IJICTR
International Journal of Information & Communication Technology Research

Volume 11- Number 3 – Summer 2019 (1 -8)

Energy Efficiency of Massive MIMO Cognitive Radio Networks in Presence of Smart Jamming

S. Fatemeh Zamanian
School of Electrical Engineering
Iran University of Science & Technology (IUST)
Tehran, Iran
f_zamanian@elec.iust.ac.ir

Mohammad Hossein Kahaei
School of Electrical Engineering
Iran University of Science & Technology (IUST)
Tehran, Iran
kahaei@iust.ac.ir

S. Mohammad Razavizadeh*
School of Electrical Engineering
Iran University of Science & Technology (IUST)
Tehran, Iran
smrazavi@iust.ac.ir

Received: 21 March 2019 - Accepted: 7 June 2019

Abstract—**We study the problem of physical layer security in massive multiple-input multiple-output (MaMIMO) cognitive radio networks (CRNs). In particular, we investigate the design of a smart jamming attack on the uplink transmission of a CRN in the presence of a single antenna jammer. The jammer is aware of the transmission protocol as well as the pilot set used for channel training in the MaMIMO systems. It attacks both the training and data transmission phases but with different powers. To have the most destructive attack, the jammer optimally divides its power between two phases to minimize the maximum energy efficiency of the secondary system. The resulting power optimization is a non-convex problem and to solve it, we propose a method to transform it into a convex optimization problem. Numerical results illustrate the effectiveness of the proposed smart jamming attack in decreasing the energy efficiency of the secondary MaMIMO system.**

Keywords-Physical layer security, massive MIMO, cognitive radio network, jamming, energy efficiency, convex optimization, power allocation.

Corresponding Author*

I. INTRODUCTION

In recent years, physical layer security in wireless networks has been attracted considerable attention. Two important attacks in wireless channels are eavesdropping and jamming [1]. In the eavesdropping attack, an illegitimate node listens to the communications in the network to extract their information, while the jammer is an illegitimate node that generates and transmits a noise-like signal or a signal that is similar to the original messages to disable the legitimate communication link. Physical layer security is referred to techniques that are employed at the physical layer by tracking the nature of physical layer transmission media to attain both authentication and confidentiality [2].

Two emerging technologies that have been adopted for using in next generation wireless networks are massive multiple-input multiple-output (MaMIMO) [3] - [4] and cognitive radio networks (CRNs) [5]. Physical layer security in both of these technologies been studied extensively before in literature. In [6] it was shown that the MaMIMO systems are secure against passive attacks and increasing the number of antennas can unlimitedly enhance the secrecy rate of the network. Nevertheless, an active attacker can limit the secrecy rate of the MaMIMO networks. There are also other papers in recent years that study the problem of *jamming detection* [7] or designing *jamming resistant receivers* [8], [9] for MaMIMO systems. [10] and [11] show that if a smart jammer that has some knowledge about the network and then optimizes its transmission parameters based on this knowledge it can significantly degrade the performance of the legitimate network. The problem of physical layer security in the CRN has also been studied before in literature [12] - [14]. In general, this problem has been studied from two different aspects, namely, spectrum sensing and cognitive communication. Spectrum sensing is vulnerable to attacks like primary user emulation (PUE) [12] and spectrum sensing data falsification (SSDF) [13]. Moreover, the jamming attack and eavesdropping can also be performed at the signal transmission phases in CRNs [14].

Combination of the MaMIMO and CR (*a.k.a.* MaMIMO CRN) can provide the benefits of both technologies [15] -[19]. Authors in [15] showed that by using a very large number of antennas at both primary and secondary base stations, the achievable sum rate of the MaMIMO CRNs considerably increases. In [16], authors investigated the power allocation problem in the MaMIMO CRNs by maximizing downlink sum rate of the secondary system through an orthogonal pilot sharing scheme. [17] proposed a joint power allocation and secondary user selection problem in the MaMIMO CRNs downlink to select the maximum number of secondary users while satisfying the quality of service requirements. Achieving maximum network energy efficiency (EE) while guaranteeing the fairness of EE among cognitive users in the MaMIMO CRNs was addressed in [18]. In [19], the problem of joint pilot and data power allocation while guaranteeing EE was investigated in the uplink of a MaMIMO CRN.

In contrast to the relatively extensive research that has been individually done on the physical layer security of MaMIMO systems and CRNs, the number of papers that study this problem in the MaMIMO CRNs is very limited [20] - [22]. In [20], secure transmissions of the MaMIMO CRNs were provided by exploiting linear precoders and artificial noise generation in the presence of the passive multi-antenna eavesdropper, and in [21] the system model of [20] was studied in the case of pilot contamination between the primary and secondary systems. Also, intercepting the confidential downlink transmissions of the primary and secondary systems along with the uplink pilots contamination by the active eavesdropper were investigated in [22].

