MINISTRY OF EDUCATION AND TRAINING

HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY AND ENGINEERING

VO TA TY

DESIGN OF WIRELESS NETWORKS EMPLOYING INTELLIGENT REFLECTING SURFACES AND ARTIFICIAL JAMMING FOR ENHANCED SECURITY PERFORMANCE

Major: Electronic Engineering

Major code: 9520203

SUMMARY OF PH.D. THESIS

HO CHI MINH CITY – 2026

This thesis was completed at

HCMC University of Technology and Engineering

Supervisor 1: Assoc. Prof. Dr. Tran Trung Duy
Supervisor 2: Assoc. Prof. Dr. Pham Ngoc Son

The thesis was presented at the primary committee of at Faculty of Electrical and Electronics Engineering, HCMC University of Technology and Engineering, on , 2026.

INTRODUCTION

Research motivation

In recent years, the rapid development of wireless communication systems has played a crucial role in driving socio-economic growth and meeting the ever-increasing demand for connectivity in the digital era. Mobile communication systems have continuously evolved through multiple generations to satisfy stringent requirements in terms of capacity, data rate, low latency, and massive connectivity. In particular, with the deployment of fifth-generation (5G) mobile networks and the ongoing evolution toward sixth-generation (6G) systems, wireless communications are shifting toward intelligent transmission environments capable of adaptive operation and performance optimization. However, the explosive growth of wireless devices, along with emerging applications such as the Internet of Things (IoT), virtual reality/augmented reality, and wireless sensor networks, has introduced significant challenges for modern wireless systems. These challenges include efficient spectrum utilization, reliable communication links, improved energy efficiency, and enhanced security in increasingly complex communication environments. Consequently, a wide range of advanced technologies has been investigated to improve overall system performance. Among these, physical layer security (PLS) has emerged as a promising approach for ensuring information security in wireless communications. Unlike conventional cryptographic techniques, PLS exploits the inherent randomness of wireless channels to guarantee that the legitimate channel is of higher quality than the eavesdropping channel, thereby enabling secure communication without relying on complex encryption algorithms. In addition, intelligent reflecting surfaces (IRS) have recently been recognized as a key enabling technology for next-generation wireless systems. By intelligently controlling the wireless propagation environment through phase and amplitude adjustments of reflecting elements, IRS can significantly enhance channel quality and overall system performance. Nevertheless, due to the broadcast nature of wireless channels, transmitted signals remain vulnerable to interception by eavesdroppers. In this context, artificial jamming (AJ) has been proposed as an effective technique to degrade the channel quality at the eavesdropper while preserving the performance of legitimate users. Therefore, the integration of IRS and AJ offers a promising solution to simultaneously improve transmission quality and enhance communication security. Motivated by these considerations,

the research topic entitled **"Design of wireless networks employing intelligent reflecting surfaces and artificial jamming for enhanced security performance"** is of significant urgency, high scientific relevance, and strong alignment with current technological trends. The outcomes of this study are expected to contribute to both theoretical foundations and practical solutions for securing next-generation wireless communication systems.

Contributions of the dissertation

First, a wireless-powered communication network assisted by IRS and AJ over Rayleigh fading channels is proposed. Closed-form analytical expressions for outage probability (OP), intercept probability (IP), average secrecy capacity (ASC), and secrecy outage probability (SOP) are derived and validated via Monte Carlo simulations for both scenarios with and without AJ. The results demonstrate that the proposed system achieves superior secrecy performance compared to the configuration without AJ. Furthermore, the impact of key system parameters on secrecy performance is comprehensively investigated, providing valuable design insights for enhancing security in next-generation wireless networks.

Second, an IRS-AJ-assisted wireless communication model over Nakagami- m fading channels is developed, where the impact of imperfect AJ cancellation is considered to better reflect practical conditions. Analytical expressions for ASC and secure energy efficiency (SEE) are established for both cases with and without AJ, demonstrating simultaneous improvements in secrecy performance and energy efficiency achieved by the proposed model. In addition, the golden section search (GSS) algorithm is employed to determine the optimal jamming power. The effects of system parameters on ASC and SEE are also thoroughly examined, revealing the trade-off between secrecy performance and energy efficiency, and confirming the superiority of the proposed scheme over benchmark models.

Third, a multi-user wireless network employing non-orthogonal multiple access (NOMA) combined with IRS and AJ is proposed over Rayleigh fading channels. Both perfect successive interference cancellation (pSIC) and imperfect SIC (ipSIC) are considered, along with the impact of imperfect AJ cancellation. Closed-form expressions for ASC, SOP, and SEE are derived and verified through Monte Carlo simulations for scenarios with and without AJ. The results indicate that the proposed system significantly outperforms benchmark schemes such as IRS-NOMA -Non Jammer, Relay-Jammer-NOMA,

and IRS-Jammer-OMA. Moreover, the influence of system parameters on secrecy performance is comprehensively analyzed, leading to important design guidelines and confirming the practical feasibility of the proposed model for next-generation multi-user wireless networks.

Chapter 1: Overview of the research problem

In recent years, PLS has been widely recognized as an effective solution for enhancing the security of 5G/6G wireless communication systems. In parallel, IRS enable the manipulation of the wireless propagation environment to strengthen the legitimate signal while attenuating the signal at the eavesdropper. Meanwhile, AJ serves as an efficient mechanism to degrade the interception capability of unauthorized receivers. However, most existing studies primarily investigate IRS or AJ in isolation, whereas research that jointly exploits both techniques remains relatively limited in both international and domestic literature. Therefore, the integration of PLS with IRS and AJ is essential to fully leverage their combined potential and to further enhance secrecy performance in next-generation wireless networks.

Chapter 2: Theoretical background

Chapter 2 presents the fundamental concepts of PLS and key performance metrics, including the OP-IP trade-off, ASC, and SOP. In addition, this chapter provides an overview of IRS, AJ, as well as the basic theoretical foundations of radio frequency energy harvesting (RF-EH) and NOMA.

Chapter 3: Secrecy performance analysis of wireless-powered communication networks using IRS and AJ

3.1. Introduction

The content of this chapter has been published in J1

Vo Ta Ty, Pham Ngoc Son, Tran Trung Duy, "Secrecy performance of RIS-assisted wireless-powered systems with artificial-jamming generation," *Physical Communication* (SCIE, Q2), vol. 69, 102592, Jan. 2025.

3.2. System model

The wireless-powered communication network integrated with IRS and AJ is illustrated in Fig. 3.1. In this model, the source node (S) is powered via energy harvesting from the base station and transmits information to the destination (D) through an IRS consisting of L passive reflecting elements. Since the eavesdropper (E) can also intercept the reflected signals from the IRS, a jammer node (J) is deployed to degrade the signal quality at E. All nodes are equipped with a single antenna, and the wireless channels are modeled as Rayleigh fading.

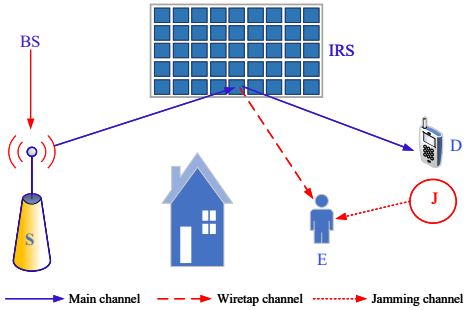

Fig. 3.1: System model.

Based on the system model, the received signal expressions at D and E are derived. Subsequently, the corresponding signal-to-noise ratio (SNR) expressions are obtained, which serve as the foundation for analyzing the secrecy performance metrics of the system.

