Xinyao WANG, Xuyan BAO, Yuzhen HUANG, Zhong ZHENG, Zesong FEI, 2023. On optimization of cooperative MIMO for underlaid secrecy Industrial Internet of Things. *Frontiers of Information Technology & Electronic Engineering*, 24(2):259-274. https://doi.org/10.1631/FITEE.2200188

On optimization of cooperative MIMO for underlaid secrecy Industrial Internet of Things

Key words: Cognitive radio network; Physical layer security; Cooperative multi-input multi-output (C-MIMO); Eigenspace-adaptive precoding; Difference convex programming

Corresponding author: Zhong ZHENG
E-mail: zhong.zheng@bit.edu.cn
 ORCID: https://orcid.org/0000-0002-3955-2510

Motivation

- **Interference control in cognitive radio network (CRN):**

1. To acquire the operation spectrum with reduced cost, the unlicensed spectrum has been introduced to Industrial Internet of Things (IIoT) systems, opportunistically exploiting airtime among other spectrum users.
2. The underlying cognitive radio (CR) is a spectrum contention-based transmission method, which is feasible to the delay-sensitive application, but the interference control to the primary user (PU) is a considerable problem.

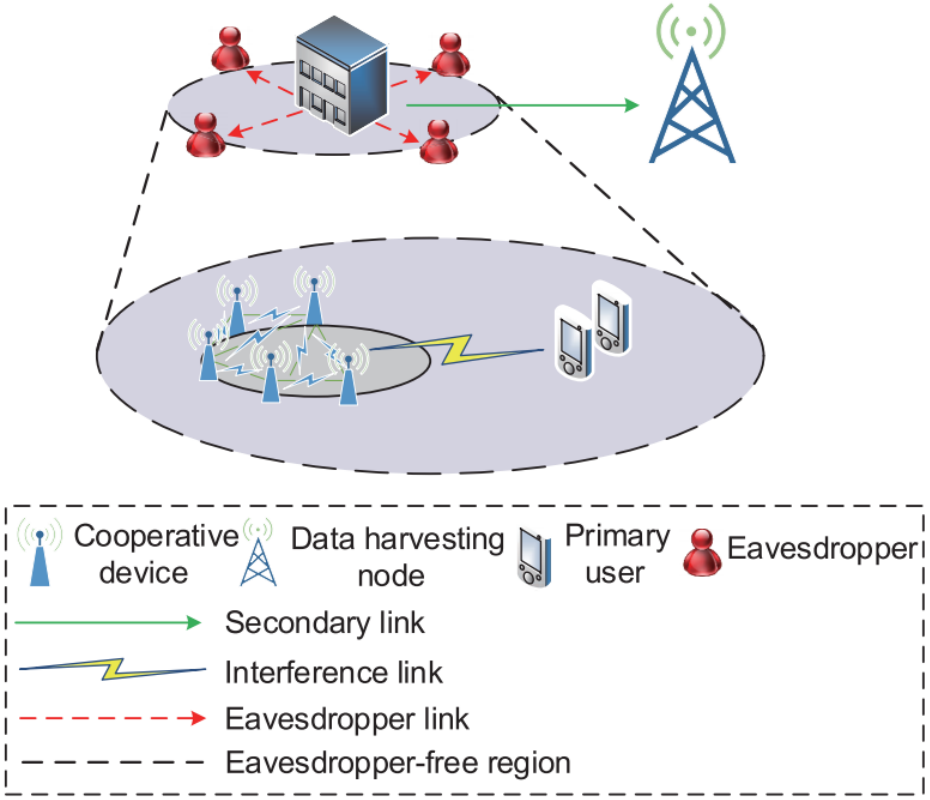
- **Secrecy transmission requirement of the underlaid CRN:**

1. Considering an Industrial Internet of Things scenario, there is generally a secure space via the physical isolation; i.e., the malicious eavesdropper cannot be inside this secure space. For example, the eavesdropper can locate only at the edge of the factory building, and intercept the information transmitted from the factory to the outside receiver.
2. The previous works either consider an over-pessimistic assumption that the eavesdropper is distributed at “anywhere” or adopt an over-optimistic assumption that the eavesdropper is located at a known location, which leads to an inaccurate estimation of the secrecy rate.