In this paper, we study the problem of physical layer security in the MaMIMO CRNs in the presence of a smart jamming attack. In our work, we see the system from the jammer's point of view and try to find the optimal attack that a smart jammer can design to have the maximum subversive effect on the performance of the legitimate system. Knowing these attacks is essential for designing the countermeasure techniques and make the systems more secure. We assume that the smart jammer has some knowledge about the legitimate network and uses this knowledge to efficiently design its attack. The performance metric is the EE of the secondary network. First, we analytically derive the EE of the secondary network and then use it as the objective of an optimization problem that the jammer performs to optimally divide its power between the training and data transmission phases. The numerical simulations show the effectiveness of the proposed jamming on decreasing the EE of the CRN. The results also show that increasing the number of antennas at both the primary and secondary networks do not improve the performance. In summary, our contributions are as follows:

- We study the physical layer security of a MaMIMO CRN in the presence of smart jamming attacks.
- We design an optimal attack for a smart jammer who has some information about the legitimate network and use it to optimize its transmission.
- We analytically calculate the EE of a MaMIMO CRN in the presence of a jamming attack.
- We formulate a power allocation problem to optimally divide the power of the jammer among the pilot and data transmission phases in the uplink transmission.
- Since the resulting optimization problem is non-convex, by utilizing relative entropy function and some transformation in the constraint functions, we form a convex optimization problem to be solved efficiently by numerical methods.

The remaining of the paper is as follows. In Section II, we introduce the system model. Analysis of the uplink transmission and EE calculation are given in Section III. Section IV is devoted to formulate the power allocation problem and its

solution. Numerical results and conclusions are expressed in Sections V and VI, respectively.

II. System Model

We study the uplink transmission of a time-division duplex (TDD) multi-user MaMIMO CRN with underlay spectrum sharing as illustrated in Fig. 1. The number of users in the primary and secondary systems are K and M, respectively, and all of them are single antenna users. Also, there is a primary base station equipped with $N_p \gg 1$ antennas and a secondary base station with $N_s \gg 1$ antennas in the network. Although both N_p and N_s are very large numbers, but the ratio between them is limited and denoted by α. The channel coherence time is denoted by T in which the first τ symbols is devoted to transmitting τ-tuple mutual orthogonal pilot sequences where $max(K, M) \leq \tau \leq T$ to estimate the channels and the rest are used for transmitting data symbols.

The channel matrix between the primary users and primary base station is shown by $\boldsymbol{G} = \boldsymbol{H}_G \boldsymbol{D}_G^{1/2}$, where $\boldsymbol{H}_G \in \mathbb{C}^{N_p \times K}$ consists of i.i.d elements distributed as $CN \sim (0,1)$ models the primary channel small scale fading, and $\boldsymbol{D}_G = diag(\beta_{g_1}, \beta_{g_2}, \ldots, \beta_{g_k}, \ldots, \beta_{g_K})$ models the large scale fading (*i.e.* path loss and shadowing) between the primary users and the primary base station. The kth column of $\boldsymbol{G}$ denoted by $\boldsymbol{g}_k$ is corresponding to the channel of the kth primary user. Similarly, for the secondary system, $\boldsymbol{F} = \boldsymbol{H}_F \boldsymbol{D}_F^{1/2}$ shows the channel matrix between the secondary users and the secondary base station, where $\boldsymbol{H}_F \in \mathbb{C}^{N_s \times M}$ and $\boldsymbol{D}_F = diag(\beta_{f_1}, \beta_{f_2}, \ldots, \beta_{f_m}, \ldots, \beta_{f_M})$ are defined similar to their primary system counterparts. Moreover, the channel of the mth secondary user is denoted by $\boldsymbol{f}_m$ which is the mth column of $\boldsymbol{F}$. Furthermore, $\boldsymbol{V} \in \mathbb{C}^{N_p \times M}$ is the channel matrix between the secondary users and the primary base station whose mth column of it is denoted by $\boldsymbol{v}_m$. Moreover, $\boldsymbol{U} \in \mathbb{C}^{N_s \times K}$ is the channel matrix between the primary users and the secondary base station whose kth column of it is denoted by $\boldsymbol{u}_k$.

As illustrated in Fig. 1, there is also a single antenna jammer in the area that targets the secondary system. The channel vectors between jammer and the primary base station and secondary base station are denoted by $\boldsymbol{h}_p$ and $\boldsymbol{h}_s$, respectively. In this paper, we like to find the worst case of the jamming attack to the secondary system. To design the worst case jamming, it is assumed that the jammer has some knowledge about the secondary system and optimizes its attack accordingly. This information includes the transmission protocols (*i.e.* the length and starting time of the pilot and data transmission phases) and also the set of pilots that are employed by the secondary system to estimate the channels. The jammer exploits this information to optimally design its transmission and make the maximum reduction to the sum EE of the secondary system.

