This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2024.3419071

Covert Communications Aided by Cooperative Jamming in Overlay Cognitive Radio Networks

Yingkun Wen, Lei Liu, Junhuai Li, Yilan Li, Kan Wang,
Shui Yu, *Fellow, IEEE,* and Mohsen Guizani, *Fellow, IEEE*

***Abstract*—This paper examines integrating jamming and secondary signals for covert communications in cognitive radio networks (CRNs), aiming to enhance covertness by using jamming and secondary signals in an overlay cooperative CRN. The scenario involves a primary base station (PBS) transmitting to a primary user (PU), with a secondary user transmitter (SU-Tx) acting as a cooperative jammer to obscure the message from a malevolent secondary user named "Willie." During idle intervals on the primary channel, the SU-Tx opportunistically accesses it to transmit secondary signals, reinforcing the covert communication of primary signals. The study quantifies the detection error probability (DEP) experienced by Willie, considering perfect and statistical channel state information (CSI) scenarios. In the perfect CSI scenario, optimization has two phases. Phase I aims to maximize the signals-to-interference-plus-noise ratio (SINR) of the PU, subject to the warden DEP exceeding a specified threshold. Phase II uses an iterative search algorithm to optimize beamforming vectors, enhancing SINR. In the statistical CSI scenario, the goal is to maximize effective transmission throughput (ETT), measuring the information transmitted from PBS to PU under covert constraints. Numerical results validate the theoretical analysis.**

***Index Terms*—Covert communications, cooperative jamming, cognitive radio network, alternate search.**

I. Introduction

Cognitive radio networks (CRNs) have been acknowledged as a paradigm for alleviating spectrum scarcity and improving spectrum utilization in next-generation wireless networks [1]–[5]. Consequently, the security and privacy of CRNs due to the broadcast nature of wireless media has emerged as an important issue. Conventional security techniques focus on the upper-level encryption, designed to construct and analyze protocols based on the information itself to prevent eavesdropping, such as cryptography approaches [6]–[9]. However, the conventional cryptography approaches will be decrypted as the computing power of eavesdroppers improves, resulting in the inability to guarantee information security. Physical layer security (PLS) technology emerges as a promising one to prevent malicious eavesdropping attacks, and it has been widely studied as an attractive alternative to complement shortcomings of conventional cryptography approaches [10]–[13].

Although both cryptography and PLS technologies can protect confidential messages from interception by unauthorized third parties, it is still challenging to deal with some malicious surveillance [14]. In CRNs, the primary user (PU) needs to shield the communication itself to evade being monitored by malicious secondary users (SU) [15]–[17]. Malicious SUs may transmit false local sensing results to the cognitive base station (CBS) or other SUs, incurring a considerable extra workload to avoid interference. More seriously, malicious monitoring causes monopolized utilization of idle spectrum, leading to spectrum congestion. This congestion prevents the concurrent transmission of PUs from properly utilizing wireless channels. Hence, the rise of an imperative to ascertain a novel communication safeguarding framework to shield the primary communication endeavors from the prying detection orchestrated by malicious SUs.

Protecting primary communication behavior in cognitive radio networks (CRNs) is known as emerging covert communications, or low probability of detection (LPD). Covert communications offer CRNs a higher level of security than PLS techniques [18]–[21].. Specifically, in covert communications, the primary base station (PBS) can reliably send messages to the primary user (PU), while a vigilant malicious secondary user (SU), referred to as "Willie," remains unaware of this primary communication. To achieve a higher level of security in covert communications, a strategy involving the use of a jammer as an ally is proposed. This strategy can increase the unpredictability of the Willie channel, thereby enhancing the covert performance of the primary communication.

A. Previous Work

Recently, covert communications in CRNs have garnered significant attention. In their studies, the authors of [22] delved into a covert cooperative cognitive radio (CCCR) system involving collaboration between primary transmitter (PT) and secondary transmitter (ST) to transmit confidential information. The investigation presented in [23] focused on short-packet covert communication within interweave CRNs, where an ST opportunistically accesses the occasionally idle spectrum under the supervision of a PT. The study detailed in [24] explored a CCCR system with multiple PTs transmitting information with the assistance of multiple STs to conserve

This work was supported by the Natural Science Foundation of Shaanxi Province under Grant 2023-JC-QN-0697; by the Natural Science Foundation of Shaanxi Province under Grant 2023-JC-QN-0741.

Yingkun Wen, Junhuai Li, Kan Wang and Yilan Li are with the School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China (E-mail: {ykwen, lijunhuai, wangkan, liyilan}@xaut.edu.cn).

Lei Liu (corresponding author) is with the Guangzhou Institute of Technology, Xidian University, Guangzhou 510555, China (E-mail:tianjiaoliulei@163.com).

Shui Yu is with the School of Computer Science, University of Technology Sydney 1001, Australia (E-mail: Shui.Yu@uts.edu.au).

Mohsen Guizani is with the Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE (Email: mguizani@ieee.org).

power consumption. The authors in [25] investigated covert communications in an overlay CRN, where multiple STs opportunistically send confidential information to a SR.

Covert communication conceals the information transmission process from the warden to prevent adversarial eavesdropping. However, it becomes challenging when the warden is mobile [26]–[28]. In [26], Chen et al. proposed a covert communication scheme against a mobile warden, which maximizes the connectivity throughput between a multi-antenna transmitter and a full-duplex jamming receiver within the covert outage probability (COP) limit. The authors of [28] introduced and evaluated a new concept of a dynamic warden. Its main novelty lies in the modification of the warden's behavior over time, making it difficult for the adaptive covert communication parties to infer its strategy and perform a successful hidden data exchange. In [27], the authors studied the effect of node mobility on the throughput scaling of covert communication over a wireless ad hoc network, where wardens can be mobile or fixed.

In addition, a series of studies have been conducted to explore the impact of fundamental limitations of covert communications in various wireless channel models on improving the security of the communication [29]–[32]. For instance, in the realm of additive Gaussian white noise (AWGN) channel, the seminal work of [29] unveiled a remarkable square root law. This law, postulating that within n channel usage, it becomes feasible to clandestinely transmit an impressive quantum of information, specifically on the order of $\mathcal{O}\sqrt{n}$ bits, to the intended recipient. Furthermore, the pioneering study conducted by [30] endeavored to shed light upon the scaling constant governing the covert information capacity within both the discrete memoryless channel (DMC) and the AWGN channel.

Different from the above LPD-based constrained ones, approaches focusing on exploring the opportunities and conditions for achieving positive covert rates have been applied [33]–[35]. Specifically, The authors in [33] effectively utilized the maximum achievable covert rate in the presence of bounded and unbounded noise uncertainty models. The authors in [34] sought to investigate how centralized and distributed multi-antenna transmitters, with randomly positioned wardens, affect covert throughput in covert communications. The resulting argument helps us to understand why covert throughput is invariant to interferer density while characterizing the covertness just by probabilistic metrics. Moreover, the authors in [35] employed a scenario involving a multi-antenna warden under constraints of delay to assess the efficacy of augmenting the warden's antenna number in relation to covert throughput.

Physical layer security (PLS) is a promising approach that take advantage of the propagation medium's features and impairments to ensure secure communication in the physical layer [36], [37]. The authors of [36] discussed challenges, solutions and visions of Physical layer security in beyond-5G networks. In [37], Physical layer security was being considered as a possible way to emancipate networks from classical complexity-based security approaches. Cooperative jamming, as a PLS-based technology, has attracted a great deal of attention in enhancing covert communications [38]–[41]. As a representative work, the recent work in [39] elegantly identified the node closest to the warden as a friendly jammer, enabling Alice to reliably and covertly transmit messages to Bob. Moreover, in the context of wireless communication systems operating under fading channels, the work in [40] adopted a full-duplex receiver capable of generating artificial noise, necessitating manual adjustment of transmit power levels to ensure covert operations.

B. Motivation and Our Contributions

The introduction of jamming signals has significantly enhanced the reliability of covert communications. Extensive research has focused on CCRNs to improve spectrum efficiency. The primary objective is to select SUs as friendly jammers to protect primary signals from detection. It is also important to note that the secondary signals of SUs can contribute to achieving covert performance in overlay CCRNs, distinguishing this approach from others. However, prior researches have made limited contributions to the simultaneous introduction of jamming signals and secondary signals in covert communications of CRNs. This gap in the literature motivates the focus of our investigation in this paper.

In this work, we focus on covert communications of a CCRN and aim to increase covertness with the aid of both jamming and secondary signals. To be specific, within the domain CCRNs, a PBS endeavors to transmit a message to a PU. Simultaneously, a transmitter of the secondary user (SU-Tx) assumes the role of a cooperative jammer, emitting jamming signals with the purpose of shielding the transmitted message from the detection of a prospective warden (Willie). It is imperative to note that the SU-Tx can transmit secondary signals to its corresponding secondary user receiver (SU-Rx) when the primary channel is idle. Fully utilization of secondary signals enables notable benefit for covert communications of primary signals, aggressively introducing additional uncertainty and more confusion to Willie. We explore the detection error probability of Willie under two distinct scenarios: perfect and statistical channel state information (CSI). Our primary contributions can be succinctly summarized as follows.

- In the scenario of perfect CSI, we evaluate the most unfavorable cases related to covert communications, where Willie possesses the ability to ingeniously engineer an optimal detection threshold. To ensure covert communication, we formulate an optimization problem that aims to maximize the signal-to-interference-plus-noise ratio (SINR) experienced by the PU, while adhering to the constraint that the detection error probability (DEP) of Willie remains above a predetermined threshold. We propose an alternative algorithm to work out the optimization problem, thereby achieving an optimal transmission power for the PBS and jammer.
- In the scenario of statistical CSI, we calculate the probabilities of false alarm and missed detection for Willie, thus confirming the feasibility of achieving a positive covert communication rate. Under the constraints of

covert operations, we determine the effective transmission throughput (ETT) as a metric that measures the amount of information that can be conveyed from the PBS to the PU, while ensuring that Willie's DEP remains at or exceeds a predetermined threshold.
- We delve into an exploration of the impact imposed by the transmission powers of primary signals, jamming signals, and secondary signals upon the realm of covert performance, encompassing both scenarios of perfect CSI and statistical CSI. Through numerical analysis, we uncover the augmentative influence that secondary signals exert upon the covertness performance. Additionally, our findings reveal that the pursuit of heightened covertness performance necessitates the acceptance of a commensurate loss in SINR and ETT.

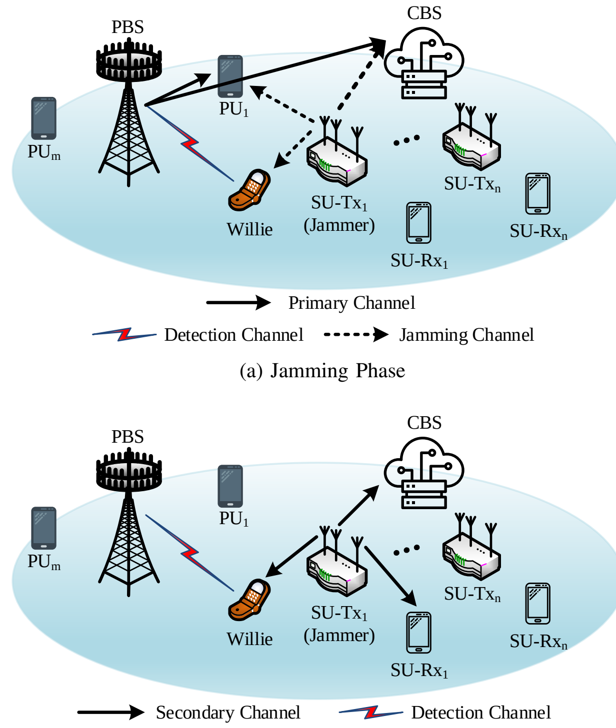
The remaining sections of the paper are organized as follows. In Section II, we provide the necessary preliminaries and present the system model. The covertness analysis, from the perspective of the warden, is presented in Section III. In Section IV, we formulate the optimization problem to maximize the secrecy performance (SINR and ETT) at the PU while adhering to a covert constraint. Numerical results are provided in Section V, and finally, we draw conclusions in Section VI.

