A Scheme for Trustworthy Friendly Jammer Selection in Cooperative Cognitive Radio Networks

Yingkun Wen, Yan Huo, Liran Ma, Tao Jing, and Qinghe Gao

***Abstract*—In this paper, we consider a centralized cooperative cognitive radio network (CCRN), where a primary base station sends a message to a primary user. Meanwhile, a secondary user transmitter (SU-Tx) acts as a friendly jammer that sends jamming signals (artificial noise) to protect the transmitted message from a potential eavesdropper (Eve). However, the SU-Tx may not be completely honest in sending jamming signals for selfish reasons, i.e., it may be untrusted. To select a trustworthy SU-Tx as a friendly jammer, we adopt the concept of *trust degree* as a selection criterion. We investigate the trust degree's influence on the secrecy performance of a CCRN in cases of perfect channel state information (CSI) and statistical CSI, respectively. In the case of perfect CSI, the accurate expected secrecy rate is derived to evaluate the secrecy performance. In the case of statistical CSI, we calculate the probabilities of the transmission and secrecy outage events, and the secrecy performance is evaluated in terms of effective secrecy throughput. In both cases, we obtain the target trust degree thresholds based on the target secrecy performance thresholds, respectively. Next, we investigate how to calculate the trust degree of each SU-Tx and establish a trust degree list of all SU-Txs. Finally, according to the trust degree list and the target trust degree thresholds, we can select a trustworthy SU-Tx as a friendly jammer in both two cases. A comprehensive simulation study is carried out to validate our secrecy performance analyses and the trust degree management.**

***Index Terms*—Cooperative cognitive radio network, physical layer security, cooperative jamming, trust degree, hypothesis testing.**

I. Introduction

COOPERATIVE cognitive radio networks (CCRNs) are emerging as a new paradigm to improve spectral efficiency [1], [2]. Due to the broadcast nature of the wireless medium, a transmitted message by a primary base station (PBS) may be intercepted and decoded by an eavesdropper (Eve) [3]. To counter eavesdropping, a cognitive base station (CBS) selects a secondary user transmitter (SU-Tx) as a friendly jammer. The jammer sends out jamming signals (i.e., artificial noise) to specifically interfere with Eve's reception so that the transmitted message cannot be decoded. In return, the selected SU-Tx is allowed to access the licensed spectrum [4], [5].

However, a selected SU-Tx may not be completely honest in helping the PBS for selfish reasons such as energy conservation [6]. Specifically, the SU-Tx just sends partial (or even none) jamming signals to gain undeserved spectral resources. In this paper, this kind of SU-Tx is defined as an untrusted friendly jammer. In the case that the jammer is untrusted, the message transmitted by the PBS could not be protected from being eavesdropped, while the SU-Tx would access undeserved spectral resources. To avoid this case to occur, it is necessary to select a trustworthy SU-Tx as a jammer. To the best of our knowledge, such a selection scheme does not exist in the current literature, which motivates our study in this paper.

In this paper, we design a scheme to select a trustworthy SU-Tx as a friendly jammer. In the scheme, the concept of *trust degree*is adopted as a selection criterion. The trust degree is defined as a belief level that the PBS can put an SU-Tx for a specific action (sending jamming signals). The trust degree is quantified based on historical observations on positive or negative behavior of the SU-Tx (whether sending jamming signals or not) [7]. In the CCRN, if a selected SU-Tx's trust degree could guarantee that the secrecy performance reaches the target secrecy performance threshold, then the SU-Tx is considered as a trustworthy jammer. Therefore, we need to analyze the trust degree's influence on the secrecy performance and calculate a target trust degree threshold. Specifically, a fundamental measure for secrecy performance is secrecy rate [8]. Thus we investigate the trust degree's influence on the secrecy rate of the PBS in the cases of perfect channel state information (CSI) and statistical CSI, respectively.

In the case of perfect CSI, we can calculate accurate secrecy rates of the PBS under trusted and untrusted jammer scenarios. Then we adopt the concept of the expected secrecy rate to evaluate the secrecy performance of the CCRN. The expected secrecy rate is calculated by combining the secrecy rates of two scenarios with different weight factors, i.e., the trust degree and the complement of the trust degree, respectively. Then for a given target expected secrecy rate, we can calculate the target trust degree threshold of SU-Txs for the perfect CSI case.

In some cases, we may only be able to acquire statistical CSI due to channel estimation and quantization errors. As a result, the accurate secrecy rate cannot be calculated. Instead, we calculate the effective secrecy throughput to evaluate the

Manuscript received July 10, 2018; revised November 28, 2018 and January 6, 2019; accepted January 20, 2019. Date of publication January 28, 2019; date of current version April 16, 2019. This work was supported by the National Natural Science Foundation of China under Grants 61871023 and 61572070, in part by the Fundamental Research Funds for the Central Universities under Grant 2017YJS035, and in part by the NSF of the US under Grant OAC-1829553. The review of this paper was coordinated by Dr. Y. Ma. *(Corresponding author: Yingkun Wen.)*

Y. Wen, Y. Huo, T. Jing, and Q. Gao are with the School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China (e-mail: 16111024@bjtu.edu.cn; yhuo@bjtu.edu.cn; tjing@bjtu.edu.cn; 14111028@bjtu.edu.cn).

L. Ma is with the Department of Computer Science, Texas Christian University, Fort Worth, TX 76129 USA (e-mail: l.ma@tcu.edu).

Digital Object Identifier 10.1109/TVT.2019.2895639

secrecy performance of the CCRN. To be specific, we first derive the probabilities of transmission and secrecy outage events for both trusted and untrusted jammer scenarios. According to these probabilities, we derive the expression of the effective secrecy throughput. Then for a given target effective secrecy throughput threshold, we could calculate the target trust degree threshold for the statistical CSI case.

After we obtain the target trust degree thresholds, it is necessary to investigate how to calculate the trust degree of each SU-Tx. In this paper, the trust degree of an SU-Tx is calculated by averaging its reputation, where the reputation is updated according to the positive or negative behavior of the SU-Tx (whether the SU-Tx sends jamming signals or not). Therefore, the CBS is in charge of detecting whether the SU-Tx sends jamming signals or not. An energy detection method is used in the perfect CSI case, while a composite hypothesis testing method is used in the statistical CSI case. According to the positive or negative detection results of an SU-Tx, we take an incentive mechanism to update its reputation. Finally, we can establish a trust degree list of all SU-Txs. If there is not any SU-Tx that could reach the target trust degree threshold, no SU-Tx would be selected. Otherwise, we would select the SU-Tx with the upmost trust degree as a trustworthy friendly jammer.

The rest of the paper is organized as follows. In Section II, the related work is reviewed. We describe the network model and assumptions in Section III. In Section IV, the expected secrecy rate is formulated in the case of perfect CSI. In Section V, the effective secrecy throughput is calculated in the case of statistical CSI. In Section VI, the scheme for trustworthy friendly jammer selection is presented. Numerical results are given in Section VII, and conclusions are drawn in Section VIII.

Notations: $(\cdot)^H$ and $|\cdot|$ denote the Hermitian transpose and the absolute value, respectively. $\mathrm{Tr}(\cdot)$ denotes the trace operator. $\mathbf{0}_{N\times N}$ represents the $N \times N$ matrix of all zeros. $\mathbf{I}_N$ is the $N \times 1$ vector of all ones. The distribution of a circularly symmetric complex Gaussian (CSCG) random variable with zero mean and variance σ^2 is denoted as $\mathcal{CN}(0, \sigma^2)$. $\langle \mathrm{A}, \mathrm{B} \rangle = \mathrm{Tr}(\mathrm{A}^{\mathrm{H}}\mathrm{B})$ and $[x]^+ = \max\{x, 0\}$.

II. Related Work

In recent years, communication security has been at the forefront of cognitive radio networks (CRNs) [9]–[12]. Traditional encryption methods at upper layers have expensive operations and are of high complexity for CRNs without infrastructures[13]. As a complement to the encryption methods, physical layer security has drawn much attention owing to the advantages of lower complexity and resource saving [14]–[16]. In [15], a tutorial is presented on several relevant methods to enhance security at the physical layer. Specifically, the cooperative jamming methods is one popular physical layer security solution for CRNs [17], [18].

By using the cooperative jamming method, CCRNs were considered as a new paradigm to improve security[19]–[21]. In [19], the authors investigated the secure communication issue for a CCRN. The authors of [20] investigated the problem of jammer selection for enhancing the secrecy goodput for a multi-input multi-output (MIMO) CCRN. In [21], Li *et al.* proposed a jamming scheme for a CCRN, where secondary users (SUs) were employed as helpers to send jamming signals. An effective cooperation strategy of helpers was also designed by using a coalition formation game.

In addition to the relationship between users in the physical layer, cooperative networks also rely on the relationship between users in the social layer. The social relationship between users has been exploited for the design of efficient cooperation strategies [22]. Trust degree was used as a key parameter to quantify the social relationship between users for cooperative networks [23], [24]. In [22], it was shown that the expected secrecy rate can be improved by exploiting the trust degree of untrustworthy users, such as untrusted relays and untrusted jammers.

Untrusted relays have been widely investigated in cooperative networks for physical layer security [25]–[27]. In [25], the authors jointly optimized the source and untrusted relay beamforming vectors for maximizing the secrecy sum rate of the two-way relay communications. In [26], physical layer security issues were investigated in the two-way untrusted relay network with the help of friendly jammers. The authors of [27] investigated the problem of physical layer security for a wireless cooperative network with multiple untrusted relays.

Untrusted jammers in cooperative networks for physical layer security were investigated in [28]–[30]. In [28], the authors investigated a untrusted jammer selection policy by jointly considering the physical channel and the relationship between users. The authors of [29] investigated how to select untrusted jammers for device-to-device (D2D) users to maximize the worst-case eavesdropping. In these studies, the social trust of a friendly jammer was just considered as a simulation parameter to analyze the secrecy performance of a network. However, to the best of our knowledge, how to quantify and evaluate the trustworthiness of a friendly jammer has never been investigated, which motivates the study of this paper.

III. System Model and Assumptions

In this paper, we consider a centralized CCRN consisting of a primary network and a cognitive network as depicted in Fig. 1. In the primary network, there is a PBS that is associated with m PUs. The PBS is equipped with N_p antennas, PUs are equipped with single antenna. In the cognitive network, there exists a CBS with n pairs of SU-Txs and SU-Rxs, where SU-Rxs are not illustrated (the reason is explained below). The CBS is equipped with single antenna, SU-Txs are all equipped with N_j antennas.

In the primary network, the PBS wants to send a message to a PU (e.g., PU_1).[1] Meanwhile, there is an Eve that wants to intercept and decode the message. To protect the transmitted message from being eavesdropped, the PBS asks the CBS to select an SU-Tx (e.g., $\mathrm{SU\text{-}Tx}_1$) as a friendly jammer to interfere with Eve. After jamming, when the primary channel is idle, $\mathrm{SU\text{-}Tx}_1$

[1] In this paper, it is assumed that spectrums for multiple PUs are orthogonal with each other. Thus the PBS can provide service to multiple PUs and there is no interference between PUs. Based on this assumption, we consider a single PU (PU_1) as an example and analyze the secrecy rate for PU_1.

