Detection of Jamming Attacks via Source Separation and Causal Inference

Luca Arcangeloni, *Graduate Student Member, IEEE*, Enrico Testi, *Member, IEEE*, and Andrea Giorgetti, *Senior Member, IEEE*

***Abstract*— 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 radio-frequency (RF) sensors external to the network to be protected. The solution relies on two key components: i) a novel underdetermined blind source separation (UBSS) method that, starting from the signal mixtures observed by the RF patrollers, is capable of separating the jamming temporal profile from the network nodes' transmission profiles; ii) a new jamming detection based on causal inference called all-versus-one transfer entropy (AvOTE). The framework is then applied to a case study where the victim network is a Long Range (LoRa)-based internet of things (IoT) system with star topology. The solution outperforms a state-of-the-art method and an approach that attempts to find the causal relationship via time series correlation, exhibiting very good performance in the presence of shadowing. Indeed, a detection probability of 90% is achieved with a false alarm probability of 6% in the presence of nuisances such as collisions and severe shadowing.**

***Index Terms*— Blind source separation, causal inference, jamming detection, transfer entropy, wireless networks.**

I. Introduction

PRIVATE information and sensitive data rely heavily on the network infrastructure's security. This aspect is becoming of paramount importance in several applications such as industrial IoT, remote e-health, and V2X communications, where the wireless medium conveys critical data. To further exacerbate the problem, the upcoming artificial intelligence (AI) revolution, while making intelligent and efficient devices on one side, may lead to a much more vulnerable technology on the other [1], [2], [3].

Considering the different security threats of wireless networks, we distinguish between passive (i.e., eavesdropping) and active attacks [4]. 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. DoS attacks are even more harmful when aimed at networks that adopt cognitive paradigms of dynamic reuse of the radio spectrum. Systems operating in industrial, scientific and medical (ISM) bands or shared commercial bands (e.g., 5G systems in Citizens Broadband Radio Service (CBRS)) foresee techniques of intelligent reuse of the spectrum in which legitimate users are authorized to communicate based on the spectrum availability, becoming extremely vulnerable to interferers [5].

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, the deceptive jammer that mimics the behavior of a legitimate user, and the reactive (smart) jammer capable of detecting ongoing communications via spectrum sensing and opportunistically interfere them [6], [7]. 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 software-defined radio, developing new techniques to counteract such attackers is now of paramount importance [8], [9].

In this scenario, a solution that recently has been proposed makes use of a spectrum patrol to enforce security of a wireless network [3], [10], [11], [12]. 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. 1. The patrollers can pair the information received by the legitimate users and e.g., the access points (APs) or the base stations (BSs) when available, with the ones extracted from the spectrum analysis to detect the presence of a jammer. Then, such information can be forwarded to the authority (and, e.g., the network of legitimate users) that will take the necessary actions to counteract the jammer. However, due to the covert nature of smart jammers that intelligently turn themself off when a communication is not taking place, most of the spectrum sensing techniques developed in the last two decades cannot be applied. This is because when the smart jammer transmits, it does so in the presence of legitimate communication; hence, discriminating between the two transmissions is very challenging. Therefore, in this work, we propose a new framework for detecting

Manuscript received 18 November 2022; revised 11 April 2023; accepted 17 May 2023. Date of publication 30 May 2023; date of current version 16 August 2023. This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART"). The associate editor coordinating the review of this article and approving it for publication was L. Xiao. *(Corresponding author: Andrea Giorgetti.)*

The authors are with the Department of Electrical, Electronic, and Information Engineering "Guglielmo Marconi" (DEI), CNIT, University of Bologna, 40126 Bologna, Italy (e-mail: luca.arcangeloni2@unibo.it; enrico.testi@unibo.it; andrea.giorgetti@unibo.it).

This article has supplementary material provided by the authors and color versions of one or more figures available at https://doi.org/10.1109/TCOMM.2023.3281467.

Digital Object Identifier 10.1109/TCOMM.2023.3281467

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

smart jammers via causal inference using a patrol of RF sensors, leveraging the cause-and-effect relationship between the jammer and the network of legitimate users.

A. Existing Works

In the last decade, several jamming detection schemes have been proposed. In [13], a network node compares its packet delivery ratio (PDR), the bad packet ratio (BPR), i.e., the ratio between the number of erroneous packets and received packets, and the energy consumption, with a threshold. In [14], 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 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 [15], 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 fading 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 [16], 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 [17], the authors study the physical layer security of a pilot-based massive multiple-input multiple-output (MIMO) system proposing a generalized likelihood ratio test (GLRT). In [18], the authors present an algorithm for jammer detection in wide-band cognitive radio networks based on compressed sensing (CS) and energy detector (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 (PSD) 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 [19], the authors propose three classifiers, namely K-nearest neighbors (K-NN), random forest, and Bayesian classifier to detect a proactive jammer. In [20], 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 [21], two neural networks (NNs) are proposed to detect and classify a jammer in orthogonal frequency division multiplexing (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 [22] to an OFDM-based satellite communication system. Both detection and classification are also performed in [23] 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 [24], a large dataset with signal features that identify jamming signals is generated. Then, random forest, support vector machine (SVM) and a NN are tested in a wireless communication network using this dataset for training. In [25], a multi-layer perceptron NN is used to classify and detect a jammer attempting to interfere DVB-S2 signals. In [26], 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.

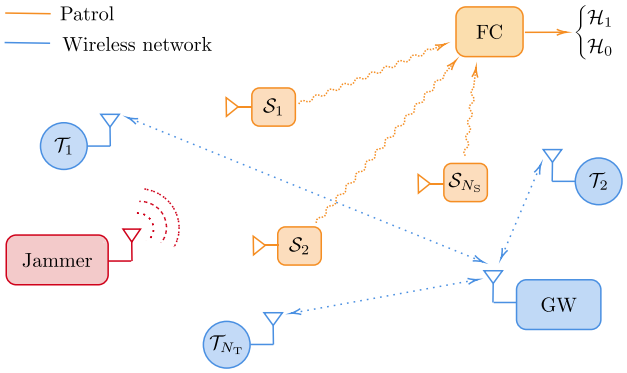


Fig. 1. A wireless network under attack by a jammer. A patrol composed of RF sensors monitors the spectrum by sharing information with a fusion center (FC) that performs jamming detection.

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 [14], the prior knowledge of the first few jamming-free bits in the preamble is assumed, while in [15] 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 [21] and [22]), then a change in the format will require a brand new training procedure. Table I summarizes and categorizes all the mentioned existing works.

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 [10], [11]. In [10], the authors address a collaborative signal detection problem in which they aim to identify the

TABLE I
COMPARISON AND KEY ASPECTS OF EXISTING DETECTORS

Category	Ref.	Key aspects
Conventional techniques	[13], [14] [15], [16] [17]	• Implemented at the receiver side • Demodulation of the signal • Bit error checking • Knowledge of the communication details
Cognitive radio	[18], [19] [20]	• Database with jamming information • Proactive jammers • Implemented at the receiver side
ML-based approaches	[21], [22] [23], [24] [25], [26]	• Knowledge of the communication details • Large dataset for training • Dependence on the training signal • Common features: RSS and PDR

optimal subset of sensors and their configurations to maximize the detection performance given certain resource limitations. In [11], 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.

B. Our Contribution

In this context, 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; such profiles retain information on the temporal behavior of the nodes without requiring demodulation. After this preprocessing stage, the solution performs blind source separation (BSS) to separate the energy profiles transmitted by each node of the network and the jammer.[1] In particular, we propose a novel solution to the UBSS problem, which includes substantial changes to the approach presented in [27] to be tailored for the specific needs. After the signal separation, we explore the temporal relation between the signals emitted by the nodes to detect the presence of an intruder. If the jammer is reactive, it transmits only after detecting the transmission of a legitimate user. Such behavior can be modeled via a causal relationship in which the user is the cause, and the jammer is the effect. Hence, we aim to detect the presence of the jammer by finding such a relationship using causal inference tools [28]. For this purpose, we propose a novel jamming detection methodology based on *directed information*, a metric that quantifies the causal relationship between time series introduced in [29] and reinvented in [30] with the name transfer entropy (TE).

