Accepted Manuscript
Version of Record at: https://doi.org/10.1109/TCCN.2023.3244539

Detection of Stealthy Jamming for UAV-Assisted Wireless Communications: An HMM-based Method

Chen Zhang, Leyi Zhang, Tianqi Mao, *Member, IEEE,* Zhenyu Xiao, *Senior Member, IEEE,* Zhu Han, *Fellow, IEEE,* and Xiang-Gen Xia, *Fellow, IEEE*

***Abstract*—Due to the high mobility, low cost and high robustness of line-of-sight (LoS) channels, unmanned aerial vehicles (UAVs) have begun to play an important role in assisting wireless communications. However, the broadcasting nature of wireless communication networks makes the electromagnetic spectrum vulnerable to jamming attacks. To ensure communication security, this paper investigates the jamming detection issue for UAV-assisted wireless communications. Different from the existing works, we consider detection of stealthy jamming with no prior knowledge of legitimate users or channel statistics, which makes the detection more challenging. To solve this problem, we design a hidden Markov model (HMM) based jamming detection (HBJD) method. First, we process the received signals with a sliding window to calculate the logarithmic received energy and use HMM to model the signal transmission under a jamming attack. Specifically, the spectrum state and logarithmic received energy are modeled as the hidden state and observable variable of HMM. Then, the Expectation-Maximization (EM) algorithm is applied to estimate the parameters of HMM. With the estimated parameters, the spectrum state of each logarithmic received energy sample can be decided according to the maximum posterior probability (MAP) criterion. Finally, we design the test statistics and derive the threshold based on the estimated HMM parameters for the final decision. Simulation results demonstrate the superiority of the proposed solution for the detection of stealthy jamming without prior knowledge of legitimate users or the channel statistics.**

***Index Terms*—Communication security, unmanned aerial vehicle, jamming detection, hidden Markov model, hypothesis test.**

I. Introduction

WITH the advantages of low cost, flexible deployment, and high robustness of line-of-sight (LoS) channel, unmanned aerial vehicle (UAV) has been considered as a promising device to assist wireless communications [1]–[4]. UAVs can be deployed as base stations (BSs) or relays to provide on-demand communication service for the Internet of Things (IoT), post-disaster networks and sudden traffic congestion of cellular networks [5]–[8]. However, the transmission of UAV-assisted wireless communication networks can be easily monitored by malicious users (MUs) because of the broadcasting nature of wireless communications, resulting in possible attacks on the employed spectrum of the legitimate users (LUs) [9]–[11].

There are different types of spectrum jamming attacks, which may be classified into three categories [12]: Constant jamming, where the jamming signals are continuously transmitted; Intermittent jamming, where the jamming signals are transmitted from time to time; Reactive jamming, where the jamming signals attack the portion of the spectrum occupied by LUs only when LUs are being monitored for transmission. By injecting jamming signals in the spectrum, the signal transmission between UAV and LUs can be destroyed [10], [13]. As a result, the performance of UAV-assisted wireless communications will degrade significantly. Moreover, compared to the other two categories, reactive jamming has shown to be not only the most stealthy but also energy-efficient [14]. Though several techniques have been proposed to eliminate jamming at the physical layer, such as spread spectrum and CDMA [15], it is still necessary to strengthen the detection capabilities of UAV to against spectrum jamming attacks. As mentioned before, jamming attacks will change their transmission time to improve concealment, so direct anti-jamming operation without considering jamming exists will cause an unnecessary reduction of the transmission rate of the legitimate user [16]. Therefore, we focus on the jamming detection at the receiver, whilst the anti-jamming operation at the transmitter is beyond the scope of this article. With the help of jamming detection, not only the warning of jammed communication links can be provided, but also the anti-jamming operation can be carried out on demand, which can help to avoid unnecessary communication efficiency reductions.

A. Related Works

A typical class of jamming detection methods is feature information based methods, which authenticate LUs and identify MUs based on the feature information injected into the spectrum by legitimate users. The most common method is to use known encrypted signals to authenticate LUs at the receiving end [17]–[19]. However, in the existing schemes, the authentication signals are usually superimposed onto the information-bearing signals, which means both of them will interfere with each other. This limits the performance of authentication-based jamming detection. For further performance improvement,

This work was supported by the Defense Industrial Technology Development Program with Grant number JCKY2020601B014 *(Corresponding authors: Zhenyu Xiao).*

C. Zhang, T. Mao and Z. Xiao are with the School of Electronic and Information Engineering, Beihang University, Beijing 100191, China (e-mail: {moon_zc, maotq, xiaozy}@buaa.edu.cn).

L. Zhang is with the ZTE Corporation, Beijing 100029, China (e-mail: zh_ly_lyaj@126.com).

Z. Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (e-mail: hanzhu22@gmail.com).

X.-G. Xia is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716, USA (e-mail: xxia@ee.udel.edu).

[20] took the physical (PHY) information of LUs as feature information for authentication operations. Besides, the authors in [21] proposed a cross-layer framework for spectrum security by jointly applying PHY-layer and network-layer information for authentication. To improve the detection performance in the fast-fading channel, a new authentication scheme at the PHY-layer was proposed in [22]. The scheme combined the techniques of blindly known interference cancellation and differential processing to suppress the deteriorating effect of fading channels without any additional preprocessing. For detecting stealthy jamming, the authors in [23] proposed a cross-layer model for intelligent reactive jamming, which takes PHY-layer information and network-layer information as feature information.

Another class of widely used jamming detection methods is cognitive radio (CR) based methods. CR-based methods utilize spectrum sensing technology, which perceives the spectrum states, i.e., jammed and unjammed, by monitoring the spectrum state information, such as received signal strength (RSS), signal energy, and channel state information (CSI) [24], [25]. Specifically, jamming signals from MUs can make spectrum state information different from that when only LUs occupy the spectrum. Comparing the monitored spectrum state information with the spectrum state information when only LUs transmit signals, whether the spectrum is jammed can be concluded [26]–[28]. A widely used scheme models the jamming detection problem as a hypothesis testing problem, considering jammed and unjammed as two fundamental assumptions. This hypothesis testing problem can be solved by designing detection thresholds and comparing the monitored test statistics with the detection thresholds, and then the spectrum state can be acknowledged. For example, the authors in [29] chose signal energy as test statistics and proposed a cooperative energy detection (ED) method for the formulated multi-hypothesis testing problem. However, when the MU imitates the transmission power of LU, the signal energy of the jammed spectrum state may be the same as that of unjammed spectrum state, resulting in the jamming attacks being too stealthy to be detected. To this end, the authors in [30] proposed a CSI-based cooperative ED method to detect cases where MU uses the same power as LU.

Another typical scheme of CR-based methods takes the features of the received signal when the channel is unjammed as reference data to design a jamming detector, which can be also called machine learning based methods. Different from the methods based on hypothesis testing, this kind of methods do not need to know the statistical distribution of normal signals. Specifically, the easily obtained reference data is used as the training set, and the machine learning or deep learning algorithm is used to train the classifier, which can distinguish the jammed signals from the unjammed signals. By classifying the spectrum state with the classifier, the detection of spectrum jamming can be achieved. As in [31], the authors proposed a mechanism that used a support vector machine (SVM) to detect low power jamming, using sufficient statistics packet drop probabilities as training data. Besides, in [32], the authors proposed a machine learning based method for jamming detection, where the training data is RSS collected from multiple anchor nodes. Similarly, the authors in [33] trained a dynamic Bayesian network to represent the spectrum states and used the Kullback-Leibler-divergence to measure the abnormality of the spectrum for UAV communications. And the authors in [34] proposed two deep learning based techniques for different application requirements related to Signal Noise Ratio (SNR) walls and generalization boundaries. The contributions of existing literature for jamming detection are summarized in Table I.

B. Motivation and Contribution

In summary, the feature information based methods have the advantages of high detection probability, but suffer from the strict requirement of monitoring devices, reduced throughput and high computation overhead [22], [35]. Compared with the feature information based methods, CR-based methods also have outstanding performance. Besides, CR-based methods do not have strict requirements for observation devices and do not need highly computationally complex operations such as decoding and demodulation. However, the role of CR-based methods in UAV-assisted wireless communications is still limited. On one hand, for the hypothesis testing based method, it is difficult to obtain prior information such as the statistical distribution of signal energy. On the other hand, though the reference data based methods do not require any information during detection, they are still unavailable because it is difficult to ensure that there are no jammed samples in the sampled training data. For example, in UAV-assisted emergency communications, channel characteristics are greatly different from those before the disaster, and the locations of users are difficult to determine, and consequently, accurate prior knowledge cannot be obtained [6], [36].

To this end, we investigate a spectrum jamming detection problem of stealthy jamming for UAV-assisted wireless communications in this paper. Specifically, for attacking the transmission of LU stealthily, an MU carries out short period jamming attacks only when monitoring LU transmitting signals, defined as reactive short period jamming (RSPJ) in [37], and the prior knowledge such as signal power and noise power in the communication system is considered to be unknown, which makes the existing methods unavailable. To detect jamming attacks without prior knowledge of signal characteristics or channel characteristics, we construct a hypothesis testing problem, where the statistical characteristics of both hypotheses are unknown. To solve such a problem, we propose a novel CR-based jamming detection method based on the hidden Markov model (HMM), which can characterize the dynamic behavior of the MU through long-term observation [38], [39]. Different from [40], we do not use the estimated parameters to design the testing threshold directly. Instead, we first process the estimated parameters to obtain test statistics with clear statistical characteristics, so that a simple and intuitive test threshold can be derived. The details of designing the test statistic and threshold can be seen in Section III.C. Besides, unlike the existing detection methods, our method directly obtains the statistical characteristics of the logarithmic received energy without requiring any prior knowledge, thus

Accepted Manuscript
Version of Record at: https://doi.org/10.1109/TCCN.2023.3244539

TABLE I
COMPARISON OF THE MAIN CONTRIBUTIONS BETWEEN RELATED WORKS AND THIS PAPER

Method category	Reference	One sentence describing the main contribution	Prior information
Feature information based method	Vireshwar Kumar [20]	Extending the precoded duobinary signaling technique to devise a new authentication scheme.	PHY-layer authentication signal
	CaLynna Sorrells [21]	Taking advantage of both network layer and PHY-layer information for authentication.	Cross-layer authentication signal
	Ning Xie [22]	Proposing an authentication scheme to improve the detection performance in fast-fading channels.	PHY-layer authentication signal
	Lijun Qian [23]	Proposing a cross-layer detection method for intelligent reactive jamming.	Cross-layer authentication signal
CR based method	Linyuan Zhang [29]	Designing a cooperative ED method for a multi-hypothesis testing problem.	Statistical distribution of signal energy
	Bikalpa Upadhyaya [30]	Proposing a CSI-based cooperative ED method to detect jamming which uses the same power as LU.	CSI and statistical distribution of signal energy
	Nalam Venkata Abhishek [31]	Using SVM to detect low power jamming.	Training data: statics packet drop probabilities
	Bikalpa Upadhyaya [32]	Proposing a machine-learning based jamming detection method which uses multiple anchor nodes to collect RSS.	Training data: RSS
	Ali Krayani [33]	Training a dynamic Bayesian network to detect spectrum abnormalities for UAV communications.	Training data: signals of UAV
	Ying Kang [34]	Proposing two deep learning based techniques for different application requirements.	Training data: raw received signals
	This Paper	Detecting stealthy jamming with no requirement for prior information.	None

providing a practical solution to a problem that has not previously been addressed in the literature on UAV-assisted wireless communications. The main contributions of this paper are summarized as follows.

