ENHANCING THE SECURITY OF MISO-NOMA SWIPT SYSTEM USING COOPERATIVE JAMMING SCHEME

[1]MASTHAN-E-SHAHINA SHAIK, [2]SHAIK .MOBEENA, [3]Y.V.SOWMYA, [4]SHAIK MEHATAB, [5]T.V.YAMINI
[1]Asst. Professor, [2,3,4,5] Final Year, B .Tech
[1]Electronics and Communications Engineering
[2,3,4,5] Geethanjali Institute of Science and Technology, Nellore, India

Abstract: The new era of wireless communication systems requires sophisticated communication techniques that can attain high spectral efficiency (SE) and give massive connectivity between the users. So, Non-orthogonal multiple access (NOMA) and simultaneously wireless information as well as power transfer (SWIPT) are two favorable methods to enhance spectral efficiency and also energy efficiency in CR networks. Here, an Artificial noise-aided beamforming design problems under both perfect and imperfect channel State information (CSI) are studied to enhance the security of a multiple-input single-output NOMA SWIPT system where a realistic non-linear ER model is used. So in order to enhance the security of the primary network, an artificial noise-aided cooperative jamming scheme for MISO-NOMA SWIPT sytem is proposed. The Artificial noise aided beamforming design problems are studied subject to the practical secrecy rate and energy harvesting constraints. Here, the transmission power minimization problems are formulated under the both perfect channel state information (CSI) and the imperfect CSI model. To resolve these non-convex problems, pair of algorithms semi definite relaxation (SDR) and a cost function algorithms are proposed. Our simulation results shown that the proposed scheme flourishes in establishing secure communication and it is envisioned that applying NOMA in CR networks is capable of significantly improving the Spectral efficiency and user connectivity. Finally, the performance of our proposed method is improved than that obtained by OMA.

Index Terms **–Non-orthogonal multiple access, SWIPT, Cognitive radio, Non-linear EH, Physical-layer secrecy, Channel state Information, cooperative jamming scheme. QOE**

I. INTRODUCTION

THE ever-increasing high data rate requirements and for the 5th generation wireless communication systems there is a unprecedented increase of mobile devices to address challenging issues, such as spectrum efficiency and massive connectivity [1], [2]. Non- orthogonal multiple access (NOMA) is a favorable technique to address these challenges [3]. NOMA can give high spectral efficiency (SE) and simultaneously serve multiple users. Unlike orthogonal multiple access (OMA), successive interference cancellation (SIC) method is requisite to diminish the mutual interference between different users owing to the utilization of non–orthogonal resources [4]. NOMA has received increasing attention since it can attain a significant gain in requisites of SE and energy efficiency (EE) compared with OMA [5]-[7].

Recently, another technique called simultaneous wireless information as well as power transfer (SWIPT) has been proposed to extend the operational life time of energy-limited devices, such as energy-limited sensors [8]. Unlike the conventional energy harvesting (EH) methods, such as solar and wind power, Simultaneous information and power transfer can provide steady and controlled power for wireless applications. Mostly ,RF signals not only identifies energy harvesting sources, but also they can transmit the information necessary for transmission. However, due to the propagating nature of NOMA and the dual purpose of RF signals, malicious energy harvesting receivers (EHRs) may be present and interrupt the secret transmitted information signals [11]-[20]. Thus, it is essential to enhance the secrecy rate of NOMA SWIPT systems.

II. LITERATURE SURVEY

In [45]-[50], beamforming design problems using SWIPT has been studied. Recently in [26],[41]-[44], some efforts have been committed to design MISO-NOMA resource. These involvements can be summarized as follows.

In order to increase the security of CRNs, many confined physical-layer techniques have been proposed by using different CSI models [45]-[50]. In [45], a robust beamforming scheme for MISO CRNs in the face of a bounded CSI error model has been proposed. It was exposed that the secrecy rate of the SUs can be significantly increased by by means of various antenna techniques, but it is reduced when the CSI inaccuracy goes up. By developing the connection between multi-antenna aided secure communications and cognitive radio communications, the authors of [46] intended an optimal beamforming design systems for MISO-aided CRNs.

Recently, the authors of [49] and [50] considered the problems of beamforming design in secure MISO multiuser unicast CRNs and of multicast CRNs, respectively. Specifically, in [49], an AN aided beamforming scheme was proposed where there is enhancing the secrecy rate by imposing artificial noise on malicious SUs. In [50], the secrecy rate of SUs was increased under the max-min fairness criterion by providing Cooperation between the primary network and the secondary network. Since energy harvesting has not been considered in [45] and [50], the beamforming schemes proposed in these existing works are unsuitable to CRNs using SWIPT.

Recently, the authors of [27], [36], [52]-[55] studied the resource allocation problems of various CRNs using SWIPT. In [27], a multi-objective optimization framework was applied in MISO-NOMA CRNs with SWIPT. The beamforming scheme, the energy signals and the covariance matrix of AN were jointly optimized. It was shown that there are several tradeoffs in CRNs using SWIPT, such as the tradeoff between the secrecy rate of SUs and the harvested power of EHRs. The authors of [27] only considered the bounded CSI error model. In [36], the authors studied the robust beamforming design problem both under the bounded CSI error model and the probabilistic CSI error model. It was shown that a performance gain can be obtained under the probabilistic CSI error model compared to the bounded CSI error model. Mohjazi et al. [51] extended the robust beamforming design problem into a multi-user MISO CRNs using SWIPT.

By together optimizing the beamforming of CBS and the power splitting factor of the energy-harvesting SUs, the transmission power of the cognitive base station (CBS) can be reduced. So, an optimal pre-coding scheme was adopted for multiple-input multiple-output (MIMO) aided CRNs using SWIPT [52], to further increase the secrecy rate and the harvested power of EHRs,.

III.EXISTING WORK

As an alternative to the conventional cryptographic techniques, physical-layer security exploits the physical characteristics (e.g., multipath fading, propagation delay, etc.) of wireless channels to accomplish secure communications. It was clearly shown that the secrecy rate of wireless communication systems directly rely on the precision of the channel state information (CSI). Moreover, the secrecy rate of SUs in CRNs is more rigorously limited. In order to protect the PUs' quality of service, their transmission power should be controlled. Hence, in order to improve the secrecy rate of SUs, multiple antennas, cooperative relaying, jamming and artificial noise (AN)-aided techniques have been applied. Hence, by designing an optimal resource allocation scheme the secrecy rate can be further improved. Moreover, the secure energy efficiency can be enhanced by using AN-aided techniques and designing the optimal resource allocation schemes. However, the performance gains attained by using these techniques are significantly influenced by the accuracy of CSI. Hence it becomes a challenge to obtain accurate CSI, especially for NOMA SWIPT systems. Thus, it is imperative to design resource allocation schemes under the imperfect CSI. Plentiful investigations have been conducted for improving the security of the conventional OMA systems by using linear EH model. In OMA,

1. The interference is very high.
2. Consumes more power.
3. Secrecy rate and efficiency is very low.

Considering all the disadvantages associative with the existing method, we came up with a new method.

IV.PROPOSED METHOD

In order to overcome the drawbacks of existing work and improve the security of primary user's (PU's),MISO-NOMA SWIPT systems using co-operative jamming scheme is proposed.

1) The AN-aided cooperative jamming scheme is proposed for MISO-NOMA CRNs using SWIPT in order to improve the security of the primary network. By using this proposed scheme, the CBS sends a jamming signal to collaborate with the primary base station (PBS) for increasing the security of the PUs. As a result, the secondary network is approved to access the frequency bands of the primary network and offer SWIPT services both for the SUs and for the EHRs in the secondary network. Furthermore, the covariance matrix of the jamming signals transmitted at CBS and the beamforming of the CBS and the PBS are jointly optimized.

2) Beamforming design problems are deliberate under both the perfect CSI model and the bounded CSI error model. In contrast to the works that only an eaves dropper was considered in the NOMA system [26], [41]-[44], we consider a more general scenario, where multiple malicious EHRs exist. The total transmission power is minimized by collectively optimizing the transmission beamforming vectors of both the PBS and the CBS as well as the covariance matrix of the jamming signal transmitted at the CBS For solving these challenging non-convex problems, pair of algorithms are proposed. One of them based on semidefinite relaxation (SDR) while the other is based on a carefully conceived cost function.

3) Our model results show that the proposed AN-aided cooperative scheme can reduce the transmission power required in MISO-NOMA CRNs using SWIPT. Moreover, when CSI is imperfect, it is shown that the performance achieved by NOMA is proven to be better than obtained by OMA. Furthermore, our simulation results also show that the cost function algorithm outperforms the algorithm based on using SDR.

