Channel-Adaptive Privacy Enhancement for NOMA-Based Antagonistic Overlay Cognitive Networks

Moh Khalid Hasan, *Member, IEEE*, Shucheng Yu, *Fellow, IEEE*, and Min Song, *Fellow, IEEE*

***Abstract*—Overlay cognitive networks based on non-orthogonal multiple access (NOMA) can introduce substantial privacy concerns, especially in antagonistic systems where primary and secondary networks lack mutual trust. This paper highlights two critical privacy challenges and investigates a NOMA-assisted purely antagonistic overlay cognitive network. As part of our privacy design, we propose a *C*hannel-*A*daptive *D*ual-*P*hase *C*ooperative *J*amming (CADP-CJ) strategy, leveraging reverse successive interference cancellation and a dynamic top-down power allocation approach based on the available channel-state information. The ergodic secrecy rate (ESR) for both single-user and multi-user scenarios is derived in closed form by means of Taylor-McLaurin expansions and Gaussian-Chebyshev quadrature, while considering Nakagami-m fading across all channels. Furthermore, the closed-form expressions for the asymptotic ESR are presented to provide deeper insights. The accuracy of our analytical results is corroborated through Monte-Carlo simulations, which also confirm that our scheme ensures a positive ESR in both single and multi-user cases. We comprehensively analyze the impact of the fading properties of the channels involved and comment on optimal jamming power using the CADP-CJ strategy. Notably, our proposed system outperforms benchmark systems, particularly those based on orthogonal multiple access, with an 86% enhancement for primary users and 64% for secondary users.**

***Index Terms*—Overlay cognitive network, non-orthogonal multiple access (NOMA), antagonistic networks, physical layer security (PLS), ergodic secrecy rate (ESR).**

I. Introduction

The sixth generation (6G) wireless networks are set to support immense mobile data traffic, offering ultra-high data rates and robust security. Yet, considering the limitations and regulations of radio spectrum resources, efficiently accommodating the anticipated data traffic surge is crucial. Although 6G is expected to gravitate towards higher spectrum bands, the sub-6 GHz band, notable for its excellent propagation and penetration abilities, remains underutilized, with usage ranging from 15-85% [1]. In recent years, there has been significant research focused on optimizing the use of the spectrum, with cognitive radio networks (CRNs) emerging as a potential solution to address the issue of spectrum scarcity. CRNs enhance spectral efficiency by enabling secondary users to utilize idle licensed channels occupied by primary users. This technique, referred to as overlay cognitive network, enables secondary users to share the spectrum without compromising primary users' service quality.

Additionally, non-orthogonal multiple access (NOMA) has recently been recognized as a promising technology to further boost spectrum efficiency [2]–[6]. NOMA can be broadly categorized into power-domain and code-domain approaches. Power-domain NOMA differentiates users by allocating distinct power levels, while code-domain NOMA assigns unique codebooks to users, which allows multiple users to share the same time-frequency resources through distinct coding patterns [7]–[9]. This study focuses on power-domain NOMA. In an overlay cognitive network, secondary users often have limited spectrum access, but power-domain NOMA optimizes this by allowing multiple users to share the spectrum simultaneously [10], [11]. Incorporating NOMA into overlay cognitive frameworks promises a scalable, efficient communication system tailored to the growing demands of upcoming 6G wireless networks.

NOMA-based Overlay cognitive networks have potential in a wide range of applications, especially in unmanned aerial vehicle (UAV)-based systems owing to their rapid and adaptable deployment [12]. Notably, UAVs prove invaluable as relays when conventional communication infrastructures falter due to natural disasters [13], [14]. In overlay cognitive networks, UAVs can serve as secondary devices, relaying signals for primary users. This role is especially advantageous in NOMA-aided systems, where UAVs help to use spectrum resources more efficiently [15]. However, UAV-based cognitive networks face a significant vulnerability to security attacks due to their open nature. Moreover, NOMA-based data transmission introduces an additional privacy concern that has yet to be extensively researched in the literature.

Developing a secure cognitive NOMA network presents several challenges, particularly in terms of ensuring system-wide privacy. These challenges become particularly daunting in purely *antagonistic settings*. An antagonistic setting is characterized by a scenario where nodes from different networks are considered untrustworthy. In modern wireless systems, it is increasingly common for primary and secondary networks to operate under distinct admissibility control. In such an antagonistic environment, especially being pronounced in overlay systems, where a node must act as a relay, the secondary node may not be trusted but is still relied upon to relay the primary node's message to extend coverage, often using NOMA for spectrum efficiency. The security issues here are particularly critical in adversarial ecosystems, such as in battlefield networks or contested UAV environments, where hardware-

This work was supported in part by the National Science Foundation under Grants ECCS-1923739 and OAC-2417890.

M. K. Hasan is with the Department of Computer Science, James Madison University, Harrisonburg, VA 22807, USA. S. Yu is with the Graduate Computer Science and Engineering Department, Yeshiva University, New York, NY 10016, USA. M. Song is with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030, USA (e-mail: dwtn6r@jmu.edu; shucheng.yu@yu.edu; min.song@stevens.edu).

constrained but protocol-compliant nodes may eavesdrop or violate data privacy.

Security in NOMA-aided overlay cognitive networks has been addressed in the literature, however, the majority of them consider an underlay cognitive network [5], [16]. For NOMA-based overlay cognitive systems, two key security challenges can be outlined. The first challenge arises when the secondary node, operating on a decode-and-forward (DF) principle, relays the primary user's data. This scenario could potentially compromise the confidentiality of the primary user's data. A potential solution involves treating the secondary transmitter as an amplify-and-forward (AF) relay [17]–[19]. However, AF relaying has several limitations, such as noise amplification, which can adversely impact the SINR at the receiver [20]. Also, when the relay is proximate to the source, DF outperforms AF and compress-and-forward relaying [21]. However, the DF relaying in untrusted scenarios is seldom discussed in existing literature.

The second challenge arises within the NOMA-based transmission framework. Here, data intended for both networks is vulnerable due to the decoding process that involves Successive Interference Cancellation (SIC). Internal eavesdropping is addressed in the existing literature, however, this challenge is overlooked in most cases by typically identifying only the near or far user as a potential untrusted node [22], [23]. In [24], the authors treated one of the NOMA users as untrusted and introduced a unique phase shift to each user's transmitted signal to ensure security. However, the system's reliance on the channel state information (CSI) for phase shifting presents a vulnerability, especially if an unidentified eavesdropper gains access to another user's CSI, especially in collusion attack scenarios. Therefore, ensuring privacy in a completely untrusted NOMA network needs more research.

Additionally, the involvement of UAV also introduces unique challenges. In conventional networks communication security can be fortified using cryptographic methods anchored by shared secret keys. The constraints of computing power and battery life on UAVs, however, make frequent data encryption and decryption less attractive. Complex cryptographic key management and distribution [25], if available, will inevitably introduce additional operations which result in protracted networking deployment. Physical Layer Security (PLS) techniques, on the other hand, has shown promise in enhancing the security and privacy in wireless communications [26] for its lightweightness, minimum to none key management, and information-theoretical security. Popular PLS techniques such as friendly jamming are frequently adopted in wireless systems. However, their application in antagonistic NOMA networks presents new difficulties due to the unique decoding requirements in NOMA and the lack of mutual trust.

In this study, we address the unique privacy challenges arising from untrusted relays and the message superposition inherent in NOMA, as well as the significant decoding difficulties these present. To tackle these issues, we propose a novel PLS approach tailored for a UAV-assisted, NOMA-based overlay cognitive network, where the secondary transmitter acts as an untrusted DF relay for the primary transmitter.

To summarize, the key contributions of this work are as follows.

- To the best of our knowledge, this work is among the first that addresses the privacy issue in a purely antagonistic NOMA system in a cognitive networking setting. We investigate an overlay cognitive network in which the secondary transmitter acts as a DF relay, and all receiving nodes are considered untrusted with respect to the opposing network. A **C**hannel-**A**daptive **D**ual-**P**hase **C**ooperative **J**amming (CADP-CJ) strategy is proposed to ensure the privacy of the primary and secondary users' data. The CADP-CJ explicitly addresses two major threats: data compromise resulting from DF relaying through an untrusted secondary transmitter, and cross-network eavesdropping enabled by SIC at the primary or secondary receivers. To mitigate these risks, and assuming full CSI[1] is available at the secondary transmitter, our privacy framework integrates reverse SIC and a dynamic top-down power allocation strategy tailored for NOMA-based transmissions. Our approach ensures the confidentiality of both primary and secondary messages, even in the presence of honest-but-curious nodes employing DF and SIC techniques.
- We theoretically derive the ergodic secrecy rate (ESR) for both primary and secondary networks, considering both single-user and multi-user scenarios. Furthermore, asymptotic analyses are conducted to gain further insights into the ESR. The upper-bound ESRs and asymptotic ESRs are derived in closed form, applying Taylor-McLaurin expansions and Gaussian-Chebyshev quadrature in intractable cases. All the mathematical models are constructed by characterizing the probabilistic behavior of all channels undergoing Nakagami-m fading.
- To verify the effectiveness of the proposed solution against the identified threats, we conduct extensive Monte Carlo simulations. The results demonstrate that CADP-CJ consistently achieves positive ESR in both single and multiple-user scenarios. Additionally, we conduct a comprehensive study on the influence of fading properties on the ESR and provide insights on optimal jamming power allocation. It is also established that our scheme surpasses benchmark strategies, particularly outperforming the conventional Orthogonal Multiple Access (OMA)-based approach.

