



CYCU ICE  
12/23/2025

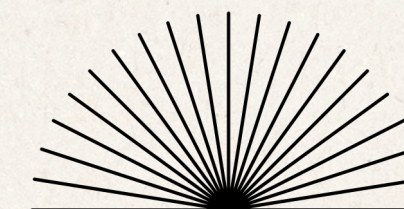
# Mobile Network Security Final Report

## NAME OF PAPER:

Secure Beamforming and  
Power Allocation for  
RIS-Assisted NOMA-ISAC Systems  
With  
Internal and External Eavesdroppers

## PRESENTED BY:

11127229 廖翊崴





# Agenda

00	議程
01	Overview
03	主要貢獻
04	主要演算法設計
10	模擬與結果
13	總結



# Overview

**標題：**具備內部與外部竊聽者之 RIS 輔助 NOMA-ISAC 系統的安全波束成形與功率分配

**問題：**在 ISAC 系統中，如何利用 RIS 與 NOMA 技術來提升安全性，尤其是同時面對內部竊聽者（合法用戶互相竊聽）和 外部竊聽者（非法竊聽者）的情境

**概覽：**ISAC + NOMA + RIS 的安全問題

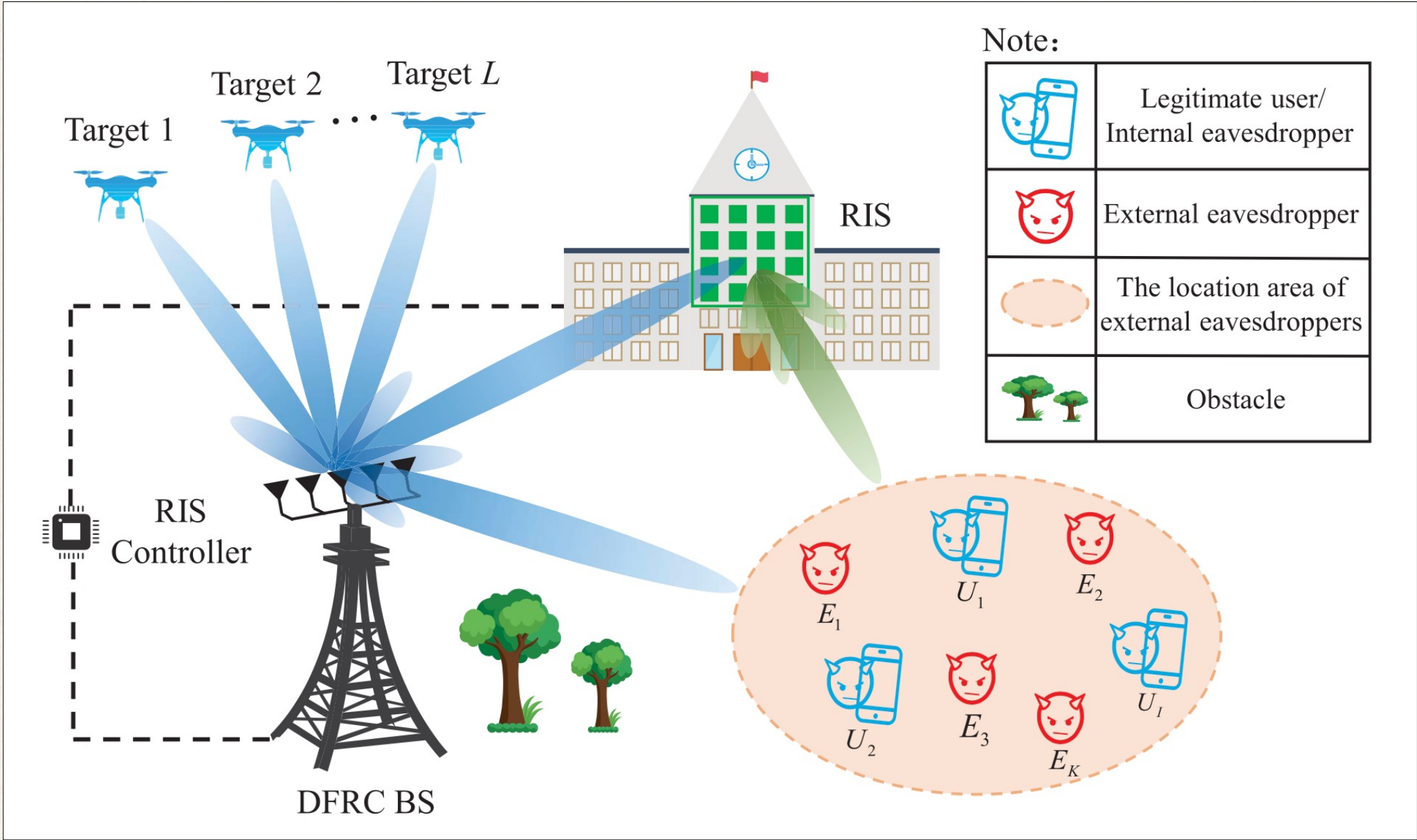
