IWCMC
The 20th International Wireless Communications & Mobile Computing Conference
27–31 May 2024 | Ayia Napa | Adams Beach Hotel, Cyprus

Deep Reinforcement Learning for IRS-assisted Secure NOMA Transmissions Against Eavesdroppers

Defeng Zhou, Shimin Gong, Lanhua Li, Bo Gu, Mohsen Guizani

Presented by **Defeng Zhou**
Email:zhoudf5@mail2.sysu.edu.cn
Affiliation: Sun Yat-sen University & MBZUAI

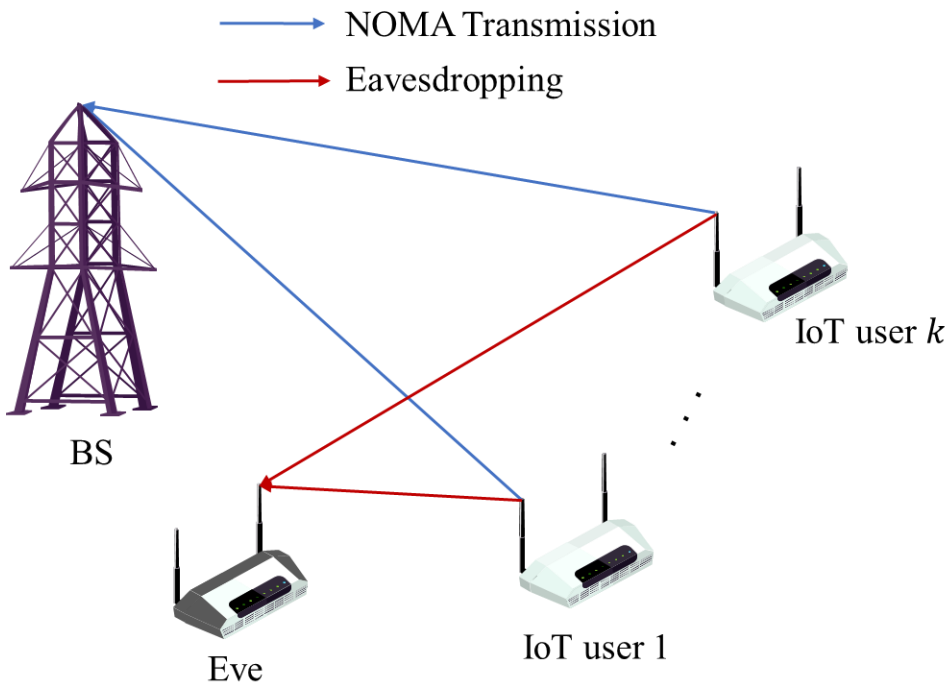