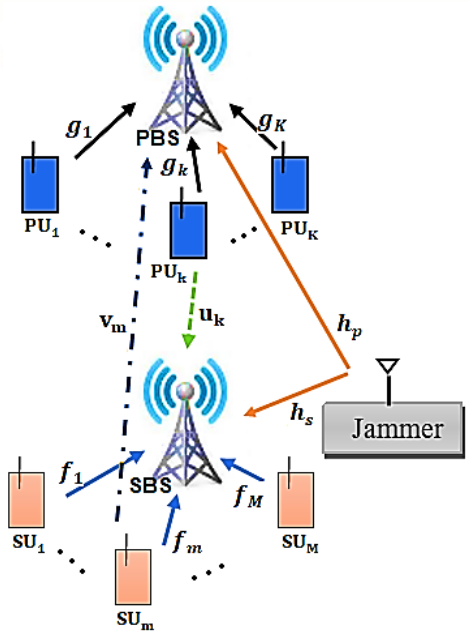

Figure 1. System Model.

III. Uplink Transmission and EE Calculation

In this section, we analyze the signal transmission in the network and derive the EE of the secondary system in the presence of the jammer. The signal transmission is performed in two phases namely pilot phase and data transmission phase which are studied in the following.

A. Pilot Transmission Phase

In the pilot transmission phase, each legitimate user sends a pilot signal chosen from a pilot set to estimate the channels. At the same time, the jammer sends a pilot-like signal to creates pilot contamination effects and to deteriorate the secondary user channel estimation. Although the jammer is aware of the transmission protocol and the set of secondary's pilot sequences, it has no information about the specific pilot assigned to each secondary user at each time slot. Therefore, the jammer sends a linear combination of all the secondary's pilot sequences. It has been proved that this is the best strategy that a jammer can adopt in massive MIMO systems [7].

The pilot sequences of the primary and secondary systems are denoted by $\boldsymbol{\Phi}_p \in \mathbb{C}^{\tau \times K}$ and $\boldsymbol{\Phi}_s \in \mathbb{C}^{\tau \times M}$, respectively. $\boldsymbol{\phi}_{\mathbf{p_k}}$ is the k th column of $\boldsymbol{\Phi}_p$ that denotes the kth primary user's pilot sequence and $\boldsymbol{\phi}_{\mathbf{s_m}}$ is the mth column of $\boldsymbol{\Phi}_s$ that denotes the mth secondary user's pilot sequence. The received signal at the secondary base station is

$$\boldsymbol{Y}_{t_s} = \sqrt{\tau p_{t_s}}\, \boldsymbol{F}\, \boldsymbol{\Phi}_s^T + \sqrt{\tau p_{t_p}}\, \boldsymbol{U}\, \boldsymbol{\Phi}_p^T + \sqrt{q_t}\, h_s\, \boldsymbol{\phi}_j^T + \boldsymbol{W}, \quad (1)$$

where p_{t_s}, p_{t_p} and q_t are the average pilot transmission powers of each secondary user, each primary user and the jammer, respectively. Moreover, $\boldsymbol{W} \in \mathbb{C}^{N_s \times M}$ is circularly-symmetric complex Gaussian noise matrix at the secondary base station

with *i.i.d.* $CN \sim (0,1)$ elements, and $\boldsymbol{\phi_j} = \sum_{m=1}^{M} \boldsymbol{\phi_{s_m}}$ is the pilot sequence of the smart jammer. Considering equation (1) and by assuming that all pilot sequences are orthogonal, *i.e.* $\boldsymbol{\Phi_p}^H \boldsymbol{\Phi_p} = \boldsymbol{I_K}$, $\boldsymbol{\Phi_s}^H \boldsymbol{\Phi_s} = \boldsymbol{I_M}$, $\boldsymbol{\Phi_p}^H \boldsymbol{\Phi_s} = \boldsymbol{0}$, and using minimum mean squared error (MMSE) estimation, the estimation of the mth secondary user channel, $\boldsymbol{f}_m$, denoted by $\hat{\boldsymbol{f}}_m$ is equal to

$$\hat{\boldsymbol{f}}_m = \frac{1}{\sqrt{\tau p_{t_s}}} \boldsymbol{Y}_{t_s} \boldsymbol{\phi}^*_{\mathbf{s_m}} \left(1 + \frac{q_t \beta_{h_s}}{\tau p_{t_s} \beta_{f_m}} + \frac{1}{\tau p_{t_s} \beta_{f_m}}\right)^{-1}. \quad (2)$$

Moreover, the covariance matrix of $\hat{\boldsymbol{f}}_m$ is obtained as

$$C_{\hat{f}_m} = \mathbb{E}\{\hat{\boldsymbol{f}}_m \hat{\boldsymbol{f}}_m{}^H\} = \frac{\tau p_{t_s} \beta^2_{f_m}}{\tau p_{t_s} \beta_{f_m} + q_t \beta_{h_s} + 1} \boldsymbol{I}_{N_s}. \quad (3)$$

