Physical Layer Security for Intelligent Reflecting Surface Assisted Two–Way Communications

Mevan Wijewardena[*], Tharaka Samarasinghe[*†], Kasun T. Hemachandra[*], Saman Atapattu[†], Jamie S. Evans[†]

[*]Department of electronic and telecommunication Engineering,
University of Moratuwa.
[†]Department of Electrical and Electronic Engineering,
The University of Melbourne.

March 17, 2025

Outline

Outline

Intelligent Reflecting Surfaces(IRS)

IRS is a technology where the wireless propagation environment is reconfigured with the use of passive reflecting elements[1]. The reflecting elements are integrated on a planar surface.

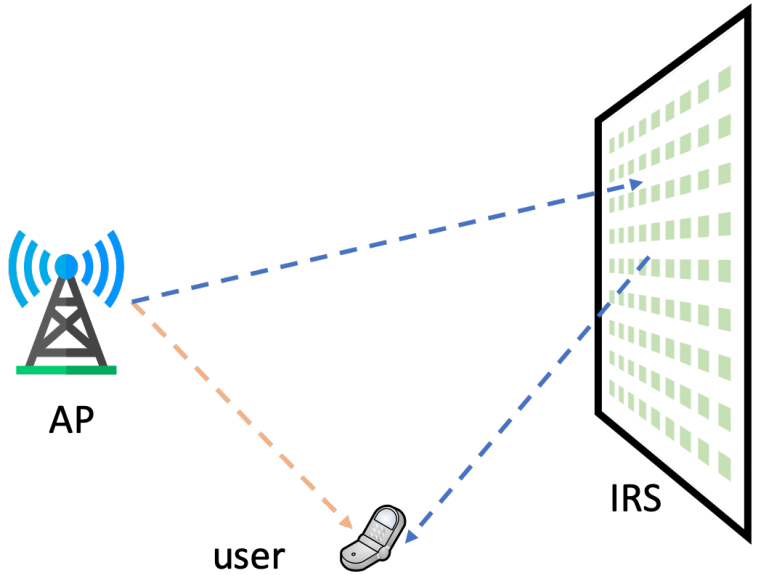


Figure 1: An IRS setup

[1] Q. Wu and R. Zhang. "Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network". In: *IEEE Commun. Mag.* 58.1 (Jan. 2020), pp. 106–112.

Physical layer security

The IRS environment is vulnerable to potential attacks by malicious users. Physical-layer (PHY) security, is considered crucial in enabling reliable IRS-assisted communications[2].

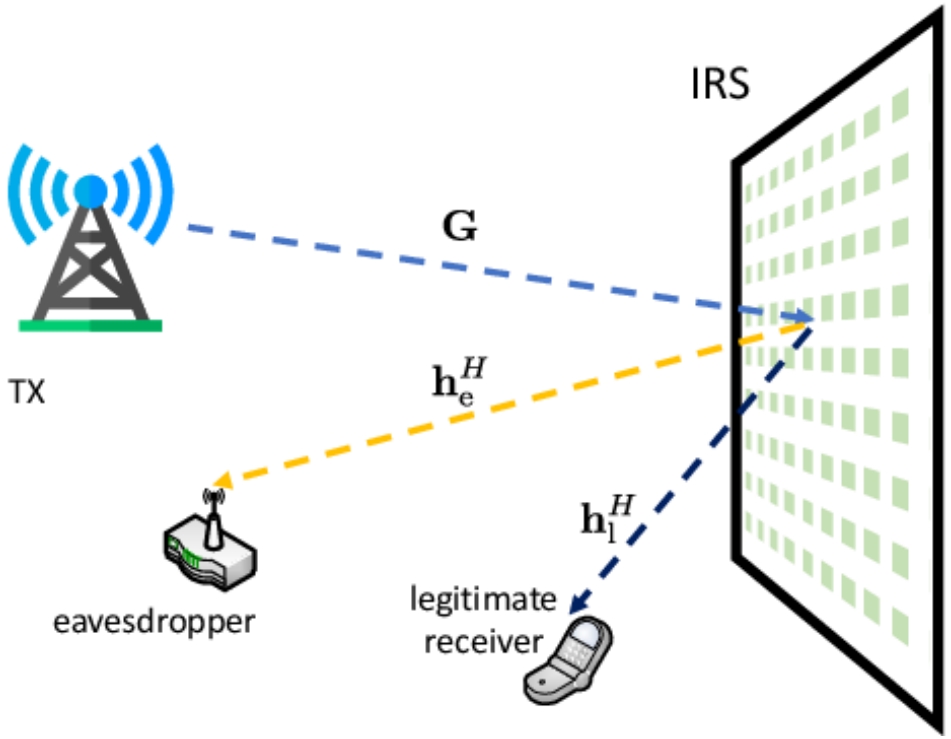


Figure 2: An IRS setup

[2] L. Yang et al. "Secrecy Performance Analysis of RIS-Aided Wireless Communication Systems". In: *IEEE Trans. Veh. Technol.* 69.10 (Oct. 2020), pp. 12296–12300.