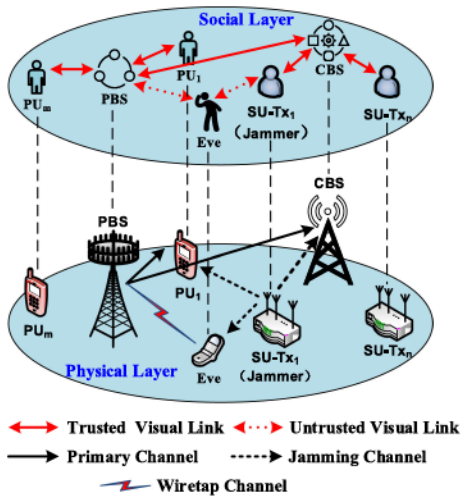

Fig. 1. Network Model for a centralized CCRN.

is allowed to access the primary channel to transmit its message. Therefore, from SU-Tx$_1$'s perspective, its transmission process consists of the following two alternating phases:

- *Jamming Phase:* When the PBS sends messages to PU$_1$, SU-Tx$_1$ transmits jamming signals to interfere with Eve.
- *Accessing Phase:* When the PBS does not send messages, SU-Tx$_1$ accesses the idle primary channel to transmit its message to SU-Rx$_1$.

In this paper, we just consider the jamming phase, while the accessing phase would be discussed in the later work (this is the reason why SU-Rxs are not illustrated in Fig. 1).

Traditionally, such a CCRN is only considered in the physical layer with a basic assumption: there is an SU-Tx that always sends jamming signals. However, when the social layer is taken into consideration, SU-Tx$_1$ may be selfish and only send partial (or even none) jamming signals to Eve. This kind of SU-Tx is termed as an untrusted jammer. In this paper, it is assumed that SU-Tx$_1$ just has two behaviors: trusted (send jamming signals) or untrusted (does not send jamming signals). We adopt the concept of the trust degree to quantify the trustworthiness of SU-Tx$_1$, which is referred as α, $0 \leq \alpha \leq 1$. When $\alpha = 1$, it means that SU-Tx$_1$ is trusted. While $\alpha = 0$, SU-Tx$_1$ is untrusted. When $1 > \alpha > 0$, SU-Tx$_1$ is partially trusted. The details about how α is initialized and updated are shown in Section VI.

If SU-Tx$_1$ is trusted, it would do its best to send jamming signals, the received signals at PU$_1$, the CBS, and Eve can be expressed as follows

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

$$y_c^1(t) = \mathbf{h}_{p,c}^H(t)\mathbf{w}_p(t)x_p(t) + \mathbf{h}_{j,c}^H(t)\mathbf{w}_j(t)x_j(t) + n_c(t), \quad (2)$$

$$y_e^1(t) = \mathbf{h}_{p,e}^H(t)\mathbf{w}_p(t)x_p(t) + \mathbf{h}_{j,e}^H(t)\mathbf{w}_j(t)x_j(t) + n_e(t), \quad (3)$$

respectively, where $\mathbf{h}_{a,b}$, $a \in \{p, j\}$, $b \in \{p, c, e\}$ are the channel responses from the transmitters (the PBS, SU-Tx$_1$) to the receivers (PU$_1$, the CBS and Eve). And $\mathbf{h}_{ab} = \hat{\mathbf{h}}_{ab}\sqrt{\theta_{a,b}}$ with $\hat{\mathbf{h}}_{ab}$ and $\theta_{a,b}$ denoting the $N_a \times 1$ complex channel vectors and the corresponding path loss of the $a \to b$ channel, respectively. The path loss can be expressed as $10\log_{10}(\theta_{a,b}) = -34.5 - 20\log_{10}(d_{a,b}[\mathrm{m}])$, where $d_{a,b}$ is the distances between transmitters and receivers. $\mathbf{w}_p \in \mathbb{C}^{N_p \times 1}$ and $\mathbf{w}_j \in \mathbb{C}^{N_j \times 1}$ are beamforming vectors of the PBS and SU-Tx$_1$, respectively. x_p is the signals transmitted from the PBS. x_j is the jamming signals transmitted from SU-Tx$_1$, where $x_j \sim \mathcal{N}(0, 1)$. n_b is the additive white Gaussian noise (AWGN) with two-sided power spectral density N_{02}. It is assumed that $n_b \sim \mathcal{N}(0, \delta_b^2)$, where $\delta_b^2 = 2N_{02}B$, and B is the channel bandwidth. All the channels are assumed to be subject to independent Rayleigh fading.

Otherwise, if SU-Tx$_1$ is untrusted, it dose not send jamming signals, then the received signals at PU$_1$, the CBS, and Eve are computed as

$$y_p^0(t) = \mathbf{h}_{p,p}^H(t)\mathbf{w}_p(t)x_p(t) + n_p(t), \quad (4)$$

$$y_c^0(t) = \mathbf{h}_{p,c}^H(t)\mathbf{w}_p(t)x_p(t) + n_c(t), \quad (5)$$

$$y_e^0(t) = \mathbf{h}_{p,e}^H(t)\mathbf{w}_p(t)x_p(t) + n_e(t). \quad (6)$$

The channel responses are closely related to CSI, where the availability of CSI varies in different cases. In certain cases, we assume that the perfect CSI is available. This is due to that the PBS is able to acquire the CSI of the primary channel through pilot sequences [31]. And one of PUs is treated as a potential Eve [32]. In other words, Eve is also a legitimate user of the network whereas its service differs from that of the destination. Since it is legitimate, we can obtain the CSI of Eve. In most cases, however, due to the channel estimation and quantization errors, the CSI may not be obtained perfectly. Specifically, accurate channel information for passive Eve cannot be acquired. Note that the statistical CSI for various channels can be obtained by a number of measurement methods. As a result, we assume that the statistical CSI is available for most cases. The channel vectors of perfect CSI case and statistical case are summarized as follows:

- Perfect CSI case: The instantaneous CSI of $\mathbf{h}_{ab}$ are known, $a \in \{p, j\}$, $b \in \{p, c, e\}$.
- Statistical CSI case: The covariance matrices of $\mathbf{h}_{a,b}$ are known, i.e., $\mathbf{h}_{p,b} \sim \mathcal{CN}(0, \sigma_{p,b}^2\mathbf{e}_{N_p})$, $\mathbf{h}_{j,b} \sim \mathcal{CN}(0, \sigma_{j,b}^2\mathbf{e}_{N_j})$.

In the CCRN, the PBS and the CBS collects the CSI of PUs and the CSI of SUs, respectively. The CBS would share the CSI of SUs with the PBS via a secure channel, such as a common control channel [33]. Then the CSI of PUs and SUs are available at the PBS, so that the transmit beamforming vectors for the PBS ($\mathbf{w}_p$) and the CBS ($\mathbf{w}_j$) are all designed at the PBS. Next, the PBS delivers the related beamforming vector ($\mathbf{w}_j$) to the CBS.

IV. Secrecy Performance Analysis in the Case of Perfect CSI

In this section, we analyze the trust degree's influence on secrecy performance in the case of perfect CSI. We formulate a secrecy rate maximization problem and provide an approximate solution for a trusted jammer. Based on the solution, we obtain the approximate optimized beamforming vectors of the PBS and the jammer.

A. Trusted Jammer

If the jammer is trusted, from (1)-(2), the instantaneous output signal-to-interference-plus-noise ratios (SINRs) at PU_1 and Eve are expressed as follows

$$\zeta_p^{\alpha}(\mathbf{w}_p,\mathbf{w}_j)=\frac{\mathbf{h}_{p,p}^H\mathbf{w}_p\mathbf{w}_p^H\mathbf{h}_{p,p}}{\mathbf{h}_{j,p}^H\mathbf{w}_j\mathbf{w}_j^H\mathbf{h}_{j,p}+\delta_p^2}=\frac{\mathrm{Tr}(\mathbf{W}_p\mathbf{H}_{p,p})}{\mathrm{Tr}(\mathbf{W}_j\mathbf{H}_{j,p})+\delta_p^2}, \quad (7)$$

$$\zeta_e^{\alpha}(\mathbf{w}_p,\mathbf{w}_j)=\frac{\mathbf{h}_{p,e}^H\mathbf{w}_p\mathbf{w}_p^H\mathbf{h}_{p,e}}{\mathbf{h}_{j,e}^H\mathbf{w}_j\mathbf{w}_j^H\mathbf{h}_{j,e}+\delta_e^2}=\frac{\mathrm{Tr}(\mathbf{W}_p\mathbf{H}_{p,e})}{\mathrm{Tr}(\mathbf{W}_j\mathbf{H}_{j,e})+\delta_e^2}, \quad (8)$$

where $\mathbf{w}_a$ is the beamforming vectors of the PBS and the jammer. $\mathbf{W}_a=\mathbf{w}_a\mathbf{w}_a^H$, $\mathbf{H}_{a,p}=\mathbf{h}_{a,p}\mathbf{h}_{a,p}^H$, $\mathbf{H}_{a,e}=\mathbf{h}_{a,e}\mathbf{h}_{a,e}^H$, $a\in\{p,j\}$. According to [34], the achievable instantaneous secrecy rate is the difference between the instantaneous rate of the primary and the eavesdropping channel. Thus, when the jammer is trusted, we can calculate the instantaneous secrecy rate of the primary channel as follows

$$R_{sec}^{\alpha}(\mathbf{w}_p,\mathbf{w}_j) = [\log_2(1+\zeta_p^{\alpha}(\mathbf{w}_p,\mathbf{w}_j))-\log_2(1+\zeta_e^{\alpha}(\mathbf{w}_p,\mathbf{w}_j))]^+. \quad (9)$$

Subsequently, the secrecy rate maximization problem can be mathematically characterized as

$$\mathbf{P1}: \max_{\mathbf{w}_p,\mathbf{w}_j} \quad R_{sec}^{\alpha} \quad (10a)$$

$$\text{s.t.}\zeta_p^{\alpha}\geq\zeta_p^{th}, \quad (10b)$$

$$\mathrm{Tr}(\mathbf{W}_j)\leq P_j^{\max}, \quad (10c)$$

$$\mathrm{Tr}(\mathbf{W}_p)\leq P_p^{\max}, \quad (10d)$$

$$\mathrm{rank}(\mathbf{W}_p)=1, \quad (10e)$$

$$\mathrm{rank}(\mathbf{W}_j)=1, \quad (10f)$$

where ζ_p^{th} is the minimal acceptable SINR of PU_1. $P_p^{\max}$ and $P_j^{\max}$ are the transmit power limits of the PBS and the jammer, respectively. (10e) and (10f) are the rank-one constraints of $\mathbf{W}_p$ and $\mathbf{W}_j$.