3.3. Secrecy performance analysis

3.3.1. Outage probability and intercept probability

The closed-form expressions for OP and IP of the proposed model and the non-jammer scheme are respectively derived as follows.

$$\mathrm{OP} = 1 - \sum_{n=1}^{N} v_n \Gamma\left(\theta, \Omega_{\mathrm{D}} \sqrt{\gamma_{\mathrm{th}}}\right). \tag{3.1}$$

$$\mathrm{IP} = \sum_{n=1}^{N} \varepsilon_n \Gamma\left(\theta, \Omega_{\mathrm{E}} \sqrt{\gamma_{\mathrm{th}}}\right). \tag{3.2}$$

$$\mathrm{OP}^{\mathrm{NJ}} = 1 - \sum_{n=1}^{N} v_n \Gamma\left(\theta, \Omega_{\mathrm{D}}^{\mathrm{NJ}} \sqrt{\gamma_{\mathrm{th}}}\right), \tag{3.3}$$

$$\mathrm{IP}^{\mathrm{NJ}} = \sum_{n=1}^{N} v_n \Gamma\left(\theta, \Omega_{\mathrm{E}}^{\mathrm{NJ}} \sqrt{\gamma_{\mathrm{th}}}\right). \tag{3.4}$$

3.3.2. Average secrecy capacity

The ASC values of the proposed model with and without AJ are respectively expressed as follows

$$\mathrm{ASC} = \frac{(1-\alpha)}{\ln 2}\frac{\left(2^{\theta}-1\right)}{\sqrt{\pi}}$$
$$\left[\sum_{n=1}^{N} v_n G_{3,5}^{5,1}\left(\frac{\Omega_{\mathrm{D}}^2}{4}\middle|_{\frac{\theta}{2},\frac{\theta+1}{2},0,\frac{1}{2},0}^{0,\frac{1}{2},1}\right) - \sum_{n=1}^{N} \varepsilon_n G_{3,5}^{5,1}\left(\frac{\Omega_{\mathrm{E}}^2}{4}\middle|_{\frac{\theta}{2},\frac{\theta+1}{2},0,\frac{1}{2},0}^{0,\frac{1}{2},1}\right)\right]. \quad (3.5)$$

$$\mathrm{ASC}^{\mathrm{NJ}} = \frac{(1-\alpha)}{\ln 2}\frac{\left(2^{\theta}-1\right)}{\sqrt{\pi}}\sum_{n=1}^{N} v_n$$
$$\left[G_{3,5}^{5,1}\left(\frac{\left(\Omega_{\mathrm{D}}^{\mathrm{NJ}}\right)^2}{4}\middle|_{\frac{\theta}{2},\frac{\theta+1}{2},0,\frac{1}{2},0}^{0,\frac{1}{2},1}\right) - G_{3,5}^{5,1}\left(\frac{\left(\Omega_{\mathrm{E}}^{\mathrm{NJ}}\right)^2}{4}\middle|_{\frac{\theta}{2},\frac{\theta+1}{2},0,\frac{1}{2},0}^{0,\frac{1}{2},1}\right)\right]. \quad (3.6)$$

3.3.3. Secrecy outage probability

The SOP expressions for the proposed model, considering both the presence and absence of AJ, are derived as follows

$$\mathrm{SOP} = 1 - \sum_{m=1}^{M}\sum_{n=1}^{N}\sum_{q=1}^{Q} \frac{\pi^2 \xi_m \sqrt{1-y_n^2}\sqrt{1-y_q^2}}{4NQ\Gamma(\theta)}\left[\ln\left(\frac{2}{1+y_q}\right)\right]^{\theta-1}$$
$$\times\, \Gamma\left(\theta, \frac{1}{\phi_{\mathrm{D}}}\sqrt{\frac{\left[\ln\left(2/(1+y_q)\right)\right]^2}{\left(\Phi_{\mathrm{E}}\right)^2} + \frac{\kappa\lambda_{\mathrm{BS}}}{\ln\left(2/\left(1+y_n\right)\right)}}\right). \quad (3.7)$$

$$\mathrm{SOP}^{\mathrm{NJ}} = 1 - \sum_{n=1}^{N}\sum_{m=1}^{M} \frac{\pi^2\sqrt{1-y_n^2}\sqrt{1-y_m^2}}{4NM[\Gamma(\theta)]^2}\left[\ln\left(\frac{2}{1+y_n}\right)\right]^{\theta-1}$$
$$\times\, \Gamma\left(\theta, \frac{1}{\phi_{\mathrm{D}}}\sqrt{\rho_{\mathrm{th}}(\phi_{\mathrm{E}})^2\left[\ln\left(\frac{2}{1+y_n}\right)\right]^2 + \frac{\kappa\lambda_{\mathrm{BS}}}{\ln\left(2/\left(1+y_m\right)\right)}}\right). \quad (3.8)$$

3.4. Simulation results

In this section, the system performance is evaluated through numerical results combined with Monte Carlo simulations to validate the accuracy of the analytical derivations. To ensure a fair comparison, the transmit power of the non-jammer scheme is set as follows: $P_{\mathrm{S}}^{\mathrm{NJ}} = P_{\mathrm{BS}} + P_{\mathrm{J}} = (1+\mu)P_{\mathrm{BS}}$.

The results in Fig. 3.2 show that as Δ_{S} increases, OP improves while IP decreases, indicating a trade-off between reliability and security due to the

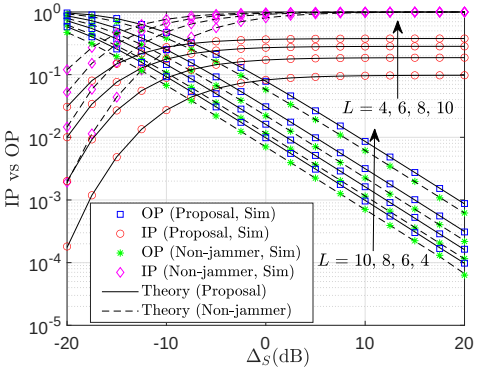

Fig. 3.2: IP and OP versus Δ_{S} with y_{E} = -0.5, μ = 0.4, and α = 0.5.

simultaneous increase in the capacities of both the main and eavesdropping channels. When L increases, OP continues to improve whereas IP degrades, highlighting a similar trade-off with respect to L. Compared with the non-jammer scheme, the proposed system exhibits a marginally higher OP but achieves a significant improvement in IP, particularly in the high Δ_{S} region. Furthermore, in the high-SNR regime, the IP of the proposed system converges to a ceiling value and becomes independent of Δ_{S}, allowing OP to be improved with negligible degradation in secrecy performance.

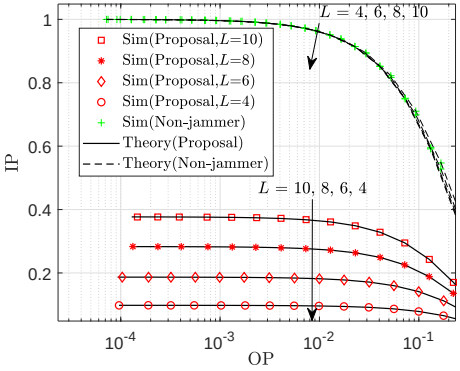

Fig. 3.3: OP–IP trade-off with $y_{\mathrm{E}} = -0.5$, $\mu = 0.4$, and $\alpha = 0.5$.

The results in Fig. 3.3 show that IP increases as OP decreases, clearly

reflecting the trade-off between reliability and security. In the proposed system, in the low-OP region, IP converges to a saturation value due to reaching its limit in the high-SNR regime. Compared with the non-jammer scheme, the proposed system achieves significantly lower IP at the same OP level, demonstrating the effectiveness of the proposed model. Moreover, as L increases, the OP-IP trade-off in the proposed system becomes more pronounced, whereas the non-jamming scheme exhibits only marginal variation.