AN- AIDED COOPERATIVE JAMMING SCHEME

The secure energy efficiency can be enhanced by using AN-aided techniques. AN-aided cooperative jamming scheme is proposed for MISO-NOMA CRN'S using SWIPT to increase the security of primary network.

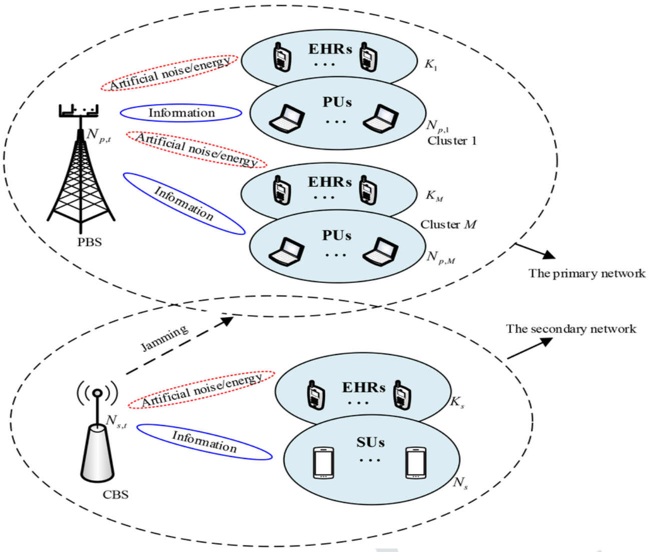
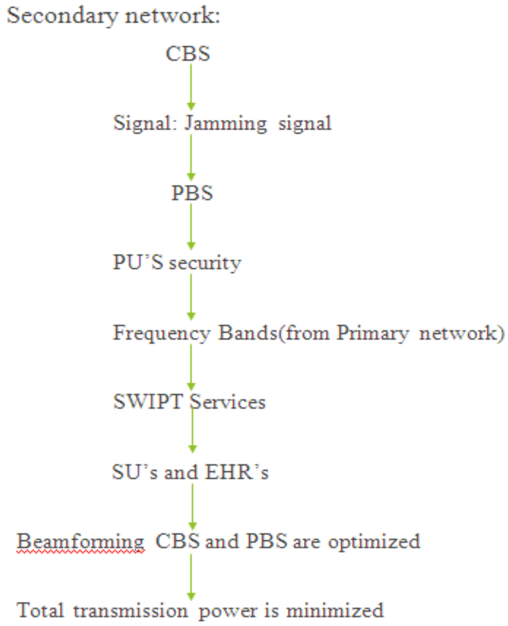


Fig 1:System Model



A. Main Contributions

In this system model, we will describe the network model and security metrics in the downlink MISO NOMA using SWIPT systems under a practical non-linear EH model. In [26], [41]-[44], only one eavesdropper has been considered in the designed NOMA systems and resource allocation schemes have been proposed. In this paper, the beamforming design problems are studied.

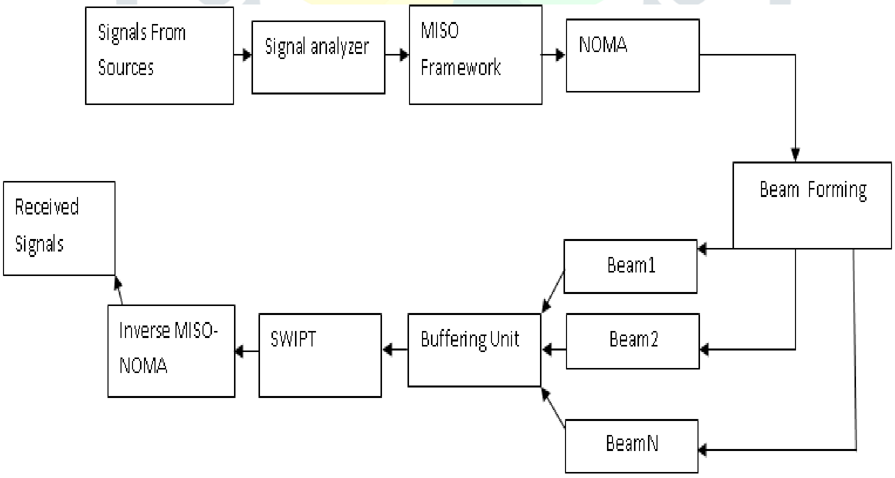


Fig.2: Schematic Block Overview of Proposed System

B.Network Model

Our downlink MISO NOMA CR network using SWIPT is shown in Fig. 1 and Fig.2. In the primary network, unicast-multicast communications are exploited since they can provide high SE and massive connectivity. This scenario is extensively encountered, for example in Internet of Things, wireless sensor networks and the cellular networks [49], [50]. Specifically, the PBS sends different confidential information-bearing signals to the PUs in the different clusters. And the primary users in each individual multicast cluster obtain the same confidential information-bearing signal from the PBS. In the secondary network, the NOMA is applied since it can attain high power transfer efficiency and SUs can perform SIC [20], [21]. In this case, the PBS broadcasts the information to the PUs in Mclusters and simultaneously transfers energy to EHRs. In the secondary network, the CBS provide SWIPT service to Ks EHRs and to Ns SUs by using NOMA.

C. Security Metrics

Let $y_{p,m,i}$ denote the signal received at the ith PU in the mth cluster, $y_{s,j}$ represent the signal received at the jth SU, $y_{e,m,k}$ denote the EH signal received at the kth EHR in the mth cluster and ye,l represent the EH signal received at the lth EHR in the secondary network, respectively, where i∈Np,m, Np,m = {1,2,⋯ ,Np,m}; j ∈Ns, Ns = {1,2,⋯ ,Ns} and l ∈Ks, Ks = {1,2,⋯ ,Ks}. These signals are respectively expressed as

$$\begin{aligned} y_{p,m,i} =& \mathbf{h}^{\dagger}_{p,m,i}\left[\sum_{m=1}^{M}(\mathbf{w}_{p,m}s_{p,m}+\mathbf{v}_{p,m})\right] \\ &+\mathbf{f}^{\dagger}_{s,m,i}\left(\sum_{j=1}^{N_s}\mathbf{w}_{s,j}s_{s,j}+\mathbf{v}_s\right)+n_{p,m,i}, \qquad \text{(1a)} \\ y_{s,j} =& \mathbf{q}^{\dagger}_{p,j}\left[\sum_{m=1}^{M}(\mathbf{w}_{p,m}s_{p,m}+\mathbf{v}_{p,m})\right] \\ &+\mathbf{h}^{\dagger}_{s,j}\left(\sum_{j=1}^{N_s}\mathbf{w}_{s,j}s_{s,j}+\mathbf{v}_s\right)+n_{s,j}, \qquad \text{(1b)} \end{aligned}$$

$$\begin{aligned} y_{e,m,k} =& \mathbf{g}^{\dagger}_{e,m,k}\left[\sum_{m=1}^{M}(\mathbf{w}_{p,m}s_{p,m}+\mathbf{v}_{p,m})\right] \\ &+\mathbf{f}^{\dagger}_{e,m,k}\left(\sum_{j=1}^{N_s}\mathbf{w}_{s,j}s_{s,j}+\mathbf{v}_s\right), \qquad \text{(1c)} \\ y_{e,l} =& \mathbf{q}^{\dagger}_{e,l}\left[\sum_{m=1}^{M}(\mathbf{w}_{p,m}s_{p,m}+\mathbf{v}_{p,m})\right] \\ &+\mathbf{g}^{\dagger}_{e,l}\left(\sum_{j=1}^{N_s}\mathbf{w}_{s,j}s_{s,j}+\mathbf{v}_s\right), \qquad \text{(1d)} \end{aligned}$$

where $h_{p,m,i}$∈ CNp,t×1 and $f_{s,m,i}$∈ CNs,t×1 are the channel vector between the PBS and the ith PU as well as that between the CBS and the ith PU in the mth cluster, respectively; $q_{p,j}$∈ CNp,t×1 and $h_{s,j}$∈ CNs,t×1 denote the channel vector between the PBS and the jth SU as well as that between the CBS and the jth SU, respectively. Furthermore, $g_{e,m,k}$∈ CNp,t×1 and $f_{e,m,k}$∈ CNs,t×1 are the channel vector between the PBS and the kth EHR and that between the CBS and the jth EHR in the mth cluster, respectively; $q_{e,l}$∈ CNp,t×1 and $g_{e,l}$∈ CNs,t×1 represent the channel vector between the PBS and the lth EHR and that between the CBS and the lth EHR in the secondary network, respectively. Still regarding to (1a), $s_{p,m}$∈ C1×1 and $w_{p,m}$∈ CNp,t×1 are the confidential information-bearing signal for the PUs in the mth cluster and the corresponding beamforming vector, respectively.