As there are fractional forms and logarithmic forms in the objective function of $\mathbf{P1}$, it is a non-convex problem. Such a problem is difficult to solve, therefore, we apply the difference of two-convex functions (D.C.) approximation programming [35], and the objective function in $\mathbf{P1}$ can be rewritten as

$$\max_{\mathbf{w}_p,\mathbf{w}_j} \quad \{f_1(\mathbf{W}_p,\mathbf{W}_j)-f_2(\mathbf{W}_p,\mathbf{W}_j)\}, \quad (11)$$

where

$$f_1(\mathbf{W}_p,\mathbf{W}_j)=\log_2(\mathrm{Tr}(\mathbf{W}_p\mathbf{H}_{p,p})+\mathrm{Tr}(\mathbf{W}_j\mathbf{H}_{j,p})+\delta_p^2) + \log_2(\mathrm{Tr}(\mathbf{W}_j\mathbf{H}_{j,e})+\delta_e^2), \quad (12)$$

$$f_2(\mathbf{W}_p,\mathbf{W}_j)=\log_2(\mathrm{Tr}(\mathbf{W}_p\mathbf{H}_{p,e})+\mathrm{Tr}(\mathbf{W}_j\mathbf{H}_{j,e})+\delta_e^2) + \log_2(\mathrm{Tr}(\mathbf{W}_j\mathbf{H}_{j,p})+\delta_p^2). \quad (13)$$

Function $f_2(\mathbf{W}_p,\mathbf{W}_j)$ is not sensitive to changes in the variables $(\mathbf{W}_p,\mathbf{W}_j)$, so $f_2(\mathbf{W}_p,\mathbf{W}_j)$ is well approximated by its first order approximation. Consequently, we approximate $f_2(\mathbf{W}_p,\mathbf{W}_j)$ by its first-order Taylor series expansion at a feasible solution $(\bar{\mathbf{W}}_p,\bar{\mathbf{W}}_j)$ of (11). Then the objective function (11) can be rewritten as

$$\max_{\mathbf{w}_p,\mathbf{w}_j} \quad \{f_1(\mathbf{W}_p,\mathbf{W}_j)-f_2(\bar{\mathbf{W}}_p,\bar{\mathbf{W}}_j) - \langle\nabla f_2(\bar{\mathbf{W}}_p,\bar{\mathbf{W}}_j),(\mathbf{W}_p,\mathbf{W}_j)-(\bar{\mathbf{W}}_p,\bar{\mathbf{W}}_j)\rangle\}, \quad (14)$$

where $\nabla f_2(\bar{\mathbf{W}}_p,\bar{\mathbf{W}}_j)$ is the gradient of $f_2(\mathbf{W}_p,\mathbf{W}_j)$ at $(\bar{\mathbf{W}}_p,\bar{\mathbf{W}}_j)$, which is given by

$$\nabla f_2(\bar{\mathbf{W}}_p,\bar{\mathbf{W}}_j)=\frac{1}{\ln 2}\left[\frac{\mathbf{H}_{p,e}^H}{\chi_0},\frac{\mathbf{H}_{j,e}^H}{\chi_0}+\frac{\mathbf{H}_{j,p}^H}{\varphi_0}\right]^H, \quad (15)$$

$$\chi_0=\mathrm{Tr}(\bar{\mathbf{W}}_p\mathbf{H}_{p,e})+\mathrm{Tr}(\bar{\mathbf{W}}_j\mathbf{H}_{j,e})+\delta_e^2, \quad (16)$$

$$\varphi_0=\mathrm{Tr}(\bar{\mathbf{W}}_j\mathbf{H}_{j,p})+\delta_p^2. \quad (17)$$

By substituting (14) and (16) into the objective function of **P1** and dropping the rank-one constraints on $\mathbf{W}_p$ and $\mathbf{W}_j$, we can obtain a convex optimization problem **P2** shown below,

$$\mathbf{P2}: \max_{\mathbf{w}_p,\mathbf{w}_j} \left\{f_1(\mathbf{W}_p,\mathbf{W}_j)-f_2(\bar{\mathbf{W}}_p,\bar{\mathbf{W}}_j) - \frac{\mathrm{Tr}\left[\mathbf{H}_{p,e}^H(\mathbf{W}_p-\bar{\mathbf{W}}_p)\right]+\mathbf{H}_{j,e}^H(\mathbf{W}_j-\bar{\mathbf{W}}_j)}{\ln 2\left[\mathrm{Tr}(\bar{\mathbf{W}}_p\mathbf{H}_{p,e})+\mathrm{Tr}(\bar{\mathbf{W}}_j\mathbf{H}_{j,e})+\delta_e^2\right]} - \frac{\mathbf{H}_{j,p}^H(\mathbf{W}_j-\bar{\mathbf{W}}_j)}{\ln 2\left[\mathrm{Tr}(\bar{\mathbf{W}}_j\mathbf{H}_{j,p})+\delta_p^2\right]}\right\} \quad (18a)$$

$$\text{s.t.} \quad \zeta_p^{\alpha}\geq\zeta_p^{th}, \quad (18b)$$

$$\mathrm{Tr}(\mathbf{W}_j)\leq P_j^{\max}, \quad (18c)$$

$$\mathrm{Tr}(\mathbf{W}_p)\leq P_p^{\max}. \quad (18d)$$

To solve **P2**, we propose a DC programming algorithm, as summarized in Algorithm 1. **P2** can be efficiently handled by available convex software, such as CVX [37]. Thus we can obtain the approximate optimal beamforming vectors $\mathbf{w}_p^{\star}$ and $\mathbf{w}_j^{\star}$ of the PBS and the jammer, respectively. When the jammer is trusted, $\mathbf{w}_j^{\star}$ is the approximate beamforming vector that the jammer should use when sending jamming signals to Eve.

Theorem 1: The DC programming algorithm generates a non-decreasing sequence $(\mathbf{W}_p^k,\mathbf{W}_j^k)$ of improved feasible solutions. Initialized from a feasible solution $(\mathbf{W}_p^0,\mathbf{W}_j^0)$, $(\mathbf{W}_p^k,\mathbf{W}_j^k)$ at the k-th iteration is generated as the approximate optimal solution of **P2**.

Proof 1: See Appendix A.

B. Untrusted Jammer

If the jammer is untrusted, from (3)-(4), the instantaneous output SINRs at PU_1 and Eve are expressed as follows

$$\zeta_p^{1-\alpha}(\mathbf{w}_p)=\frac{\mathbf{h}_{p,p}^H\mathbf{w}_p\mathbf{w}_p^H\mathbf{h}_{p,p}}{\delta_p^2}=\frac{\mathrm{Tr}(\mathbf{W}_p\mathbf{H}_{p,p})}{\delta_p^2}, \quad (19)$$

$$\zeta_e^{1-\alpha}(\mathbf{w}_p)=\frac{\mathbf{h}_{p,e}^H\mathbf{w}_p\mathbf{w}_p^H\mathbf{h}_{p,e}}{\delta_e^2}=\frac{\mathrm{Tr}(\mathbf{W}_p\mathbf{H}_{p,e})}{\delta_e^2}. \quad (20)$$

Algorithm 1: DC Programming Algorithm.

Input: $(\mathbf{W}_p^0, \mathbf{W}_j^0)$;
Output: $(\mathbf{w}_p^\star, \mathbf{w}_j^\star)$;
1: Initialize $(\mathbf{W}_p^0, \mathbf{W}_j^0) = (\mathbf{0}_{N_p \times N_p}, \mathbf{0}_{N_j \times N_j})$, the convergence threshold $\sigma > 0$, and $f^0 = 0$;
2: Set $k = 0$;
3: **repeat**
4: Find the optimal solution $(\mathbf{W}_p, \mathbf{W}_j)$ of **P2** with given $\mathbf{W}_p^k$ and $\mathbf{W}_j^k$;
5: Set $k = k + 1$;
6: Compute $(\mathbf{W}_p^k, \mathbf{W}_j^k) = (\mathbf{W}_p, \mathbf{W}_j)$;
7: Update $f^k = f_1(\mathbf{W}_p^k, \mathbf{W}_j^k) - f_2(\mathbf{W}_p^k, \mathbf{W}_j^k)$;
8: **until** $\left| f^k - f^{k-1} \right| \le \sigma$;
9: If $(\mathbf{W}_p^k, \mathbf{W}_j^k)$ are rank-one, then the principal components $(\mathbf{w}_p^\star, \mathbf{w}_j^\star)$ of $(\mathbf{W}_p^k, \mathbf{W}_j^k)$ would be the approximate optimal solution. Otherwise, we would use the randomization method to generate rank-one approximate solutions $(\mathbf{w}_p^\star, \mathbf{w}_j^\star)$ from $(\mathbf{W}_p^k, \mathbf{W}_j^k)$ [36];
10: Return $(\mathbf{w}_p^\star, \mathbf{w}_j^\star)$.

In this paper, it is assumed that the PBS is not aware of SU-Tx$_1$'s behavior. In other word, the PBS does not know whether SU-Tx$_1$ sends jamming signals or not. As a result, the PBS still applies the beamforming vector $\mathbf{w}_p^\star$ obtained from **P1** to transmit messages even when the jammer is untrusted. Then the secrecy rate of the primary channel can be expressed as

$$R_{sec}^{1-\alpha}(\mathbf{w}_p^\star) = [\log_2(1 + \zeta_p^{1-\alpha}(\mathbf{w}_p^\star)) - \log_2(1 + \zeta_e^{1-\alpha}(\mathbf{w}_p^\star))]^+. \quad (21)$$

C. Secrecy Performance

In the case of perfect CSI, we evaluate secrecy performance in terms of the expected secrecy rate. Considering the scenarios where the jammer is trusted and untrusted, the expected secrecy rate can be expressed as

$$\bar{R}_{sec}(\alpha, \mathbf{w}_p^\star, \mathbf{w}_j^\star) = \alpha R_{sec}^{\alpha}(\mathbf{w}_p^\star, \mathbf{w}_j^\star) + (1-\alpha) R_{sec}^{1-\alpha}(\mathbf{w}_p^\star), \quad 1 \ge \alpha \ge 0, \quad (22)$$

where $\mathbf{w}_p^\star$ and $\mathbf{w}_j^\star$ are the approximate optimal beamforming vectors of the PBS and the jammer, respectively. For a given target expected secrecy rate R_{sec}^{th}, the secrecy performance should satisfy that

$$\bar{R}_{sec}(\alpha, \mathbf{w}_p^\star, \mathbf{w}_j^\star) \ge R_{sec}^{th}, \quad (23)$$

then we can calculate a target trust degree threshold α_p^{th} for the perfect CSI case. Therefore, in the case of perfect CSI, we need to select an SU-Tx that satisfies $\alpha \ge \alpha_p^{th}$, and such an SU-Tx would be considered as a trustworthy jammer.