The structure of this paper is as follows: Section II discusses the relevant literature. Section III introduces the network architecture and threat model. Section IV discusses our proposed design and the performance analysis. The performance analysis based on a multi-user scenario is undertaken in Section V. In Section VI, we assess the effectiveness of our proposed system through simulations. The paper is concluded in Section VII.

[1] The assumption of complete CSI availability is standard in the PLS literature and enables adaptive jamming and power control, which are key components of the CADP-CJ scheme. Although full CSI may not always be available in practice, this assumption establishes a useful performance upper bound and provides a foundation for future extensions to partial or statistical CSI settings.

II. Related works

Recently, UAV-aided overlay cognitive networks have attracted substantial research interest. However, UAV-based communications are susceptible to eavesdropping attacks owing to their open nature. To address this vulnerability, numerous studies have focused on enhancing security within these communication settings using PLS. For instance, Tang et al. explored the PLS of a UAV-based communication system incorporating NOMA with Cognitive Radio (CR) in [27]. Their research aimed to optimize both the UAV's trajectory and power allocation to maximize the secrecy rates for secondary receivers while minimizing interference to the primary receiving end. In another study, Hasan et al. [26] delved into the uplink secrecy of a UAV-aided NOMA-based spectrum-sharing network, especially regarding potential eavesdropping threats. They emphasized the impacts of interference temperature and residual interference on secrecy performance and demonstrated that their proposed method outperformed the benchmark in Nakagami-m fading conditions. In [28], the authors investigated the secrecy performance of a UAV-borne IRS-NOMA system enhanced with friendly jamming to counteract eavesdropping threats in IoT networks. The study derived analytical expressions for secrecy metrics and developed a deep neural network model that accurately predicts secrecy outage probability. In [29], Wang et. al. proposed an autonomous aerial vehicle-assisted cognitive radio system that employs cooperative jamming to enhance physical layer security and maximize the secure communication rate under spectrum and energy constraints.

Furthermore, in [30], the PLS of a UAV-aided full-duplex relay-based NOMA network was evaluated in the context of a ground internal eavesdropper. The research assessed the secrecy performance across various scenarios and showed that introducing artificial noise led to improved secrecy rates. Zheng et al. [16] provided insights into the secrecy performance of a UAV-aided NOMA system within an underlay spectrum sharing context. Their work investigated the secrecy outage probability, considering the links subjected to Nakagami-m fading. Recent studies have also proposed reconfigurable intelligent surface (RIS)-based approaches for PLS in emerging wireless networks. For example, [31] explores a self-powered RIS design for secrecy enhancement in satellite-terrestrial networks, while [32] investigates secure transmission for symbiotic radio using active RIS under imperfect CSI. However, a common theme among these studies is their focus on external eavesdroppers. Addressing privacy concerns when internal, legitimate network nodes act as eavesdroppers presents unique challenges. This involves not only identifying the eavesdropper but also maintaining the node's performance while simultaneously reducing its eavesdropping capabilities.

Security concerns stemming from internal untrusted nodes have been a topic of investigation in existing research. Cao et al. [22] introduced a joint beamforming and power allocation approach to bolster security, particularly in situations involving untrusted near users. Additionally, they suggested the use of artificial noise as a countermeasure against external eavesdroppers. Their findings illustrated that the proposed strategies effectively mitigate eavesdropping threats and maintain robust performance at high signal-to-noise ratios. Zhang et al. [23] advanced security measures for NOMA networks by focusing on challenges posed by stronger near-user eavesdroppers. Their approach involved refining power allocation, altering the NOMA decoding order, and integrating a cooperative jammer. In a different study, Abushattal et al. [24] proposed a secure NOMA strategy employing PLS. They utilized the inherent randomness of channel properties to impose distinct phase shifts on each user's symbol. Analytical and simulation outcomes confirmed the system's security efficiency without compromising the integrity of legitimate users. Lastly, Su et al. [33] assessed the effective secrecy throughput within a cooperative NOMA framework. Their research identified and addressed threats from internal eavesdroppers, suggesting a jamming technique to enhance security. In [34], Indraganti et. al. proposed a downlink overlay CR-NOMA system that integrates PLS and CRN to improve spectral efficiency and secrecy. The research derived closed-form expressions for key secrecy and performance metrics, introduced power allocation and diversity techniques, and validated the model through simulations demonstrating its effectiveness against untrusted users.

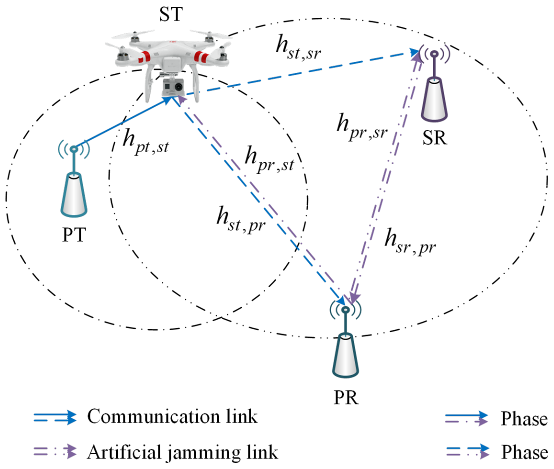

Fig. 1. System Model. Abbreviations used in the figure are as follows: PT - Primary Transmitter, PR - Primary Receiver, ST - Secondary Transmitter, and SR - Secondary Receiver.

Although aforementioned studies have explored UAV-aided CRNs using NOMA, the privacy threats originating from purely antagonistic networks have been hardly studied. The security challenges intensify when the secondary node serves as a DF relay, forwarding the primary transmitter's message. This paper addresses these research problems, delving into and resolving the security concerns with a thorough performance analysis. A comparison of our work with the related works is shown in Table I.

III. System Model

A. Network Model

In Fig. 1, we present an overlay cognitive network that comprises primary and secondary transmitter-receiver pairs.

TABLE I
COMPARISON OF CADP-CJ WITH RELATED WORKS

References	Cognitive Model	NOMA	Untrusted DF	Purely Antagonistic	Jamming Strategy	Power Allocation	Security Threat
[5]	Underlay	✓	✗	✗	✗	Dynamic	External eavesdropper
[6]	–	✓	✗	✗	✗	Fixed	External Eavesdropper
[16]	Underlay	✓	✗	✗	✗	Dynamic	External eavesdropper
[23]	–	✓	✗	✗	Single-Phase (by base station)	Dynamic	Internal near-end eavesdropper
[24]	–	✓	✗	✗	✗	Fixed	Internal eavesdropper
[34]	Overlay	✓	✗	✗	Single Phase (Not explicitly discussed)	Dynamic	Untrusted SR
[35]	–	✓	✗	✗	Single-Phase (by strong user)	Joint power sharing	External Eavesdropper
This work	Overlay	✓	✓	✓	Dual-phase, adaptive	Dynamic, CSI-driven	Inter-network mutual distrust

We assume no link exists between the Primary Transmitter (PT) and either the Primary Receiver (PR) or the Secondary Receiver (SR) due to shadowing and extreme path loss. The PT owns the spectrum. When the PT is inactive, it allows the secondary transmitter (ST) to use the spectrum. In exchange, the ST acts as a DF relay[2], which combines its data with that of the PT using NOMA, thereby extending its coverage to better reach the PR. This work assumes that the ST can perfectly detect the inactivity of the PT before initiating any transmission. In practical deployments, this is typically achieved using spectrum sensing schemes at the ST, such as advanced energy detection or deep learning-based techniques [36], [37]. However, for simplicity and analytical tractability, we assume ideal spectrum sensing, without miss-detections or false alarms.

We also assume that all nodes operate in half-duplex mode to prevent self-interference. We also posit that the channels undergo Nakagami-*m* fading. This fading model is particularly advantageous for UAV-assisted networks because of its ability to capture both line-of-sight (LoS) and non-LoS scenarios, common in UAV operations. In low-altitude scenarios, this model offers a more accurate representation of UAV channels [16]. We also assume that all channel gains follow a gamma distribution. The distance and channel coefficient between i and j are represented as $d_{i,j}$ and $h_{i,j}$, respectively, where $\forall i, j = \{pt, st, pr, sr\}$. The corresponding channel gains are shown as $\lambda_{i,j} \triangleq |h_{i,j}|^2$. The additive white Gaussian noise (AWGN) at i is represented as n_i, with a variance of σ_i^2.