Outline

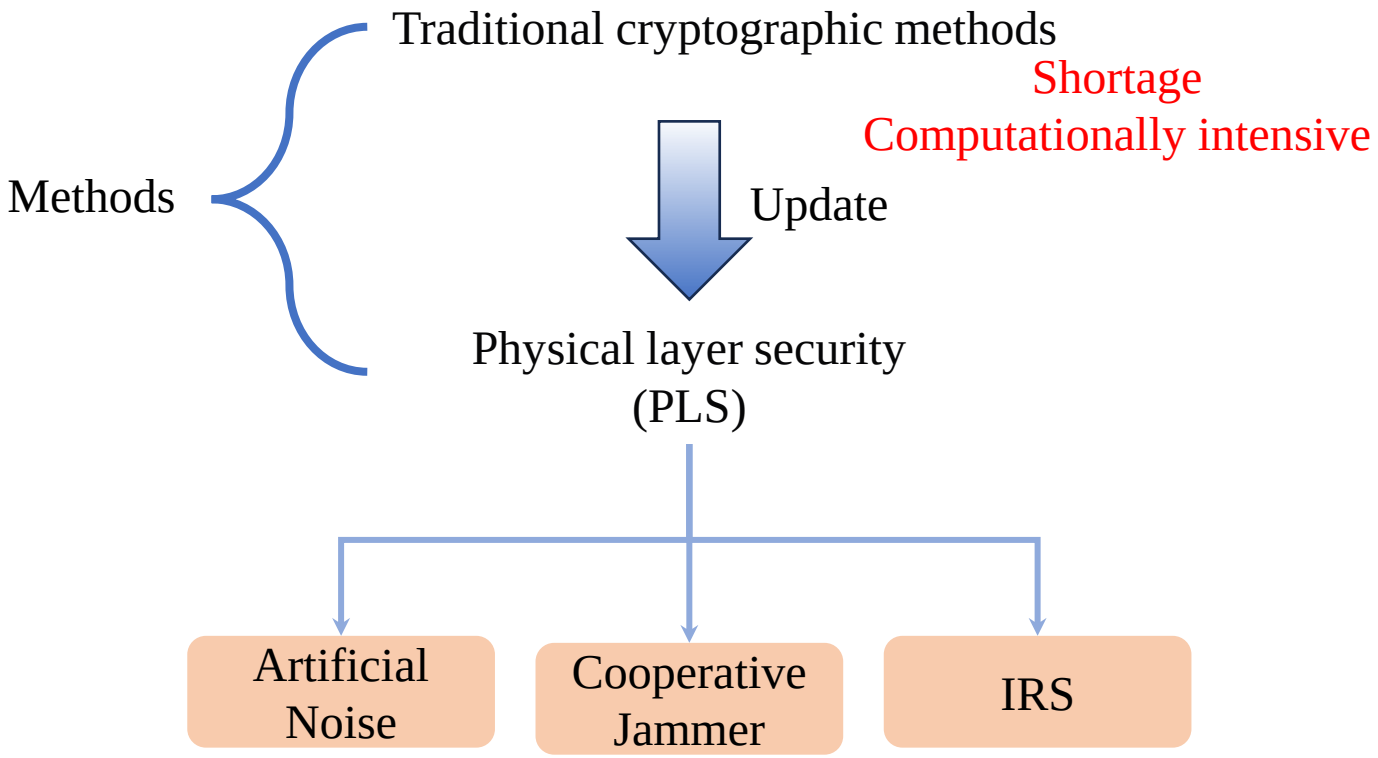
- ☐ **Background and Motivations**
- ☐ **IRS-assisted NOMA Secure Transmissions against Eavesdroppers**
- ☐ **Problem Formulation**
- ☐ **Results and Conclusions**

Background and Motivations

Secure Transmissions in 6G RANs

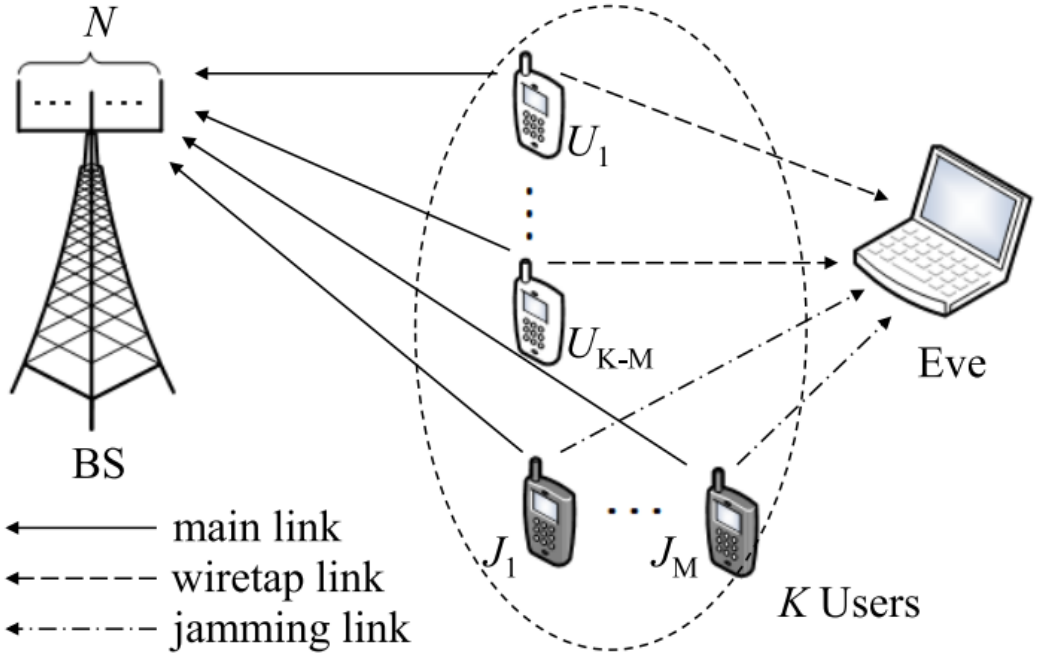
Ensuring data security is a growing focal point within sixth-generation radio access networks (6G-RANs).