Notations: The symbols $(\cdot)^H$ and $|\cdot|$ represent the concepts of Hermitian transpose and absolute value, respectively. The trace operator is denoted by $\mathrm{Tr}(\cdot)$. We utilize $\mathcal{N}(\mu, \sigma^2)$ to symbolize the normal distribution, characterized by its parameters of mean μ and variance σ^2.

II. System Model

Within the scope of this paper, our attention is captivated by an overlay centralized CCRN. This network showcases the presence of a PBS, m primary users (PUs), a malevolent SU (Willie), a CBS, and an assemblage of n interconnected entities—secondary user transmitters (SU-Txs) and secondary user receivers (SU-Rxs)—depicted in Fig. 1. Within cognitive radio networks, the presence of both a primary base station (PBS) and a cognitive base station (CBS) serves a crucial function. The PBS is responsible for managing the licensed spectrum, which is typically reserved for exclusive use by the primary users (PU). The CBS, on the other hand, is utilized by the secondary users (SU) to access the spectrum opportunistically and avoid interference with the PU.

The PBS stands adorned with N_p antennas, while each SU-Tx possessing N_j antennas. Remarkably, the PU, SU-Rx, Willie, and the CBS are each bestowed with a single antenna. Within the realm of the overlay CCRN, the PBS aims to transmit a message to a designated PU, symbolized by PU_1. However, the PBS encounters an intrinsic necessity for covert communication, to elude detection from the ever-vigilant warden (Willie) in the detection channel. In a commendable endeavor to preserve the message's integrity from the detection of Willie, the CBS astutely identifies a specific SU-Tx, embodied by $\mathrm{SU\text{-}Tx}_1$, to undertake the noble role of a friendly jammer. This chosen SU-Tx sends a cascade of meticulously engineered artificial noise upon Willie, orchestrating interference across the jamming channel.



(a) Jamming Phase

(b) Accessing Phase

Fig. 1: Network model for an overlay centralized CCRN.

Upon the cessation of jamming, during moments of idleness within the primary channel, $\mathrm{SU\text{-}Tx}_1$ is granted to engage the primary channel for the transmission of its message to its destination node, i.e., $\mathrm{SU\text{-}Rx}_1$. Thus, from the vantage point of $\mathrm{SU\text{-}Tx}_1$, its transmission unfolds through two alternating phases: Jamming Phase and Accessing Phase.

In the jamming phase, the received signals at PU_1, the CBS, and Willie can be expressed as,

$$y_p(t) = \mathbf{h}_{p,p}^H(t)\mathbf{w}_p(t)x_p(t) + \mathbf{h}_{j,p}^H(t)\mathbf{w}_j(t)x_j(t) + n_p(t), \quad (1)$$

$$y_c(t) = \mathbf{h}_{p,c}^H(t)\mathbf{w}_p(t)x_p(t) + \mathbf{h}_{j,c}^H(t)\mathbf{w}_j(t)x_j(t) + n_c(t), \quad (2)$$

$$y_w(t) = \mathbf{h}_{p,w}^H(t)\mathbf{w}_p(t)x_p(t) + \mathbf{h}_{j,w}^H(t)\mathbf{w}_j(t)x_j(t) + n_w(t). \quad (3)$$

In the accessing phase, the received signals at $\mathrm{SU\text{-}Rx}_1$, the CBS, and Willie can be expressed as

$$y_s(t) = \mathbf{h}_{s,s}^H(t)\mathbf{w}_s(t)x_s(t) + n_s(t), \quad (4)$$

$$y_c(t) = \mathbf{h}_{s,c}^H(t)\mathbf{w}_s(t)x_s(t) + n_c(t), \quad (5)$$

$$y_w(t) = \mathbf{h}_{s,w}^H(t)\mathbf{w}_s(t)x_s(t) + n_w(t), \quad (6)$$

Herein, we introduce the channel responses, denoted as $\mathbf{h}_{a,b}$, where $a \in \{p, j, s\}$ traverses the realms of transmitters encompassing the PBS, the jammer, and the $\mathrm{SU\text{-}Tx}_1$, while $b \in \{p, c, w, s\}$ embraces the receivers represented by PU_1, the CBS, Willie, and $\mathrm{SU\text{-}Rx}_1$. The expression $\mathbf{h}_{a,b} = \hat{\mathbf{h}}_{a,b}\sqrt{\theta_{a,b}}$ encapsulates this framework, where $\hat{\mathbf{h}}_{a,b}$ denotes a complex channel vector of dimensions $N_a \times 1$, with $\theta_{a,b}$ representing the path loss of $a \to b$ channel.

The path loss unveils its expression as $10\log_{10}(\theta_{a,b}) = -34.5 - 20\log_{10}(d_{a,b}[\mathrm{m}])$, where $d_{a,b}$ delineate the distances of transmitters and receivers. The beamforming vectors $\mathbf{w}_p$

and $\mathbf{w}_j$ belong to the complex vector spaces $\mathbb{C}^{N_p \times 1}$ and $\mathbb{C}^{N_j \times 1}$, respectively, representing the PBS and SU-Tx_1. The signal x_p corresponds to the transmission from the PBS, while the signal x_j represents the jamming transmission from SU-Tx_1, following a zero-mean Gaussian distribution with unit variance ($x_j \sim \mathcal{N}(0,1)$). The term n_b denotes the additive white Gaussian noise (AWGN) with a two-sided power spectral density of N_{02}. It is assumed that n_b follows a Gaussian distribution with zero mean and variance $\delta_b^2 = 2N_{02}B$, where B represents the channel bandwidth. We assume that all channels experience independent Rayleigh fading.

In this paper, the network model is quasi-static, and the position of each node is basically unchanged during the communication process. Moreover, based on the above assumption that the channel state information of the eavesdropper is known, and the candidate SUs for jammer needs to send channel state information (including jamming distance) to the CBS. Therefore, the SU knows the locations of the jammer and Eve, so the jamming distance is also known to the CBS. As shown in (1), jammer may impose some interference on the primary channel. There are typically three approaches to mitigate interference caused by a jammer on the primary channel. The first approach involves employing zero-forcing beamforming at the jammer to ensure that the interference at PU is reduced to zero. The second approach entails establishing an interference threshold and utilizing beamforming at the jammer to keep the interference at PU below this threshold. The third method involves proactive communication between PBS and the jammer. In this scenario, the jammer shares the interference signal with PBS in advance, allowing the PU to eliminate the interference signal at the receiving end. In this paper, we employ the second approach, specifying an interference temperature limit θ to ensure that the interference remains below this predefined limit.

The channel responses are intricately linked to CSI, which varies in availability across different scenarios. In the case of perfect CSI, it is assumed that the PBS can obtain the CSI of the primary channel by employing pilot sequences [42]–[47]. For example, in [42], Rider Grey Wolf Optimization (RGWO) was proposed to optimally place the pilots in the training sample or sequence in such a way to facilitate the automatic estimation of the state of the channel. In [43], a novel sequential channel estimation approach was proposed for multiband cognitive radio systems. The authors in [44] considered simultaneous PU detection and channel estimation for censoring based spectrum sensing in CRNs over fading channels.

Additionally, one of the legitimate users is designated as a potential warden (Willie) [48] . Given that Willie is also a legitimate user, we can acquire the CSI of the detection channel. Each SU-Tx measures its CSI with both PU_1 and Willie. Subsequently, each SU-Tx reports its CSI to the CBS. To facilitate secure communication, the CBS shares the CSI of SUs with the PBS via a dedicated channel, such as a common control channel [49]. Ultimately, the PBS possesses the CSI of both PUs and SUs.

In most scenarios, the acquisition of perfect CSI is hindered by channel estimation and quantization errors. Particularly, obtaining accurate channel information for the passive eavesdropper, Willie, is unattainable. It is worth noting that statistical CSI for different channels can be obtained through various measurement methods. Hence, for the majority of cases, we assume the availability of statistical CSI. The channel vectors for the perfect CSI scenario and the statistical CSI scenario are summarized as follows:

- Perfect CSI scenario: In this scenario, it is assumed that the PBS and SU-Tx are equipped with multiple antennas ($N_p \neq 1, N_j \neq 1$). The instantaneous CSI of $\mathbf{h}_{ab}$ are known, $a \in \{p, j, s\}$, $b \in \{p, c, w, s\}$.
- Statistical CSI scenario: In this scenario, it is assumed that the PBS and SU-Tx are equipped with a single antenna ($N_p = N_j = 1$). The channel gains of $h_{a,b}$ are independent complex circular Gaussian random variables with zero mean and variances δ_{ab}^2, i.e., $h_{a,b} \sim \mathcal{CN}(0, \delta_{ab}^2)$.

In this paper, the scenarios and parameters were chosen based on several factors. Firstly, we considered real-world applicability, aiming to address practical challenges faced in cognitive radio networks (CRNs). The selected scenarios represent common scenarios encountered in CRNs, ensuring that our approach is relevant and applicable in various settings. Secondly, the parameters were carefully chosen to highlight specific aspects of CRNs that are crucial for our approach. For example, we focused on parameters that impact the performance of covert communications, such as signal-to-interference-plus-noise ratio (SINR) and detection error probability (DEP). By selecting these parameters, we aim to demonstrate the effectiveness of our approach in improving the security and reliability of covert communications in CRNs.

III. Analysis of Covertness Performance

In this section, we conduct an analysis of covertness from the perspective of the warden. In the considered network, the analysis of covertness can be formulated as the detection error probability (DEP) at the warden.

Specifically, in order to detect primary signals emanating from the PBS, the warden encounters a binary hypothesis testing problem involving two events: $\mathcal{H}_0$ and $\mathcal{H}_1$. Here, $\mathcal{H}_0$ represents the null hypothesis in which the PBS does not transmit primary signals while SU-Tx_1 transmits secondary signals. On the other hand, $\mathcal{H}_1$ corresponds to the alternative hypothesis in which the PBS transmits primary signals and the jammer transmits AN to the warden. In both scenarios, the received signals at the warden can be expressed as follows:

$$\mathcal{H}_0 : y_w(t) = \mathbf{h}_{s,w}^H(t)\mathbf{w}_s(t)x_s(t) + n_w(t), \tag{7}$$

$$\begin{aligned}\mathcal{H}_1 : y_w(t) = \mathbf{h}_{p,w}^H(t)\mathbf{w}_p(t)x_p(t) + \mathbf{h}_{j,w}^H(t)\mathbf{w}_j(t)x_j(t) \\ + n_w(t).\end{aligned} \tag{8}$$

It is assumed that Y_w represents the energy received by the warden. Let τ denote the continuous value that signifies the duration of detection. The test statistic for energy detection is expressed as follows:

$$Y_w = \frac{1}{N_{02}} \int_0^{\tau} |y_w(t)|^2 \, dt \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \Gamma_p(\Gamma_s), \tag{9}$$

where Γ_p is the decision threshold under perfect CSI case, and Γ_s is the decision threshold under statistical CSI case [50]. From Willie's prospective, we assume that the received power of the PBS, the jammer, and SU-Tx$_1$ are fixed at $\hat{P}_p = \mathrm{Tr}(\mathbf{W}_p \mathbf{H}_{p,w})$, $\hat{P}_j = \mathrm{Tr}(\mathbf{W}_j \mathbf{H}_{j,w})$ and $\hat{P}_s = \mathrm{Tr}(\mathbf{W}_s \mathbf{H}_{s,w})$, respectively. Therefore, the received energy of primary signals, jamming signals, secondary signals are $\hat{P}_p\tau$, $\hat{P}_j\tau$ and $\hat{P}_s\tau$ respectively.