B. *Data Transmission Phase*

After pilot transmission and channel estimation in the pilot phase, in the data transmission phase, the users transmit their signals to the base stations. At the same time, the jammer produces a noise-like adversary signal and transmits it to the base stations. By using linear decoding at the secondary system, the resulting signal at the secondary base station is obtained as

$$\boldsymbol{y}_{d_s} = \boldsymbol{A}^H \left(\sqrt{p_{d_s}}\, \boldsymbol{F x} + \sqrt{p_{d_p}}\, \boldsymbol{U z} + \sqrt{q_d}\, \boldsymbol{h}_s s + \boldsymbol{w}\right), \quad (4)$$

where $\boldsymbol{A} \in \mathbb{C}^{N_s \times M}$ denotes linear detector at the secondary base station which depends on the secondary estimated channel. p_{d_s}, p_{d_p} and q_d are the average data transmission powers of each secondary user, each primary user and the jammer, respectively. $\boldsymbol{x} \in \mathbb{C}^{M \times 1}$ and $\boldsymbol{z} \in \mathbb{C}^{K \times 1}$ respectively denote the normalized symbol vectors transmitted by the secondary and primary users. s and $\boldsymbol{w} \in CN(0, I_{N_s})$ signify the normalized symbol of the jammer and a circularly-symmetric complex Gaussian noise at the secondary base station, respectively. The m th elements of the vector $\boldsymbol{y}_{d_s}$ in (4) is

$$y^m_{d_s} = \sqrt{p_{d_s}}\, \boldsymbol{a}_m^H\, \boldsymbol{f}_m\, x_m + \sum_{i=1, i\neq m}^{M} \sqrt{p_{d_s}}\, \boldsymbol{a}_m^H\, \boldsymbol{f}_i\, x_i + \sum_{k=1}^{K} \sqrt{p_{d_p}}\, \boldsymbol{a}_m^H\, \boldsymbol{u}_k\, z_k + \sqrt{q_d}\, \boldsymbol{a}_m^H\, \boldsymbol{h}_s\, s + \boldsymbol{a}_m^H\, \boldsymbol{w}, \quad (5)$$

where $\boldsymbol{a}_m$ is the mth column of $\boldsymbol{A}$ and the first term in the RHS of (5) is the desired signal and the other terms are considered as interference plus noise.

The secondary's sum EE (sumEE) is equal to the summation of the EE of each secondary user, and the EE of each secondary user is defined as the ratio of its spectral efficiency ($\mathrm{SE}=(1-\frac{\tau}{T})\mathbb{E}(\log_2(1+\mathrm{SINR}))$) and power consumption as [19]

$$EE_m = \frac{SE_m}{PC}. \quad (6\text{-a})$$

$$sumEE = \sum_{m=1}^{M} EE_m \quad (6\text{-b})$$

To obtain a closed-form solution of the SE_m, we have used a lower bound of it as [23]

$$SE_m \geq \overline{SE_m} \triangleq \left(1 - \frac{\tau}{T}\right) \log_2\left(1 + \mathbb{E}(SINR_s^m)\right). \quad (7)$$

Since the desired signal is independent of interference and noise signals, $\mathbb{E}(SINR_s^m)$ of the mth secondary user can be presented in equation (8) which can be obtained using the maximum ratio combining (MRC) detector in both primary and secondary base stations.

$$\mathbb{E}(SINR_s^m) = \frac{p_{d_s} \cdot |\mathbb{E}\{\hat{\boldsymbol{f}}_m^H\, \boldsymbol{f}_m\}|^2}{\Delta}, \quad (8)$$

where

$$\Delta = p_{d_s} \sum_{i=1}^{m} \mathbb{E}\left\{|\hat{\boldsymbol{f}}_m^H\, \boldsymbol{f}_i|^2\right\} - p_{d_s} |\mathbb{E}\{\hat{\boldsymbol{f}}_m^H\, \boldsymbol{f}_m\}|^2 + p_{d_p} \sum_{k=1}^{K} \mathbb{E}\left\{|\hat{\boldsymbol{f}}_m^H\, \boldsymbol{u}_k|^2\right\} + q_d \mathbb{E}\left\{|\hat{\boldsymbol{f}}_m^H\, \boldsymbol{h}_s|^2\right\} + \mathbb{E}\{||\hat{\boldsymbol{f}}_m^H||^2\}.$$

Moreover, the uplink power consumption of each secondary can be expressed as [19]

$$PC = \frac{1}{\epsilon}\left(\frac{\tau}{T} p_{t_s} + \left(1 - \frac{\tau}{T}\right) p_{d_s}\right) + P_c, \quad (9)$$

where ϵ denotes the efficiency of power amplifiers at the secondary users and P_c signifies the constant circuit operational expenditures during the uplink transmission. By using equations (6) - (9), the sumEE is obtained as in (10). It should be noted that for simplifying equation (8), we have used the channel independence, the Normal distribution properties, resulting in $\mathbb{E}\left\{||f_m||^2\right\} = N_s \beta_{f_m}$ and $\mathbb{E}\left\{||f_m||^4\right\} = N_s(N_s+2)\beta^2_{f_m}$. Furthermore, by using equations (2) and (3) we have