Main contributions

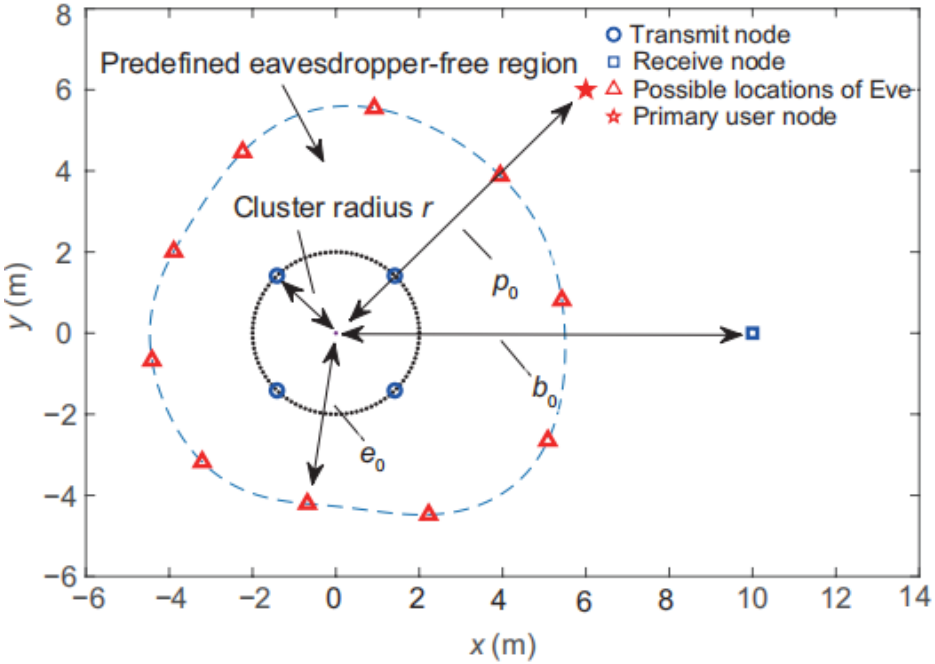
- We consider a realistic underlaid secrecy cognitive radio system, where the C-MIMO transceivers coexist with a PU and the eavesdroppers can appear at multiple possible locations in the network. This is useful to relax the “anywhere Eve” assumption in previous works, and the considered framework can take into account the practical constraints of the system topology.
- We propose an eigenspace-adaptive precoding (EAP) method for the underlaid C-MIMO system by jointly designing the signals and the AN. The signals and the AN are adaptively transmitted in the eigenspace of the main channel or the null-space of the interference channel according to the channel conditions of the secondary users (SUs) and the PUs.
- To adapt to the low-powered and massively populated device scenario, we simplify the EAP method by adopting uniform power allocation. When the null-space of the PU’s channel is considered, the orthogonal subspace projection method is adopted to improve the information rate of the legitimate channel by aligning the sub-nullspace of the PU channel with the eigenspace of the main channel.

System model



As shown above, several IIoT sensors inside the factory building form a cooperative cluster and jointly transmit to the remote data collector. The transmissions are subject to secrecy constraints that prevent eavesdroppers outside the building from intercepting confidential messages, and also to the interference constraint that avoids excessive interference toward PUs.

Mathematical model



As shown above, we consider a secondary C-MIMO system between K clustered single-antenna transmit nodes (Alice) and an N_B-antenna receive node (Bob). The cluster radius is r. The distance between the head of Alice and Bob is b_0. The secret messages can be intercepted by an N_E-antenna Eve, which is located outside an eavesdropper-free region (dotted line). We assume that an N_P-antenna PU at a distance of p_0 from the head of Alice can overhear the underlaid transmissions, which is regarded as an unnecessary interference toward the PU.