Physical layer security

Secrecy rate is the commonly used objective in the literature.

- Individual user based performance - secrecy rate[3].
- Network wide performance - sum-secrecy rate[4].

The problem of physical-layer (PHY) security for IRS is addressed for one-way communications[5] and recently for two-way communications[6].
We explore the physical-layer security for an IRS assisted two way communication system operating in the in-band full-duplex(FD) mode.

[3] J. Chen et al. "Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security". In: *IEEE Access* 7 (2019), pp. 82599–82612.

[4] Ender Tekin and Aylin Yener. "The Gaussian Multiple Access Wire-Tap Channel". In: *IEEE Transactions on Information Theory* 54.12 (2008), pp. 5747–5755. DOI: 10.1109/TIT.2008.2006422.

[5] Yang et al., "Secrecy Performance Analysis of RIS-Aided Wireless Communication Systems".

[6] L. Lv et al. "Secure Two-Way Communications via Intelligent Reflecting Surfaces". In: *IEEE Commun. Lett.* 25.3 (2021), pp. 744–748. DOI: 10.1109/LCOMM.2020.3035773.

Contributions of the paper

Following are the major contributions of the paper.

- An algorithm that maximizes the sum-secrecy rate of an IRS-assisted two-way communication system.
  - The system is operating in the in-band full-duplex (FD) mode, in the presence of an untrusted user.
  - The system is controlled by a central node equipped with a central processing unit (CPU).
  - The convergence of the algorithm is proved analytically and illustrated numerically.
- The performance of the proposed algorithm is compared with other beamformer design schemes, numerically.
  - Gains reaching 35% when the untrusted user is located in close proximity to the IRS.
  - Gains reaching 120% when the untrusted user is in close proximity to a user.

Outline

System model

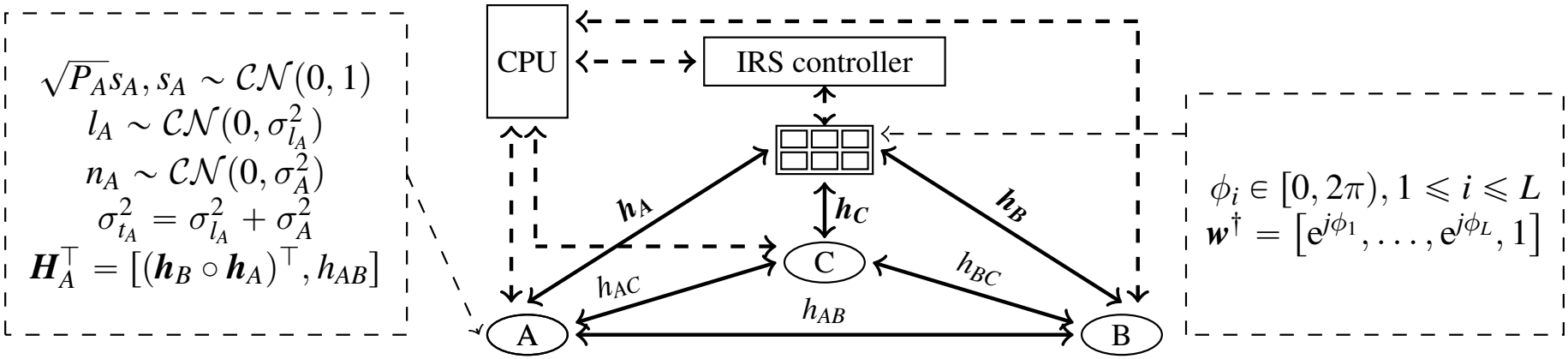


Figure 3: The IRS-assisted two-way communication model.

$$I_A = \log_2\left(1 + (P_B|\boldsymbol{w}^\dagger \boldsymbol{H}_A|^2)/\sigma_{t_A}^2\right) \text{ bps/Hz} \tag{1}$$

$$I_C = \log_2\left(1 + (P_A|\boldsymbol{w}^\dagger \boldsymbol{H}_{CA}|^2 + P_B|\boldsymbol{w}^\dagger \boldsymbol{H}_{CB}|^2)/\sigma_C^2\right) \text{ bps/Hz}, \tag{2}$$

Worst case sum-secrecy rate[7]: $R_{\text{sum}} = [I_B + I_A - I_C]^+$

[7] H. Wang, Q. Yin, and X. Xia. "Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks". In: *IEEE Trans. Signal Process* 60.7 (2012), pp. 3532–3545. DOI: 10.1109/TSP.2012.2191543.