$$sumEE = \left(\frac{\left(1-\frac{\tau}{T}\right)}{\frac{1}{\epsilon}\left(\frac{\tau}{T} p_{t_s} + \left(1-\frac{\tau}{T}\right) p_{d_s}\right) + P_c}\right) \times \sum_{m=1}^{M} \log_2\left(1 + \frac{N_s \beta^2_{f_m}}{\Delta'}\right), \quad (10)$$

where

$$\Delta' = \left(\beta_{f_m} + \frac{q_t \beta_{h_s}}{\tau p_{t_s}} + \frac{1}{\tau p_{t_s}}\right)\left(\sum_{i=1}^{M} \beta_{f_i} + \frac{1}{p_{d_s}} + \frac{p_{d_p}}{p_{d_s}} \sum_{k=1}^{K} \beta_{u_k}\right) + \beta^2_{f_m} + \frac{q_d}{p_{d_s}}\left(\beta_{h_s} \beta_{f_m} + \frac{q_t}{\tau p_{t_s}} (N_s + 2) \beta^2_{h_s} + \frac{\beta_{h_s}}{\tau p_{t_s}}\right).$$

IV. Power Allocation Problem Formulation

In this section, we intend to investigate the optimal jamming attack which imposes the most destructive effect on the sumEE of the legitimate network. For this aim, the jammer optimally allocates its power budget to attack the training and data transmission phases. This power allocation is an optimization problem in which the objective is to minimize the maximum sumEE of the secondary system. By defining

$$
\begin{aligned}
a_m &= \beta_{f_m}^2 + \beta_{f_m}\left(\sum_{i=1}^{M}\beta_{f_i}\right),\\
b_m &= \beta_{f_m}\left(p_{d_p}\sum_{k=1}^{K}\beta_{u_k}+1\right),\\
c_m &= \frac{\sum_{i=1}^{M}\beta_{f_i}}{\tau},\\
d_m &= \frac{\beta_{h_s}\sum_{i=1}^{M}\beta_{f_i}}{\tau},\\
e_m &= \beta_{h_s}\beta_{f_m},\\
f_m &= \frac{\beta_{h_s}^2(N_s+2)}{\tau},\\
g_m &= \frac{\beta_{h_s}\left(p_{d_p}\sum_{k=1}^{K}\beta_{u_k}+1\right)}{\tau},\\
h_m &= \frac{\beta_{h_s}}{\tau},\\
i_m &= \frac{\left(p_{d_p}\sum_{k=1}^{K}\beta_{u_k}+1\right)}{\tau},
\end{aligned}
$$

we formulate a $min-max$ optimization problem for jammer power allocation as (11).

$$
\begin{aligned}
&\min_{q_t,q_d}\ \max_{p_{t_s},p_{d_s}}\ \frac{\left(1-\frac{\tau}{T}\right)}{\frac{1}{\epsilon}\left(\frac{\tau}{T}p_{t_s}+\left(1-\frac{\tau}{T}\right)p_{d_s}\right)+P_c}\sum_{m=1}^{M}\log_2\left(1+\frac{N_s\beta_{f_m}^2 p_{t_s}p_{d_s}}{\Delta''}\right)\\
&s.t.\quad C_1: p_{d_s}.N_p\sum_{m=1}^{M}\beta_{v_m}\sum_{k=1}^{K}\frac{\tau p_{t_p}\beta_{g_k}^2}{\tau p_{t_p}\beta_{g_k}+q_t\beta_{h_p}+1}\le\Gamma,\\
&\quad C_2: \frac{N_s\beta_{f_m}^2 p_{t_s}p_{d_s}}{\Delta''}\ge\gamma_m,\forall\ m:1,\cdots,M\\
&\quad C_3: \tau p_{t_s}+(T-\tau)p_{d_s}\le E_{s_{max}},\\
&\quad C_4: \tau q_t+(T-\tau)q_d=QT,\\
&\quad C_5: p_{t_s}\ge 0, p_{d_s}\ge 0, q_t\ge 0, q_d\ge 0,
\end{aligned}
\tag{11}
$$

where

$$
\Delta'' = a_m p_{t_s}p_{d_s}+b_m p_{t_s}+c_m p_{d_s}+d_m p_{d_s}q_t+e_m p_{t_s}q_d+f_m q_d q_t+g_m q_t+h_m q_d+i_m.
$$

The constraints of (11) are as follows. C_1 presents the primary interference condition, where Γ is the primary interference threshold, C_2 specifies the quality of service constraint of each secondary user in which γ_m is the minimum SINR of the mth secondary user. C_3 represents the energy budget condition of each secondary user, where $E_{s_{max}}$ is the maximum allowed total energy for each secondary user. C_4 denotes the total energy of the jammer, where Q is the power budget of the jammer. Finally, C_5 constrains that all powers be positive.