Eigenspace-adaptive precoding

☐ AN-injected signal model

$$x = \tilde{V} S \Psi_{\mathrm{s}}^{1/2} s + \tilde{V} S \Psi_{\mathrm{a}}^{1/2} a,$$

where

$$S = \begin{cases} \begin{bmatrix} I_{K\times K} & 0_{K\times r} \end{bmatrix}^{\mathrm{T}}, & \text{if } V_{\mathrm{H}} \text{ is selected} \\ \begin{bmatrix} 0_{r\times K} & I_{r\times r} \end{bmatrix}^{\mathrm{T}}, & \text{if } V_{\mathrm{G}} \text{ is selected} \end{cases}$$

The eigenspace of the underlaid legitimate channel

The eigenspace selection matrix

The null-space of the primary user's channel

☐ Eigenspace precoding method

- Eigenspace precoding $\tilde{V} = V_{\mathrm{H}}$

Make the SVD of the legitimate channel

$$H = U_{\mathrm{H}} \Lambda_{\mathrm{H}}^{1/2} V_{\mathrm{H}}^{\dagger}.$$

The precoding vector for signals and AN are

$$V_{\mathrm{s}} = V_{\mathrm{a}} = \tilde{V} = V_{\mathrm{H}}$$

- Null-space precoding $\tilde{V} = V_{\mathrm{G}}$

Make the SVD of the PU's channel, and obtain the null-space eigenvectors as the precoding matrix

$$V_{\mathrm{s}} = V_{\mathrm{a}} = V_{\mathrm{G}}$$

with $GV_{\mathrm{G}} = 0.$

Problem formulation

☐ Ergodic secrecy rate maximization problem

- **Secrecy rate formulation**

$$R_{\mathrm{s}}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{s}},\boldsymbol{\Psi}_{\mathrm{a}}) = R_{\mathrm{B}}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{s}},\boldsymbol{\Psi}_{\mathrm{a}}) - \max_{1\le i\le L} R_{\mathrm{E},i}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{s}},\boldsymbol{\Psi}_{\mathrm{a}}),$$

where

$$R_{\mathrm{B}}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{s}},\boldsymbol{\Psi}_{\mathrm{a}}) = f_{\mathrm{B}}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{s}}+\boldsymbol{\Psi}_{\mathrm{a}}) - f_{\mathrm{B}}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{a}}),$$

$$R_{\mathrm{E},i}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{s}},\boldsymbol{\Psi}_{\mathrm{a}}) = f_{\mathrm{E},i}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{s}}+\boldsymbol{\Psi}_{\mathrm{a}}) - f_{\mathrm{E},i}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{a}})$$

$$f_{\mathrm{B}}(\boldsymbol{X},\boldsymbol{Y}) = \log_2 \det\left(\boldsymbol{I} + \boldsymbol{V}_{\mathrm{H}}\boldsymbol{\Lambda}_{\mathrm{H}}\boldsymbol{V}_{\mathrm{H}}^{\dagger}\tilde{\boldsymbol{V}}\boldsymbol{X}\boldsymbol{Y}\boldsymbol{X}^{\dagger}\tilde{\boldsymbol{V}}^{\dagger}\right)$$

Haar matrix approximation theory

$$\tilde{f}_{\mathrm{E}}(\boldsymbol{Z}) = \log_2 \mathbb{E}\left[\det\left(\boldsymbol{I} + \boldsymbol{W}\boldsymbol{\Sigma}^{1/2}\boldsymbol{\Phi}\boldsymbol{Z}\boldsymbol{\Phi}^{\dagger}\boldsymbol{\Sigma}^{1/2}\boldsymbol{W}^{\dagger}\right)\right]$$

☐ Problem formulation

$$\max_{\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{s}}\succeq\boldsymbol{0},\boldsymbol{\Psi}_{\mathrm{a}}\succeq\boldsymbol{0}} [R_{\mathrm{s}}(\boldsymbol{S},\boldsymbol{\Psi}_{\mathrm{s}},\boldsymbol{\Psi}_{\mathrm{a}})]^{+}$$

$$\text{s.t. } 0 \le \Psi_{\mathrm{p}}^{[kk]} \le \Gamma_{\mathrm{s}},\ k = 1,2,\ldots,K$$

