_{j,k}^m] = \frac{\Gamma(N_{\mathrm{S}}+m)}{N_{\mathrm{B}}\,\Gamma(N_{\mathrm{S}}) \int_0^1 (F^{-1}(u))^m (1-u)^{N_{\mathrm{B}}-1} du} \tag{7.9}$$

where the integral is calculated using a numerical method on Matlab.

The distribution of $V_{j,k}$ can be accurately approximated by a scaled and shifted gamma distribution

$$V_{j,k} \simeq G - \alpha \tag{7.10}$$

where α is a constant and $G \sim \mathcal{G}(\beta, \theta)$ denotes a gamma r.v. with shape parameter β and scale parameter θ. We set α, β, θ for matching the first three moments of the distribution of $V_{j,k}$ provided by (7.9) with $m = 1, 2, 3$. To this aim we recall that for the gamma r.v. the mean is $\mu_{\mathrm{g}} = \beta\theta$, the variance is $\sigma_{\mathrm{g}}^2 = \beta\theta^2$ and the skewness is $S_{\mathrm{g}} = 2/\sqrt{\beta}$. If $\mu_{\mathrm{v}} = \mathbb{E}[V_{j,k}]$, $\sigma_{\mathrm{v}}^2 = \mathbb{E}[V_{j,k}^2] - \mu_{\mathrm{v}}$, $S_{\mathrm{v}} = \frac{\mathbb{E}[V_{j,k}^3] - 3\mu_{\mathrm{v}}\sigma_{\mathrm{v}}^2 - \mu_{\mathrm{v}}^3}{\sigma_{\mathrm{v}}^3}$ are the mean, variance and skewness of the distribution of $V_{j,k}$, then matching the first three moments gives:

$$\beta = \frac{4}{S_{\mathrm{v}}^2} \tag{7.11}$$

$$\theta = \frac{\sigma_{\mathrm{v}} S_{\mathrm{v}}}{2} \tag{7.12}$$

$$\alpha = \beta\theta - \mu_{\mathrm{v}}. \tag{7.13}$$

Finally, from (7.11), (7.12), and (7.13) it is possible to compute the ap-

proximate c.d.f. of $V_{j,k}$ as

$$F_{V_{j,k}}(v) \simeq \Gamma_{\text{inc}}\left(\frac{v+\alpha}{\theta}, \beta\right). \tag{7.14}$$

7.2.4 Mixture Detector

The single statistical tests are integrated through the application of two distinct meta-analysis-based mixture detectors.

Fisher's Method

According to Fisher's method, the p-values are combined as [118, 120]

$$V_k^{\text{FM}} = -2\sum_{j=1}^{N_{\text{R}}} \ln(p_{j,k}) \tag{7.15}$$

where $V_k^{\text{FM}} \sim \chi^2_{2N_{\text{R}}}$ denotes the mixture detector test statistic for the kth bin. It is possible to compute the mixture p-value via the c.d.f. as $p_k^{\text{FM}} = 1 - F_{V_k^{\text{FM}}}(v_k^{\text{FM}})$. Finally, for each frequency bin the following test is carried out

$$p_k^{\text{FM}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} p_{\text{FA}}, \quad \forall\, k = 1, \ldots, N_{\text{B}} \tag{7.16}$$

where p_{FA} is the predefined false alarm probability set during system design.

Weighted Z-Transform

According to the z-transform method, each p-value, $p_{j,k} \in [0,1]$, is mapped into a z-value, $z_{j,k} \in [-\infty, +\infty]$, as $z_{j,k} = 1 - F_Z^{-1}(p_{j,k}) = Q^{-1}(p_{j,k})$ [97,121].[2] Then, the z-values are combined to obtain the mixture detector test statistic

$$V_k^{\text{ZT}} = \frac{\sum_{j=1}^{N_{\text{R}}} w_j z_{j,k}}{\sqrt{\sum_{j=1}^{N_{\text{R}}} w_j^2}} \sim \mathcal{N}(0,1) \tag{7.17}$$

[2] Could negative opinions from male soldiers affect women's pride in wearing the U.S. Army uniform? To answer this question, Stouffer proposed the z-transform method in footnote 15 of [122, p. 45].

where w_j is the weight assigned to $z_{j,k}$.[3] Finally, the mixture p-value is computed as $p_k^{\mathrm{ZT}} = 1 - F_{V_k^{\mathrm{ZT}}}(v_k^{\mathrm{ZT}}) = Q(v_k^{\mathrm{ZT}})$ and binary hypothesis test is carried out as for Fisher's method

$$p_k^{\mathrm{ZT}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} p_{\mathrm{FA}} \; \forall \, k = 1, \ldots, N_{\mathrm{B}}. \tag{7.18}$$

[3]The classical z-transform method can be obtained assigning equal weights to all the z-values, such that $V_k^{\mathrm{ZT}} = \frac{1}{\sqrt{N_{\mathrm{R}}}} \sum_{j=1}^{N_{\mathrm{R}}} z_{j,k}$.

Chapter 8

Framework Validation

This chapter presents a series of tests that validate the proposed frameworks for jammer detection and spectrum sensing. In particular, Section 8.1 provides a detailed account of the simulation performance for the jamming detection algorithm presented in Chapters 4, including a comprehensive analysis of the performance of our UBSS algorithm in Chapters 3. Section 8.2, on the other hand, demonstrates the efficacy of the VAE-based jamming detection algorithm in a ISAC system. Finally, Section 8.3 offers a comprehensive evaluation of the performance of cooperative WSS methods presented in Chapter 6 and Chapter 7.

8.1 Jamming Detection through Spectrum Patrol

8.1.1 Simulation Setup

As a case study, we simulated a wireless network composed of N_{T} transmitters and a gateway, a patrol of N_{R} RF sensors, and a jammer, all randomly deployed in a square area of side 100 m. The positions of all the actors (nodes, sensors, and jammer) during the following simulations are shown in Fig.8.1a. The network nodes adopt the Long Range (LoRa) modulation and Long Range Wide Area Network (LoRaWAN) MAC protocol [123, 124]. The

operating frequency is set to $f_0 = 868.1\,\text{MHz}$ and the channel bandwidth is fixed to $W = 125\,\text{kHz}$. According to the European regulation EU868, the transmission duty cycle is set to 1% [125]. We then assume that during the sensors observation time T_{ob}, each wireless node transmits one LoRa packet. Before sending the packet, each transmitter randomly selects a spreading factor (SF) between the available ones, from 7 to 12. In general, T_{ob} has to be sufficiently large to include several transmissions in order to ensure sufficient statistical significance of the estimated TE.

The collision event is defined as the overlap between the transmission of two or more signals (including the jammer), as in a collision channel model. The packets are structured according to [124] and [126], using the implicit header mode and Hamming code with rate 4/7. The MAC payload size for each packet is selected randomly in the interval between 1 byte and the maximum payload size allowed by the EU868 regional parameters [125].

Regarding the wireless channel, a power-law path-loss model with exponent $\alpha = 4$ and log-normal shadowing with intensity $\sigma_{\text{S,dB}}$ are considered. The transmit power of the nodes is $P_{\text{TX}} = 14\,\text{dBm}$ according to the EU868 regional parameters, while the jamming signal is a sine wave at 868.1 MHz with power $P_{\text{J}} = 27\,\text{dBm}$. The receive antenna gain of all the devices (RF sensors and the jammer) is set to 0 dBi and the noise figure is $F = 14\,\text{dB}$.

The sensing, attack, and idle times of the jammer are set to $T_1 = T_2 = T_{\text{I}} = T_{\text{J}} = 50\,\text{ms}$, while sensors estimate the energy of the received signal within a time bin $T_{\text{e}} = 1\,\text{ms}$.

8.1.2 Impact of Shadowing

In this section, the performance of the complete jammer detection algorithm under different shadowing regimes is discussed, and a comparison between TE and cross-correlation as a measure of causality is given. Fig. 8.2 shows the receiver operating characteristic (ROC) curves of the proposed methodology in case of different shadowing intensities using both TE and cross-correlation. For this simulation, we deployed $N_{\text{T}} = 10$ transmitters, $N_{\text{R}} = 5$ sensors, and a jammer in the area. The ROC curves are obtained across $N_{\text{MC}} = 10^4$ Monte

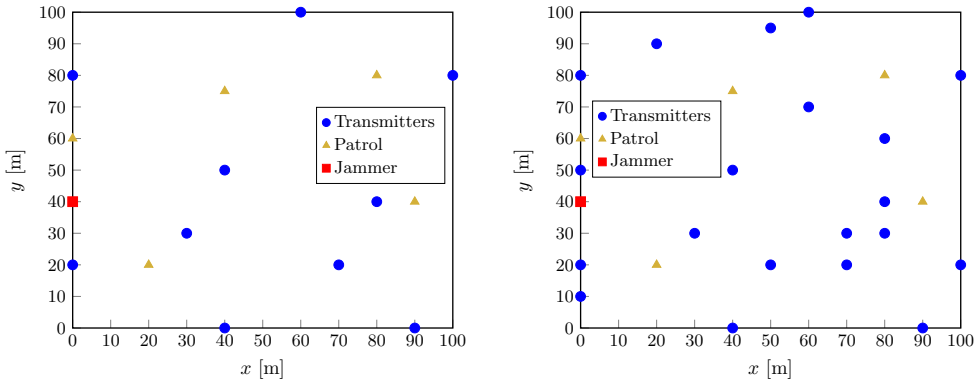

Figure 8.1: (a) Scenario with 10 transmitters, 5 patrol sensors and a jammer used for the simulation. (b) Scenario with 20 transmitters, 5 patrol sensors and a jammer.

Carlo iterations in which the traffic profiles generated by the nodes change and the position of all the actors is provided in the attachment. The patrol observation time is $T_{\text{ob}} = 20\,\text{s}$, in which every node transmits one packet. The packet transmission start times vary so that the number of collisions ranges between 0 and 2 across the Monte Carlo iterations.

Although for low false alarm probabilities, the cross-correlation ROC is above the TE's, the latter quickly outperforms the former, reaching a probability of detection over 0.9 with a relatively small false alarm probability, even in case of high shadowing regime.

Fig. 8.2 shows that, as expected, an increase in the shadowing intensity degrades the overall performance of the methodology. This is due to a non-correct reconstruction of the transmitted energy profiles by the UBSS. However, note that TE exhibits robust performance even for $\sigma_{\text{S,dB}} = 8$.

The presented method is compared with a ML-based approach for jamming detection proposed in [68], in which a gradient boosting algorithm is trained using RSS and PDR as features and used to detect and classify the jammer. Since, in our scenario, the PDR is not available at the patrol (it should be part of the network to retrieve such information), we trained the learning model using only RSS to ensure a fair comparison. Fig. 8.2 includes the performance of both solutions. Since the sensor positions are fixed during

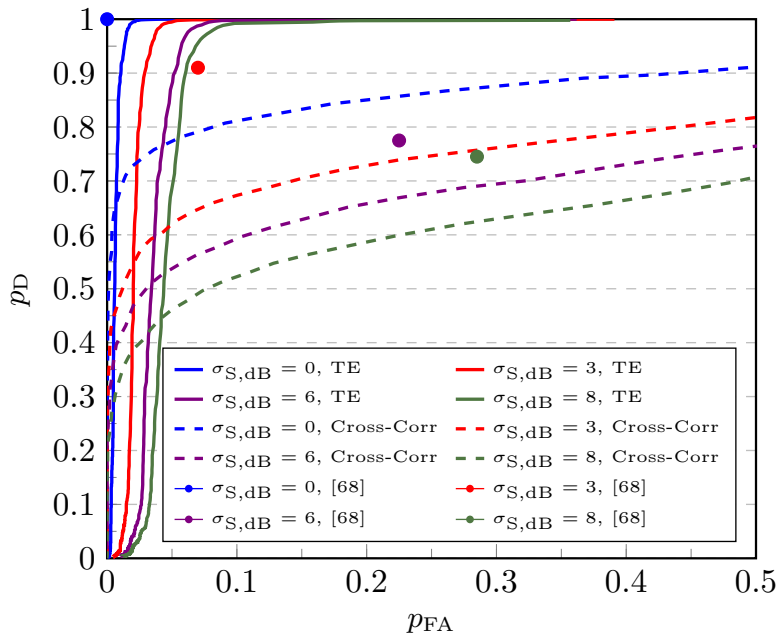

Figure 8.2: ROC curves for TE and cross-correlation with different values of shadowing intensity $\sigma_{S,dB}$. Comparison with the state-of-the-art method.

the Monte-Carlo iterations, the performance of the ML-based algorithm is optimal when $\sigma_{S,dB} = 0$. In this case, RSS is sufficient to detect the presence of the jammer transmitting at high power. However, when increasing shadowing intensity, our algorithm significantly outperforms the existing scheme.

8.1.3 Number of Patrol Sensors

In this section, we investigate the minimum number of RF sensors that guarantee a required jammer detection performance. Given $N_T = 10$ transmitters and a jammer with the same positions adopted for Subsection 8.1.2, in Fig. 8.3 we compute the ROC curve for different number of patrol sensors $N_R = \{4, 5, \ldots, 9\}$. For each of the $N_{MC} = 10^4$ Monte-Carlo iterations the sensors positions are decided in a random way keeping a minimum distance among them, in particular we set at least 40 m of distance with $N_R = 4$, 30 m for $N_R = \{5, 6, 7, 8\}$, and 25 m when $N_R = 9$. A limit of at most two collisions among transmitters in $T_{ob} = 20$ s is considered as in the previous subsection.