A. Perfect CSI Scenario

As per the findings in [50], under the hypothesis $\mathcal{H}_0$, the received energy Y_w follows a non-central chi-square distribution with $2\tau B$ degrees of freedom and a non-centrality parameter of $\frac{\hat{P}s\tau}{N_{02}}$. Similarly, under the hypothesis $\mathcal{H}_1$, Y_w follows a non-central chi-square distribution with $2\tau B$ degrees of freedom and a non-centrality parameter $\delta = \frac{\hat{P}_p\tau + \hat{P}j\tau}{N_{02}}$. When $2\tau B$ is sufficiently large, the central limit theorem (CLT) allows us to approximate Y_w under both hypotheses as follows:

$$\begin{cases} Y_w|\mathcal{H}_0 \sim \mathcal{N}(2\tau B + \frac{\hat{P}_s\tau}{N_{02}}, 4\tau B + \frac{4\hat{P}_s\tau}{N_{02}}), \\ Y_w|\mathcal{H}_1 \sim \mathcal{N}(2\tau B + \frac{(\hat{P}_p+\hat{P}_j)\tau}{N_{02}}, 4\tau B + \frac{4(\hat{P}_p+\hat{P}_j)\tau}{N_{02}}), \end{cases} \tag{10}$$

where $\mathcal{N}(\mu, \delta^2)$ represents the normal distribution with the mean μ and the variance δ^2.

1) Detection Error Probability: The warden decides whether PBS has transmitted message or not according to its received signal power. In this paper, we define the false alarm probability (P_{FA}) and the missed detection probability (P_{MD}). P_{MD} represents the probability of failing to detect any primary signals when they are actually present, while P_{FA} represents the probability of erroneously detecting primary signals when they are absent. By utilizing the approximations (10), we can derive the expressions for P_{MD} and P_{FA} as follows [51]:

$$\begin{aligned} P_{\mathrm{FA}} &= \mathrm{prob}(Y_w > \Gamma_p|\mathcal{H}_0) \\ &= \begin{cases} 1, & \Gamma_p \le \delta_w^2 \\ Q\left(\frac{\Gamma_p - (2B\tau + \frac{\hat{P}_s\tau}{N_{02}})}{\sqrt{4B\tau + \frac{4\hat{P}_s\tau}{N_{02}}}}\right), & \Gamma_p > \delta_w^2 \end{cases} \end{aligned} \tag{11}$$

$$\begin{aligned} P_{\mathrm{MD}} &= \mathrm{prob}(Y_w < \Gamma_p|\mathcal{H}_1) \\ &= \begin{cases} 0, & \Gamma_p \le \hat{P}_p\tau + \delta_w^2 \\ 1 - Q\left(\frac{\Gamma_p - (2B\tau + \frac{(\hat{P}_p+\hat{P}_j)\tau}{N_{02}})}{\sqrt{4B\tau + \frac{4(\hat{P}_p+\hat{P}_j)\tau}{N_{02}}}}\right), & \Gamma_p > \hat{P}_p\tau + \delta_w^2 \end{cases} \end{aligned} \tag{12}$$

where $Q(\cdot)$ is the standard Gaussian complementary cumulative distribution function which is shown as

$$Q(t) = \frac{1}{\sqrt{2\pi}} \int_t^{+\infty} \exp(\frac{-x^2}{2}) dx. \tag{13}$$

Since the false alarm and the missed detection events are two types of errors for warden's detection, the covertness can be measured by the DEP:

$$\begin{aligned} \xi_p =& P_{\mathrm{FA}} + P_{\mathrm{MD}} \\ =& \begin{cases} 1, & \Gamma_p \le \delta_w^2 \\ Q\left(\frac{\Gamma_p - (2B\tau + \frac{\hat{P}_s\tau}{N_{02}})}{\sqrt{4B\tau + \frac{4\hat{P}_s\tau}{N_{02}}}}\right), & \hat{P}_p\tau + \delta_w^2 \ge \Gamma_p > \delta_w^2 \\ 1 - Q\left(\frac{\Gamma_p - (2B\tau + \frac{(\hat{P}_p+\hat{P}_j)\tau}{N_{02}})}{\sqrt{4B\tau + \frac{4(\hat{P}_p+\hat{P}_j)\tau}{N_{02}}}}\right) & \\ +Q\left(\frac{\Gamma_p - (2B\tau + \frac{\hat{P}_s\tau}{N_{02}})}{\sqrt{4B\tau + \frac{4\hat{P}_s\tau}{N_{02}}}}\right), & \Gamma_p > \hat{P}_p\tau + \delta_w^2 \end{cases} \end{aligned} \tag{14}$$

It is assumed that PBS's transmission is considered covert if $\xi_p \ge 1 - \epsilon$, where ϵ is the covertness requirement.

2) Covert Performance: We consider a worst-case scenario for covert communications in which the optimal detection threshold is designed from Willie's perspective to minimize the average detection error probability.

As depicted in Fig. 3, we observe that when $\delta_w^2 < \Gamma_p < \hat{P}_p\tau + \delta_w^2$, ξ_p decreases as Γ_p increases. Furthermore, we find that ξ_p continues to decrease as Γ_p ranges from $\hat{P}_p\tau + \delta_w^2$ to Γ_p^*, whereas ξ_p increases for $\Gamma_p > \Gamma_p^*$. To determine the optimal value of Γ_p, we take the partial derivative of the function ξ_p in equation (14) with respect to Γ_p and set the derivative equal to zero. This can be expressed as follows:

$$\frac{\partial \xi_p}{\partial \Gamma_p} = 0, \tag{15}$$

The optimal Γ_p^* can be calculated as (16) at the top of the next page. Substitute $\Gamma_p = \Gamma_p^*$ into equation (14), we can achieve the minimum value of DEP $\xi_p^*(\mathbf{W}_p, \mathbf{W}_j)$.

B. Statistical CSI Scenario

In the statistical CSI scenario, we assume that $\mathbf{y_w} = y_w(t_j), j = 1, 2, ...N$ represents the sampling vector of the received signals at Willie. Under hypothesis $\mathcal{H}_0$, the distribution of $y_w(t_j)$ is assumed to be $\mathcal{CN}(0, E)$, where $E = P_s|h_{s,w}|^2 + \delta_w^2$. Conversely, under hypothesis $\mathcal{H}1$, the distribution of $y_w(t_j)$ is assumed to be $\mathcal{CN}(0, F)$, where $F = P_p|h_{p,w}|^2 + P_j|h_{j,w}|^2 + \delta_w^2$.

1) Detection Error Probability: The DEP in statistical CSI scenario can be expressed as

$$\xi_s = P_{\mathrm{FA}} + P_{\mathrm{MD}}. \tag{18}$$

Lemma 1 *We can derive expressions of P_{MD} and P_{FA} as follows*

$$\begin{aligned} P_{\mathrm{FA}} &= \mathbb{P}(Y_w > \Gamma_s|\mathcal{H}_0) \\ &= \begin{cases} 1, & \Gamma_s < \delta_w^2 \\ e^{-\frac{\Gamma_s - \delta_w^2}{P_s\delta_{bw}^2}}, & \Gamma_s \ge \delta_w^2 \end{cases} \end{aligned} \tag{19}$$

$$\Gamma_p^* = \frac{-1}{2(\hat{P}_j+\hat{P}_p-\hat{P}_s)}\sqrt{4\tau K_1(\hat{P}_j+\hat{P}_p-\hat{P}_s)+B^2\tau^2(-2\hat{P}_j-2\hat{P}_p+2\hat{P}_s)^2}-B\tau(-2\hat{P}_j-2\hat{P}_p+2\hat{P}_s), \tag{16}$$

$$\begin{aligned} K_1 =& 8B^2N_{02}\log\left(\frac{\sqrt{4B\tau+\frac{4\hat{P}_j\tau}{N_{02}}+\frac{4\hat{P}_p\tau}{N_{02}}}}{\sqrt{4B\tau+\frac{4\hat{P}_s\tau}{N_{02}}}}\right)+\frac{B\hat{P}_j^2\tau}{N_{02}}+8B\hat{P}_j\log\left(\frac{\sqrt{4B\tau+\frac{4\hat{P}_j\tau}{N_{02}}+\frac{4\hat{P}_p\tau}{N_{02}}}}{\sqrt{4B\tau+\frac{4\hat{P}_s\tau}{N_{02}}}}\right) \\ &+8B\hat{P}_p\log\left(\frac{\sqrt{4B\tau+\frac{4\hat{P}_j\tau}{N_{02}}+\frac{4\hat{P}_p\tau}{N_{02}}}}{\sqrt{4B\tau+\frac{4\hat{P}_s\tau}{N_{02}}}}\right)+8B\hat{P}_s\log\left(\frac{\sqrt{4B\tau+\frac{4\hat{P}_j\tau}{N_{02}}+\frac{4\hat{P}_p\tau}{N_{02}}}}{\sqrt{4B\tau+\frac{4\hat{P}_s\tau}{N_{02}}}}\right)+\frac{8\hat{P}_j\hat{P}_s\log\left(\frac{\sqrt{4B\tau+\frac{4\hat{P}_j\tau}{N_{02}}+\frac{4\hat{P}_p\tau}{N_{02}}}}{\sqrt{4B\tau+\frac{4\hat{P}_s\tau}{N_{02}}}}\right)}{N_{02}} \\ &+\frac{8\hat{P}_p\hat{P}_s\log\left(\frac{\sqrt{4B\tau+\frac{4\hat{P}_j\tau}{N_{02}}+\frac{4\hat{P}_p\tau}{N_{02}}}}{\sqrt{4B\tau+\frac{4\hat{P}_s\tau}{N_{02}}}}\right)}{N_{02}}+\frac{2B\hat{P}_j\hat{P}_p\tau}{N_{02}}+\frac{B\hat{P}_p^2\tau}{N_{02}}-\frac{B\hat{P}_s^2\tau}{N_{02}}+\frac{\hat{P}_j^2\hat{P}_s\tau}{{N_{02}}^2} \\ &+\frac{2\hat{P}_j\hat{P}_p\hat{P}_s\tau}{{N_{02}}^2}-\frac{\hat{P}_j\hat{P}_s^2\tau}{{N_{02}}^2}+\frac{\hat{P}_p^2\hat{P}_s\tau}{{N_{02}}^2}-\frac{\hat{P}_p\hat{P}_s^2\tau}{{N_{02}}^2}. \end{aligned} \tag{17}$$

$$\begin{aligned} P_{\mathrm{MD}} &= \mathbb{P}(Y_w<\Gamma_s|\mathcal{H}_1) \\ &= \begin{cases} 0, \Gamma_s<\delta_w^2 \\ 1-e^{-\frac{\Gamma_s-\sigma_w^2}{P_j\delta_{jw}^2}}-\frac{P_p\delta_{pw}^2}{P_p\delta_{pw}^2-P_j\delta_{jw}^2}\times \\ \left(e^{-\frac{\Gamma_s-\sigma_w^2}{P_p\delta_{pw}^2}}-e^{-\frac{\Gamma_s-\sigma_w^2}{P_j\delta_{jw}^2}}\right), \Gamma_s\geq\delta_w^2 \end{cases} \end{aligned} \tag{20}$$

Specifically, when $P_p\delta_{pw}^2=P_j\delta_{jw}^2$,

$$P_{\mathrm{MD}}=1-e^{-\frac{\Gamma_s-\sigma_w^2}{2P_p\delta_{pw}^2}} \tag{21}$$