Furthermore, $s_{s,j}$∈ C1×1 and $w_{s,j}$∈ CNs,t×1 represent the confidential information-bearing signal delivered for the jth SU and the corresponding beamforming vector, respectively. Additionally, vp,m and vs denote the noise vector artificially generated by the PBS and the CBS. It is assumed that E[|sp,m|2] = 1 and E[|ss,j|2] = 1. It is also assumed that vp,m∼ CN (0,Σp,m) and vs ∼ CN (0,Σs), where Σp,m and Σs are the AN covariance matrix. In (1), np,m,i∼CN(0,σ2p,m,i)and ns,j∼CN(0,σ2s,j)respectively denote the complex Gaussian noise at the ith PU in the mth cluster and the lth SU. The secrecy rate of the ith PU in the mth cluster and the secrecy rate of the jth SU, denoted by Rp,m,i and Rs,j, respectively, can be expressed as hp,m,ih†p,m,i; Fs,m,i = fs,m,if†s,m,i; Qp,j = qp,jq†p,j; Hs,j = hs,jh†s,j; Ge,m,k = ge,m,kg†e,m,k;Fe,m,k = fe,m,kf†e,m,k; Qe,l = qe,lq†e,l and Ge,l = ge,lg†e,l. The expressions of Γp,m,i, Γe,m,k, Γs,j, Λe,l,j, Λs,j,z and Λs,l,j are given in (3). Without loss of generalization, it is assumed that ‖h1‖ ≤ ‖h2‖ ≤ ⋯ ≤ ‖hNs‖. Similar to [12], [27]-[28], it is assumed furthermore that the EHR in the secondary network has decoded SU j's message before it decodes the SU i's message, j <i. This over-estimates the interception ability of EHRs and results in the worst-case secrecy rate of the SUs.

$$R_{p,m,i} = \left[\log\left(\frac{\Gamma_{p,m,i}}{\Gamma_{p,m,i} - \mathrm{Tr}\left(\mathbf{W}_{p,m}\mathbf{H}_{p,m,i}\right)}\right) - \max_{k\in\mathcal{K}_m} \log\left(\frac{\Gamma_{e,m,k} + \sigma^2_{e,m,k}}{\Gamma_{e,m,k} - \mathrm{Tr}\left(\mathbf{W}_{p,m}\mathbf{G}_{e,m,k}\right) + \sigma^2_{e,m,k}}\right)\right]^+, \quad (2a)$$

$$R_{s,j} \begin{cases} = \left[\log_2\left(\frac{\Gamma_{s,j}}{\Gamma_{s,j} - \mathrm{Tr}(\mathbf{W}_{s,j}\mathbf{H}_{s,j})}\right) - \max_{l\in\mathcal{L}} \log_2\left(\frac{\Lambda_{e,l,j}}{\Lambda_{s,l,j} - \mathrm{Tr}(\mathbf{W}_{s,j}\mathbf{G}_{e,l})}\right)\right]^+, \text{if } j = N_s, \\ = \left[\min_{z\in\{j,j+1,N_s\}} \log_2\left(\frac{\Lambda_{s,j,z}}{\Lambda_{s,j,z} - \mathrm{Tr}(\mathbf{W}_{s,j}\mathbf{H}_{s,z})}\right) - \max_{l\in\mathcal{L}} \log_2\left(\frac{\Lambda_{s,l,j}}{\Lambda_{s,l,j} - \mathrm{Tr}(\mathbf{W}_{s,j}\mathbf{G}_{e,l})}\right)\right]^+, \text{otherwise}. \end{cases} \quad (2b)$$

where $\mathbf{W}_{p,m} = \mathbf{w}_{p,m}\mathbf{w}^\dagger_{p,m}$; $\mathbf{W}_{s,j} = \mathbf{w}_{s,j}\mathbf{w}^\dagger_{s,j}$; $\mathbf{H}_{p,m,i} =$

hp,m,ih†p,m,i; Fs,m,i = fs,m,if†s,m,i; Qp,j = qp,jq†p,j; Hs,j = hs,jh†s,j; Ge,m,k = ge,m,kg†e,m,k; Fe,m,k = fe,m,kf†e,m,k; Qe,l = qe,lq†e,l and Ge,l = ge,lg†e,l. The expressions of Γp,m,i, Γe,m,k, Γs,j, Λe,l,j, Λs,j,z and Λs,l,j are given in (3). Without loss of generality, it is assumed that ‖h1‖ ≤ ‖h2‖ ≤ ⋯ ≤ ‖hNs‖. Similar to [12], [27]-[28], it is assumed furthermore that the EHR in the secondary network has decoded SU j's message before it decodes the SU i's message, j <i. This over-estimates the interception capability of EHRs and worst-case secrecy rate of the SUs is provided as result. This conservative assumption was also used in [27]-[28].

$$\Gamma_{p,m,i} = \mathrm{Tr}\left\{\left[\sum_{m=1}^{M}\left(\mathbf{W}_{p,m} + \mathbf{\Sigma}_{p,m}\right)\right]\mathbf{H}_{p,m,i} + \left(\sum_{j=1}^{N_s}\mathbf{W}_{s,j} + \mathbf{\Sigma}_s\right)\mathbf{F}_{s,m,i}\right\} + \sigma^2_{p,m,i}, \quad (3a)$$

$$\Gamma_{e,m,k} = \mathrm{Tr}\left\{\left[\sum_{m=1}^{M}\left(\mathbf{W}_{p,m} + \mathbf{\Sigma}_{p,m}\right)\right]\mathbf{G}_{e,m,k} + \left(\sum_{j=1}^{N_s}\mathbf{W}_{s,j} + \mathbf{\Sigma}_s\right)\mathbf{F}_{e,m,k}\right\}, \quad (3b)$$

$$\Gamma_{s,j} = \mathrm{Tr}\left\{\left[\sum_{m=1}^{M}\left(\mathbf{W}_{p,m} + \mathbf{\Sigma}_{p,m}\right)\right]\mathbf{Q}_{p,j} + \left(\mathbf{W}_{s,j} + \mathbf{\Sigma}_s\right)\mathbf{H}_{s,j}\right\} + \sigma^2_{s,j}, \quad (3c)$$

$$\Lambda_{e,l,j} = \mathrm{Tr}\left[\left[\sum_{m=1}^{M}\left(\mathbf{W}_{p,m} + \mathbf{\Sigma}_{p,m}\right)\right]\mathbf{Q}_{e,l} + \left(\mathbf{W}_{s,j} + \mathbf{\Sigma}_s\right)\mathbf{G}_{e,l}\right] + \sigma^2_{e,l}, \quad (3d)$$

$$\Lambda_{s,j,z} = \mathrm{Tr}\left\{\left[\sum_{m=1}^{M}\left(\mathbf{W}_{p,m} + \mathbf{\Sigma}_{p,m}\right)\right]\mathbf{H}_{p,z} + \left(\sum_{u=j}^{N_s}\mathbf{W}_{s,u} + \mathbf{\Sigma}_s\right)\mathbf{H}_{s,z}\right\} + \sigma^2_{s,z}, \quad (3e)$$

$$\Lambda_{s,l,j} = \mathrm{Tr}\left\{\left[\sum_{m=1}^{M}\left(\mathbf{W}_{p,m} + \mathbf{\Sigma}_{p,m}\right)\right]\mathbf{Q}_{e,l} + \left(\sum_{v=j}^{N_s}\mathbf{W}_{s,v} + \mathbf{\Sigma}_s\right)\mathbf{G}_{e,l}\right\} + \sigma^2_{e,l}. \quad (3f)$$

D.Non-linear Energy Harvesting Model

In this paper, a practical non-linear EH model is adopted. According to [55]-[57], the harvesting power of EHRs, denoted by ΦE,A, can be formulated as:

$$\Phi_{e,\Lambda} = \left(\frac{\psi_{e,\Lambda} - P^{\max}_{e,\Lambda}\Psi_{e,\Lambda}}{1-\Psi_{e,\Lambda}}\right), \qquad (4a)$$

$$\psi_{e,\Lambda} = \frac{P^{\max}_{e,\Lambda}}{1+\exp\left[-a_{e,\Lambda}\left(\Gamma_{e,\Lambda}-b_{e,\Lambda}\right)\right]}, \qquad (4b)$$

$$\Psi_{e,\Lambda} = \frac{1}{1+\exp\left(a_{e,\Lambda}b_{e,\Lambda}\right)}, \qquad (4c)$$

where *A* is the set of EHRs in the primary network and the secondary network, namely, *A* = *A*1 ∪*A*2, and *A*1 = ∪*m*2*MKm*,*m*∈ *M*, *A*2 = *Ks*;*ae;*A and *be;*A represent parameters that reflect the circuit specifications, such as the resistance, the capacitance and diode turn-on voltage Furthermore, *P*max*e;*A is the maximum harvested power of EHRs when the EH circuit is saturated. In (4b), Γ*e;*A is the RF power received at EHRs. Furthermore, Γ*e;*A = Γ*e;m;k* when the EHRs are in the primary network and Γ*e;*A = Λ*s;l;*1 −*σ*2 *e;l*when the EHRs are in the secondary network. Note that the noise power is ignored, since it is very small compared to the RF signal power.