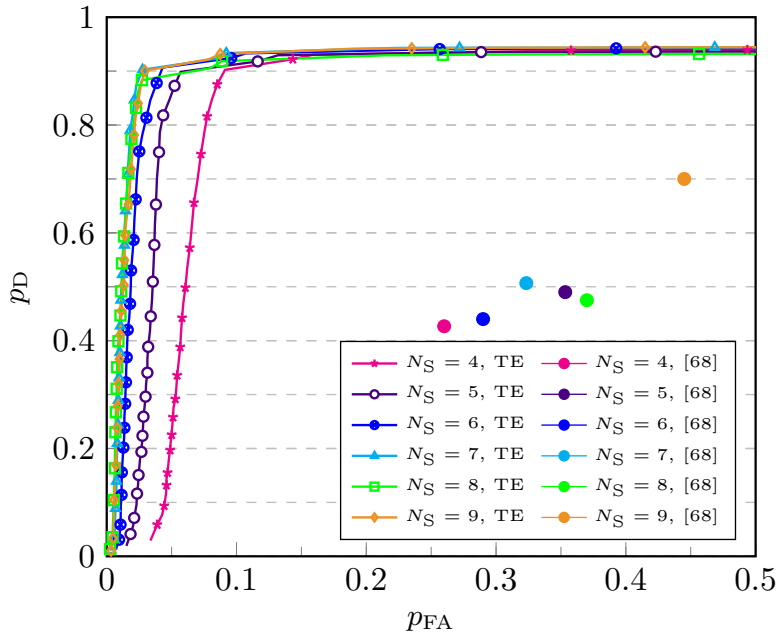

Figure 8.3: ROC curves as a function of the number of sensors N_{R}.

We consider a shadowing with $\sigma_{\mathrm{S,dB}} = 3$ both for transmitter/jammer-patrol channel and for transmitter-jammer channel. It is possible to see that from $N_{\mathrm{R}} = 4$ to $N_{\mathrm{R}} = 7$ the performance noticeably increases, while from $N_{\mathrm{R}} = 7$ to $N_{\mathrm{R}} = 9$ it remains constant. Since we tackled the underdetermined case, the number of sensors does not exceed the number of transmitters, which is 10. If more sensors are available, classical overdetermined BSS schemes, e.g., ICA can be used [127].

Comparing the ROC curve for $\sigma_{\mathrm{S,dB}} = 3$ and $N_{\mathrm{R}} = 5$ in Fig. 8.2 with the corresponding curve in Fig. 8.3, a drop in performance can be notices. The reason lies in the different setup for patrol sensors: in Fig. 8.2 sensors have fixed positions chosen for good coverage of the area, while in Fig. 8.3 at every iteration, their positions change in a random way respecting only a minimum distance, so sometimes unfavorable placement occurs. For the same reason, a complete degradation in performance is observed for the algorithm proposed by [68]. Indeed, by changing the positions, there is a loss of information contained in the RSS values used during training.

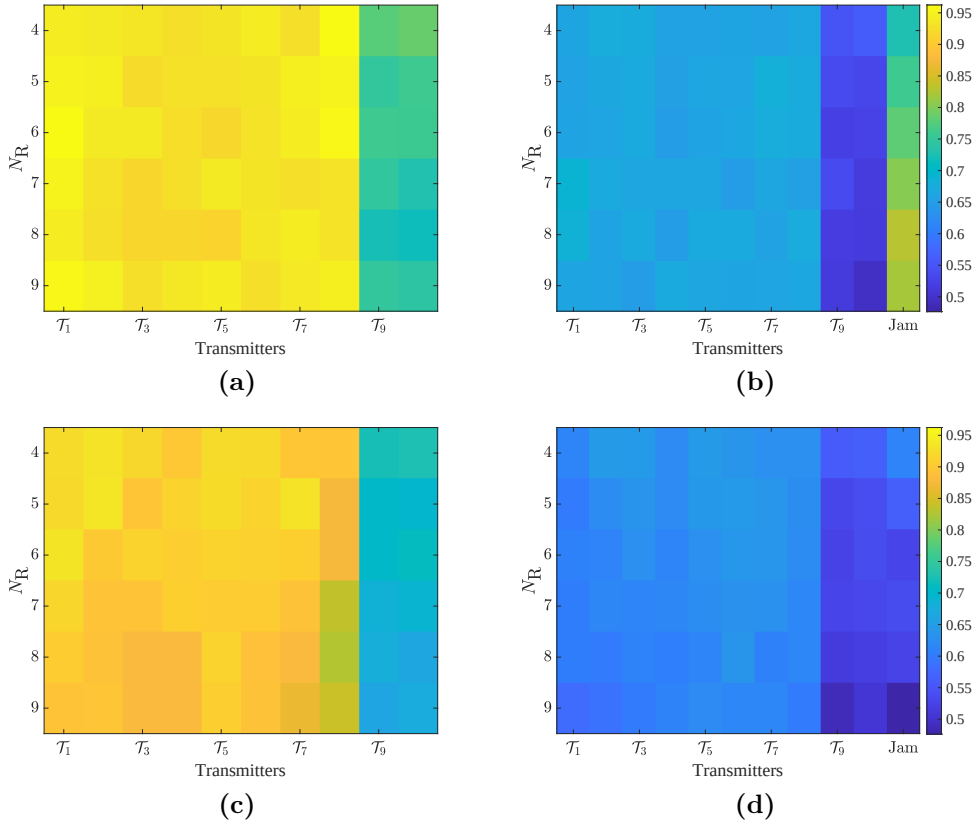

Figure 8.4: Similarity degree among transmitters profiles and estimated sources (the color scale is on the right). Each pixel of the images depicts, for a given N_R in the y-axis, the correlation coefficient of two time series: the true energy profile of the transmitter indicated in the x-axis and the corresponding profile estimated via UBSS. Performance of the proposed algorithm in Chapter 3 without, (a), and with the jammer,(b). Performance of the algorithm in [1] without, (c), and with the jammer, (d).

The same simulation setup is employed to compare the UBSS algorithm in Chapter 3 with the original algorithm in [1]. In both cases, the second step of reconstruction of the transmitted energy profiles is performed with OMP, so the difference resides in the estimate of the mixing matrix where in [1] they do not use a transmission detection and dimensionality reduction steps. To underline the different performance, given the matrix $\mathbf{Z}$, we compute the correlation among each row of $\mathbf{Z}$ and the original energy profiles in $\mathbf{X}$. The result is a matrix $\mathbf{C} \in \mathbb{R}^{L\times(N_T+1)}$ where the element c_{ij} is the correlation between the ith estimated source and the jth row of $\mathbf{X}$. From $\mathbf{C}$, only the

maximum value of each column is considered to obtain a vector $\mathbf{m} \in \mathbb{R}^{N_\mathrm{T}+1}$ that becomes a matrix $\mathbf{M} \in \mathbb{R}^{N_\mathrm{MC} \times (N_\mathrm{T}+1)}$, iterating the simulation for $N_\mathrm{MC} = 1000$. In Fig. 8.4, a pixel $p_{i,j}$ depicts the mean of $\mathbf{M}_{:,j}$ for a given number of sensors $N_\mathrm{R} = i$. This performance metric provides a measurement of similarity among original and estimated energy profiles. $p_{i,j}$ with an high value implies the original profile $\mathbf{X}_{j,:}$ is correctly estimated during the N_MC iterations for $N_\mathrm{R} = i$. In the absence of the jammer, the two methods have comparable performance: the first eight transmitters are estimated with good accuracy, while the reconstruction of the last two, which cause the collision, is affected. In the presence of a jammer, the situation is more interesting because the jamming attack is poorly estimated by the algorithm in [1], while, on the contrary, with our methodology, it is the source estimated at best.

8.1.4 Effect of Collisions

As we have seen, since collisions among nodes' packets are a nuisance in the reconstruction stage, it is necessary to investigate their impact on the performance of the proposed methodology. In particular, there are two aspects to analyze: the consequences of increased collisions and their total absence. This last case summarizes the scheduled access protocols where, since a better reconstruction performance of the UBSS should be expected, then a better jammer detection will occur.

Let us consider $N_\mathrm{T} = 10$, $N_\mathrm{R} = 5$, a jammer, with fixed positions during simulation equal to Subsection 8.1.2, $T_\mathrm{ob} = 20\,\mathrm{s}$, $\sigma_\mathrm{S,dB} = 3$, and an unique SF= 11. The jammer detection probability is computed for a false alarm probability of 5%, number of collisions N_col from 0 to 4, and $N_\mathrm{MC} = 5000$ Monte Carlo iterations. With no collisions, a time division multiple access (TDMA) protocol is simulated, so each transmitter sends its packet in a time slot equal to the packet duration, and a guard time of half the packet duration is present among the slots. A collision only occurs between two packets, e.g., $N_\mathrm{col} = 4$ and $N_\mathrm{T} = 10$ means that 8 packets are involved in the collisions. The results are shown with a orange bar plot in Fig 8.5. As already

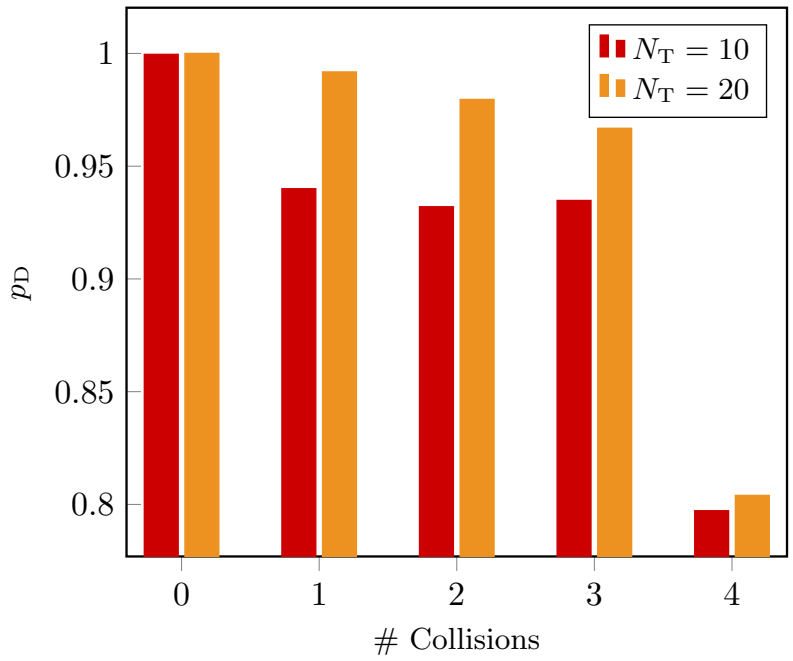

Figure 8.5: Probability of detection as a function of the number of collisions for two different values of the number of transmitting nodes N_T.

mentioned, in a TDMA protocol without collisions, the performance exceeds the other scenarios with a substantial gap. Increasing the collisions, the UBSS performance decrease, however until $N_{coll} = 3$ the detection probability remains roughly constant and above the 90%.

The orange bar plot in Fig 8.5 is obtained with the same setting but placing $N_T = 20$ and $T_{ob} = 30\,s$. This scenario is depicted in Fig. 8.1b with all actor positions.[1] Since the collisions number is unchanged, the sparsity level in $\mathbf{Y}$ is the same and the UBSS performance does not degrade. At the same time, instead, the greater presence of packets permits to capture the causal rapport more easily. Regarding $N_{col} = 4$ and $N_T = 10$ then 80% of the packets are involved in the collisions; with $N_T = 20$ the rate halves at the 40%. Thus, assuming that the collision packets are badly estimated by the UBSS, thanks to the most number of packets, the possibility to remain more faithful to the original sources enhances.

[1]The observation time is increased here to ensure that each node transmits at least one packet.

8.1.5 Impact of SJR

This section studies the performance of AvOTE varying the signal-to-jammer ratio (SJR), defined as the ratio between the nodes and the jammer transmit powers. The scenario consists of $N_{\mathrm{T}} = 10$ transmitters, $N_{\mathrm{R}} = 5$ patrol sensors, and a jammer, and for each of the $N_{\mathrm{MC}} = 3000$ Monte-Carlo iterations, the positions of the sensors are randomly chosen within the area keeping a minimum distance among them of 30 m, while the positions of network nodes and the jammer are the same of Section 8.1.2. In Fig. 8.6, the probability of detection for different values of SJR is reported, considering a false alarm probability of 5%. As expected, the detection probability reduces when the SJR grows. In fact, at high SJRs the power received from the jammer becomes comparable to or even less than the ones received from the legitimate nodes. In this situation, the drop in the detection probability is presumably due to the inability of UBSS to separate the jammer profile from the others. However, notice that if the jamming power is low, the effectiveness of the attack is also reduced.

8.1.6 Computational Complexity Analysis

This section discusses the computational complexity of the proposed jamming detection scheme. The big O notation, $\mathcal{O}(\cdot)$, is used to denote the computational complexity of algorithms.

- **Transmission detection.** Based on (2.14), each sensor computes the energy profile, so the overall complexity for Algorithm 1 is $\mathcal{O}(N_{\mathrm{R}} N_{\mathrm{e}} N_{\mathrm{d}}^2)$.

- **Estimate of the mixing matrix.** Considering loops and operations in Algorithm 2 we achieve a complexity

$$\mathcal{O}\Big(\Big((2IN_{\mathrm{R}} + IN_{\mathrm{R}}N_{\mathrm{col}} + N_{\mathrm{R}}N_k)N_{\mathrm{R}} + N_{\mathrm{R}}N_h^2\Big)\mathrm{K}\Big) \tag{8.1}$$

  where N_{col} is the number of columns of the largest sub-matrix $\mathbf{R}^i$, $i = 1, \ldots, I$. Row 5 is a quantization-based clustering algorithm that

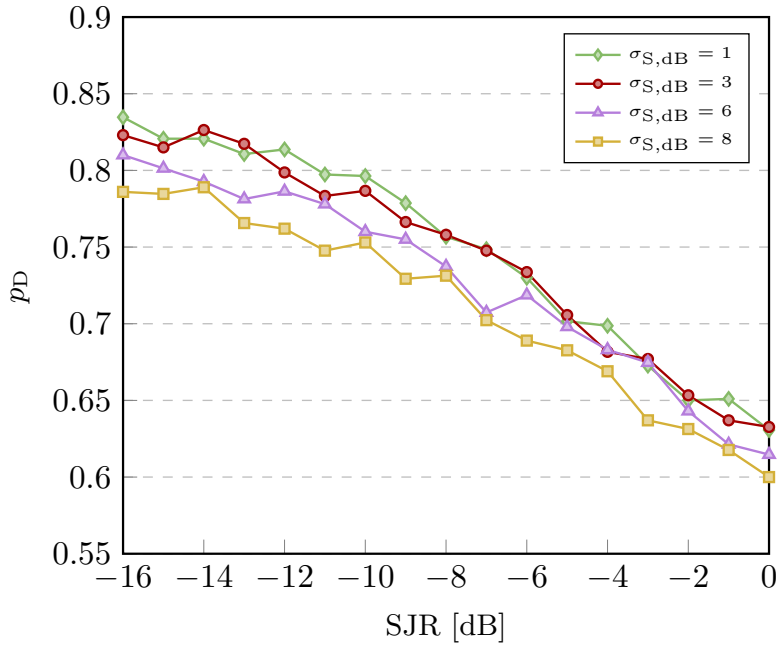

Figure 8.6: Detection probability as a function of the SJR with different shadowing intensities, $\sigma_{S,dB}$, and $p_{FA} = 5\%$.

does not contain any multiplications or sums, but comparisons, so its complexity is neglected [1].