B. Threat Model

In this work, communication nodes from different networks are deemed untrusted when they interact within a particular network. In this context, the proposed threat model views nodes from external networks as *honest-but-curious* passive eavesdroppers. Untrusted user devices within this framework serve as simple communication devices without sophisticated hardware capabilities. Data transmission in our network model primarily adheres to a two-phase Time-Division Multiple Access strategy. In Phase I, the PT sends its data to the ST, which decodes, then re-encodes the message, amalgamating it with its own message using NOMA. Subsequently, the ST broadcasts this composite message to both the PR and the SR. This two-phase transmission process exposes the network to two distinct security threats. Initially, if the link quality between the PT and the ST is sufficiently robust, the ST could potentially compromise the PT's data post-reception. Secondly, when the PR intercepts the superposed signal from the ST—which also contains the SR's intended message—the PR could, in principle, decode the SR's message by employing SIC decoding methods, thereby breaching the secondary network's confidentiality. Furthermore, the PT's message remains at risk because the SR is capable of using SIC decoding to intercept the message intended for the PR. In our research, we demonstrate that the security design we propose fortifies the confidentiality of each network, bolstering privacy defenses against passive eavesdropping by nodes from an adversarial network.

IV. PROPOSED DESIGN AND PERFORMANCE ANALYSIS

A. Proposed Design and Signal Model

In Phase I, PT transmits the symbol x_p to the ST. Simultaneously in this phase, as part of the proposed CADP-CJ approach, PR sends the jamming signal $x_j^{(1)}$ to both ST and SR. Although the SR discards the jamming signal, this jamming signal confuses the ST when it tries to receive the signal from the PT. [3] The signal that ST receives is denoted as $y_{st} = h_{pt,st}\sqrt{p_{pt}}x_p + \sqrt{p_{pr,st}^J}x_j^{(1)}h_{pr,st} + n_{st}$, where p_{pt} represents the transmitted power from the PT and $p_{pr,st}^J$ denotes the jamming power. After signal reception, the ST

[2] In this work, the secondary network's role as a DF relay is central to the security problem we address. Although DF relaying incurs higher energy costs compared to AF due to decoding and re-encoding operations, we assume that the ST operates in a context where such energy expenditure is acceptable in exchange for enhanced confidentiality.

[3] We assume that the SR lacks knowledge of the jamming signal, perceiving it as a garbled signal. Consequently, the SR cannot utilize this signal to decode the original signal intended for the PR, leading it to simply discard the signal upon reception. It's worth noting that while we view the SR as an untrusted and curious node, it does not act as a malicious or aggressive attacker for the primary network.

estimates x_p, symbolized as $\tilde{x}_p$. The SINR at ST, used for estimating x_p, is given by

$$\gamma_{st}^{(x_p)} = \frac{\rho_{pt}\lambda_{pt,st}}{\rho_{pr,st}^{J}\lambda_{pr,st}+1}, \tag{1}$$

where $\rho_{pt} = \frac{p_{pt}}{\sigma_{st}^2}$ and $\rho_{pr,st}^{J} = \frac{p_{pr,st}^{J}}{\sigma_{st}^2}$. In Phase II, the ST re-encodes $\tilde{x}_p$ using its own symbol x_s and broadcasts the subsequent signal to both the PR and the SR. The superposed signal transmitted by the ST to the PR and SR can be described as $\sqrt{\alpha_p p_{st}}\tilde{x}_p + \sqrt{\alpha_s p_{st}}x_s$, where p_{st} denotes the total transmitted power budget of the ST. α_p and α_s are the power weighting coefficients. Without any loss of generality, it is assumed they adhere to the condition $\alpha_p + \alpha_s = 1$.

In our proposed privacy model, the ST handles the power distribution for both the PR and SR based on their channel strengths. Two scenarios arise: either the PR has a superior channel strength compared to the SR or vice versa. The privacy strategy for each case is outlined below:

1) Case I- SR has superior channel strength: Following the standard NOMA principle, more power is allocated to the PR's signal due to its inferior channel. On the SR's end, it decodes an estimation of PR's symbol $\tilde{x}_p$ and then isolates it from the joint signal to decode its unique symbol x_s. Since the decoded PR's symbol is already polluted, the primary network's privacy remains intact. Conversely, the PR decodes $\tilde{x}_p$, eventually recovering x_p since it possesses adequate information about the jamming signal $x_j^{(1)}$. It views the signal meant for the SR as mere noise, ensuring the secondary network's privacy.

2) Case II- PR has superior channel strength: If adhering to the conventional NOMA principle, the PR's signal would be assigned less power than the SR's. In this instance, the SR's signal would be decipherable on the PR's end, compromising the secondary network's privacy. Introducing jamming from other nodes won't resolve the problem. If jamming hampers the PR's ability to discern the SR's signal, the PR would also struggle to recognize its own signal due to the decoding sequence. This scenario underscores a crucial privacy concern.

To counter this, we deviate from traditional NOMA principles and utilize a reverse SIC mechanism. Here, the PR's signal gets a larger power allocation. During this phase, as part of the CADP-CJ strategy, the SR dispatches a jamming signal $x_j^{(2)}$ to the PR, affecting its decodability. The allocation of jamming power should be between the power allocated for the PR and SR. Therefore, the decoding order, in this case, will be adjusted to: PR's signal → Jamming signal → SR's signal. In this case, the PR attempts to decode while treating both the jamming and SR signals as interference. Considering the uncertainty in achieving positive secrecy for Case II, our analysis in this paper will predominantly focus on this case.

With the jamming signal $x_j^{(2)}$ and jamming power $\rho_{sr,pr}^{J}$ now in play, the signal the PR receives in Phase II is $y_{pr} = h_{st,pr}\left(\sqrt{\alpha_p p_{st}}\tilde{x}_p + \sqrt{\alpha_s p_{st}}x_s\right) + h_{sr,pr}\sqrt{p_{sr,pr}^{J}}x_j^{(2)} + n_{pr}$, which then recovers x_p and then the SINR for decoding x_p can be defined as

$$\gamma_{pr}^{(x_p)} = \frac{\rho_{st,pr}\alpha_p\lambda_{st,pr}}{\rho_{sr,pr}^{J}\lambda_{sr,pr}+\rho_{st,pr}\alpha_s\lambda_{st,pr}+1}, \tag{2}$$

where $\rho_{st,pr} = \frac{p_{st}}{\sigma_{pr}^2}$ and $\rho_{sr,pr}^{J} = \frac{p_{sr,pr}^{J}}{\sigma_{pr}^2}$. Given that the PR lacks any awareness of $x_j^{(2)}$, its decoding fails. Thus, the SINR for decoding x_s is given by

$$\gamma_{pr}^{(x_s)} = \frac{\rho_{st,pr}\alpha_s\lambda_{st,pr}}{\rho_{sr,pr}^{J}\lambda_{sr,pr}+\delta\rho_{st,pr}\alpha_p\lambda_{st,pr}+1}, \tag{3}$$

where δ is called the residual interference. Since $x_j^{(2)}$ is unknown and non-decodable at the PR, it is treated solely as interference. On the secondary receiving side, the SR receives $y_{sr} = h_{st,sr}\left(\sqrt{\alpha_p p_{st}}\tilde{x}_p + \sqrt{\alpha_s p_{st}}x_s\right) + n_{sr}$ and decodes the tainted estimate $\tilde{x}_p$, setting the effective rate for decoding x_p at the SR to zero. Afterward, it subtracts $\tilde{x}_p$ from the aggregate signal. Having knowledge about the jamming signal, the SR can effortlessly separate it from the compound signal to decode x_s. Consequently, the SINR for decoding x_s is given by

$$\gamma_{sr}^{(x_s)} = \rho_{st,sr}\alpha_s\lambda_{st,sr}, \tag{4}$$

where $\rho_{st,sr} = \frac{p_{st}}{\sigma_{sr}^2}$. In the following subsections, we thoroughly analyze the secrecy performance of both primary and secondary networks.

B. Performance Analysis: Primary Network

In this section, we derive the closed-form solutions for the ESR of the primary network. The ESR represents an average metric of the secrecy rate across all possible channel realizations. Grounded in the statistical properties and inherent randomness of these channels, the ESR offers robust insights into how the communication channels impact the secrecy rate. Now, the achievable rate for decoding x_p at the legitimate node PR is estimated as $R_{x_p} = \log_2\left(1+\gamma_{pr}^{(x_p)}\right)$. Conversely, the effective achievable rate at the ST for decoding x_p is $\tilde{R}_{x_p} = \log_2\left(1+\gamma_{st}^{(x_p)}\right)$. Thus, the ESR for the primary network can be represented as

$$\begin{aligned}\overline{R}_{\text{sec},x_p} &= \frac{1}{2}\left(\overline{R}_{x_p} - \overline{\tilde{R}}_{x_p}\right)\\ &= \frac{1}{2}E\left[\log_2\left(1+\gamma_{pr}^{x_p}\right)\right] - E\left[\log_2\left(1+\gamma_{st}^{x_p}\right)\right]\\ &= \frac{1}{2}\Bigg[\int_0^\infty \log_2\left(1+\gamma_{pr}^{x_p}\right) f\left(\gamma_{pr}^{x_p}\right)\mathrm{d}\gamma_{pr}\\ &\qquad - \int_0^\infty \log_2\left(1+\gamma_{st}^{x_p}\right) f\left(\gamma_{st}^{x_p}\right)\mathrm{d}\gamma_{st}\Bigg],\end{aligned} \tag{5}$$

where $E\left[.\right]$ and $f\left(.\right)$ denote the expectation operator and the probability distribution function (PDF). Now, the cumulative distribution function (CDF) of λ_a is

$$F_{\lambda_a}\left(x\right) = 1 - \sum_{i=0}^{m_a-1}\frac{\beta_a^i x^i}{i!}\exp\left(-\beta_a x\right), \tag{6}$$

where $\beta_a = \frac{m_a}{\Omega_a}$, and $\Omega_a = E\left[\lambda_a\right]$ denotes the channel second moment, m_a signifies the fading severity parameter, and $\Gamma\left(.\right)$ is the Gamma function as defined in [[38], Eqn. (8.339.1)].

