Zelong CUI, Jun LIU, Gang YANG, 2024. XL-RIS empowered near-field physical layer security against jamming and eavesdropping attacks. *Front Inform Technol Electron Eng*, 25(12):1750-1758. https://doi.org/10.1631/FITEE.2400477

XL-RIS empowered near-field physical layer security against jamming and eavesdropping attacks

Key words: Near-field communications; Physical layer security; Extremely large-scale reconfigurable intelligent surface; Beamforming design; Reflection coefficient design

Corresponding author: Gang YANG
E-mail: yanggang@uestc.edu.cn
ORCID: https://orcid.org/0000-0002-3959-4761

Motivation

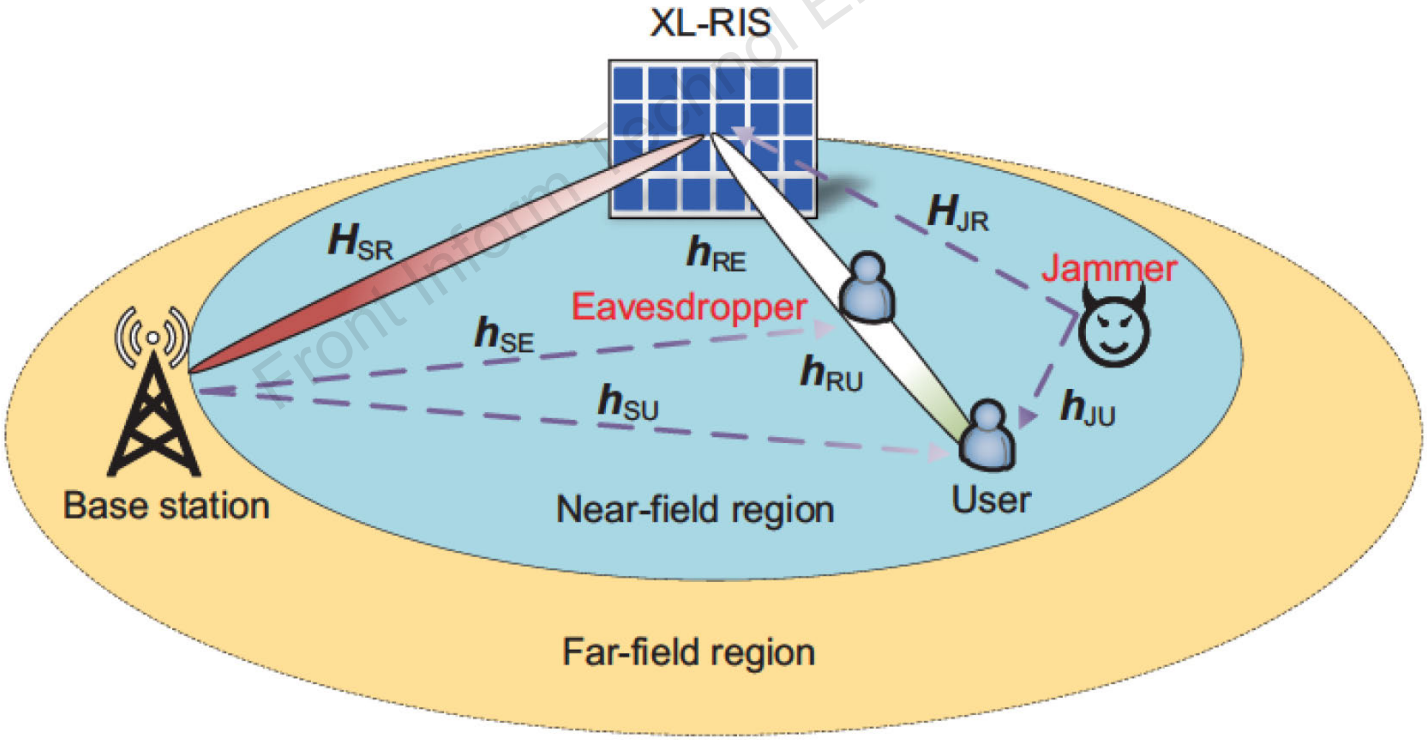
- The 6G networks start a new era of wireless communications with high speed, ultra-low latency, massive access, and strong security, which will support ubiquitous connectivity for various devices. Specifically, many applications involve sensitive information exchange, so it is crucial to ensure transmission security against malicious attacks, such as eavesdropping and jamming.
- XL-RIS can reconfigure an electromagnetic propagation environment and enhance secure communication. With the increase of array aperture and operating frequency, it becomes inevitable that wireless communication systems operate in the near-field region.
- The characteristics of electromagnetic propagation in the near field are modeled as a spherical-wave channel model. Compared with the planar-wave model, the spherical-wave channel model depends on both angular and distance, introducing the extra distance degree of freedom in the propagation characteristics.