Outline

Sum-secrecy rate maximization

The sum-secrecy rate maximization problem can be formulated as,

$$\begin{aligned}
\text{(P1):} \underset{\boldsymbol{w}, P_A, P_B}{\text{maximize}} \quad & R_{\text{sum}} && \text{(3a)}\\
\text{subject to} \quad & P_i^{\min} \leqslant P_i \quad i \in \{A, B\}, && \text{(3b)}\\
& P_A + P_B \leqslant P^{\max}, && \text{(3c)}\\
& |w^{(j)}| = 1 \qquad \forall 1 \leqslant j \leqslant L, && \text{(3d)}\\
& w^{(L+1)} = 1, && \text{(3e)}
\end{aligned}$$

where

- $P^{\max}$: aggregate maximum transmit power.
- $P_A^{\min}$ and $P_B^{\min}$: minimum allowed transmit powers of A and B.

The constraint (3e) can be absorbed into the constraint (3d) by letting $1 \leqslant i \leqslant L + 1$.

Challenges of the problem

Non-convexity of the unit modulus constraint.

- We first use the substitution $|\boldsymbol{w}^\dagger \boldsymbol{H}|^2 = \mathrm{Tr}\left(\boldsymbol{H}\boldsymbol{H}^\dagger \boldsymbol{W}\right)$, where $\boldsymbol{W} = \boldsymbol{w}\boldsymbol{w}^\dagger$.
- We then apply semidefinite relaxation (SDR)[8].
- The new equivalent objective:

$$\begin{aligned} G(\boldsymbol{W}, P_A, P_B) = \log_2 \left(\sigma_{t_B}^2 + P_A \,\mathrm{Tr}\left(\boldsymbol{H}_B \boldsymbol{H}_B^\dagger \boldsymbol{W}\right)\right) \\ + \log_2 \left(\sigma_{t_A}^2 + P_B \,\mathrm{Tr}\left(\boldsymbol{H}_A \boldsymbol{H}_A^\dagger \boldsymbol{W}\right)\right) - \log_2 F(\boldsymbol{W}, P_A, P_B), \end{aligned} \tag{4}$$

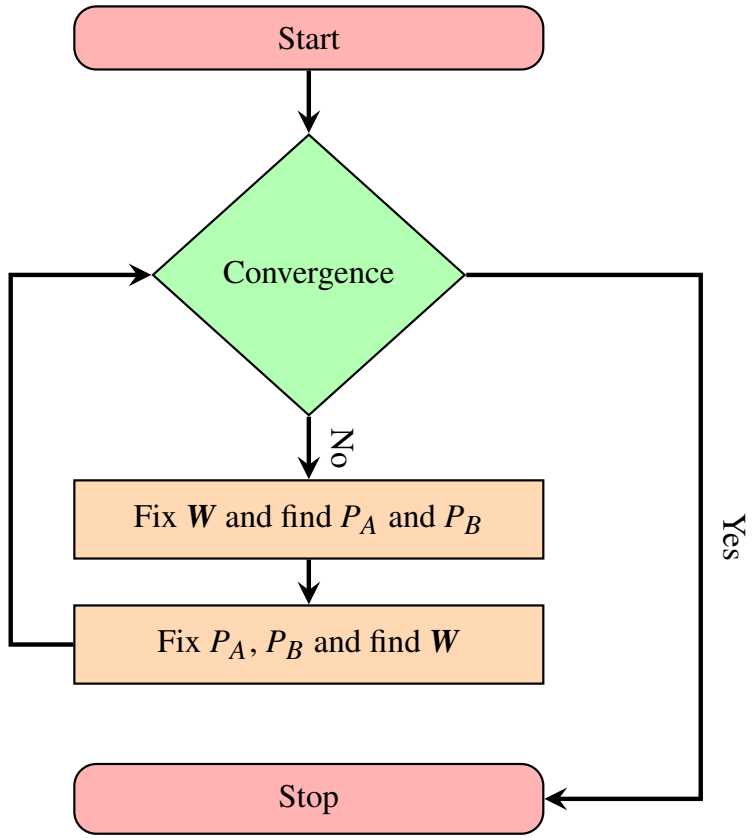
where $F(\boldsymbol{\Omega}, \alpha, \beta) = \sigma_C^2 + \alpha \,\mathrm{Tr}\left(\boldsymbol{H}_{CA} \boldsymbol{H}_{CA}^\dagger \boldsymbol{\Omega}\right) + \beta \,\mathrm{Tr}\left(\boldsymbol{H}_{CB} \boldsymbol{H}_{CB}^\dagger \boldsymbol{\Omega}\right)$,
$\boldsymbol{W} \in \mathbb{S}^{L+1}$, all diagonal elements of $\boldsymbol{W}$ are 1.