Now, from (5), we infer $\overline{R}_{x_p} = \int_0^\infty \log_2\left(1+\gamma_{pr}^{(x_p)}\right) f\left(\gamma_{pr}^{(x_p)}\right)$. Applying integration by

$$F_{\gamma_{pr}^{x_p}}(x) = 1 - \sum_{i=0}^{m_{st,pr}-1} \sum_{i_1=0}^{i} \binom{i}{i_1} \frac{\beta_{st,pr}^{i} \beta_{sr,pr}^{m_{sr,pr}} x^i}{i!\Gamma(m_{sr,pr})(\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s)^i} \times \exp\left(-\frac{\beta_{st,pr}x}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s}\right)\Gamma(m_{sr,pr}+i_1)\left(\frac{x\beta_{st,pr}\rho_{sr,pr}^{J}}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s} + \beta_{sr,pr}\right)^{-(m_{sr,pr}+i_1)} \tag{8}$$

parts, we can rewrite the expression as

$$\overline{R}_{x_p} = \frac{1}{\log 2}\int_0^\infty \frac{1-F_{\gamma_{pr}^{(x_p)}}(x)}{1+x}dx. \tag{7}$$

Lemma 1: A closed-form expression of the CDF of $\gamma_{pr}^{(x_p)}$ is given by (8), as shown in the top of this page.

Proof: Please refer to Appendix A. As derived from Lemma 1, we then substitute $F_{\gamma_{pr}^{(x_p)}}(x)$ into (7). Now, we define the primary integral as I_1 and reorganize as

$$I_1 = \int_0^\infty \frac{x^i(\alpha_p - x\alpha_s)^{-i}\exp(-x)}{1+x}dx \times \left(\frac{x\beta_{st,pr}\rho_{sr,pr}^{J}}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s} + \beta_{sr,pr}\right)^{-(m_{sr,pr}+i_1)} \tag{9}$$

Obtaining a closed-form expression for (9) is difficult. Hence, we resort to the Taylor-Maclaurin expansion. As $m_{sr,pr} > i > i_1$, expanding the term in (9), we get

$$\begin{aligned}&\left[x\left(\beta_{st,pr}\rho_{sr,pr}^{J} - \alpha_s\beta_{sr,pr}\rho_{st,pr}\right)\right.\\ &\quad\left.+\alpha_p\beta_{sr,pr}\rho_{st,pr}\right]^{-(m_{sr,pr}+i_1)}\\ &= \left(\alpha_p\beta_{sr,pr}\rho_{st,pr}\right)^{-(m_{sr,pr}+i_1)}\left(1-\psi_1 x+\psi_2 x^2+\ldots\right),\end{aligned} \tag{10}$$

where ψ_{1-2} are two constants and denoted as $\psi_1 = \frac{(m_{sr,pr}+i_1)\left(\beta_{st,pr}\rho_{sr,pr}^{J}-\alpha_s\beta_{sr,pr}\rho_{st,pr}\right)}{\alpha_p\beta_{sr,pr}\rho_{st,pr}}$, and $\psi_2 = \frac{(m_{sr,pr}+i_1)(m_{sr,pr}+i_1+1)}{2}\left(\frac{\beta_{st,pr}\rho_{sr,pr}^{J}-\alpha_s\beta_{sr,pr}\rho_{st,pr}}{\alpha_p\beta_{sr,pr}\rho_{st,pr}}\right)^2$. Given the characteristics of the fading severity parameter for the SR-PR link, the series in (10) likely converges within the initial terms. Additionally, using the generalized binomial theorem, we can expand the term $\left(1-\frac{x\alpha_s}{\alpha_p}\right)^{m_{sr,pr}+i_1-i}$ as follows

$$\left(1-\frac{x\alpha_s}{\alpha_p}\right)^{m_{sr,pr}+i_1-i} = \sum_{i_2=0}^{m_{sr,pr}+i_1-i}\binom{m_{sr,pr}+i_1-i}{i_2} \times (-1)^{i_2}\left(\frac{\alpha_s}{\alpha_p}\right)^{i_2} x^{i_2}. \tag{11}$$

Now, substituting these expanded terms and based on the Fubini's theorem [39], we can update I_1 accordingly as follows.

$$I_1 = \sum_{i_2=0}^{m_{sr,pr}+i_1-i}\binom{m_{sr,pr}+i_1-i}{i_2}(-1)^{i_2}\left(\frac{\alpha_s}{\alpha_p}\right)^{i_2} \times \int_0^\infty \frac{x^{i+i_2}(1-\psi_1+\psi_2)\exp\left(-\frac{\beta_{st,pr}x}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s}\right)}{(1+x)\left(\alpha_p\beta_{sr,pr}\rho_{st,pr}\right)^{(m_{sr,pr}+i_1)}}dx. \tag{12}$$

Now, we apply a change of variables setting $\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s = \xi$. After performing some mathematical manipulation, we obtain

$$\begin{aligned}I_1 = &\sum_{i_2=0}^{m_{sr,pr}+i_1-i}\binom{m_{sr,pr}+i_1-i}{i_2}(-1)^{i_2}\left(\frac{\alpha_s}{\alpha_p}\right)^{i_2}\\ &\times\int_0^{\rho_{st,pr}\alpha_p}\frac{\left(\frac{\rho_{st,pr}\alpha_p-\xi}{\rho_{st,pr}\alpha_s}\right)^{i+i_2}}{\rho_{st,pr}(\alpha_s+\alpha_p)-\xi}\\ &\times\left[1-\psi_1\frac{\rho_{st,pr}\alpha_p-\xi}{\rho_{st,pr}\alpha_s}+\psi_2\left(\frac{\rho_{st,pr}\alpha_p-\xi}{\rho_{st,pr}\alpha_s}\right)^2\right]\\ &\times\exp\left(-\frac{\beta_{st,pr}\left(\rho_{st,pr}\alpha_p-\xi\right)}{\xi\rho_{st,pr}\alpha_s}\right)d\xi.\end{aligned} \tag{13}$$

We apply the Gaussian–Chebyshev quadrature to solve the integral in (13). Subsequently, we obtain the closed-form solution for $\overline{R}_{x_p}$ as in (14), as shown in the top of the next page. In (14), the parameter χ_{i_3} is defined as $\chi_{i_3} = \frac{\rho_{st,pr}\alpha_p}{2}\left(\cos\left(\frac{\pi(2i_3-1)}{2\psi_3}\right)+1\right)$.

Remark 1: Observation of (14) reveals that $\overline{R}_{x_p}$ is significantly influenced by the values of $m_{st,pr}$ and $m_{sr,pr}$, primarily due to the combinatorial complexity arising from the nested summations. Moreover, $\overline{R}_{x_p}$ exhibits a monotonic increase with $\beta_{st,pr}$, evidenced by its positive exponents in the numerator. Conversely, it is reasonable to assume a monotonic decrease in $\overline{R}_{x_p}$ with an increase in $\beta_{sr,pr}$, due to its negative influence in the denominators.

Remark 2: The relationship depicted in (14) regarding transmit powers presents a complex picture. The impact of p_{st} on $\overline{R}_{x_p}$ is multifaceted; however, it is generally observed that an increase in p_{st} should lead to a higher $\overline{R}_{x_p}$. In a similar fashion, the $\overline{R}_{x_p}$ is expected to increase with an increase in α_p, and decrease with an increase in α_s.

Moreover, $\overline{\tilde{R}}_{x_p}$ can be similarly extended with the help of integration by parts, and expressed as $\overline{\tilde{R}}_{x_p} = \frac{1}{\log 2}\int_0^\infty \frac{1-F_{\gamma_{st}^{(x_p)}}(x)}{1+x}dx$.