V. Secrecy Performance Analysis in the Case of Statistical CSI

In this section, we focus on the secrecy performance analysis in the case of statistical CSI. As we only know statistical CSI, the beamforming vectors of the PBS and the jammer would be both designed as homogeneous isotropic. In this case, the accurate secrecy rate cannot be calculated. Instead, we calculate the probabilities of the transmission and secrecy outage events for both scenarios: the jammer is trusted and untrusted. On the basis of the probabilities, the secrecy performance is analyzed in terms of effective secrecy throughput.

A. Trusted Jammer

When the jammer is trusted, the received signals at PU$_1$ and Eve are expressed as (1)-(2). Thus the instantaneous output SINRs at PU$_1$ and Eve are calculated as follows

$$\psi_p^\alpha = \frac{P_p \|\mathbf{h}_{p,p}\|^2}{P_j \|\mathbf{h}_{j,p}\|^2 + \delta_p^2} = \frac{\gamma_{p,p}^\alpha}{\gamma_{j,p}^\alpha + 1}, \quad (24)$$

$$\psi_e^\alpha = \frac{P_p \|\mathbf{h}_{p,e}\|^2}{P_j \|\mathbf{h}_{j,e}\|^2 + \delta_e^2} = \frac{\gamma_{p,e}^\alpha}{\gamma_{j,e}^\alpha + 1}, \quad (25)$$

where

$$\gamma_{p,p}^\alpha = \frac{P_p \|\mathbf{h}_{p,p}\|^2}{\delta_p^2}, \gamma_{j,p}^\alpha = \frac{P_j \|\mathbf{h}_{j,p}\|^2}{\delta_p^2}. \quad (26)$$

$P_a = \mathbf{w}_a^H \mathbf{w}_a$ are the transmit powers of the PBS and the jammer. $\gamma_{a,b}^\alpha$ represents the instantaneous signal to noise ratios (SNRs) from node a to node b, for $a \in \{p, j\}$ and $b \in \{p, c, e\}$. $\bar{\gamma}_{a,b}^\alpha$ represents the average SNRs from node a to node b. It is assumed that $\mathbf{h}_{p,b}$ have the covariance matrices $\delta_{p,b}^2 \mathbf{I}_{N_p}$, i.e., $\mathbf{h}_{p,b} \sim \mathcal{CN}(0, \delta_{p,b}^2 \mathbf{I}_{N_p})$. $\mathbf{h}_{j,b}$ have the covariance matrices $\delta_{j,b}^2 \mathbf{I}_{N_j}$ i.e., $\mathbf{h}_{j,b} \sim \mathcal{CN}(0, \delta_{j,b}^2 \mathbf{I}_{N_j})$. Then we can obtain Lemma 1 and Lemma 2 as follows.

Lemma 1: Since $\mathbf{h}_{p,b} \sim \mathcal{CN}(0, \delta_{p,b}^2 \mathbf{I}_{N_p})$, it could be derived that $\gamma_{p,b}^\alpha$ is chi-square distributed variables with the mean $\bar{\gamma}_{p,b}^\alpha = \frac{P_p \delta_{p,b}^2}{\delta_b^2}$ and $2N_p$ degrees of freedom. Hence, we can compute the probability density function of $\gamma_{p,b}^\alpha$ as

$$f_{\gamma_{p,b}^\alpha}(u) = \frac{u^{N_p - 1} \mathrm{e}^{-\frac{u}{\bar{\gamma}_{p,b}^\alpha}}}{\bar{\gamma}_{p,b}^{\alpha\, N_p} (N_p - 1)!}, \quad u \ge 0. \quad (27)$$

Proof 2: See Appendix B.

Lemma 2: Similarly, $\mathbf{h}_{j,b} \sim \mathcal{CN}(0, \delta_{j,b}^2 \mathbf{I}_{N_j})$. It could be derived that $\gamma_{j,b}^\alpha$ is chi-square distributed variables with the mean $\bar{\gamma}_{j,b}^\alpha = \frac{P_j \delta_{j,b}^2}{\delta_b^2}$ and $2N_j$ degrees of freedom. Then the probability density function of $\gamma_{j,b}^\alpha + 1$ can be computed as

$$f_{\gamma_{j,b}^\alpha + 1}(v_1) = \frac{(v_1 - 1)^{N_j - 1} \mathrm{e}^{-\frac{v_1 - 1}{\bar{\gamma}_{j,b}^\alpha}}}{\bar{\gamma}_{j,b}^{\alpha\, N_j} (N_j - 1)!}, \quad v_1 \ge 1. \quad (28)$$

Proof 3: See Appendix C.

On the basis of Lemma 1 and Lemma 2, the probability density function of ψ_b^α can be computed as

$$f_{\psi_b^\alpha}(w) = \int_0^{+\infty} |v_1| f_{\gamma_{j,b}^\alpha+1}(v_1) f_{\gamma_{p,b}^\alpha}(v_1 w) dv_1, \tag{29}$$

which could be expressed as (30) shown at the bottom of the page, where $\bar{\gamma}_{p,b}^\alpha = \frac{P_p \delta_{p,b}^2}{\delta_b^2}$, $\bar{\gamma}_{j,b}^\alpha = \frac{P_j \delta_{j,b}^2}{\delta_b^2}$. In (30), ${}_1F_1(a;b;c)$ is confluent hypergeometric function, which can be given by

$${}_1F_1(a;b;c) = \sum_{n=0}^{+\infty} \frac{(a)^{(n)} z^n}{(b)^{(n)} n!}, \tag{31}$$

where $(a)^{(n)}$ is the rising factorial, defined as

$$(a)^{(n)} = \prod_{k=0}^{n-1} (a+k). \tag{32}$$

To guarantee secrecy performance, we adopt Wyner's encoding scheme with the transmission rate R_p and the secrecy rate R_s [8]. The difference between R_p and R_s is used as a redundancy rate against eavesdropping. Therefore, a PU can decode the received signal with arbitrarily low error rate only if the instantaneous capacity of the PU is larger than the transmission rate, i.e., $\log_2(1+\psi_p^\alpha) > R_p$; Otherwise, a transmission outage event occurs. Besides, secrecy outage may occur when the instantaneous capacity of Eve is larger than the redundance rate, i.e., $R_e = \log_2(1+\psi_e^\alpha) > R_p - R_s$. When the jammer is trusted, the probabilities of the transmission and secrecy outage events are denoted as P_{st}^α and P_{out}^α, respectively. The probabilities can be derived as

$$P_{st}^\alpha = Pr(\psi_p^\alpha > \xi_p) = \int_{\xi_p}^{+\infty} f_{\psi_p^\alpha}(w) dw, \tag{33}$$

$$P_{out}^\alpha = Pr(\psi_e^\alpha > \xi_e) = \int_{\xi_e}^{+\infty} f_{\psi_e^\alpha}(w) dw, \tag{34}$$

where $\xi_p = 2^{R_p} - 1$, $\xi_e = 2^{R_p - R_s} - 1$.

As the probability density function of ψ_b^α is too complex, we cannot provide the close-form expression of the cumulative distribution function of ψ_b^α. But when we know N_p and N_j, we can calculate the probabilities of the transmission (P_{st}^α) and secrecy outage (P_{out}^α) events, respectively.

Thus, when the jammer is trusted, the effective secrecy throughput (EST) can be expressed as

$$T^\alpha = R_s P_{st}^\alpha (1 - P_{out}^\alpha). \tag{35}$$

B. Untrusted Jammer

When the jammer is untrusted, the received signals at PU_1 and Eve are expressed as (3)-(4). Then we can obtain the instantaneous output SINRs at PU_1 and Eve as follows

$$\psi_p^{1-\alpha} = \gamma_{p,p}^\alpha = \frac{P_p \|\mathbf{h}_{p,p}\|^2}{\delta_p^2}, \tag{36}$$

$$\psi_e^{1-\alpha} = \gamma_{p,e}^\alpha = \frac{P_p \|\mathbf{h}_{p,e}\|^2}{\delta_e^2}. \tag{37}$$

According to Lemma 1, $\psi_b^{1-\alpha}$ is chi-square distributed variables with the mean $\bar{\gamma}_{p,b}^\alpha = \frac{P_p \delta_{p,b}^2}{\delta_b^2}$ and $2N_p$ degrees of freedom. Thus we can calculate the probability density function of $\psi_b^{1-\alpha}$ as

$$f_{\psi_b^{1-\alpha}}(u) = f_{\gamma_{p,b}^\alpha}(u) = \frac{u^{N_p-1} e^{-\frac{u}{\bar{\gamma}_{p,b}^\alpha}}}{\bar{\gamma}_{p,b}^{\alpha\, N_p} (N_p-1)!}, \quad u \geq 0. \tag{38}$$

According to (38), we can calculate the cumulative distribution function of $\psi_b^{1-\alpha}$ as

$$\begin{aligned} F_{\psi_b^{1-\alpha}}(u) &= \mathrm{P}(U \leqslant u) = \int_0^u f_{\psi_b^{1-\alpha}}(u) \\ &= \frac{\Gamma(N_p) - \Gamma\left(N_p, \frac{u}{\bar{\gamma}_{p,b}^\alpha}\right)}{(N_p-1)!}. \end{aligned} \tag{39}$$

Similarly, when the jammer is untrusted, the probabilities of the transmission and secrecy outage events are denoted as $P_{st}^{1-\alpha}$ and $P_{out}^{1-\alpha}$, respectively. The probabilities can be derived as

$$\begin{aligned} P_{st}^{1-\alpha} &= Pr(\psi_p^{1-\alpha} > \xi_p) = \int_{\xi_p}^{+\infty} f_{\psi_p^{1-\alpha}}(w) dw \\ &= 1 - F_{\psi_b^{1-\alpha}}(\xi_p), \end{aligned} \tag{40}$$

$$\begin{aligned} P_{out}^{1-\alpha} &= Pr(\psi_e^{1-\alpha} > \xi_e) = \int_{\xi_e}^{+\infty} f_{\psi_e^{1-\alpha}}(w) dw \\ &= 1 - F_{\psi_b^{1-\alpha}}(\xi_e), \end{aligned} \tag{41}$$

where $\xi_p = 2^{R_p} - 1, \xi_e = 2^{R_p - R_s} - 1$. Thus, when the jammer is untrusted, the EST can be expressed as

$$T^{1-\alpha} = R_s P_{st}^{1-\alpha} (1 - P_{out}^{1-\alpha}). \tag{42}$$

C. Secrecy Performance

In the case of statistical CSI, considering both scenarios where the jammer is trusted and untrusted, we can derive the expected

$$\begin{aligned} f_{\psi_b^\alpha}(w) = &\frac{w^{N_p-1} e^{\frac{1}{\bar{\gamma}_{j,b}^\alpha}}}{\bar{\gamma}_{j,b}^{\alpha\, N_j} \bar{\gamma}_{j,b}^{\alpha\, N_p} (N_p-1)!(N_j-1)!} \left[\left(\frac{1}{\bar{\gamma}_{j,b}^\alpha} + \frac{w}{\bar{\gamma}_{p,b}^\alpha} \right)^{-N_j-N_p} \Gamma(N_p+N_j)\, {}_1F_1\left(1-N_j; 1-N_j-Np; -\frac{\bar{\gamma}_{p,b}^\alpha + \bar{\gamma}_{j,b}^\alpha w}{\bar{\gamma}_{j,b}^\alpha \bar{\gamma}_{p,b}^\alpha}\right) \right. \\ &\left. + \frac{\pi[(-1)^{N_j} csc(N_p\pi) - csc((N_p+N_j)\pi)]\Gamma(N_j)\, {}_1F_1\left(1+N_p; 1+N_j+N_p; -\frac{\bar{\gamma}_{p,b}^\alpha + \bar{\gamma}_{j,b}^\alpha w}{\bar{\gamma}_{j,b}^\alpha \bar{\gamma}_{p,b}^\alpha}\right)}{\Gamma(-N_p)\Gamma(1+N_p+N_j)} \right], w > 0 \end{aligned} \tag{30}$$