In summary, the contributions of this work are the following:

- We introduce a novel framework for reactive jamming detection based on a patrol of RF sensors external to the network to be protected.
- The solution requires sensors to collect only raw measurements consisting of the received power calculated over short time intervals.
- The framework is blind, meaning that most network features are unknown (i.e., the number of nodes, their position, the type of traffic, and the communication protocol), and all the operations are carried out without demodulating the received signals.
- A first key ingredient is a novel UBSS method that, starting from the signal mixtures observed by the RF patrollers, allows estimating the number of nodes of the wireless network and reconstructing their transmitted energy profiles.
- The second key element is a new jamming attack detection based on causal inference called AvOTE.
- We thoroughly analyze a case study where the victim network is a LoRa-based IoT network with star topology.

Throughout the paper, capital and lowercase boldface letters denote matrices and vectors, respectively, $(\cdot)^{\mathsf{T}}$ stands for transposition, $\|\cdot\|_p$ is the l_p-norm, $|\cdot|$ is the absolute value, and $\otimes$ stands for Kronecker product. 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 $\mathbf{V}$; 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, and $\mathbf{V}_{:,j:k}$ correspond to a sub-matrix of $\mathbf{V}$ composed by the columns from jth to kth, extremes included. We use $x \sim \mathcal{N}(\mu, \sigma^2)$ to denote a Gaussian random variable (r.v.) with mean μ and variance σ^2, $z \sim \mathcal{CN}(0, \sigma^2)$ to denote a zero-mean circularly symmetric complex Gaussian r.v. with variance σ^2, $\mathbb{E}[\cdot]$ to denote the expectation operator, and $\langle\cdot\rangle$ to indicate the sample mean operator. $\mathbb{1}_{\{\mathcal{A}\}}$ is the indicator function equal to one when $\mathcal{A}$ is true and zero otherwise.

The remainder of this paper is organized as follows. We introduce the scenario and system model in Section II. Section III presents the UBSS method adopted by the patroller to separate the signals. In Section IV, a novel jamming detection algorithm based on TE is proposed. Numerical results are given in Section V. Conclusions are drawn in Section VI.

II. SYSTEM OVERVIEW

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_{S}, respectively. All the actors, namely the nodes, the sensors and the jammer are randomly deployed on a two-dimensional area. As further detailed in Section V, the proposed methodology tolerates the presence of collisions between the packets transmitted by the nodes.

[1] Since at this stage we do not know if the jammer is present, its transmission is treated without distinction from legitimate communications.

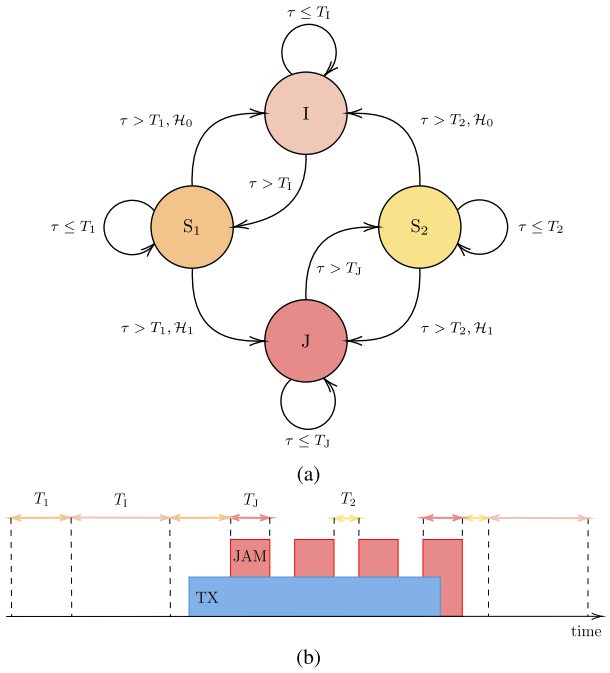


Fig. 2. (a) Finite-state machine model for the reactive jammer. Hypothesis $\mathcal{H}_1$ is the detection of a transmission, while $\mathcal{H}_0$ is the null hypothesis; S_1 and S_2 are the sensing states; I and J are the idle and jamming states, respectively; τ is the sojourn time in a given state. (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.

A. Jammer Model

In this work, we consider a reactive jammer that periodically senses the channel to detect the users transmissions and interfere. The advantage of using a reactive jammer is that, even if it consumes energy to sense the spectrum, it can perform targeted attacks that make it more efficient and less detectable than simpler jammers.

The jammer is modeled by the 4-states machine shown in Fig. 2a, 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. Then, the attacker alternates between states J and S_2, in which it performs detection with sensing time T_2.[2] Fig. 2b shows an example of a jammer attack.

1) Sensing at the Jammer: 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[3]

$$\tilde{y}_n^\mathrm{J} = \sum_{t=1}^{N_\mathrm{T}} \tilde{h}_t^\mathrm{J} \tilde{x}_{t,n} + \tilde{\omega}_n^\mathrm{J} \tag{1}$$

where $\tilde{x}_{t,n}$ for $t = 1, \ldots, N_\mathrm{T}$ is the nth sample of the signal transmitted by node t, $\tilde{h}_t^\mathrm{J}$ for $t = 1, \ldots, N_\mathrm{T}$ is the channel gain between node t and the jammer, and $\tilde{\omega}_n^\mathrm{J} \sim \mathcal{CN}(0, \sigma_\mathrm{J}^2)$ is the additive white Gaussian noise (AWGN) with independent, identically distributed (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.[4] The channel gain consists of two components $\tilde{h}_t^\mathrm{J} = g_t^\mathrm{J} e^{\sigma d_t}$, where g_t^J is the complex path gain, and $d_t \sim \mathcal{N}(0,1)$ are i.i.d. Gaussian r.v.s to model log-normal shadowing with intensity σ [33].[5]

The detection of a transmission is performed with an ED [31] represented by

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

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

2) Attack Signal: During the attack phase the jamming signal can assume several forms, e.g., white noise, a sinusoid or a signal with the same modulation of the victim communications.

B. The Patrol

Each RF sensor performs energy detection, collect the received energy samples for a period T_ob and forward the data to a FC, which could be either one of the sensors or a specific device. Information as number of transmitting nodes, their positions, and physical and medium access protocol (MAC) layer configurations are unknown to the FC. As will be better explained in Section III the observation period T_ob should be long enough to detect the causal relationship between the jammer and the victim network. Since such a relationship depends on the interaction between the jammer and the network at packet level, the observation period is much longer than the packet duration.

1) Received Signals at the Sensors: Similarly to the jammer, the nth sample of the equivalent low-pass signal received by the sth sensor is

$$\tilde{y}_{s,n} = \sum_{t=1}^{N_\mathrm{T}+1} \tilde{h}_{s,t} \tilde{x}_{t,n} + \tilde{\omega}_{s,n} \tag{3}$$

where, differently from (1) the patrol sees also the signal emitted by the jammer, indicated by $t = N_\mathrm{T} + 1$, $\tilde{h}_{s,t}$ for $t = 1, \ldots, N_\mathrm{T}$ is the channel gain between node t and sensor s, while $\tilde{h}_{s,N_\mathrm{T}+1}$ is the jammer-sensor channel gain. The term

[2]Note that the sensing time T_2 is usually shorter than T_1 to allow a more effective sensing [31], [32].

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

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

[5]The shadowing parameter is usually expressed as the standard deviation of the channel loss in deciBel by $\sigma(\mathrm{dB}) = \frac{20}{\ln 10}\sigma$.