1) We formulate the jamming detection problem of RSPJ without prior knowledge as a hypothesis testing problem. To solve such a problem, we propose an HMM-based jamming detection (HBJD) method.
2) Firstly, we use a 1-step sliding window to process the received signals to obtain a sequence of logarithmic received energy. The jamming signals injected by MU may change the statistic characteristics of the logarithmic received energy [29]. Based on this concept, we formulate the signal transmission under RSPJ as an HMM, where the spectrum state is regarded as a hidden state and the logarithmic received energy sequence is the observable sequence.
3) Secondly, we employ the Expectation-Maximization (EM) algorithm to estimate the parameters of the formulated HMM, especially the mean and variance of the logarithmic received energy under different spectrum states. With the estimated parameters, the hidden spectrum state of each logarithmic received energy sample can be decided according to the maximum posterior probability (MAP) criterion.
4) Thirdly, as HMM will always divide the logarithmic received energy sequence into two clusters, i.e., jammed and unjammed, taking the estimated results of HMM as the detection decision may cause a high probability of false alarm (P_{fa}). To reduce the false alarm rate, we construct a likelihood ratio test (LRT), design the test statistics and calculate the threshold of the hypothesis testing problem based on the estimated mean and variance of the logarithmic received energy.
5) The simulation results show that, through long-term observation, compared to the benchmark schemes, the proposed method can effectively detect jamming attacks under the assumption that the UAV has no prior knowledge and can approach the upper bound of detection performance with complete prior knowledge.

C. Organization

The rest of this paper is organized as follows. In Section II, we introduce the system model and formulate the hypothesis testing problem for jamming detection. In Section III, we detail our proposed method for the formulated problem. In Section IV, the simulation results are provided to show the superiority

Accepted Manuscript
Version of Record at: https://doi.org/10.1109/TCCN.2023.3244539

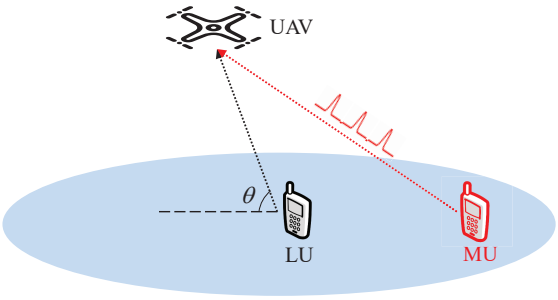


Fig. 1. The considered UAV-assisted wireless communication system under RSPJ.

of the proposed method. Finally, in Section V we conclude this paper.

II. System Model

As shown in Fig. 1, we consider a UAV-assisted wireless communication system, where the UAV is located at $\boldsymbol{\omega}_u = [x_u, y_u, h_u]^{\mathrm{T}} \in \mathbb{R}^{3\times 1}$. The LU [1] served by the UAV is located on the ground with the location $\boldsymbol{\omega}_l = [x_l, y_l]^{\mathrm{T}} \in \mathbb{R}^{2\times 1}$, which can transmit (receive) data to (from) the UAV. In addition to the LU, there is also an MU located at $\boldsymbol{\omega}_m = [x_m, y_m]^{\mathrm{T}} \in \mathbb{R}^{2\times 1}$ on the ground. In this paper, we consider an uplink wireless communication with LU transmitting data to the UAV. Meanwhile, the MU carries out an RSPJ, which may transmit malicious signals to the UAV when the LU is monitored to be active and interferes with only a small portion of LU's data to protect itself from getting detected. To protect the security of the communication system, the UAV processes the received data to distinguish whether the received data is jammed. As we emphasized before, the transmitting power of the LU and MU, the channel propagation characteristics, and the noise power are unknown to the UAV.

A. Channel Model

First, we introduce the channel response from the users to the UAV, which is given by

$$\bar{h} = P_{LoS}(\theta)\beta_0 d^{-\alpha} + P_{NLoS}(\theta)\kappa\beta_0 d^{-\alpha}, \tag{1}$$

where d is the distance between UAV and user, β_0 is the path loss at the reference distance ($d_0 = 1$m) for LoS links, $\kappa \in (0, 1)$ is a real number representing the attenuation loss for non-line-of-sight (NLoS) links, and $P_{LoS}(\theta)$ is the probability of existing an LoS link between the UAV and user when their elevation angle equals to θ, which is given by

$$P_{LoS}(\theta) = \frac{1}{1 + a\,\exp(-b(\theta - a))}, \tag{2}$$

where a and b are the modeling parameters related to the environment. Then, the probability of NLoS links can be obtained by

$$P_{NLoS}(\theta) = 1 - P_{LoS}(\theta). \tag{3}$$

[1]For simplicity, the single-LU scenario is considered in this paper, and our proposed method can be easily extended to multi-LU communication networks.

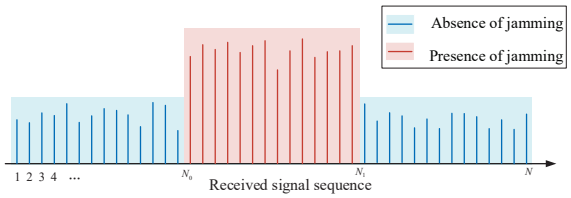


Fig. 2. Received signal under reactive short period jamming.

B. Received Signal Model

For data transmission from the LU to the UAV without jamming, the received signal in discrete form can be given by

$$r(n) = \sqrt{P_l}\bar{h}_l s_l(n) + w(n) = s_0(n) + w(n), \tag{4}$$

where r_n represents the received signal which consists of the transmitted signal affected by the channel response and the complex Gaussian noise $w(n)$ with zero mean and constant variance σ_w^2. Besides, P_l is the transmitting power of the LU, $s_l(n)$ for $n = 1, 2, \cdots, N$ denotes the transmitted complex signal by LU, $\bar{h}_l$ is the channel response between the UAV and LU, $s_0(n)$ for $n = 1, 2, \cdots, N$ means the incoming noise-free signal at the UAV without jamming.

However, once MU manages to sense the active status of the LU, it will corrupt the legal data transmission by injecting false data in LU's signal or transmitting a noise like signal, shown as

$$\tilde{s_e}(n) = \begin{cases} \tilde{s}(n), & \text{inject false data,} \\ \tilde{w}(n), & \text{transmit noise like signal,} \end{cases} \tag{5}$$

where $\tilde{s}(n)$ denotes the injected malicious signal at time n, $\tilde{w}(n)$ represents complex Gaussian noise with zero mean and unit variance transmitted by the MU.

To improve the concealment of itself, as shown in Fig. 2, the MU will decrease jamming time to prevent the UAV from observing significantly increased received signal energy. Therefore, the malicious signal received at the UAV can be expressed as

$$s_e(n) = (u(n - N_0) - u(n - N_1))\tilde{s_e}(n), \tag{6}$$

where N_0 and N_1 represent the start time and end time of the jamming attack, respectively, and $u(n)$ is the unit step signal, i.e., $u(n) = 1$ when $n \geq 0$ and 0 when $n < 0$. Then, the received signal under RSPJ can be given by

$$\begin{aligned} r(n) &= \sqrt{P_l}\bar{h}_l s_l(n) + \sqrt{P_e}\bar{h}_e s_e(n) + w(n) \\ &= s_1(n) + w(n), \end{aligned} \tag{7}$$

where P_e is the transmitting power of MU, $\bar{h}_e$ is the channel response between MU and UAV, $s_1(n)$ for $n = 1, 2, \cdots, N$ is the incoming noise-free signal at the UAV with jamming.

The channel model in Section II.A is called elevation angle-dependent probabilistic LoS model [41], which is widely used in UAV wireless communications [3], [5]. In the angle-dependent probabilistic LoS model, both LoS channel and NLoS channel are considered, where the LoS component depicts the direct path fading and the NLoS component, caused by the reflection effects of the surroundings and obstacles, de-

Accepted Manuscript
Version of Record at: https://doi.org/10.1109/TCCN.2023.3244539

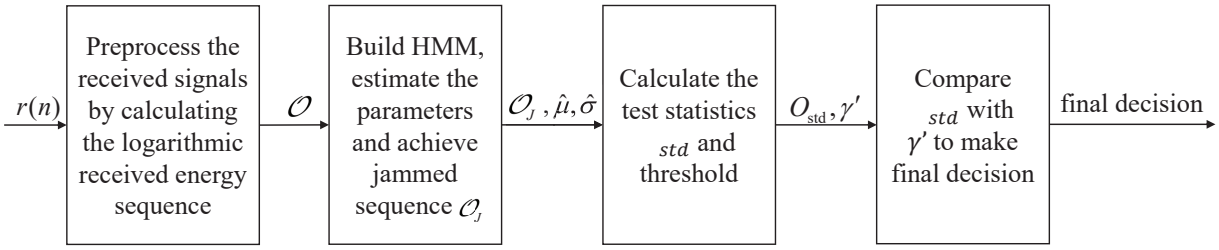


Fig. 3. The flowchart of the overall HBJD scheme.

picts the multipath fading between the receiver and transmitter. Besides, we assume that users and UAV are quasi-static in our scenario, which is common in UAV wireless communications, such as UAV-aided data collection [42] and UAV-aided IoT communication [43]. Therefore, the Doppler shift effects are omitted in this paper.