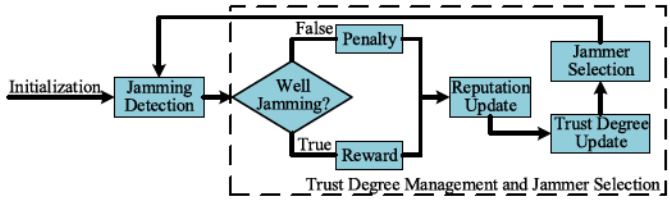

Fig. 2. A trustworthy friendly jammer selection scheme.

EST as

$$\bar{T} = \alpha T^{\alpha} + (1-\alpha)T^{1-\alpha}, \qquad 1 \geq \alpha \geq 0. \tag{43}$$

For a given target effective secrecy throughput T^{th}, the secrecy performance should satisfy that

$$\bar{T} \geq T^{th}, \tag{44}$$

thus we can calculate a target trust threshold α_s^{th} for statistical CSI case. Then we need to select an SU-Tx that satisfies $\alpha \geq \alpha_s^{th}$ in the case of statistical CSI, and such an SU-Tx would be considered as a trustworthy jammer.

VI. The Scheme to Select a Trustworthy Friendly Jammer

According to the secrecy performance analyses, we obtain the target trust degree thresholds α_p^{th} and α_s^{th} for SU-Txs in cases of perfect CSI and statistical CSI, respectively. In this section, as illustrated in Fig. 2, we design a scheme to select an SU-Tx that satisfies $\alpha \geq \alpha_p^{th}(\alpha_s^{th})$ as a trustworthy jammer.

In the scheme, the trust degree list of SU-Txs is defined as $\alpha_i, i = 1, 2, 3...n$. Here α_i is updated by averaging an SU-Tx$_i$'s reputation $r_{i,l}, l = 1, 2, 3...R$, where R is the total jamming detection rounds. In each round, the CBS is in charge of detecting whether the SU-Tx$_i$ sends jamming signals or not. According to positive or negative detection results,[1] we take an incentive mechanism (reward and penalty) to update the reputation $r_{i,l}$. Then on the basis of $r_{i,l}$, we can calculate the trust degree α_i and select a trustworthy SU-Tx. Such a selection scheme consists of three procedures: *Initialization*, *Jamming Detection*, *Trust Degree Management and Jammer Selection*.

A. Initialization

At the beginning, the CBS randomly selects an SU-Tx as a jammer and establishes an initial reputation list $r_i, i = 1, 2, ..., n, r_i \in [0, 1]$ of all SU-Txs. The initial value of the reputation is usually half less than 1. In this paper, it is assumed that: $0.3 \leq r_i \leq 0.5$. This is because a high value may bring malicious behavior, while a low value may lead to unfairness of a newly joined SU-Tx.

B. Jamming Detection

In the jamming phase, the CBS is in charge of detecting whether the selected SU-Tx sends jamming signals or not. In the case of perfect CSI, an energy detection method is employed to detect jamming signals, while in the case of statistical CSI, we use a composite hypothesis testing method.

For both cases, the problem of jamming signals detection can be formulated as a binary hypothesis testing problem with the following hypothesises:

$$\mathcal{H}_0 : y_e(t) = \mathbf{h}_{p,e}^H(t)\mathbf{w}_p(t)x_p(t) + n_e(t), \tag{45}$$

$$\mathcal{H}_1 : y_e(t) = \mathbf{h}_{p,e}^H(t)\mathbf{w}_p(t)x_p(t) + \mathbf{h}_{j,e}^H(t)\mathbf{w}_j(t)x_j(t) + n_e(t), \tag{46}$$

where hypothesis $\mathcal{H}_0$ indicates that jamming signals are absent, and hypothesis $\mathcal{H}_1$ indicates that jamming signals are present.

1) Perfect CSI Case: For the perfect CSI case, we use an energy detection method. Let τ be a continuous value denoting the detecting duration, the test statistic using energy detection is given by

$$Y = \frac{1}{N_{02}} \int_0^{\tau} |y_e(t)|^2 \, dt \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \epsilon, \tag{47}$$

where Y is the decision variable, and ϵ is the decision threshold [38]. We assume that the received power of the PBS and the jammer are fixed at $\hat{P}_p$ and $\hat{P}_j$. Therefore, the received energy of primary signals and jamming signals are $\hat{P}_p\tau$ and $\hat{P}_j\tau$, respectively.

According to [38], for the hypothesis $\mathcal{H}_0$, Y has the non-central chi-square distribution with $2\tau B$ degrees of freedom and non-centrality parameter $\frac{\hat{P}_p\tau}{N_{02}}$. Similarly, for the hypothesis $\mathcal{H}_1$, Y has the non-central chi-square distribution with $2\tau B$ degrees of freedom and non-centrality parameter $\delta = \frac{\hat{P}_p\tau + \hat{P}_j\tau}{N_{02}}$. When $2\tau B$ is large enough, based on the central limit theorem (CLT), Y under two hypothesises can be considered as the following approximations:

$$\begin{cases} Y|\mathcal{H}_0 \sim \mathcal{N}\left(2\tau B + \frac{\hat{P}_p\tau}{N_{02}}, 4\tau B + \frac{4\hat{P}_p\tau}{N_{02}}\right), \\ Y|\mathcal{H}_1 \sim \mathcal{N}\left(2\tau B + \frac{(\hat{P}_p+\hat{P}_j)\tau}{N_{02}}, 4\tau B + \frac{4(\hat{P}_p+\hat{P}_j)\tau}{N_{02}}\right), \end{cases} \tag{48}$$

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

The performance of the detection method can be measured with two probabilities: probability of detection P_D and probability of false alarm P_F. P_D is the probability of detecting jamming signals when they are truly present. P_F is the probability of detecting signals when they actually are absent. According to approximations (48), we can derive expressions of P_D and P_F as follows [39]

$$P_D = \text{prob}(Y > \epsilon|\mathcal{H}_1) = Q\left(\frac{\epsilon - (2B\tau + \frac{(\hat{P}_p+\hat{P}_j)\tau}{N_{02}})}{\sqrt{4B\tau + \frac{4(\hat{P}_p+\hat{P}_j)\tau}{N_{02}}}}\right), \tag{49}$$

$$P_F = \text{prob}(Y > \epsilon|\mathcal{H}_0) = Q\left(\frac{\epsilon - (2B\tau + \frac{\hat{P}_p\tau}{N_{02}})}{\sqrt{4B\tau + \frac{4\hat{P}_p\tau}{N_{02}}}}\right), \tag{50}$$

[2]Here, positive or negative results mean that the SU-Tx sends or does not send jamming signals.

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

$$Q(t) = \frac{1}{\sqrt{2\pi}} \int_t^{+\infty} \exp\left(\frac{-x^2}{2}\right) dx. \tag{51}$$

To obtain the detection threshold, we formulate an optimization problem to maximize the detection probability P_D subject to the target false alarm probability P_F^{th}. According to the *Neyman-Pearson* criterion, such a problem can be expressed as

$$\mathbf{P3}: \max_{\epsilon} \quad P_D \tag{52a}$$

$$\text{s.t.} \quad P_F \leq P_F^{th}. \tag{52b}$$

According to [40], we can solve **P3** when a target false alarm probability P_F^{th} is given. Let $P_F = P_F^{th}$, then the detection threshold can be obtained from (50) as

$$\epsilon^\star = \sqrt{4B\tau + \frac{4\hat{P}_p\tau}{N_{02}} Q^{-1}\left(P_F^{th}\right)} + 2B\tau + \frac{\hat{P}_p\tau}{N_{02}}. \tag{53}$$

Based on the detection threshold $\epsilon^\star$, the CBS can do jamming detection as

$$Y \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \epsilon^\star. \tag{54}$$

2) Statistical CSI Case: For the statistical CSI case, we use a composite hypothesis testing method to detect whether there are jamming signals or not. It is assumed that $\mathbf{y_c} = y_c(t_j), j = 1, 2, ...N$ is the sampling vector of the received signals at the CBS. In the hypothesis $\mathcal{H}_0$, $y_c(t_j) \sim \mathcal{CN}(0, C)$, where $C = P_p\delta_{pc}^2 + \delta_c^2$. While under the hypothesis $\mathcal{H}_1$, $y_c(t_j) \sim \mathcal{CN}(0, C + D)$, where $D = P_j\delta_{jc}^2$. Therefore, the joint probability density function under two hypothesises can be formulated as

$$f(\mathbf{y_c} \mid \mathcal{H}_0) = \left(\frac{1}{\sqrt{2\pi C}}\right)^N \mathrm{e}^{-\sum_{j=1}^{N} \frac{y_c^2(t_j)}{2C}}, \tag{55}$$

$$f(\mathbf{y_c} \mid \mathcal{H}_1) = \left(\frac{1}{\sqrt{2\pi(C+D)}}\right)^N \mathrm{e}^{-\sum_{j=1}^{N} \frac{y_c^2(t_j)}{2(C+D)}}, \tag{56}$$

then we can obtain the likelihood test ratio as follows

$$l(\mathbf{y_c}) = \frac{f(\mathbf{y_c} \mid \mathcal{H}_1)}{f(\mathbf{y_c} \mid \mathcal{H}_0)} = \left(\frac{C}{C+D}\right)^{\frac{N}{2}} \mathrm{e}^{-\sum_{j=1}^{N} \frac{D y_c^2(t_j)}{2C(C+D)}} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} l_0, \tag{57}$$

where l_0 is the testing threshold. Moving to the log domain, we obtain

$$\ln l(\mathbf{y_c}) = \frac{N}{2} \ln \frac{C}{C+D} - \frac{D}{2(C+D)} \sum_{j=1}^{N} \frac{y_c^2(t_j)}{C} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \ln l_0, \tag{58}$$

which can be expressed as

$$\sum_{j=1}^{N} \frac{y_c^2(t_j)}{C} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \frac{N(C+D)}{D} \ln \frac{C}{C+D} - \frac{2(C+D)\ln l_0}{D}. \tag{59}$$