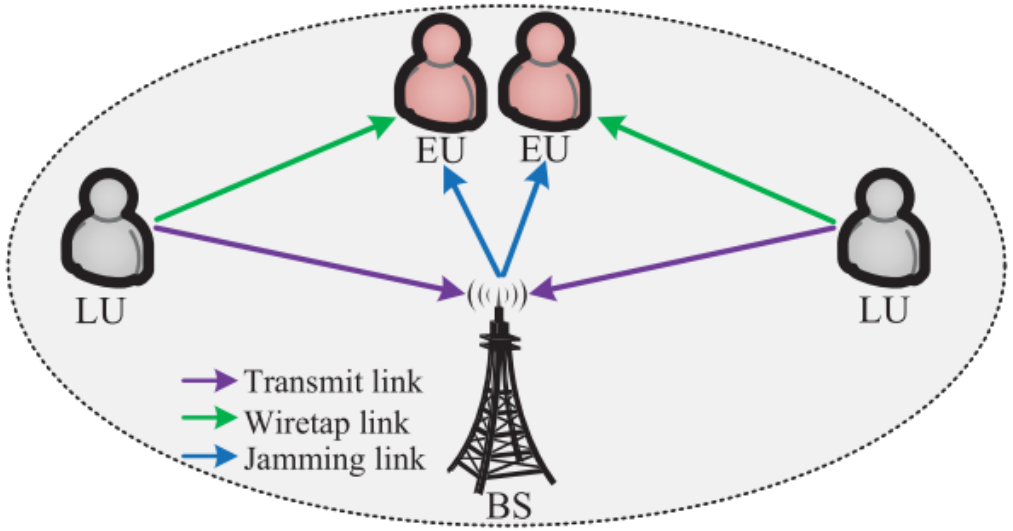


Background and Motivations

Existing PLS Methods



Cooperative Jammer(CJ)

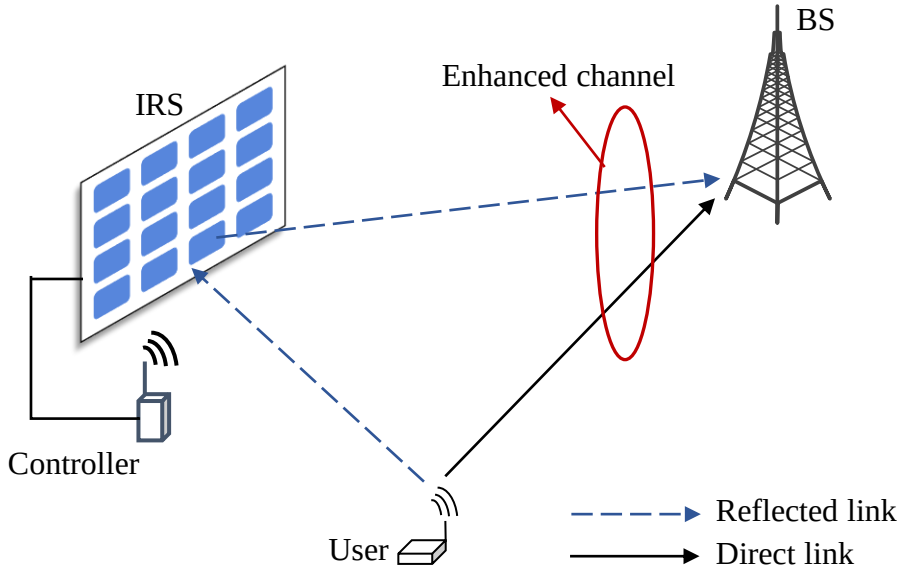


Artificial Noise(AN)

Disadvantage: Energy-Consuming, Dedicated devices

Background and Motivations

What is intelligent reflecting surface (IRS)?