Proof: See Appendix A. ■

Lemma 2 *When $P_s\delta_{sw}^2=P_j\delta_{jw}^2$, the optimal detecting threshold of Willie can be calculated as (22) at the top of the next page.*

Proof: See Appendix B. ■

2) Covert Performance: From Lemma 2, we can obtain the minimal detecting error probability of Willie ξ_s^* can be expressed as (24) at the top of the next page. Let $\eta=\frac{P_s\delta_{sw}^2}{2P_p\delta_{pw}^2}$, $\eta_1=\frac{P_j\delta_{jw}^2}{P_p\delta_{pw}^2}$, then the ξ_s^* can be rewritten as

$$\xi_s^* = \begin{cases} 1-\eta^{\frac{\eta}{1-\eta}}+\eta^{\frac{1}{1-\eta}}, P_p\delta_{pw}^2=P_j\delta_{jw}^2\neq P_s\delta_{sw}^2 \\ 1-\frac{1}{1-\eta_1}(\eta_1^{\frac{\eta_1}{1-\eta_1}}-\eta_1^{\frac{1}{1-\eta_1}}), P_s\delta_{sw}^2=P_j\delta_{jw}^2 \\ \neq P_p\delta_{pw}^2 \vee P_s\delta_{sw}^2=P_p\delta_{pw}^2\neq P_j\delta_{jw}^2 \\ 1+\frac{1}{\mathrm{e}}-\frac{1}{\sqrt{\mathrm{e}}}, P_s\delta_{sw}^2=P_p\delta_{pw}^2=P_j\delta_{jw}^2. \end{cases} \tag{23}$$

When $\xi_s^*\geq 1-\epsilon$, the PBS's transmission can be guaranteed to achieve covert communication. Let $f(\eta)=\eta^{\frac{\eta}{1-\eta}}-\eta^{\frac{1}{1-\eta}}$, $g(\eta_1)=\frac{1}{1-\eta_1}(\eta_1^{\frac{\eta_1}{1-\eta_1}}-\eta_1^{\frac{1}{1-\eta_1}})$, then the inequality can be rewritten as

$$\xi_s^* = \begin{cases} f(\eta)\leq\epsilon, P_p\delta_{pw}^2=P_j\delta_{jw}^2\neq P_s\delta_{sw}^2 \\ g(\eta_1)\leq\epsilon, P_s\delta_{sw}^2=P_j\delta_{jw}^2\neq \\ P_p\delta_{pw}^2 \vee P_s\delta_{sw}^2=P_p\delta_{pw}^2\neq P_j\delta_{jw}^2 \\ \frac{1}{\sqrt{\mathrm{e}}}-\frac{1}{\mathrm{e}}\leq\epsilon, P_s\delta_{sw}^2=P_p\delta_{pw}^2=P_j\delta_{jw}^2. \end{cases} \tag{25}$$

As show in Fig. 2, $f(\eta)(g(\eta_1))$ is strictly decreasing as $\eta(\eta_1)$ increases. Thus, for $0.24\approx\frac{1}{\sqrt{\mathrm{e}}}-\frac{1}{\mathrm{e}}\leq\epsilon\leq 1$, it is possible to achieve covert communication for any covertness requirement of ϵ. Therefore, a positive outage covert communication rate is achievable. Looking at figure

IV. Transmission Strategies with Covert Constraint

In this section, we analyze the jammer's AN transmission strategies and explore the development of a covert transmission scheme by the PBS. In the perfect CSI scenario, we start by formulating an optimization problem to determine the AN transmission strategy that maximizes the received SINR at the PU while satisfying covert constraints. In the statistical CSI scenario, we introduce the concept of ETT to evaluate the information capacity achievable from the PBS to the PU under covert constraints.

A. Perfect CSI Scenario

As the perfect CSI is available, we can obtain the instantaneous output SINRs at PU_1 and the Willie expressed as

$$\mathrm{SINR_p}=\frac{\mathbf{h}_{p,p}^H\mathbf{w}_p\mathbf{w}_p^H\mathbf{h}_{p,p}}{\mathbf{h}_{j,p}^H\mathbf{w}_j\mathbf{w}_j^H\mathbf{h}_{j,p}+\delta_p^2}=\frac{\mathrm{Tr}(\mathbf{W}_p\mathbf{H}_{p,p})}{\mathrm{Tr}(\mathbf{W}_j\mathbf{H}_{j,p})+\delta_p^2}, \tag{26}$$

where $\mathbf{W}_a=\mathbf{w}_a\mathbf{w}_a^H$, $a\in\{p,j\}$, and $\mathbf{H}_{a,p}=\mathbf{h}_{a,p}\mathbf{h}_{a,p}^H$.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2024.3419071

$$\Gamma_s^* = \begin{cases} \delta_w^2 + 2P_pP_s\delta_{pw}^2\delta_{sw}^2\frac{\log\left(2P_p\delta_{pw}^2\right)-\log\left(P_s\delta_{sw}^2\right)}{2P_p\delta_{pw}^2-P_s\delta_{sw}^2}, P_p\delta_{pw}^2 = P_j\delta_{jw}^2 \neq P_s\delta_{sw}^2 \\ \delta_w^2 + P_pP_j\delta_{pw}^2\delta_{jw}^2\frac{\log\left(P_p\delta_{pw}^2\right)-\log\left(P_j\delta_{jw}^2\right)}{P_p\delta_{pw}^2-P_j\delta_{jw}^2}, P_s\delta_{sw}^2 = P_j\delta_{jw}^2 \neq P_p\delta_{pw}^2 \vee P_s\delta_{sw}^2 = P_p\delta_{pw}^2 \neq P_j\delta_{jw}^2 \\ \delta_w^2 + P_p\delta_{pw}^2, P_s\delta_{sw}^2 = P_p\delta_{pw}^2 = P_j\delta_{jw}^2. \end{cases} \tag{22}$$

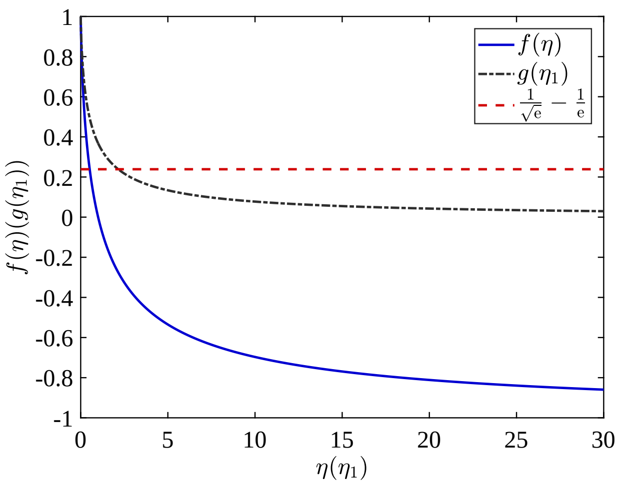


Fig. 2: Plot of $f(\eta)(g(\eta_1))$ against $\eta(\eta_1)$.

To obtain the optimal beamforming vectors of the PBS and SU_1, the secrecy rate maximization problem is mathematically characterized as

$$\max_{\mathbf{W}_p,\mathbf{W}_j} \quad \mathrm{SINR_p} \tag{27a}$$
$$\text{s.t.} \quad \mathrm{Tr}(\mathbf{W}_j) \leq P_j^m, \tag{27b}$$
$$\xi^*(\mathbf{W}_p, \mathbf{W}_j) \geq 1-\epsilon, \tag{27c}$$
$$\mathrm{Tr}(\mathbf{W}_j\mathbf{H}_{j,p}) \leq \theta, \tag{27d}$$
$$\mathrm{Tr}(\mathbf{W}_p) \leq P_p^m, \tag{27e}$$
$$\mathrm{rank}(\mathbf{W}_p) = 1, \tag{27f}$$
$$\mathrm{rank}(\mathbf{W}_j) = 1, \tag{27g}$$

The interference temperature limit imposed on PU_1 is denoted by θ, while P_p^m and P_j^m represent the transmit power limits of the PBS and $\mathrm{SU\text{-}Tx}_1$, respectively. The covert constraint is expressed in equation (27c).

Problem (27) is challenging to solve due to the fractional form in its objective and the presence of the covert constraint (27c). Consequently, we propose an alternate search approach based on the following proposition.

Proposition 1 *The objective function* $\mathrm{SINR_p}(\mathbf{W}_p, \mathbf{W}_j)$ *and the covert constraint (27c) are convex functions when* $\mathbf{W}_p$ *is fixed and* $\mathbf{W}_j$ *is varied. Similarly, they are convex functions when* $\mathbf{W}_j$ *is fixed and* $\mathbf{W}_p$ *is varied.*

Proof: For a fixed $\mathbf{W}_j$, the objective function of problem (27) is convex. In this paper, the PBS's transmission is considered covert only when $\xi^* \geq 1-\epsilon$, where ϵ represents a predetermined threshold for the covert transmission requirement. When $\xi^* = 1-\epsilon$, we can derive $P_p^{covert} = (\xi^*)^{-1}(1-\epsilon)$, where $(\xi^*)^{-1}(1-\epsilon)$ denotes the inverse function of ξ^*. If the PBS's power exceeds P_p^{covert}, the covert constraint cannot be satisfied. Therefore, to fulfill the covert constraint, the permissible range of P_p can be expressed as follows:

$$\mathrm{Tr}(\mathbf{W}_p) \leq \min(P_p^m, P_p^{covert}). \tag{28}$$

Till now, the covert constraint (27c) can be transformed into a transmission power constraint at the PBS. Next, we employ the semidefinite relaxation (SDR) technique to eliminate the two rank-one constraints (27f) and (27g). This transformation allows us to convert problem (27) into:

$$\max_{\mathbf{W}_p} \quad \mathrm{SINR_p} \tag{29a}$$
$$\text{s.t.} \quad \mathrm{Tr}(\mathbf{W}_p) \leq \min(P_p^m, P_p^{covert}). \tag{29b}$$

Alternatively, for a fixed $\mathbf{W}_p$, the objective of problem (27) is a convex function. It is assumed to be covert only when $\xi^* \geq 1-\epsilon$. When $\xi^* = 1-\epsilon$, we can obtain $P_j^{\mathrm{covert}} = (\xi^*)^{-1}(1-\epsilon)$. If the jammer's power is lower than P_j^{covert}, the covert constraint cannot be satisfied. Thus, to satisfy the covert constraint, the allowable range of P_j can be expressed as

$$P_j^{\mathrm{covert}} \leq \mathrm{Tr}(\mathbf{W}_j) \leq P_j^m. \tag{30}$$

Till now, the covert constraint (27c) can be transformed into a transmission power constraint at the jammer, which is a convex function. Then problem (27) can be transformed into

$$\min_{\mathbf{W}_j} \quad \frac{1}{\mathrm{SINR_p}} \tag{31a}$$
$$\text{s.t.} \quad P_j^{\mathrm{covert}} \leq \mathrm{Tr}(\mathbf{W}_j) \leq P_j^m, \tag{31b}$$
$$\mathrm{Tr}(\mathbf{W}_j\mathbf{H}_{j,p}) \leq \theta \tag{31c}$$

Obviously, problem (29) and (31) are convex problems, and can be handled by available convex softwares, such as CVX [52]. ■

By solving problems (29) and (31) during each iteration of the alternate search, we can obtain the optimal solution. The algorithm for the alternate search is summarized in Algorithm 1, where K_μ represents the maximum allowed number of iterations. Given a starting point and a convergence threshold μ, the iterative process can be terminated when $|\mathrm{SINR_p}(\mathbf{W}_p^k, \mathbf{W}_j^k) - \mathrm{SINR_p}(\mathbf{W}_p^{k-1}, \mathbf{W}_j^{k-1})| \leq \mu$ is satisfied. The convergence of the alternate search can be proven by the following Theorem 1.