Single BS power constraint

$$0 \le \mathrm{tr}\left(\boldsymbol{G}\tilde{\boldsymbol{V}}\boldsymbol{S}(\boldsymbol{\Psi}_{\mathrm{s}}+\boldsymbol{\Psi}_{\mathrm{a}})\boldsymbol{S}^{\dagger}\tilde{\boldsymbol{V}}^{\dagger}\boldsymbol{G}^{\dagger}\right) \le \Gamma_{\mathrm{I}}$$

Interference constraint for PU

Optimization algorithm

☐ Problem transform

- when $\tilde{V} = V_{\mathrm{H}}$, the problem is rewritten as

$$\max_{\boldsymbol{\Psi}_{\mathrm{s}}, \boldsymbol{\Psi}_{\mathrm{a}} \succeq \mathbf{0}} [R_{\mathrm{s}}^{(\mathrm{H})}(\boldsymbol{\Psi}_{\mathrm{s}}, \boldsymbol{\Psi}_{\mathrm{a}})]^{+}$$

$$\text{s.t. } 0 \le \Psi_{\mathrm{p}}^{[kk]} \le \Gamma_{\mathrm{s}}, \ k = 1, 2, \ldots, K$$

$$0 \le \mathrm{tr}\left(\boldsymbol{G}\boldsymbol{V}_{\mathrm{H}}(\boldsymbol{\Psi}_{\mathrm{s}} + \boldsymbol{\Psi}_{\mathrm{a}})\boldsymbol{V}_{\mathrm{H}}^{\dagger}\boldsymbol{G}^{\dagger}\right) \le \Gamma_{\mathrm{I}}$$

where $\boldsymbol{\Psi}_{\mathrm{p}} = \boldsymbol{V}_{\mathrm{H}}(\boldsymbol{\Psi}_{\mathrm{s}} + \boldsymbol{\Psi}_{\mathrm{a}})\boldsymbol{V}_{\mathrm{H}}^{\dagger}$.

- when $\tilde{V} = V_{\mathrm{G}}$, the problem is rewritten as

$$\max_{\boldsymbol{\Psi}_{\mathrm{s}}, \boldsymbol{\Psi}_{\mathrm{a}} \succeq \mathbf{0}} [R_{\mathrm{s}}^{(\mathrm{G})}(\boldsymbol{\Psi}_{\mathrm{s}}, \boldsymbol{\Psi}_{\mathrm{a}})]^{+}$$

$$\text{s.t. } 0 \le \Psi_{\mathrm{p}}^{[kk]} \le \Gamma_{\mathrm{s}}, \ k = 1, 2, \ldots, K$$

where $\boldsymbol{\Psi}_{\mathrm{p}} = \boldsymbol{V}_{\mathrm{G}}(\boldsymbol{\Psi}_{\mathrm{s}} + \boldsymbol{\Psi}_{\mathrm{a}})\boldsymbol{V}_{\mathrm{G}}^{\dagger}$.

☐ Power allocation algorithm

The two sub-problems in the left are still non-convex, which can be further converted into a CDC problem and solved by the iterative outer approximation method as shown in Algorithm 1.

Algorithm 1 Optimal power allocation

1: **Initialization**
2: Determine a feasible solution $\boldsymbol{w}_0 \in H^{(x)} \cap \partial G^{(x)}$
3: **for** $k \ge 1$ **do**
4: Solve the sub-problem

$$\boldsymbol{z}_k = \arg\max_{\boldsymbol{z}} \{g^{(x)}(\boldsymbol{z}) : h^{(x)}(\boldsymbol{z}) \le 0, t_{\boldsymbol{z}} \le t_{\boldsymbol{w}_{k-1}}\}$$

5: **if** $g^{(x)}(\boldsymbol{z}_k) \ge \epsilon$ **then**
6: $\boldsymbol{w}_k = \pi(\boldsymbol{z}_k)$, $k \to k+1$
7: **else**
8: Set the output $\boldsymbol{w}^* = \boldsymbol{z}_k$
9: **return**
10: **end if**
11: **end for**