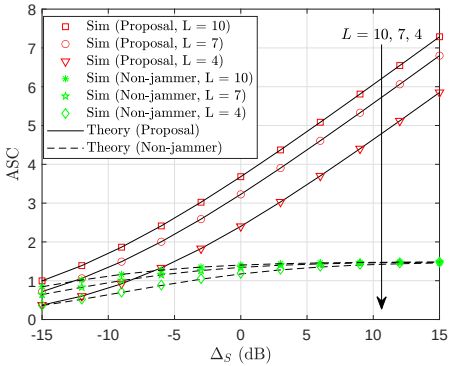

Fig. 3.4: ASC versus Δ_{S} with $y_{\mathrm{E}} = -0.5$, $\mu = 0.3$, and $\alpha = 0.25$.

The results in Fig. 3.4 show that the ASC of both systems increases as Δ_{S} and L increase. Notably, the proposed model consistently achieves higher ASC compared to the non-jammer scheme. In the high-SNR regime, the ASC of the proposed system continues to increase, whereas the non-jammer system reaches a saturation level since its capacity depends only on the IRS-assisted links and no longer depends on Δ_{S}.

The results in Fig. 3.5 show that SOP decreases as Δ_{S} and L increase. The proposed system achieves superior performance compared to the non-jammer scheme, particularly in the medium and high SNR regions. In the high-SNR regime, the SOP of the non-jammer system reaches a saturation level, whereas the proposed system continues to improve due to the effect of artificial jamming. Moreover, as L increases, the SOP of the proposed system is significantly reduced, while the non-jamming scheme exhibits only marginal improvement.

The results in Fig. 3.6 show that the SOP of the proposed system is consistently better than that of the non-jammer scheme. Moreover, there exists an

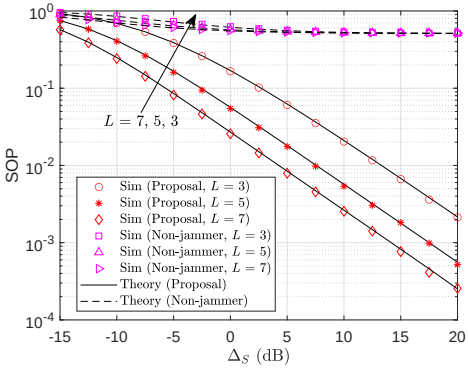

Fig. 3.5: SOP versus Δ_S with $y\mathrm{E} = -0.4$, $\mu = 0.3$, and $\alpha = 0.4$.

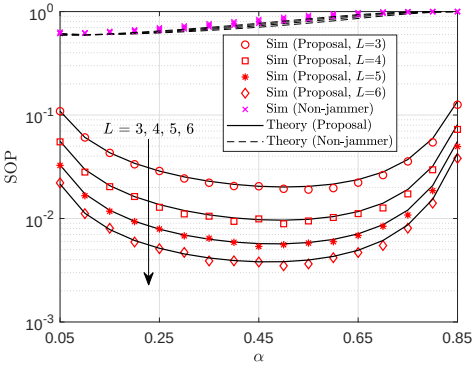

Fig. 3.6: Impact of α on SOP.

optimal value of α at which the system achieves the best secrecy performance.

3.5. Conclusion

Chapter 3 proposes a wireless communication model integrating RF-EH, IRS, and AJ to enhance secrecy performance. Closed-form expressions for OP, IP, ASC, and SOP are derived and validated via simulations, and comparisons are conducted with the non-jammer configuration. The results demonstrate that the proposed system significantly improves secrecy performance, whereas the benchmark scheme exhibits high IP and saturation in the high-SNR regime, thereby confirming the effectiveness of combining IRS,

AJ, and RF-EH. However, the current model does not consider imperfect AJ cancellation, and both D and E are assumed to receive signals only through the IRS. Therefore, Chapter 4 extends the analysis to a more general scenario by incorporating imperfect interference cancellation, the presence of direct links, and Nakagami-m fading channels to better reflect practical conditions.

Chapter 4: Secrecy capacity and energy efficiency analysis of IRS-AJ-assisted wireless networks based on MRC

4.1. Introduction

The content of this chapter has been published in J3.

Vo Ta Ty, Tran Trung Duy, Tran Manh Hoang, Pham Ngoc Son, "Enhancing average secrecy capacity and secure energy efficiency of SISO system using RIS with artificial jamming over Nakagami-m fading channels," *REV Journal on Electronics and Communications*, vol. 15, no. 3, Jul. 2025.

4.2. System model

The secure wireless communication system assisted by IRS and AJ is illustrated in Fig. 4.1.

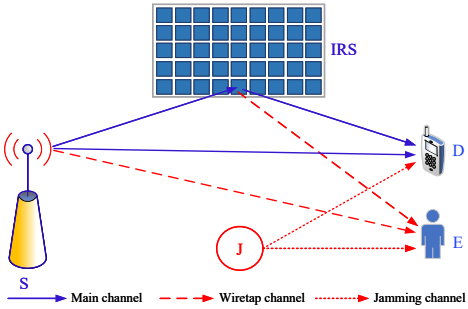

Fig. 4.1: System model

The considered model is an IRS-AJ-assisted wireless network, where the signals from S to D and E are transmitted through both direct links and IRS-reflected links. To enhance secrecy performance, a jammer is deployed to degrade the interception capability of E, while imperfect interference cancellation at D is taken into account to better reflect practical conditions. In addition, all nodes are equipped with a single antenna.

From the system model, the received signal expressions at D and E are derived. Subsequently, the corresponding SNR expressions are obtained, which serve as the basis for analyzing the secrecy performance and SEE of the system.

4.3. Secrecy performance analysis

4.3.1. Average secrecy capacity

The ASC values of the proposed model with and without AJ are respectively expressed as follows

$$\mathrm{ASC} = \frac{1}{\ln 2}\sum_{n=1}^{N}\sum_{m=1}^{M}\varepsilon_n\varepsilon_m\Gamma\Big(\omega_1, \phi_1\sqrt{\frac{\mathrm{A_D}}{P_\mathrm{S}}\frac{1-v_m}{1+v_m}}\Big) - \frac{1}{\ln 2}\sum_{w=1}^{W}\sum_{q=1}^{Q}\varepsilon_w\varepsilon_q\Gamma\Big(\omega_2, \phi_2\sqrt{\frac{\mathrm{A_E}}{P_\mathrm{S}}\frac{1-v_q}{1+v_q}}\Big). \tag{4.1}$$

$$\mathrm{ASC}^{\mathrm{NJ}} = \frac{1}{\ln 2}\frac{1}{\Gamma(\omega_1)}\varepsilon_{k_1}\Gamma\Big(\omega_1, \phi_1\sqrt{\frac{\delta_\mathrm{D}^2}{P_\mathrm{S}^{\mathrm{NJ}}}\frac{1-v_{k_1}}{1+v_{k_1}}}\Big) - \frac{1}{\ln 2}\frac{1}{\Gamma(\omega_2)}\varepsilon_{k_2}\Gamma\Big(\omega_2, \phi_2\sqrt{\frac{\delta_\mathrm{D}^2}{P_\mathrm{S}^{\mathrm{NJ}}}\frac{1-v_{k_2}}{1+v_{k_2}}}\Big). \tag{4.2}$$

4.3.2. Secure energy efficiency

The SEE expressions of the proposed model and the non-jammer scheme are expressed as follows

$$\eta = \frac{R_{\mathrm{sec}}}{P_i}, \tag{4.3}$$

where R_{sec} denotes the secrecy rate of the system. The secrecy rates of the proposed system and the non-jammer scheme are respectively determined from (4.1) and (4.2). $P_i \in \{P_{\mathrm{tol}}, P_{\mathrm{tol}}^{\mathrm{NJ}}\}$ represents the total power consumption.

