Received 8 July 2021; revised 18 August 2021; accepted 14 September 2021. Date of publication 21 September 2021; date of current version 29 September 2021.

Digital Object Identifier 10.1109/OJCOMS.2021.3114382

Attacking Massive MIMO Cognitive Radio Networks by Optimized Jamming

S. FATEMEH ZAMANIAN[1], MOHAMMAD HOSSEIN KAHAEI[1], S. MOHAMMAD RAZAVIZADEH[1] (Senior Member, IEEE), AND TOMMY SVENSSON[2] (Senior Member, IEEE)

[1]School of Electrical Engineering, Iran University of Science and Technology, Tehran 1684613114, Iran

[2]Department of Electrical Engineering, Chalmers University of Technology, 41296 Gothenburg, Sweden

CORRESPONDING AUTHOR: S. M. RAZAVIZADEH (e-mail: smrazavi@iust.ac.ir)

ABSTRACT Massive multiple-input multiple-output (MaMIMO) and cognitive radio networks (CRNs) are two promising technologies for improving spectral efficiency of next-generation wireless communication networks. In this paper, we investigate the problem of physical layer security in the networks that jointly use both technologies, named MaMIMO-CRN. Specifically, to investigate the vulnerability of this network, we design an optimized attacking scenario to MaMIMO-CRNs by a jammer. For having the most adversary effect on the uplink transmission of the legitimate MaMIMO-CRN, we propose an efficient method for power allocation of the jammer. The legitimate network consists of a training and a data transmission phase, and both of these phases are attacked by the jammer using an optimized power split between them. The resulting power allocation problem is non-convex. We thus propose three different efficient methods for solving this problem, and we show that under some assumptions, a closed-form solution can also be obtained. Our results show the vulnerability of the MaMIMO-CRN to an optimized jammer. It is also shown that increasing the number of antennas at the legitimate network does not improve the security of the network.

INDEX TERMS Massive MIMO, cognitive radio network, physical layer security, jamming, optimization, power allocation, spectral efficiency.

I. INTRODUCTION

IN RECENT years, the increasing demands for bandwidth and also inefficient usage of the frequency spectrum have caused a severe shortage of this communication resource. Cognitive radio networks (CRN) and massive multiple-input multiple-output (MaMIMO) systems are two efficient solutions to this problem [1]–[3]. The main goal of the CRN is to efficiently utilize the scarce spectrum by sharing the spectrum between different networks or by opportunistically using the unused frequency bands [1]. On the other hand, in the MaMIMO systems, by using a large number of antennas at the base stations (BSs), very high spectral efficiency is achievable with low complexity transmitters and receivers [3]. The combination of these two techniques; which we refer to as MaMIMO-CRN; can boost these gains and is considered as an efficient method for substantial improvement in the wireless network performance in terms of sum rate and spectral efficiency [4]–[10].

In [4], authors showed that the achievable sum rate of the CRN increases if both primary and secondary BSs have a large number of antennas. In addition, it is shown that increasing the number of antenna at the secondary system has the advantage of reducing the channel estimation error and improving spectrum sensing procedure [5]. Three problems of resource allocation, interference mitigation, and user selection in underlay MaMIMO-CRNs were studied in [6]. Authors in [7] proposed an orthogonal pilot sharing scheme at the training phase and formulated a power allocation problem in a MaMIMO-CRN that provides the maximum downlink sum rate in the secondary system. In [8], selecting the maximum number of secondary users and satisfying the required quality of service in a MaMIMO-CRN

were investigated and a joint power allocation and secondary user selection algorithm was proposed. Authors in [9] proposed a fair energy-efficient optimization problem in MaMIMO-CRN. In [10], a power allocation problem for pilot and data transmission phases with an energy efficiency guarantee in the uplink of the MaMIMO-CRNs was investigated. Moreover, a conventional method for combating these attacks is using encryption techniques that are related to upper layers of the networks. However, physical layer attacks can be efficiently mitigated by techniques performed at that layer which are known as physical layer security techniques [11]–[12]. Physical layer security has been widely studied in the context of massive MIMO systems as well as CRNs. Authors in [13] showed that MaMIMO systems are secure against passive attacks but vulnerable against active attacks. For example, if an active attacker attacks the training phase of a MaMIMO network, it can produce a pilot contamination effect that makes the channel estimation erroneous [14]. Furthermore, in [15], authors studied the effect of eavesdropping in a multi-user MaMIMO system, where there is one active eavesdropper per user. They assumed that each eavesdropper obtains the pilot used by one user and re-transmits it to disrupt the network quality. Then, they proposed an uplink data aided double channel training scheme, which can accurately detect the presence of an attacker and estimate the legitimate channels. Moreover, authors in [16] studied physical layer security in the presence of a full-duplex active eavesdropper that uses jamming attacks to improve its eavesdropping mode. Also, some issues around the jamming attack such as jamming detection as well as designing jamming resistant receivers were studied in [17]–[19]. It has been shown in the literature that a smart jammer that has some pieces of information about the MaMIMO network and accordingly uses them to optimize its attack, can disrupt the performance of the legitimate network considerably.

For instance, a worst-case smart jamming attack over MIMO Gaussian channels was proposed in [20]. On the other hand, in the CRNs, the problem of physical layer security has been studied from two different aspects [21]. Spectrum sensing data falsification and primary user emulation are some known attacks that destroy the spectrum sensing phase [22]–[23]. On the other hand, jamming and eavesdropping are the attacks that are performed at the cognitive communications phase [24]–[25]. Despite many papers published on the physical layer security of the MaMIMO and CRN networks, related to MaMIMO-CRN the number of papers is very limited. For example, in [26], providing secure transmissions in the MaMIMO-CRNs against a passive multi-antenna eavesdropper with a pilot contamination attack was studied. Likewise, intercepting the confidential downlink transmissions of the MaMIMO-CRNs in the presence of an active eavesdropper was investigated in [27]. Moreover, in [28], a smart jamming attack on the uplink transmission of the MaMIMO-CRN was designed to destruct the performance of the secondary system.

In this paper, we investigate the maximum degradation that a jammer can have on MaMIMO-CRNs. In fact, we design and evaluate the most destructive strategy that a smart jammer may adopt to attack a MaMIMO-CRN in order to minimize spectral efficiency. In this scenario, the jammer optimizes its transmission parameters to have the worst adversary effect on the legitimate network. Particularly, it optimally allocates its power between the training and data transmission phases of the legitimate MaMIMO-CRN network to minimize the spectral efficiency of the primary network. This is an important problem and can be considered as the prerequisite step for developing countermeasure algorithms that are then designed and used to protect the MaMIMO-CRNs from illegal and destructive attacks.

We formulate the aforementioned power allocation problem as a non-convex $min - max$ optimization problem. To solve this problem, we propose three different solution methods. In the first method, we present a geometric programming based solution. The second method presents a closed-form solution for the problem which can be obtained under specific realizations of the channel matrices. In the third method, we utilize an epigraph form of the objective function and certain transformations of the constraint functions to solve the problem. In addition, to illustrate and compare the performance of the proposed solution methods, our analytical and simulation results also show that a jammer with optimized power allocation can efficiently degrade the spectral efficiency of the MaMIMO-CRNs. In this case, even increasing the number of antennas at the base stations cannot improve the performance of the legitimate network. The aim of this study is to help network designers to develop efficient countermeasure techniques to secure MaMIMO-CRNs against jamming attacks.

The remainder of this paper is as follows. In Section II, we introduce the system model. Problem formulation for the jammer power allocation and the proposed solutions to the optimization problem are given in the Sections III and IV, respectively. Section V is devoted to the jammer optimization in the presence of primary system optimal power. Numerical results and conclusions are expressed in Section VI and Section VII, respectively.

II. SYSTEM MODEL

As illustrated in Fig. 1, we consider the uplink transmission of a TDD multi-user MaMIMO-CRN using underlay spectrum sharing. The network consists of a primary and a secondary system. The primary system consists of K legitimate single antenna users and a primary base station (PBS) equipped with $N_p \gg 1$ antennas. Also, the secondary system consists of M legitimate single antenna users and a secondary base station (SBS) with $N_s \gg 1$ antennas. We denote the ratio between N_p and N_s by κ. There is also a jammer in the area whose target is to destroy the communication of the primary system. We denote the coherence time of the channel by T in which the first η symbols are used for transmitting η-tuple ($K + M \leq \eta \leq T$) mutual orthogonal pilot

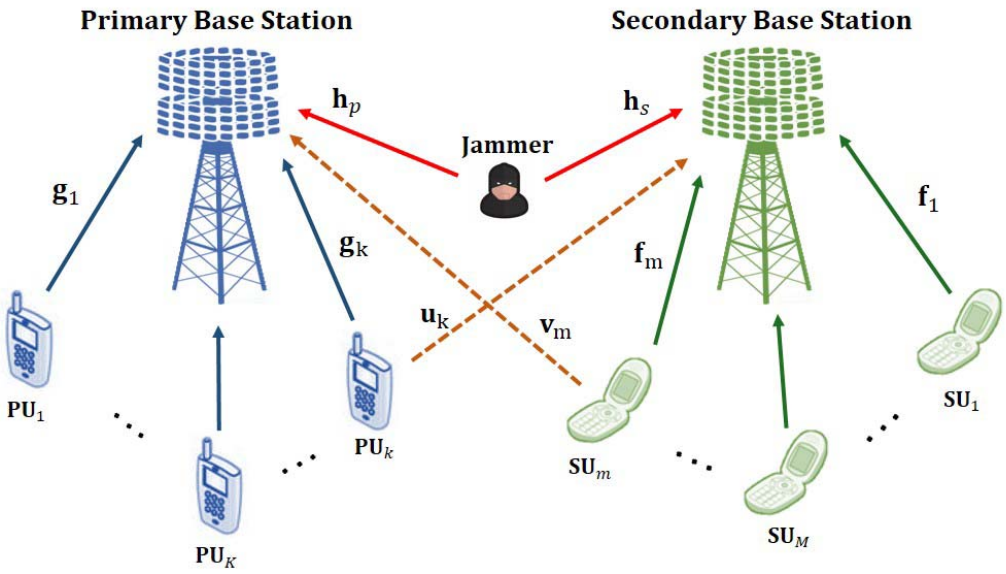

FIGURE 1. An MaMIMO-CRN consisting of a primary and a secondary system and a jammer that attacks the network.

sequences to estimate the channels and the rest of T is used to transmit uplink data symbols.