We define that $\widehat{y} = \sum_{j=1}^{N} \frac{y_c^2(t_j)}{C}$, then we can obtain that

$$\widehat{y} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \frac{N(C+D)}{D} \ln \frac{C}{C+D} - \frac{2(C+D)\ln l_0}{D} = \beta. \tag{60}$$

Then the probability density function of $\widehat{y}$ under hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ can be expressed as

$$f(\widehat{y} \mid \mathcal{H}_0) = \frac{\left(\frac{1}{2}\right)^{\frac{N}{2}}}{\Gamma\left(\frac{N}{2}\right)} \widehat{y}^{\frac{N-2}{2}} \mathrm{e}^{\frac{-\widehat{y}}{2}}, \tag{61}$$

$$f(\widehat{y} \mid \mathcal{H}_1) = \frac{C^2}{(C+D)\Gamma\left(\frac{N}{2}\right)} \left(\frac{C^2\widehat{y}}{2(C+D)}\right)^{\frac{N-2}{2}} \mathrm{e}^{-\frac{C^2\widehat{y}}{2(C+D)}}. \tag{62}$$

Therefore, the probability of false alarm P_F and the probability of detection P_D can be calculated as

$$P_F = \mathrm{prob}(\widehat{y} < \beta \mid \mathcal{H}_0) \tag{63}$$

$$= \int_{-\infty}^{\beta} f(\widehat{y} \mid \mathcal{H}_0) d\widehat{y} = \frac{1}{\Gamma\left(\frac{N}{2}\right)} \gamma\left(\frac{N}{2}, \frac{\beta}{2}\right), \tag{64}$$

$$P_D = \mathrm{prob}(\widehat{y} < \beta \mid \mathcal{H}_1) = \int_{-\infty}^{\beta} f(\widehat{y} \mid \mathcal{H}_1) d\widehat{y}. \tag{65}$$

Based on *Neyman-Pearson* criterion, a target false alarm probability P_F^{th} is given. Let $P_F = P_F^{th}$, we can obtain the testing threshold l_0. According to l_0, the CBS could detect whether there are jamming signals as

$$l(\mathbf{y_c}) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} l_0. \tag{66}$$

C. Trust Degree Management and Jammer Selection

In this section, we detail the trust degree management and the jammer selection scheme as illustrated in the dotted box of Fig. 2. According to (54) and (66), we can detect whether there are jamming signals or not ($\mathcal{H}_1$ or $\mathcal{H}_0$) in perfect CSI and statistical CSI case, respectively. Based on the detection results, the CBS takes an incentive mechanism to SU-Tx$_1$. The incentive mechanism consists of reward and penalty, then SU-Tx$_1$'s reputation can be updated as

$$r_{(\text{updated})} = \left[\rho_1 r_{(\text{past})} + \rho_2(-p)^e\right]^+, 0 \leq r_{(\text{updated})} < 1, \tag{67}$$

where $r_{(\text{updated})}$ is the updated reputation of SU-Tx$_1$. $r_{(\text{past})}$ is the historical reputation of SU-Tx$_1$. $e \in \{0, 1\}$ is the current reputation evidence of SU-Tx$_1$ which can determine whether the incentive mechanism is reward or penalty.

- **Reward**: When the detection result shows that there are jamming signals ($\mathcal{H}_1$): $e = 0$, then the value of the reputation is increased by $\rho_2 * 1$;
- **Penalty**: When the detection result shows there is no jamming signals ($\mathcal{H}_0$): $e = 1$, then the value of the reputation is decreased by $\rho_2 * p$.

The value of p is the degree of penalty and it is related to the damage level caused by selfish behavior of a jammer. The basic setting principle of the incentive mechanism is to slow down the

increasing rate and speed up the decreasing rate of the value of reputation.

ρ_1 and ρ_2 are weight factors that satisfy $\rho_1 + \rho_2 = 1$. They can be changed based on the requirement of the CCRN. When the long term of the reputation plays a more important role, we increase ρ_1. Then an SU-Tx needs to maintain good behavior for a longer time to get a higher reputation. Otherwise, when the demand for the sensitivity of reputation collection is higher, we increase ρ_2. Then an SU-Tx's current jamming behavior has a greater influence on the reputation.

At the initial stage of the selection scheme, each SU-Tx has a chance to be selected as a jammer. In a transmission of the PBS, the CBS would do R rounds jamming detection for each SU-Tx. The detection duration of each round is τ. Thus, the reputation evidences are $e_{i,l}$, and the reputations are $r_{i,l}, l = 1, 2, ..., R$. By averaging the reputation $r_{i,l}$ of an SU-Tx, its trust degree can be calculated as

$$\alpha_i = \frac{1}{R}\sum_{l=1}^{R} r_{i,l}, \tag{68}$$

then we can obtain the trust degree list $\alpha_i, i = 1, 2, ...n$. After the trust degree list is updated, we consider a trustworthy jammer selection scheme expressed as follows:

Step 1: Based on the trust degree list α_i, if all trust degrees satisfy that $\alpha_i < \alpha_p^{th}(\alpha_s^{th})$, then there is no SU-Tx that is trustworthy enough to be selected as a jammer. Otherwise, the CBS selects the SU-Tx with the uppermost trust degree as the jammer to protect the next transmission of the PBS. If there are multiple SU-Txs with uppermost trust degree, the CBS would randomly selects one. Then the SU-Tx could be considered as the trustworthy jammer.

Step 2: After the SU-Tx is selected as the jammer, the CBS would keep on updating its reputation and return to Step 1.

By using such a scheme, we could select a trustworthy SU-Tx as a friendly jammer.

VII. Numerical Results

In this section, numerical results are presented to evaluate the secrecy performance of a CCRN for the cases of perfect and statistical CSI. In addition, we present numerical results of different kinds of incentive mechanisms. The simulation parameters are shown in Table I.

TABLE I
Simulation Parameters

Simulation parameter	value
The maximum power of the PBS P_p^{max}(dBm)	30
The maximum power of the jammer P_j^{max}(dBm)	30
The number of antennas of the PBS	4
The number of antennas of the jammer	4
The minimal acceptable SINR of PU_1 ζ_p^{th} (dB)	8
The distances between the PBS to PU_1 and Eve $d_{p,p}(d_{p,e})$ (m)	200
The distance between the jammer to PU_1 $d_{j,p}$ (m)	200
The distance between the jammer to Eve $d_{j,e}$ (m)	100
The tolerance error for **Algorithm** 1 δ	0.001
Noise power spectral density N_{02} (dBm/Hz)	-127
Transmission bandwidth B (MHz)	10

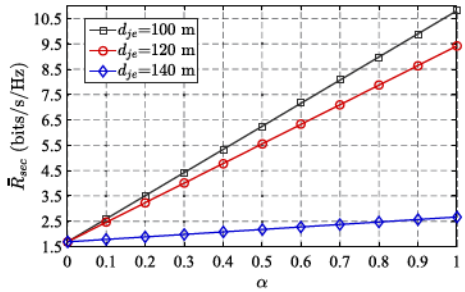

Fig. 3. $\bar{R}_{sec}$ *v.s.* α.

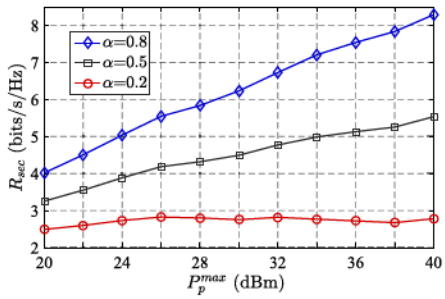

Fig. 4. R_{sec} *v.s.* $P_p^{\max}$.

A. Perfect CSI Case

In this subsection, the expected secrecy rate for perfect CSI case is illustrated. All channels are assumed to be independent Rayleigh fading, and the channel vectors are generated by independent CSCG random variables distributed as $\mathcal{CN}(0, 1)$. The simulation results are obtained by Monte Carlo simulations with 1000 random channel vectors.

Fig. 3 shows the performance comparisons of different distances between the jammer and Eve. Obviously, we can get better secrecy performance when the jammer is closer to Eve, and the trust degree can hardly influence the secrecy performance when the jammer is far away from Eve. The reason is that the jammer has a stronger interference onto Eve when they are closer. When the jammer is far away, it cannot send enough jamming signals to Eve. More interestingly, it is shown that a closer untrusted jammer has a better jamming effect (a higher secrecy rate) than a farther trusted jammer.

In Fig. 4, for the given trust degrees: $\alpha = 0.2$, $\alpha = 0.5$, $\alpha = 0.8$, the expected secrecy rate is plotted regarding to the transmit power of the PBS. We observe that the expected secrecy rate increases with a higher transmit power. This can be explained that the PBS could allocate more power to transmit messages, thus the primary channel rate would be improved. In addition, we can see that as the trust degree increases, higher expected secrecy rates are obtained. While the jammer has a lower level of trust degree, the expected secrecy rate stays the same. This means that the jammer can hardly protect the PBS's transmission with a low trust level.

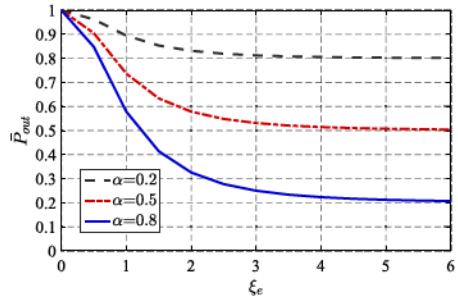

Fig. 5. $\bar{P}_{out}$ *v.s.* ξ_e.

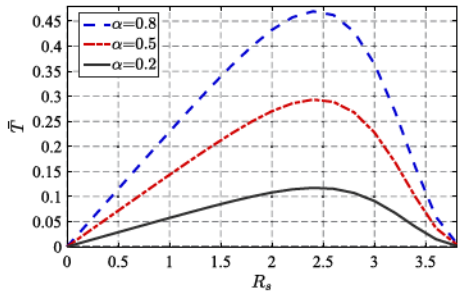

Fig. 6. Effective secrecy throughput.

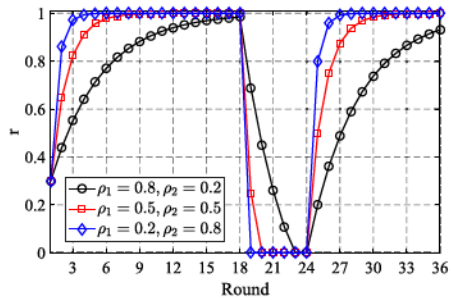

Fig. 7. Reputation at $p = 0.5$.