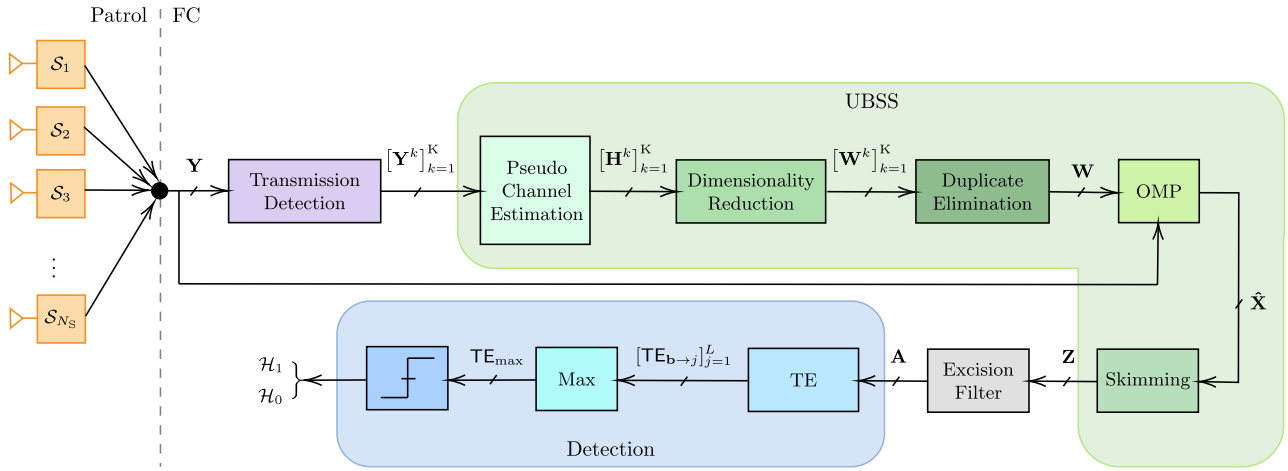


Fig. 3. Block diagram of the patrol system with N_S sensors. In the FC, after a transmission detection, UBSS is performed, then separated energy profiles are transformed into binary series analyzed by TE to detect the presence of a jamming attack.

$\tilde{\omega}_{s,n} \sim \mathcal{CN}(0, \sigma_S^2)$ is the AWGN at the sth sensor with i.i.d. real and imaginary parts, noise power $\sigma_S^2 = 2N_0^S W$ and two-sided power spectral density N_0^S.

Since the jammer and the patrol operate in the same propagation environment, also the links between sensors and transmitters/jammer is affected by log-normal shadowing with intensity σ.

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 $T_{ob} = N_e T_e$, where N_e is the number of energy samples. Thus, we obtain the matrix $\mathbf{Y} \in \mathbb{R}^{N_S \times N_e}$, whose entries $y_{s,i}$ are the energy samples

$$y_{s,i} = \frac{1}{W} \sum_{j=1}^{N_d} |\tilde{y}_{s,(i-1)N_d+j}|^2 \tag{4}$$

where $N_d = T_e W$ 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 through causal inference.

2) Received Energy Profiles: Under the assumptions of signals emitted by the nodes mutually uncorrelated and uncorrelated with the noise, we can express $\mathbf{Y}$ as[6]

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{\Omega} \tag{5}$$

where the tth row of $\mathbf{X} \in \mathbb{R}^{(N_T+1)\times N_e}$ is the corresponding transmitter's energy profile and the last row contains the energy profile of the jammer. The entries $\omega_{s,i} = \frac{1}{W}\sum_{j=1}^{N_d} |\tilde{\omega}_{s,(i-1)N_d+j}|^2$ of $\mathbf{\Omega} \in \mathbb{R}^{N_S \times N_e}$ are the noise energy samples and $\mathbf{H} \in \mathbb{R}^{N_S \times (N_T+1)}$ is the matrix of the channel power gains $h_{s,t} = |\tilde{h}_{s,t}|^2$.

The energy profiles are sent to a FC that performs the jammer detection. The proposed methodology requires the temporal dynamics of the transmitted packets for each node of the wireless network and the jammer; thus, the first processing stage is BSS. After the separation, we propose a jamming detection algorithm that seeks a causal relationship between the energy profiles transmitted by the nodes and the jammer. The complete processing chain is depicted in Fig. 3.

[6]Equation (5) holds for sufficiently large sample size $N_d = T_e W$; see the numerical results for values of practical interest for our problem.

III. Blind Source Separation

The BSS aims at recovering the source matrix $\mathbf{X}$ starting from the observations, $\mathbf{Y}$, without any prior knowledge of the channel matrix $\mathbf{H}$. Without loss of generality, 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 [27], we tackle the UBSS problem by first estimating the mixing matrix and then the source matrix, leveraging on its sparse nature, i.e., assuming that each column of $\mathbf{X}$ has few non-zero entries [34], [35], [36]. 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 [27] 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 [27].

A. 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

Algorithm 1 Transmission Detection

Input : $\mathbf{Y} \in \mathbb{R}^{N_\mathrm{S} \times N_\mathrm{e}}$, $\epsilon^\dagger$
Output: $\mathbf{Y}^1, \ldots, \mathbf{Y}^\mathrm{K}$
1 $k \leftarrow 1$
2 Initialize $\mathbf{Y}^k \leftarrow \mathbf{0}$
3 **for** i **from** 1 **to** N_e **do**
4 $\quad \mathrm{TX}_i = \mathit{false}$
5 $\quad v_s \leftarrow \frac{2}{\sigma_\mathrm{S}^2} y_{s,i} > \epsilon,\ \forall s = 1, \ldots, N_\mathrm{S}$
6 $\quad$ **if** at least one v_s is *true* **then**
7 $\quad\quad \mathbf{Y}^k = \left[\mathbf{Y}^k\ \mathbf{y}_{:,i}\right]$
8 $\quad\quad \mathrm{TX}_i = \mathit{true}$
9 $\quad$ **else**
10 $\quad\quad$ **if** $\mathrm{TX}_{i-1} = \mathit{true}$ **and** $2 \leq i < N_\mathrm{e}$ **then**
11 $\quad\quad\quad k \leftarrow k+1$
12 $\quad\quad\quad$ Initialize $\mathbf{Y}^k \leftarrow \mathbf{0}$
13 $\quad\quad$ **end**
14 $\quad$ **end**
15 **end**

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

introduce the general estimation methodology and then remark two different situations: with or without jammer.

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 $\mathbf{Y}$ 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. 4 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. (5) as

$$\mathbf{Y}^k = \mathbf{H}\mathbf{X}^k + \mathbf{\Omega}^k \tag{6}$$

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

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 [27], 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

$$\mathbf{R} = \mathbf{Y}^k / \mathbf{y}^k_{q,:}. \tag{7}$$

Fig. 4 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 [27]. Fig. 4 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 $I = \sum_{j=1}^{N_\mathrm{S}} I_j$ sub-matrices. For more details about the clustering algorithm please refer to [27, Section II].

Considering the generic sub-matrix $\mathbf{R}^i$, we now estimate the corresponding column of the pseudo channel matrix as [27]

$$\widehat{\mathbf{h}}_{:,i} = \frac{[\langle \mathbf{r}^i_{1,:} \rangle, \ldots, \langle \mathbf{r}^i_{N_\mathrm{S},:} \rangle]^\mathsf{T}}{\| [\langle \mathbf{r}^i_{1,:} \rangle, \ldots, \langle \mathbf{r}^i_{N_\mathrm{S},:} \rangle]^\mathsf{T} \|_2} \qquad i = 1, \ldots, I \tag{8}$$

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

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 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.,

$$N_w = \sum_{n=1}^{N_h} \mathbb{1}_{\{\Lambda_n > \Lambda_1 \bar{\Lambda}\}} \tag{9}$$

where $\bar{\Lambda}$ is the singular value selection parameter chosen, e.g., according to the scree plot approach [37]. 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

$$\mathbf{W}^k = \hat{\mathbf{H}}^k \tilde{\mathbf{V}} \tag{10}$$

where $\mathbf{W}^k \in \mathbb{R}^{N_\mathrm{S} \times N_w}$ is the kth reduced pseudo channel matrix.[7] Iterating the procedure for each pseudo channel

[7]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.