Lemma 2: A closed-form expression of the CDF of $\gamma_{st}^{(x_p)}$ is given by

$$\begin{aligned}F_{\gamma_{st}^{(x_p)}}(x) = 1 - &\sum_{i=0}^{m_{pt,st}-1}\sum_{i_1=0}^{i}\binom{i}{i_1}\frac{x^i(\rho_{pr,st}^{J})^{i_1}\beta_{pr,st}^{m_{pr,st}}}{\rho_{pt}^{i}i!\Gamma(m_{pr,st})}\\ &\times\beta_{pt,st}^{i}\left(\frac{\beta_{pt,st}x\rho_{pr,st}^{J}}{\rho_{pt}}+\beta_{pr,st}\right)^{-(m_{pr,st}+i_1)}\\ &\times\exp\left(-\frac{\beta_{pt,st}x}{\rho_{pt}}\right)\Gamma(m_{pr,st}+i_1).\end{aligned} \tag{15}$$

$$\overline{R}_{x_p} = \sum_{i=0}^{m_{st,pr}-1} \sum_{i_1=0}^{i} \sum_{i_2=0}^{m_{sr,pr}+i_1-i} \sum_{i_3=0}^{\psi_3} \binom{m_{sr,pr}+i_1-i}{i_2} (-1)^{i_2} \binom{i}{i_1} \frac{\pi \beta_{st,pr}^{i} \left(\rho_{sr,pr}^{J}\right)^{i_1} \alpha_p^{m_{sr,pr}+i_1-i+1}}{2i! \psi_3 \log\left(2\right) \Gamma\left(m_{sr,pr}\right) \beta_{sr,pr}^{i_1} \alpha_s^{i}} \\ \times \frac{\rho_{st,pr}^{m_{sr,pr}+i_1-i+1} \left(\rho_{st,pr}\alpha_p - \chi_{i_3}\right)^{i+i_2}}{\left(\rho_{st,pr}\alpha_s + \rho_{st,pr}\alpha_p - \chi_{i_3}\right)} \times \left(1 - \psi_1 \frac{\rho_{st,pr}\alpha_p - \chi_{i_3}}{\rho_{st,pr}\alpha_s} + \psi_2 \left(\frac{\rho_{st,pr}\alpha_p - \chi_{i_3}}{\rho_{st,pr}\alpha_s}\right)^2\right) \\ \times \exp\left(-\frac{\beta_{st,pr}\left(\rho_{st,pr}\alpha_p - \chi_{i_3}\right)}{\chi_{i_3}\rho_{st,pr}\alpha_s}\right) \Gamma\left(m_{sr,pr}+i_1\right) \tag{14}$$

$$\overline{\tilde{R}}_{x_p} = \sum_{i=0}^{m_{pt,st}-1} \sum_{i_1=0}^{i} \sum_{i_2=0}^{m_{pr,st}+i_1} \left(\begin{array}{c} i \\ i_1 \end{array}\right) \left(\begin{array}{c} m_{pr,st}+i_1+i_2-1 \\ i_2 \end{array}\right) (-1)^{i_2} \frac{\beta_{pt,st}^{i} \beta_{pr,st}^{m_{pr,st}} \left(\rho_{pr,st}^{J}\right)^{i_1} \rho_{pt}^{m_{pr,st}+i_1} \left(\rho_{pt}\beta_{pr,st}\right)^{i_2}}{\log 2 \rho_{pt}^{i} i! \left(\beta_{pt,st}\rho_{pr,st}^{J}\right)^{\left(m_{pr,st}+i_1+i_2\right)}} \\ \times \exp\left(\frac{\beta_{pt,st}}{\rho_{pt}}\right) \frac{\Gamma\left(m_{pr,st}+i_1\right) \Gamma\left(i-m_{pr,st}-i_1-i_2+1\right) \Gamma\left(m_{pr,st}+i_1+i_2-i, \frac{\beta_{pt,st}}{\rho_{pt}}\right)}{\Gamma\left(m_{pr,st}\right)} \tag{16}$$

Proof: Please refer to Appendix B.

After substituting $F_{\gamma_{st}^{(x_p)}}(x)$, let us denote the resulting integral as I_2. To solve I_2, we slightly modify and employ the binomial expansion for the term $\left(\beta_{pt,st} x \rho_{pr,st}^{J} + \rho_{pt}\beta_{pr,st}\right)^{-(m_{pr,st}+i_1)}$. Finally, we update and solve I_2 with the help of [[38], Eqn. (3.383-10)], and obtain the closed-form expression of $\overline{\tilde{R}}_{x_p}$ as (16), which is shown at the top of this page. In (16), $\Gamma(z_1, z_2)$ is called the upper incomplete Gamma fucntion, where $\Gamma\left(z_1, z_2\right) = \int_{z_2}^{\infty} x^{z_1-1} \exp\left(-x\right) dx$. Now, using (14), (16), and (5), a final form of $\overline{R}_{\text{sec},x_p}$ can be obtained.

Remark 3: Concerning $\overline{R}_{\text{sec},x_p}$, an essential observation emerges when considering the characteristics of the involved channels. Assuming other channel parameters remain constant, the changes in channel parameters discussed in Remark 1 are also applicable to $\overline{R}_{\text{sec},x_p}$. However, in this scenario, the impact of increasing $\beta_{pt,st}$ on $\overline{R}_{\text{sec},x_p}$ is more complex due to its presence in an exponential term. Nevertheless, $\overline{R}_{\text{sec},x_p}$ is expected to exhibit a monotonic decrease with an increase in $\beta_{pr,st}$, as indicated by Equation (16).

Remark 4: It is distinctly noticeable that increasing the jamming power $p_{pr,st}^{J}$ leads to a monotonic enhancement of $\overline{R}_{\text{sec},x_p}$. This improvement escalates with an increase in $m_{pr,st}$, which aligns with the expectation that a higher channel gain between PR and ST, coupled with increased jamming power $p_{pr,st}^{J}$, should positively influence the overall secrecy rate. However, it is important to note that an increase in p_{pt} results in a decrease of $\overline{R}_{\text{sec},x_p}$.

Ergodic Asymptotic Behavior

To gain further intuitive insights, we conduct an ergodic asymptotic analysis of the secrecy rate within the primary network. It can be readily inferred from (2) that a positive secrecy rate in the primary network is assured if $p_{st} \to \infty$ and $\gamma_{pr}^{(x_p)} \to \infty$; consequently, $R_{x_p} \to \infty$. Similarly, if $p_{pt} \to \infty$, then $\gamma_{st}^{(x_p)} \to \infty$, leading to $\tilde{R}_{x_p} \to \infty$, which implies that $R_{\text{sec},x_p} \to 0$ is significant.

Therefore, we examine the asymptotic performance by allowing both p_{st} and p_{pt} to jointly approach infinity. As a result, under the condition where $p_{st} \to \infty \&\& p_{pt} \to \infty$, we arrive at the following relationships.

$$\hat{\gamma}_{pr}^{(x_p)} = \frac{\alpha_p}{\alpha_s}, \hat{\gamma}_{st}^{(x_p)} = p_{pt}\lambda_{pt,st}, \tag{17}$$

where $\hat{a}$ represents the asymptotic expression for a. By incorporating these values, we formulate the asymptotic ESR (AESR) as

$$\overline{\hat{R}}_{\text{sec},x_p} = \frac{1}{2}\left(\overline{\hat{R}}_{x_p} - \overline{\hat{\tilde{R}}}_{x_p}\right) \\ = \frac{1}{2}E\left[\log_2\left(1+\hat{\gamma}_{pr}^{(x_p)}\right)\right] - \frac{1}{2}E\left[\log_2\left(1+\hat{\gamma}_{st}^{(x_p)}\right)\right]. \tag{18}$$

We can write $E\left[\log_2\left(1+\hat{\gamma}_{pr}^{(x_p)}\right)\right] = \log_2\left(1+\hat{\gamma}_{pr}^{(x_p)}\right)$, as the SINR is deterministic, not subject to the random fluctuations typically associated with channel fading. Conversely, $\overline{\hat{\tilde{R}}}_{x_p}$ can be elaborated upon as

$$\overline{\hat{\tilde{R}}}_{x_p} = E\left[\log_2\left(1+\hat{\gamma}_{st}^{(x_p)}\right)\right] = \frac{1}{\log 2}\int_0^{\infty} \frac{1-F_{\hat{\gamma}_{st}^{(x_p)}}\left(x\right)}{1+x} dx, \tag{19}$$

where $F_{\lambda_{pt,st}}\left(x\right) = 1 - \sum_{i=0}^{m_{pt,st}-1} \frac{\beta_{pt,st}^{i}(x)^{i}}{p_{pt}^{i} i!} \exp\left(-\frac{x\beta_{pt,st}}{p_{pt}}\right)$. Inserting $F_{\lambda_{pt,st}}\left(x\right)$ into (19), and resolving with the aid of [[38], Eqn. (3.383-10)], we deduce

$$\overline{\hat{\tilde{R}}}_{x_p} = \sum_{i=0}^{m_{pt,st}-1} \frac{\beta_{pt,st}^{i}\Gamma\left(i+1\right)\Gamma\left(-i, \frac{\beta_{pt,st}}{p_{pt}}\right)}{p_{pt}^{i} i! \log 2} \exp\left(\frac{\beta_{pt,st}}{p_{pt}}\right). \tag{20}$$

Ultimately, we derive the closed-form expression of $\overline{\hat{R}}_{\text{sec},x_p}$ as

$$\overline{\hat{R}}_{\text{sec},x_p} = \frac{1}{2}\left[\log_2\left(1+\frac{\alpha_p}{\alpha_s}\right) - \right. \\ \left. \sum_{i=0}^{m_{pt,st}-1} \frac{\beta_{pt,st}^{i}\Gamma\left(i+1\right)\Gamma\left(-i, \frac{\beta_{pt,st}}{p_{pt}}\right)}{p_{pt}^{i} i! \log 2} \exp\left(\frac{\beta_{pt,st}}{p_{pt}}\right)\right]. \tag{21}$$

Remark 5: Notably, as $p_{st} \to \infty \&\& p_{pt} \to \infty$, the outcome in (21) is predominantly influenced by the ratio $\frac{\alpha_p}{\alpha_s}$. Despite $\exp\left(\frac{\beta_{pt,st}}{p_{pt}}\right) \to 1$ with larger p_{pt} values, $\frac{\beta_{pt,st}}{p_{pt}} \to 0$ correspondingly. The Gamma function $\Gamma(i+1)$ and $i!$ in (21) barely affect $\overline{\hat{R}}_{\text{sec},x_p}$ as they counterbalance one another, given that i is invariably a positive integer. Other parameters remain unaffected by p_{pt}, thus exerting a negligible impact on $\overline{\hat{R}}_{\text{sec},x_p}$.