Main idea

- We study an XL-RIS empowered near-field PLS communication system. An optimization problem is formulated to maximize the secrecy capacity of the communication system, subject to the transmit power and unit-modulus constraints.
- An AO-based algorithm is proposed to solve the optimization problem. For the beamforming and AN design at the BS, we propose an SCA-based algorithm. For the reflection coefficient matrix design at the XL-RIS, an MO-based algorithm is proposed to address the other subproblems with large-scale variables and unit-modulus constraints.

System model

- An XL-RIS empowered near-field communication system against jamming and eavesdropping attacks consists of a legitimate transmitter equipped with M (M>1) antennas, a legitimate user equipped with a single antenna, an eavesdropper equipped with a single antenna, and a jammer equipped with L (L>1) antennas.



Problem formulation and joint beamforming design

- We propose an AO-based algorithm to deal with the coupling optimization problem. First, when $\boldsymbol{\Theta}$ is fixed, we introduce auxiliary variables to reformulate the subproblem into a more tractable problem and then propose the SCA-based algorithm to solve the reformulated problem. Second, when $\boldsymbol{w}$ and $\boldsymbol{v}$ are fixed, we reformulate the subproblem at the XL-RIS and propose an MO-based algorithm to solve it.

$$\max_{\boldsymbol{w},\boldsymbol{v},\boldsymbol{\Theta}} C_{\mathrm{S}}\left(\boldsymbol{w},\boldsymbol{v},\boldsymbol{\Theta}\right)$$

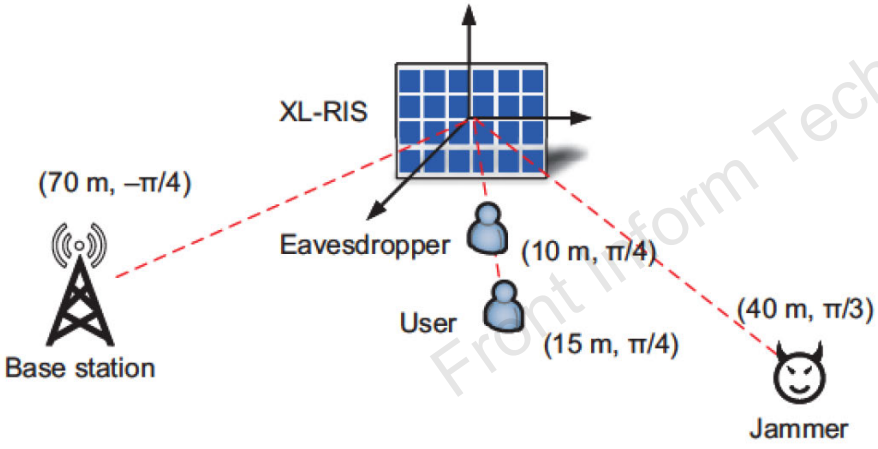
$$\text{s.t.} \begin{cases} \|\boldsymbol{w}\|_2^2 + \|\boldsymbol{v}\|_2^2 \leq P, \\ |\theta_i| = 1, \forall i = 1,2,\ldots,N, \end{cases}$$

Algorithm 1 Alternating optimization of $\boldsymbol{w}$, $\boldsymbol{v}$, and $\boldsymbol{\theta}$