[8] Zhi-quan Luo et al. "Semidefinite Relaxation of Quadratic Optimization Problems". In: *IEEE Signal Processing Magazine* 27.3 (2010), pp. 20–34. DOI: 10.1109/MSP.2010.936019.

Challenges of the problem

It is hard to come up with a good approximation of the objective which is jointly convex in $(\boldsymbol{W}, P_A, P_B)$.

- We use an alternating optimization technique.



Transmit power optimization

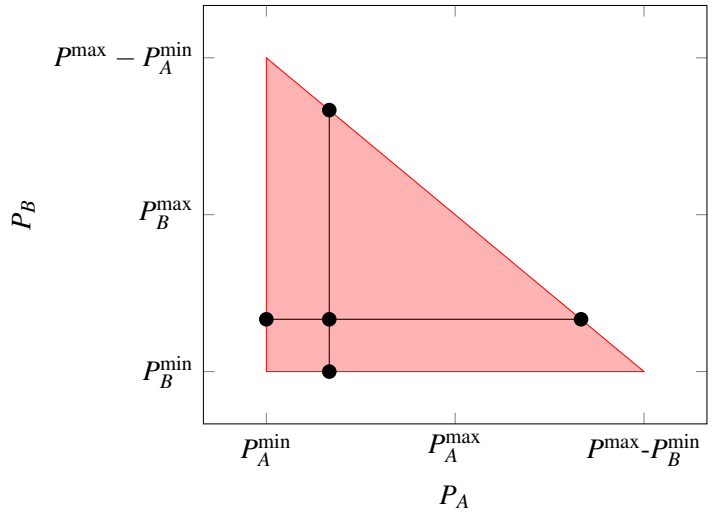
The transmit power optmization problem can be given by,

$$\text{(P2):} \underset{P_A, P_B}{\text{maximize}} \quad G(\boldsymbol{W}, P_A, P_B) \tag{5a}$$

$$\text{subject to} \quad P_i^{\min} \leqslant P_i \quad i \in \{A, B\}, \tag{5b}$$

$$P_A + P_B \leqslant P^{\max}. \tag{5c}$$

The feasibility region of the above problem is shown below.

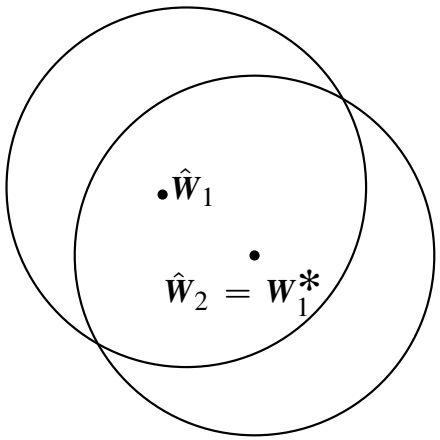


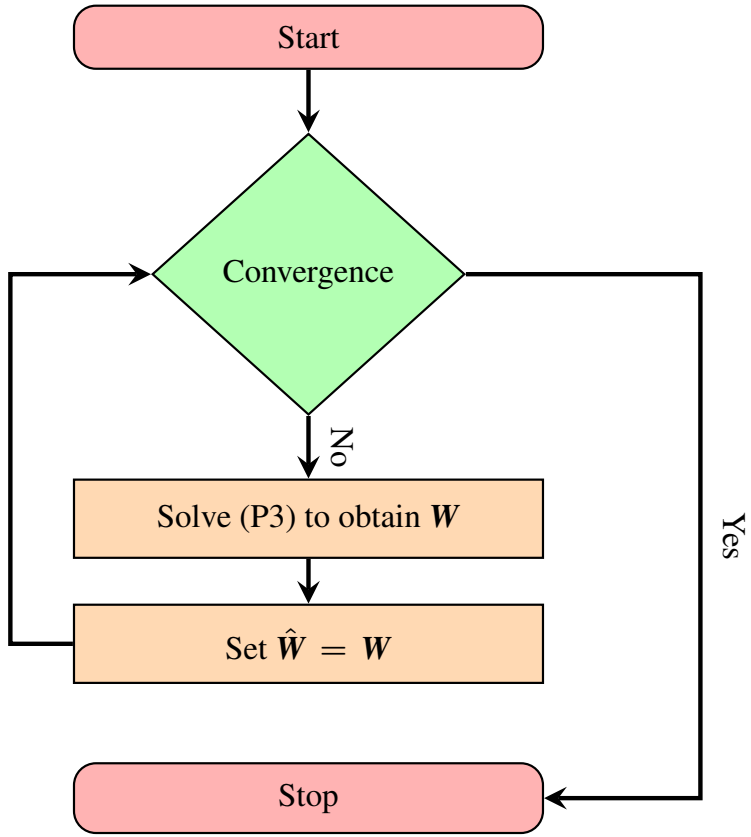
$G(\boldsymbol{W}, P_A, P_B)$ is monotonic in P_A for fixed P_B.