AN-AIDED BEAMFORMING DESIGN UNDER PERFECT CSI

AN-aided beamforming design is formulated in MISO NOMA CRN's using SWIPT under perfect CSI. The CSI between the two networks can be obtained with the collaboration between the primary and secondary network. Under perfect CSI, the power minimization problem is formulated as follows:

$$\mathrm{P}_1: \min_{\substack{\mathbf{W}_{p,m},\Sigma_{p,m}\\ \mathbf{W}_{s,j},\Sigma_s}} \mathrm{Tr}\left[\sum_{m=1}^{M}\left(\mathbf{W}_{p,m}+\mathbf{\Sigma}_{p,m}\right)+\sum_{j=1}^{N_s}\mathbf{W}_{s,j}+\mathbf{\Sigma}_s\right] \qquad (5a)$$

s.t.

$$C1: R_{p,m,i} \geq \gamma_{p,m,i}, i \in \mathcal{N}_{p,m}, m \in \mathcal{M}, \qquad (5b)$$

$$C2: R_{s,j} \geq \gamma_{s,j}, j \in \mathcal{N}_s, \qquad (5c)$$

$$C3: \Phi_{e,A_1} \geq \zeta_{e,A_1}, k \in \mathcal{K}_m, m \in \mathcal{M}, \qquad (5d)$$

$$C4: \Phi_{e,A_2} \geq \zeta_{e,A_2}, l \in \mathcal{K}_s, \qquad (5e)$$

$$C5: \mathrm{Rank}\left(\mathbf{W}_{p,m}\right)=1, \mathrm{Rank}\left(\mathbf{W}_{s,j}\right)=1 \qquad (5f)$$

$$C6: \mathbf{W}_{p,m} \succeq \mathbf{0}, \mathbf{W}_{s,j} \succeq \mathbf{0}. \qquad (5g)$$

In (5), *γp;m;I* and *γs;j*are the minimum secrecy rate requirements of the *i*th PU in the *m*th cluster and of the *j*th SU; *ζe;A*1 and *ζe;A*2 are the minimum EH requirements of EHRs in the primary and the secondary network. The constraints*C*1 and *C*2 are imposed to promise the secrecy rates of the PUs and SUs, respectively; the constraints *C*3 and *C*4 are the constraints that can gratify the harvested power requirements of the EHRs in both the primary and secondary networks; and the constraint *C*5 is the rank-one constraint which is essential for obtaining rank-one beamforming. Note that the optimization objective of P1 can be identified as the weight objective of a multiple-objective optimization problem that has two optimization objectives (e.g., the transmission power of the PBS and the CBS) with the same weight. Due to the constraints *C*1, *C*2 and *C*5, P1 is non-convex and difficult to solve. In order to solve this problem, a pair of suboptimal schemes are proposed as follows.

Suboptimal Solution Based on SDR

To address the constraint *C*1, an auxiliary variable *τm*, *m* ∈*M*, is introduced. Then, the constraint *C*1 can be equivalentlyexpressed as

$$\log\left\{\frac{\Gamma_{p,m,i}}{\left[\Gamma_{p,m,i}-\mathrm{Tr}\left(\mathbf{W}_{p,m}\mathbf{H}_{p,m,i}\right)\right]\tau_m}\right\} \geq \gamma_{p,m,i}, \qquad (6a)$$

$$\log\left\{\frac{\Gamma_{e,m,k}+\sigma^2_{E,m,k}}{\left[\Gamma_{e,m,k}-\mathrm{Tr}\left(\mathbf{W}_{p,m}\mathbf{G}_{e,m,k}\right)+\sigma^2_{e,m,k}\right]\tau_m}\right\} \leq 1, \qquad (6b)$$

where *k* ∈ *Km* and *m* ∈ *M*. Using successive convex approximation (SCA), the constraints given by (6a) and (6b) can be approximated as (7) and (8)

$$\exp\left(\alpha_{p,m,i} + \beta_m - \lambda_{p,m,i}\right) \le 2^{-\gamma_{p,m,i}}, \quad (7a)$$
$$\Gamma_{p,m,i} - \mathrm{Tr}\left(\mathbf{W}_{p,m}\mathbf{H}_{p,m,i}\right) \le \exp\left(\widetilde{\alpha}_{p,m,i}\right)\left(\alpha_{p,m,i} - \widetilde{\alpha}_{p,m,i} + 1\right), \quad (7b)$$
$$\tau_m \le \exp\left(\widetilde{\beta}_m\right)\left(\beta_m - \widetilde{\beta}_m + 1\right), \quad (7c)$$
$$\Gamma_{p,m,i} \ge \exp\left(\lambda_{p,m,i}\right), \quad (7d)$$

$$\exp\left(\mu_{e,m,k} - \rho_{e,m,k} - \delta_m\right) \le 1, \quad (8a)$$
$$\Gamma_{e,m,k} + \sigma^2_{e,m,k} \le \exp\left(\widetilde{\mu}_{e,m,k}\right)\left(\mu_{e,m,k} - \widetilde{\mu}_{e,m,k} + 1\right), \quad (8b)$$
$$\Gamma_{e,m,k} - \mathrm{Tr}\left(\mathbf{W}_{p,m}\mathbf{G}_{e,m,k}\right) + \sigma^2_{e,m,k} \ge \exp\left(\rho_{e,m,k}\right), \quad (8c)$$
$$\tau_m \ge \exp\left(\delta_m\right), \quad (8d)$$

secrecy rate constraint of the N_sth SU can be formulated as

$$\exp\left(\alpha_{s,N_s} + \beta_{s,N_s} - \lambda_{s,N_s}\right) \le 2^{-\gamma_{s,N_s}}, \quad (9a)$$
$$\Gamma_{s,N_s} - \mathrm{Tr}\left(\mathbf{W}_{s,N_s}\mathbf{H}_{S,N_s}\right) \le \exp\left(\widetilde{\alpha}_{s,N_s}\right)\left(\alpha_{s,N_s} - \widetilde{\alpha}_{s,N_s} + 1\right), \quad (9b)$$
$$\tau_{s,N_s} \le \exp\left(\widetilde{\beta}_{s,N_s}\right)\left(\beta_{s,N_s} - \widetilde{\beta}_{s,N_s} + 1\right), \quad (9c)$$
$$\Gamma_{s,N_s} \ge \exp\left(\lambda_{s,N_s}\right), \quad (9d)$$
$$\exp\left(\mu_{e,l} - \rho_{s,l} - \omega_{s,N_s}\right) \le 1, l \in \mathcal{K}_s, \quad (9e)$$
$$\Lambda_{e,l,N_s} \le \exp\left(\widetilde{\mu}_{e,l}\right)\left(\mu_{E,l} - \widetilde{\mu}_{e,l} + 1\right), \quad (9f)$$
$$\Lambda_{e,l,N_s} - \mathrm{Tr}\left(\mathbf{W}_{s,N_s}\mathbf{G}_{e,l}\right) \ge \exp\left(\rho_{s,l}\right), \quad (9g)$$
$$\tau_{s,N_s} \ge \exp\left(\omega_{s,N_s}\right), \quad (9h)$$

where $\alpha p;m;i$, βm, $\lambda p;m;i$, $\mu e;m;k$, $\rho e;m;k$, and $\delta m$are auxiliary variables. Furthermore, e$\alpha p;m;i$, eβm and e$\mu e;m;k$ are approximate values, and they are equal to $\alpha p;m;i$, βm and $\mu e;m;k$, respectively, when the constraints are tight. When j = 1,2,··· ,Ns−1, the secrecy rate constraint of the jth SU can be formulated as