At the beginning of each coherence interval, each legitimate user transmits its assigned pilot. At the same time, the jammer transmits its signal which is a combination of the pilots in the training phase. Next, in the data transmission phase, the jammer sends a noise-like signal simultaneously with the users that send their data signals. For this goal, the jammer needs some information including the transmission protocol (i.e., the timing of transmission) and the pilot set. We assume that before attacking the legitimate system, this information is provided to the jammer or the optimized (smart) jammer by itself acquiring this information during some coherence time before starting to attack the network [17].

Furthermore, $\mathbf{g}_k$ denotes the channel between the kth primary user and the PBS, i.e., the kth column of the channel matrix between the primary users and the PBS. We denote this matrix by $\mathbf{G} = \mathbf{H}_G \mathbf{D}_G{}^{1/2}$ in which $\mathbf{H}_G \in \mathbb{C}^{N_p \times K}$ models small scale fading of the primary channel with i.i.d elements distributed as $\mathcal{CN} \sim (0, 1)$. In addition, β_{g_k} is the kth diagonal element of the diagonal matrix $\mathbf{D}_G \in \mathbb{R}^{K \times K}$ that models the path loss and shadowing effect between the kth primary user and the PBS. Also, $\mathbf{f}_m$ denotes the channel between the mth secondary user and the SBS, i.e., the mth column of the channel matrix between the secondary users and the SBS. We denote this matrix by $\mathbf{F} = \mathbf{H}_F \mathbf{D}_F{}^{1/2}$ in which $\mathbf{H}_F \in \mathbb{C}^{N_s \times M}$ models the small scale fading of the secondary channel with i.i.d elements distributed as $\mathcal{CN} \sim (0, 1)$. Likewise, β_{f_m} is the mth diagonal element of the diagonal matrix $\mathbf{D}_F \in \mathbb{R}^{M \times M}$ that models the path loss and shadowing effect between the mth secondary user and the SBS. Also, $\mathbf{h}_p$ and $\mathbf{h}_s$ are the channel vectors between the single antenna jammer and the PBS and the SBS, respectively. In addition, β_{h_p} and β_{h_s} model the path loss and shadowing effect between the jammer and PBS and SBS, respectively. Furthermore, $\mathbf{v_m}$ is the mth column of $\mathbf{V} \in \mathbb{C}^{N_p \times M}$ that denotes the channel vector between the mth secondary user and the PBS where β_{v_m} models the path loss and shadowing effect of it , and $\mathbf{u_k}$ is the kth column of $\mathbf{U} \in \mathbb{C}^{N_s \times K}$ that denotes the channel vector between the kth primary user and the SBS where β_{u_k} models the path loss and shadowing effect of this channel.

To formulate the destructive power allocation problem, we consider the case that the jammer uses all information that it obtained from the jamming phase.

III. PROBLEM FORMULATION AND ASYMPTOTIC SPECTRAL EFFICIENCY

In this section, we formulate the primary spectral efficiency minimization problem, targeted by the jammer, and also analyze its asymptotic behavior. For this purpose, we consider two phases of transmission, namely pilot transmission phase and data transmission phase.

A. TRAINING (PILOT TRANSMISSION) PHASE

As we mentioned before, in order to increase the impact of jamming on the primary system, we assume that the jammer knows the set of pilot sequences of the primary system and the transmission protocol. It should be noted that the jammer has no information about the specific pilot sequence that is assigned to each primary user at any time slot. The jammer adopts a pilot contamination attack strategy, and to this end sends a linear combination of the primary's pilot sequences in the training phase.

The pilot sequences of the primary and secondary systems are denoted by two matrices of $\Phi_p \in \mathbb{C}^{\eta \times K}$ and $\Phi_s \in \mathbb{C}^{\eta \times M}$, respectively. The kth column of Φ_p, $\boldsymbol{\phi}_{\mathbf{p_k}}$, denotes the kth primary user's pilot sequence and the mth column of Φ_s, $\boldsymbol{\phi}_{\mathbf{s_m}}$, denotes the mth secondary user's pilot sequence.

The received signal at the PBS is

$$\mathbf{Y}_t^p = \sqrt{\eta p_p}\mathbf{G}\Phi_p^T + \sqrt{\eta p_s}\mathbf{V}\Phi_s^T + \sqrt{p_j}\mathbf{h}_p\boldsymbol{\phi}_\mathbf{j}^T + \mathbf{N}, \quad (1)$$

where p_p, p_s and p_j are the average transmission powers of each primary user, secondary user and the jammer during the training phase, respectively. The matrix $\mathbf{N} \in \mathbb{C}^{N_p \times K}$ is a circularly-symmetric complex Gaussian receiver noise matrix at the PBS with i.i.d. $\mathcal{CN} \sim (0, 1)$ elements, and $\boldsymbol{\phi}_\mathbf{j} = \sum_{k=1}^{\eta} \boldsymbol{\phi}_{\mathbf{p_k}}$ is the jammer's pilot sequence.

Since $(K+M \leq \eta \leq T)$, the MaMIMO-CRN can allocate mutual orthogonal pilot sequences to $K+M$ primary and secondary users. Therefore, in the MaMIMO-CRN the primary system is effectively protected from the secondary system in the training phase, i.e., $\boldsymbol{\phi}_\mathbf{p}{}^\mathbf{H}\boldsymbol{\phi}_\mathbf{p} = \mathbf{I_K}$, $\boldsymbol{\phi}_\mathbf{s}{}^\mathbf{H}\boldsymbol{\phi}_\mathbf{s} = \mathbf{I_M}$, $\boldsymbol{\phi}_\mathbf{p}{}^\mathbf{H}\boldsymbol{\phi}_\mathbf{s} = \mathbf{0}$. Thus, by using mutual orthogonal pilot sequences and minimum mean square error (MMSE) estimation [29], the estimation of $\mathbf{g}_k$ denoted by $\hat{\mathbf{g}}_k$ is obtained as

$$\begin{aligned}\widehat{\mathbf{g}}_k &= \frac{1}{\sqrt{\eta p_p}}\mathbf{Y}_t^p\boldsymbol{\phi}_{\mathbf{p_k}}^*\mathcal{B} \\ &= \left(\mathbf{g}_k + \sqrt{\frac{p_j}{\eta p_p}}\mathbf{h}_p + \sqrt{\frac{1}{\eta p_p}}\mathbf{N}\boldsymbol{\phi}_{\mathbf{p_k}}^*\right)\mathcal{B}, \end{aligned} \quad (2)$$

where

$$\mathcal{B} = \frac{\eta p_p \beta_{g_k}}{\eta p_p \beta_{g_k} + p_j \beta_{h_p} + 1}. \quad (3)$$

The variance of $\hat{\mathbf{g}}_k$ is equal to

$$C_{\hat{\mathbf{g}}_k} = E\left\{\hat{\mathbf{g}}_k\hat{\mathbf{g}}_k^H\right\} = \sigma_{\hat{g}_k}^2\mathbf{I}_{N_p}, \quad (4)$$

where $\sigma_{\hat{g}_k}^2 = \frac{\eta p_p \beta_{g_k}^2}{\eta p_p \beta_{g_k} + p_j \beta_{h_p} + 1}$.

It should be noted that, due to $K < \eta$, PBS can use pilot(s) utilized only by jammer to estimate the jammer's channel and obtain $p_j\beta_{h_p}$ [17]. After that, by using the pilot utilized by each user and the information about $p_j\beta_{h_p}$, each user's channel and $p_p\beta_{g_k}$ can be estimated. Then, by using the closed-form solution of the MMSE estimator, $\hat{g}_k$ is estimated as Eq. (2) and consequently, $\sigma_{\hat{g}_k}^2$ is obtained from (4).

B. DATA TRANSMISSION PHASE

In this phase, the jammer sends its adversary signal at the same time slot as the users send their data to the BSs. Let $\mathbf{y}_d^p$ be the $N_p \times 1$ received vector at the PBS defined as

$$\mathbf{y}_d^p = \sqrt{q_p}\mathbf{G}\mathbf{x} + \sqrt{q_s}\mathbf{V}\mathbf{z} + \sqrt{q_j}\mathbf{h}_p s + \mathbf{n}, \quad (5)$$

where q_p, q_s and q_j are the average transmission powers of each primary user, each secondary user and the jammer during data transmission phase, respectively. Moreover, $\mathbf{x} \in \mathbb{C}^{K\times 1}$ and $\mathbf{z} \in \mathbb{C}^{M\times 1}$ denote the normalized symbol vectors transmitted by the primary and secondary users, respectively where $E\{\mathbf{x}\mathbf{x}^\mathbf{H}\} = \mathbf{I_K}$ and $E\{\mathbf{z}\mathbf{z}^\mathbf{H}\} = \mathbf{I_M}$. Furthermore, s denotes the normalized random symbol of the jammer where $E\{|s|^2\} = 1$. Also, the PBS receiver noise $\mathbf{n}$ follows a zero mean circularly-symmetric complex Gaussian distribution. Then, the received signal at the PBS is decoded as

$$\mathbf{y}_{d_p} = \mathbf{A}^H\mathbf{y}_d^p, \quad (6)$$

where $\mathbf{A} \in \mathbb{C}^{N_p\times K}$ denotes the linear detection matrix at the PBS which depends on the primary estimated channel. The kth element of $\mathbf{y}_{d_p}$ becomes

$$\begin{aligned} y_{d_p}^k = \sqrt{q_p}\mathbf{a}_k^H\mathbf{g}_k x_k + \sum_{i=1, i\neq k}^{K}\sqrt{q_p}\mathbf{a}_k^H\mathbf{g}_i x_i \\ + \sum_{m=1}^{M}\sqrt{q_s}\mathbf{a}_k^H\mathbf{v}_m z_m + \sqrt{q_j}\mathbf{a}_k^H\mathbf{h}_p s + \mathbf{a}_k^H\mathbf{n}, \end{aligned} \quad (7)$$

where $\mathbf{a}_k$ is the kth column of $\mathbf{A}$. The first term in (7) is the desired signal which is independent of the other terms. In order to find a closed-form solution for spectral efficiency of the kth primary user, we use the lower band for the spectral efficiency as follows [30]

$$\mathcal{R}_p^k \geq \mathcal{S}_p^k \triangleq \left(1 - \frac{\eta}{T}\right)\log_2\left(1 + \overline{SINR_p^k}\right). \quad (8)$$