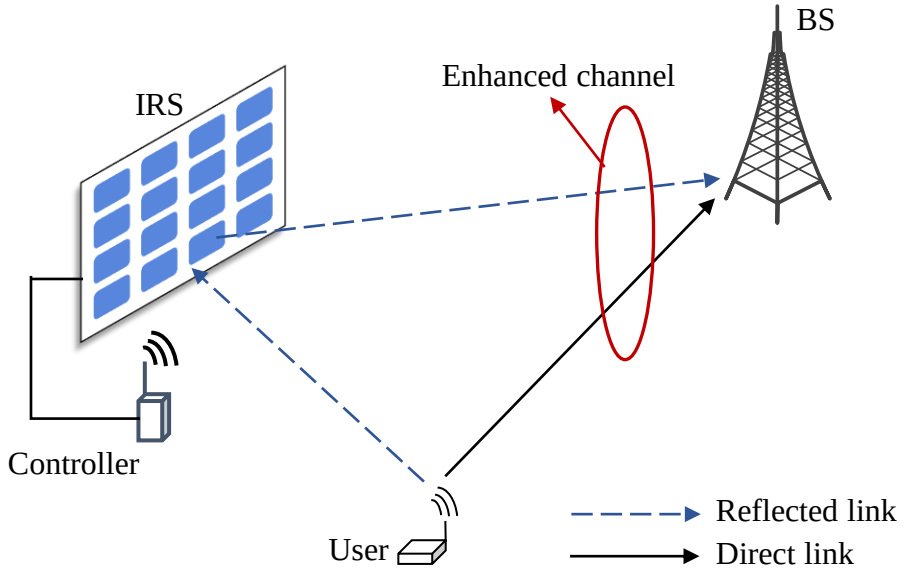


- Intelligent reflecting surface (IRS) with massive low-cost passive reflecting elements (each is able to induce an phase change in the incident signal)

- Low energy consumption (without the use of any transmit RF chains), high spectral efficiency (full-duplex, noiseless reflection)

Background and Motivations

What is intelligent reflecting surface (IRS)?

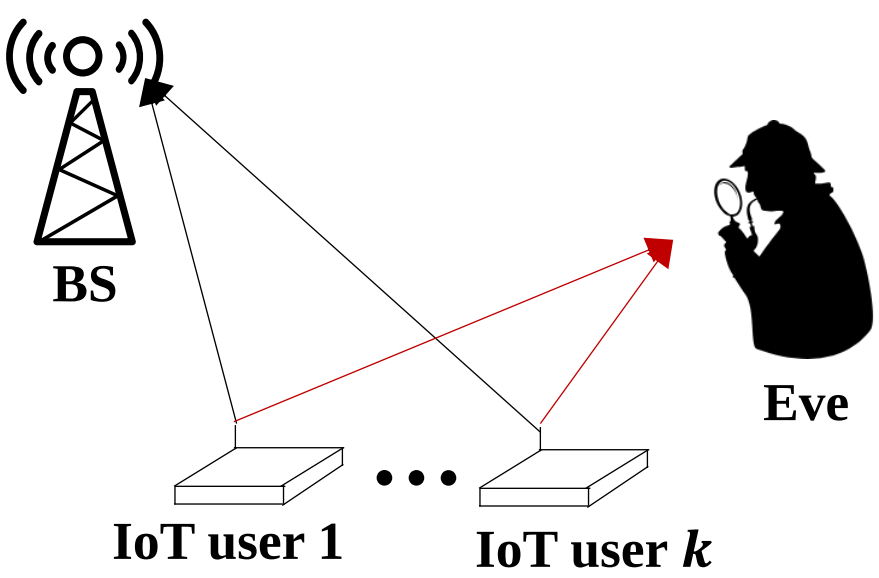


- Intelligent reflecting surface (IRS) with massive low-cost passive reflecting elements (each is able to induce an phase change in the incident signal)

- Low energy consumption (without the use of any transmit RF chains), high spectral efficiency (full-duplex, noiseless reflection)