4.4. Simulation Results

In this section, the system performance is evaluated based on numerical results combined with Monte Carlo simulations to verify the accuracy of the theoretical analysis. To ensure a fair comparison, the transmit power of the non-jammer scheme is set as follows: $P_\mathrm{S}^{\mathrm{NJ}} = P_\mathrm{S} + P_\mathrm{J} = (1+\mu)P_\mathrm{S}$.

The results in Fig. 4.2 show that ASC initially increases with P_J, reaches a maximum at an optimal value, and then decreases due to the impact of AJ on both E and D. In addition, there exists an optimal value of P_J that maximizes ASC, which can be efficiently determined using the GSS algorithm, as presented in Table 1. These results provide important insights for system design in balancing secrecy performance and SEE.

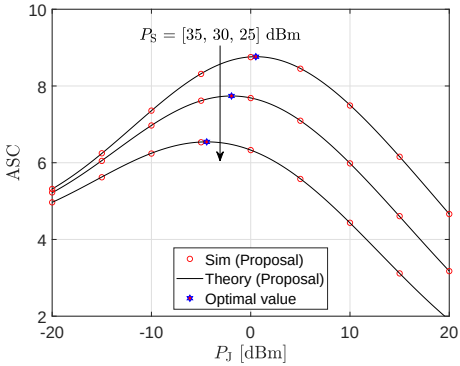

Fig. 4.2: ASC versus P_J with P_S = 25, 30, 35 dBm, f_c = 3 GHz, and L = 40.

Table 1. Optimization algorithm for determining P_J^*

Input: Set $P_{J_{min}}$ = -20 dBm, $P_{J_{max}}$ = 20 dBm, golden search coefficient $\omega = \frac{\sqrt{5}-1}{2}$, and stopping threshold $\delta = 10^{-3}$.
Output: Optimal value P_J^* that maximizes ASC.
Initialization:
1. Construct the points $\epsilon_1 = P_{J_{min}} + (P_{J_{max}} - P_{J_{min}})\omega$ and
   $\epsilon_2 = P_{J_{max}} - (P_{J_{max}} - P_{J_{min}})\omega$.
2. **While** $P_{J_{max}} - P_{J_{min}} \geq \delta$ **do**
   Evaluate: ASC(ϵ_1).
   Evaluate: ASC(ϵ_2).
   If ASC(ϵ_2) > ASC(ϵ_1) **then**
      Update: $P_{J_{min}} \leftarrow \epsilon_1$.
   Else
      Update: $P_{J_{max}} \leftarrow \epsilon_2$.
   End if.
3. **End while**.
4. Return $P_J^* = \frac{P_{J_{max}} + P_{J_{min}}}{2}$.
End.

The results in Fig. 4.3 show that ASC decreases as the carrier frequency f_c increases. In addition, the proposed system consistently achieves significantly higher ASC than the non-AJ scheme across the entire frequency range, confirming the effectiveness of AJ in enhancing secrecy performance.

The results in Fig. 4.4 show that the effectiveness of AJ cancellation

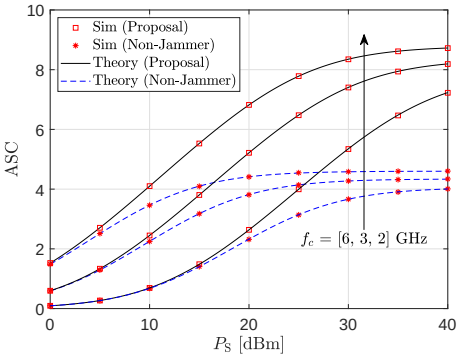

Fig. 4.3: Impact of f_c on ASC.

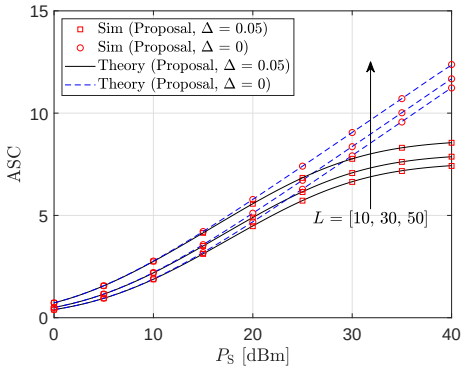

Fig. 4.4: Impact of Δ on ASC.

has a significant impact on ASC. When P_S is low, the difference between perfect and imperfect interference cancellation is negligible; however, in the high transmit power regime, perfect cancellation yields a noticeably higher ASC. This is because P_J increases with P_S, which degrades the performance at the legitimate user under imperfect interference cancellation. These results highlight the critical role of interference cancellation techniques in enhancing the secrecy performance of the system.

The results in Fig. 4.5 show that the SEE of both systems is nearly identical at low P_S; however, the proposed system significantly outperforms

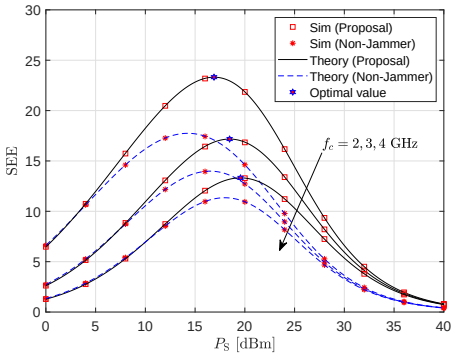

Fig. 4.5: SEE versus P_S with $f_c = 2$, 3, 4 GHz, and $L = 30$.

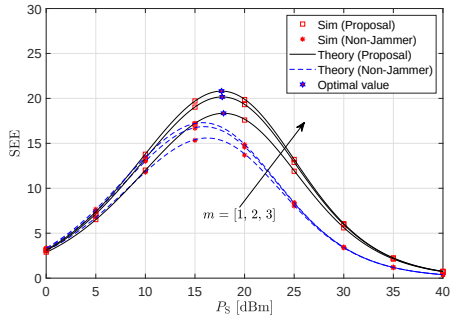

Fig. 4.6: Impact of the parameter m on SEE.

the non-AJ scheme as P_S increases. Moreover, for each f_c, there exists an optimal value of P_S that maximizes SEE. In addition, SEE decreases as f_c increases, which is consistent with the observations in Fig. 4.3.

The results in Fig. 4.6 show that m has a significant impact on SEE, and for each value of m, there exists an optimal P_S that maximizes SEE. Moreover, the proposed system consistently achieves higher SEE than the non-jammer scheme.

Conclusion

Chapter 4 proposes an IRS-AJ-assisted model to enhance secrecy performance in wireless networks under the presence of an eavesdropper. Closed-form expressions for ASC and SEE are derived and validated via simulations,

demonstrating that the proposed system achieves superior performance compared to the non-jamming configuration. However, Chapter 4 only considers a single-user scenario. Therefore, Chapter 5 extends the analysis to a multi-user system employing NOMA combined with IRS and AJ, while also considering ipSIC and imperfect AJ cancellation at legitimate users to provide a more comprehensive evaluation of secrecy performance.

Chapter 5: Secrecy analysis of multi-user wireless networks using NOMA combined with IRS and AJ

5.1. Introduction

The content of this chapter has been published in J2.

Vo Ta Ty, Tran Trung Duy, Pham Ngoc Son, "Enhancing the secrecy performance and secure energy efficiency of NOMA systems using RIS with artificial jamming," *International Journal of Communication Systems* (SCIE, Q2), vol. 39, no. 7, p.e70474, Mar. 2026.