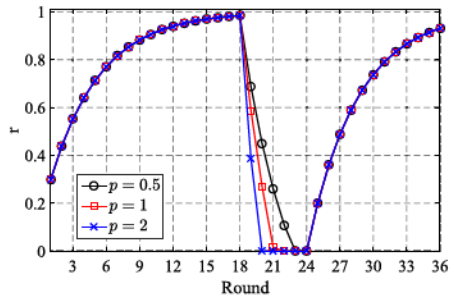

Fig. 8. Reputation at $\rho_1 = 0.8, \rho_2 = 0.2$.

B. Statistical CSI Case

In this subsection, we illustrate the secrecy performance for different trust degrees in the case of statistical CSI. In Fig. 5, the expected secrecy outage probability for three different trust degrees is plotted as a function of ξ_e. In Fig. 5, $\bar{P}_{out} = \alpha P_{out}^{\alpha} + (1-\alpha)P_{out}^{1-\alpha}$, where $P_{out}^{1-\alpha} \approx 1$. Obviously, the expected secrecy outage probability declines as the trust degree increases. Fig. 5 also illustrates that as ξ_e increases, the secrecy outage probability converges to a fixed state. This can be explained that all ψ_e^{α} converges to 0 when ξ_e is large enough.

Fig. 6 depicts the effective secrecy throughput with respect to R_s for different trust degrees, and one can obtain the following observations. Firstly, we can see that for a given trust degree, the effective secrecy throughput goes up and then descends later with regard to R_s. This result shows that there exists a maximum value for each effective secrecy throughput, which means that we can find an optimal R_s to achieve the maximum effective secrecy throughput. Secondly, a higher trust degree improves the effective secrecy throughput. From the second observation, it is shown that a higher trust degree leads to a better secrecy performance. This phenomenon can be explained that the higher the trust degree is, the higher probability the jammer would send jamming signals to Eve.

In Fig. 7 and Fig. 8, we illustrate the reputation update process with different kinds of incentive mechanisms. ρ_1 and ρ_2 are weight factors that satisfy $\rho_1 + \rho_2 = 1$. As shown in (67), ρ_1 is the weight factor of historical behavior of the jammer, and ρ_2 is the weight factor of current jamming behavior of the jammer. As illustrated in Fig. 7, when ρ_1 goes up and ρ_2 goes down, both the rates of increasing and decreasing slow down. In such a situation, the historical reputation plays a more important role while the trust management model is not sensitive to the current behavior of the jammer.

In Fig. 8, it is observed that when p decreases, the rate of increasing stays the same while the rate of decreasing slows down. As the value of p is the degree of penalty and it is related to the damage level caused by selfish behavior of a jammer. When the detection result shows that there are jamming signals: $e = 0$, then the value of the reputation is increased by $\rho_2 * 1$; When the detection result shows there is no jamming signals, $e = 1$, then the value of the reputation is decreased by $\rho_2 * p$. Therefore, a lower value of p means a lower penalty while the reward stays the same.

VIII. Conclusion

In this paper, we design a scheme for trustworthy friendly jammer selection. In this scheme, trust degree is considered as a selection criterion. Firstly, we investigate the trust degree's influence on the secrecy performance in the cases of perfect and statistical CSI, respectively. For both cases, we obtain the target trust degree thresholds based on the target secrecy performance thresholds, respectively. Secondly, we investigate how to calculate the trust degree of each SU-Tx and calculate a trust degree list of SU-Txs. Finally, based on the trust degree list and target trust degree thresholds, we could select a trustworthy SU-Tx as a friendly jammer in the CCRN. Numerical results are presented to validate our secrecy performance analysis and trust degree management. In the future, we are going to investigate how to design a scheme for trustworthy friendly jammer selection in a distributed CCRN.

Appendix A

PROOF OF THEOREM 1

Assuming that $(\bar{\mathbf{W}}_p^i, \bar{\mathbf{W}}_j^i)$ and $(\bar{\mathbf{W}}_p^{i+1}, \bar{\mathbf{W}}_j^{i+1})$ are approximate optimal solutions in **P2** at iteration i and $i+1$, respectively. We obtain $(\bar{\mathbf{W}}_p^{i+1}, \bar{\mathbf{W}}_j^{i+1})$ via **P2**, and it is the approximate optimal solution of (11) at iteration $i+1$, whereas $(\bar{\mathbf{W}}_p^i, \bar{\mathbf{W}}_j^i)$ is a feasible solution of (11) at iteration $i+1$. Therefore, we can get inequations as follows

$$\begin{aligned} & f_1\left(\bar{\mathbf{W}}_p^{i+1}, \bar{\mathbf{W}}_j^{i+1}\right) - f_2\left(\bar{\mathbf{W}}_p^{i+1}, \bar{\mathbf{W}}_j^{i+1}\right) \\ & \approx f_1\left(\bar{\mathbf{W}}_p^{i+1}, \bar{\mathbf{W}}_j^{i+1}\right) - f_2\left(\bar{\mathbf{W}}_{\mathbf{p}}^i, \bar{\mathbf{W}}_j^i\right) - \frac{\mathbf{H}_{jp}^H\left(\bar{\mathbf{W}}_j^{i+1} - \bar{\mathbf{W}}_j^i\right)}{\varphi_0\left(\bar{\mathbf{W}}_j^i\right)\ln 2} \\ & - \frac{\mathrm{Tr}\left[\mathbf{H}_{pe}^H\left(\bar{\mathbf{W}}_p^{i+1} - \bar{\mathbf{W}}_p^i\right) + \mathbf{H}_{je}^H\left(\bar{\mathbf{W}}_j^{i+1} - \bar{\mathbf{W}}_j^i\right)\right]}{\chi_0\left(\bar{\mathbf{W}}_p^i, \bar{\mathbf{W}}_j^i\right)\ln 2} \\ & \geq f_1\left(\bar{\mathbf{W}}_p^i, \bar{\mathbf{W}}_j^i\right) - f_2\left(\bar{\mathbf{W}}_p^i, \bar{\mathbf{W}}_j^i\right), \end{aligned} \tag{69}$$

which yields that the Algorithm 1 produces a non-decreasing sequence with the solution being updated. In other words, $(\bar{\mathbf{W}}_p^i, \bar{\mathbf{W}}_j^i)$ converges to the approximate optimal solution.

APPENDIX B
PROOF OF LEMMA 1

It is assumed that $\mathbf{h}_{p,b} = (h_{p,b1}, h_{p,b2}, ...h_{p,bN_p})$, for $b \in \{p, c, e\}$, where $h_{p,bi} \sim \mathcal{CN}(0, \delta_{p,b}^2)$, $i = 1, 2, ...N_p$, and we can obtain that

$$||\mathbf{h}_{p,b}||^2 = \sum_{i=1}^{N_p} |h_{p,bi}|^2, \tag{70}$$

where $|h_{p,bi}|^2 \sim \exp(\frac{1}{\delta_{p,b}^2})$. Thus, the probability density function of $||\mathbf{h}_{p,b}||^2$ is

$$f_{||\mathbf{h}_{p,b}||^2}(\theta) = \frac{\theta^{N_p-1}}{\delta_{p,b}^{2N_p}(N_p-1)!}\mathrm{e}^{-\frac{\theta}{\delta_{p,b}^2}}, \quad \theta \geq 0. \tag{71}$$

For statement (71), we use mathematical inductions to prove it.

Basis: Show that the statement holds for $N_p = 1$;
$\mathbf{h}_{p,b} = (h_{p,b1})$, $||\mathbf{h}_{p,b}||^2 = |h_{p,b1}|^2 \sim \exp(\frac{1}{\delta_{p,b}^2})$, then

$$f_{||\mathbf{h}_{p,b}||^2}(\theta) = \frac{1}{\delta_{p,b}^2}\mathrm{e}^{-\frac{\theta}{\delta_{p,b}^2}}, \quad \theta \geq 0. \tag{72}$$

The two sides are equal, so the statement holds for $N_p = 1$.

Inductive step: Show that if the statement holds for $N_p = k$, then it also holds for $N_p = k+1$.

$$||\mathbf{h}_{p,b}||_k^2 = \sum_{i=1}^{k} |h_{p,bi}|^2, \tag{73}$$

$$||\mathbf{h}_{p,b}||_{k+1}^2 = \sum_{i=1}^{k} |h_{p,bi}|^2 + |h_{p,b(k+1)}|^2, \tag{74}$$

$$= ||\mathbf{h}_{p,b}||_k^2 + |h_{p,b(k+1)}|^2. \tag{75}$$

Based on the fact that

$$f_{||\mathbf{h}_{p,b}||_k^2}(\theta_1) = \frac{\theta_1^{k-1}}{\delta_{p,b}^{2k}(k-1)!}\mathrm{e}^{-\frac{\theta_1}{\delta_{p,b}^2}}, \quad \theta_1 \geq 0. \tag{76}$$

$$f_{|\mathbf{h}_{p,b(k+1)}|^2}(\theta_2) = \frac{1}{\delta_{p,b}^2}\mathrm{e}^{-\frac{\theta_2}{\delta_{p,b}^2}}, \quad \theta_2 \geq 0, \tag{77}$$

we could obtain

$$\begin{aligned} f_{||\mathbf{h}_{p,b}||_{k+1}^2}(\theta) &= \int_0^\theta f_{||\mathbf{h}_{p,b}||_k^2}(\theta_1) f_{|\mathbf{h}_{p,b(k+1)}|^2}(\theta - \theta_2) d\theta_1 \\ &= \int_0^\theta \frac{\theta_1^{k-1}}{\delta_{p,b}^{2k}(k-1)!}\mathrm{e}^{-\frac{\theta_1}{\delta_{p,b}^2}} \frac{1}{\delta_{p,b}^2}\mathrm{e}^{-\frac{\theta_2}{\delta_{p,b}^2}} d\theta_1 \\ &= \frac{\mathrm{e}^{-\frac{\theta}{\delta_{p,b}^2}}}{\delta_{p,b}^{2(k+1)}(k-1)!}\int_0^\theta \theta_1^{k-1} d\theta_1 \\ &= \frac{\mathrm{e}^{-\frac{\theta}{\delta_{p,b}^2}}}{\delta_{p,b}^{2(k+1)}(k-1)!} \times \frac{\theta^k}{k}\Big|_0^\theta \\ &= \frac{\theta^{[(k+1)-1]}\mathrm{e}^{-\frac{\theta}{\delta_{p,b}^2}}}{\delta_{p,b}^{2(k+1)}((k+1)-1)!}, \quad \theta \geq 0, \end{aligned} \tag{78}$$

thereby showing that $N_p = k+1$ indeeds holds.

Since both the basis and the inductive step have been proved by mathematical inductions, the statement (71) holds for all natural numbers N_p.