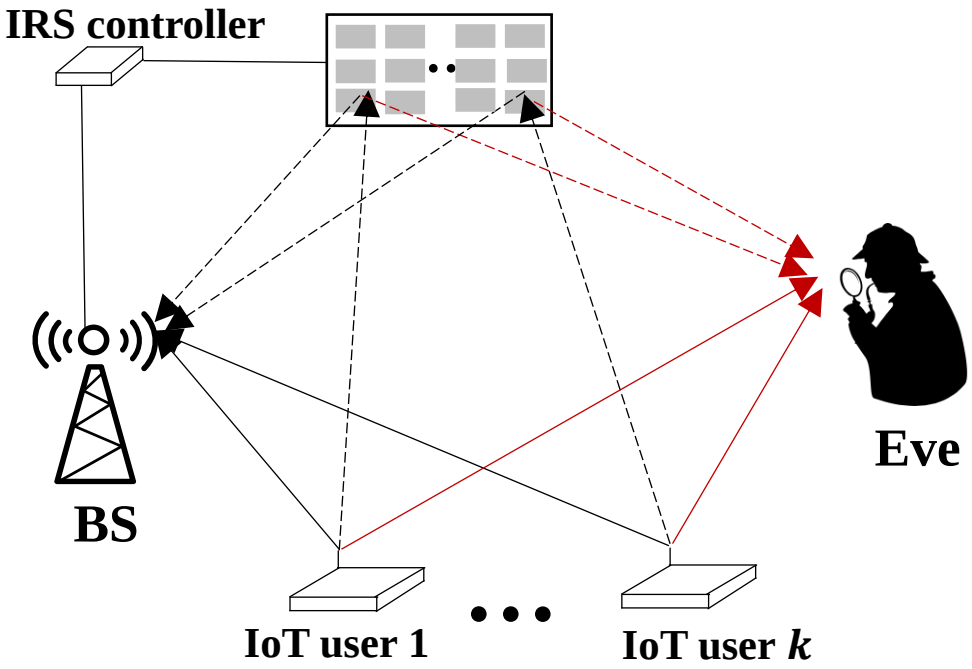
Background and Motivations

How to unleash the potential of IRS in the secure transmission



Integrate IRS into NOMA systems

Optimize IRS beamforming



(a) The IRS can be used to enhance the NOMA users' sum rates

(b) The IRS also could weaken the Eve's channel condition, causing the inter-user interference at the Eve, which could be seen as an artificial noise