5.2. System model

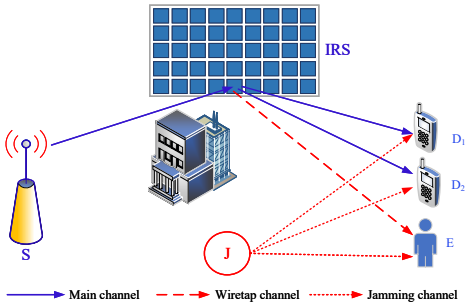

Fig.5.1: System model.

The considered IRS-Jammer-NOMA system consists of S, J, an IRS with L reflecting elements, two users D_1, D_2, and an eavesdropper E. Imperfect interference cancellation and ipSIC are also taken into account. In addition, all nodes are equipped with a single antenna.

Based on the system model, the received signal expressions at D_1, D_2, and E are derived. Subsequently, the corresponding SINR expressions are obtained, which serve as the basis for analyzing the secrecy performance of the system.

5.3. Secrecy performance analysis

5.3.1. Average secrecy capacity

The ASC values of the proposed model with and without AJ are respectively expressed as follows

$$\mathrm{ASC}^{x_1} = \frac{1}{\ln 2}\sum_{n=1}^{N}\sum_{u_1=1}^{U_1}\xi_n\xi_{u_1}\Gamma\Big(\theta, \frac{\omega_{\mathrm{D}_1}}{\sqrt{\alpha_2 P_{\mathrm{S}}}}\sqrt{\frac{1+v_{u_1}}{1-v_{u_1}}}\Big) - \frac{1}{\ln 2}\sum_{q=1}^{Q}\sum_{u_2=1}^{U_2}\xi_q\xi_{u_2}\Gamma\Big(\theta, \frac{\omega_{\mathrm{E}}}{\sqrt{\alpha_1 P_{\mathrm{S}}}}\sqrt{\frac{1-v_{u_2}}{1+v_{u_2}}}\Big). \tag{5.1}$$

$$\mathrm{ASC}^{x_2}_{\mathrm{ipSIC}} = \frac{1}{\ln 2}\sum_{m=1}^{M}\sum_{u_{31}=1}^{U_{31}}\xi_m\xi_{u_{31}}\Gamma(\theta, \omega_{\mathrm{D}_2^1}\sqrt{\frac{\varphi_{v_{u_{31}}}}{P_{\mathrm{S}}(\alpha_2-\varphi_{u_{31}}\alpha_1\rho)}}) + \frac{1}{\ln 2}\sum_{k=1}^{K}\sum_{u_{41}=1}^{U_{41}}\xi_k\xi_{u_{41}}\Gamma\Big(\theta, \omega_{\mathrm{D}_2^2}\sqrt{\frac{\varphi_{v_{u_{41}}}}{P_{\mathrm{S}}(\alpha_1-\varphi_{v_{u_{41}}}\alpha_2)}}\Big) - \frac{1}{\ln 2}\sum_{q=1}^{Q}\sum_{u_2=1}^{U_2}\xi_q\xi_{u_2}\Gamma\Big(\theta, \frac{\omega_{\mathrm{E}}}{\sqrt{\alpha_2 P_{\mathrm{S}}}}\sqrt{\frac{1-v_{u_2}}{1+v_{u_2}}}\Big). \tag{5.2}$$

$$\mathrm{ASC}^{\mathrm{NJ}}_{x_1} = \frac{1}{\ln 2}\sum_{w_1=1}^{W_1}\xi_{w_1}\Gamma\Big(\theta, \frac{\delta_{\mathrm{D}_1}}{\phi_{\mathrm{D}_1}\sqrt{\alpha_2 P_{\mathrm{S}}^{\mathrm{NJ}}}}\sqrt{\frac{1+v_{w_1}}{1-v_{w_1}}}\Big) - \frac{1}{\ln 2}\sum_{w_2=1}^{W_2}\xi_{w_2}\Gamma\Big(\theta, \frac{\delta_{\mathrm{E}}}{\phi_{\mathrm{E}}\sqrt{\alpha_1 P_{\mathrm{S}}^{\mathrm{NJ}}}}\sqrt{\frac{1-v_{w_2}}{1+v_{w_2}}}\Big). \tag{5.3}$$

$$\mathrm{ASC}^{\mathrm{NJ-ipSIC}}_{x_2} = \frac{1}{\ln 2}\sum_{w_{31}=1}^{W_{31}}\xi_{w_{31}}\Gamma\Big(\theta, \frac{\delta_{\mathrm{D}2}}{\phi_{\mathrm{D}_2}}\sqrt{\frac{\varphi_{v_{w_{31}}}}{P_{\mathrm{S}}^{\mathrm{NJ}}(\alpha_2-\alpha_1\rho\varphi_{v_{w_{31}}})}}\Big) + \frac{1}{\ln 2}\sum_{w_{41}=1}^{W_{41}}\xi_{w_{41}}\Gamma\Big(\theta, \frac{\delta_{\mathrm{D}2}}{\phi_{\mathrm{D}_2}}\sqrt{\frac{\varphi_{v_{w_{41}}}}{P_{\mathrm{S}}^{\mathrm{NJ}}(\alpha_1-\varphi_{v_{w_{41}}}\alpha_2)}}\Big) - \frac{1}{\ln 2}\sum_{w_2=1}^{W_2}\xi_{w_2}\Gamma\Big(\theta, \frac{\delta_{\mathrm{E}}}{\phi_{\mathrm{E}}\sqrt{\alpha_2 P_{\mathrm{S}}^{\mathrm{NJ}}}}\sqrt{\frac{1-v_{w_2}}{1+v_{w_2}}}\Big). \tag{5.4}$$

5.3.2. Secrecy Outage Probability

The SOP expressions for the proposed model, considering both the presence and absence of AJ, are derived as follows

$$\mathrm{SOP}^{x_1} = 1 - \Bigg[\sum_{n=1}^{N} \sum_{q=1}^{Q} \sum_{b_1=1}^{B_1} \xi_n \, \xi_q \, \xi_{b_1} \frac{A_{\mathrm{E}_1}^{\theta}}{2} \mho_{b_1}^{\frac{\theta}{2}-1} \exp\big(- A_{\mathrm{E}_1} \sqrt{\mho_{b_1}} \big)$$
$$\times \; \Gamma\Bigg(\theta, \omega_{\mathrm{D}_1} \sqrt{\frac{2^{\mathcal{R}^{x_1}} \mho_{b_1} + 2^{\mathcal{R}^{x_1}} - 1}{P_{\mathrm{S}} \Big(\alpha_1 - \alpha_2 \big(2^{\mathcal{R}^{x_1}} \mho_{b_1} + 2^{\mathcal{R}^{x_1}} - 1 \big) \Big)}} \Bigg) \Bigg]. \tag{5.5}$$