C. Jamming Detection

It can be concluded from (4) and (7) that different spectrum states correspond to different received signal models. According to the received signal models, the jamming detection problem under RSPJ can be formulated as a binary hypothesis test, expressed by

$$\begin{cases} \mathcal{H}_0 : \mathbf{r} = \mathbf{s}_0 + \mathbf{w}, \\ \mathcal{H}_1 : \mathbf{r} = \mathbf{s}_1 + \mathbf{w}, \end{cases} \tag{8}$$

where $\mathbf{r} = [r(1), r(2), \cdots, r(N)]^{\mathrm{T}}$ denotes the received signals, $\mathbf{w} = [w(1), w(2), \cdots, w(N)]^{\mathrm{T}}$ represents the noise signals, $\mathbf{s}_0 = [s_0(1), s_0(2), \cdots, s_0(N)]^{\mathrm{T}}$ represents the incoming noise-free signals at the UAV without jamming, and $\mathbf{s}_1 = [s_1(1), s_1(2), \cdots, s_1(N)]^{\mathrm{T}}$ means the the incoming noise-free signals at the UAV with jamming. Besides, hypothesis $\mathcal{H}_0$ represents the absence of spectrum jamming during LU's transmission and hypothesis $\mathcal{H}_1$ represents some received signals are jammed by the MU.

It is noteworthy that in the existing works, the statistical characteristics of $\mathbf{r}$ are required to design test statistics and thresholds. For example, in [29], the authors assumed that the noise power, the channel response and the transmitting power are known in prior. Thus, jamming detection can be easily achieved by the ED method. However, in this paper, we assume that UAV cannot use any prior knowledge for hypothesis testing threshold design, which makes the problem in (8) cannot be solved by methods similar to [29]. To solve such a problem, a novel detection scheme is designed in this article. In the next section, we will describe our proposed method in detail, i.e., the HBJD that obtains the statistics of the logarithmic received energy through long-term observation in the static scenario, and designs the detection based on the obtained statistics.

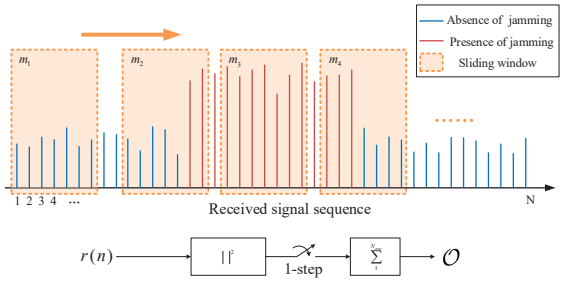


Fig. 4. The preprocessing of received signals, where the received energy is calculated with the sliding window moving 1 step with updating a new signal.

III. Proposed Method

In this section, we detail the proposed HBJD method for solving the hypothesis testing problem in (8), which uses the statistical characteristics of logarithmic received energy in different spectrum states to design test threshold and make the final decision. The basic processing flowchart is shown in Fig. 3 and it is explained in detail below.

A. Signal Preprocessing and Hidden Markov Model

For jamming detection, the received signals are preprocessed by a 1-step sliding window to estimate the received energy of N_{ave} signals, as shown in Fig. 4. The obtained received energy sequence is denoted by $\mathcal{O}_e = \{o_{e,1}, ..., o_{e,m}, ...o_{e,M}\}$, and the m-th sample in $\mathcal{O}_e$ is defined as

$$o_{e,m} = \sum_{i=m}^{m+N_{ave}-1} |r(i)|^2 = \sum_{i=m}^{m+N_{ave}-1} |s(i) + w(i)|^2, \tag{9}$$

where $r(i)$ is the received complex signal superimposed with complex Gaussian noise, and $s(i)$ can be $s_0(i)$ or $s_1(i)$. Then, $\frac{o_{e,m}}{\sigma_w^2}$ has a χ^2 distribution when $s(i)$ is known. Further, we define $o_m = 10\log_{10} o_{e,m}$ and $\mathcal{O} = \{o_1, \cdots, o_m, \cdots, o_M\}$. As can be seen in [38], [44], [45], o_m approximately follows a Gaussian distribution. In addition, considering that the logarithmic value may be less sensitive to changes, in Section III.C, we use the joint distribution of multiple observations to make the final decision to reduce the impact of the insensitivity of a single observation on the detection.

As we can see from Fig. 4, there are three cases of o_m, corresponding to different statistics of the logarithmic received

Accepted Manuscript
Version of Record at: https://doi.org/10.1109/TCCN.2023.3244539

energy. The first one is that there is no jammed signal in the sliding window, whilst the second one is that all the signals in the sliding window are jammed by the MU. These two cases can be exemplified by the regions within the m_1-th and m_3-th sliding windows in Fig. 4, respectively. Besides, signals within a sliding window can also be partially jammed, such as the m_2-th and m_4-th sliding windows in Fig. 4. The values of o_{m_2} and o_{m_4} are excepted to be within the interval between o_{m_1} and o_{m_3}. For the third case, because different lengths of jamming signals in a sliding window correspond to different distributions of the logarithm of received energy, it may be difficult to use a clear statistic to characterize the partially jammed case. After saying so, when the sliding window length is shorter, the third case occurs less. Therefore, we next approximately divide the statistics of logarithmic received energy into two categories according to the spectrum states, i.e., $z_m = 0$ and $z_m = 1$, respectively, representing unjammed and jammed spectrum states. The longer jamming signals in the m-th sliding window, the more likely o_m follows the distribution of $z_m = 1$, vice versa, and otherwise, the more likely o_m follows the distribution of $z_m = 0$. The specific distribution is defined as

$$o_m \sim \mathcal{N}(\mu_0, \sigma_0^2), \quad z_m = 0, \tag{10a}$$
$$o_m \sim \mathcal{N}(\mu_1, \sigma_1^2), \quad z_m = 1, \tag{10b}$$

where μ_i and σ_i are the mean and standard deviation of random variable o_m corresponding to $z_m = i$, $\forall i \in \{0, 1\}$.

From Fig. 4 and (10), we can conclude that the signal transmission process under RSPJ has hidden Markov characteristics: 1) The invisible spectrum state z_m will change over time, which means the spectrum state has Markov characteristics; 2) The observed value o_m, for $m = 1, 2, \cdots, M$, by the UAV from the Gaussian memoryless channel follows different distributions in different spectrum states. Thus, to estimate the statistical parameters of the logarithmic received energies corresponding to different spectrum states, we model an HMM to depict the signal transmission under RSPJ. [2] As shown in Fig. 5, the spectrum state sequence $\mathcal{Z} = \{z_1, \cdots, z_M\}$ and logarithmic received energy sequence $\mathcal{O}$ are regarded as the hidden Markov chain and observable sequence, respectively. The set of required HMM parameters is denoted as $\lambda = \{\pi, G, \mu, \sigma^2\}$, where $\mu = \{\mu_0, \mu_1\}, \sigma = \{\sigma_0, \sigma_1\}$, and λ consists of three parts.

1) Initial distribution of the spectrum state $\pi = \{\pi_0, \pi_1\}$, where π_i represents the probability of $z_1 = i$, $\forall i \in \{0, 1\}$.
2) State transition probability $G = [g_{ik}]_{0 \le i,j \le 1}$, where $g_{ik} = \Pr(z_{m+1} = k | z_m = i)$, for $m = 1, 2, \cdots, M$.
3) The conditional probability density function (PDF) of o_m for $z_m = i$, formulated as $p_{m,i} = \frac{1}{\sqrt{2\pi}\sigma_i} \exp(-\frac{(o_m - \mu_i)^2}{2\,\sigma_i^2})$.

To decide whether the received signals are jammed by the MU, the HMM parameters in λ should be estimated first. Then the hidden spectrum state of each element in the observation sequence $\mathcal{O}$ is decided with the estimated λ according to the maximum MAP criterion. The final decision of jamming detection is made by comparing the statistics of elements with jammed hidden spectrum state in $\mathcal{O}$ with the derived threshold. Such processes will be detailed next.

[2]There may be other methods for classification and parameter estimation, but due to the hidden Markov characteristics of signal transmission, HMM is the most appropriate one. In Section IV, we compare the performance of HMM and SVM, and the superiority of applying HMM can be seen.

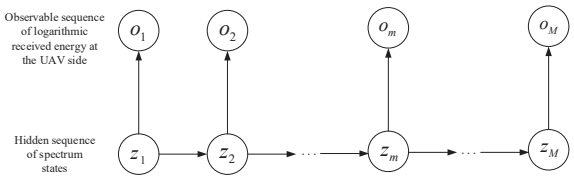


Fig. 5. Hidden Markov Model over M samples of logarithmic received energy.

B. HMM Parameter Estimation

In order to estimate the parameters in λ, we formulate a Maximum Likelihood Estimator (MLE) as

$$\begin{aligned} \hat{\lambda} &= \arg\max_{\lambda} \Pr(\mathcal{O}|\lambda) \\ &= \arg\max_{\lambda} \Pr(o_1, ..., o_m, ..., o_M|\lambda). \end{aligned} \tag{11}$$

The problem in (11) can be addressed with the EM algorithm. The principle of the EM algorithm is to find the maximum log-likelihood estimates of parameters in a statistical model with hidden variables, such as HMM, by shifting between an expectation (E) step and a maximum (M) step. The τ-th E-step formulates the expected log-likelihood function based on the distribution of hidden variables being determined by the optimal parameter $\hat{\lambda}^{(\tau-1)}$ found in the $(\tau-1)$-th M-step, where $\tau = 1, 2, ..., T_{iter}$ and T_{iter} is the maximum number of iterations. Besides, the τ-th M-step obtains the optimal parameters $\hat{\lambda}^{(\tau)}$ which maximize the expected log-likelihood function formulated in the τ-th E-step [46].