IRS phase shift optimization

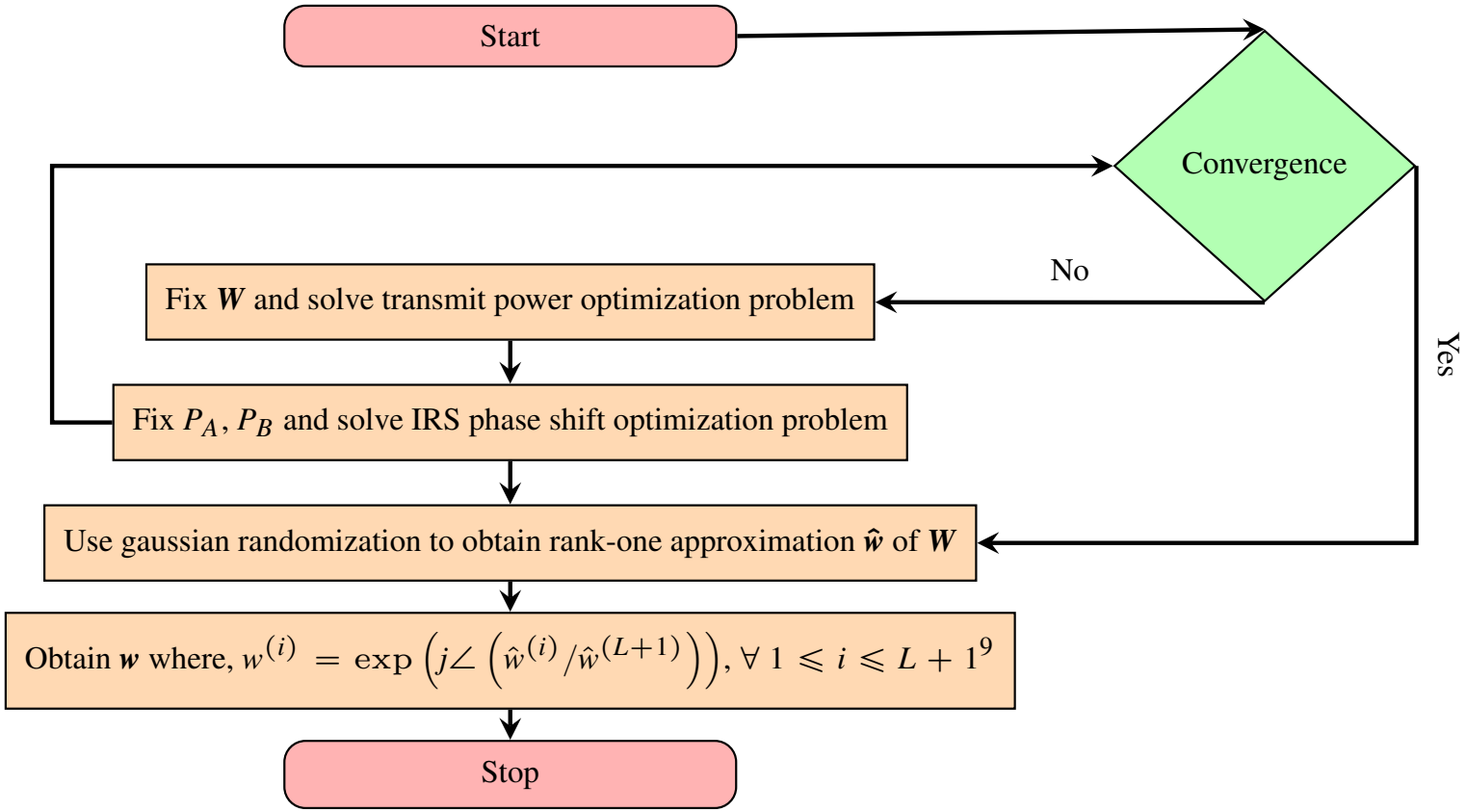
We apply first-order Taylor series expansion for $\log_2(F(\boldsymbol{W}, P_A, P_B))$ in $G(\boldsymbol{W}, P_A, P_B)$ around $\hat{\boldsymbol{W}}$ to obtain the lower-bound $G_{\hat{\boldsymbol{W}}}(\boldsymbol{W}, P_A, P_B)$.