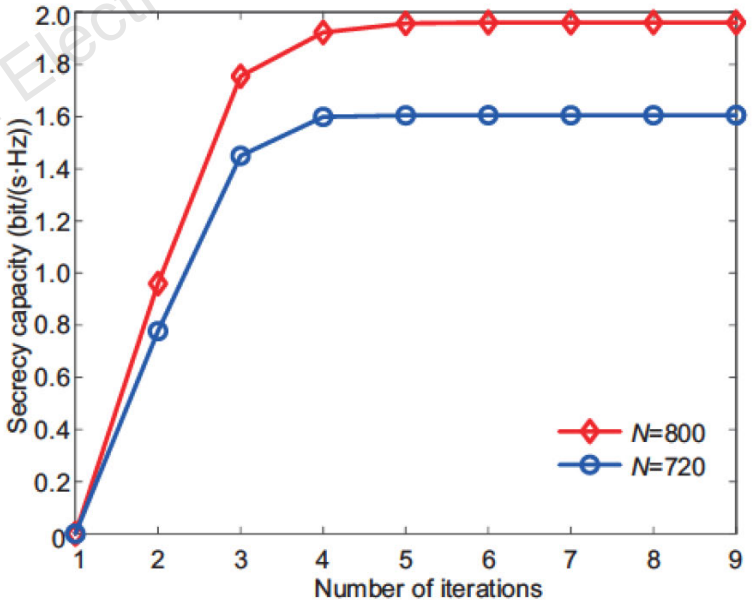
1: Initialization: secrecy capacity accuracy ε, beamforming vectors $\boldsymbol{w}^{(0)}$, $\boldsymbol{v}^{(0)}$, and $\boldsymbol{\theta}^{(0)}$, secrecy capacity $C_{\mathrm{S}}^{(0)}$ calculated by $\boldsymbol{w}^{(0)}$, $\boldsymbol{v}^{(0)}$, and $\boldsymbol{\theta}^{(0)}$, $t = 0$
2: **repeat**
3: $t = t + 1$
4: Update $\boldsymbol{w}$ and $\boldsymbol{v}$ by solving problem (18)
5: Update $\boldsymbol{\theta}$ by using the MO algorithm
6: Update $C_{\mathrm{S}}^{(t)}$ by using the updated $\boldsymbol{w}$, $\boldsymbol{v}$, and $\boldsymbol{\theta}$
7: **until** $\left|C_{\mathrm{S}}^{(t)} - C_{\mathrm{S}}^{(t-1)}\right| < \varepsilon$
Ensure: $C_{\mathrm{S}}^{\star}$

Numerical results

- It can be observed that the secrecy at the legitimate user increases monotonically and converges within a few number of iterations. Moreover, the secrecy capacity increases as the number of reflection elements of the XL-RIS increases.



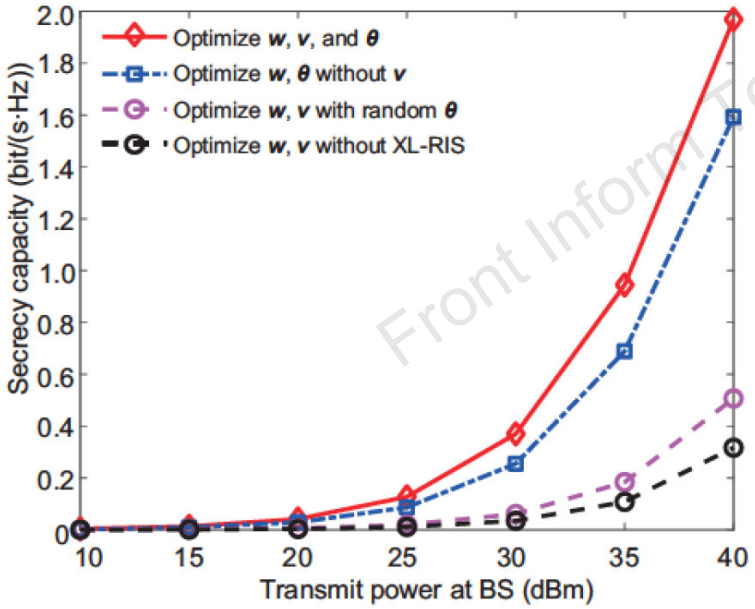
Deployment of an XL-RIS empowered near-field PLS communication system against jamming and eavesdropping