雙重竊聽者：內部竊聽（合法通信用戶）和外部竊聽（非法）

外部竊聽 CSI 不可得 → 傳統 secrecy rate 失效

**解法核心：**少給通訊功率，多給 radar / AN



RIS 輔助之 NOMA-ISAC 安全系統  
示意圖，其中包含一個 DFRC 基  
站、一個被動式 RIS、L 個感知目  
標、I 個合法通信用戶（亦即內部  
竊聽者），以及 K 個隨機分佈於  
作業區域內的外部竊聽者





# 主要貢獻

- 首次在 RIS-NOMA-ISAC 框架下同時考慮內部與外部竊聽者，並納入不完美 SIC。
- 在通道選擇策略上利用 NOMA 解碼順序，選擇性地破壞部分內部竊聽者通道，降低竊聽能力。
- 建立一個同時滿足通信速率、安全性與感知性能的安全波束成形與功率分配問題。
- 提出 SDR + Penalty AO 演算法，並分析收斂性與計算複雜度。
- 延伸至不完美 CSI 的情境，提出 robust beamforming scheme，保證系統的安全性與性能，不會因通道估計誤差而導致安全性能大幅下降。

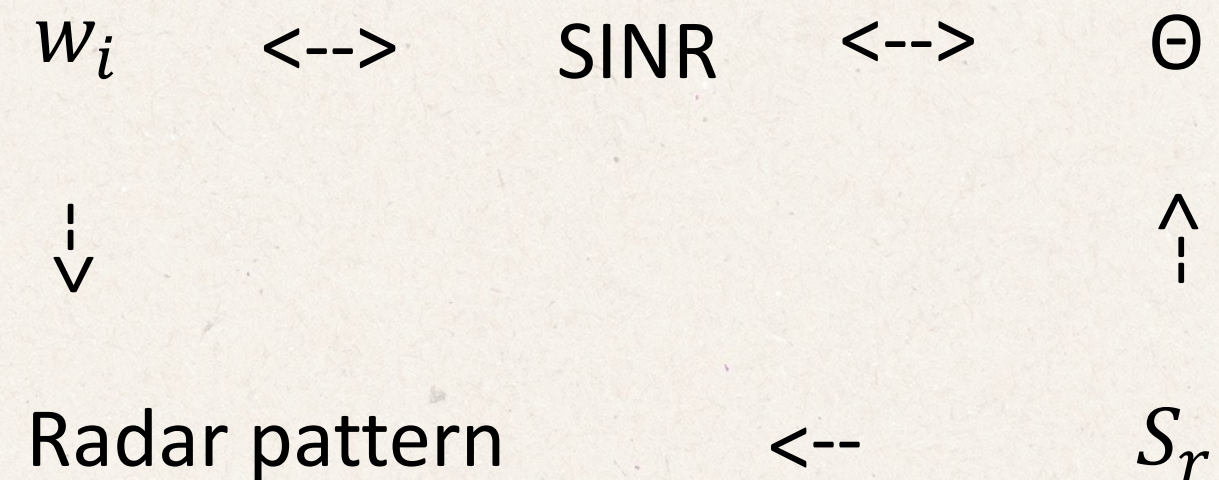


# 主要演算法設計

- Why Is the Optimization Difficult ?