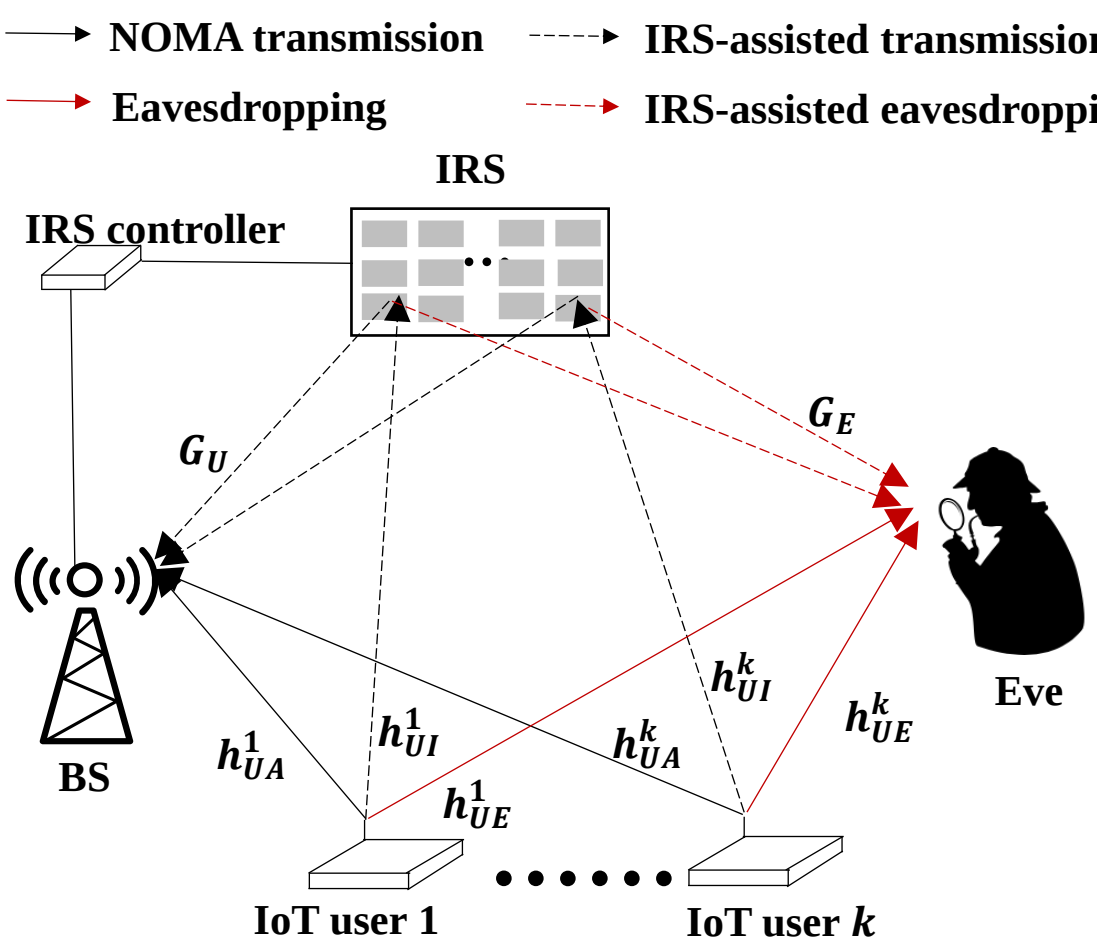
Outline

- Background and Motivations
- **IRS-assisted NOMA Secure Transmissions against Eavesdroppers**
- Problem Formulation
- Results and Conclusions

IRS-assisted NOMA Secure Transmissions against Eavesdroppers

What do we need to optimize to guarantee the security

We investigate an IRS-assisted uplink secure NOMA system, including a multi-antenna AP with N, antennas, a single-antenna Eve, an IRS with a set of reflection elements, and K single-antenna IoT users



How to maximize the secure performance?

- IRS beamforming Θ
- Schedule policy Φ
  Bit indicator for every device $\phi_k \in [0,1]$
- BS receive beamforming w

Constraints: SINR thresholds at the BS

$$\gamma_k(t) = \frac{p|f_U^k(t)\omega(t)|^2}{\sum_{i>k}^{K}\phi_i(t)p|f_U^i(t)\omega(t)|^2+\sigma_u^2} \geq \gamma_{min}$$

Outline

- Background and Motivations
- IRS-assisted NOMA Secure Transmissions against Eavesdroppers
- **Problem Formulation**
- Results and Conclusions

Secure Rate Maximization Formulation

We formulate the average secure rate maximization problem by jointly optimizing the users' scheduling policy $\widetilde{\Phi} \triangleq \{\Phi(t)\}_{t\in T}$, the AP's receive beamforming $\widetilde{\omega} = \{\omega(t)\}_{t\in T}$, and the IRS's passive beamforming $\widetilde{\Theta} \triangleq \{\Theta(t)\}_{t\in T}$, subject to the individual users' SINR constraints.

$$\max_{\widetilde{\Theta},\widetilde{\omega},\widetilde{\Phi}} \frac{1}{T}\sum_{t=1}^{T}\sum_{k=1}^{K}(R_U^k(t) - R_E^k(t))^+$$ → Maximum secure rate of the system

s.t. $\gamma_k \geq \gamma_{min}, if\ \phi_k > 0, \forall k \in K,$ → Individual users' SINR constraints

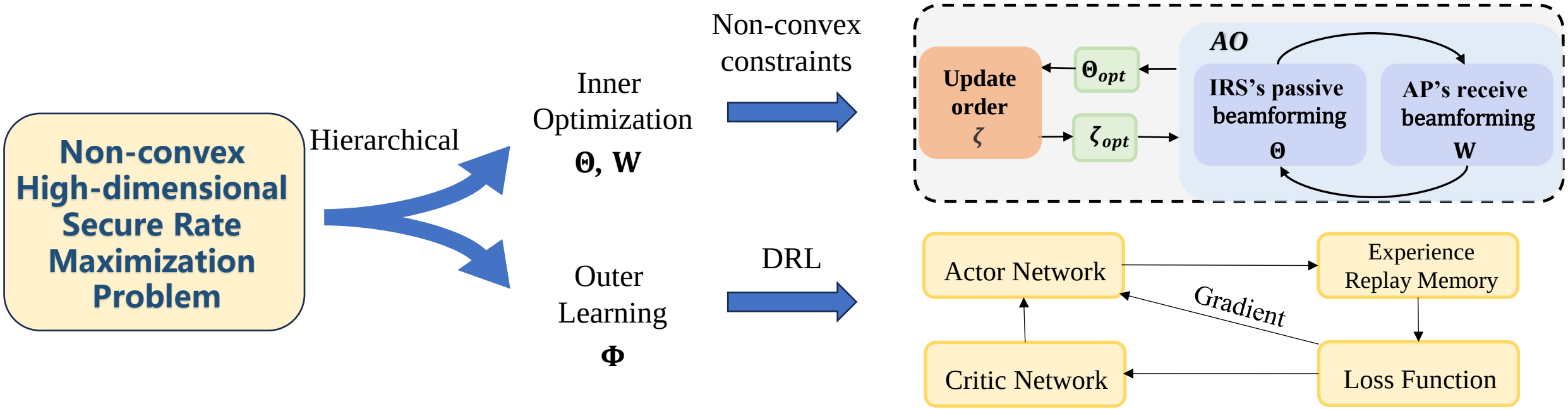
$\theta_m \in (0,2\pi], \forall m \in M,$ → Passive beamforming of the IRS