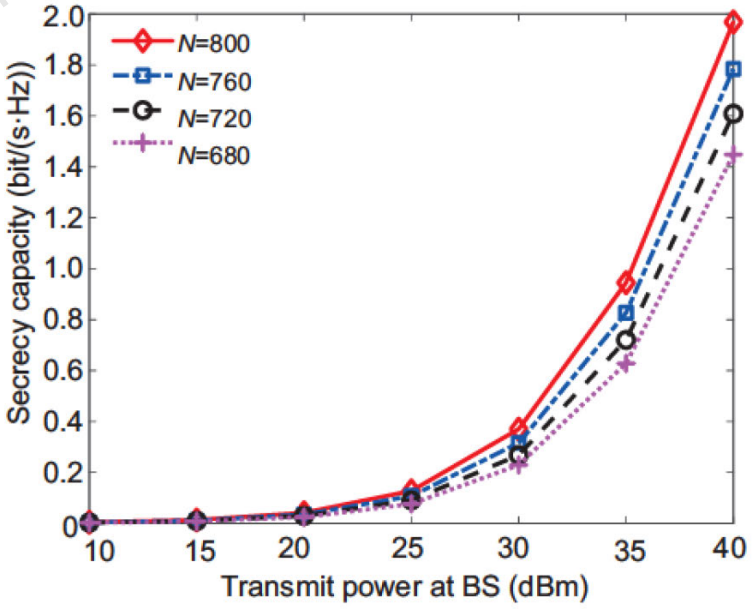
Convergence behaviors of the proposed algorithm for different sizes of XL-RIS

Numerical results

- The secrecy capacity of the proposed algorithm is higher than that of the three other baseline schemes, especially when the transmit power of the BS reaches 40 dBm.
- When the BS transmit power P is fixed, the secrecy capacity increases as the number of reflection elements increases.



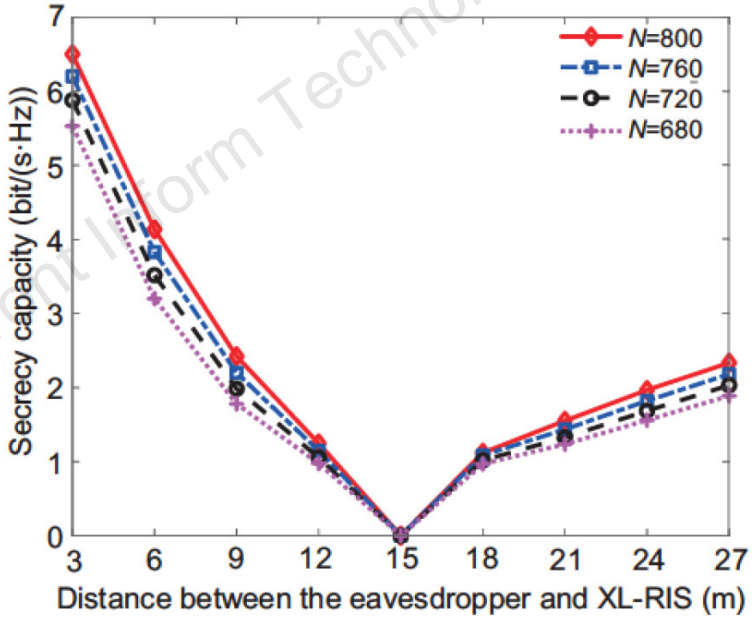
Secrecy capacity comparison versus transmit power P for different baseline schemes



Secrecy capacity comparison versus transmit power P for various sizes of XL-RIS N

Numerical results

- The secrecy capacity when the eavesdropper is at the same distance from the user but closer to XL-RIS (3 m) is higher than when it is further away from XL-RIS (27 m). This indicates that with the eavesdropper moving closer to XL-RIS, the beam focusing ability of XL-RIS becomes stronger. Consequently, less legitimate signal energy is leaked to the eavesdropper.



Secrecy capacity comparison versus locations of the eavesdropper for various sizes of XL-RIS *N*

Conclusions

- In this paper, we have studied an XL-RIS empowered near-field PLS communication system against jamming and eavesdropping attacks. We introduced artificial noise to contaminate the received legitimate signal at the eavesdropper and formulated an optimization problem. Numerical results demonstrated that:
  (1) XL-RIS can ensure secure communication even if the eavesdropper is located at the same direction as the legitimate user and closer to the XL-RIS, which cannot be realized in conventional far-field communications.
  (2) The secrecy capacity is improved as the size of the XL-RIS reflecting elements increases.
  (3) The artificial noise can improve the secrecy capacity.