$$\kappa_j - \omega_j 2^{\gamma_{s,j}} \ge 0, \quad (10a)$$
$$\exp\left(\alpha_{s,j,z} + \xi_{s,j} - \lambda_{s,j,z}\right) \le 1, z \in \{j, j+1, N_s\}, \quad (10b)$$
$$\Lambda_{s,j,z} - \mathrm{Tr}\left(\mathbf{W}_{s,j}\mathbf{H}_{s,z}\right) \le \exp\left(\widetilde{\alpha}_{s,j,z}\right)\left(\alpha_{s,j,z} - \widetilde{\alpha}_{s,j,z} + 1\right), \quad (10c)$$
$$\kappa_j \le \exp\left(\widetilde{\xi}_{s,j}\right)\left(\xi_{s,j} - \widetilde{\xi}_{s,j} + 1\right), \quad (10d)$$
$$\Lambda_{s,j,z} \ge \exp\left(\lambda_{s,j,z}\right), \quad (10e)$$
$$\exp\left(\mu_{e,l,j} - \rho_{s,l,j} - \tau_{s,j}\right) \le 1, \quad (10f)$$
$$\Lambda_{s,l,j} \le \exp\left(\widetilde{\mu}_{e,l,j}\right)\left(\mu_{e,l,j} - \widetilde{\mu}_{E,l,j} + 1\right), \quad (10g)$$
$$\Lambda_{s,l,j} - \mathrm{Tr}\left(\mathbf{W}_{s,j}\mathbf{G}_{e,l}\right) \ge \exp\left(\rho_{s,l,j}\right), \quad (10h)$$
$$\omega_j \ge \exp\left(\tau_{s,j}\right), \quad (10i)$$

where κj, ωj, αs,j,z, ξs,j, λs,j,z, μe,l,j, ρs,l,j and τs,j denote auxiliary variables. Furthermore, e αs,j,z, e ξs,j and e μe,l,j are approximate values and equal to αs,j,z, ξs,j and μe,l,j, respectively, when the constraints are tight. Constraints C3 and C4 can be equivalently expressed as

$$\Gamma_{e,A} \geq b_{e,A} - \frac{1}{a_{e,A}} \ln \left\{ \frac{P_{e,A}^{\max}}{\zeta_{e,A}\left(1-\Psi_{e,A}\right) + P_{e,A}^{\max}\Psi_{e,A}} - 1 \right\}. \tag{11}$$

Based on (7) and (11), using SDR, P_1 can be solved by iteratively solving P_2, given as

$$P_2: \min_{\Xi} \ \mathrm{Tr}\left[\sum_{m=1}^{M} \left(\mathbf{W}_{p,m} + \mathbf{\Sigma}_{p,m}\right) + \sum_{j=1}^{N_s} \mathbf{W}_{s,j} + \mathbf{\Sigma}_s \right] \tag{12a}$$

$$\text{s.t. } C6, (7) - (11), \tag{12b}$$

SDR-Based ALGORITHM

SDR-Based algorithm is a powerful computationally efficient approximation technique for a host of very difficult optimization problems. SDR can be used to provide an accurate approximation and provides an precise optimal solution to the original problems.

TABLE I: The SCA-based algorithm

Algorithm 1: The SCA-based algorithm for P_1

1: **Setting:**
$\gamma_{p,m,i}$, $\gamma_{s,j}$ $\Upsilon_{m,i}$, ζ_{e,A_1}, ζ_{e,A_1}, $i \in \mathcal{N}_{p,m}$, $k \in \mathcal{K}_m$, $m \in \mathcal{M}$ $l \in \mathcal{K}_s$ and the tolerance error ϖ;
2: **Initialization:**
The iterative number $n = 1$, $\widetilde{\alpha}_{p,m,i}^n$, $\widetilde{\beta}_m^n$, $\widetilde{\mu}_{e,m,k}^n$, $\widetilde{\alpha}_{s,N_s}^n$, $\widetilde{\beta}_{s,N_s}^n$, $\widetilde{\mu}_{e,l}^n$, $\widetilde{\alpha}_{s,j,z}^n$, $\widetilde{\xi}_{s,j}^n$ and $\widetilde{\mu}_{e,l,j}^n$ and P_{opt}^n;
3: **Repeat:**
solve P_2 by using CVX for the given approximate values;
obtain $\widetilde{\alpha}_{p,m,i}^{n+1}$, $\widetilde{\beta}_m^{n+1}$, $\widetilde{\mu}_{e,m,k}^{n+1}$, $\widetilde{\alpha}_{s,N_s}^{n+1}$, $\widetilde{\beta}_{s,N_s}^{n+1}$, $\widetilde{\mu}_{e,l}^{n+1}$, $\widetilde{\alpha}_{s,j,z}^{n+1}$, $\widetilde{\xi}_{s,j}^{n+1}$ and $\widetilde{\mu}_{e,l,j}^{n+1}$ and P_{opt}^{n+1};
if Rank $(\mathbf{W}_{p,m}) = 1$ and Rank $(\mathbf{W}_{s,j}) = 1$
Obtain optimal $\mathbf{W}_{p,m}$ and $\mathbf{W}_{s,j}$;
else
Obtain suboptimal $\mathbf{W}_{p,m}$ and $\mathbf{W}_{s,j}$;
end
update the iterative number $n = n + 1$;
calculate the total transmit power P_{opt}^n;
if $\left|P_{opt}^n - P_{opt}^{(n-1)}\right| \leq \varpi$
break;
end;
4: **Obtain resource allocation:**
$\mathbf{W}_{p,m}$, $\mathbf{W}_{s,j}$, $\mathbf{\Sigma}_{p,m}$ and $\mathbf{\Sigma}_s$.

AN-AIDED BEAMFORMING DESIGN UNDER IMPERFECTCSI

AN-aided beamforming design is formulated in MISO-NOMA using SWIFT system under imperfect CSI. The CSI between the two networks are imperfect due to the limited co-operation between primary and secondary network

$$\mathbf{q}_{e,l} = \overline{\mathbf{q}}_{e,l} + \Delta\mathbf{q}_{e,l}, l \in \mathcal{K}_s, \tag{13a}$$

$$\mathbf{\Psi}_{e,l} \triangleq \left\{ \Delta\mathbf{q}_{e,l} \in C^{N_{p,t}\times 1} : \Delta\mathbf{q}_{e,l}^{\dagger}\Delta\mathbf{q}_{e,l} \leq \mathcal{E}_{e,l}^2 \right\}, \tag{13b}$$

while the channel vector $\mathbf{f}_{e,m,k}$ can be expressed as

$$\mathbf{f}_{e,m,k} = \overline{\mathbf{f}}_{e,m,k} + \Delta\mathbf{f}_{e,m,k}, m \in M, k \in \mathcal{K}_m, \tag{14a}$$

$$\mathbf{\Psi}_{e,m,k} \triangleq \left\{ \Delta\mathbf{f}_{e,m,k} \in C^{N_{s,t}\times 1} : \Delta\mathbf{f}_{e,m,k}^{\dagger}\Delta\mathbf{f}_{e,m,k} \leq \mathcal{E}_{e,m,k}^2 \right\}, \tag{14b}$$

where **q***e;l* and **f** *e;m;k* are the estimates of **q***e;l* and **f***e;m;k*, respectively; *e;l*and *e;m;k* represent the uncertainty regions of the channel vectors **q***e;l* and **f***e;m;k*, respectively; Δ**q***e;l* and Δ**f***e;m;k* denote the channel estimation errors of **q***e;l* and **f***e;m;k*, *$e;l* and *$e;m;k* are the radii of the uncertainty regions *e;l* and *e;m;k*, respectively. Based on the bounded error models for **q***e;l* and **f***e;m;k*, the power minimization problem subject to the constraints on the secrecy rates of the PUs and the SUs as well as on the harvested power requirements of EHRsP5 can be formulated as:

$$\min_{\substack{\mathbf{W}_{p,m},\boldsymbol{\Sigma}_{p,m}\\ \mathbf{W}_{s,j},\boldsymbol{\Sigma}_s}} \operatorname{Tr}\left[\sum_{m=1}^{M}\left(\mathbf{W}_{p,m}+\boldsymbol{\Sigma}_{p,m}\right)+\sum_{j=1}^{N_s}\mathbf{W}_{s,j}+\boldsymbol{\Sigma}_s\right] \quad (15a)$$

s.t.

$$C6: R_{p,m,i} \geq \gamma_{p,m,i}, i \in \mathcal{N}_{p,m}, m \in \mathcal{M}, \forall \Delta\mathbf{f}_{e,m,k} \in \boldsymbol{\Psi}_{e,m,k}, \quad (15b)$$

$$C7: R_{s,j} \geq \gamma_{s,j}, j \in \mathcal{N}_s, \forall \Delta\mathbf{q}_{e,l} \in \boldsymbol{\Psi}_{e,l}, \quad (15c)$$

$$C8: \Phi_{e,A_1} \geq \zeta_{e,A_1}, k \in \mathcal{K}_m, m \in \mathcal{M}, \forall \Delta\mathbf{f}_{e,m,k} \in \boldsymbol{\Psi}_{e,m,k}, \quad (15d)$$

$$C9: \Phi_{e,A_2} \geq \zeta_{e,A_2}, l \in \mathcal{K}_s, \forall \Delta\mathbf{q}_{e,l} \in \boldsymbol{\Psi}_{e,l}, \quad (15e)$$

$$C10: \operatorname{Rank}\left(\mathbf{W}_{p,m}\right)=1, \operatorname{Rank}\left(\mathbf{W}_{s,j}\right)=1 \quad (15f)$$

$$C11: \mathbf{W}_{p,m} \succeq \mathbf{0}, \mathbf{W}_{s,j} \succeq \mathbf{0}. \quad (15g)$$

The problem P5 is more challenging to solve due to the infinite inequality constraints imposed by the uncertain regions, *e;l*and*e;m;k*and owing to the non-convex constraints *C*6- *C*10.