- **Orthogonal matching pursuit.** Based on [128], the complexity of reconstructing the transmitted energy profiles is $\mathcal{O}(\gamma N_R N_W N_e)$.

- **All-versus-one transfer entropy.** The input vectors are sequences of 0s and 1s of length N_e, hence, one computation of TE takes $\mathcal{O}(N_e)$ [72], [129]. Since TE is calculated inside 3 loops in AvOTE algorithm, the complexity for this step is $\mathcal{O}\big(Lk_{max}r_{max}N_e + L(L-1)\big)$, where the term $L(L-1)$ is due to the sum in row 3 of Algorithm 3.

- **Cross-correlation.** Adopting FFT to compute the cross-correlation, the complexity for this version of Algorithm 3 is $\mathcal{O}\big(LN_e \log_2(N_e)\big)$.

Considering $T_{ob} = 20\,s$ and $W = 125\,kHz$, we have $N_d N_e \sim 10^6$. Hence, the largest term of UBSS complexity is the one related to the computation

of the energy. Therefore, the overall complexity of the UBSS can be reduced to $\mathcal{O}(N_{\mathrm{R}}N_{\mathrm{e}}N_{\mathrm{d}}^2)$.

8.2 Jamming Detection through Latent Model

8.2.1 Simulation Setup

The performance of the VAE-based jamming detection solution are evaluated and compared in this section with that of a conventional autoencoder (AE). For all the simulations, 5G new radio (NR) signals compliant with 3GPP Technical Specification in [130] are considered. According to the 5G NR standard, we employed a carrier frequency of $f_0 = 28\,\mathrm{GHz}$, an EIRP $P_{\mathrm{T}}G_{\mathrm{T}} = 13\,\mathrm{dBW}$, subcarrier spacing $\Delta f = 120\,\mathrm{kHz}$, number of antennas $N_{\mathrm{A}} = 50$, and the number of subcarriers used for the radar set to $N_{\mathrm{B}} = 500$. In addition, a quadrature phase shift keying (QPSK) modulation alphabet is used for the generation of the OFDM signal, and the parameter ρ is set to 0.5. As shown in Fig. 2.3, the system scans the environment in the range $[-\theta_0, \theta_0]$, with $\theta_0 = 60^\circ$ and a beamwidth $\Delta\Theta = 5.3^\circ$ at $-10\,\mathrm{dB}$ gain relative to the beam direction. Therefore, the number of step to cover the entire range is $N_{\mathrm{step}} = \lceil \frac{2\theta_0}{\Delta\Theta} \rceil = 23$.

The self-interference attenuation α_{SI} is computed using the signal-to-self interference ratio (SSIR) defined as $\mathsf{SSIR} = (\alpha_{\mathrm{t}}^{(i)}/\alpha_{\mathrm{SI}}^{(i)})^2 = 20\,\mathrm{dB}$. The target RCS is assumed to adhere to the Swerling I model, i.e., $\sigma_{\mathrm{RCS}}^{(i)} \sim \exp(\bar{\sigma}_{\mathrm{RCS}})$ where the mean is $\bar{\sigma}_{\mathrm{RCS}} = 1\,\mathrm{m}^2$. The noise power spectral density is $N_0 = k_{\mathrm{B}}T_0F$, where $k_{\mathrm{B}} = 1.38 \cdot 10^{-23}\,\mathrm{JK}^{-1}$ is the Boltzmann constant, $T_0 = 290\,\mathrm{K}$ is the reference temperature, and $F_{\mathrm{dB}} = 8\,\mathrm{dB}$ is the receiver noise figure.

8.2.2 Parameter Settings

The VAE's encoder comprises a deep feed-forward neural network architecture, with the input layer receiving the normalized vector $\mathbf{g}_{:,i} \in \mathbb{R}^{2N_{\mathrm{B}}\times 1}$, which has unit modulus. Following this, the encoder employs 5 hidden layers

with $728, 256, 64, 32$, and L neurons each, respectively. The encoder outputs two vectors, $\boldsymbol{\beta}[i]$ and $\boldsymbol{\vartheta}[i]$, each having a latent dimension of $L = 10$. The decoder takes the latent variable $\mathbf{z}_{:,i} = \boldsymbol{\beta}[i] + \boldsymbol{\vartheta}[i] \odot \boldsymbol{\epsilon}$ as input, where $\boldsymbol{\epsilon} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_{\mathrm{L}})$. The decoder's architecture mirrors that of the encoder, producing the vectors $\boldsymbol{\mu}[i] \in \mathbb{R}^{2N_{\mathrm{B}} \times 1}$ and $\boldsymbol{\sigma}[i] \in \mathbb{R}^{2N_{\mathrm{B}} \times 1}$ as output. Each hidden layer employs the rectified linear unit (ReLU) activation function, except for the layers computing $\boldsymbol{\beta}[i]$ and $\boldsymbol{\vartheta}[i]$, which employ a linear activation function. Since the input is normalized with unit modulus, the output layer for $\boldsymbol{\mu}[i]$ adopts the hyperbolic tangent activation function. Training is conducted using the Adagrad optimizer with learning rate $\eta = 0.005$, for $N_{\mathrm{epoch}} = 4000$ epochs, and batch size $N_{\mathrm{bs}} = 460$. The training objective is to minimize the negative ELBO, which is defined in (5.9).

To validate our VAE-based approach, we compare its performance with a conventional AE. The AE's encoder also employs a feed-forward deep neural network architecture, comprising 7 hidden layers with $728, 512, 256, 128, 64, 32$, and 10 neurons each, respectively, where 10 denotes the bottleneck dimension. The decoder mirrors the encoder's architecture, giving as output the reconstructed vector $\hat{\mathbf{g}}_{:,i}$. Each hidden layer employs the ReLU activation function, while the output layer uses the hyperbolic tangent activation function. The AE is trained using the Adagrad optimizer with learning rate $\eta = 0.001$, over $N_{\mathrm{epoch}} = 2000$ epochs, and a batch size of $N_{\mathrm{bs}} = 200$. The loss function used for the training is the mean-square error (MSE).

For both training and validation, we use a matrix $\mathbf{G} \in \mathbb{R}^{2N_{\mathrm{B}} \times N}$ with $N = 57.5 \cdot 10^3$ observations. Specifically, 80% of the observations are used for training, and the remaining 20% for validation. Both the VAE and AE architectures were selected after extensive parameter searches to achieve their optimal performance. To obtain a comprehensive training set that enables the VAE to learn a general representation of the latent space, we assume that independent observations are collected across various environments. Specifically, we assume that for each observation, the target position and the parameters related to the channel realization between the target and the BS

are generated according to the following distributions:

$$\phi_{\mathrm{t}}^{(i)},\, \phi_{\mathrm{SI},1},\, \ldots,\, \phi_{\mathrm{SI},N_{\mathrm{R}}} \sim \mathcal{U}(0, 2\pi), \tag{8.2}$$

$$r_{\mathrm{t}}^{(i)} \sim \mathcal{U}(20, 85), \tag{8.3}$$

$$\theta_{\mathrm{t}}^{(i)},\, \theta_{\mathrm{BS,J}}^{(i)} \sim \mathcal{U}[\theta_{\mathrm{T}}^{(i)} - \frac{\Delta\Theta}{2}, \theta_{\mathrm{T}}^{(i)} + \frac{\Delta\Theta}{2}]. \tag{8.4}$$

For the nth observation, the direction of the BS' beam is set according to

$$\theta_{\mathrm{T}}^{(i)} = \theta_{\mathrm{R}}^{(i)} = -\theta_0 + \mathrm{mod}(i-1, N_{\mathrm{step}})\Delta\Theta \tag{8.5}$$

where $\mathrm{mod}(a, b)$ is the modulo operator which returns the remainder of the division between the two positive numbers a and b.

To evaluate the efficacy of the anomaly detector, the input for the test is a matrix comprising 4600 observations. Of these, 2300 represent instances where only the target is present, while the remaining observations include both the target and the jammer. Also for the test dataset we assume that, for each observation, the target position and the parameters related to the channel realization between the target and the BS are generated according to (8.2), (8.3), and (8.4), while the parameters related to the jammer are generated according to $N_{\mathrm{J}} = 10$, $\phi_{\mathrm{J}}^{(i)} \sim \mathcal{U}(0, 2\pi)$, $\theta_{\mathrm{J}}^{(i)} \sim \mathcal{U}(0, 2\pi)$, and $\theta_{\mathrm{J,BS}}^{(i)} \sim \mathcal{U}[\theta_{\mathrm{J}}^{(i)} - \frac{\Delta\Theta_j}{2}, \theta_{\mathrm{J}}^{(i)} + \frac{\Delta\Theta_j}{2}]$, where $\Delta\Theta_j = 14°$.

8.2.3 Impact of SJR

In this subsection, the performance of the proposed jamming detection method varying the SJR, is studied. The SJR is defined as the ratio between the EIRP of the legitimate signal and that of the jammer signal, i.e.,

$$\mathsf{SJR} = \frac{\rho P_{\mathrm{T}} G_{\mathrm{T}}}{P_{\mathrm{J}} G_{\mathrm{J}}}. \tag{8.6}$$

The test is performed assuming the jammer is in a fixed position, i.e., $r_j^{(i)} = r_j = 90\,\mathrm{m}$, implying that the jammer is attempting to deceive the BS by staying outside its coverage area. For each observation, the injected false delay is

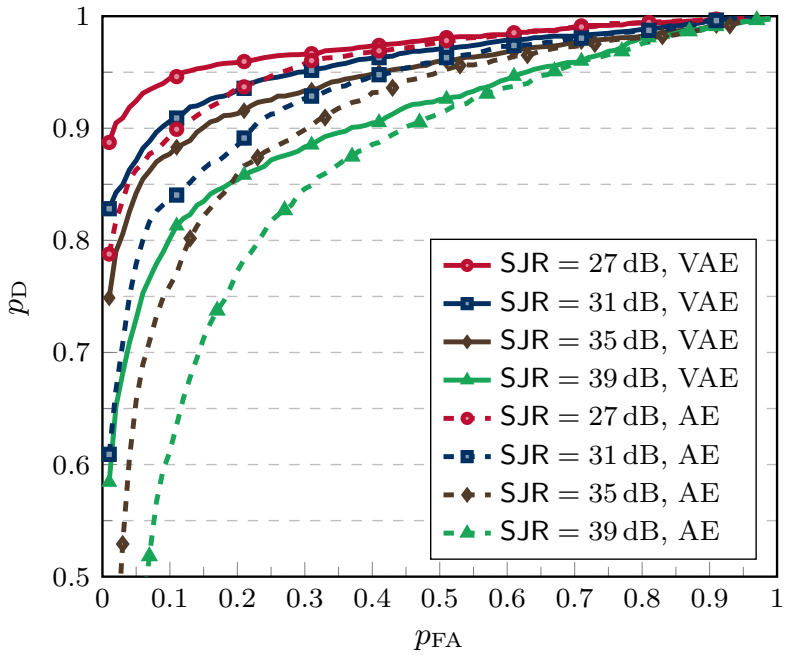

Figure 8.7: ROC curves of the proposed VAE and the conventional AE for different SJR values.

set to $\tau_{\mathrm{f}}^{(i)} = 0.17\,\mu\mathrm{s}$, corresponding to a false distance of 50 m. Fig. 8.7 shows the ROC curves for different SJR values for both the proposed VAE and the conventional AE. Considering a false alarm probability $p_{\mathrm{FA}} = 0.05$, the VAE achieves a detection probability $p_{\mathrm{D}} = 0.93$ for SJR = 27 dB. However, when the jammer's transmit power is significantly lower than BS's sensing power, the detection performance deteriorates. Moreover, from Fig. 8.7 it is evident that the VAE outperforms the conventional AE for each of the SJR values. The best performance produced by the VAE with regard to AE are caused by the difference between reconstruction probability and reconstruction error. The latent variables in a VAE are stochastic, whereas in autoencoders, they are defined by deterministic mappings. As the VAE employs a probabilistic encoder to model the distribution of latent variables rather than the variables themselves, it is able to account for the variability of the latent space through the sampling process. This increases the expressive power of the VAE, as it is capable of capturing differences in variability even when

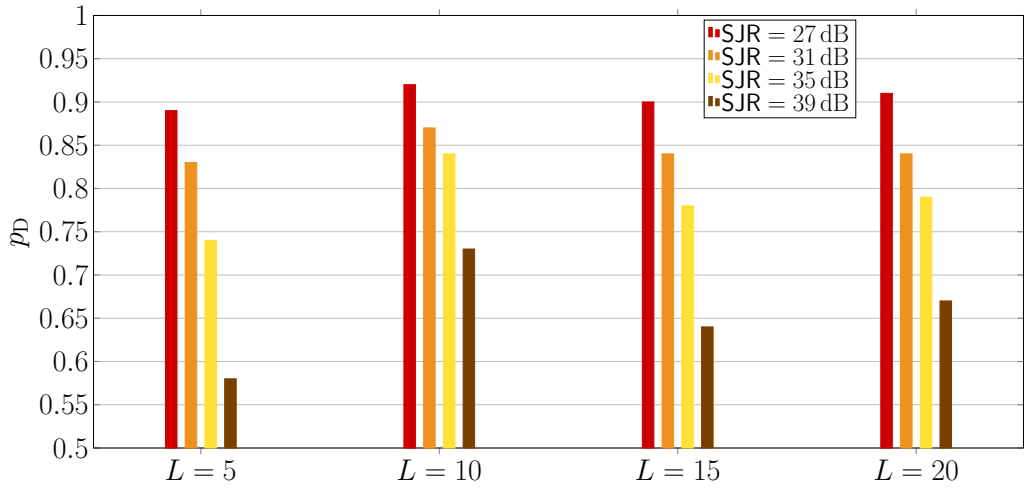

Figure 8.8: Probability of detection p_D for different latent space dimensions, L, and SJR values, with a false alarm probability $p_{FA} = 0.05$.

normal and anomalous data share the same mean value [89].