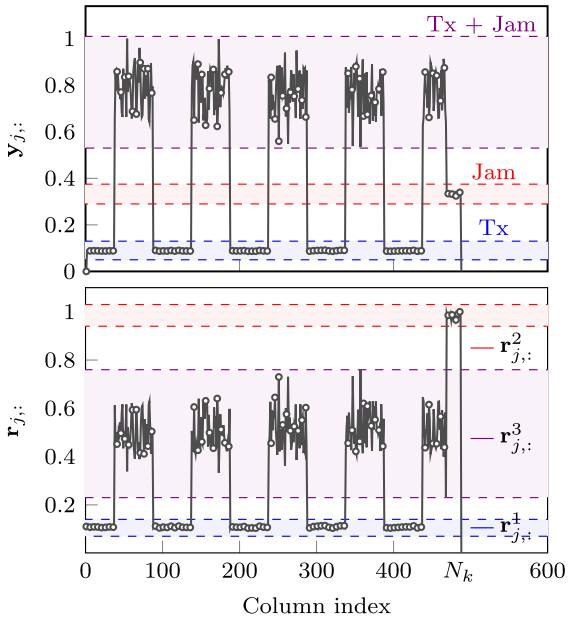


Fig. 4. Above, example of the jth row of $\mathbf{Y}^k$ in a scenario with a transmitter and the jammer. Below, the corresponding jth row of $\mathbf{R}$ where we note the presence of three clusters. $\mathbf{R}^1$, $\mathbf{R}^2$, and $\mathbf{R}^3$ are the sub-matrices obtained after the clustering operation and corresponding to the samples associated to the user transmission, the jammer, and the overlap of the two, respectively.

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 $\tilde{\mathbf{W}} = [\mathbf{W}^1, \mathbf{W}^2, \ldots, \mathbf{W}^K]$.

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

$$\|\tilde{\mathbf{w}}_{:,j} - \tilde{\mathbf{w}}_{:,i}\|_2 < \beta \tag{11}$$

where β is the elimination threshold. In the end, we obtain the estimated channel matrix $\mathbf{W} \in \mathbb{R}^{N_\mathrm{S} \times N_\mathrm{W}}$, where N_W is the number of estimated columns.

Remark 1. 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. 5, 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.[8] 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, (6) becomes $\mathbf{Y}^k = \mathbf{h}_{:,k} \otimes \mathbf{p}_k$ and the entries of $\mathbf{R}$ are $r_{i,j} = h_{i,k}/h_{q,k}$. Hence, the estimator (8) reduces to

$$\widehat{\mathbf{h}}_{:,k} = \frac{\mathbf{h}_{:,k}}{\|\mathbf{h}_{:,k}\|_2} \tag{12}$$

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 $\mathbf{H}$.

[8]To simplify the algorithm explanation, without loss of generality, the example in Fig. 5 considers one transmitted packet per node.

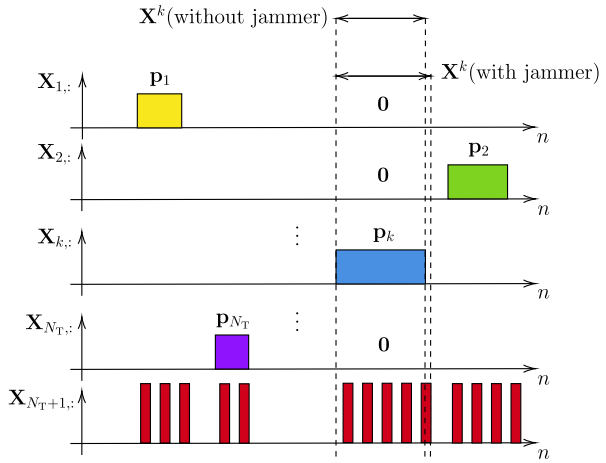


Fig. 5. An illustration of the rows of $\mathbf{X}$. Row $\mathbf{X}_{N_\mathrm{T}+1}$ contains the energy profile of the signal emitted by the jammer. If the jammer is absent it is a row of zeros.

Remark 2. 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.[9] In this case, a graphical illustration of the matrix $\mathbf{X}^k$ is shown in Fig. 5, 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 4. 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 (8) 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.

B. Unmixing by Orthogonal Matching Pursuit

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 $\mathbf{W}$, exploiting the sparsity of the sources. The problem is thus formulated as follows

$$\begin{aligned} &\min_{\mathbf{x}_{:,i}} \|\mathbf{x}_{:,i}\|_0 \\ &\text{s.t. } \mathbf{W}\mathbf{x}_{:,i} = \mathbf{y}_{:,i} \end{aligned} \tag{13}$$

[9]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.

for $i = 1, \ldots, N_{\mathrm{e}}$. This problem is known to be NP-hard and can be tackled with a greedy iterative method or using the well-known basis pursuit (BP) technique [38]. In this work, we reformulate (13) to be solved via the orthogonal matching pursuit (OMP) algorithm [39], i.e.,

$$\begin{aligned} &\min_{\mathbf{x}_{:,i}} \|\mathbf{y}_{:,i} - \mathbf{W}\mathbf{x}_{:,i}\|_2 \\ &\text{s.t. } \|\mathbf{x}_{:,i}\|_0 \leq \gamma \end{aligned} \tag{14}$$

where γ is the sparsity constraint. The value of γ is chosen according to the mutual coherence, the largest normalized inner product between distinct columns of $\mathbf{W}$, i.e.,

$$\mu(\mathbf{W}) = \max_{1 \leq i,j \leq N_{\mathrm{W}}, i \neq j} \frac{|\mathbf{w}_{:,i}^{\mathsf{T}} \mathbf{w}_{:,j}|}{\|\mathbf{w}_{:,i}\|_2 \|\mathbf{w}_{:,j}\|_2}. \tag{15}$$

A large $\mu(\mathbf{W})$ means that the columns of $\mathbf{W}$ are highly correlated and, thus, the signal reconstruction is hard (or even impossible). It has been proved in [40] that if the problem (14) admits a solution $\mathbf{x}_{:,i}$ with $\|\mathbf{x}_{:,i}\|_0 < \frac{1}{2}\left(1 + \frac{1}{\mu(\mathbf{W})}\right)$, then it is the sparsest possible. Hence, the sparsity constraint is set to

$$\gamma = \frac{1}{2}\left(1 + \frac{1}{\mu(\mathbf{W})}\right). \tag{16}$$

The output of the OMP is a matrix $\hat{\mathbf{X}} \in \mathbb{R}^{N_{\mathrm{W}} \times N_{\mathrm{e}}}$ 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

$$\frac{\max \hat{\mathbf{X}}_{i,:}}{\max \hat{\mathbf{X}}} < \Gamma \tag{17}$$

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

IV. Jammer Attack Detection

After separating the transmitted energy profiles of legitimate nodes and the jammer, we analyze the temporal relationship between such emitted profiles, exploiting a causal inference tool to detect the jammer.