Then we can calculate the cumulative distribution function of $||\mathbf{h}_{p,b}||^2$ as follows

$$\begin{aligned} F_{||\mathbf{h}_{p,b}||^2}(\theta) &= \int_0^\theta \frac{\theta^{N_p-1}}{\delta_{p,b}^{2N_p}(N_p-1)!}\mathrm{e}^{-\frac{\theta}{\delta_{p,b}^2}} d\theta \\ &= 1 - \frac{\Gamma(N_p, \frac{\theta}{\delta_{p,b}^2})}{(N_p-1)!}, \end{aligned} \tag{79}$$

where $\Gamma(v, z)$ is incomplete gamma function which could be expressed as

$$\Gamma(v, z) = \int_0^z u^{v-1}\mathrm{e}^{-u} du, \quad (|z| < \infty, \mathrm{Re}(v) > 0). \tag{80}$$

$\gamma_{p,b}^\alpha = \frac{P_p||\mathbf{h}_{p,b}||^2}{\delta_b^2}$, then the cumulative distribution function of $\gamma_{p,b}^\alpha$ is expressed as

$$\begin{aligned} F_{\gamma_{p,b}^\alpha}(u) &= P(U \leq u) = P\left(\frac{P_p\theta}{\delta_b^2} \leq u\right) \\ &= P\left(\theta \leq \frac{u\delta_b^2}{P_p}\right) = 1 - \frac{\Gamma\left(N_p, \frac{u}{\bar{\gamma}_{p,b}^\alpha}\right)}{(N_p-1)!}. \end{aligned} \tag{81}$$

Thus, we can obtain the probability density function of $\gamma_{p,b}^\alpha$ as

$$f_{\gamma_{p,b}^\alpha}(u) = F_{\gamma_{p,b}^\alpha}{}'(u) = \frac{u^{N_p-1}\mathrm{e}^{-\frac{u}{\bar{\gamma}_{p,b}^\alpha}}}{\bar{\gamma}_{p,b}^{\alpha N_p}(N_p-1)!}, \quad u \geq 0. \tag{82}$$

APPENDIX C
PROOF OF LEMMA 2

According to Lemma 1, we derive that the probability density function of $\gamma_{j,p}^{\alpha}$ can be computed as

$$f_{\gamma_{j,p}^{\alpha}}(v) = \frac{v^{N_j-1}\mathrm{e}^{-\frac{v}{\bar{\gamma}_{j,p}^{\alpha}}}}{\bar{\gamma}_{j,p}^{\alpha N_j}(N_j-1)!}, \quad v \geq 0. \tag{83}$$

Obviously, based on (81), the cumulative distribution function of $\gamma_{j,p}^{\alpha}$ can be expressed as

$$F_{\gamma_{j,b}^{\alpha}}(v) = 1 - \frac{\Gamma\left(N_j, \frac{v}{\bar{\gamma}_{j,b}^{\alpha}}\right)}{(N_j-1)!}. \tag{84}$$

It is assumed that $V_1 = V + 1 = \gamma_{j,b}^{\alpha} + 1$.

$$\begin{aligned} F_{\gamma_{j,b}^{\alpha}+1}(v_1) &= P(V_1 \leq v_1) = P(V+1 \leq v_1) \\ &= P(V \leq v_1 - 1) = \frac{\Gamma\left(N_j, \frac{v_1-1}{\bar{\gamma}_{j,b}^{\alpha}}\right)}{(N_j-1)!}. \end{aligned} \tag{85}$$

And thus the probability density function of $\gamma_{j,b}^{\alpha} + 1$ is

$$f_{\gamma_{j,b}^{\alpha}+1}(v_1) = F'_{\gamma_{j,b}^{\alpha}+1}(v_1) = \frac{(v_1-1)^{N_j-1}\mathrm{e}^{-\frac{v_1-1}{\bar{\gamma}_{j,b}^{\alpha}}}}{\bar{\gamma}_{j,b}^{\alpha N_j}(N_j-1)!}, \quad v_1 \geq 1. \tag{86}$$

ACKNOWLEDGMENT

We are very grateful to all reviewers who have helped improve the quality of this paper.

REFERENCES

[1] K. Chopra, R. Bose, and A. Joshi, "Secrecy performance of threshold-based decode-and-forward cooperative cognitive radio network," *IET Commun.*, vol. 11, no. 9, pp. 1396–1406, 2017.

[2] F. Wang and X. Zhang, "Secure resource allocation for polarization-enabled green cooperative cognitive radio networks with untrusted secondary users," in *Proc. 51st Annu. Conf. Inf. Sci. Syst.*, 2017, pp. 1–6.

[3] Y. Jia, Y. Chen, X. Dong, P. Saxena, J. Mao, and Z. Liang, "Man-in-the-browser-cache: Persisting https attacks via browser cache poisoning," *Comput. Secur.*, vol. 55, pp. 62–80, 2015.

[4] F. Lin, Y. Zhou, X. An, I. You, and K.-K. R. Choo, "Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of internet of things devices," *IEEE Consum. Electron. Mag.*, vol. 7, no. 6, pp. 45–50, Nov. 2018.

[5] F. Lin, X. Lü, I. You, and X. Zhou, "A novel utility based resource management scheme in vehicular social edge computing," *IEEE Access*, vol. 6, pp. 66673–66684, 2018.

[6] J. Mao *et al.*, "Detecting malicious behaviors in javascript applications," *IEEE Access*, vol. 6, pp. 12284–12294, 2018.

[7] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 108–114, Apr. 2008.

[8] A. D. Wyner, "The wire-tap channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[9] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 2, pp. 373–387, Feb. 2016.

[10] A. Al-Talabani, Y. Deng, A. Nallanathan, and H. X. Nguyen, "Enhancing secrecy rate in cognitive radio networks via multilevel stackelberg game," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1112–1115, Jun. 2016.

[11] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[12] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surv. Tut.*, vol. 15, no. 1, pp. 428–445, First Quarter 2013.

[13] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 40–47, Feb. 2012.

[14] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, May/Jun. 2013.

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

[16] D. Han, B. Zheng, Z. Chen, and S. Li, "Cost efficiency in coordinated multiple-point system based on multi-source power supply," *IEEE Access*, vol. 6, pp. 71994–72001, 2018.

[17] V.-D. Nguyen, T. Q. Duong, O. A. Dobre, and O.-S. Shin, "Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 11, pp. 2609–2623, Nov. 2016.

[18] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 148–153, Feb. 2018.

[19] X. Wang, Y. Ji, H. Zhou, and J. Li, "Auction-based frameworks for secure communications in static and dynamic cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2658–2673, Mar. 2017.

[20] Q. Gao *et al.*, "Joint design of jammer selection and beamforming for securing MIMO cooperative cognitive radio networks," *IET Commun.*, vol. 11, no. 8, pp. 1264–1274, 2017.

[21] Z. Li, T. Jing, Y. Huo, and J. Qian, "Achieving secure communications in multi-antenna cooperative cognitive radio networks using cooperative jamming," *Int. J. Sensor Netw.*, vol. 22, no. 2, pp. 100–110, 2016.

[22] J. Y. Ryu, J. Lee, and T. Q. Quek, "Confidential cooperative communication with trust degree of potential eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3823–3836, Jun. 2016.

[23] M. Zhang, X. Chen, and J. Zhang, "Social-aware relay selection for cooperative networking: An optimal stopping approach," in *Proc. IEEE Int. Conf. Commun.*, 2014, pp. 2257–2262.

[24] J. Mao, W. Tian, J. Jiang, Z. He, Z. Zhou, and J. Liu, "Understanding structure-based social network de-anonymization techniques via empirical analysis," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 279, 2018.

[25] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.

[26] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[27] G. Luo, J. Li, Z. Liu, X. Tao, and F. Yang, "Physical layer security with untrusted relays in wireless cooperative networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2017, pp. 1–6.

[28] L. Wang, H. Wu, and G. L. Stüber, "Cooperative jamming-aided secrecy enhancement in P2P communications with social interaction constraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1144–1158, Feb. 2017.

[29] L. Wang and H. Wu, "Jamming partner selection for maximising the worst D2D secrecy rate based on social trust," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 2, p. e2992, 2017.

[30] Z. Li, T. Jing, L. Ma, Y. Huo, and J. Qian, "Worst-case cooperative jamming for secure communications in CIoT networks," *Sensors*, vol. 16, no. 3, p. 339, 2016.

[31] F. Gao, R. Zhang, Y.-C. Liang, and X. Wang, "Optimal design of learning based MIMO cognitive radio systems," in *Proc. IEEE Int. Symp. Inf. Theory*, 2009, pp. 2537–2541.

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

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

[34] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, 2006, pp. 356–360.

[35] H. H. Kha, H. D. Tuan, and H. H. Nguyen, "Fast global optimal power allocation in wireless networks by local DC programming," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 510–515, Feb. 2012.

[36] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semi-definite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
[37] M. Grant, S. Boyd, M. Grant, and S. Boyd, "CVX: Matlab software for disciplined convex programming," in *Recent Advances in Learning and Control*. New York, NY, USA: Springer-Verlag, pp. 95–110.
[38] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.
[39] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 4–17, Feb. 2008.
[40] H. V. Poor, *An Introduction to Signal Detection and Estimation*. New York, NY, USA: Springer-Verlag, 2013.

Yingkun Wen received the B.S. degree from North China Electric Power University, Baoding, China, in 2015. He is currently working toward the Ph.D. degree with the School of Electronic and Infomation Engineering, Beijing Jiaotong University, Beijing, China. His current research interests include cognitive radio networks, physical layer security, and cooperative communication.

Yan Huo received the B.E. and Ph.D. degrees in communication and information system from Beijing Jiaotong University, Beijing, China, in 2004 and 2009, respectively. He has been a faculty member with the School of Electronics and Information Engineering at Beijing Jiaotong University since 2011, where he is currently a Professor. His current research interests include wireless communication theory, Internet of Things, security and privacy, and cognitive radio and signal processing.

Liran Ma received the D.Sc. degree in computer science from George Washington University, Washington DC, USA. He is currently an Associate Professor with the Department of Computer Science at Texas Christian University, Fort Worth, TX, USA. His current research focuses on wireless, mobile, and embedded systems, including security and privacy, smart phones, smart health, mobile computing, data analytics, Internet of Things, and cloud computing. It involves building and simulating prototype systems and conducting real experiments and measurements.

Tao Jing received the M.S. and Ph.D. degrees from the Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun, China, in 1994 and 1999, respectively. He is currently a Professor with the School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China. His current research interests include capacity analysis, spectrum prediction and resource management in cognitive radio networks, RFID in intelligent transporting system, and smart phone application.

Qinghe Gao received the B.E. degree in communication engineering from North China Electric Power University (Baoding), China, in 2013. She is currently working toward the Ph.D. degree in communication and information system with Beijing Jiaotong University, Beijing, China. She was a Visiting Scholar with the Department of Computer Science, George Washington University, Washington DC, USA, from 2015 to 2017. Her research interests include cognitive radio networks, physical layer security, and energy harvesting.