By using the maximum ratio combining (MRC) detector at both the primary and secondary base stations, where the detector matrix $\mathbf{A}$ is equal to matrix $\widehat{\mathbf{G}}$ which is estimated in the training phase, the $\overline{SINR}$ of the kth primary user is obtained as in (9), as shown at the bottom of this page. By assuming that all channels are independent with Normal distributions and using some algebra, as stated in Appendix A, the sum spectral efficiency of the primary system can be written as (10), shown at the bottom of this page.

From the previous discussions, we have the following result.

Corollary 1: When the number of antennas at the PBS, N_p, in (10) goes to infinity, the performance of the primary

$$\overline{SINR_p^k} = \frac{q_p.\left|E\left\{\hat{\mathbf{g}}_k^H\mathbf{g}_k\right\}\right|^2}{q_p\sum_{i=1}^{K}E\left\{\left|\hat{\mathbf{g}}_k^H\mathbf{g}_i\right|^2\right\} - q_p\left|E\left\{\hat{\mathbf{g}}_k^H\mathbf{g}_k\right\}\right|^2 + q_s\sum_{m=1}^{M}E\left\{\left|\hat{\mathbf{g}}_k^H\mathbf{v}_m\right|^2\right\} + q_jE\left\{\left|\hat{\mathbf{g}}_k^H\mathbf{h}_p\right|^2\right\} + E\left\{\left\|\hat{\mathbf{g}}_k^H\right\|^2\right\}} \quad (9)$$

$$\mathcal{S} = \sum_{k=1}^{K}\left(1 - \frac{\eta}{T}\right)\log_2\left(1 + \frac{N_p\beta_{g_k}^2}{\left(\beta_{g_k} + \frac{p_j\beta_{h_p}}{\eta p_p} + \frac{1}{\eta p_p}\right)\left(\sum_{i=1}^{K}\beta_{g_i} + \frac{1}{q_p} + \frac{q_s}{q_p}\sum_{m=1}^{M}\beta_{v_m}\right) + \beta_{g_k}^2 + \frac{q_j}{q_p}\left(\beta_{h_p}\beta_{g_k} + \frac{p_j}{\eta p_p}(N_p+2)\beta_{h_p}^2 + \frac{\beta_{h_p}}{\eta p_p}\right)}\right) \quad (10)$$

system is saturated due to the pilot contamination effect that is produced by the jammer. This result can be expressed as

$$\mathcal{S} \to_{N_p \to \infty} \sum_{k=1}^{K} \left(1 - \frac{\eta}{T}\right) \log_2 \left(1 + \eta \frac{p_p}{p_j} \frac{q_p}{q_j} \left(\frac{\beta_{g_k}}{\beta_{h_p}}\right)^2\right). \quad (11)$$

This result shows that the MaMIMO-CRN is vulnerable to a jammer that attacks the pilot phase. It is also observed that increasing the number of antennas will not improve the spectral efficiency performance.

To illustrate destructive effect of the jamming attack on the performance of the MaMIMO-CRN, we propose an optimal power allocation mechanism by the jammer.

IV. OPTIMAL POWER ALLOCATION

In order to design the optimal jammer that has the highest destruction on the performance of the primary system in the training and data transmission phases, the jammer should optimally divide its power budget between the training and data transmission phases. To do so, the jammer solves a power optimization problem to minimize the maximum sum spectral efficiency of the primary system as follows. By defining

$$\begin{aligned}
a_k &= N_p \beta_{g_k}^2, \\
b_k &= \beta_{g_k}^2 + \left(\sum_{i=1}^{K} \beta_{g_i} + \frac{1}{q_p}\right)\left(\beta_{g_k} + \frac{1}{\eta p_p}\right), \\
c_k &= \left(\frac{\sum_{m=1}^{M} \beta_{v_m}}{q_p}\right)\left(\beta_{g_k} + \frac{1}{\eta p_p}\right), \\
d_k &= \left(\sum_{i=1}^{K} \beta_{g_i} + \frac{1}{q_p}\right)\left(\frac{\beta_{h_p}}{\eta p_p}\right), \\
e_k &= \frac{\beta_{h_p}\beta_{g_k}}{q_p} + \frac{\beta_{h_p}}{\eta p_p q_p}, \\
f_k &= \left(\frac{\sum_{m=1}^{M} \beta_{v_m}}{q_p}\right)\left(\frac{\beta_{h_p}}{\eta p_p}\right), \\
g_k &= \frac{(N_p + 2)\beta_{h_p}^2}{\eta p_p q_p}, \\
a_{2_m} &= N_s \beta_{f_m}^2, \\
b_{2_m} &= \beta_{f_m}^2 + \beta_{f_m}\left(\sum_{i=1}^{M} \beta_{f_i}\right), \\
c_{2_m} &= \beta_{f_m}\left(q_p \sum_{k=1}^{K} \beta_{u_k} + 1\right), \\
d_{2_m} &= \frac{\sum_{i=1}^{M} \beta_{f_i}}{\eta}, \\
e_{2_m} &= \frac{q_p \sum_{k=1}^{K} \beta_{u_k} + 1}{\eta}, \\
f_{2_m} &= \beta_{h_s}\beta_{f_m}, \\
g_{2_m} &= \frac{\beta_{h_s}}{\eta},
\end{aligned}$$

we formulate the optimization problem as in (12) at the bottom of this page.

In (12), C_1 denotes the primary interference constraint, in which Γ is the maximum allowable interference from the secondary system on the primary system; C_2 represents the quality of service requirement of the secondary users which is defined by their SINR. In addition, C_3 is the energy budget constraint of each secondary user; $E_{s_{max}}$ specifies the maximum allowed total energy for each secondary user; C_4 shows that sum of energies at the training and data transmission phases is equal to the jammer's maximum energy budget and Q denotes the jammer's maximum power budget.

The optimization problem in (12) is non-convex and cannot be solved efficiently. In the following, we propose three efficient methods to solve it. Firstly, we propose a geometric programming (GP) model for the *max* part of (12) for a given realization of the channel matrices, and then use standard numerical methods to obtain the optimal value of (12). To reduce the complexity, in the second proposed method, we derived a closed-form solution for (12) under some constraints on the channel gains. Finally, in the third proposed method, by use of epigraph form of the objective function and some manipulations on the constraints, we transform (12) to an equivalent convex optimization problem.

A. GEOMETRIC PROGRAMMING (GP) METHOD

In this solution, because of the multiplication of the variables, we study the GP model for the *max* problem of (12) [31].

$$\begin{aligned}
\min_{p_j, q_j} \max_{p_s, q_s} \quad & \sum_{k=1}^{K} \left(1 - \frac{\eta}{T}\right) \log_2 \left(1 + \frac{a_k}{b_k + c_k q_s + d_k p_j + e_k q_j + f_k q_s p_j + g_k q_j p_j}\right) \\
\text{s.t.} \quad & C_1\text{: } q_s . N_p \sum_m \beta_{v_m} \sum_k \frac{\eta p_p \beta_{g_k}^2}{\eta p_p \beta_{g_k} + p_j \beta_{hp} + 1} \le \Gamma, \\
& C_2\text{: } \frac{a_{2_m} p_s q_s}{b_{2_m} p_s q_s + c_{2_m} p_s + d_{2_m} q_s + e_{2_m} + f_{2_m} q_j p_s + g_{2_m} q_j} \ge \gamma_m, \forall m : 1, \ldots, M \\
& C_3\text{: } \eta p_s + (T - \eta) q_s \le E_{s_{max}}, \\
& C_4\text{: } \eta p_j + (T - \eta) q_j = QT, \\
& C_5\text{: } p_j \ge 0, p_s \ge 0, q_j \ge 0, q_s \ge 0
\end{aligned} \quad (12)$$

Thus, for a given realization of the channel matrices and by using the monotonicity of the log function we have

$$\begin{aligned}\min_{p_j,q_j}\ \max_{q_s,p_s}\ & \frac{a}{b+cq_s+dp_j+eq_j+fq_sp_j+gq_jp_j}\\ \text{s.t.}\ \ C_1:\ & q_s \le \frac{\Gamma.\left(\eta p_p\beta_g+p_j\beta_{hp}+1\right)}{N_p.M.K.\beta_v.\eta.p_p.\beta_g^2},\\ C_2:\ & a_2p_sq_s \ge \gamma.(b_2p_sq_s\\ & \quad +c_2p_s+d_2q_s+e_2+f_2q_jp_s+g_2q_j\big),\\ C_3:\ & \eta p_s+(T-\eta)q_s \le E_{s_{max}},\\ C_4:\ & \eta p_j+(T-\eta)q_j = QT,\\ C_5:\ & p_j\ge 0, p_s\ge 0, q_j\ge 0, q_s\ge 0. \end{aligned} \tag{13}$$

The objective function of (13) is not a posynomial function and thus, is not in GP definitions [31]. Therefore, by using the inverse of the objective function of (13), we obtain a posynomial objective function. According to [32], inversing the objective function of a $min-max$ problem results in an equivalent $max-min$ problem. Therefore, our problem is transformed to a $max-min$ problem as follows

$$\begin{aligned}\max_{p_j,q_j}\ \min_{q_s,p_s}\ & \frac{b+cq_s+dp_j+eq_j+fq_sp_j+gq_jp_j}{a}\\ \text{s.t.}\ \ & C_1, C_2, C_3, C_4, C_5. \end{aligned} \tag{14}$$

Since the objective function and constraints of (14) are posynomial functions w.r.t q_s and p_s, the *min* problem of (14) is a GP optimization problem [31]. Then, to solve the $max-min$ problem (14), we find the solution of the *min* problem of (14) for a finite set of pairs (p_j, q_j) satisfying $p_j, q_j \ge 0$ and $\eta p_j + (T-\eta)q_j = QT$. Then, we choose the pair which results in the maximum value for the solution of the *min* problem of (14). Note that the aforementioned set has a cardinality of $\mathcal{N} = \frac{QT}{\eta.\delta}$, where δ is the step size of discretization of the valid interval of p_j, and therefore our search is computationally affordable.