Theorem 1 *As problem (29) and (31) are solvable. Then the sequence* $\mathrm{SINR_p}(\mathbf{W}_p^k, \mathbf{W}_j^k)$ *generated by alternate search algorithm converges monotonically.*

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2024.3419071

$$\xi_s^* = \begin{cases} 1 - \left(\frac{2P_p\delta_{pw}^2}{P_s\delta_{sw}^2}\right)^{\frac{P_s\delta_{sw}^2}{P_s\delta_{sw}^2 - 2P_p\delta_{pw}^2}} + \left(\frac{2P_p\delta_{pw}^2}{P_s\delta_{sw}^2}\right)^{\frac{2P_p\delta_{pw}^2}{2P_p\delta_{pw}^2 - P_s\delta_{sw}^2}}, P_p\delta_{pw}^2 = P_j\delta_{jw}^2 \neq P_s\delta_{sw}^2 \\ 1 - \frac{P_p\theta_{pw}^2}{P_p\theta_{pw}^2 - P_j\delta_{jw}^2}\left[\left(\frac{P_p\delta_{pw}^2}{P_j\delta_{jw}^2}\right)^{\frac{P_j\delta_{jw}^2}{P_j\delta_{jw}^2 - P_p\delta_{pw}^2}} - \left(\frac{P_p\delta_{pw}^2}{P_j\delta_{jw}^2}\right)^{\frac{P_p\delta_{pw}^2}{P_j\delta_{jw}^2 - P_p\delta_{pw}^2}}\right], \\ P_s\delta_{sw}^2 = P_j\delta_{jw}^2 \neq P_p\delta_{pw}^2 \vee P_s\delta_{sw}^2 = P_p\delta_{pw}^2 \neq P_j\delta_{jw}^2 \\ 1 + \frac{1}{\mathrm{e}} - \frac{1}{\sqrt{\mathrm{e}}}, P_s\delta_{sw}^2 = P_p\delta_{pw}^2 = P_j\delta_{jw}^2. \end{cases} \tag{24}$$

Algorithm 1 Alternate Search Algorithm

Input: ϵ

Output: $(\mathbf{W}_p^*, \mathbf{W}_j^*)$

1: Initialize a starting point $(\mathbf{W}_p^0, \mathbf{W}_j^0)$, calculate $\mathrm{SINR}_p(\mathbf{W}_p^0, \mathbf{W}_j^0)$; and set $k = 0$;
2: **repeat**
3: For the fixed $\mathbf{W}_j^k$, find the optimal solution $\mathbf{W}_p^{k+1}$ of problem (29);
4: For the obtained $\mathbf{W}_p^{k+1}$, find the optimal solution $\mathbf{W}_j^{k+1}$ of problem (31);
5: $k := k + 1$;
6: Calculate $\mathrm{SINR}_p(\mathbf{W}_p^k, \mathbf{W}_j^k)$;
7: **until** $|\mathrm{SINR}_p(\mathbf{W}_p^k, \mathbf{W}_j^k) - \mathrm{SINR}_p(\mathbf{W}_p^{k-1}, \mathbf{W}_j^{k-1})| \leq \mu$, or $k > K_\mu$;
8: Return $\mathbf{W}_p^* = \mathbf{W}_p^k, \mathbf{W}_j^* = \mathbf{W}_j^k$;

Proof: For a given $\mathbf{W}_j^k$, the optimal solution $\mathbf{W}_p^{k+1}$ of problem (29) is obtained, while $\mathbf{W}_p^k$ is only a feasible solution of problem (29) in this case. Thus we can conclude

$$\mathrm{SINR}_p(\mathbf{W}_p^{k+1}, \mathbf{W}_j^k) \geq \mathrm{SINR}_p(\mathbf{W}_p^k, \mathbf{W}_j^k). \tag{32}$$

Similarly, with the obtained $\mathbf{W}_p^{k+1}$, the optimal solution $\mathbf{W}_j^{k+1}$ of problem (31) is calculated, while $\mathbf{W}_j^k$ is only a feasible solution of problem (31). It follows that

$$\mathrm{SINR}_p(\mathbf{W}_p^{k+1}, \mathbf{W}_j^{k+1}) \geq \mathrm{SINR}_p(\mathbf{W}_p^{k+1}, \mathbf{W}_j^k). \tag{33}$$

Obviously, we have

$$\mathrm{SINR}_p(\mathbf{W}_p^{k+1}, \mathbf{W}_j^{k+1}) \geq \mathrm{SINR}_p(\mathbf{W}_p^k, \mathbf{W}_j^k), \tag{34}$$

which implies monotonic increasing of the sequence $\mathrm{SINR}_p(\mathbf{W}_p^k, \mathbf{W}_j^k)$. Since the SINR is upper bounded by $\mathrm{SINR}_p \leq \frac{\mathrm{Tr}(\mathbf{W}_p^m \mathbf{H}_{p,p})}{\delta_p^2}$, where $\mathrm{Tr}(\mathbf{W}_p^m) = P_p^m$, finally this generated sequence is convergent. ∎

B. Statistical CSI Scenario

In this section, we begin by evaluating the transmission outage probability, denoted as P_{out}, for covert communication between the PBS and PU_1 in the statistical CSI scenario. Both the PBS and the jammer are assumed to be equipped with a single antenna. Since the accurate transmission rate cannot be calculated in this scenario, we analyze the performance based on probabilities, specifically focusing on ETT. ETT represents the measure of information transmitted from the PBS to the PU while adhering to covert constraints in CRNs. Subsequently, we design the optimal transmission power for the PBS and the jammer to maximize the ETT while satisfying the covertness constraint.

According to (1), the instantaneous output SINRs at PU_1 and Willie are calculated as follows

$$\psi_p = \frac{P_p|h_{p,p}|^2}{P_j|h_{j,p}|^2 + \delta_p^2} = \frac{\gamma_{p,p}}{\gamma_{j,p} + 1}, \tag{35}$$

where

$$\gamma_{p,p} = \frac{P_p|h_{p,p}|^2}{\delta_p^2}, \gamma_{j,p} = \frac{P_j|h_{j,p}|^2}{\delta_p^2}. \tag{36}$$

Since $h_{p,p} \sim \mathcal{CN}(0, \delta_{p,p}^2)$, $h_{j,p} \sim \mathcal{CN}(0, \delta_{j,p}^2)$, $|h_{p,p}|^2$ and $|h_{j,p}|^2$ are chi-square distributed variables with 2 degrees of freedom, the mean $\delta_{p,p}^2$ and $\delta_{j,p}^2$, respectively. Therefore, $\gamma_{p,p}$ and $\gamma_{j,p}$ are chi-square distributed variables with 2 degrees of freedom, the mean $\beta_p = \frac{P_p\delta_{p,p}^2}{\delta_p^2} = P_p\alpha_p$ and $\beta_j = \frac{P_j\delta_{j,p}^2}{\delta_p^2} = P_j\alpha_j$, respectively. The probability density function of $\gamma_{p,p}$ and $\gamma_{j,p}$ can be computed as

$$f_{\gamma_{p,p}}(y) = \frac{1}{\beta_p} e^{-\frac{y}{\beta_p}}, y > 0, \tag{37}$$

$$f_{\gamma_{j,p}}(x) = \frac{1}{\beta_j} e^{-\frac{x}{\beta_j}}, x > 0, \tag{38}$$

respectively. The cumulative distribution function of $\gamma_{j,p}$ can be expressed as

$$\begin{aligned} F_{\gamma_{j,p}}(x) &= \int_{-\infty}^{x} \frac{1}{\beta_j} e^{-\frac{x}{\beta_j}} \, \mathrm{d}x \\ &= 1 - e^{-\frac{x}{\beta_j}}. \end{aligned} \tag{39}$$

Let $X_1 = X + 1 = \gamma_{j,p} + 1$, then the cumulative distribution function of X_1 can be calculated as

$$\begin{aligned} F_{\gamma_{j,p}}(x_1) &= P(X_1 \leq x_1) = P(X + 1 \leq x_1) \\ &= P(X \leq x_1 - 1) = 1 - e^{-\frac{x-1}{\beta_j}}. \end{aligned} \tag{40}$$

Then the probability density function of $X_1 = \gamma_{j,p} + 1$ is expressed as

$$f_{\gamma_{j,p}+1}(x_1) = F'_{\gamma_{j,p}+1}(x_1) = \frac{1}{\beta_j} e^{-\frac{x_1 - 1}{\beta_j}}, x_1 > 1, \tag{41}$$

Let $Y = \gamma_{p,p}$, $X_1 = \gamma_{j,p} + 1$, then we can obtain that $Z = \psi_p = \frac{Y}{X_1}$. On the basis of (37) and (41), the probability density function of ψ_p can be computed as

$$f_{\psi_p}(z) = \int_0^{+\infty} |x_1| f_{\gamma_{j,p}+1}(x_1) f_{\gamma_{p,p}}(x_1 z)\, \mathrm{d}x_1 = \frac{\beta_p \beta_j e^{\frac{1}{\beta_j}}}{(\beta_j + \beta_p z)^2}. \tag{42}$$

In the network, a transmission outage event occurs when the channel capacity $C = \log_2(1 + \psi_p)$ falls below the fixed transmission rate R, i.e., $C < R$. The transmission outage probability can be derived as

$$P_{\text{out}} = \mathbb{P}[\log_2(1 + \psi_p) < R] = \int_0^{2^R-1} \frac{\beta_p \beta_j e^{\frac{1}{\beta_j}}}{(\beta_j + \beta_p z)^2}\, \mathrm{d}z = \frac{\beta_p \beta_j e^{\frac{1}{\beta_j}}}{\beta_p \beta_j + \frac{\beta_p^2}{2^R-1}}. \tag{43}$$

Let $\alpha_p = \frac{\delta_{p,p}^2}{\delta_p^2}$ and $\alpha_j = \frac{\delta_{j,p}^2}{\delta_p^2}$, then the ETT is given by

$$T = R(1 - P_{\text{out}}), \tag{44}$$

which is used to assess the covert performance in the statistical CSI scenario. The optimization problem for the PBS aims to maximize the ETT while satisfying a specific covert communication constraint.

$$\max_{P_p, P_j} \quad T \tag{45a}$$

$$\text{s.t.} \quad \xi_s^*(P_p, P_j) \geq 1 - \epsilon, \tag{45b}$$

$$P_j \leq P_j^m, \tag{45c}$$

$$P_p \leq P_p^m, \tag{45d}$$

where P_p^m and P_j^m are the transmit power limits of the PBS and SU-Tx$_1$, respectively. (45b) is the covert constraint with the covert requirement ϵ. As shown in Fig. 8 and Fig. 9, $\xi_s^*(P_p, P_j)$ is monotonically decreasing function of P_p and is monotonically increasing function of P_j, respectively. It is assumed to be covert only when $\xi_s^* \geq 1 - \epsilon$. When $\xi_s^* = 1 - \epsilon$, we can obtain $P_j^{\text{covert}} = (\xi_s^*)^{-1}(1 - \epsilon)$. If the jammer's power is lower than P_j^{covert}, the covert constraint cannot be satisfied. Similarly, When $\xi_s^* = 1 - \epsilon$, we can obtain $P_p^{\text{covert}} = (\xi_s^*)^{-1}(1 - \epsilon)$. if the PBS's power is higher than P_p^{covert}, the covert constraint cannot be satisfied. Therefore, the optimization problem (45) can be rewritten as

$$\max_{P_p, P_j} \quad T \tag{46a}$$

$$\text{s.t.} \quad P_j^{\text{covert}} \leq P_j \leq P_j^m, \tag{46b}$$

$$P_p \leq \min(P_p^{\text{covert}}, P_p^m). \tag{46c}$$

Let $\alpha_p = \frac{\delta_{p,p}^2}{\delta_p^2}$ and $\alpha_j = \frac{\delta_{j,p}^2}{\delta_p^2}$, then the ETT is given by

$$T = R(1 - P_{\text{out}}) = \frac{\alpha_p \alpha_j P_p P_j e^{\frac{1}{\alpha_j P_j}}}{\alpha_p \alpha_j P_p P_j + \frac{\alpha_p^2 P_p^2}{2^R-1}}. \tag{47}$$

It can be seen from (47) that, given a fixed P_j, T increases monotonically with P_p. Similarly, given a fixed P_p, T monotonically decreases with P_j. Therefore, the optimization problem (46) can be solved by applying alternate search algorithm in Algorithm 1 in the set of (46b) and (46c), and we can obtain the transmission power of the PBS and the jammer.