目標是最小化通訊功率，但同時要滿足通訊 QoS、內部竊聽限制、雷達 Beampattern。

變數 BS beamforming、RIS phase、Radar covariance，彼此高度耦合。



$$\min \sum_i \|\mathbf{w}_i\|^2$$



- No CSI ? Increase AN Power

- 外部竊聽 CSI 不可得
- 傳統 secrecy rate 不可算
- 解法：固定總功率、最小化通訊功率、剩下全給 radar / AN

Total Power：Communication 下降；Radar / AN 上升

$$\mathbf{s} = \sum_{i=1}^I \mathbf{w}_i x_i + \mathbf{s}_r$$

S：基站的總發射信號

I：系統中合法用戶的數量

w\_i：第 i 個用戶的波束成形向量（beamforming vector）

x\_i：第 i 個合法用戶的通信信號

s\_r：雷達信號（人工噪聲 AN）



- 合法用戶 / 內部竊聽者的 SINR

$$\text{SINR}_{\mathbf{U}_i}^{\mathbf{U}_j} = \frac{|\mathbf{g}_{\mathbf{U}_i}^H \mathbf{w}_j|^2}{\bar{I}_i^j + \beta(\tilde{I}_i^j + \mathbf{g}_{\mathbf{U}_i}^H \mathbf{S}_r \mathbf{g}_{\mathbf{U}_i}) + \sigma_U^2}, \forall i, j$$

對象：第  $i$  個合法用戶（同時可能是內部竊聽者）

意涵：描述合法用戶在進行逐次干擾消除（SIC）後，解碼第  $j$  個訊號時的 SINR

特點：考慮了不完美 SIC（殘留干擾因子  $\beta$ ），因此不是理想化的情況

- 外部竊聽者的 SINR

$$\text{SINR}_{\mathbf{E}_k}^{\mathbf{U}_j} = \frac{|\mathbf{g}_{\mathbf{E}_k}^H \mathbf{w}_j|^2}{\mathbf{g}_{\mathbf{E}_k}^H \mathbf{S}_r \mathbf{g}_{\mathbf{E}_k} + \sum_{i=1, i \neq j}^I |\mathbf{g}_{\mathbf{E}_k}^H \mathbf{w}_i|^2 + \sigma_E^2}, \forall i, j$$

對象：第  $k$  個外部竊聽者

意涵：描述外部竊聽者在嘗試解碼第  $j$  個訊號時的 SINR

特點：外部竊聽者無法使用 SIC，因此干擾項包含所有其他用戶的訊號



## ● 通道選擇策略（Channel Selection）

- 若同時考慮所有內部竊聽者通道，優化問題會變得不可解。

策略：利用 NOMA 解碼順序，選擇性地破壞部分通道，降低內部竊聽者的解碼能力。

效果：在保證合法用戶通信速率的同時，削弱內部竊聽者的竊聽性能。

解碼順序的功率條件為以下，用來決定 NOMA 解碼順序，

並作為通道選擇的依據：

$$\mathbf{g}_{U_i}^H \mathbf{S}_r \mathbf{g}_{U_i} \geq |\mathbf{g}_{U_i}^H \mathbf{w}_1|^2 \geq \cdots \geq |\mathbf{g}_{U_i}^H \mathbf{w}_I|^2$$

$$\mathbf{g}_{U_i}^H = \mathbf{h}_{B,U_i}^H + \mathbf{h}_{R,U_i}^H \mathbf{\Theta} \mathbf{H}_{B,R}.$$



## ● SDR + Penalty AO 演算法框架

挑戰：原始問題是非凸優化，難以直接求解。

- SDR (Semidefinite Relaxation)：將 rank-one 約束鬆弛為半定規劃問題。
- AO (Alternating Optimization)：交替優化波束成形與功率分配。
- Penalty Iteration：加入懲罰項，逼近 rank-one 解，避免 SDR 過度鬆弛。

優點：演算法收斂性可證，計算複雜度可分析

發射信號的共變異數矩陣：

$$\mathbf{R}_s = \mathbb{E}\left\{\mathbf{s}\mathbf{s}^H\right\} = \sum_{i=1}^I \mathbf{w}_i \mathbf{w}_i^H + \mathbf{S}_r.$$

beam pattern 誤差 (MSE)：

$$L(\eta, \mathbf{R}_s) = \frac{1}{S} \sum_{s=1}^S \left| \eta \hat{p}(\theta_s) - \mathbf{a}_L^H(\theta_s) \mathbf{R}_s \mathbf{a}_L(\theta_s) \right|^2$$