B. CLOSED-FORM SOLUTION

In this solution, we first study the *max* problem of (12). It should be noted that the objective function of the *max* problem just depends on q_s. Thus, we want to obtain the optimal value of q_s. At first, according to Appendix B, we demonstrate that the objective function of the *max* problem in (12) has a non-increasing behavior. Then for simplicity, we show the feasible set of the *max* problem in (12) in Fig. 2 (See Appendix C).

Under this feasible set and non-increasing behavior of the objective function, we realize that the smallest q_s in the feasible set is the optimal value of q_s. The smallest value of q_s is shown in Fig. 2 by a black dot. Therefore, we should find the intersection of the boundary of C_2 with largest horizontal asymptotic with that of C_3 to find the smallest q_s.

The optimal values of q_s and p_s are obtained as functions of q_j (Appendix D). After that, by using C_4, i.e., $p_j = \frac{QT-(T-\eta)q_j}{\eta}$, we have a minimization problem with one variable as follows

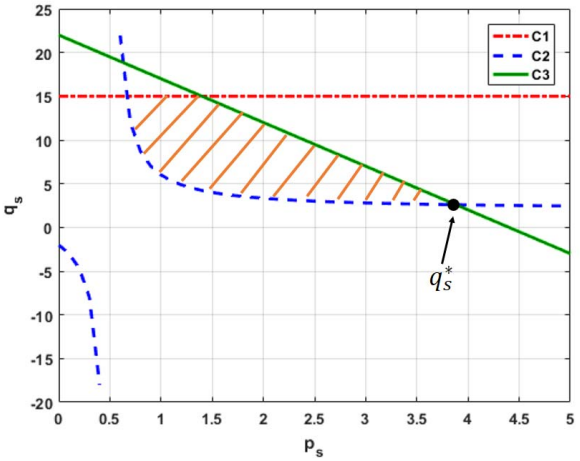

FIGURE 2. The feasible set of the *max* problem in (12) for a given realization of the channel matrices.

$$\min_{0\le q_j\le\Lambda}\ \sum_{k=1}^{K}\left(1-\frac{\eta}{T}\right)\log_2\left(1+\frac{a_k}{F_k(q_j)}\right), \tag{15}$$

where

$$\begin{aligned}F_k(q_j) = {} & b_k+(d_k+g_kq_j)\left(\frac{QT-(T-\eta)q_j}{\eta}\right)+e_kq_j\\ & +\left(E_{s_{max}}-\eta\left(\frac{-c_{2_m}(T-\eta)-f_{2_m}q_j(T-\eta)-\alpha_{1_m}\pm\sqrt{\Delta}}{2A_m}\right)\right)\\ & \times\frac{1}{(T-\eta)}\left(c_k+f_k\left(\frac{QT-(T-\eta)q_j}{\eta}\right)\right),\end{aligned}$$

and Λ is the upper bound of q_j (Appendix E). Finally, by setting the derivative of the objective function of (15) equal to zero, we can find optimal values of q_j and p_j. Also, a closed-form solution for q_j and p_j can be obtained for a given realization of the channel matrices (Appendix D).

C. CONVEX TRANSFORMATION (CT) METHOD

In this method, we try to find the convex model for the *max* problem of (12). We know that for $x>0$, $\log_2(1+\frac{1}{x})$ is a convex and non-increasing function. Moreover, the combination of any non-increasing convex function with a linear or concave function is always convex, and the summation of convex functions on the same domain is also convex [31]. Therefore, the objective function in (12) is a convex function w.r.t q_s. Due to the maximization of a convex function is not a convex problem, we use the epigraph form of the objective function of (12) as follows

$$\begin{aligned}\max_{p_s,q_s,\lambda}\ & \lambda\\ \text{s.t.}\ \ C_1:\ & \sum_{k=1}^{K}\log_2\left(\frac{p_k}{q_k}\right)\ge\lambda/\left(1-\frac{\eta}{T}\right),\\ C_2:\ & q_s\le\frac{\Gamma}{N_p\sum_m\beta_{V_m}\sum_k\frac{\eta\quad p_p\beta_{g_k}^2}{\eta p_p\beta_{g_k}+p_j\beta_{hp}+1}}=\Gamma',\\ C_3:\ & \left(a_{2_m}-\gamma_mb_{2_m}\right)p_sq_s\end{aligned}$$

$$\geq \gamma_m.\left(c_{2_m}p_s + d_{2_m}q_s + e_{2_m} + f_{2_m}q_jp_s + g_{2_m}q_j\right) \ \forall m,$$
$$C_4 : \eta p_s + (T-\eta)q_s \leq E_{s_{max}},$$
$$C_5 : p_s, q_s \geq 0, \tag{16}$$

where $q_k = b_k + c_kq_s + d_kp_j + e_kq_j + f_kq_sp_j + g_kq_jp_j$ and $p_k = a_k + q_k$. In (16), C_1 and C_3 are not convex sets [31]. To convexify C_1, we exploit the concavity of the negative relative entropy function, i.e., $q_k \log \frac{p_k}{q_k}$. To this end, we multiply q_k by the LHS of C_1. Then, to have a valid constraint, we should multiply the upper bound of q_k by the RHS of C_1. Moreover, to convexify C_3 we define $x = p_sq_s$. Thus, we have a convex problem as follows

$$\max_{p_s,q_s,\lambda,x,\lambda_k,p_k,q_k} \quad \lambda$$
$$\text{s.t.} \quad C_1 : \left(1-\frac{\eta}{T}\right)\sum_{k=1}^{K} q_k \log_2\left(\frac{p_k}{q_k}\right) \geq \sum_{k=1}^{K}\lambda_k\zeta_k,$$
$$C_2 : q_s \leq \Gamma',$$
$$C_3 : \left(a_{2_m} - \gamma_m b_{2_m}\right)x \geq \gamma_m.\left(c_{2_m}p_s + d_{2_m}q_s + e_{2_m} + f_{2_m}q_jp_s + g_{2_m}q_j\right) \ \forall m,$$
$$C_4 : \eta p_s + (T-\eta)q_s \leq E_{s_{max}},$$
$$C_5 : x \leq \mathrm{X},$$
$$C_6 : q_k \leq \zeta_k, p_k \leq \omega_k,$$
$$C_7 : \lambda = \sum_{k=1}^{K}\lambda_k,$$
$$C_8 : p_s, q_s \geq 0, \tag{17}$$

where X is the upper bound of x. Moreover, ζ_k and ω_k are the upper bounds of q_k and p_k, respectively.

Finally, to solve the $min - max$ problem, we find the solution of the max problem for a finite set of pairs (p_j, q_j) satisfying $p_j, q_j \geq 0$ and $\eta p_j + (T-\eta)q_j = QT$. Then, we choose the pair which results in the minimum value for the solution of the max problem. Note that the aforementioned set has a cardinality of $\mathcal{N} = \frac{QT}{\eta.\delta}$, where δ is the step size of discretization of the valid interval of p_j, and therefore our search is computationally affordable.

Remark 1: By assuming that the SNR value is calculated for the three methods, the computational complexity can be analyzed as follows. The first method consists of two min and max parts. The min part of the problem is formulated as a GP problem, which is solved using the interior point method whose computational complexity is upper bounded by $\mathcal{O}(n^4L)$, where n is the number of variables and L is the bit-length of the input data [33]. There are two variables p_s and q_s, and therefore, computational complexity of the GP part of the method is of order of a constant value. Moreover, the max part of the problem is a finite search over a set of cardinality of $\frac{QT}{\eta.\delta}$. Hence, the total computational complexity of this method is in the order of $\mathcal{O}(n^4\frac{QT}{\eta.\delta}L) = \mathcal{O}(16\frac{QT}{\eta.\delta}L)$. The second method consists of min and max parts. The min-max problem is solved in a closed form, and therefore, no iteration is performed to find the solution. Hence, the computational complexity is in the order of $\mathcal{O}(1)$. In the third method, due to that the relative entropy function is a special type logarithmic barrier functions, the interior point method is applied for solving it [31]. Therefore, similar computational complexity with the first method, can be stated, except that the number of variables according to problem (17) is $3K+4$. Hence, the computational complexity is at worst $\mathcal{O}(n^4\frac{QT}{\eta.\delta}L) = \mathcal{O}((3K+4)^4\frac{QT}{\eta.\delta}L)$.