Numerical results

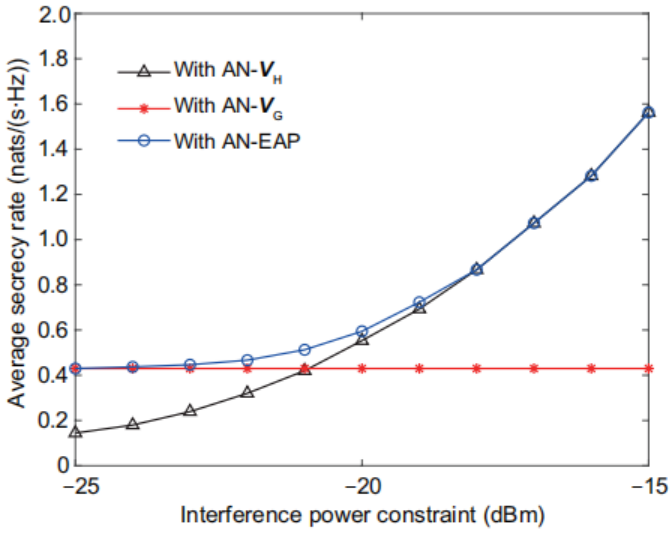


Fig. 4 Average secrecy rate of the C-MIMO system via the V_H, V_G, and EAP schemes with AN injection under different interference power constraints Γ_I when $K=4$, $N_B=4$, $N_E=2$, $N_P=2$, $r=3$ m, $e_0=10$ m, and $\Gamma_s=23$ dBm (AN: artificial noise; C-MIMO: cooperative multi-input multi-output; EAP: eigenspace-adaptive precoding)

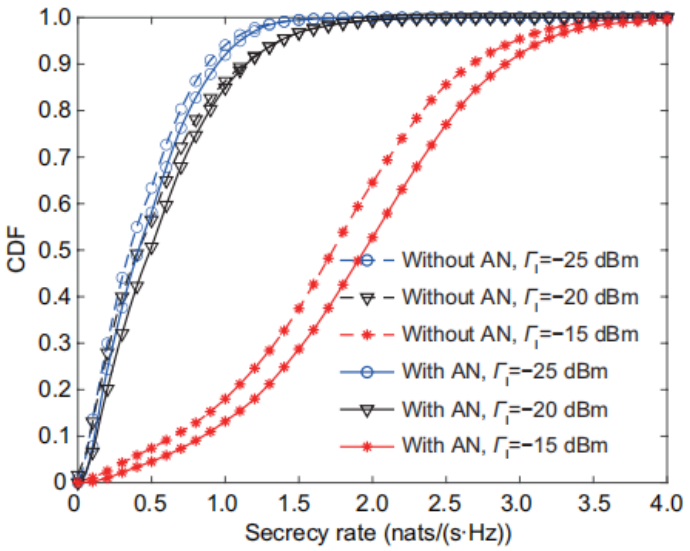


Fig. 5 CDFs of the C-MIMO system secrecy rate via EAP when $K=4$, $N_B=4$, $N_E=2$, $N_P=2$, $r=3$ m, $e_0=10$ m, and $\Gamma_s=23$ dBm (CDFs: cumulative distribution functions; C-MIMO: cooperative multi-input multi-output; EAP: eigenspace-adaptive precoding)

Conclusion:

- From Fig. 4, it is observed that the proposed EAP method can outperform the fixed eigenspace precoding method under either the tight interference constraint or the loose interference constraint.
- From Fig. 5, we can see that the secrecy outage is eliminated using the EAP method and the gain from AN-injection is improved when loosing the interference power constraint.