According to the EM algorithm, the following parameters in $\hat{\lambda}^{(\tau+1)}$ can be obtained

$$\hat{\pi}_i^{(\tau+1)} = \frac{\Pr(z_1 = i|\mathcal{O}, \hat{\lambda}^{(\tau)})}{\sum_{i=0}^{1} \Pr(z_1 = i|\mathcal{O}, \hat{\lambda}^{(\tau)})}, \tag{12}$$

$$\hat{g}_{ik}^{(\tau+1)} = \frac{\sum_{m=1}^{M} \Pr(z_m = i, z_{m+1} = k|\mathcal{O}, \hat{\lambda}^{(\tau)})}{\sum_{k=0}^{1} \sum_{m=1}^{M} \Pr(z_m = i, z_{m+1} = k|\mathcal{O}, \hat{\lambda}^{(\tau)})}, \tag{13}$$

$$\hat{\mu}_i^{(\tau+1)} = \frac{\sum_{m=1}^{M} \Pr(z_m = i|\mathcal{O}, \hat{\lambda}^{(\tau)}) o_m}{\sum_{m=1}^{M} \Pr(z_m = i|\mathcal{O}, \hat{\lambda}^{(\tau)})}, \tag{14}$$

$$\hat{\sigma}_i^{2(\tau+1)} = \frac{\sum_{m=1}^{M} \Pr(z_m = i|\mathcal{O}, \hat{\lambda}^{(\tau)}) (o_m - \hat{\mu}_i^{(\tau)})^2}{\sum_{m=1}^{M} \Pr(z_m = i|\mathcal{O}, \hat{\lambda}^{(\tau)})}. \tag{15}$$

Note that direct calculation of $\Pr(z_m = i, z_{m+1} = k|\mathcal{O}, \hat{\lambda}^{(\tau)})$ and $\Pr(z_m = i|\mathcal{O}, \hat{\lambda}^{(\tau)})$ for $m = 1, 2, \cdots, M$ can induce high computational complexity of $O(M \times 2^M)$ when M is large. To simplify the calculation, we define the following intermediate variables:

1) The forward recursion factor $\alpha^{(\tau)} = \left\{\alpha_1^{(\tau)}, \cdots, \alpha_M^{(\tau)}\right\}$, where $\alpha_m^{(\tau)} = \{\alpha_m^{(\tau)}(0), \alpha_m^{(\tau)}(1)\}$, for $m = \{1, 2, \cdots, M\}$, represents the conditional joint probability defined as

$$\alpha_m^{(\tau)}(i) = \Pr(o_1, ..., o_m, z_m = i|\hat{\lambda}^{(\tau)}), \tag{16}$$

where $i = 0, 1$. Obviously, $\alpha_m(i)$ can be updated in an iterative manner as

$$\alpha_m^{(\tau)}(i) = \sum_{k=0}^{1} \alpha_{m-1}^{(\tau)}(k)\hat{g}_{ki}^{(\tau)}\hat{p}_{m,i}^{(\tau)}, \tag{17}$$

where $m = 2, 3, ..., M$. Besides, we have $\alpha_1^{(\tau)}(i) = \hat{\pi}_i^{(\tau)}\hat{p}_{1,i}^{(\tau)}$.

2) The backward recursion factor $\beta^{(\tau)} = \left\{\beta_1^{(\tau)}, \cdots, \beta_M^{(\tau)}\right\}$, where $\beta_m^{(\tau)} = \{\beta_m^{(\tau)}(0), \beta_m^{(\tau)}(1)\}$, for $m = 1, 2, \cdots, M$, means the conditional probability defined as

$$\beta_m^{(\tau)}(i) = \Pr(o_{m+1}, ..., o_M|z_m = i, \hat{\lambda}^{(\tau)}). \tag{18}$$

Similarly, $i \in \{0, 1\}$ and $\beta_m^{(\tau)}(i)$ can be updated as

$$\beta_m^{(\tau)}(i) = \sum_{k=0}^{1} \beta_{m+1}{}^{(\tau)}(k)\hat{g}_{ik}^{(\tau)}\hat{p}_{m+1,i}^{(\tau)}, \tag{19}$$

where $m = 1, 2, \cdots, M-1$ and $\beta_M^{(\tau)}(i) = 1$.

After the recursive calculation of $\alpha^{(\tau)}$ and $\beta^{(\tau)}$, $\Pr(z_m = i, z_{m+1} = k|\mathcal{O}, \lambda^{(\tau)})$ and $\Pr(z_m = i|\mathcal{O}, \lambda^{(\tau)})$ can be derived as

$$\Pr(z_m = i|\mathcal{O}, \hat{\lambda}^{(\tau)}) = \frac{\alpha_m^{(\tau)}(i)\beta_m^{(\tau)}(i)}{\sum_{i=0}^{1} \alpha_m^{(\tau)}(i)\beta_m^{(\tau)}(i)}, \tag{20}$$

and

$$\Pr(z_m = i, z_{m+1} = k|\mathcal{O}, \hat{\lambda}^{(\tau)}) = \frac{\alpha_m^{(\tau)}(i)\hat{g}_{ik}^{(\tau)}\beta_{m+1}^{(\tau)}(k)\hat{p}_{m+1,k}^{(\tau)}}{\sum_{i=0}^{1}\sum_{k=0}^{1} \alpha_m^{(\tau)}(i)\hat{g}_{ik}^{(\tau)}\beta_{m+1}^{(\tau)}(k)\hat{p}_{m+1,k}^{(\tau)}}. \tag{21}$$

By substituting (20) and (21) into (13)-(15), the final expressions of $\lambda^{(\tau+1)}$ with respect to $\lambda^{(\tau)}$ for $\tau = 1, 2, \cdots, T_{iter}$ can be obtained.

Continue the parameter estimation process in (12)−(15) until the maximum number of iterations T_{iter} is reached or the parameter values converge to a certain extent. The final estimation of the HMM parameters according to the observed sequence $\mathcal{O}$ is denoted as $\hat{\lambda}$. Based on $\hat{\lambda}$, the hidden state $\hat{z}_m$ can be estimated according to the MAP criterion

$$\hat{z}_m = \arg\max_{z_m} \Pr(z_m|\mathcal{O}, \hat{\lambda}). \tag{22}$$

Details of the HMM parameter estimation algorithm are presented in Algorithm 1.

Algorithm 1: HMM parameter estimation algorithm

Input:
The observation sequence $\mathcal{O} = \{o_1, \cdots, o_M\}$;
The maximum number of iterations T_{iter}
Output:
Estimated HMM parameter set $\hat{\lambda}$;
Estimated state sequence $\hat{\mathcal{Z}} = \{\hat{z}_1, \cdots, \hat{z}_M\}$

```
Initialize λ^(0) = {π^(0), G^(0), μ^(0), σ^(0)};
for τ = 1 : T_iter do
    Calculate the forward recursion factor α^(τ) and
    backward recursion factor β^(τ) according to λ̂^(τ−1).
    For each m = {1, ··· , M}, calculate
    Pr(z_m = i|O, λ̂^(τ−1)) and
    Pr(z_m = i, z_{m+1} = k|O, λ̂^(τ−1)).
    Update λ̂^(τ) according to (12)−(15).
end for
λ̂ = λ̂^(τ).
Estimate ẑ_m according to (22).
return λ̂, Ẑ
```

C. Final Decision Making

After the estimation of HMM parameters, we obtain the statistics of logarithmic received energy under different spectrum states, i.e., $\left(\hat{\mu}_0, \hat{\sigma}_0^2\right)$ and $\left(\hat{\mu}_1, \hat{\sigma}_1^2\right)$. Then the hidden spectrum state corresponding to each element in $\mathcal{O}$ can be estimated according to (22), and the obtained set of logarithmic received energy with jammed state can be, for convenience, denoted as $\mathcal{O}_J = \{o_1, o_2, \cdots, o_J\}$, where $\mathcal{O}_J \subsetneq \mathcal{O}$ and $\hat{z}_j = 1$, for $j = 1, 2, \cdots, J$ with $J < M$. Unfortunately, due to the randomness of the received signals, $\mathcal{O}_J$ may not be empty even when there is no jamming. Therefore, directly taking the detection result of HMM as the final decision can cause a high P_{fa}. To avoid this issue, we make a modification to detect whether the received data sequence is jammed according to O_J.

The distributions of o_j under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ are

$$\begin{cases} \mathcal{H}_0 : o_j \sim \mathcal{N}\left(\hat{\mu}_0, \hat{\sigma}_0^2\right), j = 1, 2, \ldots, J, \\ \mathcal{H}_1 : o_j \sim \mathcal{N}\left(\hat{\mu}_1, \hat{\sigma}_1^2\right), j = 1, 2, \ldots, J. \end{cases} \tag{23}$$

According to the Neyman-Pearson (NP) Lemma, we exploit the likelihood ratio test (LRT) to decide which hypothesis is true. Specifically, the LRT can be given as

$$\begin{aligned} L\left(\mathcal{O}_J\right) &= \frac{p\left(\mathcal{O}_J; \mathcal{H}_1\right)}{p\left(\mathcal{O}_J; \mathcal{H}_0\right)} \\ &= \frac{\left(2\pi\hat{\sigma}_1^2\right)^{-J/2} \exp\left(-\frac{1}{2\hat{\sigma}_1^2}\sum_{j=1}^{J}\left(o_j - \hat{\mu}_1\right)^2\right)}{\left(2\pi\hat{\sigma}_0^2\right)^{-J/2} \exp\left(-\frac{1}{2\hat{\sigma}_0^2}\sum_{j=1}^{J}\left(o_j - \hat{\mu}_0\right)^2\right)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma, \end{aligned} \tag{24}$$

where $p(\mathcal{O}_J; \mathcal{H}_i)$ is the joint PDF of $\mathcal{O}_J$ under hypothesis $\mathcal{H}_i$. By applying logarithmic operation on both sides of (24), we

can obtain

$$\frac{\hat{\sigma}_1^2-\hat{\sigma}_0^2}{2\hat{\sigma}_0^2\hat{\sigma}_1^2}\sum_{j=1}^{J}o_j^2+\frac{\hat{\mu}_1\hat{\sigma}_0^2-\hat{\mu}_0\hat{\sigma}_1^2}{\hat{\sigma}_0^2\hat{\sigma}_1^2}\sum_{j=1}^{J}o_j\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\log\left(\gamma\cdot\left(\frac{\hat{\sigma}_1}{\hat{\sigma}_0}\right)^J\right)-\frac{J\left(\hat{\mu}_0^2\hat{\sigma}_1^2-\hat{\mu}_1^2\hat{\sigma}_0^2\right)}{2\hat{\sigma}_0^2\hat{\sigma}_1^2}. \tag{25}$$