Moreover, computational complexity of the SINR, presented in (9), depends on the number of antenna elements, which is in order of N_p^2, where N_p is the number of primary system antennas. Simulation results on the computational complexity shows that the running time of the third method is more than the two other methods. Also, the second method is the fastest method.

V. JAMMER OPTIMAL POWER ALLOCATION USING PRIMARY OPTIMAL POWERS

In previous sections, the jammer's effect on the fixed primary's powers was investigated. Here, we study a scenario that both the primary and secondary users have optimal power allocation. Therefore, in order to increase the destructive effect on the primary system, the jammer designs its attack by considering the following assumption and solves (18), as shown at the bottom of the next page, in which P_p is the total transmit power of each primary user.

By using the solution similar to the CT method for a given realization of the channel matrices, we have a convex problem as follows

$$\max_{p_s,q_s,p_p,q_p,\lambda,p,q,x_1,x_2,x_3} \quad \lambda,$$
$$\text{s.t.} \quad C_1 : \left(1-\frac{\eta}{T}\right)K.q\log_2\left(\frac{p}{q}\right) \geq \lambda\xi,$$
$$C_2 : x_1N_pKM\eta\beta_g^2\beta_v \leq \Gamma.\left(\eta p_p\beta_g + p_j\beta_{h_p} + 1\right),$$
$$C_3 : \frac{x_2N_s\beta_f^2}{\gamma} \geq \left(x_2M\beta_f^2 + p_s\beta_f + x_3\beta_f\beta_uK + \frac{q_sM\beta_f}{\eta}\right) + \left(\frac{1}{\eta} + \frac{q_pMK\beta_u}{\eta} + x_2\beta_f^2 + q_j\left(\beta_{h_s}\beta_{f_m}p_s + \frac{\beta_{h_s}}{\eta}\right)\right),$$
$$C_4 : \eta p_s + (T-\eta)q_s \leq E_{s_{max}},$$
$$C_5 : \eta p_p + (T-\eta)q_p \leq P_pT,$$
$$C_6 : x_1 \leq \mathrm{X}_1, x_2 \leq \mathrm{X}_2, x_3 \leq \mathrm{X}_3,$$
$$C_7 : q \leq \xi, p \leq \omega,$$
$$C_8 : p_s \geq 0, q_s \geq 0, p_p \geq 0, q_p \geq 0, \tag{19}$$

where $x_1 = p_pq_s$, $x_2 = p_sq_s$ and $x_3 = p_sq_p$. Their upper bounds are denoted by X_1, X_2 and X_3, respectively. Here, ξ and ω are the upper bounds of $q = (\beta_{g_k} + \frac{p_j\beta_{h_p}}{\eta p_p} + \frac{1}{\eta p_p})(\sum_{i=1}^{K}\beta_{g_i} + \frac{1}{q_p} + \frac{q_s}{q_p}\sum_{m=1}^{M}\beta_{v_m}) + \beta_{g_k}^2 + \frac{q_j}{q_p}(\beta_{h_p}\beta_{g_k} + \frac{p_j}{\eta p_p}(N_p+2)\beta_{h_p}^2 + \frac{\beta_{h_p}}{\eta p_p})$ and $p = N_p\beta_{g_k}^2 + q$, respectively.

Finally, we use numerical methods to obtain the optimal powers of the system.

TABLE 1. Simulation parameters.

Parameter	Value
Channel coherence time (T)	200
Length of the pilot sequences (η)	40
Number of primary users (K)	20
Number of secondary users (M)	20
Ratio between N_p and N_s (κ)	1
Maximum energy of each secondary user ($E_{s_{max}}$)	1000 j
Minimum SINR of each secondary user (γ_m)	-10 dB
Power budget of the jammer (Q[1])	10 dB

VI. NUMERICAL RESULTS

In this section, the performance of the proposed methods is investigated. In particular, we consider a MaMIMO CRN consisting of a primary system, a secondary system and a jammer as depicted in Fig. 1. In this network, we evaluate the sum spectral efficiency of the primary system in different scenarios. The number of primary users is $K = 20$ and the number of secondary users is $M = 20$. The coherence time of the channel is $T = 200$ symbols. The parameters that we use in this section are presented in Table 1. It should be noted that we use CVX toolbox of MATLAB to solve the GP and CT methods.

We define ρ and ζ as the ratio of the training phase energy to the total energy for the primary users and the jammer, respectively. Therefore, we have

$$p_p = \frac{\rho.P_p.T}{\eta}, \quad q_p = \frac{(1-\rho).P_p.T}{(T-\eta)} \tag{20a}$$

$$p_j = \frac{\zeta.Q.T}{\eta}, \quad q_j = \frac{(1-\zeta).Q.T}{(T-\eta)}. \tag{20b}$$

1. Due to the variance of the noise is normalized to one, the power budget of each primary user and the jammer, denoted by P_p and Q, respectively is measured in dB and, therefore, dimensionless.

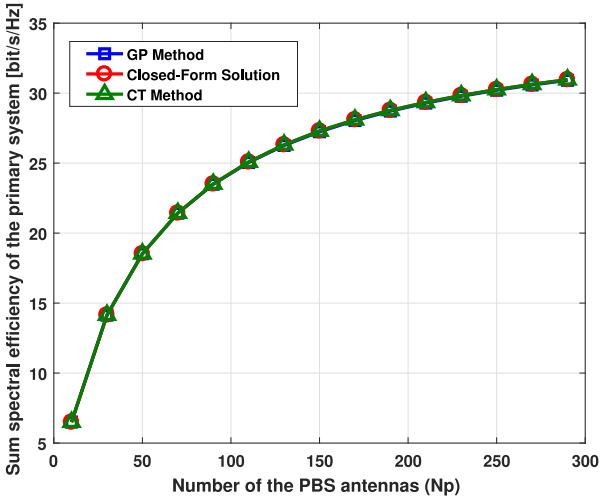

FIGURE 3. Sum spectral efficiency of the primary system versus the number of primary base station antennas (N_P) for the proposed methods (with $P_p = 5$ dB and $\rho = 0.6$).

Fig. 3 compares the sum spectral efficiency of the primary system versus the number of antennas at the PBS for three different solution methods for the optimization problem (12). It is seen that in all the number of antennas, the performance of the three methods is almost the same. Thus, the three proposed methods are efficient and have the same results, hence, we can use the most rapid one to solve Eq. (12). It should be noted that since we assume $\kappa = 1$, the number of antennas at the SBS is equal to the number of antennas at the PBS.

Fig. 4 shows the effect of the value of ζ that obtained from three proposed solution methods on the sum spectral efficiency of the primary system versus the number of antennas at the PBS. As shown in Fig. 4, the sum spectral efficiency of the primary system for the obtained ζ, i.e., $\zeta = 0.5$, has the lowest value. To give an intuition, consider the denominator of the inner part of the objective function

$$\min_{p_j,q_j} \max_{q_s,p_s,q_p,p_p} \sum_{k=1}^{K} \left(1-\frac{\eta}{T}\right)\log_2\left(1+\frac{N_p\beta_{g_k}^2}{\left(\left(\beta_{g_k}+\frac{p_j\beta_{h_p}}{\eta p_p}+\frac{1}{\eta p_p}\right)\left(\sum_{i=1}^{K}\beta_{g_i}+\frac{1}{q_p}+\frac{q_s}{q_p}\sum_{m=1}^{M}\beta_{v_m}\right)+\beta_{g_k}^2+\right.\right.$$
$$\left.\left.+\frac{q_j}{q_p}\left(\beta_{h_p}\beta_{g_k}+\frac{p_j}{\eta p_p}(N_p+2)\beta_{h_p}^2+\frac{\beta_{h_p}}{\eta p_p}\right)\right)\right)$$

$$\text{s.t. } C_1\colon q_s.N_p\sum_m\beta_{v_m}\sum_k\frac{\eta p_p\beta_{g_k}^2}{\eta p_p\beta_{g_k}+p_j\beta_{hp}+1}\le\Gamma,$$

$$C_2\colon \frac{N_s\beta_{f_m}^2}{\left(\beta_{f_m}+\frac{1}{\eta p_s}\right)\left(\sum_{i=1}^{M}\beta_{f_i}+\frac{1}{q_s}+\frac{q_p}{q_s}\sum_{k=1}^{K}\beta_{u_k}\right)+\beta_{f_m}^2+\frac{q_j}{q_s}\left(\beta_{h_s}\beta_{f_m}+\frac{\beta_{h_s}}{\eta p_s}\right)}\ge\gamma_m\ \forall m:1,\ldots.M,$$

$$C_3\colon \eta p_s+(T-\eta)q_s\le E_{s_{max}},$$

$$C_4\colon \eta p_p+(T-\eta)q_p\le P_pT,$$

$$C_5\colon \eta p_j+(T-\eta)q_j=QT,$$

$$C_6\colon p_j\ge 0, p_s\ge 0, q_j\ge 0, q_s\ge 0, p_p\ge 0, q_p,\ge 0 \tag{18}$$

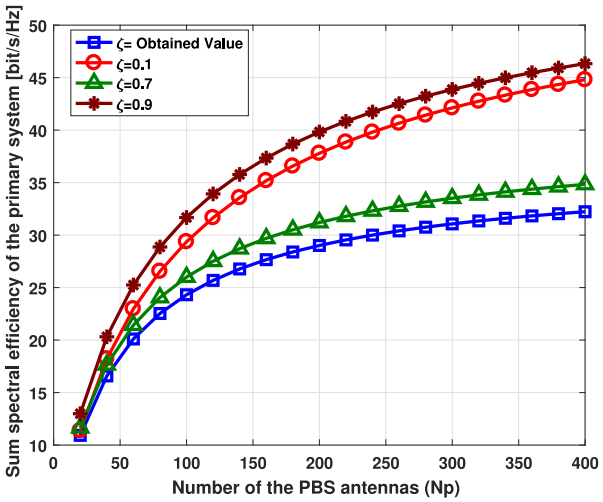

FIGURE 4. Sum spectral efficiency of the primary system versus the number of primary base station antennas (N_p) in different values of energy allocation ratio of the jammer ζ (with $P_p = 5$ dB and $\rho = 0.6$).