Suboptimal Solution Based on Cost Function

In order to make P5 tractable, the *S*-Procedure of [45] is applied. *Lemma 2* (*S-Procedure*) [45]: Let *fi* (**z**) = **z***y***A***i***z**+ 2 Re{**b***yi***z**}+ *ci*, *i* ∈{1, 2}, where **z** ∈**C***N*_1, **A***i* ∈H*N*,**b***i*∈**C***N*_1 and *ci* ∈R. Then, the expression *f*1 (**z**) ≤ 0 ⇒*f*2 (**z**) ≤ 0 holds if and only if there exists a ς ≥ 0 such that we have:

$$\varsigma\begin{bmatrix}\mathbf{A}_1 & \mathbf{b}_1\\ \mathbf{b}_1^{\dagger} & c_1\end{bmatrix}-\begin{bmatrix}\mathbf{A}_2 & \mathbf{b}_2\\ \mathbf{b}_2^{\dagger} & c_2\end{bmatrix}\succeq 0, \quad (16)$$

provided that there exists a vector b**z** so that we have *fi* (b**z**) <0.Using Lemma 2 and SCA, the constraint *C*6 of P5 can be approximated as (20) at the top of the next page. In (20), *λe;m;k*≥ 0 and *ue;m;k*≥ 0 are slack variables while *θe;m;k* and *oe;m;k* are auxiliary variables. Similarly, the constraint *C*7is approximated as follows. When *j* = *Ns*, one has (21) at the top of the next page and when *j* = 1, 2, ・・・,*Ns*− 1, the secrecy rate constraint of the *j*th SU can be approximated as (22) at the top of the next page. Where *ωe;l*≥ 0, *κe;l*≥ 0, *τ* ≥ 0 and *ηe;l*≥ 0 are slack variables. The constraints *C*8 and *C*9 can be equivalently expressed as (23) at the top of the next two pages. In (23), *χe;m;k*≥ 0 and *φe;l*≥ 0 are slack variables. By using (20)-(23), P5 can be solved by iteratively solving P6, given as

$$\mathrm{P}_6: \min_{\Xi_1} f\left(\mathbf{W}_{p,m}^{n+1}, \mathbf{W}_{s,j}^{n+1}\right) \quad (17a)$$

$$\text{s.t. } C11, (20)-(23), \quad (17b)$$

Where *f*(**W***n*+1*p;m* ,**W***n*+1*s;j*) is given by (15), and Ξ1 denotes the set including all optimization variables, auxiliary variables and slack variables. Since P6 is convex, it can be readily solved by using CVX. Similar to P1, Algorithm 2 can be used to solveP5.

COST FUNCTION ALGORITHM

Cost function algorithm is power loss estimation technique. Cost function is a precise formula used to chart how production expenses will vary at different output levels. The algorithm executed by each task tends to be very simple. Cost function performs the power budget analysis.

TABLE II: The cost function-based algorithm

Algorithm 2: The cost function-based algorithm for P_1

1: **Setting:**
$\gamma_{p,m,i}$, $\gamma_{s,j}$ $\Upsilon_{m,i}$, ζ_{e,A_1}, ζ_{e,A_1}, $i \in \mathcal{N}_{p,m}$, $k \in \mathcal{K}_m$, $m \in \mathcal{M}$
$l \in \mathcal{K}_s$ and the tolerance error ϖ;
2: **Initialization:**
The iterative number $n = 1$, $\bar{\alpha}^n_{p,m,i}$, $\bar{\beta}^n_m$, $\bar{\mu}^n_{e,m,k}$, $\bar{\alpha}^n_{s,N_s}$, $\bar{\beta}^n_{s,N_s}$,
$\mathbf{W}^n_{p,m}$ and $\mathbf{W}^n_{s,j}$;
3: **Repeat:**
solve P_4 by using CVX for the given approximate values;
obtain $\bar{\alpha}^{n+1}_{p,m,i}$, $\bar{\beta}^{n+1}_m$, $\bar{\mu}^{n+1}_{e,m,k}$, $\bar{\alpha}^{n+1}_{s,N_s}$, $\bar{\beta}^{n+1}_{s,N_s}$, $\bar{\mu}^{n+1}_{e,l}$,
$\mathbf{W}^{(n+1)}_{p,m}$ and $\mathbf{W}^{(n+1)}_{s,j}$;
set $\ell = 2\ell$;
end if
update the iterative number $n = n + 1$;
calculate the total transmit power P^m_{opt};
if $\mathrm{Tr}\left(\mathbf{W}^{n+1}_{p,m}\right) - \lambda_{\max}\left(\mathbf{W}^n_{p,m}\right) \leq \varpi$
and $\mathrm{Tr}\left(\mathbf{W}^{n+1}_{s,j}\right) - \lambda_{\max}\left(\mathbf{W}^n_{s,j}\right) \leq \varpi$
break;
end;
4: **Obtain resource allocation:**
$\mathbf{w}^n_{p,m}$, $\mathbf{w}^n_{s,j}$, $\mathbf{\Sigma}_{p,m}$ and $\mathbf{\Sigma}_s$.

ADVANTAGES OF PROPOSED METHOD

- Interference is controlled.
- Consumes very low power.
- Secrecy rate and efficiency is very high.

RESULTS & DISCUSSIONS

In this section, the performance of the proposed cognitive beamforming designs for the NOMA cooperative jamming scheme is evaluated through Simulation and results are provided for comparing the performance obtained by using NOMA to that achieved by OMA.

TABLE II: Simulation Parameters

Parameters	Notation	Typical Values
Numbers of antennas of the PBS	$N_{P,t}$	10
Numbers of antennas of the CBS	$N_{S,t}$	5
Numbers of the clusters	M	2
Numbers of SUs	N_s	3
The maximum harvested power	$P^{\max}_{E,A}$	24 mW
Circuit parameter	$a_{E,A}$	1500
Circuit parameter	$b_{E,A}$	0.0022
The minimum secrecy rate of PUs	$\gamma_{P,m,i}$	2 bits/s/Hz
The minimum secrecy rate of SUs	$\gamma_{S,j}$	1 bits/s/Hz
The maximum interference power	$\Upsilon_{m,i}$	10 mW
The minimum EH of EHRs in set A_1	ζ_{E,A_1}	15 mW
The minimum EH of EHRs in set A_2	ζ_{E,A_2}	5 mW
The tolerance error	ϖ	10^{-4}

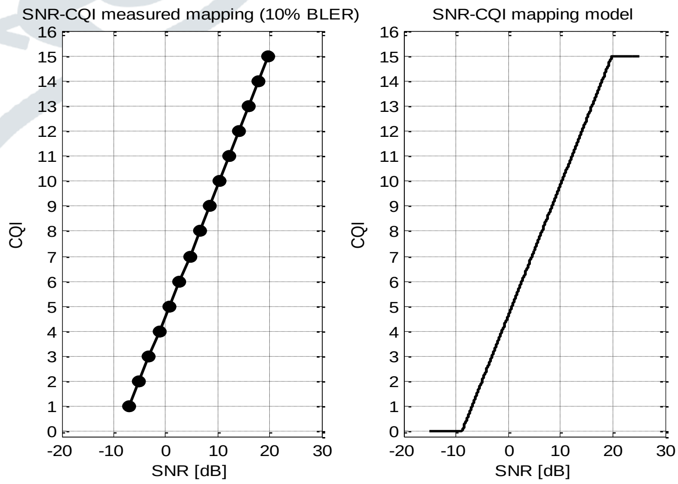
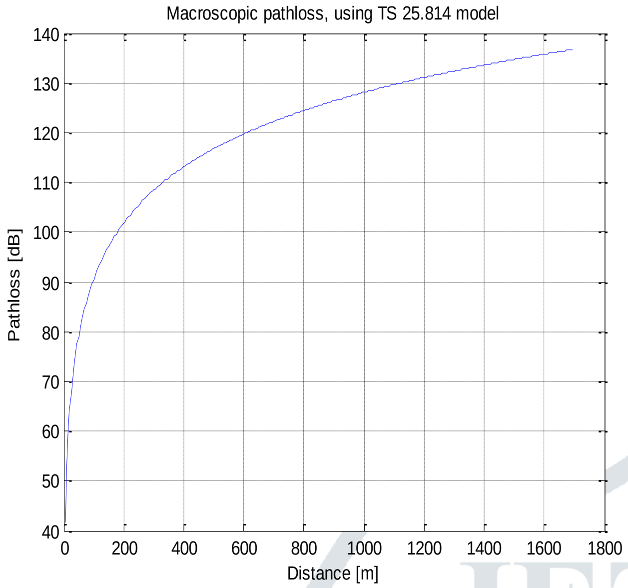
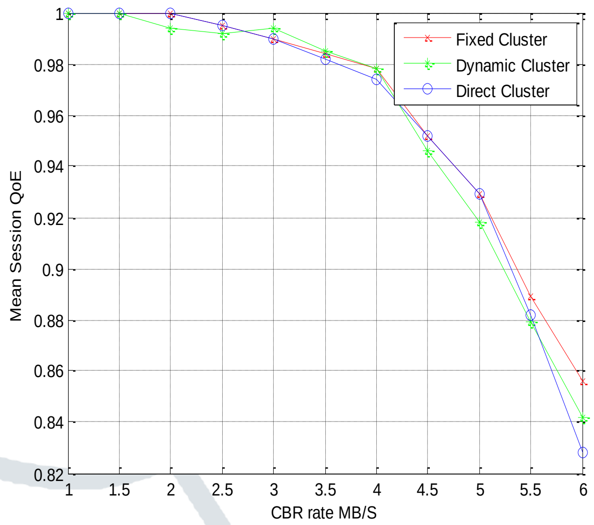