The $min-max$ optimization problem in (11) is a non-convex problem. Thus, we first propose a convex form for the max part of (11) by some approximation (*i.e.* we define some auxiliary variables and calculate their bounds), and then use numerical methods to solve it. To calculate the approximated-convex form of the max part of (11), we use the relative entropy function, *i.e.*$x\log\frac{x}{y}$. The relative entropy function and summation of the relative entropies are convex [24]. By defining

$$
A=\frac{1}{\frac{1}{\epsilon}\left(\frac{\tau}{T}p_{t_s}+\left(1-\frac{\tau}{T}\right)p_{d_s}\right)+P_c},
$$

$$
\begin{aligned}
B_m &= a_m p_{t_s}p_{d_s}+b_m p_{t_s}+c_m p_{d_s}+d_m p_{d_s}q_t\\
&\quad +e_m p_{t_s}q_d+f_m q_d q_t+g_m q_t+h_m q_d+i_m,
\end{aligned}
$$

$$
C_m=\frac{\left(B_m+N_s\beta_{f_m}^2 p_{t_s}p_{d_s}\right)A}{B_m},
$$

$$
D=p_{t_s}p_{d_s},
$$

And calculating the upper bounds of them, we can formulate the convex form of the max part of (11) as follows

$$
\begin{aligned}
&\max_{p_{t_s},p_{d_s},A,C_m}\ \left(1-\frac{\tau}{T}\right)\sum_{m=1}^{M}A\ \log_2\left(\frac{C_m}{A}\right)\\
&s.t.\quad C_1: p_{d_s}.N_p\sum_{m}\beta_{v_m}\sum_{k}\frac{\tau p_{t_p}\beta_{g_k}^2}{\tau p_{t_p}\beta_{g_k}+q_t\beta_{h_p}+1}\le\Gamma,\\
&\quad C_2: (N_s\beta_{f_m}^2-\gamma_m a_m)D\ge\\
&\qquad \gamma_m(b_m p_{t_s}+c_m p_{d_s}+d_m p_{d_s}q_t+e_m p_{t_s}q_d\\
&\qquad +f_m q_d q_t+g_m q_t+h_m q_d+i_m),\forall\ m:1,\cdots,M\\
&\quad C_3: \tau p_{t_s}+(T-\tau)p_{d_s}\le E_{s_{max}},\\
&\quad C_4: A\le a, D\le d, C_m\le c'_m,\\
&\quad C_5: p_{t_s}\ge 0, p_{d_s}\ge 0,
\end{aligned}
\tag{12}
$$

where a, d and c'_m are the upper bounds of A, D and C_m, respectively. The objective function in the maximization problem in (12) is a concave function, since it is a negative convex function. Furthermore, all the constraints in (12) are convex. Therefore, (12) is a convex optimization problem and we use CVX toolbox of MATLAB to solve it. Finally to obtain the optimal powers of the jammer, we find the solution of (12) for a finite set of pairs (q_t,q_d) satisfying $q_t,q_d\ge 0$ and $\tau q_t+(T-\tau)q_d=QT$, and choose the pair which results in the minimum value for the solution of (12). Note that the aforementioned set is a set with a cardinality of $\mathcal{N}=\frac{QT}{\tau\Delta q_t}$, where Δq_t is the step size of discretization of the valid interval of q_t, and therefore our search is computationally affordable.

V. NUMERICAL RESULTS

In this section, the performance of the MaMIMO CRN under the proposed jamming attack is investigated. The parameters that we use in this section have been presented in Table I[1].

TABLE I. PARAMETERS.

Parameter	Value
Channel coherence time (T)	200
Length of the pilot sequences (τ)	20
Number of primary users (K)	5
Number of secondary users (M)	10
Ratio between N_p and N_s (α)	1
Maximum energy for secondary users ($E_{s_{max}}$)	1000 j
Power budget of each primary user (P)	10 dB
Minimum SINR of each secondary user (γ_m)	-10 dB
Interference threshold of the primary system (Γ)	10 dBw
Efficiency of power amplifiers (ϵ)	0.4
Constant circuit operational expenditures (P_c)	-10 dBw

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

$$p_{t_p} = \frac{\rho.P.T}{\tau}, \qquad p_{d_p} = \frac{(1-\rho).P.T}{(T-\tau)}, \qquad \text{(13-a)}$$

$$q_t = \frac{\zeta.Q.T}{\tau}, \qquad q_d = \frac{(1-\zeta).Q.T}{(T-\tau)}. \qquad \text{(13-b)}$$

In the following, we present three experiments to study the performance of the system model.

Experiment 1: In this experiment, we study the effect of increasing the number of secondary base station antennas, N_s, on the sumEE of the secondary system and ζ. As illustrated in Fig. 2, by increasing N_s, the sumEE of the secondary system decreases for any value of ρ. This means that, surprisingly by increasing the number of antennas at the secondary base station, the smart jammer can more successfully degrade the secondary system performance. Also, from Fig. 2, we see that varying the value of ρ slightly affects the sumEE of the secondary system in each N_s. Also, we see that in the large number of N_s, different energy allocation at the primary users does not affect the sumEE. It means that in the MaMIMO CRN, the jammer does not need any information about the primary system.