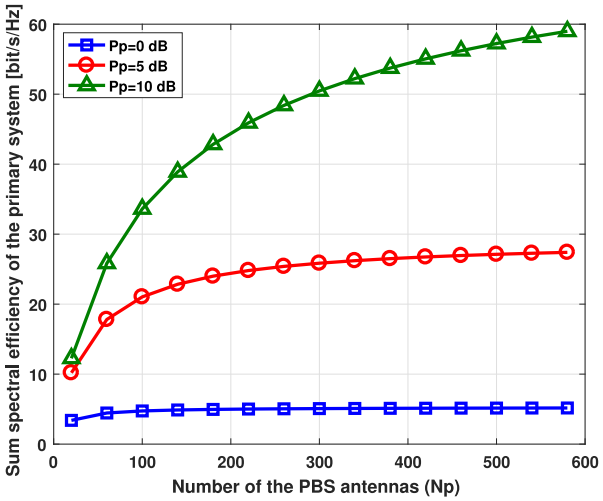

FIGURE 5. Sum spectral efficiency of the primary system versus the number of primary base station antennas (N_p) in different power budgets (P_p) of each primary user (with $\rho = 0.2$).

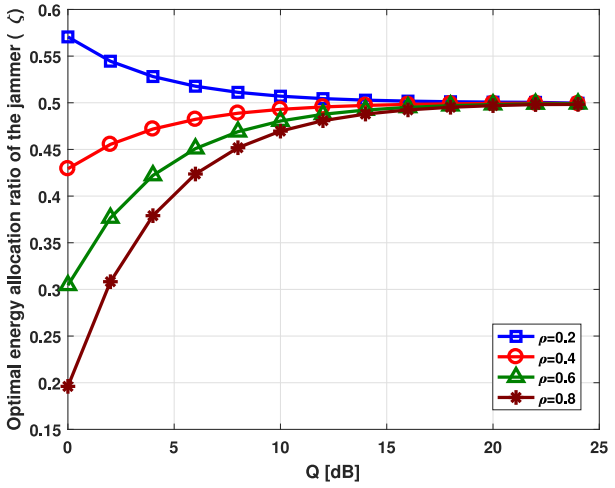

FIGURE 6. Optimal energy allocation ratio of the jammer (ζ) versus the jammer's power budget (Q) in different values of energy allocation ratio of the primary system (ρ) (with $P_p = 5$ dB and $N_p = N_s = 150$).

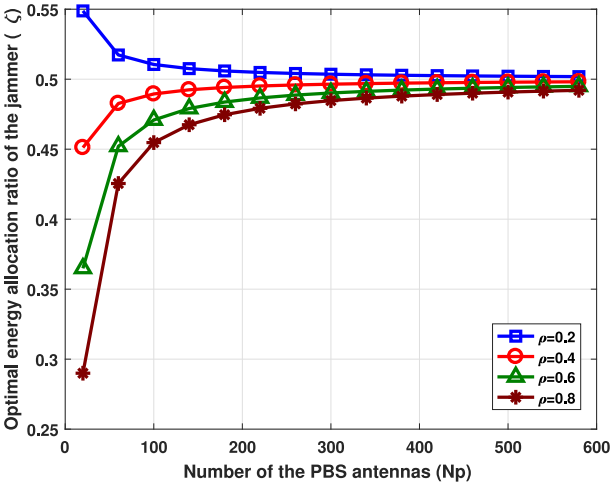

FIGURE 7. Optimal energy allocation ratio of the jammer (ζ) versus the number of primary base station antennas (N_p) in different values of energy allocation ratio of the primary system (ρ) (with $P_p = 5$ dB).

of the problem 12, and also assume that the coefficients d_k, e_k, and g_k are equal to 1. Then, the maximum of the denominator would be obtained for the equal value of p_j and q_j, or equivalently $\zeta = 0.5$. This result means that we have obtained the optimal power allocation of the jammer to degrade most the MaMIMO-CRN performance.

Fig. 5 illustrates the sum spectral efficiency of the primary system versus the number of antennas at the PBS in different power budgets (P_p) of each primary user. This figure validates the result of equation (11), which states that with the large number of N_p, the sum spectral efficiency of the primary is saturated. Also, it is deduced from Fig. 5 that the proposed system model with a lower value of P_p is more vulnerable to the jamming attack.

Fig. 6 and Fig. 7 indicate the effect of the jammer's power budget and the number of the PBS antennas on the energy allocation ratio of the jammer, respectively. As shown in Fig. 6, by increasing the jammer's power budget in different ρ, ζ approximately tends to 0.5. Thus, the jammer can allocate equal energy to each uplink transmission phase to destroy the MaMIMO-CRN. Moreover, it is seen from Fig. 6 that by increasing the energy allocation ratio of the primary system (ρ), the optimal energy allocation ratio of the jammer (ζ) decreases. This is intuitive, because, as much as primary system pay more energy in the data transmission phase, it is more beneficial to the jammer to transmit more energy in the other phase, *i.e.,* training phase.

Similar results are obtained from Fig. 7, in the case that the number of the PBS antennas varies and Q is fixed. Thus, in a large value of Q or N_p, the jammer has the vulnerable effect very easily. Therefore, the jammer does not need to know any information about the primary and secondary systems to solve problem (12) to have a destructive attack and just should allocate equal energy to each uplink transmission phase to degrade the performance of the MaMIMO-CRN.

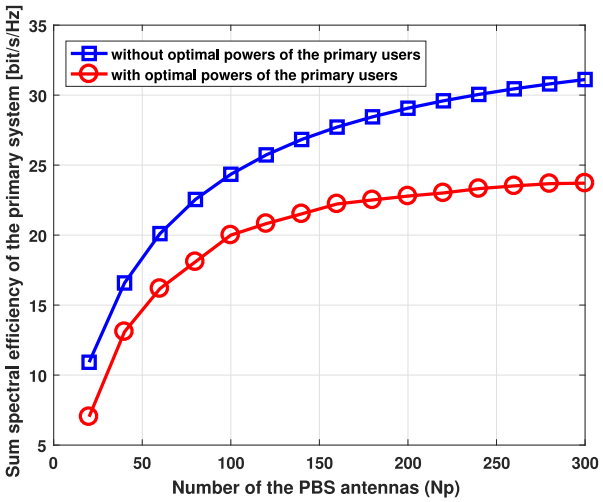

FIGURE 8. Sum spectral efficiency of the primary system versus the number of primary base station antennas (N_p) with and without optimal powers of primary users (with $\rho = 0.6$).

Fig. 8 shows the sum spectral efficiency of the primary system versus the number of primary base station antennas with and without the optimal powers of primary users. According to Fig. 8, when the jammer attacks the system with the optimal powers of the primary and secondary systems, the destructive effect of the jammer increases. Also, according to the proposed attack scenario, a jammer has a more destructive effect if it attacks the optimum MaMIMO-CRN.

VII. CONCLUSION

We studied the sum spectral efficiency behavior of a multi-user MaMIMO-CRN in the presence of a jammer. The pilot contamination within the training phase of the primary system was due to a jammer, which could optimally allocate its power budget to attack the training and data transmission phases of the primary system. We showed that even with a large number of antennas at the primary and secondary base stations, the jammer could destruct the sum spectral efficiency of the primary system. Moreover, it is illustrated that even in the case of a large number of antennas at both the primary and secondary base stations, for a large amount of the jammer's power budget, the jammer requires no process to allocate its power budget to optimally attack each uplink transmission phase.

APPENDIX A

Here we simplify the numerator and denominator of the right hand side (RHS) of the equation (9).

Assume that all channels are independent and with zero mean Normal distributions . Now, by considering (2), the numerator of the RHS of (9) can be written as follows,

$$E\left\{\hat{\mathbf{g}}_k^H \mathbf{g}_k\right\} = \mathcal{B}.E\left\{\mathbf{g}_k^H \mathbf{g}_k + \sqrt{\frac{p_j}{\eta p_p}}\mathbf{h}_p^H \mathbf{g}_k + \sqrt{\frac{1}{\eta p_p}}\boldsymbol{\phi}_{\mathbf{p_k}}^{\mathbf{T}} \mathbf{N}^H \mathbf{g}_k\right\}$$
$$= \mathcal{B}.E\left\{\mathbf{g}_k^H \mathbf{g}_k\right\} = \mathcal{B}N_p\beta_{g_k}. \quad (21)$$

To simplify the denominator of the RHS of (9), the following terms are calculated.

$$E\left[\left|\hat{\mathbf{g}}_k^H \mathbf{g}_i\right|^2\right] \overset{a}{=} E\left[Tr\left[\hat{\mathbf{g}}_k^H \mathbf{g}_i \mathbf{g}_i^H \hat{\mathbf{g}}_k\right]\right]$$
$$\overset{b}{=} E\left[Tr\left[\hat{\mathbf{g}}_k \hat{\mathbf{g}}_k^H \mathbf{g}_i \mathbf{g}_i^H\right]\right] \overset{c}{=} Tr\left[E_{g_i}\left[E_{\hat{g}_k}\left[\hat{\mathbf{g}}_k \hat{\mathbf{g}}_k^H \mathbf{g}_i \mathbf{g}_i^H | \mathbf{g}_i\right]\right]\right]$$
$$\overset{d}{=} Tr\left[\sigma_{\hat{g}_k}^2 \mathbf{I}_{N_p} E_{g_i}\left[\mathbf{g}_i \mathbf{g}_i^H\right]\right] \overset{e}{=} Tr\left[\sigma_{\hat{g}_k}^2 \mathbf{I}_{N_p} \beta_{g_i} \mathbf{I}_{N_p}\right] = N_p \beta_{g_i} \sigma_{\hat{g}_k}^2 \quad (22)$$

where $i \neq k$, $Tr[\,\cdot\,]$ calculates the trace of a matrix, and the equalities a, b, c and d are due to the trace properties and also the independence of the channels.