$$\begin{aligned}
\text{(P3):} \underset{\boldsymbol{W}}{\text{maximize}} \quad & G_{\hat{\boldsymbol{W}}}(\boldsymbol{W}, P_A, P_B) && \text{(6a)} \\
\text{subject to} \quad & \boldsymbol{W} \succeq 0, && \text{(6b)} \\
& \operatorname{diag}(\boldsymbol{W}) = 1, && \text{(6c)} \\
& \left\| \boldsymbol{W} - \hat{\boldsymbol{W}} \right\| < \xi. && \text{(6d)}
\end{aligned}$$





Alternating optimization algorithm



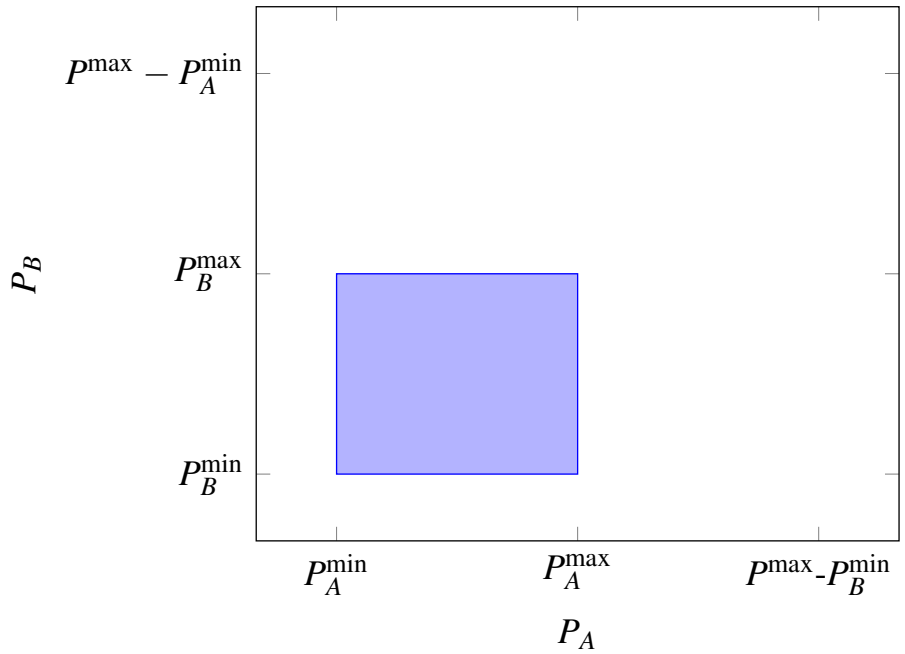
The detailed algorithm and the proof of convergence is provided in the paper. The computational complexity is $\mathcal{O}(I_o I_i L^6 + L^3 N_S)$.

[9] X. Guan, Q. Wu, and R. Zhang. "Intelligent Reflecting Surface Assisted Secrecy Communication: Is Artificial Noise Helpful or Not?" In: *IEEE Wireless Commun. Lett.* 9.6 (2020), pp. 778–782.

Extension to individual maximum power constraints

We employ the steps of the original algorithm with only the power optimization problem modified. The feasibility region of the power optimization problem is now a rectangle.

$$
\begin{aligned}
\text{(P4):} \quad \underset{P_A, P_B}{\text{maximize}} \quad & G(\boldsymbol{W}, P_A, P_B) && \text{(7a)} \\
\text{subject to} \quad & P_A^{\min} \leqslant P_A, && \text{(7b)} \\
& P_B^{\min} \leqslant P_B, && \text{(7c)} \\
& P_A \leqslant P_A^{\max}, && \text{(7d)} \\
& P_B \leqslant P_B^{\max}. && \text{(7e)}
\end{aligned}
$$