Because there are two test statistics in (25), $\sum_{j=1}^{J}o_j^2$ and $\sum_{j=1}^{J}o_j$, it is difficult to construct a unique threshold from (25). To propose a simple detector, we eliminate the first component of the left side and normalize o_j as

$$o_{std,j}=\frac{o_j}{\mathrm{var}\left(\mathcal{O}_J\right)}, \tag{26}$$

where $\mathrm{var}\left(\mathcal{O}_J\right)$ represents the standard deviation of $\mathcal{O}_J$. Consequently, we can obtain the following hypotheses

$$\begin{cases}\mathcal{H}_0: o_{std,j}\sim\mathcal{N}\left(\frac{\hat{\mu}_0}{\hat{\sigma}_0},1\right), j=1,2,\cdots,J,\\ \mathcal{H}_1: o_{std,j}\sim\mathcal{N}\left(\frac{\hat{\mu}_1}{\hat{\sigma}_1},1\right), j=1,2,\cdots,J.\end{cases} \tag{27}$$

Then, by substituting (27) into (25), where $o_j\sim\mathcal{N}\left(\hat{\mu},\hat{\sigma}\right)$ is replaced with $o_{std,j}\sim\mathcal{N}\left(\frac{\hat{\mu}}{\hat{\sigma}},1\right)$, we have

$$\left(\frac{\hat{\mu}_1}{\hat{\sigma}_1}-\frac{\hat{\mu}_0}{\hat{\sigma}_0}\right)\sum_{j=1}^{J}o_{std,j}\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\log\gamma-\frac{J}{2}\left(\frac{\hat{\mu}_0^2}{\hat{\sigma}_0^2}-\frac{\hat{\mu}_1^2}{\hat{\sigma}_1^2}\right), \tag{28}$$

where $\sum_{j=1}^{J}o_{std,j}$ is the test statistic and the first component of the left hand side in (25) has been removed. However, the distribution of $\sum_{j=1}^{J}o_{std,j}$ is difficult to be described by the classical probability model, and the definite detection threshold cannot be derived based on (28). Therefore, we further define a new test statistic as

$$O_{std}=\frac{1}{\sqrt{J}}\sum_{j=1}^{J}\frac{o_j}{\sigma'}, \tag{29}$$

and σ' means the sample standard deviation, i.e.,

$$\sigma'=\sqrt{\frac{1}{J-1}\sum_{j=1}^{J}\left(o_j-\mu'\right)^2}, \tag{30}$$

where $\mu'=\frac{1}{J}\sum_{j=1}^{J}o_j$ representing the sample mean value of $\mathcal{O}_J$.

Then, to calculate the threshold of O_{std} for jamming detection, the statistical distribution of O_{std} in different spectrum states must be determined, which is given in the following proposition.

Proposition 1.

$$\begin{cases}\mathcal{H}_0: O_{std}\sim t\left(J-1,\sqrt{J}\frac{\hat{\mu}_0}{\hat{\sigma}_0}\right),\\ \mathcal{H}_1: O_{std}\sim t\left(J-1,\sqrt{J}\frac{\hat{\mu}_1}{\hat{\sigma}_1}\right),\end{cases} \tag{31}$$

where $t\left(J-1,\sqrt{J}\frac{\mu}{\sigma}\right)$ *represents* t *distribution with* $J-1$ *degrees of freedom and non-centrality parameter* $\frac{\mu}{\sigma}$.

Proof. See Appendix A. □

Algorithm 2: Final decision making algorithm

Input:
The observation sequence $\mathcal{O}=\{o_1,\cdots,o_M\}$;
State sequence $\mathcal{Z}=\{z_1,\cdots,z_M\}$
Output:
The final decision
Initialize empty sequence $\mathcal{O}_J$.
for $m=1:M$ **do**
  if $z_m==1$ **then**
    Add o_m to sequence $\mathcal{O}_J$.
  end if
end for
Calculate O_{std}, c_0 and c_1.
if $c_0\le c_1$ **then**
  Calculate the threshold γ' according to (33) and make final decision.
else
  Calculate the threshold γ' according to (34) and make final decision.
end if
return final decision

Under different hypotheses, the distribution parameters of O_{std} are different. The non-centrality parameter of the two distributions in (31) can be calculated as

$$c_i=\sqrt{J}\frac{\hat{\mu}_i}{\hat{\sigma}_i},\quad\forall i\in\{0,1\}. \tag{32}$$

Finally, we obtain a test statistic that follows t-distribution with the non-central parameter given by (32), which may be helpful to derive a clear detection threshold. In different cases, the jamming decision threshold γ' can be designed according to the constraint on the probability of false alarm, which is generally predefined and denoted as P_{FA}.

1) $c_0\le c_1$

$$\gamma'=t^{-1}_{n=J-1,\Delta=\sqrt{J}\frac{\hat{\mu}_0}{\hat{\sigma}_0}}\left(1-P_{FA}\right). \tag{33}$$

With the threshold calculated in (33), the decision can be made by comparing O_{std} with γ'. Specifically, when $O_{std}\ge\gamma'$, the received signals will be claimed to be jammed and normal otherwise.

2) $c_0>c_1$

$$\gamma'=t^{-1}_{n=J-1,\Delta=\sqrt{J}\frac{\hat{\mu}_0}{\hat{\sigma}_0}}\left(P_{FA}\right). \tag{34}$$

When $O_{std}\le\gamma'$, the received signals will be claimed to be jammed and normal otherwise.

The scheme of final decision making is detailed in Algorithm 2.

D. Computational Complexity Analysis

The computational complexity of the whole proposed jamming detection scheme is analyzed in this subsection. As shown in Fig. 3, in signal preprocessing, the computational

Accepted Manuscript
Version of Record at: https://doi.org/10.1109/TCCN.2023.3244539

complexity is $O(M \times N_{ave})$ in terms of complex multiplication and addition. In HMM parameter estimation, which is presented in Algorithm 1, let D represent the number of spectrum states. In each iteration, the computational complexity of calculating a single forward recursion factor $\alpha_m^{(\tau)}(i)$ is $O(D)$. Therefore, in line 3, the complexity of obtaining $\alpha^{(\tau)}$ is $O(M \times D^2)$, and the same is for calculating $\beta^{(\tau)}$. In (20) and (21), the numbers of real number multiplication are $O(D)$ and $O(D^2)$, respectively. Thus, the complexity of line 4 is $O(M \times D^2)$. The complexity of (12)-(15) are $O(D)$, $O(M \times D)$, $O(M)$, and $O(M)$, respectively. Therefore, line 5 has the complexity of $O(M \times D^2)$. Since the iteration number is T_{iter}, the overall computational complexity of Algorithm 1 is $O(M \times D^2 \times T_{iter})$. Since we have $D = 2$ in HMM, which can be ignored compared with M and T_{iter}, the complexity can be written as $O(M \times T_{iter})$. In the final decision described in Algorithm 2, the complexity is $O(M + J)$. Since $J < M$, the complexity can be simplified as $O(M)$. In summary, the computational complexity of the whole scheme is $O(M \times (N_{ave} + T_{iter}))$.

IV. Numerical Results

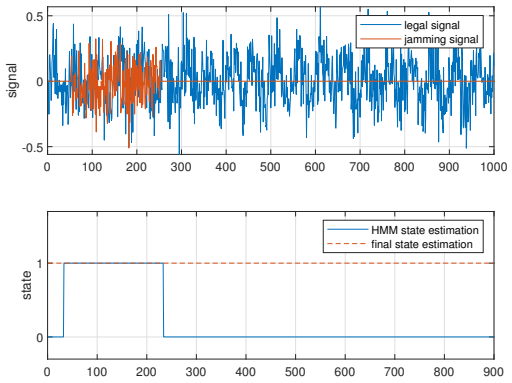
In this section, the performance of the proposed algorithm is evaluated via simulations. Specifically, we investigate the performance of HBJD under varying SNR and SIR, which is defined as the ratio of signal power to jamming power, at first. Then, we use the Receiver Operating Characteristic (ROC) curves to evaluate the probability of detection (P_d) of HBJD under various constraints of P_{FA}. The parameter settings in simulations are shown in Table II.

The real part of the received signal, the performance of HMM state estimation and final decision making are presented in Fig. 6, where states 0 and 1 represent the situation of jamming absence and jamming presence, respectively. As shown in Fig. 6(a), when the received signal is partially jammed, several samples among the logarithmic received energy sequence are estimated to be jammed according to HMM and the spectrum state is detected to be jammed after final decision making. Besides, in Fig. 6(b), the spectrum jamming attack is absent. In this paper, we assume that there are two hidden states, i.e., the spectrum is jammed or unjammed. For estimating parameters, HMM first divides the observation sequence into two clusters, and then alternately iterates the parameter estimation and sequence classification to obtain the final estimation results. During the whole process of HMM parameter estimation, any set of observation samples corresponding to the hidden spectrum state will not be empty. As a result, there are still a few logarithmic received energy samples being estimated though the jamming is absent, causing a high false alarm probability. Fortunately, with the help of final decision making, the false alarm probability and the true spectrum state can be modified.