V. Numerical Results

In this section, we present numerical results concerning the covert performance and secrecy performance in both scenarios with perfect CSI and statistical CSI. For all simulation experiments in this study, we employ Matlab (version 2017a), which provides a reliable platform for simulating wireless communication systems. A high-quality pseudo-random number generator (PRNG) is used to simulate the actual channel environment, ensuring the accuracy and validity of the results. The default simulation parameters are outlined in Table I. The channel vectors were generated using independent complex circularly-symmetric Gaussian (CSCG) random variables with a mean of zero and variance of one. To evaluate the system's performance, we conducted Monte Carlo simulations using 10,000 randomly generated channel-quadruplets. The simulation parameters are provided in Table I.

TABLE I: Simulation Parameters

Simulation parameter	value
The maximum power of the PBS P_p^m(dBm)	30
The maximum power of SU-Tx$_1$ P_j^m(dBm)	30
The number of antennas of the PBS	4
The number of antennas of SU-Tx$_1$	4
The interference temperature limit imposed at PU$_1$ θ	0.1
The distances between the PBS to PU$_1$ and Willie $d_{p,p}(d_{p,w})$ (m)	120
The distance between SU-Tx$_1$ to PU$_1$ $d_{j,p}$ (m)	150
The distance between SU-Tx$_1$ to Willie $d_{j,w}$ (m)	100
The target covert transmission threshold ϵ	0.1
The detecting duration τ (ms)	0.5
Noise power spectral density N_{02} (dBm/Hz)	-127
Transmission bandwidth B (MHz)	10

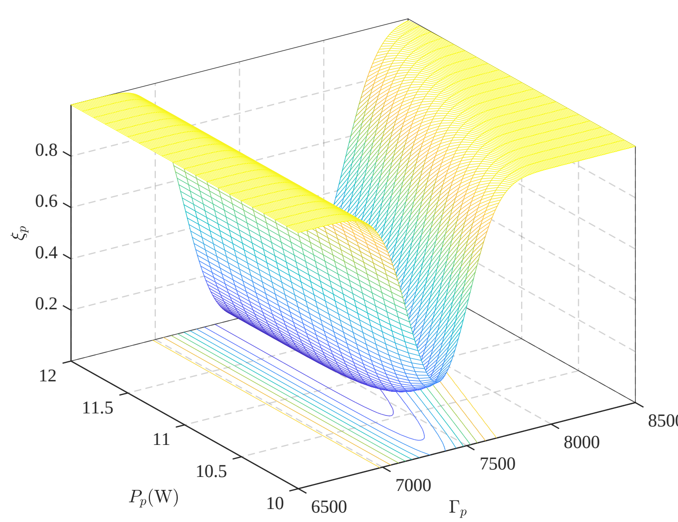


Fig. 3: DEP ξ_p against the detection threshold Γ_p for different $\hat{P}_p$.

A. Perfect CSI Scenario

Fig. 3 illustrates the covert performance in terms of DEP (ξ_p) as a function of the detection threshold (Γ_p), considering various levels of received power of primary signals ($\hat{P}_p$). With the increase of the detection threshold, the DEP first decreases and then increases. Furthermore, Fig. 3 demonstrates that the Detection DEP decreases as the received power of primary signals ($\hat{P}_p$) increases. This observation can be attributed to the fact that higher received power enhances Willie's ability to detect the primary signals.

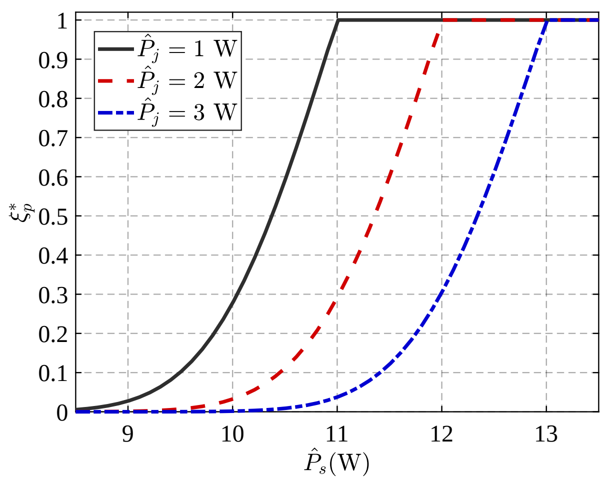


Fig. 4: Optimal DEP ξ_p^* against $\hat{P}_s$ for different $\hat{P}_j$.

In Fig. 4, we depict the optimal DEP ξ_p^* as a function of the received power of secondary signals $\hat{P}_s$ for various received power levels of jamming signals $\hat{P}_j$. It is observed that the DEP increases as the received power of secondary signals rises. When the received power of secondary signals surpasses or equals the combined power of primary and jamming signals, the DEP converges to 1. This signifies that ensuring covert performance of the primary signals is possible when the power of the secondary signals exceeds or equals the combined power of the primary and jamming signals.

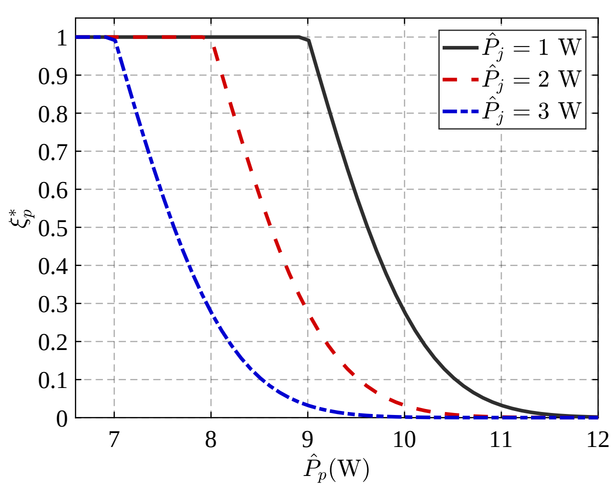


Fig. 5: Optimal DEP ξ_p^* against $\hat{P}_p$ for different $\hat{P}_j$.

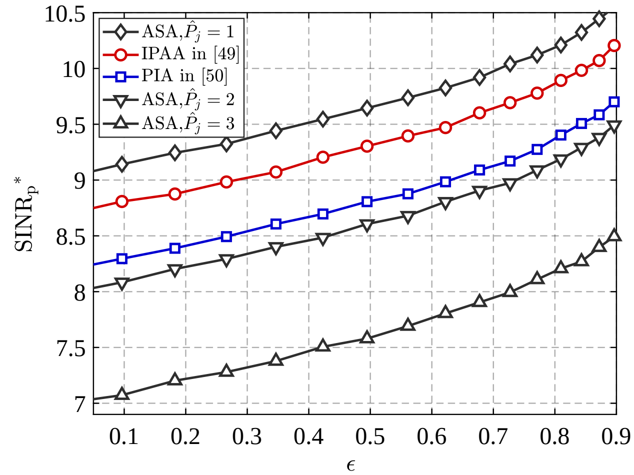


Fig. 6: Optimal $\mathrm{SINR}_\mathrm{p}^*$ against ϵ.

Fig. 5 depicts the optimal DEP ξ_p^* as a function of the received power of primary signals $\hat{P}_p$ for various levels of received jamming signals $\hat{P}_j$. It is evident that the DEP gradually decreases as the received power of primary signals increases. Furthermore, it is observed that when the received power of primary signals is less than or equal to the difference between the power of the secondary signals and the power of jamming signals, the DEP converges to 1. In combination with Fig. 4, we can obtain that $\hat{P}_p$, $\hat{P}_j$ and $\hat{P}_s$ need to be carefully designed to meet the equation $\hat{P}_p + \hat{P}_j$, so as to achieve the covert requirement of primary signals.

Fig. 6 plots the optimal $\mathrm{SINR}_\mathrm{p}^*$ versus ϵ for different $\hat{P}_j$. For comparison, the performance of the two benchmark schemes are also investigated, namely the Proposed Iterative Algorithm (PIA) proposed in [53] and the Iterative Power Allocation Algorithm (IPAA) proposed in [54]. It is assumed to be covert for PU when $\xi^* \geq 1 - \epsilon$. It can be seen that compared with the algorithms in the above literatures, the Alternate Search Algorithm (ASA) in this paper has a better SINR. This is because we jointly optimize $\mathbf{W}_p$ and $\mathbf{W}_j$ to optimize SINR. In addition, it can be seen that the lower the ϵ, the higher the requirement for covert performance. Fig. 6 shows that the lower ϵ is, the lower the SINR is. This shows that in order to achieve a better covert performance, the reduction of SINR is a cost. In addition, the SINR decreases with $\hat{P}_j$ due to the interference at PU. Hence, it is better to transmit jamming signals below a temperature limit θ. This figure demonstrates that the introduction of jamming signals in order to achieve covert performance pays the price of reducing the SINR.

Fig. 7 investigates the optimal $\hat{P}_j^*$ against ϵ for different $\hat{P}_p$. It is clear that a higher ϵ leads to a higher received power of jamming signals. This means that the improvement of covert performance requirement does not require more jamming signals. Additionally, it can be observed that $\hat{P}_j^*$ decreases as $\hat{P}_p$ increases. This implies that when $\hat{P}_p$ reaches a sufficiently high level, additional jamming signals become unnecessary. Consequently, the power of the jamming signals must be meticulously designed to fulfill the covert performance requirement.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2024.3419071

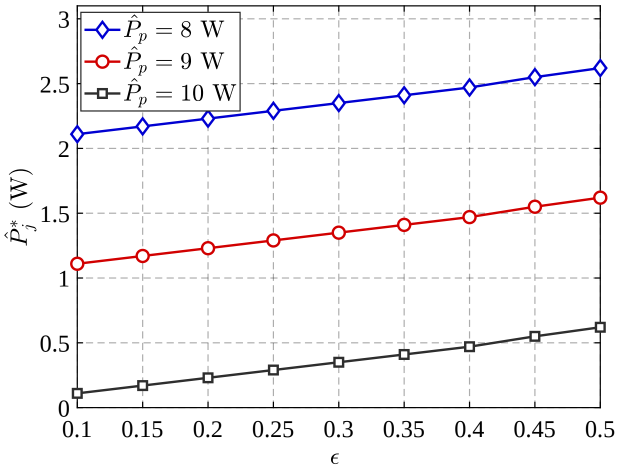


Fig. 7: Optimal $\hat{P}_j^*$ against ϵ for different $\hat{P}_p$.