## ● Robust Beamforming 設計

- 外部竊聽者 CSI 不可得，合法用戶 CSI 也可能有估計誤差。

設計思路：在不完美 CSI 的情境下，提出強健波束成形方案，確保安全性能不因通道誤差而大幅下降。

發射波束圖可表示為：

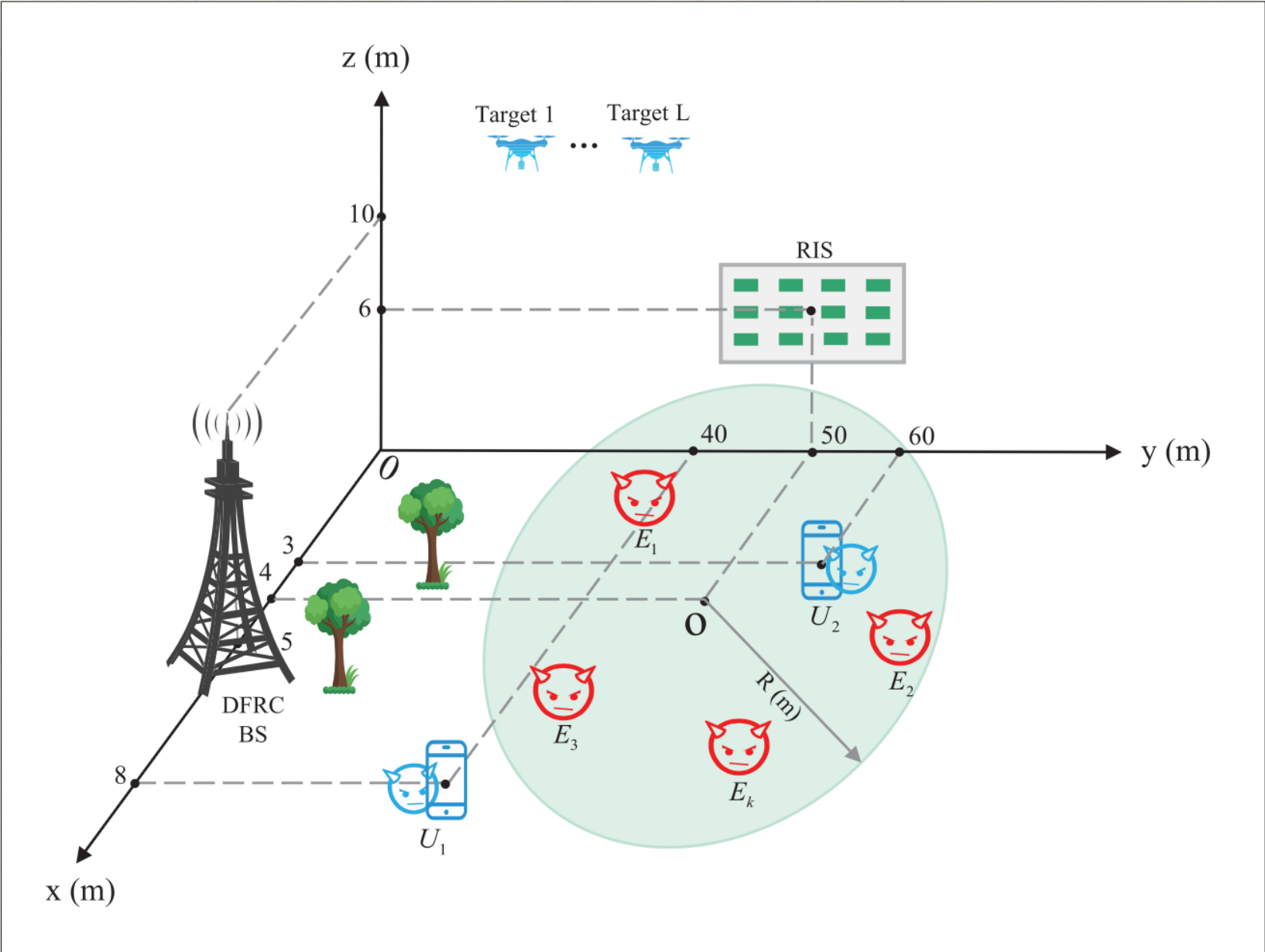
$$p(\theta) = \mathbb{E} \left\{ |\mathbf{a}_L^H(\theta) \mathbf{s}|^2 \right\} = \mathbf{a}_L^H(\theta) \mathbf{R}_s \mathbf{a}_L(\theta).$$