8.2.4 Latent space dimension

Finally, we assess the impact of the latent space dimension hyperparameter, L, on the VAE's detection performance. Fig. 8.8 shows the probability of detection p_D, for different SJR values and latent space dimensions 5, 10, 15 and 20, with a false alarm probability $p_{FA} = 0.05$. Tipically, setting a low latent space dimension prevents the VAE from capturing all the trends and variations in the training observations. Conversely, high values of L tend to keep the regularization term $D_{KL}\left(q_{\boldsymbol{\varphi}}(\mathbf{z}_{:,i}|\mathbf{g}_{:,i})||p(\mathbf{z}_{:,i})\right)$ low during the training [131]. From Fig. 8.8, it is evident that setting $L = 10$ provides the best performance, even considering different SJR values. When $L = 5$, the VAE is unable to correctly learn the latent space, resulting in degraded detection probability. Similarly, for $L = 15$ and $L = 20$, the impact on the regularization term prevents the algorithm from fully exploiting its learning potential, leading to suboptimal performance. Therefore, both lower and higher values of L negatively affect the detection probability.

8.2.5 Computational Complexity Analysis

As the training phase can be performed offline, the computational complexity of the NNs is evaluated based solely on the forward propagation. The number of operations is determined by the architecture's neuron count and layer configuration, and is expressed as a function of both the input and latent space dimensions.

- **VAE.** For the architecture detailed in Subsection 8.2.2, the network's complexity is given by $\mathcal{O}(2((2N_{\mathrm{B}})728 + 32L) + 32L + L^2)$. Assuming $L \ll N_{\mathrm{B}}$, this simplifies to $\mathcal{O}((4N_{\mathrm{B}})728)$.

- **AE.** Under the same assumption, the complexity also simplifies to $\mathcal{O}((4N_{\mathrm{B}})728)$.

8.3 Cooperative WSS

8.3.1 Simulation Setup

In this Subsection, we evaluate the performance of the proposed cooperative WSS techniques in a realistic scenario, accounting for multiple PUs and channel impairments such as path-loss, multipath propagation (frequency-selectivity), shadowing, and unequal noise power at the sensors.

Without loss of generality, we consider equivalent low-pass signals and all frequencies are normalized with respect to the sampling frequency at the receivers. The scenario consists of two PUs which emit independent band-limited Gaussian processes mimicking the OFDM signals, with normalized center frequencies $f_1 = 0.3$ and $f_2 = 0.8$, respectively, and normalized bandwidths $B_1 = B_2 = 0.3$ [132].

The N_{R} sensors experience AWGN with different noise powers. This is accounted by the noise power spread among the N_{R} sensors, $\Delta\sigma^2_{\mathrm{N,dB}}$, which represents the difference among the noise power of sensor $\mathcal{S}_1$ and sensor $\mathcal{S}_{N_{\mathrm{R}}}$; such spread is then equally distributed among the remaining sensors. For example, if $\Delta\sigma^2_{\mathrm{N,dB}} = 2$ and $N_{\mathrm{R}} = 5$ then the noise power at the receivers

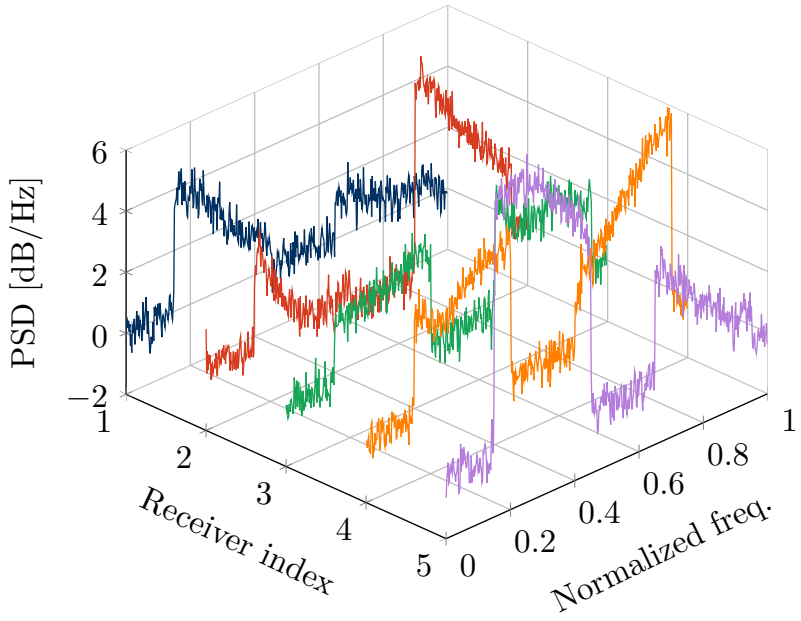

Figure 8.9: An illustration of the received signals in frequency domain for $N_{\mathrm{R}} = 5$ sensors, setting $N_{\mathrm{B}} = 512$ and $\mathsf{SNR} = 0\,\mathrm{dB}$.

in ascending order is $\sigma^2_{\mathrm{N,dB}} + \{1, 0.5, 0, -0.5, -1\}$ where $\sigma^2_{\mathrm{N,dB}}$ is the nominal noise power.

Because of the wideband nature of the signals and receivers involved, we consider frequency-selective multipath channels between the PUs and the sensors. In particular, we consider the ITU EPA channel model, which consists of seven independent Rayleigh distributed paths as detailed in Subsection 2.1.2. Each PU-sensor link is also subject to log-normal shadowing with intensity $\sigma_{\mathrm{S,dB}}$. Moreover, to account for different path-loss experienced by PU-sensor links we define a nominal SNR, SNR, and the SNR spread, $\Delta\mathsf{SNR}_{\mathrm{dB}}$, i.e., the maximum difference among the SNR at receivers. For the sake of clarity, if $\Delta\mathsf{SNR}_{\mathrm{dB}} = 10$ and $N_{\mathrm{R}} = 5$ then the SNRs at the sensors are $\mathsf{SNR}_{\mathrm{dB}} + \{5, 2.5, 0, -2.5, -5\}$. An illustration of the frequency representation of the received signals when $N_{\mathrm{R}} = 5$ is reported in Fig. 8.9. Note the different frequency-selective fading experienced by the receivers. If not otherwise specified, in the following results we consider $N_{\mathrm{S}} = 100$, $N_{\mathrm{B}} = 512$ bins, $N_{\mathrm{R}} = 5$ sensors, $\Delta\mathsf{SNR}_{\mathrm{dB}} = 10$, $\Delta\sigma^2_{\mathrm{N,dB}} = 4$, and $\sigma_{\mathrm{S,dB}} = 3$.

8.3.2 Figure of Merit

For each parameter setup, $N_{\mathrm{MC}} = 10^3$ Monte Carlo trials are carried out over the channel realizations (noise, multipath, shadowing) to obtain averaged performance. Let us define the ground truth matrix $\mathbf{B} \in \{0,1\}^{N_{\mathrm{B}} \times N_{\mathrm{MC}}}$, whose entry $b_{j,i}$ can be either 0 or 1. If $b_{j,i} = 1$, then the jth frequency bin is occupied (i.e., at least one PU is transmitting in that bin) at the ith Monte Carlo iteration. Then, we also define matrix $\hat{\mathbf{B}} \in \{0,1\}^{N_{\mathrm{B}} \times N_{\mathrm{MC}}}$, with entries $\hat{b}_{j,i}$, such that $\hat{b}_{j,i} = 1$ means that the jth bin is declared occupied by the VBFA (or Meta Analysis) algorithm at the ith Monte Carlo iteration. Given k^* occupied frequency bins among the total number N_{B} of bins available, the performance of the proposed cooperative WSS techniques are assessed considering the following metrics:

$$P_{\mathrm{d}} = \frac{\sum_{i=1}^{N_{\mathrm{MC}}} \sum_{j=1}^{N_{\mathrm{B}}} b_{j,i} \hat{b}_{j,i}}{k^* N_{\mathrm{MC}}} \tag{8.7}$$

$$P_{\mathrm{fa}} = \frac{\sum_{i=1}^{N_{\mathrm{MC}}} \sum_{j=1}^{N_{\mathrm{B}}} (1 - b_{j,i}) \hat{b}_{j,i}}{(N_{\mathrm{B}} - k^*) N_{\mathrm{MC}}} \tag{8.8}$$

$$P_{\mathrm{d}}^{\mathrm{all}} = \frac{\sum_{i=1}^{N_{\mathrm{MC}}} \mathbb{1}_{\{\sum_{j=1}^{N_{\mathrm{B}}} (b_{j,i} \hat{b}_{j,i}) = k^*\}}}{N_{\mathrm{MC}}} \tag{8.9}$$

where $\mathbb{1}_{\{x=y\}}$ is the indicator function equal to one when $x = y$ and zero otherwise. P_{d} is the probability of detection at a given bin under the hypothesis that a PU signal is present in that bin, P_{fa} is the probability of false alarm at a given bin under the hypothesis that only noise is present in that bin, and $P_{\mathrm{d}}^{\mathrm{all}}$ is the probability to detect all the bins that contain the PU signals.

To compute the statistical test in (6.33), (6.38), (7.18), and (7.16), the probability of false alarm is set to $P_{\mathrm{fa}} = 0.05$.

8.3.3 Parameter Settings for VBFA Algorithm

Table 8.1 summarizes the parameter settings adopted when executing Algorithm 5. The prior parameters are set to $a = v = b_d = e_j = 10^{-4}$ for $d = 1, \ldots, N$ and $j = 1, \ldots, 2N_{\mathrm{R}}$; $\mathbb{E}[\alpha_d] = \tilde{a}/\tilde{b}_d$ and $\mathbb{E}[\psi_j] = \tilde{v}/\tilde{e}_j$ are ini-

Table 8.1: VBFA simulation parameters for cooperative WSS.

Parameter	a, v, b_d, e_j	$\mathbb{E}[\alpha_d]$	$\mathbb{E}[\psi_j]$	$\boldsymbol{\mu}_a^{(j)}$	$\tilde{\boldsymbol{\Sigma}}_a^{(j)}$	λ	g
Value	10^{-4}	10^{-2}	10^{-2}	$\sim \mathcal{U}(0,1)$	$\frac{1}{2N_\mathrm{R}}\mathbf{U}\mathbf{U}^\mathsf{T}$	10^{-5}	100

tialized to 10^{-2} for all d and j; $\boldsymbol{\mu}_a^{(j)}$, $j = 1, \ldots, 2N_\mathrm{R}$, is initialized as a vector of values drawn from a uniform distribution between 0 and 1. Called $\mathbf{U} = [\boldsymbol{\mu}_a^{(1)}, \ldots, \boldsymbol{\mu}_a^{(2N_\mathrm{R})}]$, we set $\tilde{\boldsymbol{\Sigma}}_a^{(j)} = \frac{1}{2N_\mathrm{R}}\mathbf{U}\mathbf{U}^\mathsf{T}$ for all j.

The CAVI algorithm stops when $\mathcal{L}(q^*)$ converges, i.e., the exit condition is satisfied when

$$\frac{|\mathcal{L}(q^*)_n - \mathcal{L}(q^*)_{n-t}|}{|\mathcal{L}(q^*)_{n-t}|} < \lambda \tag{8.10}$$

where $\lambda = 10^{-5}$, $t = 100$, and $\mathcal{L}(q^*)_n$ is the ELBO evaluated at the nth iteration.

8.3.4 State of the Art

We compared our WSS algorithms with three state-of-the-art algorithms, namely the GMM and K-means-based solutions proposed in [99] and the cascade of a sparse autoencoder (SAE) and a GMM proposed in [111]. These are data-driven unsupervised clustering algorithms aimed at assigning each of the processed frequency bins to one of two clusters: one corresponding to noise-only signal and the other to the presence of at least one PU signal. Therefore, such algorithms are required to detect which of the clusters corresponds to the noise-only case, e.g., by estimating the noise power. Since there can be at most 2 PU signals in the considered bandwidth, we set the number of clusters to 3, assuming prior knowledge of the noise cluster. Contrarily, our proposed VBFA-based algorithm does not require prior noise power estimation.

In the following results, the clustering algorithms proposed in [99] are fed as input with the matrix of received power samples $\mathbf{R} \in \mathbb{R}^{N_\mathrm{B} \times N_\mathrm{R}}$, where $r_{k,j} = \frac{1}{N_\mathrm{S}} \sum_{i=1}^{N_\mathrm{S}} |\mathbf{x}_{j,k}^{(i)}|^2$. The SAE introduced in [111] is based on a deep feed-forward neural network architecture. The network's input layer processes the power matrix $\tilde{\mathbf{R}} \in \mathbb{R}^{LN_\mathrm{B} \times N_\mathrm{R}}$, which has been normalized by the noise

power. We set $L = 110$ to expand the input matrix $\tilde{\mathbf{R}}$ where the 90% of the observations are used for training, and the remaining 10% for validation. The architecture consists of four hidden layers with neuron configurations of $15, 20, 15$, and N_{R}, respectively. A Sigmoid activation function is applied to each hidden layer, while the output layer utilizes a linear activation function. The model is trained using the Adam optimizer with a learning rate set to 0.0001, over 2000 epochs with a batch size of 400. The training process minimizes the MSE loss, augmented by a sparsity penalty on the bottleneck, as detailed in eq. (13) of [111].