Furthermore, the asymptotic behavior concerning the jamming powers is straightforward, i.e., $\rho^J_{sr,pr} \to \infty \&\& \gamma^{(x_p)}_{pr} \to 0$, and consequently $R_{x_p} \to 0$. The result is a null ESR for the primary network. Conversely, if $\rho^J_{pr,st} \to \infty$, then $\gamma^{(x_p)}_{st} \to 0$ is true, and as a result $\tilde{R}_{x_p} \to \infty$. It is not advocated to increase $\rho^J_{pr,st}$ significantly as it may impede the PR's ability to decode x_p. In such scenarios, striking a balance between the jamming powers becomes contingent upon the channel characteristics and the decoding prowess of the ST.

Additionally, although our work focuses on a single-antenna configuration for all the nodes, the proposed framework can be extended to MIMO systems. For instance, in MIMO scenarios, let us consider the channel matrix for the channel between PT and ST as $\mathbf{H}_{pt,st} \in {}^{N_{pt}\times N_{st}}$, where N_{pt} and N_{st} are the number of antennas at the PT and ST. Therefore, the channel gain becomes $\|\mathbf{H}_{pt,st}\|^2_F = \sum_{m=1}^{N_{pt}}\sum_{n=1}^{N_{st}} |h_{pt,st}|^2$[4], which can be approximated via moment matching using the Gamma distribution, with shape and scale parameters scaled by the number of antennas at the transmitter and receiver [40]. This allows the preservation of a closed-form analytical structure similar to the single antenna case.

C. Performance Analysis: Secondary Network

The achievable rate for decoding x_s at the SR node is represented by $R_{x_s} = \log_2\left(1+\gamma^{(x_s)}_{sr}\right)$. For the secondary network, the PR node is considered untrusted. The achievable rate for decoding x_s at PR is given by $\tilde{R}_{x_s} = \log_2\left(1+\gamma^{(x_s)}_{pr}\right)$. Consequently, we can estimate the secrecy rate for the secondary network as $R_{\text{sec},x_s} = \max\left(0, R_{x_s} - \tilde{R}_{x_s}\right)$. Therefore, the ESR can be expressed as

$$\begin{aligned}\overline{R}_{\text{sec},x_s} &= \overline{R}_{x_s} - \overline{\tilde{R}}_{x_s}\\ &= \int_0^\infty \log_2\left(1+\gamma^{(x_s)}_{sr}\right) f\left(\gamma^{(x_s)}_{sr}\right)\\ &\quad - \int_0^\infty \log_2\left(1+\gamma^{(x_s)}_{pr}\right) f\left(\gamma^{(x_s)}_{pr}\right).\end{aligned} \tag{22}$$

$\overline{R}_{x_s}$ can further be extended as $\overline{R}_{x_s} = \frac{1}{\log 2}\int_0^\infty \frac{1-F_{\gamma^{(x_s)}_{sr}}(x)}{1+x}dx$. We consider $\delta = 0$ for analytical tractability. Next, $F_{\gamma^{(x_s)}_{sr}}(x)$ can simply be derived as

$$F_{\gamma^{(x_s)}_{sr}}(x) = 1 - \sum_{i=0}^{m_{st,sr}-1} \frac{\beta^i_{st,sr}\left(\frac{x}{\rho_{st,sr}\alpha_s}\right)^i}{i!} \exp\left(-\frac{\beta_{st,sr}x}{\rho_{st,sr}\alpha_s}\right). \tag{23}$$

Substituting $F_{\gamma^{(x_s)}_{sr}}(x)$ into the original integral, we derive the closed-form expression of $\overline{R}_{x_s}$ as follows.

$$\overline{R}_{x_s} = \sum_{i=0}^{m_{st,sr}-1} \frac{\beta^i_{st,sr}\exp\left(\frac{\beta_{st,sr}}{\rho_{st,sr}\alpha_s}\right)\Gamma(i+1)\Gamma\left(-i, \frac{\beta_{st,sr}}{\rho_{st,sr}\alpha_s}\right)}{i!(\rho_{st,sr}\alpha_s)^i \log 2}. \tag{24}$$

Remark 6: While an increase in $\beta_{st,sr}$ suggests an enhancement of $\overline{R}_{x_s}$, this increase is not direct or linear, largely owing to the involvement of the incomplete gamma function in the equation. A comparable phenomenon can be observed with $p_{st,sr}$ and α_s, where their effects on $\overline{R}_{x_s}$ are likewise influenced by complex factors.

On the other hand, $\overline{\tilde{R}}_{x_s}$ can be similarly extended to $\overline{\tilde{R}}_{x_s} = \frac{1}{\log 2}\int_0^\infty \frac{1-F_{\gamma^{(x_s)}_{pr}}(x)}{1+x}dx$.

Lemma 3: A closed-form expression for $F_{\gamma^{(x_s)}_{pr}}(x)$ is given by (25), as shown in the top of the next page.

Proof: The proof of Lemma 3 follows the same pattern of Lemma 1, albeit with distinct symbols and equations. Please refer to Appendix A for the underlying proof approach.

Following Lemma 3, we substitute $F_{\gamma^{(x_s)}_{pr}}(x)$ in the $\overline{\tilde{R}}_{x_s}$ equation, and denote the resulting integral as I_3. Now, directly solving I_3 is difficult due to its complexity. To simplify, using the generalized binomial theorem, we approximate the term $\left(\beta_{sr,pr} + \frac{\rho^J_{sr,pr}\beta_{st,pr}x}{\rho_{st,pr}\alpha_s}\right)^{-m_{sr,pr}-i_1} \approx \beta^{-m_{sr,pr}-i_1}_{sr,pr} - \psi_4 x + \psi_5 x^2$, where ψ_{4-5} are two constants and defined as $\psi_4 = \frac{\rho^J_{sr,pr}\beta_{st,pr}(m_{sr,pr}+i_1)}{\rho_{st,pr}\alpha_s\beta^{m_{sr,pr}+i_1+1}_{sr,pr}}$ and $\psi_5 = \frac{1}{2}(m_{sr,pr}+i_1)(m_{sr,pr}+i_1+1) \times \beta^{-m_{sr,pr}-i_1-2}_{sr,pr}\left(\frac{\rho^J_{sr,pr}\beta_{st,pr}}{\rho_{st,pr}\alpha_s}\right)^2$.

After substituting these expanded terms into I_3, we solve the integral using [[38], Eqn. (3.353-5)]. Furthermore, after some mathematical manipulations, we attain the closed-form expression for $\overline{\tilde{R}}_{x_s}$ as (26), shown at the top of the next page. In (26), ψ_6 is defined as $\psi_6 = \frac{\beta_{st,pr}}{\rho_{st,pr}\alpha_s}$. Finally, with the help of (26), (24), and (22), we obtain the final form of $\overline{R}_{\text{sec},x_s}$.

Remark 7: It is evident from (26) that $\overline{\tilde{R}}_{x_s}$ decreases as the jamming power $\rho^J_{sr,pr}$ increases. However, the impact of fading channels on this trend is somewhat complex. It is clear that stronger ST-PR links increase $\overline{\tilde{R}}_{x_s}$, whereas stronger SR-PR links, which also constitute the jamming link, lead to a decrease in $\overline{\tilde{R}}_{x_s}$.

Ergodic Aasymptotic Behavior

We provide the asymptotic analysis in this section to enhance our understanding of the secrecy performance of the secondary network. By allowing $p_{st} \to \infty$, we arrive at the following expressions

$$\hat{\gamma}^{(x_s)}_{pr} = p_{st}\alpha_s\lambda_{st,pr}, \hat{\gamma}^{(x_s)}_{sr} = p_{st}\alpha_s\lambda_{st,sr}. \tag{27}$$

Consequently, we can represent the AESR for the secondary network as

$$\begin{aligned}\overline{\hat{R}}_{\text{sec},x_s} &= \overline{\hat{R}}_{x_s} - \overline{\hat{\tilde{R}}}_{x_s}\\ &= \frac{1}{\log 2}\left(\int_0^\infty \frac{1-F_{\hat{\gamma}^{(x_s)}_{sr}}(x)}{1+x}dx - \int_0^\infty \frac{1-F_{\hat{\gamma}^{(x_s)}_{pr}}(y)}{1+y}dy\right),\end{aligned} \tag{28}$$

[4] $\|.\|_F$ denotes the Frobenius norm.