Outline

Simulation setup

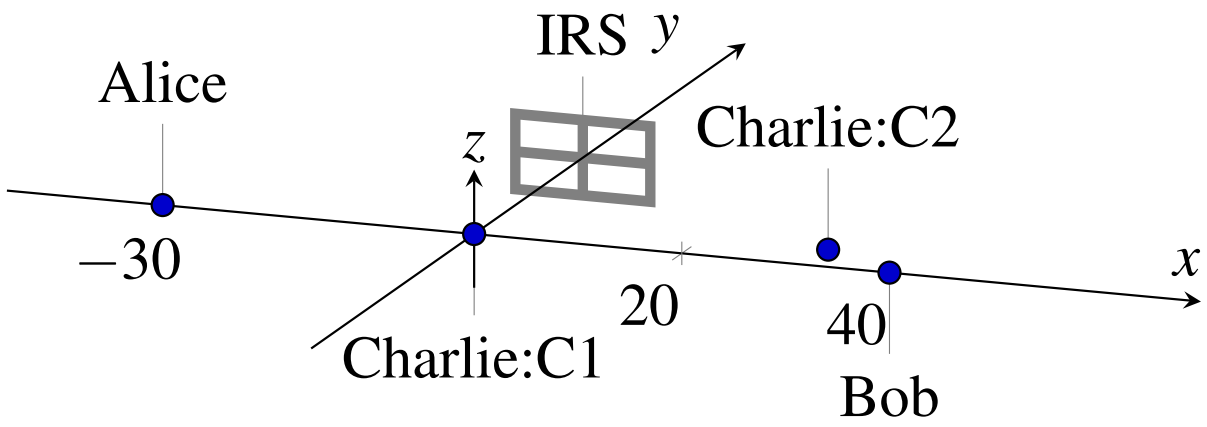


Figure 4: The simulation setup.

We consider two configurations.

- C1 - Charlie is close to the IRS.
- C2 - Charlie is close to Bob.

Convergence of the algorithm

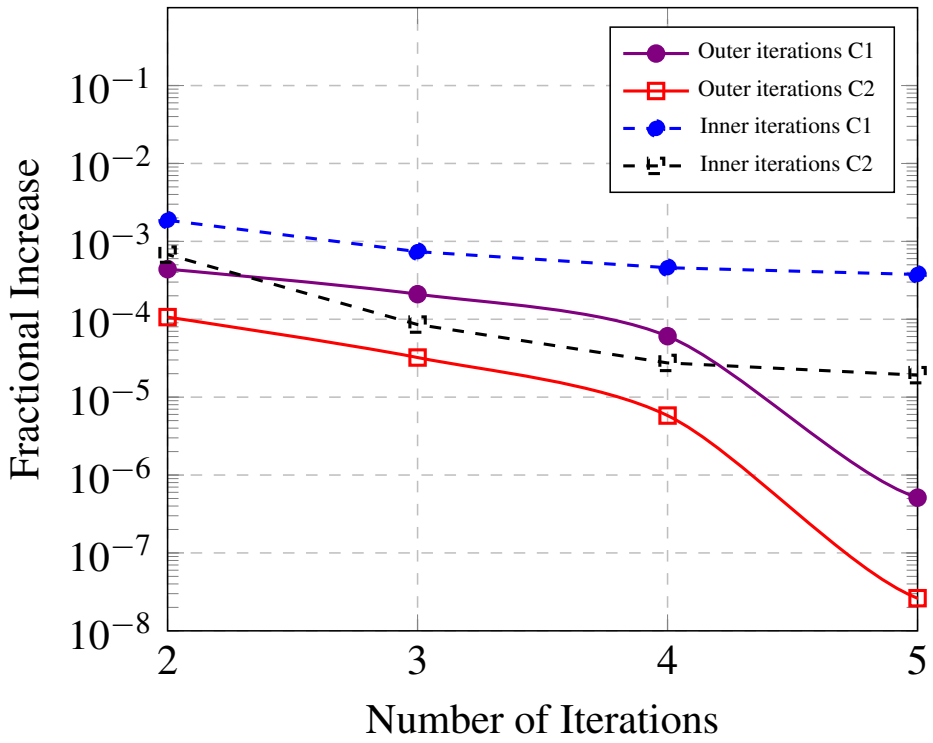


Figure 5: Average fractional increase of the objective vs no. of outer/inner iterations of Algorithm for $L = 20$.

Optimization schemes used for comparison

We compare the performance of the following beamformer design schemes with the proposed scheme.

- S:$(\boldsymbol{w}^*, \boldsymbol{P}^*)$ - the scheme introduced in the paper.
- S:$(\boldsymbol{w}^*, \boldsymbol{P}^{\text{box}})$ - the scheme with individual maximum power constraints.
- S:$(\boldsymbol{w}, \boldsymbol{P}^*)$ - the scheme with IRS phase shifts set randomly and the transmit powers optimized by solving the power optimization problem.
- S:$(\text{No-IRS}, \boldsymbol{P}^*)$ - the scheme without an IRS, where the transmit powers are optimized by solving the power optimization problem.

Exhaustive search

We adopt an exhaustive search based approach (scheme S:(ES, $\boldsymbol{P}^*$)) to compare the performance of the algorithm for smaller values of L.