8.3.5 Impact of SNR

In this section, we compare the performance of our spectrum sensing methods with that of the genie-aided detector presented in Section 6.4 and the three solutions exposed in the previous subsection. In particular, for the SAE, the network is trained from scratch each time for each SNR value.

In Fig. 8.10a and Fig. 8.10b, P_{d} and $P_{\mathrm{d}}^{\mathrm{all}}$ for all the detectors are shown for different SNR values. For the Z-transform, three variants are considered: equal weights for all the sensors, $\mathbf{w}_1 = [0.05, 0.1, 0.2, 0.25, 0.4]$, and $\mathbf{w}_2 = [0.1, 0.1, 0.2, 0.3, 0.3]$. The weights are assigned sequentially, such that the sensor with the highest noise power has the lowest weight. The Fisher's method yields higher detection probability compared to the Z-transform, which exhibits a slight performance increase when using weights. In the case of low SNR values, the performance of VBFA is observed to be slightly inferior to that of Fisher. However, as the SNR increases, the curves for P_{d} converge. Our solutions outperform the state-of-the-art algorithms, approaching the genie-aided detector in high-SNR regimes.

8.3.6 Number of Sensors

The performance of cooperative WSS strongly depends on the number of SUs performing joint detection. In Fig. 8.10c, $P_{\mathrm{d}}^{\mathrm{all}}$ and P_{d} varying the number of sensors N_{R} from 2 to 10 with $\mathsf{SNR} = -7\,\mathrm{dB}$ are shown. We kept $\Delta\mathsf{SNR}_{\mathrm{dB}}$ and $\Delta\sigma^2_{\mathrm{N,dB}}$ constant, such that while the number of SUs increases,

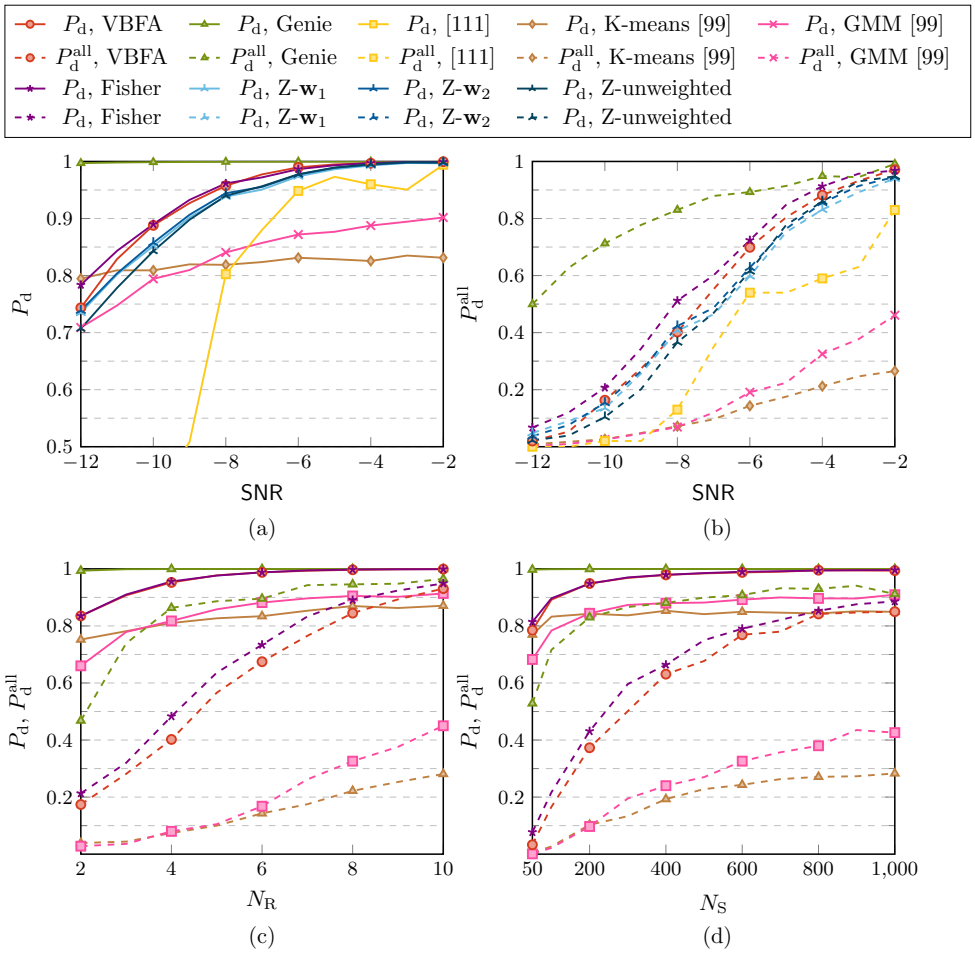

Figure 8.10: P_d and P_d^{all} varying different simulation parameters: (a)-(b) performance is shown for different SNR values; (c) simulations are carried out for different number of sensors deployed in the area, N_R; (c) detection probabilities as a function of the number of independent observations, N_S.

the maximum difference among the SNRs at receivers remains constant.[2] As expected, performance improve as the number of SUs increases. VBFA and Fisher's method achieve $P_d = 0.9$ for $N_R = 3$ and approaches the genie-aided benchmark for $N_R = 6$. In terms of P_d^{all}, Fisher's method gives the highest detection probability.

[2]Given that the Fisher's method yields a higher detection probability than the Z-transform, for the purposes of illustrating the impact of varying N_R and N_S on performance, we will focus on the results obtained using the Fisher's method.

8.3.7 Number of Observations

In Fig. 8.10d, $P_{\mathrm{d}}^{\mathrm{all}}$ and P_{d} are shown for $N_{\mathrm{S}} \in [50, 10^3]$, $\mathsf{SNR} = -10\,\mathrm{dB}$, and $N_{\mathrm{R}} = 5$. Again, VBFA approaches the performance of the Fisher's method for P_{d}, but remains lower for $P_{\mathrm{d}}^{\mathrm{all}}$. Moreover, the state-of-the-art algorithms are not able to match our solution performance.

Increasing the number of collected observations, N_{S}, enhances detection probability by capturing more signal and channel realizations into the input matrix $\mathbf{G}_k$, helping the VBFA algorithm to approximate better the posterior distribution $q(\boldsymbol{\Theta})$, thus maximizing the ELBO. However, a larger N_{S} increases computational cost, as detailed in Algorithm 5, due to its effect on the loop operations. Additionally, a high N_{S} value extends the observation time, potentially causing significant time lags, which undermines the assumption that PUs' occupancy remains constant during the N_{S} observations.

8.3.8 Impact of Channel Model

The simulations in the previous numerical results' subsections are performed using the EPA channel model. However, in [9], other two channel models are proposed as reported in Tab. 2.1.

In Fig. 8.11, the values of P_{d} and $P_{\mathrm{d}}^{\mathrm{all}}$ are presented for various SNR levels across all three channel models. While the individual bin detection probability P_{d} remains relatively stable, we observe that $P_{\mathrm{d}}^{\mathrm{all}}$ varies depending on the channel model. The ETU model is the one yielding the worst performance; this is probably due to the stronger multipath effect and significant path delays, leading to higher frequency selectivity.

8.3.9 Performance of KL Divergence Metric

We will now focus on the VBFA algorithm proposed in Chapter 6. In principle, the first three terms in (6.25), derived from $-D_{\mathrm{KL}}(q(\mathbf{Z})||p(\mathbf{Z}))$, can be used as a metric to perform spectrum sensing via binary hypothesis testing in line 28 of Algorithm 5, after the convergence of the ELBO. In absence of a signal we obtain $D_{\mathrm{KL}}(q(\mathbf{Z})||p(\mathbf{Z})) = 0$, while with an occupied frequency

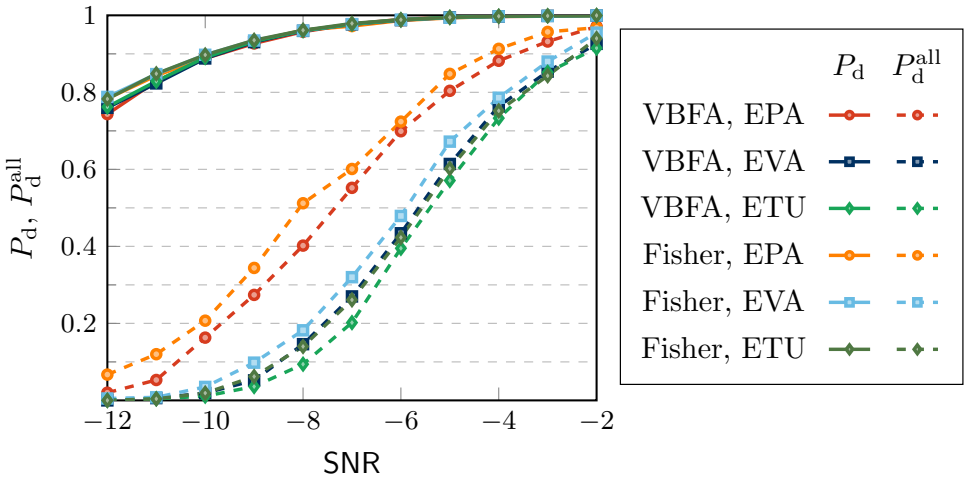

Figure 8.11: P_d and $P_\mathrm{d}^\mathrm{all}$ are shown for different SNR values using three channel models proposed in Tab. 2.1. P_fa is set to 0.05.

bin, the Kullback-Leibler divergence is small but greater than zero.

In order to verify this assertion, two ROC curves are shown in Fig. 8.12 for $\mathsf{SNR} = -2\,\mathrm{dB}$. The blue curve was obtained using a statistical test with the ELBO as metric, while the red curve corresponds to a statistical test with $-D_\mathrm{KL}(q(\mathbf{Z})||p(\mathbf{Z}))$. It is evident that ELBO provides better performance, and this is probably due to the fact that the remaining terms in (6.25), which are not derived from the Kullback-Leibler divergence, assume different values depending on whether the PU is present or not, enhancing the ability of the detector in distinguishing between the two hypotheses. For example, if the bin contains only noise, the algorithm will tend to turn off all directions in the latent space, i.e. it will set high values for α_d with $d = 1, ..., N$. However, to have large entries in $\boldsymbol{\alpha}$, the algorithm sets low values for $\tilde{b}_d$, namely the terms $-\tilde{a}\sum_{d=1}^{N} \ln \tilde{b}_d$ has the same behavior of $-D_\mathrm{KL}(q(\mathbf{Z})||p(\mathbf{Z}))$ increasing in presence of only noise. Thus, the highest probability of detection is obtained using the statistical test in (6.33).

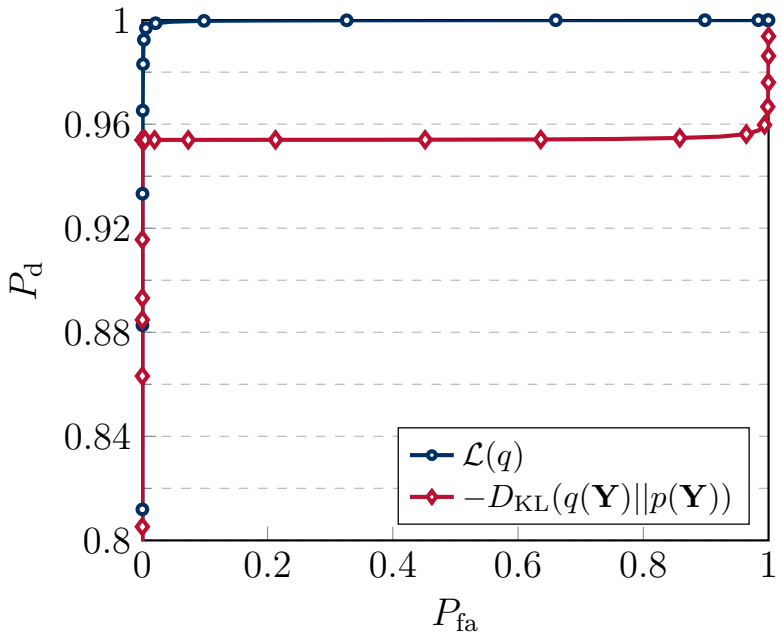

Figure 8.12: ROC curves for ELBO and Kullback-Leibler-based statistical tests setting $\mathsf{SNR} = -2\,\mathrm{dB}$. In particular, the blue curve is obtained using (6.33), while the red one is produced by employing a statistical test based on the negative Kullback-Leibler divergence $-D_{\mathrm{KL}}(q(\mathbf{Z})||p(\mathbf{Z}))$.

8.3.10 Noise Estimation Performance

The jth sensor noise power can be estimated from the approximate posterior distribution by recalling that $1/\mathbb{E}[\psi_{j,j}] = \tilde{e}_j/\tilde{v}$ in (6.18), and this leads to

$$\widehat{\sigma}_j^2 = \frac{\tilde{e}_j}{\tilde{v}} + \frac{\tilde{e}_{j+N_{\mathrm{R}}}}{\tilde{v}} \tag{8.11}$$

for $j = 1, \ldots, N_{\mathrm{R}}$.