B. Statistical CSI Scenario

Fig. 8 displays the results of the false alarm probability (P_{FA}), miss detection probability (P_{MD}), and total error probability (DEP) as functions of Willie's detection threshold (Γ_s). The simulated curves are obtained from the preliminary analysis of (19), (20) and (14), respectively. To acquire the simulated curves, extensive Monte-Carlo simulations were conducted, involving the generation of a substantial number of random values for P_p, P_j, P_s, $|h_{pw}|^2$, $|h_{jw}|^2$ and $|h_{sw}|^2$. Upon observing Fig. 8, it becomes evident that the simulated results align closely with the corresponding theoretical predictions, thus affirming the validity of Lemma 1. What is striking about the DEP ξ_s in this figure is that there is an optimal value of Γ_s that minimizes ξ_s, thereby corroborating the assertion made in Lemma 2.

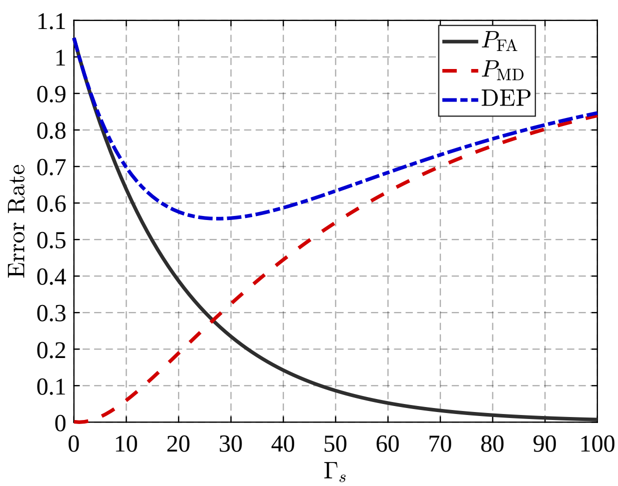


Fig. 8: Error rate against the detection threshold Γ_s.

The minimal detection error probability ξ_s^* is examined across different values of N_p and N_j in Fig. 9. The results reveal that, with an increase in N_p, ξ_s^* consistently decreases. This phenomenon is attributable to the heightened transmission power of the PBS, rendering it more susceptible to detection by Willie. However, a point of convergence is observed as N_p continues to rise, signifying that the transmit power of PBS has reached a threshold, halting further enhancement in Willie's detection capability. Similarly, an increase in N_j corresponds to a gradual increase in ξ_s^*. This can be elucidated by noting that higher values of N_j result in increased power of jamming signals, optimizing the beamforming design and intensifying interference against Willie. Nonetheless, a point of convergence is again witnessed as N_j persists in its ascent, indicating that the transmission power of the jamming signals has attained a threshold, leading to a cessation in the decline of Willie's detection.

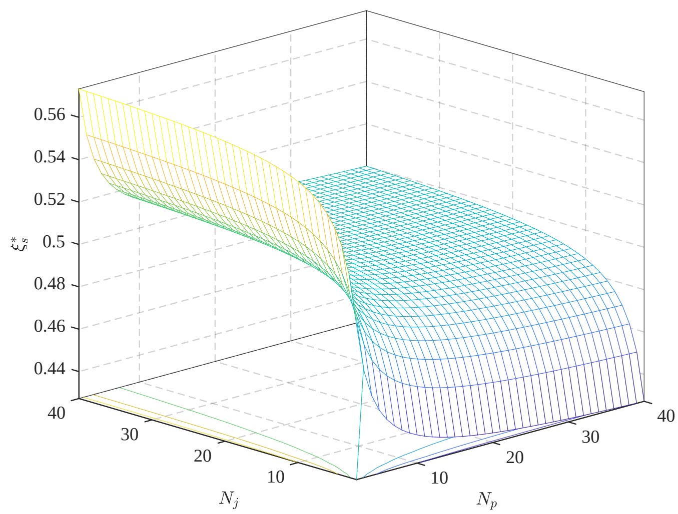


Fig. 9: Minimal detection error probability ξ_s^* against the N_p with different N_j.

ETT represents the measure of information transmitted from the PBS to the PU while adhering to covert constraints in CRNs. In Figure 10, ETT is depicted as a function of N_p and N_j, illustrating how different antennas affect the amount of information that can be effectively transmitted from the PBS to the PU under covert communication constraints. Obviously, T increases monotonically with N_p and decreases monotonically with N_j, consistent with the analysis in Section IV-B. Since increasing N_j will cause the interference signal power to increase, T will decrease. Therefore, it is crucial to strike a balance between covert performance improvements and ETT. N_j needs to be accurately designed so that the transmission power P_j of the interference signal satisfies $P_j = P_j^{\mathrm{covert}}$.

Figure 11 further elaborates on the relationship between ETT and P_p for various transmission rates R, providing a detailed analysis of the impact of these parameters on the transmission throughput. The results reveal that T initially increases and then decreases as the transmission rate R varies, indicating the existence of an optimal value R^* that maximizes T. Moreover, we observe that increasing P_p leads to a higher ETT. Hence, the transmission power of primary signals, P_p, should be set as $P_p = \min(P_p^{\mathrm{covert}}, P_p^m)$.

VI. Conclusion

In recent years, significant attention has been given to exploring the fundamental limits of covert communications

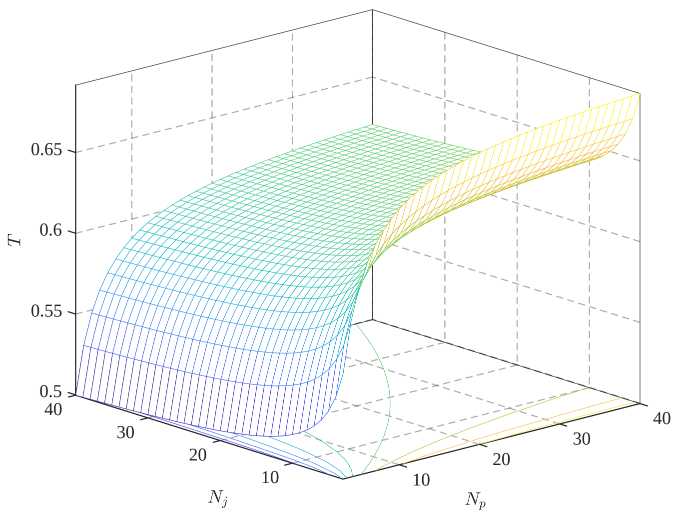


Fig. 10: Effective transmission throughput (ETT) T against N_p with different N_j.

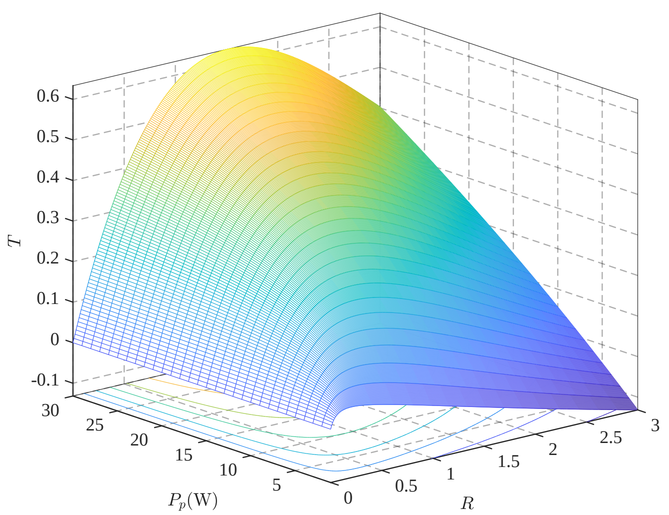


Fig. 11: Effective transmission throughput (ETT) T against the fixed transmission rate R with different P_p.

at the physical layer for CCRNs. Nevertheless, limited research has been conducted on the simultaneous integration of jamming and secondary signals to guarantee covertness. To address this gap, the present paper delves into covert communications within an overlay CCRN and thoroughly examines the concurrent introduction of jamming and secondary signals. The objective is to enhance covertness through the combined use of jamming and secondary signals in CCRNs. In the CCRN, the PBS aims to transmit messages covertly to a PU under the surveillance of a warden, Willie. Additionally, an SU-Tx is selected as a friendly jammer, emitting jamming signals to confuse Willie. In the scenario of perfect CSI, we formulate an optimization problem to maximize the SINR at the PU while satisfying a covert constraint, namely, ensuring the DEP at Willie exceeds a certain threshold. To solve this optimization problem, we propose an alternate search algorithm. In the statistical CSI scenario, we formulate a different optimization problem that aims to maximize the ETT while adhering to the covert constraint. Furthermore, we present numerical results to demonstrate the performance of the covertness in both scenarios.

There are potential vulnerabilities and attack scenarios that could compromise the security and effectiveness of our techniques. Firstly, while this paper considers the scenario of a single Willie, in reality, there may be multiple colluding intelligent Willies, multiple cooperative jammers are needed to interfere with them respectively. Secondly, cooperative jammers may be manipulated to become untrustworthy nodes, so CBS needs to regularly detect and monitor the behavior of cooperative jammers. Thirdly, wardens may be dynamic, requiring cooperative jammers to adjust their jamming strategy in real-time. In addition, the model discussed in this paper is centralized, and the potential of a distributed model should be further explored.

REFERENCES

[1] W. Zhang, A. Tait, C. Huang, T. Ferreira de Lima, S. Bilodeau, E. C. Blow, A. Jha, B. J. Shastri, and P. Prucnal, "Broadband physical layer cognitive radio with an integrated photonic processor for blind source separation," *Nature communications*, vol. 14, no. 1, p. 1107, 2023.

[2] W. U. Khan, Z. Ali, E. Lagunas, A. Mahmood, M. Asif, A. Ihsan, S. Chatzinotas, B. Ottersten, and O. A. Dobre, "Rate splitting multiple access for next generation cognitive radio enabled leo satellite networks," *IEEE Transactions on Wireless Communications*, 2023.

[3] M. Wasilewska, H. Bogucka, and H. V. Poor, "Secure federated learning for cognitive radio sensing," *IEEE Communications Magazine*, vol. 61, no. 3, pp. 68–73, 2023.

[4] A. F. Tayel, S. I. Rabia, A. H. Abd El-Malek, and A. M. Abdelrazek, "Throughput maximization of hybrid access in multi-class cognitive radio networks with energy harvesting," *IEEE Transactions on Communications*, vol. 69, no. 5, pp. 2962–2974, 2021.

[5] Y. Wen, T. Jing, and Q. Gao, "Trustworthy jammer selection with truth-telling for wireless cooperative systems," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–17, 2021.

[6] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent advances in post-quantum cryptography for networks: A survey," in *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*. IEEE, 2022, pp. 1–8.

[7] F. Mallouli, A. Hellal, N. S. Saeed, and F. A. Alzahrani, "A survey on cryptography: comparative study between rsa vs ecc algorithms, and rsa vs el-gamal algorithms," in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, 2019, pp. 173–176.

[8] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in internet of things (iot) using cryptography and steganography techniques," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 73–80, 2019.

[9] Y. Wen, Y. Huo, T. Jing, and Q. Gao, "A reputation framework with multiple-threshold energy detection in wireless cooperative systems," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.

[10] Y. Wen, T. Jing, Y. Huo, Z. Li, and Q. Gao, "Secrecy energy efficiency optimization for cooperative jamming in cognitive radio networks," in *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2018, pp. 795–799.

[11] X. Li, Y. Zheng, W. U. Khan, M. Zeng, D. Li, G. Ragesh, and L. Li, "Physical layer security of cognitive ambient backscatter communications for green internet-of-things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1066–1076, 2021.

[12] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.

[13] Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, "A scheme for trustworthy friendly jammer selection in cooperative cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3500–3512, 2019.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2024.3419071

[14] K. Li, R. C. Voicu, S. S. Kanhere, W. Ni, and E. Tovar, "Energy efficient legitimate wireless surveillance of uav communications," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2283–2293, 2019.