According to Fig. 3., for small numbers of secondary base station's antennas the jammer should allocate more energy to jam the data transmission phase especially in lower ρ, and as the number of secondary base station's antennas increases, the jammer's optimal energy allocation ratio tends to a fixed value which is 0.45. This means that, the jammer requires no preprocessing for finding the optimal energy allocation ratio in the case of jamming MaMIMO CRN and only needs to have a constant energy allocation ratio.

[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 and Q, respectively is measured in dB and, therefore, dimensionless.

Experiment 2: In this experiment, we investigate that the value of ζ that obtained from Fig. 3. of experiment 1, is the optimal value for a given number of antennas or not. For this aim, we consider the impact of some values of ζ on sumEE of the secondary system. As shown in Fig. 4., the sumEE of the secondary system with the value of ζ, obtained from Fig. 3. for any given number of antennas at the secondary base station has the most destructive impact on the MaMIMO CRN network and can be used for optimal jamming attacks. Thus, our proposed convexify solution has good performance to solve the optimization problem for design a destructive jamming attack.

Experiment 3: In this experiment, we consider the effect of increasing the jammer's power budget on the sumEE of the secondary system. Fig. 5. shows that by increasing Q, the sumEE of the secondary system tends to zero for any value of ρ. Thus, as expected, if the jammer attacks the MaMIMO CRNs with higher power budgets, it can more effectively degrade the performance of the secondary system. Also, we see that for small values of Q, larger values of ρ results in larger sumEE of the secondary system.

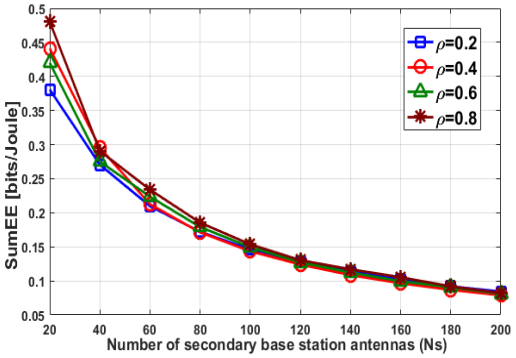

Figure 2. Sum energy efficiency (sumEE) of the secondary system versus the number of secondary base station antennas (N_s) in different values of energy allocation ratio of the primary system (ρ) (with Q=10dB).

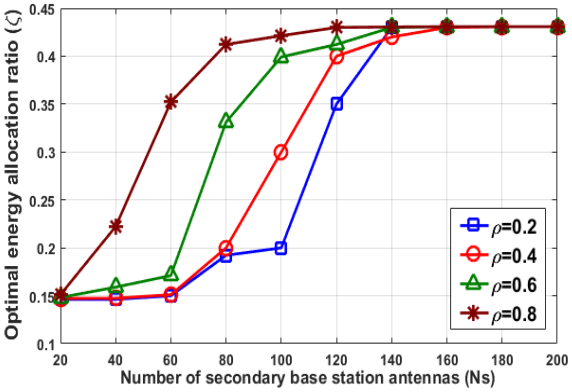

Figure 3. Optimal energy allocation ratio of the jammer (ζ) versus the number of secondary base station antennas (N_s) in different values of energy allocation ratio of the primary system (ρ) (with Q=10dB).

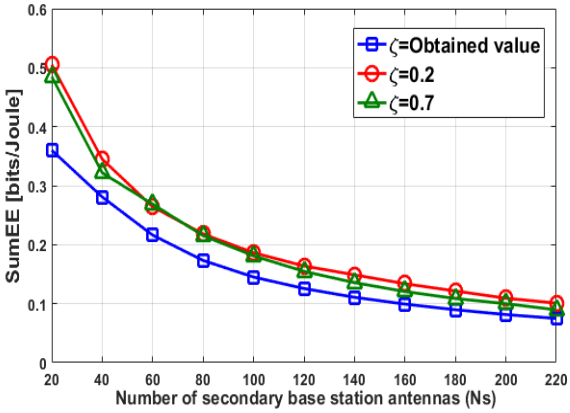

Figure 4. Sum energy efficiency (sumEE) of the secondary system versus the number of secondary base station antennas (N_s) in different values of energy allocation ratio of the jammer (ζ) (with ρ=0.5 and Q=10 dB).

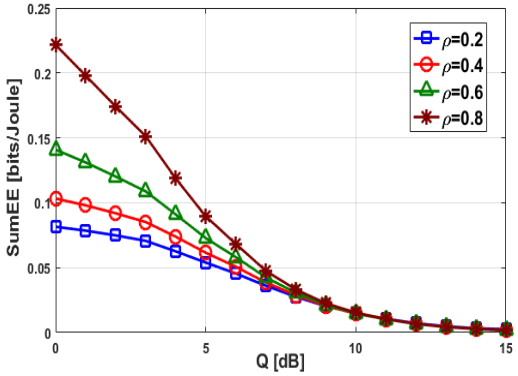

Figure 5. Sum energy efficiency (sumEE) of the secondary system versus the jammer's power budget (Q) in different values of energy allocation ratio of the primary system (ρ) (with N_s=100 and Γ=20 dBw).