$$\mathrm{SOP}_{\mathrm{ipSIC}}^{x_2} = 1 - \Bigg[\sum_{m=1}^{M} \sum_{q=1}^{Q} \sum_{b_{21}=1}^{B_{21}} \xi_m \, \xi_q \, \xi_{b_{21}} \frac{A_{\mathrm{E}_2}^{\theta}}{2} \mho_{b_{21}}^{\frac{\theta}{2}-1} \exp\big(- A_{\mathrm{E}_2} \sqrt{\mho_{b_{21}}} \big)$$
$$\times \; \Gamma\Bigg(\theta, \omega_{\mathrm{D}_2^1} \sqrt{\frac{2^{\mathcal{R}^{x_2}} \mho_{b_{21}} + 2^{\mathcal{R}^{x_2}} - 1}{P_{\mathrm{S}} \Big(\alpha_2 - \alpha_1 \rho \big(2^{\mathcal{R}^{x_2}} \mho_{b_{21}} + 2^{\mathcal{R}^{x_2}} - 1 \big) \Big)}} \Bigg)$$
$$+ \sum_{k=1}^{K} \sum_{q=1}^{Q} \sum_{b_{31}=1}^{B_{31}} \xi_k \, \xi_q \, \xi_{b_{31}} \frac{A_{\mathrm{E}_2}^{\theta}}{2} \mho_{b_{31}}^{\frac{\theta}{2}-1} \exp\big(- A_{\mathrm{E}_2} \sqrt{\mho_{b_{31}}} \big)$$
$$\times \; \Gamma\Bigg(\theta, \omega_{\mathrm{D}_2^2} \sqrt{\frac{2^{\mathcal{R}^{x_2}} \mho_{b_{31}} + 2^{\mathcal{R}^{x_2}} - 1}{P_{\mathrm{S}} \Big(\alpha_1 - \alpha_2 \big(2^{\mathcal{R}^{x_2}} \mho_{b_{31}} + 2^{\mathcal{R}^{x_2}} - 1 \big) \Big)}} \Bigg) \Bigg]. \tag{5.6}$$

$$\mathrm{SOP}_{x_1}^{\mathrm{NJ}} = 1 - \Bigg[\sum_{b_4=1}^{B_4} \xi_{b_4} \frac{(A_{\mathrm{E}_1}^{\mathrm{NJ}})^{\theta}}{2} \mho_{b_4}^{\frac{\theta}{2}-1} \exp\big(- A_{\mathrm{E}_1}^{\mathrm{NJ}} \sqrt{\mho_{b_4}} \big)$$
$$\times \Gamma\Bigg(\theta, \frac{1}{\phi_{\mathrm{D}_1}} \sqrt{\frac{\big(2^{\mathcal{R}^{x_1}} \mho_{b_4} + 2^{\mathcal{R}^{x_1}} - 1 \big) \delta_{\mathrm{D}_1}^2}{P_{\mathrm{S}} \big(\alpha_1 - \alpha_2 \big(2^{\mathcal{R}^{x_1}} \mho_{b_4} + 2^{\mathcal{R}^{x_1}} - 1 \big) \big)}} \Bigg) \Bigg]. \tag{5.7}$$

$$\mathrm{SOP}_{x_2}^{\mathrm{NJ-ipSIC}} = 1 - \Bigg[\sum_{b_{51}=1}^{B_{51}} \xi_{b_{51}} \frac{\big(A_{\mathrm{E}_2}^{\mathrm{NJ}} \big)^{\theta}}{2} \mho_{b_{51}}^{\frac{\theta}{2}-1} \exp\big(- A_{\mathrm{E}_2}^{\mathrm{NJ}} \sqrt{\mho_{b_{51}}} \big)$$
$$\times \Gamma\Bigg(\theta, \frac{1}{\phi_{\mathrm{D}_2}} \sqrt{\frac{A_{b_{51}} \delta_{\mathrm{D}_2}^2}{P_{\mathrm{S}} \Big(\alpha_2 - \alpha_1 \rho A_{b_{51}} \Big)}} \Bigg)$$
$$+ \sum_{b_{61}=1}^{B_{61}} \xi_{b_{61}} \frac{\Big(A_{\mathrm{E}_2}^{\mathrm{NJ}} \Big)^{\theta}}{2} \mho_{b_{61}}^{\frac{\theta}{2}-1} \exp\big(- A_{\mathrm{E}_2}^{\mathrm{NJ}} \sqrt{\mho_{b_{61}}} \big)$$
$$\times \Gamma\Bigg(\theta, \frac{1}{\phi_{\mathrm{D}_2}} \sqrt{\frac{A_{b_{61}} \delta_{\mathrm{D}_2}^2}{P_{\mathrm{S}} \Big(\alpha_1 - \alpha_2 A_{b_{61}} \Big)}} \Bigg) \Bigg]. \tag{5.8}$$

5.3.3. Secure energy efficiency

The SEE expressions of the proposed model and the non-jammer scheme are expressed as follows

$$\eta = \frac{R_{\text{sec}}}{P_i}, \tag{5.9}$$

where the secrecy rates of the proposed system and the non-jammer scheme are respectively determined from (5.1)-(5.4).

5.4. Simulation results

In this section, the system performance is evaluated based on numerical analysis and further validated through Monte Carlo simulations to ensure consistency between theoretical analysis and simulation results. To ensure a fair comparison, the transmit power of the non-jammer scheme is set as: $P_{\text{S}}^{\text{NJ}} = P_{\text{S}} + P_{\text{J}} = (1+\mu)P_{\text{S}}$.

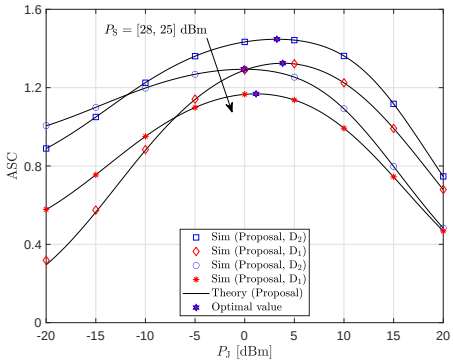

Fig. 5.2: ASC versus P_{J} with P_{S} = 25, 28 dBm, L = 30, and $\rho = 0$.

The results in Fig. 5.2 indicate that, for each P_{S}, there exists an optimal value of P_{J} that maximizes the ASC at D_1 and D_2. Specifically, the ASC initially increases with P_{J} due to the degradation of the eavesdropping channel. However, when P_{J} becomes excessively large, the ASC decreases as a result of imperfect AJ cancellation at the legitimate users. Since deriving a closed-form optimal solution is analytically intractable, the GSS algorithm is employed to determine the optimal P_{J}. The obtained results are consistent with the theoretical analysis and provide a solid basis for practical system design.

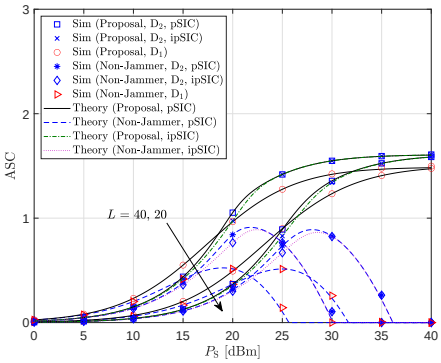

Fig. 5.3: ASC at D_1 and D_2 versus P_S for $L = 20, 40$.

The results in Fig. 5.3 show that the proposed system achieves superior ASC compared to the non-jammer scheme, while the ASC significantly increases as L grows. In the high transmit power regime, the ASC of the proposed system reaches a saturation level, whereas that of the non-jammer scheme degrades markedly. Under the ipSIC condition, the ASC is lower than that under pSIC; however, this performance gap becomes negligible in the high-power regime.

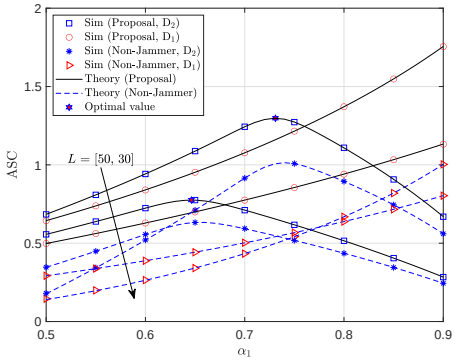

Fig. 5.4: Impact of α_1 on the ASC at D_1 and D_2.