理想波束圖定義：

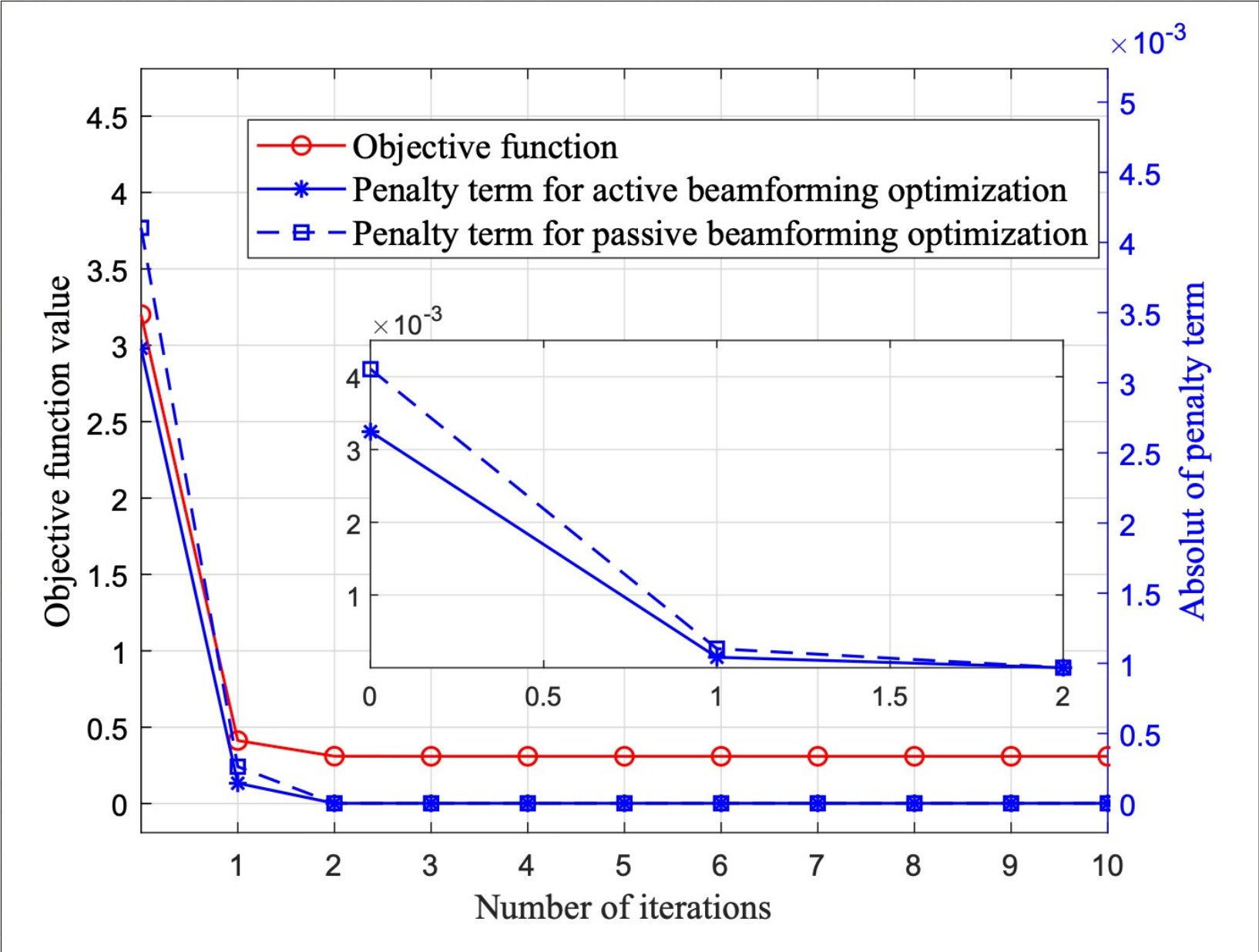
$$\hat{p}(\theta) = \begin{cases} 1, & \theta_l - \frac{\Delta\theta}{2} \leq \theta \leq \theta_l + \frac{\Delta\theta}{2}, \\ 0, & \text{otherwise,} \end{cases}$$