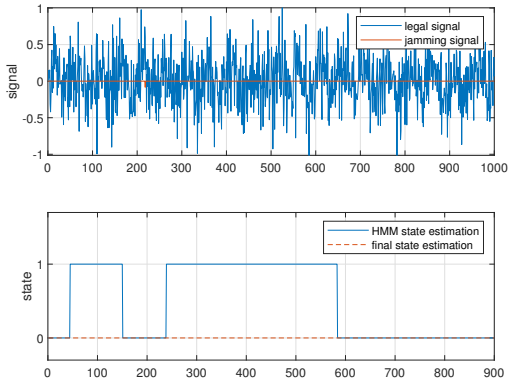
TABLE II
Simulation Parameters

Parameter	Physical Meaning	Value
β_0	Path loss parameter	7×10^{-5} [41]
κ	Attenuation loss parameter	0.01 [41]
α	Path loss exponent	2 [41]
N	The number of samples	1000
P_s	The transmitting power	0.01 w
T_{iter}	The maximum number of iteration	200

Next, we present numerical results to demonstrate the performance superiority of the proposed HBJD method. Each point is an average result of 5,000 different simulations. We choose the energy detection (ED) algorithm, which is the most widely used algorithm in spectrum sensing and jamming detection, as one of the benchmark schemes in the simulation. The energy of the received signals is calculated and compared with a predetermined threshold. If the energy is higher than the threshold, the spectrum is claimed to be jammed. Following the processing in [47], when the signal power, the noise power and the path loss are unknown, i.e., no prior knowledge, the threshold for ED is calculated based on the estimation of the received signal energy using the first 1/4 part of the samples. Besides, if the signal power, the noise power and the path loss are known, i.e., complete prior knowledge, the optimal



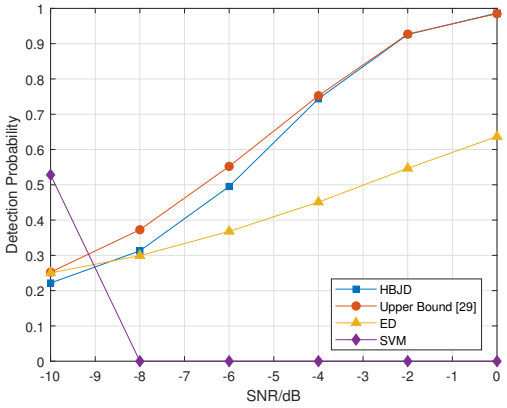
(a) Received signal sequence, estimated results of HMM and final decided spectrum state when jamming is present.



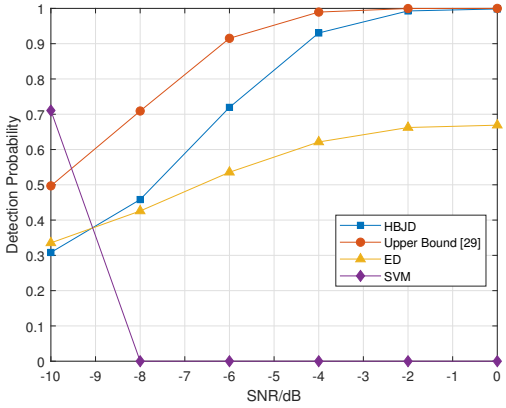
(b) Received signal sequence, estimated results of HMM and final decided spectrum state when jamming is absent.

Fig. 6. Final decided spectrum state, estimated spectrum state of each sample according to HMM and real received signal sequence in the presence and absence of jamming, where the horizontal axis is the sample index, 0 and 1 indicate that the sample is not jammed and jammed, respectively.

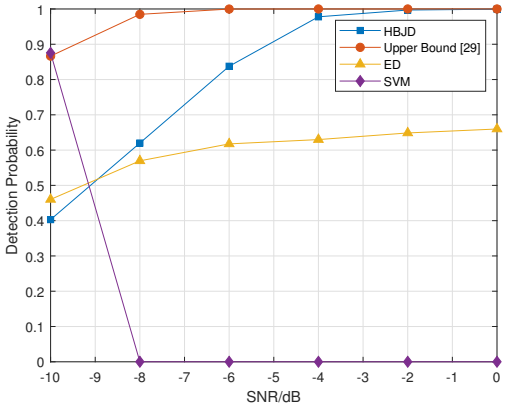
Accepted Manuscript
Version of Record at: https://doi.org/10.1109/TCCN.2023.3244539



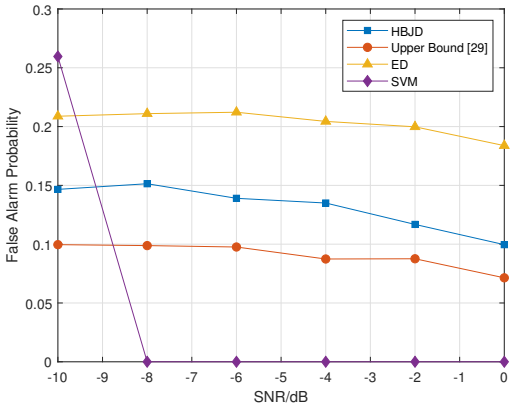
(a) Comparison of detection probability with varying SNR when using different jamming detection algorithms, where the jamming ratio is 0.125.



(b) Comparison of detection probability with varying SNR when using different jamming detection algorithms, where the jamming ratio is 0.25.



(c) Comparison of detection probability with varying SNR when using different jamming detection algorithms, where the jamming ratio is 0.5.



(d) Comparison of false alarm probability with varying SNR when using different jamming detection algorithms.

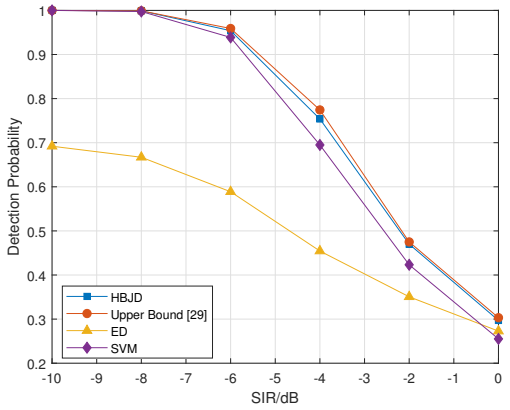
Fig. 7. The comparison of detection performance under varying SNR between the proposed HBJD scheme, SVM, energy detection without prior knowledge and energy detection with complete prior knowledge.

threshold can be easily calculated with the analysis in [29]. The performance of the scheme based on the optimal threshold can be viewed as the upper bound of the jamming detection method. What's more, we also design another benchmark based on SVM, which uses 1000 samples of received signal energy without jamming and 1000 samples of received signal energy with jamming as training data.

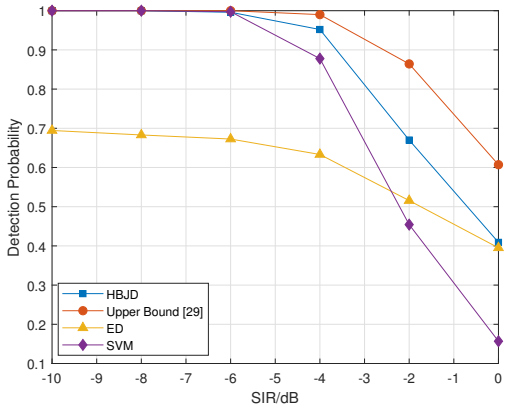
The result of comparing P_d and P_{fa} when using different algorithms under varying SNR is shown in Fig. 7. Figs. 7(a), 7(b), and 7(c) show the comparison of P_d with varying SNR, where the SIR is set to be -4 dB. It can be seen that SVM can only achieve jamming detection under the training condition of SNR = -10 dB. Once the SNR changes, SVM cannot detect jamming attacks effectively. This is because the SVM is only trained under the condition of SNR = -10 dB, and under other conditions, the trained SVM when SNR = -10 dB is directly applied for detecting jamming without retraining. This phenomenon shows that the machine learning based jamming detection methods can only be applied in a specific environment. Once the environmental characteristics, e.g. SNR, change, such methods have to be retrained for detecting jamming. Besides, for the other three detection schemes, it can be observed that with increasing SNR, the detection probability improves and finally approaches to 1. This is because the reduction of noise power makes it easier to distinguish jammed samples from unjammed ones in the received signal sequence. Furthermore, with a fixed SNR, the higher jamming ratio brings higher detection probability, since longer jamming time leads to more jammed samples, and the parameters can be estimated to be more precise. Moreover, the P_d of ED being higher than that of HBJD when the SNR is low does not indicate that the detection performance of ED outperforms HBJD under low SNR conditions. Actually, such a result comes from the inaccurate estimation of received signal energy caused by high noise power, which also induces high P_{fa}, just as shown in Fig. 7(d).

The result of comparing P_d when using different algorithms under varying SIR is shown in Fig. 8. It can be observed that the detection performance of all schemes decreases with the SIR increasing. This is because when SIR increases, the

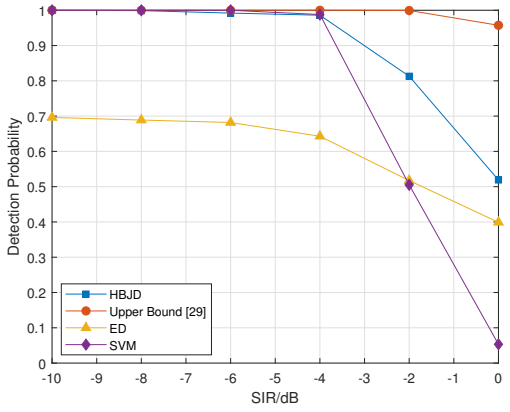
Accepted Manuscript
Version of Record at: https://doi.org/10.1109/TCCN.2023.3244539



(a) Comparison of detection probability with varying SIR when using different jamming detection algorithms, where the jamming ratio is 0.125.



(b) Comparison of detection probability with varying SIR when using different jamming detection algorithms, where the jamming ratio is 0.25.



(c) Comparison of detection probability with varying SIR when using different jamming detection algorithms, where the jamming ratio is 0.5.