This section investigates the performance of noise power estimation carried out using (8.11). Fig. 8.13 shows the normalized root mean square error (NRMSE) between $\widehat{\sigma}_j^2$ and σ_j^2 in three different conditions, namely, when no PU is present, and when a PU is present with $\mathsf{SNR} = -12\,\mathrm{dB}$ and $\mathsf{SNR} = 2\,\mathrm{dB}$, respectively. The simulations parameters are $N_{\mathrm{S}} = 500$,

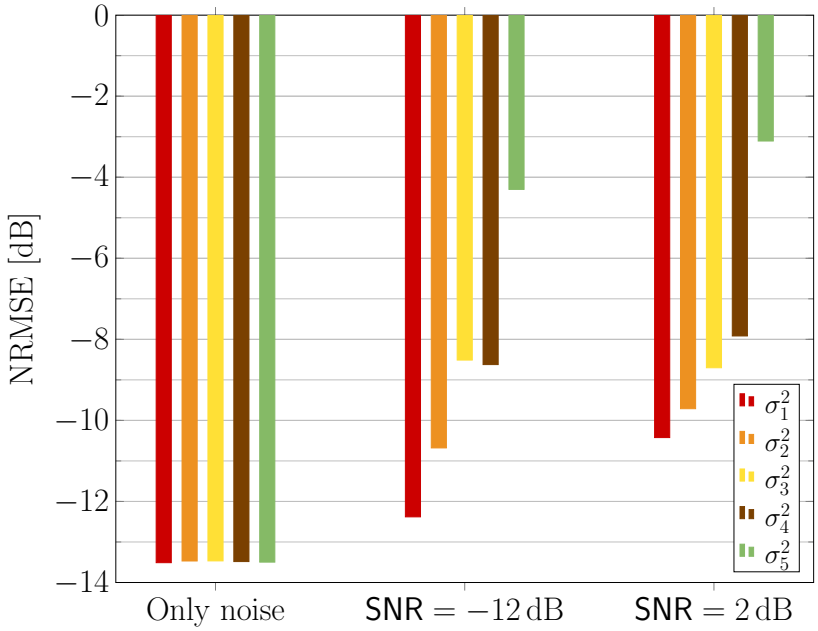

Figure 8.13: NRMSE with $N_{\mathrm{R}} = 5$, computed when a PU is present for two different SNR values and when no PU is transmitting, i.e., there is only noise. The noise powers at the sensors are indicated in ascending order as $\sigma_1^2 < \sigma_2^2 < \cdots < \sigma_5^2$.

$N_{\mathrm{R}} = 5$, and $N_{\mathrm{MC}} = 2 \times 10^4$. The NRMSE_j for the jth sensor is defined as

$$\mathrm{NRMSE}_j = \frac{1}{\sigma_j^2} \sqrt{\frac{1}{N_{\mathrm{MC}}} \sum_{i=1}^{N_{\mathrm{MC}}} \left(\widehat{\sigma}_j^2 - \sigma_j^2\right)^2}.$$

Remarkably, Fig. 8.13 illustrates that in the absence of the PU signal, the NRMSE is minimal, resulting in a high-quality estimation of the noise power of all sensors. However, as expected, the presence of the PU signal increases the NRMSE, leading to a degradation in noise power estimation performance. This is particularly evident in this specific scenario where the sensor subject to the highest noise power, σ_5^2, also experiences the highest SNR, given by $\mathsf{SNR}_{\mathrm{dB}} + \Delta\mathsf{SNR}_{\mathrm{dB}}/2$, which leads to a deterioration in noise power estimation.

8.3.11 PU Counting Performance

To conclude the analysis, we assess the performance of the estimation of the number of PUs through VBFA. For this test, we added a third PU with a normalized center frequency of $f_3 = 0.4$ and bandwidth of $B_3 = 0.3$ to the scenario. The third PU signal bandwidth overlaps by 66% with that of the first one. Hence, in the occupied frequency bins, two situations are possible: $N_{\mathrm{T,k}} = 1$ or $N_{\mathrm{T,k}} = 2$. All the three PU signals emit independent band-limited Gaussian processes mimicking the OFDM signals. They are subjected to the same nominal SNR value SNR and SNR spread $\Delta\mathsf{SNR}_{\mathrm{dB}} = 10$. In a security-related context, the occurrence of two PUs within the same frequency band may be indicative of the presence of an intentional interferer, such as a jammer, which has the potential to disrupt the primary legitimate communication.

To estimate the latent space dimension accurately, we set the stopping parameters for VBFA to $\lambda = 10^{-8}$ and $g = 1000$. The simulation is performed with $N_{\mathrm{S}} = 1000$, $N_{\mathrm{R}} = 5$, and each sensor receives the same power from each PU. Since the estimated size of the latent space might be a non-integer value, we provide the PU counting performance under two different rounding rules obtained by ceiling and floor operations, respectively. Fig. 8.14 displays the confusion matrices obtained by estimating the number of active PUs in each frequency bin. The rows represent the actual number of PUs while the columns are the estimated ones. Fig. 8.14a is obtained by applying the ceiling operation to the estimated latent space dimension, while Fig. 8.14b results from applying the floor operation. In the low SNR regime, the algorithm exhibits a bias towards the scenario where $N_{\mathrm{T},k} = 1$. This occurs because, despite maintaining good detection performance at low SNR values (e.g., at $\mathsf{SNR} = -4$, $P_{\mathrm{d}} = 1$ as shown in Fig. 8.10a), the VBFA algorithm fails to distinguish between the contributions of multiple PUs. Consequently, while the algorithm successfully detects an occupied frequency bin, it cannot accurately infer the correct dimensionality of the latent variables. In such cases, the estimated number of PUs defaults to $\hat{N}_{\mathrm{T,k}} = 1$.

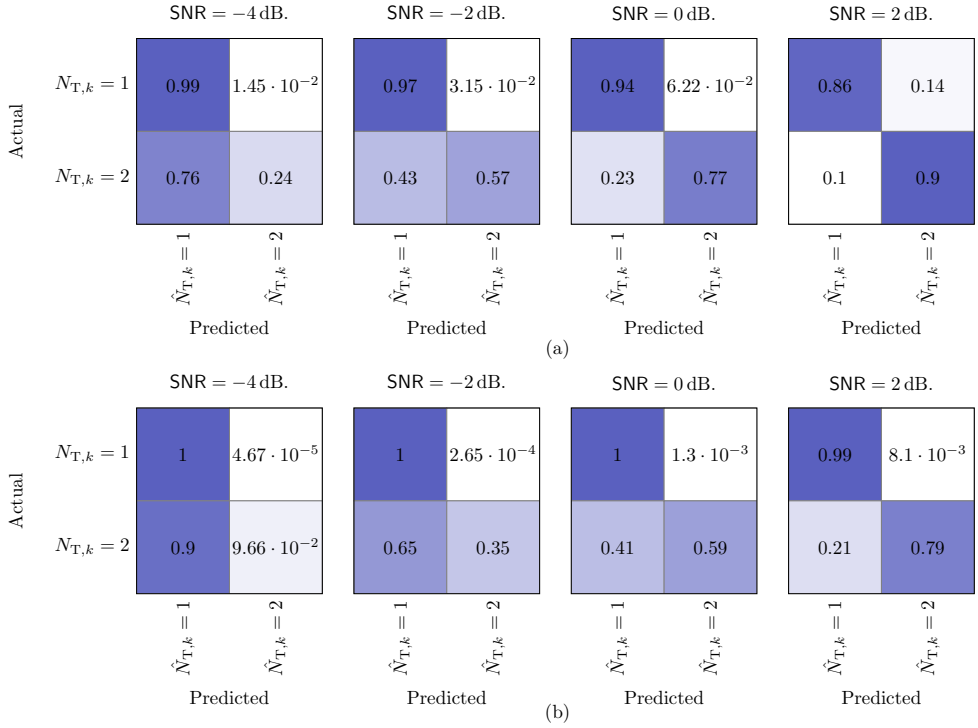

Figure 8.14: Confusion matrices for the PU counting algorithm for different SNR and rounding rules: (a) a ceiling operation is performed, i.e., $\hat{N}_{\mathrm{T,k}} = \lceil ||\mathbf{y}_{:,i}||_0/2 \rceil$; (b) a floor operation is performed, i.e., $\hat{N}_{\mathrm{T,k}} = \lfloor ||\mathbf{y}_{:,i}||_0/2 \rfloor$.

8.3.12 Computational Complexity Analysis

Both Z-transform and Fisher methods have a computational complexity of $\mathcal{O}(3N_{\mathrm{S}}N_{\mathrm{B}})$, which is mostly determined by the computation of $V_{j,k}$ in (7.3).

The complexity of the VBFA algorithm is more challenging to determine. Referring to Algorithm 5, the key complexity components are as follows:

- The computation of $\tilde{\boldsymbol{\Sigma}}_z$ has a complexity of $\mathcal{O}(8N_{\mathrm{R}}^3)$.[3]
- The update of $\boldsymbol{\mu}_z^{(i)}$, for $i = 1, \ldots, N_{\mathrm{S}}$, requires $\mathcal{O}(8N_{\mathrm{R}}^3 N_{\mathrm{S}})$.
- The computation of $\tilde{\boldsymbol{\Sigma}}_a^{(j)}$, for $j = 1, \ldots, 2N_{\mathrm{R}}$, has a complexity of $\mathcal{O}(8N_{\mathrm{R}}^3 N_{\mathrm{S}} + 16N_{\mathrm{R}}^4)$.

[3]For a matrix $A \in \mathbb{R}^{N \times N}$, the matrix inversion operation has a complexity of $\mathcal{O}(N^3)$. For matrices $A \in \mathbb{R}^{N \times M}$ and $B \in \mathbb{R}^{M \times L}$, the complexity of the multiplication AB is $\mathcal{O}(NML)$.

- The update of $\boldsymbol{\mu}_a^{(j)}$, for $j = 1, \ldots, 2N_{\mathrm{R}}$, requires $\mathcal{O}(4N_{\mathrm{R}}^2 N_{\mathrm{S}} + 8N_{\mathrm{R}}^3)$.
- The calculation of $\tilde{\mathbf{b}}$ has a complexity of $\mathcal{O}(8N_{\mathrm{R}}^3)$.
- The computation of $\tilde{\mathbf{e}}$ dominates with a complexity of $\mathcal{O}(16N_{\mathrm{R}}^4 N_{\mathrm{S}})$.

Thus, the overall complexity for each iteration is primarily dictated by the calculation of $\tilde{\mathbf{e}}$. These operations must be repeated until the ELBO converges, and this process applies across all frequency components. Therefore, the total complexity of the VBFA method is $\mathcal{O}(16N_{\mathrm{R}}^4 N_{\mathrm{S}} N_{\mathrm{B}} N_{\mathrm{iter}})$, where N_{iter} represents the number of iterations required for the convergence of the ELBO, as defined by the stopping criterion in (8.10).

Chapter 9

Conclusions

The objective of this thesis was the development of a novel framework for monitoring the RF spectrum and, when present, detecting smart jammers. The framework relies only on over-the-air signals captured by RF sensors.

Through the use of UBSS, the system effectively separated mixed over-the-air signals captured by the RF sensors, isolating traffic patterns for further analysis. The extracted traffic profiles were subjected to a causal inference methodology, enabling the accurate identification of jammers. Additionally, the patrol monitored spectrum usage by processing frequency-domain representations of received signals, detecting occupied portions of the band and estimating the number of signals present.

Lastly, a novel jamming detection algorithm is introduced for an ISAC application, where a deceptive jammer attempts to manipulate target range estimation. By leveraging the capabilities of a latent variables model, an anomaly detector is employed to distinguish between the presence of a jammer (anomalous condition) and its absence (normal condition).

Jamming Detection through Spectrum Patrol

This work demonstrated that combining an UBSS approach with a causal inference tool can be effectively utilized to detect reactive jammers.

The proposed UBSS methodology demonstrated its ability to effectively reconstruct the transmitted energy profile, even in underdetermined scenar-

ios. By accounting for the occurrence of collisions, the sparsity assumption was validated, showing that the jammer's energy profile can be accurately recovered. Moreover, numerical results confirmed that our UBSS approach surpasses the performance of existing method in the literature.

From the causal inference perspective, TE was employed. Specifically, we introduced a novel algorithm, AvOTE, which identifies the causal relationship where the combined signals from the network nodes act as the cause, and the jamming signal represents the effect. A subsequent statistical test confirms the presence of the jammer.

The overall methodology achieves excellent performance, with detection probabilities reaching up to 99% in scenarios without user packet collisions, surpassing the results of a state-of-the-art approach. A comprehensive analysis further revealed that performance degradation is primarily caused by poor source reconstruction by UBSS, which occurs in conditions of high shadowing, insufficient sensor numbers, or frequent collisions.

Jammer Detection in ISAC system

A novel framework for deceptive jamming detection in monostatic ISAC-OFDM systems was introduced. This framework leverages the received signal at the BS to detect the presence of a jammer capable of falsifying target localization. The proposed framework employs a VAE to learn a latent space representation of the echoes received from a target. Specifically, the reconstruction probability is utilized as a test statistic to detect the presence of a jammer. Our approach demonstrated significant detection performance, achieving a detection probability P_{d} of 93% for an SJR of 27 dB, and notably outperforming a properly trained conventional AE.

Cooperative WSS

Two distinct methodologies were proposed for cooperative WSS to estimate the occupancy state of multiple narrow spectrum bands within a broad bandwidth, utilizing signals collected by a network of RF sensors. The first approach applied VBFA to develop a spectrum sensing metric, which was used

in binary hypothesis testing, where the test statistic, the ELBO, was analytically derived in Chapter 6. The second approach employed a statistical technique called meta-analysis to combine detection results from all sensors, yielding a more accurate and reliable final decision.

Extensive numerical evaluations showed that both approaches substantially outperformed several state-of-the-art algorithms, achieving a detection probability P_{d} of 0.9 at a SNR of -10,dB. The performance of these methods was also tested under varying key system parameters, including the number of sensors and the number of independent observations.

Among the two, the Fisher meta-analysis approach demonstrated the highest overall performance. However, while VBFA exhibited slightly lower detection capability, it provided deeper insight into the spectrum, as it leveraged a latent variable model through factor analysis. This allowed VBFA to estimate both the noise power at each sensor and the number of PUs within each frequency bin.

Ringraziamenti

Desidero esprimere la mia sincera gratitudine al mio supervisor, il prof. Andrea Giorgetti, per il suo supporto e la sua guida durante questi anni di dottorato. La sua esperienza e i suoi consigli sono stati fondamentali per lo sviluppo del mio lavoro di ricerca.

Un ringraziamento speciale va anche a Enrico Testi, con cui ho condiviso questi tre anni di studio e lavoro. Grazie per la collaborazione, le idee e il supporto nelle fasi più complesse del mio percorso.

Bibliography

[1] Y. Li, S. Amari, A. Cichocki, D. Ho, and S. Xie, "Underdetermined blind source separation based on sparse representation," *IEEE Trans. Signal Process.*, vol. 54, no. 2, pp. 423–437, Feb. 2006.