A. Excision Filter

The jamming detection algorithm presented in Section IV-C 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 [34]. The output is matrix $\mathbf{A} \in \mathbb{R}^{L \times N_{\mathrm{e}}}$ with entries

$$a_{l,n} = \begin{cases} 1 \text{ if } z_{l,n} \geq \lambda_l \\ 0 \quad \text{otherwise} \end{cases} \tag{18}$$

Algorithm 2 Estimate of the Mixing Matrix

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

for k **from** 1 **to** K **do**
  $\hat{\mathbf{H}}^k \leftarrow [\,]$
  for q **from** 1 **to** N_{S} **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**
      $\hat{\mathbf{h}}_{:,i} \leftarrow \frac{[\langle \mathbf{r}^i_{1,:} \rangle, \ldots, \langle \mathbf{r}^i_{N_{\mathrm{S}},:} \rangle]^{\mathsf{T}}}{\|[\langle \mathbf{r}^i_{1,:} \rangle, \ldots, \langle \mathbf{r}^i_{N_{\mathrm{S}},:} \rangle]^{\mathsf{T}}\|_2}$
      $\hat{\mathbf{H}}^k \leftarrow \left[\hat{\mathbf{H}}^k\ \hat{\mathbf{h}}_{:,1} \ldots \hat{\mathbf{h}}_{:,I}\right]$
    end
  end
  $\mathbf{W}^k \leftarrow$ Step 3: DimensionalityReduction($\hat{\mathbf{H}}^k$)
end
$\mathbf{W} \leftarrow$ Step 4: DuplicateElimination($\mathbf{W}^1, \ldots, \mathbf{W}^{\mathrm{K}}$)

Step 2: Pseudo Channel Matrix Estimation

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

$$\lambda_l = q \cdot \max_n z_{l,n}, \quad l = 1, \ldots, L. \tag{19}$$

B. Transfer Entropy for Causal Inference

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 transfer entropy (TE) [29], [30]. 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

$$\begin{aligned} \mathsf{TE}_{i \to j}(k, r) &= \mathcal{I}\left(a_{j,n}; \mathbf{a}_{i,n-1:n-r} | \mathbf{a}_{j,n-1:n-k}\right) \\ &= \mathbb{E}\left[\log_2 \frac{p\left(a_{j,n} | \mathbf{a}_{i,n-1:n-r}, \mathbf{a}_{j,n-1:n-k}\right)}{p\left(a_{j,n} | \mathbf{a}_{j,n-1:n-k}\right)}\right] \end{aligned} \tag{20}$$

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 [28], 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.

C. 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

Algorithm 3 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
$\mathsf{TE}_{\max} \leftarrow \max_j \{v_j\}$
$\mathcal{H} \leftarrow \mathsf{TE}_{\max} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta$

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 $\mathbf{b} \in \mathbb{R}^{1 \times N_e}$, 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

$$\mathsf{TE}_{\max} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta. \tag{21}$$

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 $p_{\text{FA}} = \mathbb{P}(\mathsf{TE}_{\max} > \theta | \mathcal{H}_0)$, where the null distribution, is calculated via histogram based probability density function estimation. 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.

V. Numerical Results

In this section, several tests to evaluate the performance of the whole processing chain are presented. As a case study, we simulated a wireless network composed of N_{T} transmitters and a gateway, a patrol of N_{S} 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 the supplementary file. The network nodes adopt the LoRa modulation and Long Range Wide Area Network (LoRaWAN) MAC protocol [41], [42]. The operating frequency is set to $f_0 = 868.1$ MHz and the channel bandwidth is fixed to $W = 125$ kHz. According to the European regulation EU868, the transmission duty cycle is set to 1% [43]. 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 [42] and [44], 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 [43].

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

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

A. Algorithms' Parameter Settings

Table II summarizes the parameter settings adopted in the processing chain depicted in Fig. 3. The thresholds ξ and ϵ, for transmission detection by the patrol and ED in the jammer, respectively, ensure a false alarm probability $p_{\text{FA}} = 0.01$.

The quantization-based clustering algorithm proposed in [27] requires the setting of three parameters, the number of bins M_0 and two thresholds J_1 and J_2 that regulate the number

TABLE II
SYSTEM PARAMETERS FOR THE CASE STUDY

	UBSS						TE		
Parameter	$\bar{\Lambda}$	β	γ	Γ	M_0	J_1, J_2	q	$k_{\max}$	$r_{\max}$
Value	0.01	0.05	1	0.001	50	50	0.01	8	8

of non-negligible bins that have to be considered. We consider $J_1 = J_2 = J$ and set both M_0 and J at 50, i.e., quantization is performed over 50 bins, and if one of them has a number of samples less than 50, it is discarded.

The singular value selection parameter $\bar{\Lambda}$ is fixed to 0.01 according to the scree plot approach [37]. The duplicate elimination in the UBSS is carried out with a threshold $\beta = 0.05$. Skimming is performed with $\Gamma = 0.001$ since the negligible rows of $\hat{\mathbf{X}}$ are several orders of magnitude lower than the significant ones.

Let us discuss the setting of the UBSS parameter, γ. Since the estimated channel matrix, $\mathbf{W}$, might have duplicated columns, then $\mu(\mathbf{W}) \simeq 1$ and $\gamma = 1$ from eq. (16). Setting the sparsity constraint to 1 has a direct consequence in the estimation of the sources, clearly portrayed in Fig. 6, in which a scenario with $N_{\mathrm{S}} = 5$ sensors, a single transmitter, and the jammer is considered. In fig. 6, 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 following simulations. Moreover, Fig. 6 shows how dimensionality reduction allows a more accurate reconstruction of the sources.

The excision filter threshold is set to $q = 0.01$, while the time lags for TE are set to $k_{\max} = r_{\max} = 8$ samples.

B. TE, Cross-Correlation and Impact of Shadowing

As detailed in Section IV, TE is the tool we propose to infer the causality between the jammer and the network nodes. However, a much simpler approach is to use the cross-correlation as an indicator of a possible causal relationship between two time series. In this case, given two reconstructed energy profiles $\mathbf{a}_{i,:}$ and $\mathbf{a}_{j,:}$, the cross-correlation is

$$\mathbf{c}_{i\leftrightarrow j}(m) = \sum_{n=1}^{N_{\mathrm{e}}-m} a_{i,n} a_{j,n+m} \tag{22}$$

where n indicates the time samples and m is the time lag. For jamming detection through the cross-correlation, it is possible to modify the Algorithm 3 by removing the lines from 4 to 14 corresponding to grid search for TE, while lines 15, 17, and 18 are replaced with

$$v_j \leftarrow \max_m |\mathbf{c}_{\mathbf{b}\leftrightarrow j}(m)| \tag{23}$$

$$\mathsf{CC}_{\max} \leftarrow \max_j \{v_j\} \tag{24}$$

$$\mathsf{CC}_{\max} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta. \tag{25}$$

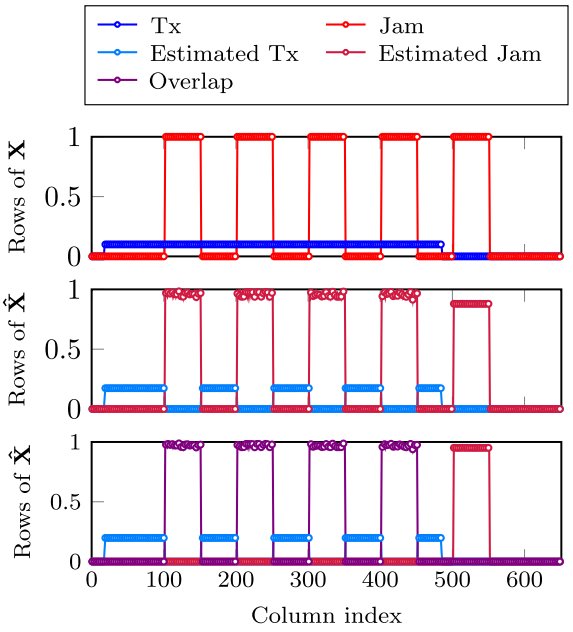


Fig. 6. Above are the true energy profiles of a single transmitter and the jammer. In the middle, the energy profiles recovered with the algorithm in Section III. Below is the result with the algorithm in [27]. For both algorithms, $N_{\mathrm{S}} = 5$, and OMP is used in the second step. Notice that 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.