Fig. 8. The comparison of detection performance under varying SIR between the proposed HBJD scheme, SVM, energy detection without prior knowledge and energy detection with complete prior knowledge.

difference between the received signal energy when jamming presence and jamming absence becomes less obvious, which makes spectrum jamming detection more difficult. Meanwhile, with fixed SIR, the detection probability of HBJD is signifi-

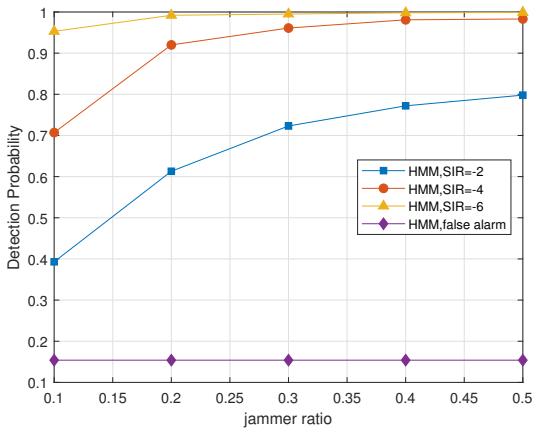


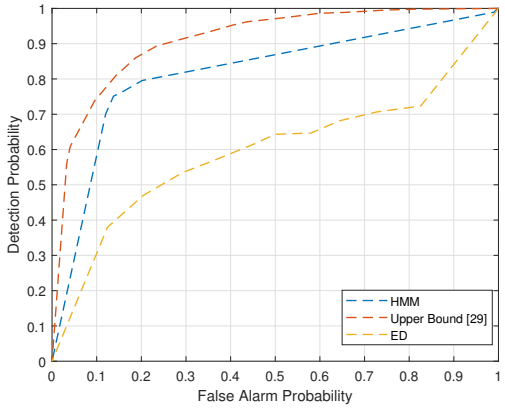
Fig. 9. Detection performance of HBJD versus jamming ratio under different values of SIR.

cantly better than ED and close to Upper Bound, and as SIR increases, the superiority of HBJD over SVM becomes more obvious. What's more, we compare the detection performance of HBJD with the varying jamming ratio in Fig. 9. It can be seen that, as the jamming ratio increases, the detection probability of HBJD becomes higher. Similar to the reason of Fig. 7, a higher proportion of jamming signals produces more samples being jammed, and the corresponding parameters are estimated more accurately. On the other hand, the false alarm probability of HBJD is unrelated to the jamming ratio, which is because false alarms will only occur when jamming is absent. Taking Figs. 7, 8 and 9 into consideration, we can conclude that HBJD can achieve considerable detection performance for reactive short period jamming. Besides, compared to the other benchmarks, HBJD does not require any prior knowledge, such as the statistical characteristics of received signal energy and reference data, which proves the feasibility of HBJD in practical UAV-assisted wireless communications.

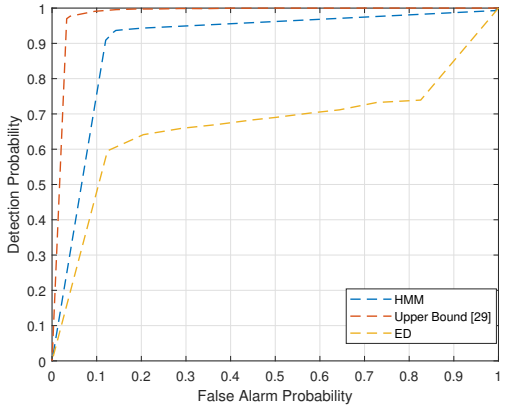
Then, the ROC curves of different jamming detection algorithms, i.e., curves of detection probability versus false alarm probability, are compared in Fig. 10 under various jamming ratios of 0.125, 0.25 and 0.5. As shown in Fig. 10, under the constraints of P_{FA} over a wide range, the P_d of the proposed HBJD method is significantly better than that of ED on a large scale. Besides, under the same P_{FA}, the P_d of HBJD can approach the upper bound. Both the phenomena of better than ED and close to upper bound can be observed under different ratios of jamming, as shown in Figs. 10(a), 10(b) and 10(c). In addition, when the ratio of jamming increases, the detection of jamming attacks becomes easier. However, HBJD still achieves good performance at a low jamming ratio. As shown in Fig. 10(a), when $P_{FA} = 0.2$, the P_d of HBJD can be 0.8, compared to $P_d = 0.47$ of ED, the probability of detection has been improved by 70%. Fig. 10 demonstrates the superiority of HBJD in the detection of jamming attacks in UAV-assisted wireless communication systems, that is, detecting jamming effectively without requiring prior knowledge.

Finally, we discuss the effect of the length of the sliding window on the performance of jamming detection. As shown in Fig. 11, when the window length is relatively small, i.e.,

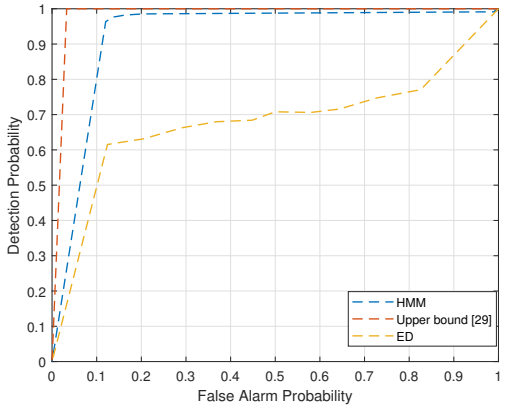
Accepted Manuscript
Version of Record at: https://doi.org/10.1109/TCCN.2023.3244539



(a) Detection probability versus false alarm probability under different schemes, where the jamming ratio is 0.125.



(b) Detection probability versus false alarm probability under different schemes, where the jamming ratio is 0.25.



(c) Detection probability versus false alarm probability under different schemes, where the jamming ratio is 0.5.

Fig. 10. Detection performance versus false alarm probability of using HBJD, energy detection with no prior knowledge, i.e., ED, and energy detection with complete prior knowledge, i.e. Upper bound.

$N_{ave} = 50$, the influence of noise signal is difficult to be eliminated by smoothing. Thus, under the strict false alarm constraints ($P_{FA} \leq 0.1$), the detection performance of HBJD when $N_{ave} = 50$ is worse than that of other window lengths. As for the jamming detection performance under other window length settings, it seems that increasing the length of the sliding window can not improve the jamming detection performance. To find out the most suitable window length in a certain jamming ratio, it is necessary to carry out multiple tests and choose window length by comparing detection performance.

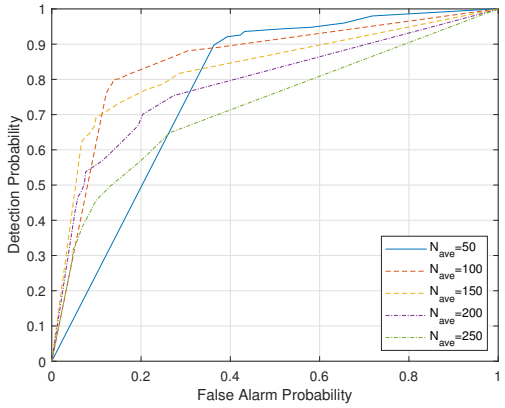


Fig. 11. Detection performance versus false alarm probability of using HBJD under different lengths of the sliding window when the jamming ratio is 0.125.

V. Conclusion and Future Perspectives

In this paper, a jamming detection method based on HMM is proposed, aiming to detect reactive short period jamming without prior knowledge of signal or channel characteristics for UAV-assisted wireless communications. We first process the received signals with a sliding window to calculate the logarithmic received energy and formulate an HMM to represent the data transmission process attacked by RSPJ. Then, to obtain the statistics of the logarithmic received energy in different spectrum states, we use the EM algorithm to estimate the parameters of HMM. Finally, to make a final decision with a low probability of false alarm, a concise test statistic is designed and the distributions of the test statistics in different states are derived according to the mean and variance of the logarithmic received energy, which are elements of the estimated HMM parameters. The numerical results show that through long-term observation, the proposed solution can effectively detect stealthy jamming under the assumption that the UAV has no prior knowledge of transmission power, path loss or noise power, and can approach the upper bound of jamming detection performance with the complete prior knowledge.

Aside from jamming detection in static environments, it is also important to jointly optimize the detection method and UAV trajectory in dynamic environments, which can improve the service performance of UAVs in dynamic scenarios such as jamming source tracking. In addition, due to the influence of Doppler effects and fast fading channels in dynamic environments, it is difficult to obtain the closed-form solution of detection probability and signal characteristics to solve the problem of hypothesis testing. Therefore, it is of great significance to design real-time accurate estimation methods to improve the estimation accuracy of signal and channel statistical characteristics to solve the hypothesis testing problems of jamming detection in dynamic environments. Detailed research will be set aside as our future work.

APPENDIX A
THE PROOF OF PROPOSITION 1

First, we know that if $x_1, x_2, ..., x_n$ are n independent samples follow a Gaussian distribution with standard deviation σ, and sample mean $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$, the sample variance $D(x) = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2$ will follow a non-central χ^2 with $(n-1)$ degrees of freedom. Besides, the distribution of $(n-1)\frac{D(x)}{\sigma^2}$ can be given by

$$(n-1)\frac{D(x)}{\sigma^2} \sim \chi^2_{n-1}. \tag{35}$$

We also know that if X follows a normal distribution with zero mean and unit variance, and Y is a χ^2 random variable with n degrees of freedom which is independent of X,

$$Z = \frac{X + \Delta}{\sqrt{Y/n}} \tag{36}$$

will follow a non-central t distribution with n degrees of freedom and non-centrality parameter Δ, which means $Z \sim t(n, \Delta)$.

Recall O_{std} in (29), which can be rewritten as

$$O_{std} = \frac{\frac{1}{\sqrt{J}}\sum_{j=1}^{J}\frac{o_j}{\hat{\sigma}}}{\sqrt{\frac{(J-1)\sigma'^2}{(J-1)\hat{\sigma}^2}}}, \tag{37}$$

where $\hat{\sigma}$ and σ' are given by (15) and (30), respectively. According to the analysis mentioned before, o_j approximately follows a Gaussian distribution with mean $\hat{\mu}$ and standard deviation $\hat{\sigma}$. Therefore, we can obtain the distribution of the numerator in (37) as

$$\frac{1}{\sqrt{J}}\sum_{j=1}^{J}\frac{o_j}{\hat{\sigma}} \sim \sqrt{J}\frac{\hat{\mu}}{\hat{\sigma}} + \mathcal{N}(0,1). \tag{38}$$

Then, we can conclude

$$(J-1)\frac{\sigma'}{\hat{\sigma}} \sim \chi^2_{J-1}. \tag{39}$$

Finally, based on the results in (36) , (38) and (39), we can draw the conclusion in (31).