[2] E. Testi and A. Giorgetti, "Wireless network analytics for the new era of spectrum patrolling and monitoring," *IEEE Wireless Commun.*, pp. 1–7, May 2024.

[3] A. Chakraborty, A. Bhattacharya, S. Kamal, S. R. Das, H. Gupta, and P. M. Djuric, "Spectrum patrolling with crowdsourced spectrum sensors," in *IEEE Conf. on Comp. Comm (INFOCOM)*, Honolulu, USA, Apr. 2018, pp. 1682–1690.

[4] A. Krayani, A. S. Alam, M. Calipari, L. Marcenaro, A. Nallanathan, and C. Regazzoni, "Automatic modulation classification in cognitive-iot radios using generalized dynamic bayesian networks," in *IEEE World Forum on Internet of Things (WF-IoT)*, New Orleans, LA, USA, Jul. 2021, pp. 235–240.

[5] N. Radhakrishnan, S. Kandeepan, X. Yu, and G. Baldini, "Soft fusion based cooperative spectrum prediction using LSTM," in *IEEE International Conference on Signal Processing and Communication Systems (ICSPCS)*, Sydney, Australia, Dec. 2021, pp. 1–7.

[6] A. Mariani, A. Giorgetti, and M. Chiani, "Recent advances on wideband spectrum sensing for cognitive radio," in *Cognitive Communications and Cooperative HetNet Coexistence, Signals and Communication*

Technology (M.-G. Di Benedetto and F. Bader, Eds.). Switzerland: Springer Int. Pub., 2014, ch. 1.

[7] E. Testi and A. Giorgetti, "Blind wireless network topology inference," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1109–1120, Feb. 2021.

[8] C. Zhan, H. Gupta, A. Bhattacharya, and M. Ghaderibaneh, "Efficient localization of multiple intruders in shared spectrum system," in *19th ACM/IEEE Int. Conf. on Inf. Processing in Sensor Networks (IPSN)*, Sydney, NSW, Australia, Jun. 2020, pp. 205–216.

[9] 3GPP TS 36.104, *Base Station (BS) radio transmission and reception.* 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Evolved Universal Terrestrial Radio Access (E-UTRA), 2016.

[10] D. Marabissi, S. Morosi, and L. Mucchi, "Green security in ultra-dense networks," *IEEE Trans. Veh. Technol.*, vol. 73, no. 6, pp. 8736–8749, 2024.

[11] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 98–105, Dec. 2017.

[12] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 126–132, Mar. 2020.

[13] D. Marabissi, L. Mucchi, and S. Casini, "Physical-layer security metric for user association in ultra-dense networks," in *Int. Conf. on Computing, Networking and Comm. (ICNC)*, Big Island, HI, USA, Feb. 2020, pp. 487–491.

[14] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, April 2011.

[15] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, Dec. 2009.

[16] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. of the ACM Int. symp. on Mobile ad hoc netw. and comp.*, Urbana-Champaign, IL, USA, May 2005.

[17] T. Perković, H. Rudeš, S. Damjanović, and A. Nakić, "Low-cost implementation of reactive jammer on LoraWan network," *Electronics*, vol. 10, no. 7, Apr. 2021.

[18] L. Xiao, C. Xie, M. Min, and W. Zhuang, "User-centric view of unmanned aerial vehicle transmission against smart attacks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3420–3430, Apr. 2018.

[19] A. Dutta and M. Chiang, ""See something, say something" crowdsourced enforcement of spectrum policies," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 67–80, Aug. 2016.

[20] J. Li, J. Xu, W. Liu, S. Gong, and K. Zeng, "Robust optimal spectrum patrolling for passive monitoring in cognitive radio networks," in *IEEE Int. Conf. on Comp. and Inf. Tech. (CIT)*, Helsinki, Finland, Aug. 2017, pp. 63–68.

[21] H. Shokri-Ghadikolaei, F. Boccardi, C. Fischione, G. Fodor, and M. Zorzi, "Spectrum sharing in mmWave cellular networks via cell association, coordination, and beamforming," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 11, pp. 2902–2917, Nov. 2016.

[22] W. S. H. M. W. Ahmad, N. A. M. Radzi, F. Samidi, A. Ismail, F. Abdullah, M. Z. Jamaludin, and M. Zakaria, "5G technology: Towards dynamic spectrum sharing using cognitive radio networks," *IEEE Access*, vol. 8, pp. 14 460–14 488, Jan. 2020.

[23] D. Uvaydov, S. D'Oro, F. Restuccia, and T. Melodia, "Deepsense: Fast wideband spectrum sensing through real-time in-the-loop deep learning," in *IEEE Conf. on Comp. Comm. (INFOCOM)*, Vancouver, Canada, May 2021, pp. 1–10.

[24] A. Rabbachin, T. Q. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 480–493, Feb. 2011.

[25] L. Arcangeloni, E. Testi, and A. Giorgetti, "Detection of jamming attacks via source separation and causal inference," *IEEE Trans. Commun.*, vol. 71, no. 8, pp. 4793–4806, Aug. 2023.

[26] A. Tani, D. Marabissi, and R. Fantacci, "Facing the SNR wall detection in full duplex cognitive radio networks using a GLRT multipath-based detector," *IEEE Trans. Wireless Commun.*, vol. 21, no. 5, pp. 3116–3130, May 2022.

[27] A. Gorcin and H. Arslan, "Signal identification for adaptive spectrum hyperspace access in wireless communications systems," *IEEE Commun. Mag.*, vol. 52, no. 10, pp. 134–145, Oct. 2014.

[28] T. V. Nguyen, H. Shin, T. Q. S. Quek, and M. Z. Win, "Sensing and probing cardinalities for active cognitive radios," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1833–1848, Apr. 2012.

[29] G. Caso, L. D. Nardis, O. Holland, and M.-G. D. Benedetto, "Impact of spatio-temporal correlation in cooperative spectrum sensing for mobile cognitive radio networks," in *The Tenth Int. Symp. on Wireless Comm. Systems (ISWCS)*, Ilmenau, Germany, Aug. 2013, pp. 1–5.

[30] L. De Nardis, D. Domenicali, and M.-G. Di Benedetto, "Clustered hybrid energy-aware cooperative spectrum sensing (chess)," in *4th Int. Conf. on Cognitive Radio Oriented Wireless Networks and Comm.*, Hanover, Germany, Jun. 2009, pp. 1–6.

[31] G. Caso, L. De Nardis, G. C. Ferrante, and M.-G. Di Benedetto, "Cooperative spectrum sensing based on majority decision under CFAR and CDR constraints," in *IEEE 24th Int. Symp. on Personal, Indoor and Mobile Radio Comm. (PIMRC Workshops)*, London, UK, Sep. 2013, pp. 51–55.

[32] H. Ma, X. Yuan, L. Zhou, B. Li, and R. Qin, "Joint block support recovery for sub-nyquist sampling cooperative spectrum sensing," *IEEE Wireless Commun. Lett.*, vol. 12, no. 1, pp. 85–88, Jan. 2023.

[33] J. Wu, M. Su, L. Qiao, X. Xu, X. Liang, H. Wang, J. Bao, and W. Cao, "Quick parallel cooperative spectrum sensing in cognitive wireless sensor networks," *IEEE Sensors Letters*, vol. 8, no. 8, pp. 1–4, Aug 2024.

[34] A. Mariani, A. Giorgetti, and M. Chiani, "Wideband spectrum sensing by model order selection," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6710–6721, Dec. 2015.

[35] C. Zhang, L. Wang, R. Jiang, J. Hu, and S. Xu, "Radar jamming decision-making in cognitive electronic warfare: A review," *IEEE Sensors J.*, vol. 23, no. 11, pp. 11 383–11 403, Jun. 2023.

[36] J. A. Zhang, M. L. Rahman, K. Wu, X. Huang, Y. J. Guo, S. Chen, and J. Yuan, "Enabling joint communication and radar sensing in mobile networks—a survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 306–345, 2022.

[37] T. Wild, V. Braun, and H. Viswanathan, "Joint design of communication and sensing for beyond 5G and 6G systems," *IEEE Access*, vol. 9, pp. 30 845–30 857, Feb. 2021.

[38] Z. Huang, K. Wang, A. Liu, Y. Cai, R. Du, and T. X. Han, "Joint pilot optimization, target detection and channel estimation for integrated sensing and communication systems," *IEEE Trans. Wireless Commun.*, vol. 21, no. 12, pp. 10 351–10 365, Dec. 2022.

[39] E. Favarelli, E. Matricardi, L. Pucci, W. Xu, E. Paolini, and A. Giorgetti, "Sensor fusion and resource management in MIMO-OFDM joint sensing and communication," *arXiv preprint arXiv:2312.07379*, 2023.

[40] L. Pucci, E. Paolini, and A. Giorgetti, "System-level analysis of joint sensing and communication based on 5G new radio," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 7, pp. 2043–2055, Mar. 2022.

[41] A. Mariani, A. Giorgetti, and M. Chiani, "Effects of noise power estimation on energy detection for cognitive radio applications," *IEEE Trans. Commun.*, vol. 59, no. 12, pp. 3410–3420, Dec. 2011.

[42] C. Cordeiro, K. S. Challapali, D. Birru, and N. Sai Shankar, "IEEE 802.22: An introduction to the first wireless standard based on cognitive radios." *Journal of Commun.*, vol. 1, no. 1, pp. 38–47, Apr. 2006.

[43] X. Yu, D. Hu, and J. Xu, *Blind Source Separation: Theory and Applications*, 1st ed. Wiley Publishing, 2014.

[44] M. Joho, H. Mathis, and R. H. Lambert, "Overdetermined blind source separation: using more sensors than source signals in a noisy mixture," in *Int. Conf. on Indep. Comp. Analysis and Blind Signal Sep. (ICA)*, Helsinki, Finland, Jun 2000, pp. 81–86.

[45] S. Choi and A. Cichocki, "Adaptive blind separation of speech signals: Cocktail party problem," in *Int. Conf. on speech processing*, Dec. 1997, pp. 617–622.

[46] A. Cichocki, R. Zdunek, and S. Amari, "New algorithms for non-negative matrix factorization in applications to blind source separation," in *IEEE Int. Conf. on Acoustics Speech and Sig. Processing Proceedings*, vol. 5, Toulouse, France, June 2006.

[47] A. Cichocki, D. Mandic, L. De Lathauwer, G. Zhou, Q. Zhao, C. Caiafa, and H. A. Phan, "Tensor decompositions for signal processing applications: From two-way to multiway component analysis," *IEEE Signal Process. Mag.*, vol. 32, no. 2, pp. 145–163, 2015.

[48] G. Ivkovic, P. Spasojevic, and I. Seskar, "Localization of packet based radio transmitters in space, time, and frequency," in *Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, Nov. 2008, pp. 288–292.

[49] O. Yilmaz and S. Rickard, "Blind separation of speech mixtures via time-frequency masking," *IEEE Trans. Signal Process.*, vol. 52, no. 7, pp. 1830–1847, Jul. 2004.

[50] F. Abrard and Y. Deville, "A time–frequency blind signal separation method applicable to underdetermined mixtures of dependent sources," *Signal processing*, vol. 85, no. 7, pp. 1389–1403, Feb 2005.

[51] I. T. Jolliffe, *Principal Component Analysis.* New York: Springer-Verlag, 2002.

[52] K. Qian, Y. Wang, P. Jung, Y. Shi, and X. X. Zhu, "Basis pursuit denoising via recurrent neural network applied to super-resolving SAR tomography," *IEEE Trans. Geosci. Remote Sens.*, vol. 60, pp. 1–15, Dec. 2022.

[53] D. L. Donoho and M. Elad, "Maximal sparsity representation via l1 minimization," *Proc. Nat. Aca. Sci*, vol. 100, no. 5, pp. 2197–2202, 2003.

[54] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.

[55] A. M. Tillmann and M. E. Pfetsch, "The computational complexity of the restricted isometry property, the nullspace property, and related concepts in compressed sensing," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1248–1259, Feb. 2014.

[56] D. L. Donoho and M. Elad, "Optimally sparse representation in general (nonorthogonal) dictionaries via l^1 minimization," in *Proc. of the Na-*

tional Academy of Sciences, vol. 100, no. 5. National Acad Sciences, Feb. 2003, pp. 2197–2202.

[57] S. Amuru and R. M. Buehrer, "Optimal jamming against digital modulation," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2212–2224, Oct 2015.

[58] Y. Shi, X. Lu, Y. Li, and K. An, "Active detection for symbol-level jamming," *IEEE Trans. Wireless Commun.*, pp. 1–1, May 2024.

[59] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of reactive jamming in DSSS-based wireless communications," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1593–1603, Mar. 2014.

[60] M. Strasser, B. Danev, and S. Čapkun, "Detection of reactive jamming in sensor networks," *ACM Trans. on Sensor Netw. (TOSN)*, vol. 7, no. 2, pp. 1–29, Aug. 2010.

[61] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," in *IEEE Int. Conf. on Localization and GNSS (ICL-GNSS)*, Gothenburg, Sweden, Jun. 2015, pp. 1–6.

[62] H. Akhlaghpasand, S. M. Razavizadeh, E. Björnson, and T. T. Do, "Jamming detection in massive MIMO systems," *IEEE Commun. Lett.*, vol. 7, no. 2, pp. 242–245, Apr. 2018.

[63] M. O. Mughal, K. Dabcevic, L. Marcenaro, and C. S. Regazzoni, "Compressed sensing based jammer detection algorithm for wide-band cognitive radio networks," in *Int. Work. on Compr. Sens. Theory and its Appl. to Radar, Sonar and Remote Sensing (CoSeRa)*, Pisa, Italy, Jun. 2015, pp. 119–123.

[64] H. B. Salameh, S. Otoum, M. Aloqaily, R. Derbas, I. Al Ridhawi, and Y. Jararweh, "Intelligent jamming-aware routing in multi-hop IoT-based opportunistic cognitive radio networks," *Ad Hoc Networks*, vol. 98, p. 102035, Mar. 2020.