VI. Conclusion

In this paper, we investigated the EE performance of a multi-user MaMIMO CR system in the presence of a smart jammer. The jammer caused pilot contamination during the training phase of the secondary system and sent artificial noise during the data transmission phase, and also optimally allocated its power budget to attack the training and data transmission phases of the secondary system. We showed that even with a large number of antennas at the primary and secondary base stations, the jammer could decrease the sumEE of the secondary system. Also, in a large number of antennas at both base stations, the jammer needed no processing to achieve the optimal power allocation and used the constant optimal energy allocation ratio. Furthermore, to have a destructive attack, the jammer did not need to know any information about the primary system. Moreover, if the jammer attacked with a high value of its power budget, it could tent the sumEE to zero and disable the secondary system. Finally, we showed that our proposed convexify method could obtain optimal solutions.

References

[1] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Physical-Layer security in TDD Massive MIMO," IEEE Transactions on Information Theory, vol. 64, no. 11, pp. 7359–7380, Nov. 2018.

[2] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 347–376, 2016.

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

[4] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling Up MIMO: Opportunities and Challenges with Very Large Arrays," IEEE Signal Processing Magazine, vol. 30, no. 1, pp. 40–60, Jan. 2013.

[5] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," IEEE Communications Magazine, vol. 46, pp. 40–48, April. 2008.

[6] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," IEEE Communications Magazine, vol. 53, no. 6, pp. 21-27, 2015.

[7] H. Akhlaghpasand, S. M. Razavizadeh, E. Björnson, and T. T. Do, "Jamming detection in massive MIMO systems," IEEE Wireless Communications Letters, vol. 7, no. 2, pp. 242–245, 2017.

[8] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 210–223, 2017.

[9] H. Akhlaghpasand, E. Bjö rnson, and S. M. Razavizadeh, "Jamming suppression in massive MIMO systems," IEEE Transactions on Circuits and Systems II: Express Briefs, pp. 1–1, 2019.

[10] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," IEEE Transactions on Wireless Communications, vol. 11, no. 3, pp. 903–907, 2012.

[11] H. Pirzadeh, S. M. Razavizadeh, and E. Björnson, "Subverting massive MIMO by smart jamming," IEEE Wireless Communications Letters, vol. 5, no. 1, pp. 20–23, 2015.

[12] R. Chen, J. Park, and J.H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[13] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1342–1363, 2015.

[14] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1023–1043, 2014.

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

[16] 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 Transactions on Vehicular Technology, vol. 67, pp. 1174–1186, 2018.

[17] S. Chaudhari and D. Cabric, "Qos aware power allocation and user selection in massive MIMO underlay cognitive radio networks," IEEE Transactions on Cognitive Communications and Networking, vol. 4, no. 2, pp. 220–231, 2018.

[18] 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.

[19] 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.
[20] G. Amarasuriya and R. F. Schaefer, "Secure transmission in cognitive massive MIMO systems with underlay spectrum sharing," in 2016 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC), pp. 380–384, IEEE, 2016.
[21] H. Al-Hraishawi, G. Amarasuriya, and R. F. Schaefer, "Secure communication in underlay cognitive massive MIMO systems with pilot contamination," in GLOBECOM 2017-2017 IEEE Global Communications Conference, pp. 1–7, IEEE, 2017.
[22] S. Timilsina, G. A. Aruma Baduge and R. F. Schaefer, "Secure communication in spectrum-sharing massive MIMO systems with active eavesdropping," in IEEE Transactions on Cognitive Communications and Networking, vol. 4, no. 2, pp. 390–405, Jun. 2018.
[23] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," IEEE Transactions on Communications, vol. 61, no. 4, pp. 1436–1449, 2013.
[24] S. Boyd and L. Vandenberghe, Convex optimization. Cambridge university press, 2004.

S. Fatemeh Zamanian received her B.Sc. degree in Electrical Engineering from Shahrekord University, Shahrekord, Iran, in 2016, and M.Sc. degree in Secure Communication from Iran University of Science and Technology (IUST), Tehran, Iran, in 2018. She is currently a Ph.D. student at IUST. 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 his B.Sc. degree from 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, 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 is an associate professor and head of communications group at the School of Electrical Engineering at Iran University of Science and Technology (IUST). He also serves as the director of 5G Research Center (5GRC) at IUST. Before joining IUST in 2011, he was with ICT Research Institute (ITRC) as a research assistant professor from 2006 to 2011. He has held several visiting positions at University of Waterloo, Korea University and Chalmers University of Technology. Dr. Razavizadeh received his B.Sc., M.Sc. and Ph.D. degrees all in electrical engineering from IUST in 1997, 2000 and 2006, respectively. His research interests are mainly in the area of Wireless Communication Systems. He is a Senior Member of the IEEE.