Numerical results (Cont'd)

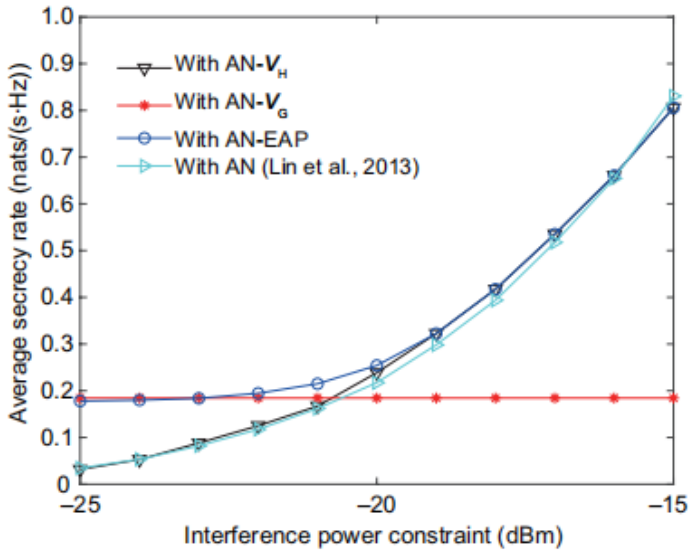


Fig. 9 Average secrecy rate of C-MIMO system via different AN-aided precoding methods when K=4, N_B=2, N_E=2, N_P=2, r=3 m, e_0=10 m, Γ_s=23 dBm, and Γ_I=−15 dBm (AN: artificial noise; C-MIMO: cooperative multi-input multi-output)

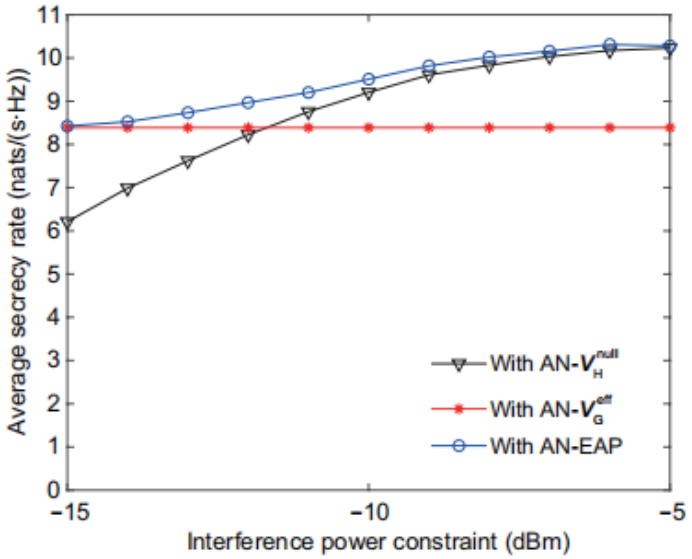


Fig. 10 Average secrecy rate of the large-dimensional C-MIMO system via V_H^{null}, V_G^{eff}, and the simplified EAP methods when K=64, N_B=4, N_E=2, N_P=2, r=3 m, e_0=10 m, and Γ_s=13 dBm (C-MIMO: cooperative multi-input multi-output; EAP: eigenspace-adaptive precoding)

Conclusion:

- Fig. 9 shows that the EAP method can outperform the generalized AN-aided precoding in Lin et al. (2013) when the interference power constraint dominates the problem.
- From Fig. 10, we can see that the average secrecy rate is significantly improved under the large-dimensional MIMO system via the EAP method.

Conclusions

- EAP together with AN-assisted secrecy transmission is considered for a C-MIMO system coexisting with a PU. The design of underlaid secrecy communications exploits the geographical location constraint of the eavesdropper as well as the eigenspace of the channels.
- Specifically, the eigenvectors are adaptively selected by the transmitter according to the channel conditions.
- To reduce the complexity, a simplified EAP method is proposed for the large-dimensional C-MIMO system.
- Numerical results showed that the proposed EAP method outperforms the fixed eigenvector precoding method.
- Moreover, EAP can eliminate the secrecy outage even when the eavesdroppers are located closer to the transmitter.
- In addition, the simplified EAP method for large-dimensional C-MIMO transmission can significantly improve the secrecy rate with low complexity.