The results in Fig. 5.4 show that as α_1 increases, the ASC at D_1 increases monotonically, whereas the ASC at D_2 first increases to a maximum value and then decreases, indicating the existence of an optimal power allo-

cation factor. The optimal α_1 can be efficiently determined using the GSS algorithm, thereby providing a practical basis for system design. Moreover, the proposed system consistently achieves higher ASC compared to the non-jamming configuration.

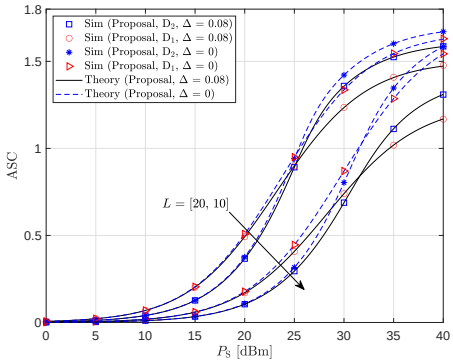

Fig. 5.5: Impact of Δ on the ASC at D_1 and D_2.

Fig. 5.5 illustrates that the impact of interference cancellation is negligible in the low transmit power regime but becomes pronounced as P_S increases. In the high-power region, ideal cancellation achieves significantly higher ASC compared to the imperfect case. This is because P_J scales with P_S, leading to performance degradation at the legitimate users in the presence of residual interference. This observation highlights the critical role of effective AJ cancellation in enhancing the system's secrecy performance.

The results in Fig. 5.6 show that, at low P_S, the Relay-Jammer-NOMA system achieves higher ASC. However, as P_S increases, the IRS-Jammer-NOMA system becomes superior since its ASC continues to improve, whereas the relay-based scheme saturates and eventually degrades. This observation confirms the effectiveness of IRS in enhancing secrecy performance, particularly in the moderate and high transmit power regimes.

The results in Fig. 5.7 show that, in the moderate transmit power regime, the IRS-Jammer-NOMA system achieves superior ASC compared to the OMA scheme. However, in the high-power regime, the ASC of NOMA gradually saturates, while that of OMA continues to increase due to the absence of inter-user interference. Nevertheless, the proposed system remains more suitable for practical deployments thanks to its higher spectral efficiency, flexible

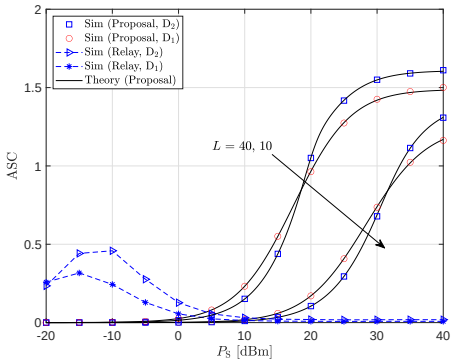

Fig. 5.6: ASC comparison of the proposed and relay-based schemes.

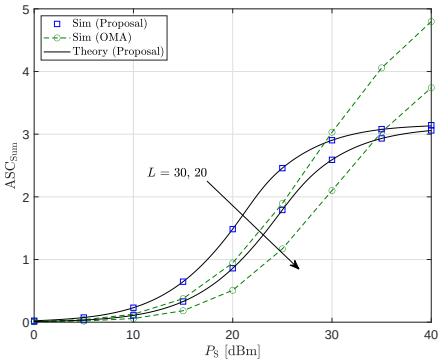

Fig. 5.7: ASC comparison between the proposed model and the OMA scheme.

power allocation capability, and its ability to effectively balance secrecy performance and SEE.

Fig. 5.8 demonstrates that the use of AJ significantly improves the SOP compared to the non-jammer configuration. In the high-SNR regime, the SOP of the system without AJ approaches 1, whereas the proposed system achieves a lower outage floor, indicating superior secrecy performance. In addition, increasing L enhances the SOP performance. The ipSIC case yields worse SOP than pSIC; however, this performance gap gradually diminishes in the high-power regime. At high SNR, the SOP converges to a constant value and

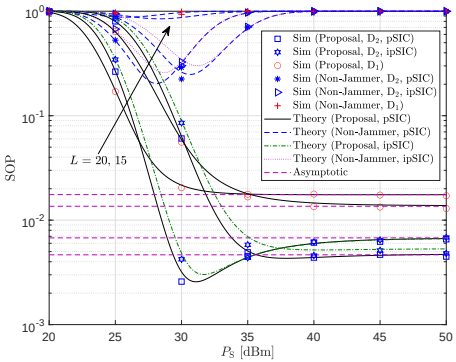

Fig. 5.8: SOP versus P_S for $L = 15, 20$ and $\mu = 0.002$.

becomes independent of P_S, indicating that the secrecy diversity order of the system is zero.

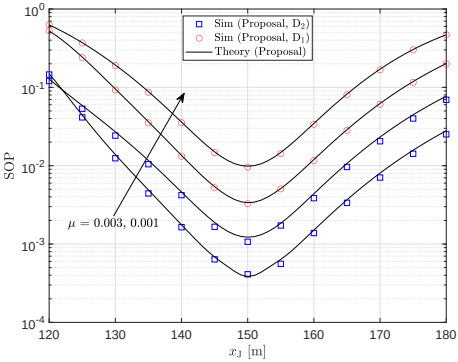

Fig. 5.9: Impact of x_J on the SOP.

Fig. 5.9 shows that J has a significant impact on the SOP. Specifically, the SOP achieves its optimal performance when J is located close to the eavesdropper, as this enhances the interference at E while minimizing its impact on the legitimate users. As J moves farther away from E, the secrecy performance degrades due to the reduced interference at the eavesdropper. In addition, increasing the factor μ improves the SOP by boosting the jamming power, thereby further degrading the eavesdropping capability.

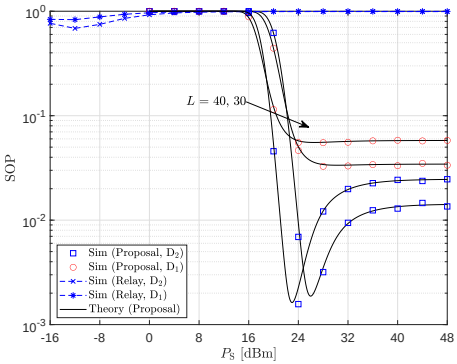

Fig. 5.10: SOP comparison of the proposed and relay-based schemes.

The results in Fig. 5.10 show that, in the low transmit power regime, the Relay-Jammer-NOMA system achieves better SOP performance. However, as P_S increases, the IRS-Jammer-NOMA system becomes significantly superior in terms of secrecy performance. In addition, increasing L considerably improves the SOP of the proposed system.

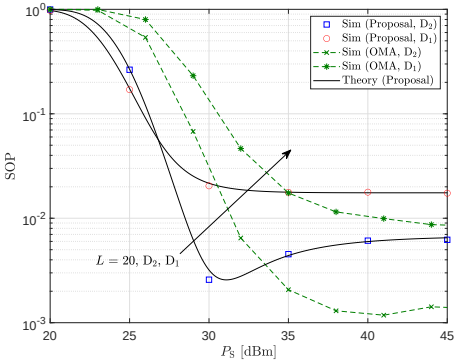

Fig. 5.11: SOP comparison between the proposed model and the OMA scheme.

Fig. 5.11 shows that, in the moderate P_S regime, the IRS-Jammer-NOMA system achieves superior SOP compared to the IRS-Jammer-OMA scheme. However, in the very high P_S region, OMA tends to exhibit slight secrecy performance improvement due to the elimination of inter-user interference.