$\| \omega(t) \| = 1, \forall t \in T.$ → Receive beamforming of the AP

Problem Formulation

Solution to Non-convex Complex Problem

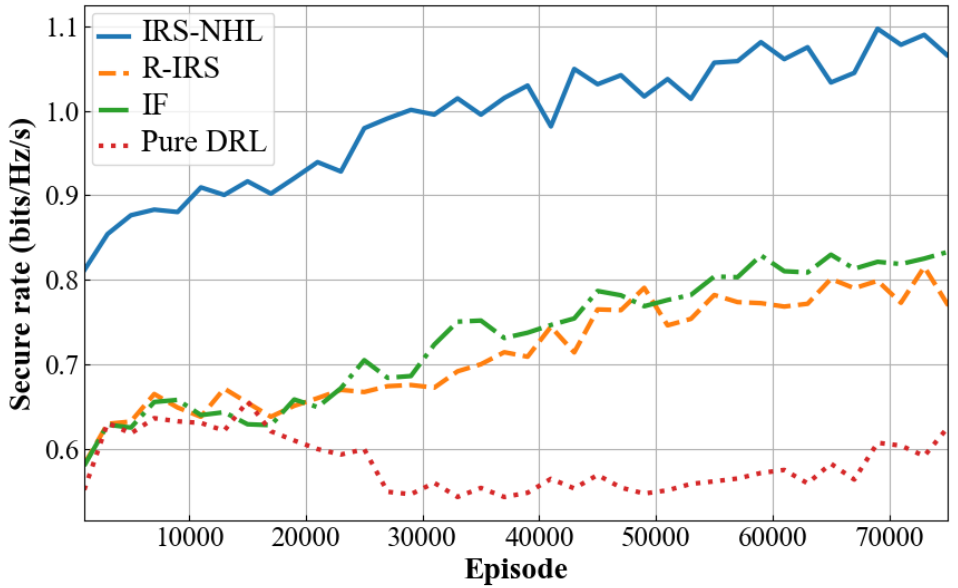
In order to solve the non-convex and high-dimensional problem, we propose a novel hierarchical framework which can be decomposed into the outer learning phase for the users' scheduling strategy and the inner optimization phase for beamforming strategy.



Outline

- Background and Motivations
- IRS-assisted NOMA Secure Transmissions against Eavesdroppers
- Problem Formulation
- **Results and Conclusions**