REFERENCES

[1] Z. Xiao, P. Xia, and X.-G. Xia, "Enabling UAV cellular with millimeter-wave communication: Potentials and approaches," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 66–73, May 2016.

[2] Z. Xiao, L. Zhu, and X.-G. Xia, "UAV communications with millimeter-wave beamforming: Potentials, scenarios, and challenges," *China Commun.*, vol. 17, no. 9, pp. 147–166, Sep. 2020.

[3] C. Zhang, L. Zhang, L. Zhu, T. Zhang, Z. Xiao, and X.-G. Xia, "3D deployment of multiple UAV-mounted base stations for UAV communications," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2473–2488, Apr. 2021.

[4] Z. Ullah, F. Al-Turjman, and L. Mostarda, "Cognition in UAV-aided 5G and beyond communications: A survey," *IEEE Trans. Cog.*, vol. 6, no. 3, pp. 872–891, Jan. 2020.

[5] Y. Liu, K. Liu, J. Han, L. Zhu, Z. Xiao, and X.-G. Xia, "Resource allocation and 3-D placement for UAV-enabled energy-efficient IoT communications," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1322–1333, Feb. 2021.

[6] K. Miranda, A. Molinaro, and T. Razafindralambo, "A survey on rapidly deployable solutions for post-disaster networks," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 117–123, Apr. 2016.

[7] Z. Xiao, L. Zhu, Y. Liu, P. Yi, R. Zhang, X.-G. Xia, and R. Schober, "A survey on millimeter-wave beamforming enabled UAV communications and networking," *IEEE Commun. Surveys Tutor.*, vol. 24, no. 1, pp. 557–610, 1st Quart. 2022.

[8] L. Zhu, J. Zhang, Z. Xiao, X. Cao, D. O. Wu, and X.-G. Xia, "Millimeter-wave NOMA with user grouping, power allocation and hybrid beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5065–5079, Nov. 2019.

[9] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: Interaction between source, eavesdropper, and friendly jammer," *EURASIP J. Wireless Commun. Netw. (Special Issue on Wireless Physical Layer Security)*, vol. 2009, pp. 1–10, Jun. 2010.

[10] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. MobiHoc*, NY, May 2005, p. 46–57.

[11] A. Toma, A. Krayani, M. Farrukh, H. Qi, L. Marcenaro, Y. Gao, and C. S. Regazzoni, "AI-based abnormality detection at the PHY-layer of cognitive radio by learning generative models," *IEEE Trans. Cog.*, vol. 6, no. 1, pp. 21–34, Mar. 2020.

[12] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tutor.*, vol. 13, no. 2, pp. 245–257, 2nd Quart. 2011.

[13] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tutor.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart. 2019.

[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] H. Jung, B. V. Nguyen, I. Song, and K. Kim, "Design of anti-jamming waveforms for time-hopping spread spectrum systems in tone jamming environments," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 728–737, Jan. 2020.

[16] 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.

[17] J.-M. Park, J. H. Reed, A. A. Beex, T. C. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing," *Proc. IEEE*, vol. 102, no. 3, pp. 270–281, Mar. 2014.

[18] Z. Zhang, L. Yang, Y. Zhu, B. Y. Zhao, and H. Zheng, "Enforcing dynamic spectrum access with spectrum permits," in *Proc. 20th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Seoul, Oct. 2012, pp. 195–204.

[19] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[20] V. Kumar, J.-M. J. Park, and K. Bian, "PHY-layer authentication using duobinary signaling for spectrum enforcement," *IEEE Trans. Inf. Forensics Security.*, vol. 11, no. 5, pp. 1027–1038, May 2016.

[21] C. Sorrells, P. Potier, L. Qian, and X. Li, "Anomalous spectrum usage attack detection in cognitive radio wireless networks," in *Proc. IEEE Int. Conf. HST*, MA, Nov. 2011, pp. 384–389.

[22] N. Xie and S. Zhang, "Blind authentication at the physical layer under time-varying fading channels," *IEEE J. Select. Areas Commun.*, vol. 36, no. 7, pp. 1465–1479, Jul. 2018.

[23] L. Qian, X. Li, and S. Wei, "Cross-layer detection of stealthy jammers in multihop cognitive radio networks," in *2013 International Conference on Computing, Networking and Communications (ICNC)*, San Diego, CA, Jan. 2013, pp. 1026–1030.

[24] Z. Qin, X. Zhou, L. Zhang, Y. Gao, Y.-C. Liang, and G. Y. Li, "20 years of evolution from cognitive to intelligent communications," *IEEE Trans. Cog.*, vol. 6, no. 1, pp. 6–20, Mar. 2020.

[25] Y.-C. Liang, Q. Zhang, E. G. Larsson, and G. Y. Li, "Symbiotic radio: Cognitive backscattering communications for future wireless networks," *IEEE Trans. Cog.*, vol. 6, no. 4, pp. 1242–1255, Dec. 2020.

[26] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, May 2006.

[27] M. Young and R. Boutaba, "Overcoming adversaries in sensor networks: A survey of theoretical models and algorithmic approaches for tolerating malicious interference," *IEEE Commun. Surveys Tutor.*, vol. 13, no. 4, pp. 617–641, 4th Quart. 2011.

[28] Z. Yu, Z. Kaplan, Q. Yan, and N. Zhang, "Security and privacy in the emerging cyber-physical world: A survey," *IEEE Commun. Surveys Tutor.*, vol. 23, no. 3, pp. 1879–1919, 3rd Quart. 2021.

[29] L. Zhang, G. Ding, Q. Wu, and Z. Han, "Spectrum sensing under spectrum misuse behaviors: A multi-hypothesis test perspective," *IEEE Trans. Inf. Forensics Security.*, vol. 13, no. 4, pp. 993–1007, Apr. 2018.
[30] B. Upadhyaya, S. Sun, and B. Sikdar, "Multihypothesis sequential testing for illegitimate access and collision-based attack detection in wireless IoT networks," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11 705–11 716, Jul. 2021.
[31] N. Venkata Abhishek and M. Gurusamy, "Jade: Low power jamming detection using machine learning in vehicular networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 10, pp. 2210–2214, Oct. 2021.
[32] B. Upadhyaya, S. Sun, and B. Sikdar, "Machine learning-based jamming detection in wireless IoT networks," in *Proc. IEEE VTS Asia Pac. Wireless Commun. Symp. (APWCS)*, Singapore, Aug. 2019.
[33] A. Krayani, M. Baydoun, L. Marcenaro, A. S. Alam, and C. Regazzoni, "Self-learning bayesian generative models for jammer detection in cognitive-UAV-radios," in *Proc. IEEE Glob. Commun. Conference: Cogn. Radio AI-Enabled Netw. Symp.*, Taipei, Dec. 2020.
[34] Y. Kang, H. Wu, Z. Zhao, Y. Li, and J. Meng, "DL-based anomaly detection at the physical-layer of cognitive radio by deep support vector data description," *IEEE Trans. Cog.*, pp. 1–1, Early Acess 2022.
[35] P. Zhang, T. Taleb, X. Jiang, and B. Wu, "Physical layer authentication for massive MIMO systems with hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1563–1576, Mar. 2020.
[36] N. Zhao, W. Lu, M. Sheng, Y. Chen, J. Tang, F. R. Yu, and K.-K. Wong, "UAV-assisted emergency networks in disasters," *IEEE Wirel. Commun.*, vol. 26, no. 1, pp. 45–51, Feb. 2019.
[37] B. DeBruhl and P. Tague, "How to jam without getting caught: Analysis and empirical study of stealthy periodic jamming," in *Proc. 10th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw. (SECON)*, New Orleans, LS, Jun. 2013, pp. 496–504.
[38] Y. Sun, B. L. Mark, and Y. Ephraim, "Online parameter estimation for temporal spectrum sensing," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4105–4114, Aug. 2015.
[39] X. Chen, H. Zhang, A. B. MacKenzie, and M. Matinmikko, "Predicting spectrum occupancies using a non-stationary hidden Markov model," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 333–336, Aug. 2014.
[40] H. V. Poor, *An introduction to signal detection and estimation*. Springer Science & Business Media, 1998.
[41] Y. Zeng, Q. Wu, and R. Zhang, "Accessing from the sky: A tutorial on UAV communications for 5G and beyond," *Proc. IEEE*, vol. 107, no. 12, pp. 2327–2375, Dec. 2019.
[42] W. Chen, S. Zhao, R. Zhang, Y. Chen, and L. Yang, "UAV-assisted data collection with nonorthogonal multiple access," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 501–511, Jan. 2021.
[43] R. Chen, Y. Sun, L. Liang, and W. Cheng, "Joint power allocation and placement scheme for UAV-assisted IoT with QoS guarantee," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 1066–1071, Jan. 2022.
[44] S. Liu, L. J. Greenstein, W. Trappe, and Y. Chen, "Detecting anomalous spectrum usage in dynamic spectrum access networks," *Ad Hoc Netw.*, vol. 10, no. 5, pp. 831–844, Jul. 2012.
[45] J. M. Bruno and B. L. Mark, "A recursive algorithm for wideband temporal spectrum sensing," *IEEE Trans. Commun.*, vol. 66, no. 1, pp. 26–38, Jan. 2018.
[46] X. He, H. Dai, and P. Ning, "HMM-based malicious user detection for robust collaborative spectrum sensing," *IEEE J. Select. Areas Commun.*, vol. 31, no. 11, pp. 2196–2208, Nov. 2013.
[47] G. Zhang, X. Wang, Y.-C. Liang, and J. Liu, "Fast and robust spectrum sensing via Kolmogorov-Smirnov test," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3410–3416, Dec. 2010.