Fig (1): channel Quality Improvement (CQI) versus SNR(dB)

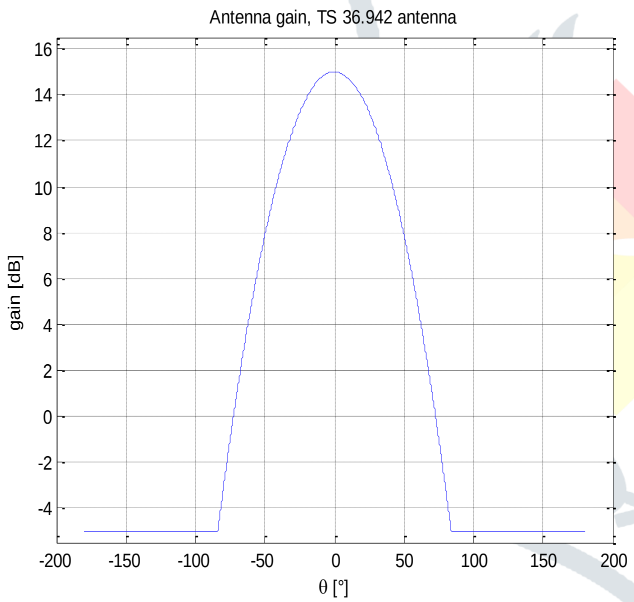
Fig.(1) shows the Channel Quality Improvement versus SNR (dB) achieved by NOMA cooperative Jamming Scheme. It is clearly shown that if channel has 10% Block error rate(BLER) then the efficiency is 90% and if the channel does not have BLER then the efficiency of that image is 100%. Fig.(2) shows the Microscopic Path loss versus Distance. From the Fig.(2) it is clearly shown that as distance in communication increases the losses in the channel path will be increases.



Fig(2) : Macroscopic Pathloss versus Distance



Fig(3): Mean Session Quality Of Experience (QOE) versus channel bit rate(Mb/S).



Fig(4):Antenna Gain versus Angle

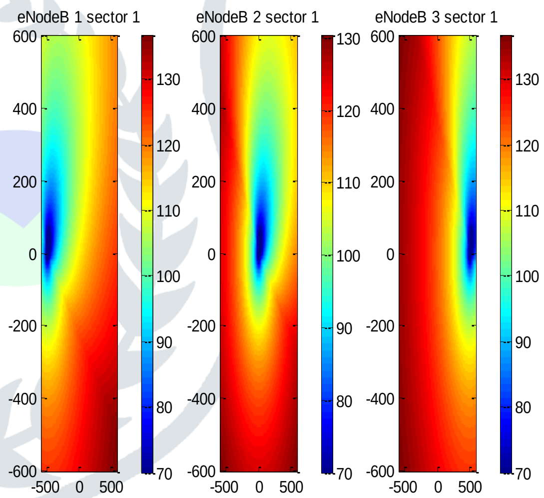
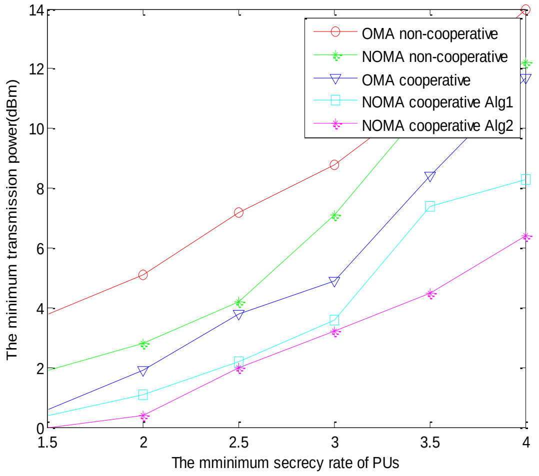


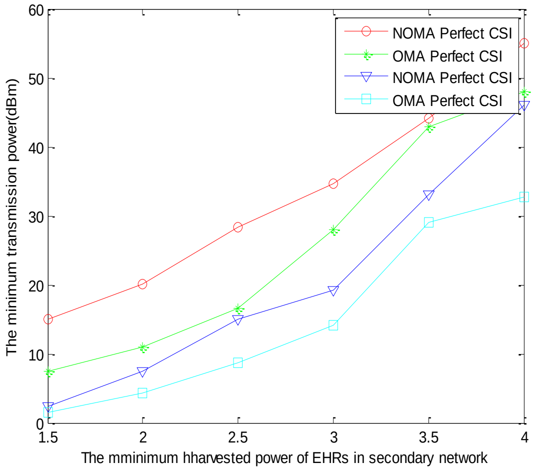
Fig (5): Beamforming of signals

Fig.(3) shows the Mean Session Quality of Experience (QOE) versus channel bit rate (Mb/s). Here, our Proposed NOMA cooperative jamming scheme uses fixed cluster which provide better Quality of experience with respect to channel bit rate compared to the existing work. Fig.(4) represents the gain with respect to angle. This figure shows how strong a signal is transmitted by the antenna. Fig.(5) shows that the signal transmitted into beams.

Fig.(6) shows that the transmission power increases with respect to secrecy rate. The minimum transmission power without cooperative NOMA is higher than that cooperative NOMA. Here Algorithm 2 i.e cost function produces minimum transmission power than SDR. Fig.(7) shows that minimum transmission power consumed by using OMA is higher than NOMA. The Reason is that secrecy rate for NOMA is higher than OMA.



Fig(6): minimum transmission power versus secrecy rate



Fig(7): Minimum transmission power versus Minimum Harvested Power.

CONCLUSIONS

In this paper, an artificial noise aided cooperative jamming scheme under a practical non-linear EH model was proposed to enhance the security of MISO-NOMA SWIPT system. The transmission beamforming vectors and AN-aided covariance matrix were together optimized to reduce the total transmission power of the network, while the secrecy rates of both PUs and SUs as well as the EH requirement of EHRs were satisfied. The beamforming design problems were investigated under both the perfect CSI and the bounded CSI error model. To solve these challenging non-convex problems, two pair of algorithms were proposed. It was shown that the performance achieved by using NOMA is better than that obtained by using OMA. Simulation results also show that cost function algorithm is superior to the SDR algorithm. Moreover, our proposed artificial noise-aided cooperative jamming scheme is efficient to improve the security of MISO NOMA cognitive radio networks (CRN's) using SWIPT.

REFERENCES

[1] Z Wel, et al, "Optimal resource allocation for power-efficient MC-NOMA with imperfect channel state Information? ," *IEEE Trans. Commun.*, vol.65, no.9,pp.3944-3961, Sept. 2016.

[2] F. Zhou, *et al.*, "Energy-efficient optimal power allocation for fading cognitive radio channels: ergodic capacity, outage capacity and minimum-rate capacity," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2741-2755, Apr.2016.

[3] Dai, *et al.*, "Joint pilot and payload power control for uplink MIMO-NOMA with MRC-SIC receivers," *IEEE Commun. Lett.*, to appear,2018.

[4]Z. Wei, *et al.*, "Energy-efficient transmission design in Non-orthogonal multiple access," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2852- 2857, Mar. 2017.