Results and Conclusions

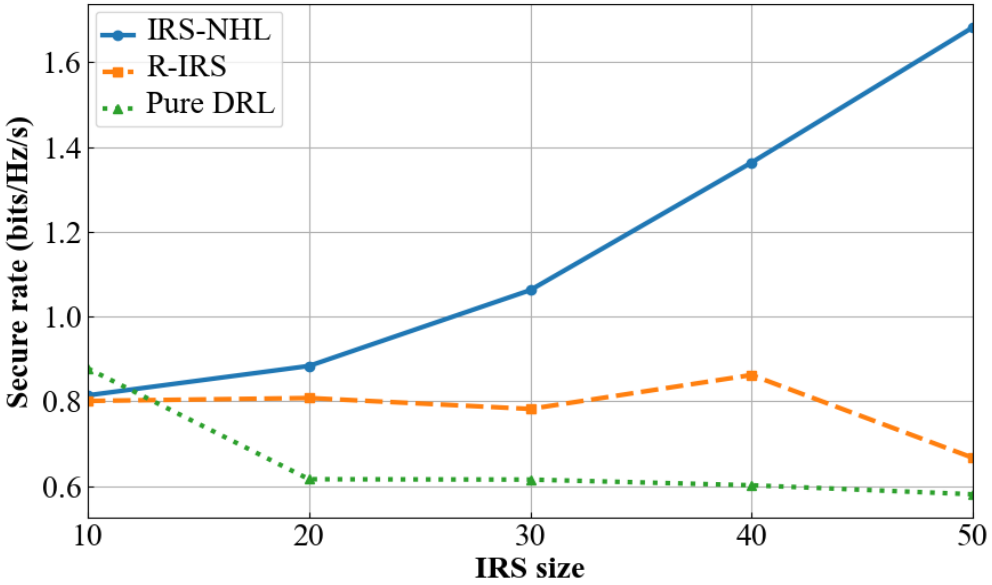


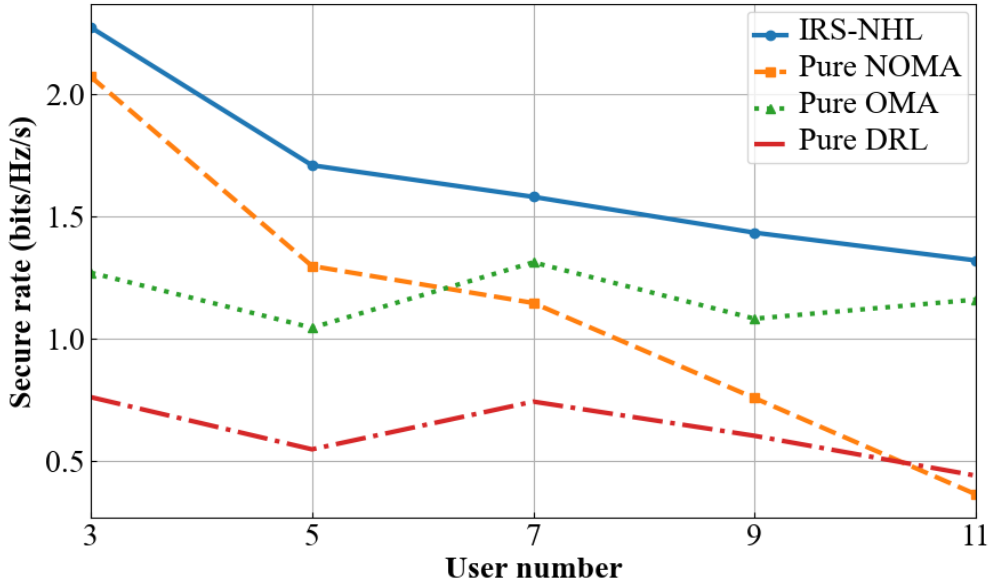
"IRS-NHL" scheme converge at a high value

Compare to the “IF” and “R-IRS”: validate the role of optimizing IRS’s beamforming

Compare to the “Pure DRL” : validate the role of hierarchical DRL framework

Results and Conclusions





- The small-size IRS plays a limited role in assisting the network performance
- "Pure DRL" gradually deteriorates due to the larger action space caused by the increasing IRS size.
- "R-IRS" could not work well since the phase of IRS shifts randomly.

- "IRS-NHL" could schedule the user intelligently
- "Pure NOMA" decreases sharply because the intel-user interference at the AP increases as the increase of scheduled user number.
- "Pure DRL" gradually deteriorates due to the larger action space caused by the increasing number of users

Results and Conclusions

Conclusions

- IRS-assisted NOMA secure Transmission
  - Explore the potential of security enhancement by integrating IRS into NOMA systems instead of turning to a cooperative jammer or dedicated artificial noise.
  - Propose a novel hierarchical framework to solve the non-convex, high-dimensional problem
  - Introduce the PPO-based DRL to optimize the schedule policy, balancing between the sum rates and the security risks in NOMA systems.

Promising Directions for Future Work

- More flexible approach to guarantee the security in the environment closer to reality
- Low complexity algorithm design
- Scalability in the number of the Eavesdropper

Questions & Answers

Thanks for listening!

Contact: zhoudf5@mail2.sysu.edu.cn