$$E\left[\left|\hat{\mathbf{g}}_k^H \mathbf{g}_k\right|^2\right] = E\left[\hat{\mathbf{g}}_k^H \mathbf{g}_k \mathbf{g}_k^H \hat{\mathbf{g}}_k\right]$$
$$\overset{g}{=} E\left[\left(\|\mathbf{g}_k\|^4 + \frac{p_j}{\eta p_p}\mathbf{h}_p^H \mathbf{g}_k \mathbf{g}_k^H \mathbf{h}_p + \frac{\boldsymbol{\phi}_{p_k}^T \mathbf{N}^H \mathbf{g}_k \mathbf{g}_k^H \mathbf{N} \boldsymbol{\phi}_{p_k}^*}{\eta p_p}\right)\mathcal{B}^2\right]$$
$$= \left(N_p(N_p+2)\beta_{g_k}^2 + \frac{p_j}{\eta p_p} N_p \beta_{h_p} \beta_{g_k} + \frac{N_p \beta_{g_k}}{\eta p_p}\right)\mathcal{B}^2, \quad (23)$$

where the equality g can be verified by considering (2) and the independence of the channels. The equality $E\{\|\mathbf{g}_k\|^4\} = N_p(N_p+2)\beta_{g_k}^2$ can be easily verified due to Normal distribution of $\mathbf{g}_k$. Moreover, $E\{\mathbf{h}_p^H \mathbf{g}_k \mathbf{g}_k^H \mathbf{h}_p\}$ and $E\{\boldsymbol{\phi}_{p_k}^T \mathbf{N}^H \mathbf{g}_k \mathbf{g}_k^H \mathbf{N} \boldsymbol{\phi}_{p_k}^*\}$ are simplified using the trace trick and independence of the random variables, similar to (21). Finally, the remaining terms of the denominator are calculated in the same manner as mentioned, where for brevity the details are removed. Accordingly, we have,

$$E\left\{\left|\hat{\mathbf{g}}_k^H \mathbf{v}_m\right|^2\right\} = N_p \sigma_{\hat{g}_k}^2 \beta_{v_m},$$
$$E\left\{\left\|\hat{\mathbf{g}}_k^H\right\|^2\right\} = N_p \sigma_{\hat{g}_k}^2,$$
$$E\left\{\left|\hat{\mathbf{g}}_k^H \mathbf{h}_p\right|^2\right\} = \left(N_p \beta_{g_k} \beta_{h_p} + \frac{p_j}{\eta p_p} N_p (N_p+2)\beta_{h_p}^2 + \frac{N_p \beta_{h_p}}{\eta p_p}\right)\mathcal{B}^2.$$

APPENDIX B

We know that the derivative of the combination of two functions is calculated as follows

$$(f(g(x)))' = f'(g(x))g'(x). \quad (24)$$

In the spectral efficiency that we calculated, $f(x) = log_2(1+\frac{1}{x})$ that for $x > 0$ is a non-increasing function [14], and $g(x) = (b_k + c_k q_s + d_k p_j + e_k q_j + f_k q_s p_j + g_k q_j p_j)/a_k$ is an increasing function w.r.t q_s. Therefore, the spectral efficiency of each primary user is a non-increasing function w.r.t q_s. Also, according to the rule that $(f+g+h+\cdots)' = f'+g'+h'+\cdots$, the sum spectral efficiency of the primary system is a non-increasing function as q_s is increasing.

APPENDIX C

After simplifying C_2 in (12), we have:

$$q_s\left[p_s\left(a_{2_m} - \gamma_m b_{2_m}\right) - \gamma_m d_{2_m}\right]$$
$$\geq \gamma_m\left[p_s\left(c_{2_m} + f_{2_m} q_j\right) + e_{2_m} + g_{2_m} q_j\right], \quad (25)$$

since the powers and other terms in (25) are positive, the right hand side of (25) is positive and therefore the left hand side of (25) should be positive. Thus we have

$$p_s\left(a_{2_m} - \gamma_m b_{2_m}\right) - \gamma_m d_{2_m} \geq 0. \tag{26}$$

Since p_s must always be positive, the only allowed mode of inequality (26) exists with the condition $a_{2_m} - \gamma_m b_{2_m} \geq 0$ as follows

$$p_s \geq \frac{\gamma_m d_{2_m}}{a_{2_m} - \gamma_m b_{2_m}}. \tag{27}$$

Eventually, C_2 is obtained as follows

$$q_s \geq \frac{\gamma_m\left[p_s\left(c_{2_m} + f_{2_m} q_j\right) + e_{2_m} + g_{2_m} q_j\right]}{p_s\left(a_{2_m} - \gamma_m b_{2_m}\right) - \gamma_m d_{2_m}}. \tag{28}$$

The inequality (28) is a homogeneous function, therefore, to plot (28) we should calculate the horizontal and vertical asymptotics of it. These asymptotics in our problem are positive and equal to

$$q_s = \frac{\gamma_m\left(c_{2_m} + f_{2_m} q_j\right)}{\left(a_{2_m} - \gamma_m b_{2_m}\right)}, \tag{29a}$$

$$p_s = \frac{\gamma_m d_{2_m}}{a_{2_m} - \gamma_m b_{2_m}}. \tag{29b}$$

It should be noted that to obtain the intersection of C_2 with C_1 and C_3, we should find the largest horizontal asymptotic of C_2 for all $m : 1, \ldots, M$.

Also, calculating the derivative of the fraction in (28) shows that its derivative is always negative. Therefore, the homogeneous function in (28) is always decreasing.

APPENDIX D

By finding the intersection of the boundary of C_3 with that of C_2 with largest horizontal asymptotic, the optimal value of p_s is obtained as

$$p_s^* = \frac{-c_{2_m}(T-\eta) - f_{2_m} q_j (T-\eta) - \alpha_{1_m} \pm \sqrt{\Delta}}{2A_m}, \tag{30}$$

where

$$\alpha_{1_m} = E_{s_{max}} b_{2_m} - \frac{E_{s_{max}} - a_{2_m}}{\gamma_m} - \eta d_{2_m},$$
$$\Delta = \sqrt{\beta_{1_m} q_j{}^2 + \beta_{2_m} q_j + \beta_{3_m}},$$
$$A_m = \frac{\eta a_{2_m}}{\gamma_m} - \eta b_{2_m},$$

which is defined as

$$\beta_{1_m} = (T-\eta)^2 f_{2_m}^2,$$
$$\beta_{2_m} = 2c_{2_m} f_{2_m}(T-\eta)^2 + f_{2_m}\alpha_{2_m} - 4A_m g_{2_m}(T-\eta),$$
$$\beta_{3_m} = (T-\eta)^2 c_{2_m}^2 + \alpha_{1_m}^2 + c_{2_m}\alpha_{2_m} - 4A_m\left(E_{s_{max}} d_{2_m} + e_{2_m}(T-\eta)\right),$$
$$\alpha_{2_m} = 2(T-\eta)\left(E_{s_{max}} b_{2_m} - \frac{E_{s_{max}} a_{2_m}}{\gamma_m} - \eta d_{2_m}\right).$$

The optimal value of q_s is obtain from $q_s^* = \frac{E_{s_{max}} - \eta p_s^*}{T-\eta}$.

By using q_s^* and p_s^* and setting the derivative of the objective function in (15) equal to zero for a given realization of the channel matrices, we have a quartic equation as follows

$$A_1 q_j^4 + B_1 q_j{}^3 + C_1 q_j^2 + D_1 q_j + E_1 = 0, \tag{31}$$

where

$$A_1 = \Gamma_2^2\beta_1 + \left(A'\beta_1 + B'\right)^2,$$
$$B_1 = \Gamma_2^2\beta_2 + 2\Gamma_1\Gamma_2\beta_1 + 2\left(A'\beta_1 + B'\right)\left(A'\beta_2 + C'\right),$$
$$C_1 = \Gamma_1^2\beta_1 + \Gamma_2^2\beta_3 + 2\Gamma_1\Gamma_2\beta_2 + \left(A'\beta_2 + C'\right)^2 + 2\left(A'\beta_1 + B'\right)\left(A'\beta_3 + D'\right),$$
$$D_1 = \Gamma_1^2\beta_2 + 2\Gamma_1\Gamma_2\beta_3 + 2\left(A'\beta_2 + C'\right)\left(A'\beta_3 + D'\right),$$
$$E_1 = \Gamma_1^2\beta_3 + \left(A'\beta_3 + D'\right)^2,$$

in which

$$A' = -af,$$
$$B' = \frac{-af\beta_1}{2A},$$
$$C' = \frac{a}{\eta - T}\left(\frac{\beta_2 f(T-\eta)}{4A} - \frac{\eta\beta_1\left(c + \frac{fQT}{\eta}\right)}{2A}\right),$$
$$D' = \frac{a\eta\beta_2}{4A(T-\eta)}\left(c + \frac{fQT}{\eta}\right),$$
$$\Gamma_1 = \left(E_{sMAX} + \frac{C_2(T-\eta)\eta}{2A} + \frac{\eta\alpha_1}{2A}\right)\left(\frac{af}{\eta}\right) - \frac{a}{T-\eta}\left(\frac{\eta f_2(T-\eta)}{2A}\right)\left(C + \frac{fQT}{\eta}\right) - a\left(e + \frac{gQT}{\eta} - \frac{d(T-\eta)}{\eta}\right),$$
$$\Gamma_2 = \frac{aff_2(T-\eta)}{A} + a\frac{2g(T-\eta)}{\eta}.$$

We now use the following solution to solve a quartic equation as $ax^4 + bx^3 + cx^2 + dx + e = 0$. The roots of this equation are obtained as

$$x_{1,2} = -\frac{b}{4a} - s \pm \frac{1}{2}\sqrt{-4s^2 - 2p + \frac{q}{s}},$$
$$x_{3,4} = -\frac{b}{4a} + s \pm \frac{1}{2}\sqrt{-4s^2 - 2p - \frac{q}{s}}. \tag{32}$$

where

$$p = \frac{8ac - 3b^2}{8a^2},$$
$$q = \frac{b^3 - 4ac + 8a^2 d}{8a^3},$$
$$s = \frac{1}{2}\sqrt{-\frac{2}{3}p + \frac{1}{3a}\left(Q + \frac{\Delta_0}{Q}\right)},$$

in which

$$Q = \sqrt[3]{\frac{\Delta_1 + \sqrt{\Delta_1^2 - 4\Delta_0^3}}{2}},$$

$$\Delta_0 = C^2 - 3bd + 12ae,$$
$$\Delta_1 = 2C^3 - 9bcd + 27b^2e + 27ad^2 - 72ace.$$

Therefore, by using (32) and $0 \leq q_j \leq \Lambda$ we find the optimal value of q_j.