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. 7 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 $N_{\mathrm{T}} = 10$ transmitters, $N_{\mathrm{S}} = 5$ sensors, and a jammer in the area. The ROC curves are obtained across $N_{\mathrm{MC}} = 10^4$ Monte 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 $T_{\mathrm{ob}} = 20\,\mathrm{s}$, 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. 7 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

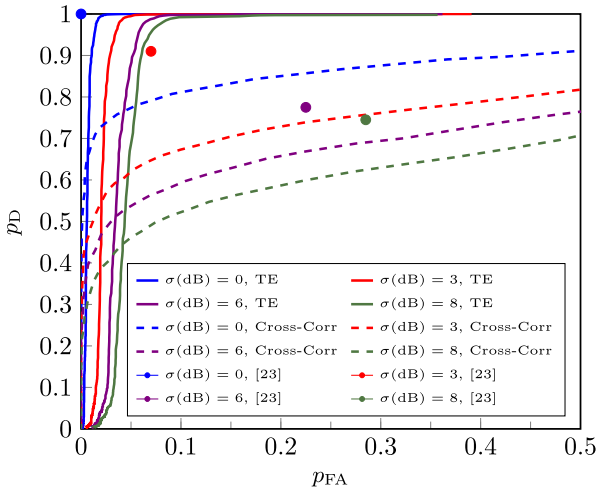


Fig. 7. ROC curves for TE and cross-correlation with different values of shadowing intensity $\sigma(\text{dB})$. Comparison with the state-of-the-art method [23].

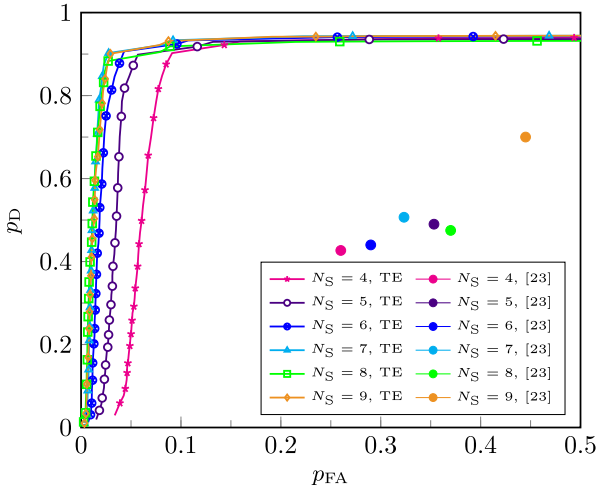


Fig. 8. ROC curves as a function of the number of sensors N_S.

energy profiles by the UBSS. However, note that TE exhibits robust performance even for $\sigma = 8\,\text{dB}$.

The presented method is compared with a ML-based approach for jamming detection proposed in [23], 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. 7 includes the performance of both solutions. Since the sensor positions are fixed during the Monte-Carlo iterations, the performance of the ML-based algorithm is optimal when $\sigma(\text{dB}) = 0$. 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.

C. 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 V-B, in Fig. 8 we compute the ROC curve for different number of patrol sensors $N_S = \{4, 5, \ldots, 9\}$. 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 $N_S = 4$, 30 m for $N_S = \{5, 6, 7, 8\}$, and 25 m when $N_S = 9$. A limit of at most two collisions among transmitters in $T_{ob} = 20\,\text{s}$ is considered as in the previous subsection. We consider a shadowing with $\sigma(\text{dB}) = 3$ both for transmitter/jammer-patrol channel and for transmitter-jammer channel. It is possible to see that from $N_S = 4$ to $N_S = 7$ the performance noticeably increases, while from $N_S = 7$ to $N_S = 9$ 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., independent component analysis (ICA) can be used [45].

Comparing the ROC curve for $\sigma(\text{dB}) = 3$ and $N_S = 5$ in Fig. 7 with the corresponding curve in Fig. 8, a drop in performance can be notices. The reason lies in the different setup for patrol sensors: in Fig. 7 sensors have fixed positions chosen for good coverage of the area, while in Fig. 8 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 [23]. Indeed, by changing the positions, there is a loss of information contained in the RSS values used during training.

The same simulation setup is employed to compare the UBSS algorithm in Section III with the original algorithm in [27]. 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 [27] 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 $\mathbf{m} \in \mathbb{R}^{N_T+1}$ that becomes a matrix $\mathbf{M} \in \mathbb{R}^{N_{MC} \times (N_T+1)}$, iterating the simulation for $N_{MC} = 1000$. In Fig. 9, a pixel $p_{i,j}$ depicts the mean of $\mathbf{M}_{:,j}$ for a given number of sensors $N_S = i$. 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 $N_S = i$. 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 [27], while, on the contrary, with our methodology, it is the source estimated at best.

D. Effect of Collisions

As we have seen, since collisions among nodes' packets are a nuisance in the reconstruction stage, it is necessary

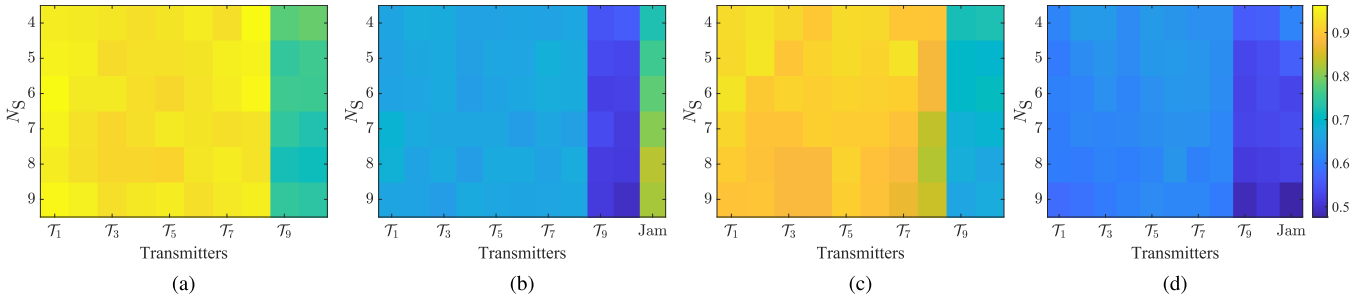


Fig. 9. Similarity degree among transmitters profiles and estimated sources (the color scale is on the right). Each pixel of the images depicts, for a given N_S in the y-axis, the correlation coefficient of two time series: the true energy profile of the transmitter indicated in the x-axis and the corresponding profile estimated via UBSS. Performance of the proposed algorithm in Section III without, (a), and with the jammer,(b). Performance of the algorithm in [27] without, (c), and with the jammer, (d).

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 $N_T = 10$, $N_S = 5$, a jammer, with fixed positions during simulation equal to Subsection V-B, $T_{ob} = 20\,s$, $\sigma(dB) = 3$, 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 $N_{MC} = 5000$ 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., $N_{col} = 4$ and $N_T = 10$ means that 8 packets are involved in the collisions. The results are shown with a orange bar plot in Fig 10. As already 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 red bar plot in Fig 10 is obtained with the same setting but placing $N_T = 20$ and $T_{ob} = 30\,s$.[10] 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.

E. Impact of signal-to-jammer ratio (SJR)

This section studies the performance of AvOTE varying the SJR, defined as the ratio between the nodes and the jammer transmit powers. The scenario consists of $N_T = 10$ transmitters, $N_S = 5$ patrol sensors, and a jammer, and for each of the $N_{MC} = 3000$ 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 V-B. In Fig. 11, 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.

[10]This scenario is also detailed in the supplementary file with all actor positions. Furthermore, the observation time is increased here to ensure that each node transmits at least one packet.