[65] X. Wang, J. Wang, Y. Xu, J. Chen, L. Jia, X. Liu, and Y. Yang, "Dynamic spectrum anti-jamming communications: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 79–85, Feb. 2020.

[66] S. Gecgel, C. Goztepe, and G. K. Kurt, "Jammer detection based on artificial neural networks: A measurement study," in *Proc. of the ACM Work. on Wireless Sec. and Machine Learning (WiseML 2019)*, Miami, USA, May 2019, pp. 43–48.

[67] S. Gecgel and G. K. Kurt, "Intermittent jamming against telemetry and telecommand of satellite systems and a learning-driven detection strategy," in *Proc. of the ACM Work. on Wireless Sec. and Machine Learning (WiseML 2021)*, Abu Dhabi, United Arab Emirates, Jun. 2021, pp. 43–48.

[68] K. G.S, J. Ansh, and S. Jagdeep, "Detection and classification of radio frequency jamming attacks using machine learning," in *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 11, no. 4, Dec. 2020, pp. 49–62.

[69] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi, and N. Kaabouch, "A novel jamming attacks detection approach based on machine learning for wireless communication," in *IEEE Int. Conference on Information Networking (ICOIN)*, Barcelona, Spain, Jan. 2020, pp. 459–464.

[70] S. Ujan, M. Same, and R. Landry, "A robust jamming signal classification and detection approach based on multi-layer perceptron neural network," *Int. Journal of Research Studies in Comp. Science and Engineering (IJRSCSE)*, vol. 7, pp. 1–12, Mar. 2020.

[71] T. Nawaz, D. Campo, M. O. Mughal, L. Marcenaro, and C. S. Regazzoni, "Jammer detection algorithm for wide-band radios using spectral correlation and neural networks," in *Int. Wireless Comm. and Mobile Comp. Conf. (IWCMC)*, Valencia, Spain, Jun. 2017, pp. 246–251.

[72] P. Sharma, D. J. Bucci, S. K. Brahma, and P. K. Varshney, "Communication network topology inference via transfer entropy," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 562–575, Jan. 2019.

[73] J. Massey, "Causality, feedback and directed information," in *Proc. Int. Symp. Inf. Theory Applic.(ISITA-90)*, Waikiki, Hawaii, Nov. 1990, pp. 303–305.

[74] T. Schreiber, "Measuring information transfer," *Physical review letters*, vol. 85, no. 2, p. 461, Jul. 2000.

[75] A. Elzanaty, A. Giorgetti, and M. Chiani, "Limits on sparse data acquisition: RIC analysis of finite Gaussian matrices," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1578–1588, Mar. 2019.

[76] J. Peters, D. Janzing, and B. Schölkopf, *Elements of causal inference: foundations and learning algorithms*. The MIT Press, 2017.

[77] C. W. Granger, "Investigating causal relations by econometric models and cross-spectral methods," *Econometrica: journal of the Econometric Society*, vol. 37, no. 3, pp. 424–438, Jul. 1969.

[78] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, Jun. 2022.

[79] H. Huang, Y. Zhang, H. Zhang, C. Zhang, and Z. Han, "Illegal intelligent reflecting surface based active channel aging: When jammer can attack without power and CSI," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 11 018–11 022, Aug 2023.

[80] H. Huang, H. Zhang, W. Mei, J. Li, Y. Cai, A. L. Swindlehurst, and Z. Han, "Integrated sensing and communication under DISCO physical-layer jamming attacks," *arXiv preprint arXiv:2404.07477*, Apr. 2024.

[81] J. Xu, D. Li, Z. Zhu, Z. Yang, N. Zhao, and D. Niyato, "Anti-jamming design for integrated sensing and communication via aerial IRS," *IEEE Trans. Commun.*, pp. 1–1, Mar. 2024.

[82] N. Su, F. Liu, and C. Masouros, "Sensing-assisted eavesdropper estimation: An ISAC breakthrough in physical layer security," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 3162–3174, Apr. 2024.

[83] M. Greco, F. Gini, and A. Farina, "Radar detection and classification of jamming signals belonging to a cone class," *IEEE Trans. Signal Process.*, vol. 56, no. 5, pp. 1984–1993, May 2008.

[84] S. Zhao, Y. Zhou, L. Zhang, Y. Guo, and S. Tang, "Discrimination between radar targets and deception jamming in distributed multiple-radar architectures," *IET Radar, Sonar & Navigation*, vol. 11, no. 7, pp. 1124–1131, Jul. 2017.

[85] C. Xu, L. Yu, Y. Wei, and P. Tong, "Research on active jamming recognition in complex electromagnetic environment," in *IEEE Int. Conf. on Signal, Inf. and Data Processing (ICSIDP)*, Chongqing, China, Dec. 2019, pp. 1–5.

[86] X. Wang, G. Zhang, X. Wang, Q. Song, and F. Wen, "ECCM schemes against deception jamming using OFDM radar with low global PAPR," *Sensors*, vol. 20, no. 7, p. 2071, Apr. 2020.

[87] J. Sun, Y. Yuan, M. S. Greco, F. Gini, and W. Yi, "Anti-deception jamming power optimization strategy for multi-target tracking tasks in multi-radar systems," in *IEEE Int. Conf. on Acoustics, Speech and Signal Proc. (ICASSP)*. Seoul, Korea: IEEE, Apr. 2024, pp. 8941–8945.

[88] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," *arXiv preprint arXiv:1312.6114*, 2013.

[89] J. An and S. Cho, "Variational autoencoder based anomaly detection using reconstruction probability," *Special lecture on IE*, vol. 2, no. 1, pp. 1–18, 2015.

[90] H. Xu, W. Chen, N. Zhao, Z. Li, J. Bu, Z. Li, Y. Liu, Y. Zhao, D. Pei, Y. Feng *et al.*, "Unsupervised anomaly detection via variational auto-encoder for seasonal kpis in web applications," in *World Wide Web Conference (WWW)*, Lyon, France, Apr. 2018, pp. 187–196.

[91] D. Zimmerer, S. A. Kohl, J. Petersen, F. Isensee, and K. H. Maier-Hein, "Context-encoding variational autoencoder for unsupervised anomaly detection," *arXiv preprint arXiv:1812.05941*, 2018.

[92] R. Yao, C. Liu, L. Zhang, and P. Peng, "Unsupervised anomaly detection using variational auto-encoder based feature extraction," in *IEEE Int. Conf. on Prognostics and Health Management (ICPHM)*, San Francisco, CA, USA, Jun. 2019, pp. 1–7.

[93] M. D. Hoffman, D. M. Blei, C. Wang, and J. Paisley, "Stochastic variational inference," *Journal of Machine Learning Research*, vol. 14, no. 40, pp. 1303–1347, May 2013.

[94] C. M. Bishop, *Pattern Recognition and Machine Learning*. Springer Verlag, Aug. 2006.

[95] D. M. Blei, A. Kucukelbir, and J. D. McAuliffe, "Variational inference: A review for statisticians," *Journal of the American statistical Association*, vol. 112, no. 518, pp. 859–877, Jul. 2017.

[96] E. Hanafi, P. A. Martin, P. J. Smith, and A. J. Coulson, "On the distribution of detection delay for quickest spectrum sensing," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 502–510, Feb. 2016.

[97] R. Senanayake, P. J. Smith, P. A. Dmochowski, A. Giorgetti, and J. S. Evans, "Mixture detectors for improved spectrum sensing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 4335–4348, Mar. 2020.

[98] P. J. Smith, R. Senanayake, P. A. Dmochowski, and J. S. Evans, "Distributed spectrum sensing for cognitive radio networks based on the sphericity test," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 1831–1844, Mar. 2019.

[99] K. M. Thilina, K. W. Choi, N. Saquib, and E. Hossain, "Machine learning techniques for cooperative spectrum sensing in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2209–2221, Nov. 2013.

[100] P. B. Gohain, S. Chaudhari, and V. Koivunen, "Cooperative energy detection with heterogeneous sensors under noise uncertainty: SNR wall and use of evidence theory," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 4, no. 3, pp. 473–485, Sep. 2018.

[101] Y. Wang and G. Zhang, "Compressed wideband spectrum sensing based on discrete cosine transform," *The Scientific World Journal*, vol. 2014, pp. 1–5, Jan. 2014.

[102] Y. Ma, Y. Gao, Y.-C. Liang, and S. Cui, "Reliable and efficient sub-nyquist wideband spectrum sensing in cooperative cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2750–2762, Oct. 2016.

[103] H. Sun, A. Nallanathan, S. Cui, and C.-X. Wang, "Cooperative wideband spectrum sensing over fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1382–1394, Mar. 2016.

[104] G. Morghare and S. S. Bhadauria, "Wideband spectrum compressive sensing technique in cognitive radio networks," in *Proc. of Int. Conf. on Comm. and Computational Technologies (ICCCT)*. Springer, Feb. 2022, pp. 1–16.

[105] A. Elzanaty, A. Giorgetti, and M. Chiani, "Lossy compression of noisy sparse sources based on syndrome encoding," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 7073–7087, Oct. 2019.

[106] H. Wang, J. Fang, H. Duan, and H. Li, "Compressive wideband spectrum sensing and signal recovery with unknown multipath channels," *IEEE Trans. Wireless Commun.*, vol. 21, no. 7, pp. 5305–5316, Jul. 2022.

[107] R. Zhao, Y. Ruan, and Y. Li, "Cooperative time-frequency localization for wideband spectrum sensing with a lightweight detector," *IEEE Commun. Lett.*, vol. 27, no. 7, pp. 844–1848, Jul. 2023.

[108] Ł. Kułacz and A. Kliks, "Federated learning-based spectrum occupancy detection," *Sensors*, vol. 23, no. 14, p. 6436, Jul. 2023.

[109] R. Mei and Z. Wang, "Deep learning-based wideband spectrum sensing: A low computational complexity approach," *IEEE Commun. Lett.*, vol. 27, no. 10, pp. 2633–2637, Oct. 2023.

[110] ——, "Compressed spectrum sensing of sparse wideband signals based on deep learning," *IEEE Trans. Veh. Technol.*, pp. 1–11, Jan. 2024.

[111] N. A. Khalek and W. Hamouda, "Deepsense: An unsupervised deep clustering approach for cooperative spectrum sensing," in *IEEE Int. Conf. on Comm. (ICC)*, Rome, Italy, Jun. 2023.

[112] S. Roweis and Z. Ghahramani, "A unifying review of linear Gaussian models," *Neural computation*, vol. 11, no. 2, pp. 305–345, Feb. 1999.

[113] C. Bishop, "Variational principal components," in *Proc. Ninth Int. Conf. on Artificial Neural Networks, ICANN.* Edinburgh, UK: IEE, Sep. 1999, pp. 509–514.

[114] S. Bazaou, O. Winther, and L. K. Hansen, "Variational bayes latent variable models and mixture extensions," Master's thesis, Technical University of Denmark (DTU), Lyngby, Denmark, 2004.

[115] F. B. Nielsen, O. Winther, and L. K. Hansen, "Variational approach to factor analysis and related models," Master's thesis, Citeseer, 2004.

[116] G. Parisi, *Statistical Field Theory.* Basic Books, 1988.

[117] A. Bhattacharya, A. Chakraborty, S. R. Das, H. Gupta, and P. M. Djurić, "Spectrum patrolling with crowdsourced spectrum sensors," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 6, no. 1, pp. 271–281, Mar. 2020.

[118] R. A. Fisher, *Statistical methods for research workers.* Edinburgh,U.K.: Oliver & Boyd, 1925.

[119] H. A. David and H. N. Nagaraja, *Order statistics*, 3rd ed. John Wiley & Sons, Aug. 2003.

[120] W. A. Wallis, "Compounding probabilities from independent significance tests," *Econometrica, J. of the Econometric Society*, vol. 10, pp. 229–248, Oct. 1942.

[121] M. C. Whitlock, "Combining probability from independent tests: the weighted z-method is superior to Fisher's approach," *J. Evol. Biol.*, vol. 18, no. 5, pp. 1368–1373, Sep. 2005.

[122] S. A. Stouffer, E. A. Suchman, L. C. DeVinney, S. A. Star, and R. M. Williams Jr, *The american soldier: Adjustment during army life.* New Jersey, USA: Princeton Univ. Press, 1949, vol. 1.

[123] M. Chiani and A. Elzanaty, "On the LoRa modulation for IoT: Waveform properties and spectral analysis," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8463–8470, Oct. 2019.

[124] N. Sornin and A. Yegin, "Lorawan^{TM} 1.1 specification," *LoRa Alliance*, pp. 1–101, Oct. 2017.

[125] LoRa Alliance. (2020) RP002-1.0.2 LoRaWAN® Regional Parameters. [Online]. Available: https://lora-alliance.org/resource_hub/rp2-102-lorawan-regional-parameters/

[126] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A study of LoRa: Long range & low power networks for the Internet of things," *Sensors*, vol. 16, no. 9, p. 1466, Sep. 2016.

[127] C. Xiyuan, Z. Wei, and W. Shilian, "Blind source separation anti-jamming technology based on pade-fastica algorithm," in *IEEE Int. Conf. on Communication Technology (ICCT)*, Nanning, China, Oct. 2020, pp. 1179–1183.

[128] A. M. Bruckstein, D. L. Donoho, and M. Elad, "From sparse solutions of systems of equations to sparse modeling of signals and images," *SIAM review*, vol. 51, no. 1, pp. 34–81, Mar. 2009.

[129] J. T. Lizier, "JIDT: An information-theoretic toolkit for studying the dynamics of complex systems," *Frontiers in Robotics and AI*, vol. 1, p. 11, Dec. 2014.

[130] 5G, NR, *Physical Channels and Modulation.* 3GPP, Jul. 2020, vol. version 16.2.0 Release 16.

[131] C. Doersch, "Tutorial on variational autoencoders," *arXiv preprint arXiv:1606.05908*, 2016.

[132] H. Ochiai and H. Imai, "On the distribution of the peak-to-average power ratio in OFDM signals," *IEEE Trans. Commun.*, vol. 49, no. 2, pp. 282–289, Feb. 2001.