APPENDIX E

In order to maintain the feasibility of the optimization problem (12), the horizontal asymptotic obtained from (29) should not violate condition C1. Therefore,

$$\frac{\Gamma}{N_p \sum_m \beta_{v_m} \sum_k \frac{\eta p_{tp} \beta_{gk}^2}{\eta p_{tp} \beta_{gk} + q_t \beta_{hp} + 1}} > \frac{r_m \left(c_{2_m} + f_{2_m} q_d\right)}{\left(a_{2_m} - r_m b_{2_m}\right)}. \quad (33)$$

Considering $q_t = \frac{QT - (T-\eta) q_d}{\eta}$, (33) can be rearranged to obtain an upper bound for q_d. The intersection of the aforementioned upper bound and the upper bound $q_d \leq \frac{QT}{T-\eta}$ obtained from the conditions C4 and C5, an upper bound for q_d is obtained which is denoted by Λ.

REFERENCES

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 40–48, Apr. 2008.

[2] F. Rusek *et al.*, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, Jan. 2013.

[3] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[4] H. Al-Hraishawi and G. Amarasuriya, "Sum rate analysis of cognitive massive MIMO systems with underlay spectrum sharing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2016, pp. 1–7.

[5] L. Wang, H. Q. Ngo, M. Elkashlan, T. Q. Duong, and K.-K. Wong, "Massive MIMO in spectrum sharing networks: Achievable rate and power efficiency," *IEEE Syst. J.*, vol. 11, no. 1, pp. 20–31, Mar. 2017.

[6] S. Chaudhari, "Interference mitigation and resource allocation in underlay cognitive radio networks," 2019. [Online]. Available: arXiv:1905.04572.

[7] W. Hao, O. Muta, H. Gacanin, and H. Furukawa, "Power allocation for massive MIMO cognitive radio networks with pilot sharing under SINR requirements of primary users," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1174–1186, Feb. 2018.

[8] S. Chaudhari and D. Cabric, "QoS aware power allocation and user selection in massive MIMO underlay cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 2, pp. 220–231, Jun. 2018.

[9] M. Cui, B.-J. Hu, X. Li, H. Chen, S. Hu, and Y. Wang, "Energy-efficient power control algorithms in massive MIMO cognitive radio networks," *IEEE Access*, vol. 5, pp. 1164–1177, 2017.

[10] M. Cui, B.-J. Hu, J. Tang, and Y. Wang, "Energy-efficient joint power allocation in uplink massive MIMO cognitive radio networks with imperfect CSI," *IEEE Access*, vol. 5, pp. 27611–27621, 2017.

[11] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[12] X. Lu, W. Yang, X. Guan, and Y. Cai, "DCE-based secure transmission for massive MIMO relay system against active eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13045–13059, Nov. 2020.

[13] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[14] H. Pirzadeh, S. M. Razavizadeh, and E. Björnson, "Subverting massive MIMO by smart jamming," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 20–23, Feb. 2016.

[15] W. Wang, N. Cheng, K. C. Teh, X. Lin, W. Zhuang, and X. Shen, "On countermeasures of pilot spoofing attack in massive MIMO systems: A double channel training based approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6697–6708, Jul. 2019.

[16] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A Hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.

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

[18] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 210–223, 2018.

[19] H. Akhlaghpasand, E. Björnson, and S. M. Razavizadeh, "Jamming suppression in massive MIMO systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 1, pp. 182–186, Jan. 2020.

[20] J. Gao, S. A. Vorobyov, H. Jiang, and H. V. Poor, "Worst-case jamming on MIMO Gaussian channels," *IEEE Trans. Signal Process.*, vol. 63, no. 21, pp. 5821–5836, Nov. 2015.

[21] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2nd Quart., 2015.

[22] K. G. Shin, H. Kim, A. W. Min, and A. Kumar, "Cognitive radios for dynamic spectrum access: From concept to reality," *IEEE Wireless Commun.*, vol. 17, no. 6, pp. 64–74, Dec. 2010.

[23] R. Biswas, J. Wu, X. Du, and Y. Yang, "Mitigation of the spectrum sensing data falsifying attack in cognitive radio networks," *Cyber-Phys. Syst.*, vol. 7, no. 3, pp. 159–178, 2021.

[24] J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in cognitive radio networks," *China Commun.*, vol. 12, no. 3, pp. 132–150, 2015.

[25] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[26] H. Al-Hraishawi, G. Amarasuriya, and R. F. Schaefer, "Secure communication in underlay cognitive massive MIMO systems with pilot contamination," in *Proc. IEEE Global Commun. Conf.*, 2017, pp. 1–7.

[27] S. Timilsina, G. A. A. Baduge, and R. F. Schaefer, "Secure communication in spectrum-sharing massive MIMO systems with active eavesdropping," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 2, pp. 390–405, Jun. 2018.

[28] S. F. Zamanian, M. H. Kahaei, and S. M. Razavizadeh, "Energy efficiency of massive MIMO cognitive radio networks in presence of smart jamming" *Int. J. Inf. Commun. Technol. Res.*, vol. 11, no. 3, pp. 1–8, 2019.

[29] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.

[30] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[31] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[32] C.-Y. Chi, W.-C. Li, and C.-H. Lin, *Convex Optimization for Signal Processing and Communications: From Fundamentals to Applications*. Boca Raton, FL, USA: CRC press, 2017.

[33] F. A. Potra and S. J. Wright, "Interior-point methods," *J. Comput. Appl. Math.*, vol. 124, no. 1, pp. 281–302, 2000.

S. FATEMEH ZAMANIAN received the B.Sc. degree in electrical engineering from Shahrekord University, Shahrekord, Iran, in 2016, and the M.Sc. degree in secure communication from the Iran University of Science and Technology, Tehran, Iran, in 2018, where she is currently pursuing the Ph.D. degree. Her research interests are in the area of massive MIMO systems, cognitive radio networks, and physical layer security in wireless communication systems.

MOHAMMAD HOSSEIN KAHAEI received the B.Sc. degree from the Isfahan University of Technology, Isfahan, Iran, in 1986, the M.Sc. degree from the University of the Ryukyus, Okinawa, Japan, in 1994, and the Ph.D. degree in signal processing from the School of Electrical and Electronic Systems Engineering, Queensland University of Technology, Brisbane, QLD, Australia, in 1998. Since 1999, he has been with the School of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran, where he is currently an Associate Professor and the Head of Signal and System Modeling Laboratory. His research interests include array signal processing with primary emphasis on compressed sensing, blind source separation, localization, tracking, DOA estimation, and wireless sensor networks.

S. MOHAMMAD RAZAVIZADEH (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the Iran University of Science and Technology (IUST), Tehran, Iran, in 2006. From 2005 to 2011, he was with the Iran Telecommunication Research Center, as a Research Assistant Professor. Since 2011, he has been with the School of Electrical Engineering, IUST, where he is currently an Associate Professor. He held several visiting positions with the University of Waterloo, Canada; Korea University, South Korea; and Chalmers University, Sweden. His research interests are in the area of signal processing for wireless communication systems and cellular networks.

TOMMY SVENSSON (Senior Member, IEEE) received the Ph.D. degree in information theory from the Chalmers University of Technology, Gothenburg, Sweden, in 2003. He is a Full Professor of Communication Systems with the Chalmers University of Technology, where he is leading the wireless systems research on air interface and wireless backhaul networking technologies for future wireless systems. He has worked with Ericsson AB with core networks, radio access networks, and microwave transmission products. He served as the Coordinator of the Communication Engineering Master's Program with the Chalmers University of Technology. He was involved in the European WINNER and ARTIST4G projects that made important contributions to the 3GPP LTE standards, the EU FP7 METIS, and the EU H2020 5GPPP mmMAGIC and 5GCar projects towards 5G, and currently the Hexa-X, RISE-6G, and SEMANTIC projects towards 6G, as well as in the ChaseOn antenna systems excellence center with Chalmers targeting mm-wave and (sub)-THz solutions for 5G/6G access, backhaul/fronthaul and V2X scenarios. He has coauthored five books, 100 journal papers, 132 conference papers, and 61 public EU projects deliverables. His research interests include design and analysis of physical layer algorithms, multiple access, resource allocation, cooperative systems, moving networks, and satellite networks. He is the Chairman of the IEEE Sweden joint Vehicular Technology/ Communications/ Information Theory Societies Chapter, the Founding Editorial Board Member and an Editor of IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Series on Machine Learning in Communications and Networks, has been an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS LETTERS, the guest editor of several top journals, organized several tutorials and workshops at top IEEE conferences.