[15] R. Ahmed, Y. Chen, B. Hassan, and L. Du, "Cr-iotnet: Machine learning based joint spectrum sensing and allocation for cognitive radio enabled iot cellular networks," *Ad Hoc Networks*, vol. 112, p. 102390, 2021.

[16] A. Nasser, H. Al Haj Hassan, J. Abou Chaaya, A. Mansour, and K.-C. Yao, "Spectrum sensing for cognitive radio: Recent advances and future challenge," *Sensors*, vol. 21, no. 7, p. 2408, 2021.

[17] M. S. Gupta and K. Kumar, "Progression on spectrum sensing for cognitive radio networks: A survey, classification, challenges and future research issues," *Journal of Network and Computer Applications*, vol. 143, pp. 47–76, 2019.

[18] R. Chen, Z. Li, J. Shi, L. Yang, and J. Hu, "Achieving covert communication in overlay cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 113–15 126, 2020.

[19] X. Liao, J. Si, J. Shi, Z. Li, and H. Ding, "Generative adversarial network assisted power allocation for cooperative cognitive covert communication system," *IEEE Communications Letters*, vol. 24, no. 7, pp. 1463–1467, 2020.

[20] Z. Li, X. Liao, J. Shi, L. Li, and P. Xiao, "Md-gan-based uav trajectory and power optimization for cognitive covert communications," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 10 187–10 199, 2021.

[21] T. Cao, L. Liu, K. Wang, and J. Li, "A fractional integral and fractal dimension-based deep learning approach for pavement crack detection in transportation service management," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 4201–4212, 2022.

[22] R. Chen, J. Yang, H. Zhou, R. Lu, and D. Zeng, "Covert communication in two-hop cooperative cognitive radio system," *IEEE Transactions on Vehicular Technology*, 2023.

[23] X. Lu, S. Yan, W. Yang, C. Liu, and D. W. K. Ng, "Short-packet covert communication in interweave cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2649–2654, 2022.

[24] Z. Li, R. Chen, J. Shi, L. Yang, and S. Ma, "A game-theoretic approach to achieve covert communication in cognitive radio systems," *IEEE Transactions on Vehicular Technology*, 2023.

[25] R. Chen, Z. Li, J. Shi, L. Yang, and J. Hu, "Achieving covert communication in overlay cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 113–15 126, 2020.

[26] X. Chen, Z. Chang, N. Zhao, Y. Chen, F. R. Yu, and T. Hämäläinen, "Multi-antenna covert communication with jamming in the presence of a mobile warden," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. IEEE, 2021, pp. 1–6.

[27] H.-S. Im and S.-H. Lee, "Mobility-assisted covert communication over wireless ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1768–1781, 2020.

[28] W. Mazurczyk, S. Wendzel, M. Chourib, and J. Keller, "Countering adaptive network covert communication with dynamic wardens," *Future Generation Computer Systems*, vol. 94, pp. 712–725, 2019.

[29] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on awgn channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, 2012.

[30] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493–3503, 2016.

[31] F. Shu, T. Xu, J. Hu, and S. Yan, "Delay-constrained covert communications with a full-duplex receiver," *IEEE Wireless Communications Letters*, vol. 8, no. 3, pp. 813–816, 2019.

[32] T. Cao, Y. Wang, and S. Liu, "Pavement crack detection based on 3d edge representation and data communication with digital twins," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, 2023.

[33] B. He, S. Yan, X. Zhou, and V. K. Lau, "On covert communication with noise uncertainty," *IEEE Communications Letters*, vol. 21, no. 4, pp. 941–944, 2017.

[34] T.-X. Zheng, H.-M. Wang, D. W. K. Ng, and J. Yuan, "Multi-antenna covert communications in random wireless networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 3, pp. 1974–1987, 2019.

[35] K. Shahzad, X. Zhou, and S. Yan, "Covert wireless communication in presence of a multi-antenna adversary and delay constraints," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 12 432–12 436, 2019.

[36] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, and H. Haas, "Physical-layer security in 6g networks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1901–1914, 2021.

[37] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6g wireless: The role of physical layer security," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 102–108, 2022.

[38] Y. Wen, L. Liu, J. Li, X. Hou, N. Zhang, M. Dong, M. Atiquzzaman, K. Wang, and Y. Huo, "A covert jamming scheme against an intelligent eavesdropper in cooperative cognitive radio networks," *IEEE Transactions on Vehicular Technology*, 2023.

[39] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 11, pp. 7252–7267, 2018.

[40] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.

[41] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communications in iot systems: Hiding information in interference," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 46–52, 2018.

[42] D. Raghunatharao, T. J. Prasad, and M. Giri Prasad, "Optimal pilot-based channel estimation in cognitive radio," *Wireless Personal Communications*, vol. 114, pp. 2801–2819, 2020.

[43] R. Caromi, S. Mohan, and L. Lai, "Optimal sequential channel estimation and probing for multiband cognitive radio systems," *IEEE Transactions on Communications*, vol. 62, no. 8, pp. 2696–2708, 2014.

[44] J. Mansukhani and P. Ray, "Simultaneous detection and channel estimation for censoring-based spectrum sensing in cognitive radio networks," *IEEE Wireless Communications Letters*, vol. 7, no. 3, pp. 292–295, 2017.

[45] H. Yazdani, A. Vosoughi, and X. Gong, "Achievable rates of opportunistic cognitive radio systems using reconfigurable antennas with imperfect sensing and channel estimation," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 3, pp. 802–817, 2021.

[46] Z. Wang, H. Xu, L. Zhao, X. Chen, and A. Zhou, "Deep learning for joint pilot design and channel estimation in symbiotic radio communications," *IEEE Wireless Communications Letters*, vol. 11, no. 10, pp. 2056–2060, 2022.

[47] F. Gao, R. Zhang, Y.-C. Liang, and X. Wang, "Optimal design of learning based mimo cognitive radio systems," in *2009 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2009, pp. 2537–2541.

[48] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, 2013.

[49] B. F. Lo, "A survey of common control channel design in cognitive radio networks," *Physical Communication*, vol. 4, no. 1, pp. 26–39, 2011.

[50] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

[51] R. Tandra and A. Sahai, "Snr walls for signal detection," *IEEE Journal of selected topics in Signal Processing*, vol. 2, no. 1, pp. 4–17, 2008.

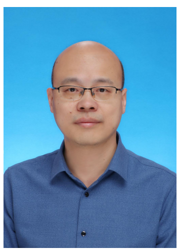
[52] M. Grant, S. Boyd, and Y. Ye, "CVX: Matlab software for disciplined convex programming," 2008.

[53] M. Forouzesh, F. S. Khodadad, P. Azmi, A. Kuhestani, and H. Ahmadi, "Simultaneous secure and covert transmissions against two attacks under practical assumptions," *IEEE Internet of Things Journal*, 2023.

[54] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Joint information-theoretic secrecy and covert communication in the presence of an untrusted user and warden," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7170–7181, 2020.

Yingkun Wen received the B.S. degree from North China Electric Power University, Baoding, China, in 2015, and the Ph.D degree from Beijing Jiaotong University, Beijing, China. He is current an Instructor with the school of computer science and engineering, Xi'an University of Technology, Xi'an, China. His research interests include physical layer security, covert communication, cognitive radio networks and cooperative communication.

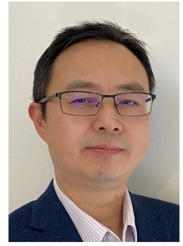
Lei Liu received the B.Eng. degree in communication engineering from Zhengzhou University, Zhengzhou, China, in 2010, and the M.Sc.and Ph.D. degrees in communication engineering from Xidian University, Xian, China, in 2013 and 2019, respectively. From 2013 to 2015, he worked in a technology company. From 2018 to 2019, he was supported by China Scholarship Council to be a visiting Ph.D. student with the University of Oslo, Oslo, Norway. He is currently a Lecture with the Department of Electrical Engineering and Computer Science, Xidian University. His research interests include vehicular ad hoc networks, intelligent transportation, mobile-edge computing, and Internet of Things.



Junhuai Li received the B.S. degree in electrical automation from the Shaanxi Institute of Mechanical Engineering, Xi'an, China, in 1992, the M.S. degree in computer application technology from the Xi'an University of Technology, Xi'an, in 1999, and the Ph.D. degree in computer software and theory from Northwest University, Xi'an, in 2002. He is currently a Professor with the School of Computer Science and Engineering, Xi'an University of Technology, China. His research interests include the Internet of Things technology and network computing.

Kan Wang received the Ph.D. degree in military communications from the State Key Laboratory of Integrated Services Networks, Xidian University, Xidian University, Xi'an, China, in 2016. Since March 2017, he has been with the School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China. His current research interests include wireless resource allocation, network slicing, convex optimization, and machine learning.

Yilan Li received her B.S. degree in Information Engineering from Xian Jiaotong University, in 2012, the M.S. degree in Electrical Engineering and Computer Science from Syracuse University, in 2015, and the Ph.D. degree in Electrical and Computer Engineering from Syracuse University, in 2021. She is currently an Instructor at School of Computer Science and Technology in Xi'an University of Technology, China. Her research interests include neuromorphic systems for unmanned aerial vehicles planning and control, natural language processing, neural network architecture optimization, etc.



Shui Yu (IEEE F'23) obtained his PhD from Deakin University, Australia, in 2004. He is a Professor of School of Computer Science, Deputy Chair of University Research Committee, University of Technology Sydney, Australia. His research interest includes Cybersecurity, Network Science, Big Data, and Mathematical Modelling. He has published five monographs and edited two books, more than 500 technical papers at different venues, such as IEEE TDSC, TPDS, TC, TIFS, TMC, TKDE, TETC, ToN, and INFOCOM. His current h-index is 74. Professor Yu promoted the research field of networking for big data since 2013, and his research outputs have been widely adopted by industrial systems, such as Amazon cloud security. He is currently serving the editorial boards of IEEE Communications Surveys and Tutorials (Area Editor) and IEEE Internet of Things Journal (Editor). He served as a Distinguished Lecturer of IEEE Communications Society (2018-2021). He is a Distinguished Visitor of IEEE Computer Society, and an elected member of Board of Governors of IEEE VTS and ComSoc, respectively. He is a member of ACM and AAAS, and a Fellow of IEEE.

Mohsen Guizani (Fellow, IEEE) received the B.S. (with distinction), M.S. and Ph.D. degrees in electrical and computer engineering from Syracuse University, Syracuse, NY, USA, in 1985, 1987, and 1990,respectively. He is currently a Professor of machine learning and the Associate Provost with the Mo-hamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE. He was with different institutions in the USA. He is the author of ten books and more than publications. His research interests include applied machine learning and artificial intelligence, Internet of Things (IoT), intelligent autonomous systems, smart city, and cybersecurity. He was elevated to the IEEE Fellow in 2009 and was listed as a Clarivate Analytics Highly Cited Researcher in Computer Science in 2019, 2020 and 2021. Dr. Guizani was the recipient of several research awards, including the 2015 IEEE Communications Society Best Survey Paper Award, the Best ComSoc Journal Paper Award in 2021 and five Best Paper Awards from ICC and Globecom Conferences. He was also the recipient of the 2017 IEEE Communications Society Wireless Technical Committee Recognition Award, 2018 AdHoc Technical Committee Recognition Award, and 2019 IEEE Communications and Information Security Technical Recognition Award. He was the Editor-in-Chief of IEEE Network and is currently serving on the Editorial Boards of many IEEE Transactions and Magazines. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He was the IEEE Computer Society Distinguished Speaker and is currently the IEEE ComSoc Distinguished Lecturer.