$$F_{\gamma_{pr}^{(x_s)}}(x) = 1 - \sum_{i=0}^{m_{st,pr}-1} \sum_{i_1=0}^{i} \begin{pmatrix} i \\ i_1 \end{pmatrix} \frac{\beta_{st,pr}^{i} \Gamma(m_{sr,pr}+i_1)}{i! \beta_{sr,pr}^{m_{sr,pr}} x^i \left(\rho_{sr,pr}^{J}\right)^{i_1} \left(\rho_{st,pr}\alpha_s\right)^{i} \Gamma(m_{sr,pr})} \times \exp\left(-\frac{\beta_{st,pr}x}{\rho_{st,pr}\alpha_s}\right) \left(\beta_{sr,pr} + \frac{\rho_{sr,pr}^{J}\beta_{st,pr}x}{\rho_{st,pr}\alpha_s}\right)^{-(m_{sr,pr}+i_1)} \quad (25)$$

$$\overline{\tilde{R}}_{x_s} = \sum_{i=0}^{m_{st,pr}-1} \sum_{i_1=0}^{i} \begin{pmatrix} i \\ i_1 \end{pmatrix} \frac{\beta_{st,pr}^{i} \Gamma(m_{sr,pr}+i_1)\, i \psi_6^{-i-2} \Gamma(i)}{i! \beta_{sr,pr}^{m_{sr,pr}} \left(\rho_{sr,pr}^{J}\right)^{i_1} (\rho_{st,pr}\alpha_s)^{i} \Gamma(m_{sr,pr}) \log 2} \begin{pmatrix} \psi_6^2 \exp(\psi_6)\left(\beta_{sr,pr}^{-m_{sr,pr}-i_1} + \psi_4 + \psi_5\right) \\ E_{i+1}(\psi_6) + \psi_5(i+1) - \psi_6(\psi_4+\psi_5) \end{pmatrix} \quad (26)$$

$$\overline{\hat{R}}_{\text{sec},x_s} = \frac{1}{\log 2} \left(\sum_{i=0}^{m_{st,sr}-1} \frac{\beta_{st,sr}^{i} \Gamma(i+1) \Gamma\left(-i, \frac{\beta_{st,sr}}{p_{st}\alpha_s}\right) \exp\left(\frac{\beta_{st,sr}}{p_{st}\alpha_s}\right)}{(p_{st}\alpha_s)^{i} i!} - \sum_{j=0}^{m_{st,pr}-1} \frac{\beta_{st,pr}^{j} \Gamma(j+1) \Gamma\left(-j, \frac{\beta_{st,pr}}{p_{st}\alpha_s}\right) \exp\left(\frac{\beta_{st,pr}}{p_{st}\alpha_s}\right)}{(p_{st}\alpha_s)^{j} j!} \right) \quad (31)$$

where we can estimate $F_{\hat{\gamma}_{sr}^{(x_s)}}(x)$ and $F_{\hat{\gamma}_{pr}^{(x_s)}}(y)$ as follows.

$$F_{\hat{\gamma}_{sr}^{(x_s)}}(x) = 1 - \sum_{i=0}^{m_{st,sr}-1} \frac{\beta_{st,sr}^{i}\left(\frac{x}{p_{st}\alpha_s}\right)^{i}}{i! \exp\left(\beta_{st,sr}\frac{x}{p_{st}\alpha_s}\right)}, \quad (29)$$

$$F_{\hat{\gamma}_{pr}^{(x_s)}}(y) = 1 - \sum_{j=0}^{m_{st,pr}-1} \frac{\beta_{st,pr}^{j}\left(\frac{y}{p_{st}\alpha_s}\right)^{j}}{j! \exp\left(-\beta_{st,pr}\frac{y}{p_{st}\alpha_s}\right)}. \quad (30)$$

By substituting these two CDF expressions in (28) and solving, we deduce $\overline{\hat{R}}_{\text{sec},x_s}$ as in (31), shown at the top of this page.

Remark 8: As $p_{\underline{st}} \to \infty$, the 'fading severity parameter' markedly impacts $\overline{\hat{R}}_{\text{sec},x_s}$ as can be noticed in (31). When the fading severity between the ST and SR is substantial, it leads to a reduced secrecy rate. Conversely, when considering the fading severity between the ST and PR, the impact is the opposite. Therefore, the fading properties between these points play a crucial role. The influence of the Gamma functions in (31) could be marginal if we consider their potential equivalence to factorials, especially since both i and j are positive integers.

V. Design and Analysis in Multiple-User Case

In this section, we study the privacy implications within an overlay cognitive network with n SRs[5]. The privacy design complexity escalates with an increasing number of receivers, notably in the aspect of determining the decoding order for NOMA. A further complication in security arises from the coordination complexity required for the jamming signal, particularly in pinpointing the specific jamming node within the SRs. It is critical to manage the jamming signal such that it does not interfere with the transmission to other receivers. The jammer should be selected in a manner that disrupts the PR's decodability with minimal power allocated to the jamming signal.

We represent the channel coefficients for the SRs as h_{st,sr_a}, where $\forall a = \{1, 2, 3, ...,n\}$, with their respective channel gains noted as $\lambda_{st,sr_a} \triangleq |h_{st,sr_a}|^2$. We assume that these channel gains satisfy the inequality $\lambda_{st,sr_1} > \lambda_{st,sr_2} > ... > \lambda_{st,sr_n}$. The power allocation coefficients are represented as $\alpha_{s,a}$, while the AWGN at the receivers is denoted by n_{sr_a}, possessing a variance of $\sigma_{sr_a}^2$. The fading channel conditions and all ancillary parameters adhere to those defined for a single-user scenario. Symbols intended for the SRs are designated as $x_{s,a}$. The ST broadcasts $x_{s,a}$ with $\tilde{x}_p$ using NOMA. All SRs also receive the jamming signal $x_j^{(1)}$ dispatched by the PR to the ST in Phase I. As the SRs belong to the same network, we assume that non-jamming SRs have prior knowledge of the jamming signal structure. This allows them to subtract or cancel the jamming interference during reception, which ensures that their decoding performance is unaffected. This assumption is practical and consistent with coordinated secondary networks found in UAV or IoT deployments. In Phase II, the SR nearest to the PR is selected to transmit the jamming signal $x_j^{(2)}$ to the PR. This selection is facilitated by CSI at the ST. If the b-th SR is chosen, the signal that the PR receives is a superposition denoted by

$$y_{pr} = h_{st,pr}\left(\sqrt{\alpha_p p_{st}}\tilde{x}_p + \sum_{i=1}^{n}\sqrt{\alpha_{s,i}p_{st}}x_{s,i}\right) + h_{sr_b,pr}\sqrt{\rho_{sr,pr}^{J}}x_j^{(2)} + n_{pr}, \quad (32)$$

where $h_{sr_b,pr}$ is the channel coefficient between the b-th SR and the PR. When determining the decoding order and privacy design for NOMA transmission, we encounter two distinct

[5] The work can be further extended with multiple PRs. Nonetheless, introducing additional PRs escalates the complexity involved in preserving privacy and crafting the NOMA framework. In such expanded configurations, an SR would be required to jam multiple PRs simultaneously, significantly intensifying the complexity of the analytical model. To keep the scope of this study both concentrated and practical, our current focus remains on scenarios with multiple SRs. The intricate design challenges that arise from integrating numerous PRs will be systematically tackled in future iterations of this research.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2025.3606837

scenarios. In the first, the PR has the weakest channel relative to all receivers, necessitating the highest power allocation for the PR with a subsequent power distribution for the SRs following $\alpha_{s,1} < \alpha_{s,2} < ... < \alpha_{s,n}$. Due to this higher power allocation, the PR can decode $\tilde{x}_p$ with ease, treating the remaining signal as noise. The SIC decoding sequence for the SRs is given by $\tilde{x}_p \to x_{s,n} \to x_{s,n-1} \to x_{s,n-2} \to .... \to x_{s,2} \to x_{s,1}$, wherein, the effective rate for decoding x_p is nullified since $\tilde{x}_p$ is contaminated. This ensures privacy for both primary and secondary networks in this scenario. Conversely, the second scenario presents a situation where the PR's channel strength is variable, stronger than some SRs but weaker than others. Within this scenario is the unique case where PR has the strongest channel. This scenario demands an alternative strategy as the standard privacy design and NOMA decoding order adjustments are not applicable. Hence, our analysis focuses primarily on this scenario. We adopt a reverse SIC approach, granting maximal power to the PR's signal, while the power strategy for secondary users remains unchanged. Once the PR intercepts the superposed signal, it decodes and extracts x_p using the SINR as follows.

$$\gamma_{pr(m)}^{(x_p)} = \frac{\rho_{st,pr}\alpha_p\lambda_{st,pr}}{\rho_{sr_b,pr}^{J}\lambda_{sr_b,pr} + \sum_{i=1}^{n}\left[\rho_{st,pr}\alpha_{s,i}\lambda_{st,pr}\right] + 1}. \quad (33)$$

The PR's inability to decode $x_j^{(2)}$ precludes its removal from the combined signal using SIC, leaving the SINRs for decoding the a^{th} and 1^{st} symbols as

$$\gamma_{pr(m)}^{(x_{s,a})} = \frac{\rho_{st,pr}\alpha_{s,a}\lambda_{st,pr}}{\rho_{sr_b,pr}^{J}\lambda_{sr_b,pr} + \sum_{i=a+1}^{n}\left[\rho_{st,pr}\alpha_{s,i}\lambda_{st,pr}\right] + 1}, \quad (34)$$

$$\gamma_{pr(m)}^{(x_{s,1})} = \frac{\rho_{st,pr}\alpha_{s,1}\lambda_{st,pr}}{\rho_{sr,pr}^{J}\lambda_{sr,pr} + 1}. \quad (35)$$