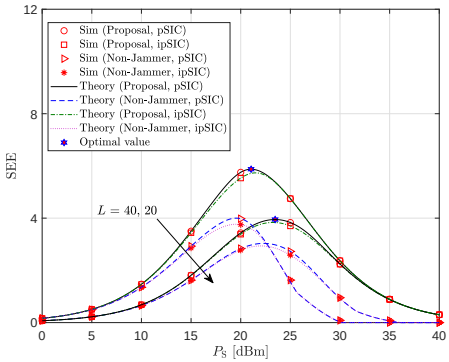

Fig. 5.12: SEE versus P_S for $L = 20, 40$.

The results in Fig. 5.12 show that, for each value of L, there exists an optimal P_S that maximizes the SEE, and this optimal value decreases as L increases. This indicates that the optimal SEE can be achieved with lower transmit power when a larger L is employed. In addition, the proposed system consistently attains higher SEE compared to the non-jamming configuration, while the ipSIC case yields lower performance than pSIC. Furthermore, the optimal P_S can be efficiently determined using the GSS algorithm.

Conclusion

Chapter 5 proposes and analyzes a wireless network model employing NOMA with the assistance of IRS and AJ to enhance security. Closed-form expressions for ASC, SOP, and SEE are derived and validated for both the proposed model and the non-jammer configuration, under pSIC and ipSIC conditions, as well as considering imperfect AJ cancellation. The results demonstrate that the proposed system achieves superior secrecy performance compared to the benchmark schemes. These findings confirm the potential of integrating IRS, AJ, and NOMA in secure and efficient wireless systems for next-generation networks.

Chapter 6: Conclusion and future research directions

6.1. Dissertation conclusions

1. This dissertation proposes and analyzes a wireless network assisted by IRS, integrated with RF-EH and AJ, to enhance secrecy performance over Rayleigh fading channels. Closed-form expressions for key performance metrics, including OP, IP, ASC, and SOP, are derived and validated through

Monte Carlo simulations. The results demonstrate that the proposed system significantly outperforms the non-jammer configuration, particularly in terms of OP-IP trade-off, ASC, and SOP. In addition, the secrecy performance can be substantially improved by increasing the number of IRS reflecting elements, enhancing the jamming power, and optimizing the EH process.

2. The secrecy performance and energy efficiency of an IRS-AJ-assisted wireless network over Nakagami-m fading channels are investigated. Closed-form expressions for ASC and SEE are derived and verified via Monte Carlo simulations. The results show that the integration of IRS and AJ provides considerable performance gains compared to non-jamming schemes. Furthermore, the impacts of key system parameters, such as the number of reflecting elements, interference cancellation capability at legitimate users, carrier frequency, inter-node distances, and jamming power are comprehensively analyzed, thereby revealing the system behavior. In addition, the GSS algorithm is employed to determine optimal system parameters for maximizing secrecy performance and SEE.

3. A wireless network model employing NOMA with the assistance of IRS and AJ over Rayleigh fading channels is developed and analyzed, considering both pSIC and ipSIC conditions. Closed-form expressions for ASC, SOP, and SEE are derived for both scenarios with and without AJ. The results indicate that the proposed system achieves superior secrecy performance compared to benchmark schemes such as IRS-Non Jammer-NOMA, Relay-Jammer-NOMA, and IRS-Jammer-OMA. Moreover, the effects of key system parameters, including the number of reflecting elements, jammer location, eavesdropper location, interference cancellation capability at legitimate users, source transmit power, and jamming power are thoroughly investigated, providing practical insights for system design. The GSS algorithm is also effectively applied to determine optimal parameters that maximize secrecy performance and SEE.

The findings of this dissertation confirm the significant potential of integrating IRS and AJ in developing secure, efficient, and sustainable wireless communication systems for next-generation networks.

6.2. Future research directions

Based on the achieved results, several promising research directions can be further explored as follows:

1. Extend the proposed models by considering imperfect CSI and phase errors at the IRS to better reflect practical deployment conditions and provide a more accurate evaluation of system performance.

2. Investigate more complex network scenarios, such as multiple users, multiple eavesdroppers, and multiple jammers, in order to assess system performance in more realistic environments.

3. Integrate IRS with advanced communication technologies such as mmWave/THz, RSMA, and Fountain codes to simultaneously enhance secrecy performance and energy efficiency. In addition, emerging IRS architectures, including active IRS (ARIS), hybrid active–passive IRS, and STAR-RIS, can be considered for further performance improvements.

4. Apply advanced machine learning techniques, particularly reinforcement learning and deep reinforcement learning, to address complex optimization problems in the system. These approaches enable the joint optimization of multiple parameters, such as power allocation, IRS configuration, and jamming control, while leveraging channel data to improve CSI accuracy and resource allocation efficiency.

LIST OF PUBLICATIONS

A. Publications included in the dissertation

[J1]. Vo Ta Ty, Pham Ngoc Son, Tran Trung Duy, "Secrecy performance of RIS-assisted wireless-powered systems with artificial-jamming generation," *Physical Communication*, vol.69, 2025, 102592, https://doi.org/10.1016/j.phycom.2024.102592 (SCIE - Q2).

[J2]. V. Ta Ty, T. Trung Duy, and P. Ngoc Son, "Enhancing the Secrecy Performance and Secure Energy Efficiency of NOMA Systems Using RIS with Artificial Jamming," *International Journal of Communication Systems*, vol. 39, no. 7, p. e70474, 2026 https://doi.org/10.1002/dac.70474 (SCIE - Q2).

[J3]. Vo Ta Ty, Tran Trung Duy, Tran Manh Hoang, Pham Ngoc Son, "Enhancing average secrecy capacity and secure energy efficiency of SISO system using RIS with artificial jamming over Nakagami-m fading channels," *REV Journal on Electronics and Communications*, Vol. 15, No. 3, Jul. 2025, http://dx.doi.org/10.21553/rev-jec.413.

B. Publications not included in the dissertation

[C1]. Vo Ta Ty, Tran Trung Duy, Lam-Thanh Tu, Tien-Tung Nguyen, D.Trinh, Tan Hanh, "Security-reliability tradeoff of multi-hop secure communication networks using Fountain codes and RIS-aided cooperative communication," in 2023 International Conference on Advanced Technologies For Communications (ATC), 2023, pp. 499-504, IEEE.

[C2]. Vo Ta Ty, Nguyen Van Hien, Tran Trung Duy, Lam-Thanh Tu, Pham Ngoc Son, "On performance evaluation of intelligent reflecting surface-aided NOMA systems using Fountain codes with presence of colluding eavesdroppers," in 2025 International Conference on Advanced Technologies For Communications (ATC), 2025, pp. 1-6, IEEE.

[C3]. Vo Ta Ty, Le Thi Ngoc Diep, Tran Van Vinh, Tran Trung Duy, Pham Ngoc Son, "Secrecy performance analysis of RIS-assisted RSMA systems with Artificial Jamming," the 8th International Conference on Green Technology and Sustainable Development (GTSD 2026). The abstract has been accepted, and the PhD candidate is currently finalizing the full manuscript for submission by April 30, 2026.

[J4]. Hieu T. Nguyen, Nguyen-Thi Hau, Nguyen Van Toan, Vo Ta Ty, and Tran Trung Duy, "Fountain Coding Based Two-Way Relaying Cognitive Radio Networks Employing Reconfigurable Intelligent Surface and Energy Harvesting", vol.6, no.1., 2024, *Telecom*, indexed in Web of Science (ESCI) and Scopus (Q2).

[J5]. Vo Ta Ty, Tran Trung Duy, Tran Manh Hoang, Pham Ngoc Son, "Physical-Layer Security Enhancement via RSMA-Enabled RIS with Artificial Jamming and RF Energy Harvesting," *Digital Signal Processing*, 2026, (SCIE - Q2), (The manuscript was submitted to the journal on January 26, 2026, and is currently under review).