Table 1: S:($\boldsymbol{w}^*, \boldsymbol{P}^*$) vs S:(ES, $\boldsymbol{P}^*$) for C1 and C2

L	C1		C2	
	S:($\boldsymbol{w}^*, \boldsymbol{P}^*$)	S:(ES, $\boldsymbol{P}^*$)	S:($\boldsymbol{w}^*, \boldsymbol{P}^*$)	S:(ES, $\boldsymbol{P}^*$)
1	2.417026	2.417026	0.091384	0.091384
2	2.487426	2.487426	0.097806	0.097806
3	2.550649	2.550650	0.103917	0.103917

Sum-secrecy rate vs number of IRS elements

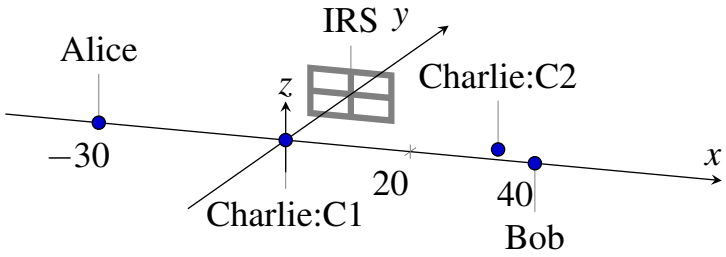


Figure 6: The simulation setup.

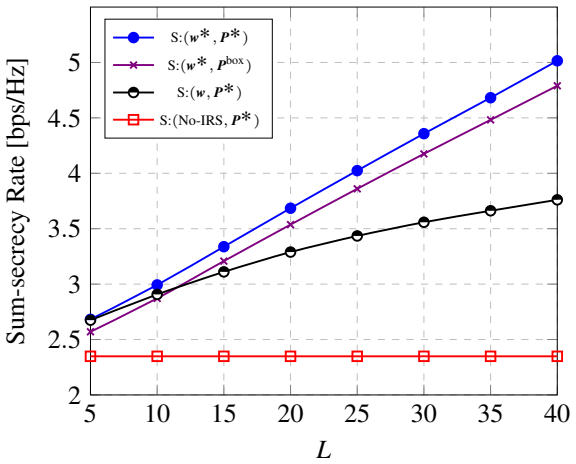


Figure 7: Sum-secrecy rate vs the number of IRS elements for C1.

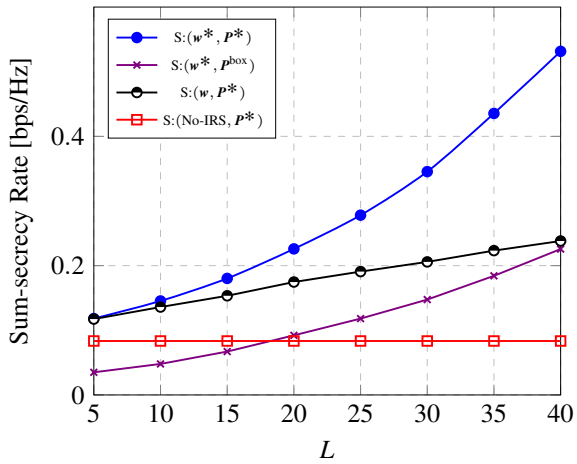


Figure 8: Sum-secrecy rate vs the number of IRS elements for C2.

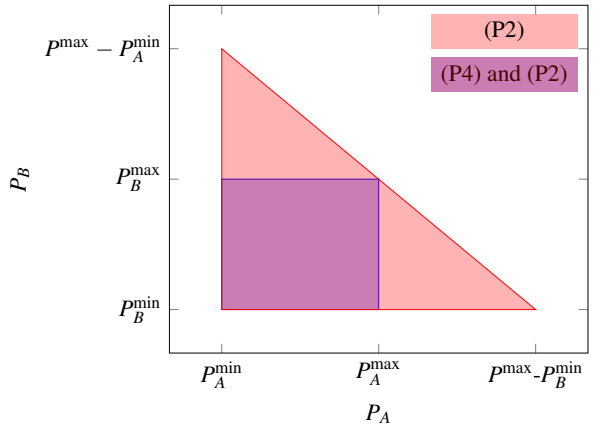


Figure 9: The feasibility regions for the power optimization problems of S:$(\boldsymbol{w}^*, \boldsymbol{P}^*)$ and S:$(\boldsymbol{w}^*, \boldsymbol{P}^{\text{box}})$

Outline

Conclusions

Following are the major conclusions of our work.

- An iterative algorithm to maximize the sum-secrecy rate of an IRS-aided two-way communication system by adjusting the user transmit powers and the IRS phase shifts is introduced.
- The convergence of the algorithm was proved analytically and fast convergence was illustrated numerically.
- The achievable sum-secrecy rate of the algorithm was compared with four baseline schemes and the performance gains were quantified.
- Maximizing secrecy fairness between users, multi-antenna systems and multi-user networks are possible future extensions of the work presented in this paper.

Thank You