[5] B. Wang, *et al.*, "Spectrum and energy efficient beamspace MIMO-NOMA for millimeter-wave communications using lensantennaarray," *IEEE J. Sel. Areas Commun.*, to be published,2017.

[6] L. Liu *et al.*, "Gaussian message passing iterative detection for MIMO-NOMA systems with massive users," in *Proc. IEEE GLOBECOM 2016*, Washington, USA, Dec.2016.

[7] Y. Zhang *et al.*, "Energy-efficient transmission design in Non-orthogonal multiple access," *IEEE Trans. Veh.Technol.*, vol. 66, no. 3, pp. 2852-2857, Mar. 2017.

[8] Z. Zhu, *et al.*, "Outage constrained robust beamforming for secure broadcasting systems with energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7610-7620, Nov.2016.

[9] Y. Liu, *et al.*, "Cooperative nonorthogonal multiple access with simultaneous wireless information and power transfer" *IEEE J. Select. Areas Commun.*, vol. 34, no. 4, pp. 938-953, Apr.2016.

[10] Y. Xu, *et al.*, "Joint beamforming and power-splitting control in downlink cooperative SWIPT NOMA systems," *IEEE Trans. Signal Proces.*, vol. 65, no. 18, pp. 4874-4886, Sept. 2017.

[11] F. Zhou, *et al.*, "Robust AN-Aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEETrans.WirelessCommun.*, vol. 16, no. 4, pp. 2450-2464, April2017.

[12] H. Wang and X. Xia, "Enhancing wireless secrecy via cooperation: signal design and optmization," *IEEE Commun. Magz.*, vol. 53, no.12,pp: 47-53,2015.

[13] E. Boshkovska, *et al.*, "Robust resource allocation for MIMO wireless powered communication networks based on a non-linearEH model," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 1984-1999, May2017.

[14] E. Boshkovska, *et al.*, "Secure SWIPT networks based on a non-linear energy harvesting model," in *Proc. IEEE WCNC*

2017,San Francisco, CA, USA, 2017.

[15] J. G. Andrews, S. Buzzi, W. Choi, et al., "What will 5G be?," IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1065-1082, Jun. 2014.

[16] Y. C. Liang, K. C. Chen, G. Y. Li, and P. Mahonen, "Cognitive radio networking and communications: an overview," IEEE Trans. Veh. Technol., vol. 60, no. 7, pp. 3386-3407, Sept. 2011.

[17] Z. Zhang, H. Sun, and R. Q. Hu, "Downlink and uplink non-orthogonal multiple access in a dense wireless network," IEEE J. Sel. Areas Commun., to be published, 2017.

[18] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. Bhargava, "A survey on non-orthognonal multiple access for 5G networks: Research chanllenges and future trends," IEEE J. Sel. Areas Commun., to be published, 2017.

[19] B. Wang, L. Dai, Z. Wang, N. Ge, and S. Zhou, "Spectrum and energy efficient beamspace MIMO-NOMA for millimeter-wave communications using lens antenna array," IEEE J. Sel. Areas Commun., to be published, 2017.

[20] Y. Liu, Z. Ding, M. Elkashlan, and J. Yuan, "Nonorthogonal multiple access in large-scale underlay cognitive radio networks," IEEE Trans. Veh. Technol., vol. 65, no. 12, pp. 10152-10157, Dec. 2016.

[21] L. Lv, J. Chen, Q. Ni, and Z. Ding, "Design of cooperative nonorthogonal multicast cognitive multiple access for 5G systems: user scheduling and performance analysis," IEEE Trans. Commun., vol. 65, no. 6, pp. 2641-2656, June 2017.

[22] F. Zhou, N. C. Beaulieu, Z. Li, J. Si, and P. Qi, "Energy-efficient optimal power allocation for fading cognitive radio channels: ergodic capacity, outage capacity and minimum-rate capacity," IEEE Trans. Wireless Commun., vol. 15, no. 4, pp. 2741-2755, Apr. 2016.

[23] D. Feng, C. Jiang, G. Lim, L. J. Cimini, G. Feng, and G. Y. Li, "A survey of energy-eficient wireless communications," IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 167-178, Feb. 2013.

[24] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," IEEE Commun. Surveys Tuts., vol. 17, pp. 757-789, Second Quarter, 2015.

[25] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," IEEE Trans. Inf. Theory, vol. 62, no. 7, pp. 3880-3900, 2016.

[26] Y. Zhang, H. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," IEEE Commun.Lett., vol. 20, no. 5, pp. 930-933, 2016.

[27] D. W. K. Ng, E. S. Lo, and R. Schober, "Multi-objective resource allocation for secure communication in cognitive radio networks with wireless information and power transfer," IEEE Trans. Veh. Technol., vol. 20, no. 2, pp. 328-331, Feb. 2016.

[28] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission in the presence of an active eavesdropper," in Proc. IEEE ICC 2015, London, UK, 2015.

[29] Y. Zou, B. Champagne, W. Zhu, and L. Hanzo, "Relay-selection improves the security-reliablity trade-off in cognitive radio systems," IEEE Trans. Commun., vol. 63, no. 1, pp. 215-228, Jan. 2015.

[30] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun.SurveysTuts.*, vol. 19, no. 2, pp. 1027-1053, Second Quarter, 2017.

[31] Y. Wu, J. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," *IEEE Trans.Commun.*, vol. 65, no. 8, pp. 3614-3628, June 2017.

[32] Y. Pei, Y. C. Liang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[33] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission in the presence of an active eavesdropper," in *Proc.IEEE ICC 2015*, London, UK, 2015.

[34] Y. Zou, X. Li, and Y. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222-2236, Nov. 2014.

[35] Y. Zou, J. Zhu, X. Li, and L. Hanzo, "Relay selection for wireless communications against eavesdropping: A security-reliablity trade-off persepective," *IEEE Network*, vol. 30, no. 5, pp. 74-79, May, 2016.

[36] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-Aided Beamform-ing and Power Splitting Design for Secure MISO Cognitive Radio With SWIPT," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 2450-2464, April 2017.

[37] D. Wang, P. Ren, Q. Du, L. Sun, and Y. Wang, "Security provisioning for vehicular relay networks via cooperative jamming and signal super-position," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10732-10747, Dec. 2017.

[38] D. Wang, P. Ren, Q. Du, J. Chen, and Y. Wang, "Achieving full secrecy rate with energy-efficient transmission control," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5386-5400, Dec. 2017.

[39] Q. Zhang, Q. Li, and J. Qin, "Robust beamforming for nonorthongonalmuliple-access systems in MISO channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10231-10236, Dec. 2016.

[40] F. Alavi, K. Cumanan, Z. Ding, and A. G. Burr, "Robust beaforming techniques for non-orthogonal multiple access systems with bounded channel uncertainties," *IEEE Commun. Lett.*, to be published, 2017.

[41] B. He, A. Liu, N. Yang, V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, to be published, 2017.

[42] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Trans.Veh. Technol.*, vol. 66, no. 8, pp. 7563-7567, Aug. 2017.

[43] J. Lei, J. Zhang, K. H. Park, *et al.*, "On secure NOMA systems with tranmit antennas selection schemes," *IEEE Access*, to be published, 2017.

[44] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin, “Secrecy sum rate opti-mization for downlink MIMO non-orthogonal multiple access systems,” *IEEE Signal Process. Lett.*, vol. 24, no. 8, pp. 1113-1117, Aug. 2017.

[45] Y. Pei, Y. C. Liang, K. Teh, and K. H. Li, “Secure communication in multiantenna cognitive radio networks with imperfect channel state information,” *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683-1693, Apr. 2011.

[46] L. Zhang, R. Zhang, Y. C. Liang, Y. Xin, and S. Cui, “On the relationship between the multi-antenna secrecy communications and cognitive radio communications,” *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877-1886, June 2010.

[47] C. Wang, and H. Wang, “On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels,” *IEEE Trans.Inf. Forensics Security*, vol.9, no. 11, pp. 1814-1827, Nov. 2014.

[48] W. Zeng, Y. Zheng, and C. Xiao, “Multiantenna secure cognitive radio networks with finite-alphabet inputs: A global optimization approach for precoderdesing,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3044-3057, Apr. 2016.

[49] D. W. K. Ng, M. Shaqfeh, R. Schober, and H. Alnuweiri, “Robust layered transmission in secure MISO multiuser unicast cognitive radio systems,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8267-8282, Oct. 2016.

[50] V. Nguyen, T. Duong, O. Shin, A. Nallanathan, and G. K. Karagiannidis, “Enhancing PHY security of cooperative cognitive radio multicast communications,” *IEEE Trans. Cogn. Net.*, to be published, 2017.