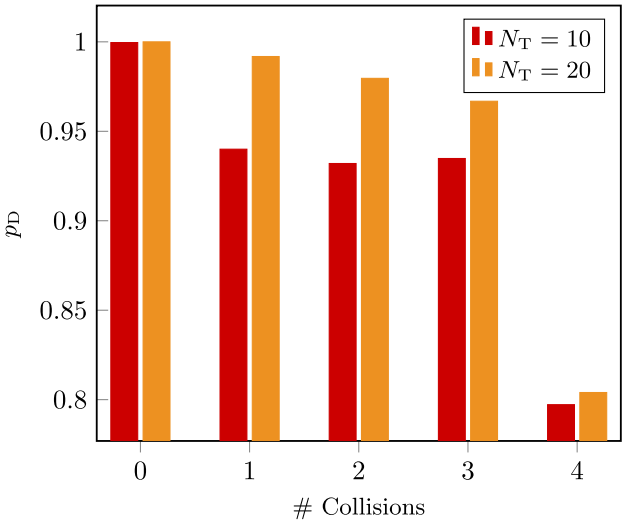


Fig. 10. Probability of detection as a function of the number of collisions for two different values of the number of transmitting nodes N_T.

F. Computational Complexity

This section discusses the computational complexity of the proposed jamming detection scheme. To determine the complexity, addition, subtraction, multiplication, and division are valued one floating-point operation (FLOP).

- **Transmission detection.** Based on (4), each sensor computes the energy profile, so the overall complexity for Algorithm 1 is $\mathcal{O}(N_S N_e N_d^2)$.

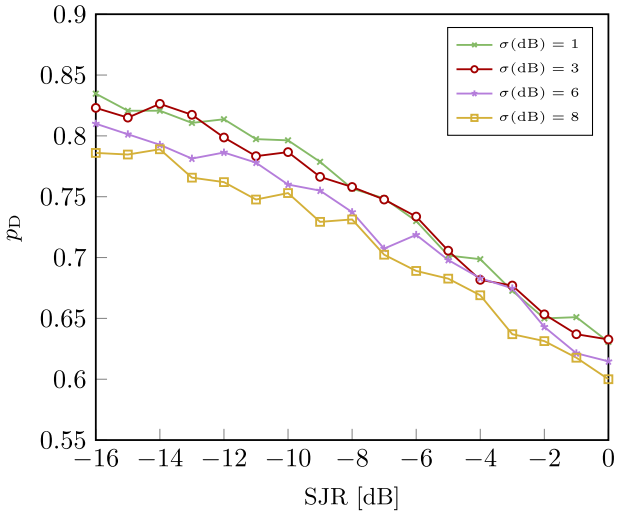


Fig. 11. Detection probability as a function of the SJR with different shadowing intensities, $\sigma(\mathrm{dB})$, and $p_{\mathrm{FA}} = 5\%$.

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

$$\mathcal{O}\left(\left((2IN_{\mathrm{S}} + IN_{\mathrm{S}}N_R + N_{\mathrm{S}}N_k)N_{\mathrm{S}} + N_{\mathrm{S}}N_h^2\right)\mathrm{K}\right) \tag{26}$$

  where N_R is the number of columns of the largest submatrix $\mathbf{R}^i$, $i = 1, \ldots, I$. Row 5 is a quantization-based clustering algorithm that does not contain any multiplications or sums, but comparisons, so its complexity is neglected [27].
- **Orthogonal matching pursuit.** Based on [46], the complexity of reconstructing the transmitted energy profiles is $\mathcal{O}(\gamma N_{\mathrm{S}} N_{\mathrm{W}} N_{\mathrm{e}})$.
- **All-versus-one transfer entropy.** The input vectors are sequences of 0s and 1s of length N_{e}, hence, one computation of TE takes $\mathcal{O}(N_{\mathrm{e}})$ [28], [47]. Since TE is calculated inside 3 loops in AvOTE algorithm, the complexity for this step is $\mathcal{O}\big(Lk_{\max}r_{\max}N_{\mathrm{e}} + L(L-1)\big)$, where the term $L(L-1)$ is due to the sum in row 3 of Algorithm 3.
- **Cross-correlation.** Adopting fast Fourier transform (FFT) to compute the cross-correlation, the complexity for this version of Algorithm 3 is $\mathcal{O}\big(LN_{\mathrm{e}}\log_2(N_{\mathrm{e}})\big)$.

Considering $T_{\mathrm{ob}} = 20\,\mathrm{s}$ and $W = 125\,\mathrm{kHz}$, we have $N_{\mathrm{d}}N_{\mathrm{e}} \sim 10^6$. 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 $\mathcal{O}(N_{\mathrm{S}}N_{\mathrm{e}}N_{\mathrm{d}}^2)$.

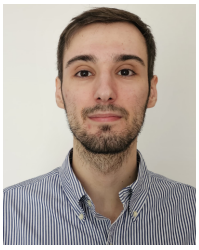
VI. Conclusion

We proposed a novel framework for reactive jammer detection using a patrol of RF sensors external to the network to be protected. Sensors collect the received power computed over short time intervals and share such energy profiles with a FC. A novel UBSS method, grounded on [27], is performed at the FC to separate the transmitted energy profiles from the mixtures received by the sensors. Finally, the TE is adopted as a causal inference test to detect the presence of a reactive jammer. Extensive numerical results proved that our UBSS approach outperforms the reference method in literature, guaranteeing satisfactory reconstruction of the jammer temporal activity profile, and that the overall methodology exhibits excellent performance: up to 99% detection probability in the absence of collisions between user packets, outperforming a state-of-the-art algorithm. To provide a complete investigation of the solution, we demonstrated that performance degradation arises primarily when the sources are poorly reconstructed by UBSS due to high shadowing intensity, an insufficient number of sensors, and in the presence of many collisions.

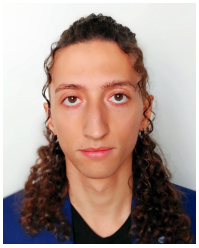
References

[1] C. Jiang, H. Zhang, Y. Ren, Z. Han, K. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 98–105, Apr. 2017.
[2] 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, Oct. 2020.
[3] E. Testi and A. Giorgetti, "Blind wireless network topology inference," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1109–1120, Feb. 2021.
[4] Y.-S. Shiu, S. Chang, H.-C. Wu, S. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
[5] M. Massaro and F. Beltrán, "Will 5G lead to more spectrum sharing? Discussing recent developments of the LSA and the CBRS spectrum sharing frameworks," *Telecommun. Policy*, vol. 44, no. 7, Aug. 2020, Art. no. 101973.
[6] 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, 4th Quart., 2009.
[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile ad hoc Netw. Comput.*, May 2005, pp. 1–9.
[8] T. Perković, H. Rudeš, S. Damjanović, and A. Nakić, "Low-cost implementation of reactive jammer on LoRaWAN network," *Electronics*, vol. 10, no. 7, p. 864, Apr. 2021.
[9] 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.
[10] A. Chakraborty, A. Bhattacharya, S. Kamal, S. R. Das, H. Gupta, and P. M. Djuric, "Spectrum patrolling with crowdsourced spectrum sensors," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2018, pp. 1682–1690.
[11] 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.
[12] J. Li, J. Xu, W. Liu, S. Gong, and K. Zeng, "Robust optimal spectrum patrolling for passive monitoring in cognitive radio networks," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Helsinki, Finland, Aug. 2017, pp. 63–68.
[13] M. Çakiroglu and A. T. Özcerit, "Jamming detection mechanisms for wireless sensor networks," in *Proc. 3rd Int. ICST Conf. Scalable Inf. Syst.*, Vico Equense, Italy, Jun. 2008, pp. 1–10.
[14] 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.
[15] M. Strasser, B. Danev, and S. Čapkun, "Detection of reactive jamming in sensor networks," *ACM Trans. Sensor Netw.*, vol. 7, no. 2, pp. 1–29, Aug. 2010.
[16] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Gothenburg, Sweden, Jun. 2015, pp. 1–6.
[17] H. Akhlaghpasand, S. M. Razavizadeh, E. Björnson, and T. T. Do, "Jamming detection in massive MIMO systems," *IEEE Wireless Commun. Lett.*, vol. 7, no. 2, pp. 242–245, Apr. 2018.
[18] M. O. Mughal, K. Dabcevic, L. Marcenaro, and C. S. Regazzoni, "Compressed sensing based jammer detection algorithm for wide-band cognitive radio networks," in *Proc. 3rd Int. Workshop Compressed Sens. Theory Appl. Radar, Sonar Remote Sens. (CoSeRa)*, Pisa, Italy, Jun. 2015, pp. 119–123.