# 模擬與結果

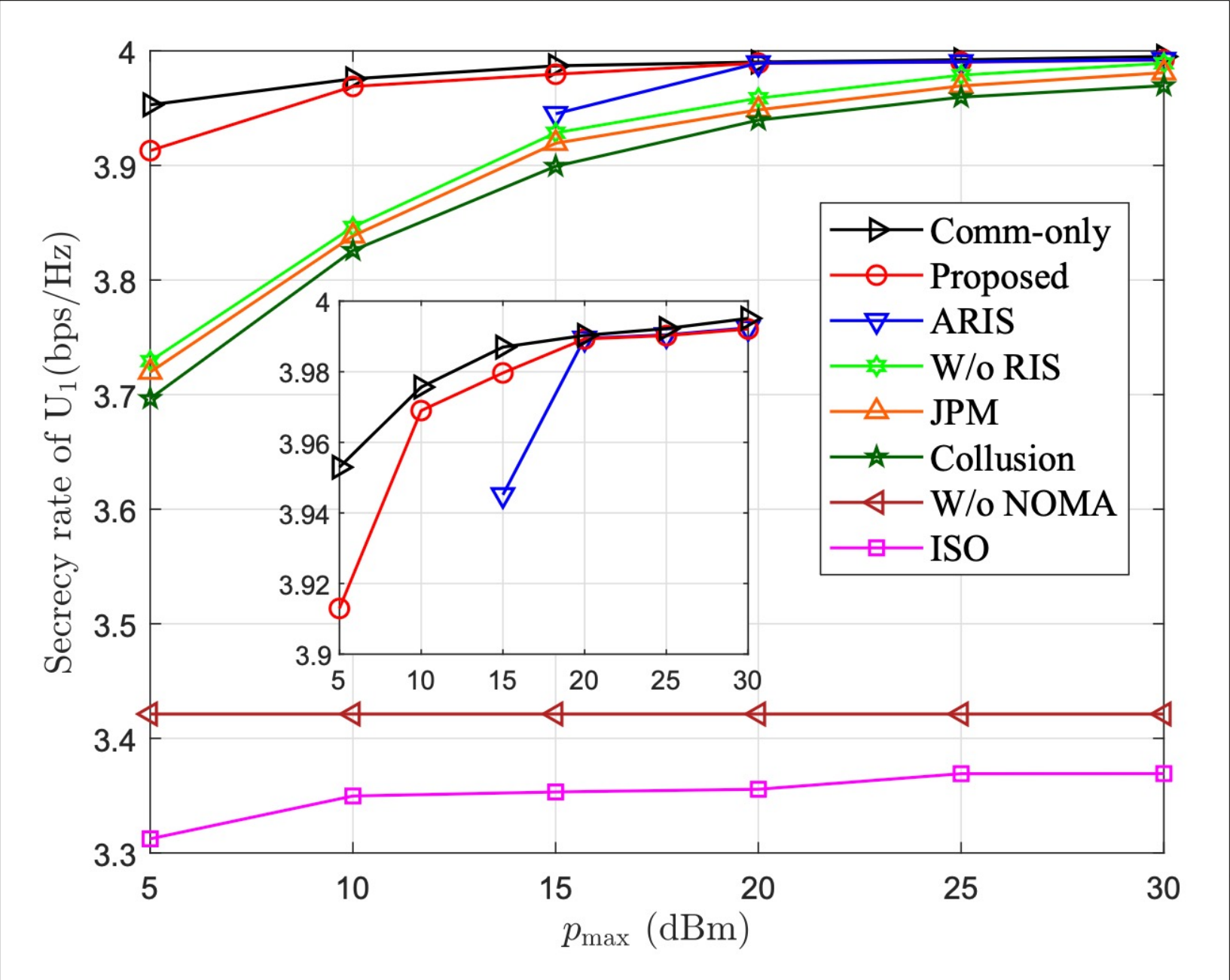


系統架構

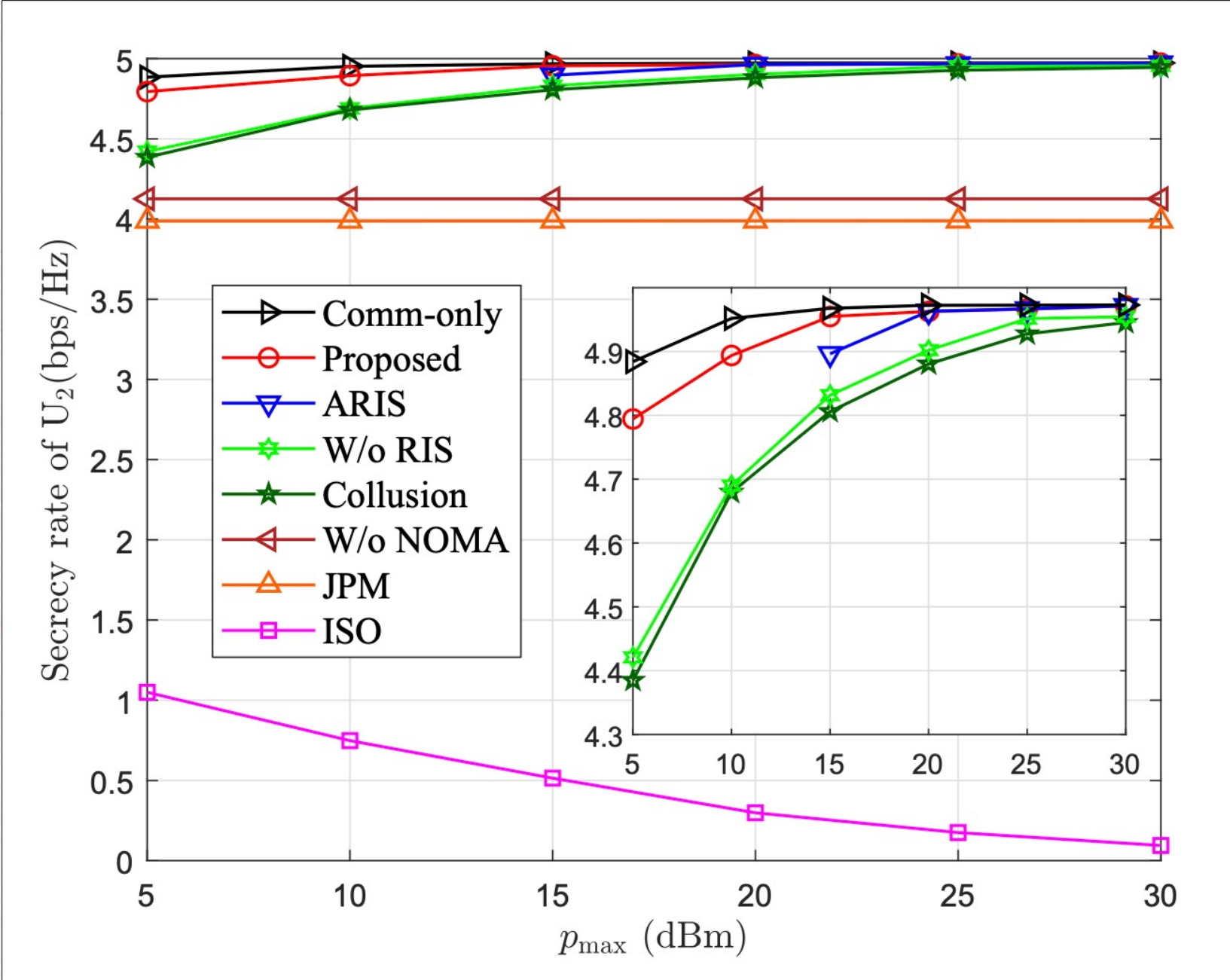


SDR + Penalty AO 演算法



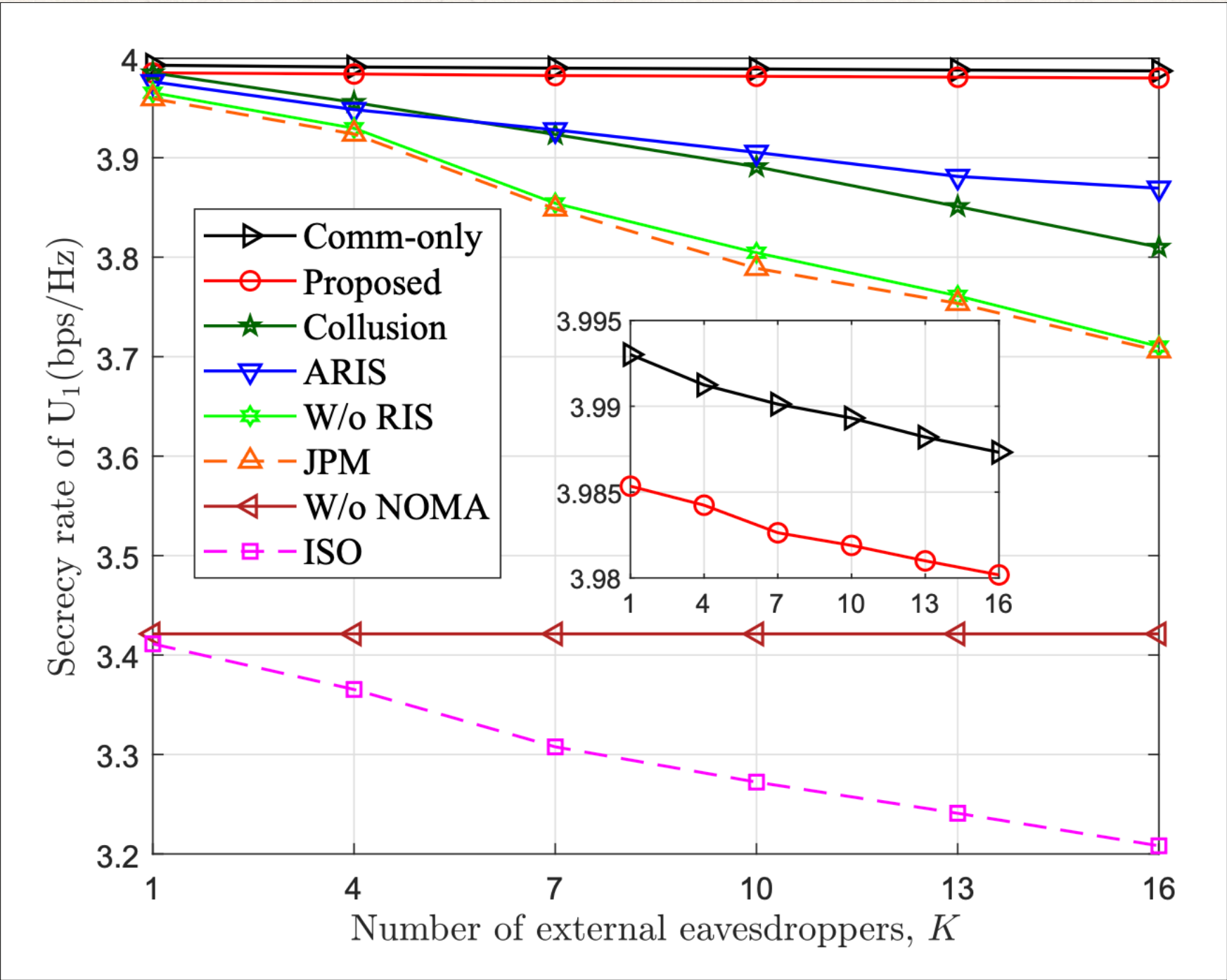


使用者 U1



使用者 U2





在外部竊聽者數量增加時的穩健性



# 總結

- ✦ 本文提出一個 RIS-assisted NOMA-ISAC 架構，在同時存在內部與外部竊聽者的情境下，透過最小化通訊功率來有效提升整體安全性。
  - ✦ 藉由通道選擇策略與 SDR + Penalty AO 演算法，所提方法能在不需外部竊聽者 CSI 的況下穩定收斂並取得近乎無損的通訊效能。
  - ✦ 模擬結果顯示，本方法在多使用者與多竊聽者場景中皆具良好穩健性，證實 RIS 與 ISAC 在安全通訊上的實質互補性。
-



# Thank you