[19] H. B. Salameh, S. Otoum, M. Aloqaily, R. Derbas, I. A. Ridhawi, and Y. Jararweh, "Intelligent jamming-aware routing in multi-hop IoT-based opportunistic cognitive radio networks," *Ad Hoc Netw.*, vol. 98, Mar. 2020, Art. no. 102035.
[20] X. Wang et al., "Dynamic spectrum anti-jamming communications: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 79–85, Feb. 2020.
[21] S. Gecgel, C. Goztepe, and G. K. Kurt, "Jammer detection based on artificial neural networks: A measurement study," in *Proc. ACM Workshop Wireless Secur. Mach. Learn.*, Miami, FL, USA, May 2019, pp. 43–48.
[22] S. Gecgel and G. K. Kurt, "Intermittent jamming against telemetry and telecommand of satellite systems and a learning-driven detection strategy," in *Proc. 3rd ACM Workshop Wireless Secur. Mach. Learn.*, Abu Dhabi, United Arab Emirates, Jun. 2021, pp. 43–48.
[23] G. Kasturi, A. Jain, and J. Singh, "Detection and classification of radio frequency jamming attacks using machine learning," *J. Wireless Mob. Netw. Ubiquitous Comput. Dependable Appl.*, vol. 11, no. 4, pp. 49–62, 2020.
[24] Y. Arjoune, F. Salahdine, Md. S. Islam, E. Ghribi, and N. Kaabouch, "A novel jamming attacks detection approach based on machine learning for wireless communication," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Barcelona, Spain, Jan. 2020, pp. 459–464.
[25] S. Ujan, M. Same, and R. Landry, "A robust jamming signal classification and detection approach based on multi-layer perceptron neural network," *Int. J. Res. Stud. Comp. Sci. Eng. (IJRSCSE)*, vol. 7, pp. 1–12, Mar. 2020.
[26] 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 *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 246–251.
[27] Y. Li, S. Amari, A. Cichocki, D. W. C. 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.
[28] 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. 2020.
[29] J. L. Massey, "Causality, feedback and directed information," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Waikiki, HI, USA, Nov. 1990, pp. 303–305.
[30] T. Schreiber, "Measuring information transfer," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 461–464, Jul. 2000.
[31] 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.
[32] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar, "IEEE 802.22: An introduction to the first wireless standard based on cognitive radios," *J. Commun.*, vol. 1, no. 1, pp. 38–47, Apr. 2006.
[33] A. Giorgetti, M. Z. Win, P. C. Pinto, and M. Chiani, "A stochastic geometry approach to coexistence in heterogeneous wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1268–1282, Sep. 2009.
[34] 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.
[35] 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.
[36] A. Elzanaty, A. Giorgetti, and M. Chiani, "Weak RIC analysis of finite Gaussian matrices for joint sparse recovery," *IEEE Signal Process. Lett.*, vol. 24, no. 10, pp. 1473–1477, Oct. 2017.
[37] I. T. Jolliffe, *Principal Component Analysis*. New York, NY, USA: Springer-Verlag, 2002.
[38] 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, 2022, Art. no. 4710015.
[39] S. K. Sahoo and A. Makur, "Signal recovery from random measurements via extended orthogonal matching pursuit," *IEEE Trans. Signal Process.*, vol. 63, no. 10, pp. 2572–2581, May 2015.
[40] D. L. Donoho and M. Elad, "Optimally sparse representation in general (nonorthogonal) dictionaries via ℓ^1 minimization," in *Proc. Nat. Acad. Sci. USA*, vol. 100, no. 5, Feb. 2003, pp. 2197–2202.
[41] 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.
[42] *Lorawan 1.1 Specification*, LoRa Alliance, Oct. 2017, pp. 1–101.
[43] LoRa Alliance. (2020). *RP002-1.0.2 LoRaWAN Regional Parameters*. [Online]. Available: https://lora-alliance.org/resource_hub/rp2-102-lorawan-regional-parameters/
[44] A. Augustin, J. Yi, T. Clausen, and W. Townsley, "A study of LoRa: Long range & low power networks for the Internet of Things," *Sensors*, vol. 16, no. 9, p. 1466, Sep. 2016.
[45] C. Xiyuan, Z. Wei, and W. Shilian, "Blind source separation anti-jamming technology based on pade-FastICA algorithm," in *Proc. IEEE 20th Int. Conf. Commun. Technol. (ICCT)*, Nanning, China, Oct. 2020, pp. 1179–1183.
[46] A. M. Bruckstein, D. L. Donoho, and M. Elad, "From sparse solutions of systems of equations to sparse modeling of signals and images," *SIAM Rev.*, vol. 51, no. 1, pp. 34–81, Feb. 2009.
[47] J. T. Lizier, "JIDT: An information-theoretic toolkit for studying the dynamics of complex systems," *Frontiers Robot. AI*, vol. 1, p. 11, Dec. 2014.



Luca Arcangeloni (Graduate Student Member, IEEE) received the M.Sc. degree (magna cum laude) in electronics and telecommunications engineering from the University of Bologna in 2021, where he is currently pursuing the Ph.D. degree with the Department of Electrical, Electronic, and Information Engineering. His current research focuses on the development of algorithms for intelligent jamming detection and spectrum sensing for cognitive radio applications. His research interests include spectrum awareness for next-generation wireless networks, using machine learning techniques.



Enrico Testi (Member, IEEE) received the M.S. degree (magna cum laude) in electronics and telecommunications engineering for energy and the Ph.D. degree in electronics, telecommunications, and information technologies engineering from the University of Bologna, Italy, in 2018 and 2022, respectively. He is currently a Junior Assistant Professor with the Department of Electrical, Electronic, and Information Engineering "Guglielmo Marconi" (DEI), University of Bologna. His research interests include machine learning (ML), reinforcement learning (RL), and deep learning (DL) techniques for spectrum monitoring, massive multiple access, and satellite communications.

Andrea Giorgetti (Senior Member, IEEE) received the Dr.-Ing. degree (summa cum laude) in electronic engineering and the Ph.D. degree in electronic engineering and computer science from the University of Bologna, Bologna, Italy, in 1999 and 2003, respectively. From 2003 to 2005, he was a Researcher with the National Research Council, Italy. In 2006, he joined the Department of Electrical, Electronic, and Information Engineering "Guglielmo Marconi," University of Bologna, as an Assistant Professor, where he was promoted to an Associate Professor, in 2014. In Spring 2006, he was with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA. Since then, he has been a frequent Visitor with the Wireless Information and Network Sciences Laboratory, MIT, where he holds the Research Affiliate appointment. He has coauthored the book *Cognitive Radio Techniques: Spectrum Sensing, Interference Mitigation, and Localization* (Artech House, 2012). His research interests include ultra-wide bandwidth communication systems, active and passive localization, wireless sensor networks, cognitive radio, and integrated sensing and communications. He was the Technical Program Committee Co-Chair of several symposia at the IEEE International Conference on Communication and IEEE Global Communication Conference. From 2017 to 2018, he was the Elected Chair of the IEEE Communications Society's Radio Communications Technical Committee. He is a past Editor of the IEEE COMMUNICATIONS LETTERS and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

Open Access funding provided by 'Alma Mater Studiorum - Università di Bologna' within the CRUI CARE Agreement