The expression of $\gamma_{pr(m)}^{(x_{s,a})}$ provides a generalized formula, which, by nullifying interference terms, derives $\gamma_{pr(m)}^{(x_{s,1})}$. Conversely, at the SR, SINRs for decoding the a^{th} and 1^{st} symbols are expressed as

$$\gamma_{sr(m)}^{(x_{s,a})} = \frac{\rho_{st,sr_a}\alpha_{s,a}\lambda_{st,sr_a}}{\sum_{i=a+1}^{n}\left[\rho_{st,sr_a}\alpha_{s,i}\lambda_{st,sr_a}\right] + 1}, \quad (36)$$

$$\gamma_{sr(m)}^{(x_{s,1})} = \rho_{st,sr_1}\alpha_{s,1}\lambda_{st,sr_1}. \quad (37)$$

Next, we conduct an ESR analysis for both the primary and secondary networks. The ESR for the primary network in the multiple-user scenario can be expressed as $\overline{R}_{\mathrm{sec},x_p(m)} = \frac{1}{2}\left(\overline{R}_{x_p(m)} - \tilde{\overline{R}}_{x_p(m)}\right)$. Notably, the SINR expression in (33) closely resembles the mathematical structure of (2). Hence, the probabilistic approach to determine the closed-form expression for $\overline{R}_{x_p(m)}$ can be directly applied from the solution of $\overline{R}_{x_p}$ by evaluating at α_s equals $\sum_{i=1}^{n}\alpha_{s,i}$, $\rho_{sr,pr}^{J}$ equals $\rho_{sr_b,pr}^{J}$, and $\lambda_{sr,pr}$ equals $\lambda_{sr_b,pr}$. This approach yields the closed-form expression for $\overline{R}_{\mathrm{sec},x_p(m)}$ as follows.

$$\overline{R}_{\mathrm{sec},x_p(m)} = \frac{1}{2}\left(\overline{R}_{x_p}\Big|_{\Omega} - \tilde{\overline{R}}_{x_p}\right), \quad (38)$$

$$\Omega = \left\{\alpha_s = \sum_{i=1}^{n}\alpha_{s,i}\&\&\rho_{sr,pr}^{J} = \rho_{sr_b,pr}^{J}\&\&\lambda_{sr,pr} = \lambda_{sr_b,pr}\right\},$$

where $\overline{R}_{x_p(m)} = \overline{R}_{x_p}\big|_{\Omega}$. Furthermore, the ESR associated with decoding the a^{th} symbol in the secondary network can be denoted by $\overline{R}_{\mathrm{sec},x_{s,a}} = \overline{R}_{x_{s,a}} - \tilde{\overline{R}}_{x_{s,a}}$, which we extend further to

$$\begin{aligned}\overline{R}_{\mathrm{sec},x_{s,a}} = &\int_0^{\infty}\log_2\left(1+\gamma_{sr(m)}^{(x_{s,a})}\right)f\left(\gamma_{sr(m)}^{(x_{s,a})}\right)\\ &-\int_0^{\infty}\log_2\left(1+\gamma_{pr(m)}^{(x_{s,a})}\right)f\left(\gamma_{pr(m)}^{(x_{s,a})}\right)\end{aligned} \quad (39)$$

To expand $\overline{R}_{x_{s,a}}$, we obtain $\overline{R}_{x_{s,a}} = \frac{1}{\log 2}\int_0^{\infty}\frac{1-F_{\gamma_{sr(m)}^{(x_{s,a})}}(x)}{1+x}dx$, where $F_{\gamma_{sr(m)}^{(x_{s,a})}}(x)$ can be extended to (40), as shown at the top of the next page. We can substitute $F_{\gamma_{sr(m)}^{(x_{s,a})}}(x)$ in the original equation; let us denote the resulting integral as I_{m_1}. It is difficult to obtain a closed-form expression for I_{m_1} because of the structure of the exponential term. To make it tractable, we set $\rho_{st,sr}\alpha_{s,a} - x\sum_{i=a+1}^{n}\left[\rho_{st,sr}\alpha_{s,i}\right] = \xi_1$. Consequently, I_{m_1} can be expressed as (41), as shown at the top of the next page. (41) can be solved by applying Gaussian–Chebyshev quadrature. Let us denote $\chi_k = \frac{\rho_{st,sr_a}\alpha_{s,a}}{2}\left(\cos\left(\frac{\pi(2k-1)}{2\psi_7}\right)+1\right)$, where ψ_7 is a constant. Now, we obtain the closed-form expression for $\bar{R}_{x_{s,a}}$ as in (42), as shown in top of the next page. Conversely, the expression for $\gamma_{pr(m)}^{(x_{s,a})}$ exhibits a mathematical structure similar to that of $\gamma_{pr(m)}^{(x_p)}$. Thus, the probabilistic analysis to deduce the closed-form expression for $\tilde{\bar{R}}_{x_{s,a}}$ can be straightforwardly executed based on the solution of $\overline{R}_{x_p(m)}$ by evaluating $\sum_{i=1}^{n}\alpha_{s,i}$ at $\sum_{i=a+1}^{n}\alpha_{s,i}$, i.e., $\tilde{\overline{R}}_{x_{s,a}} = \overline{R}_{x_p(m)}\Big|_{\sum_{i=1}^{n}\alpha_{s,i}=\sum_{i=a+1}^{n}\alpha_{s,i}}$ Consequently, we acquire the closed-form expression of $\overline{R}_{\mathrm{sec},x_{s,a}}$ as follows.

$$\overline{R}_{\mathrm{sec},x_{s,a}} = \bar{R}_{x_{s,a}} - \overline{R}_{x_p(m)}\Big|_{\sum_{i=1}^{n}\alpha_{s,i}=\sum_{i=a+1}^{n}\alpha_{s,i}} \quad (43)$$

Note that in the single-user case, we consider a static power allocation strategy, setting the power allocation factor for the primary and secondary users at η, i.e., $\frac{\alpha_p}{\alpha_s} = \frac{\eta}{1-\eta}$. This approach simplifies the power allocation process and ensures a stable performance for the primary and secondary users. However, in the multiple-user scenario discussed in this section, the power allocation becomes more complex due to the presence of n SRs. In this case, the available power must be carefully partitioned to accommodate the SRs and the PR, while still maintaining a certain quality of service (QoS) at the PR's end.

To address this challenge, we developed a dynamic, top-down power allocation strategy based on the involved channel

$$F_{\gamma_{sr(m)}^{(x_{s,a})}}(x) = 1 - \sum_{j=0}^{m_{st,sr_a}-1} \frac{\beta_{st,sr_a}^{j} x^{j} \left(\rho_{st,sr_a}\alpha_{s,a} - x\sum\limits_{i=a+1}^{n}\left[\rho_{st,sr_a}\alpha_{s,i}\right]\right)^{-j}}{j!} \exp\left(-\frac{\beta_{st,sr_a} x}{\rho_{st,sr_a}\alpha_{s,a} - x\sum\limits_{i=a+1}^{n}\left[\rho_{st,sr_a}\alpha_{s,i}\right]}\right) \tag{40}$$

$$I_{m_1} = \int_0^{\rho_{st,sr_a}\alpha_{s,a}} \frac{\xi_1^{-j}\left(\rho_{st,sr_a}\alpha_{s,a} - \xi_1\right)^{j+1} \exp\left(-\frac{\beta_{st,sr_a}\left(\rho_{st,sr_a}\alpha_{s,a} - \xi_1\right)}{\xi_1 \sum\limits_{i=a+1}^{n} \rho_{st,sr_a}\alpha_{s,i}}\right)}{\left(\sum\limits_{i=a+1}^{n} \rho_{st,sr_a}\alpha_{s,i} + \rho_{st,sr_a}\alpha_{s,a} - \xi_1\right)\left(\sum\limits_{i=a+1}^{n} \rho_{st,sr_a}\alpha_{s,i}\right)^{j+1}} d\xi_1 \tag{41}$$

$$\bar{R}_{x_{s,a}} = \sum_{j=0}^{m_{st,sr}-1} \sum_{k=0}^{\psi_7} \frac{\pi \beta_{st,sr_a}^{j} \rho_{st,sr_a}\alpha_{s,a}}{2j! \log 2} \frac{\chi_k^{-j}\left(\rho_{st,sr_a}\alpha_{s,a} - \chi_k\right)^{j+1} \exp\left(-\frac{\beta_{st,sr_a}\left(\rho_{st,sr_a}\alpha_{s,a} - \chi_k\right)}{\chi_k \sum\limits_{i=a+1}^{n}\left[\rho_{st,sr_a}\alpha_{s,i}\right]}\right)}{\psi_7 \left(\sum\limits_{i=a+1}^{n}\left[\rho_{st,sr_a}\alpha_{s,i}\right] + \rho_{st,sr_a}\alpha_{s,a} - \chi_k\right)\left(\sum\limits_{i=a+1}^{n}\left[\rho_{st,sr_a}\alpha_{s,i}\right]\right)^{j+1}} \tag{42}$$

strengths, maintaining the constraint $\alpha_{s,1} < \alpha_{s,2} < ... < \alpha_{s,n} < \alpha_p$. The primary objective is to ensure PR adheres to the constraint that $\overline{R}_{\text{sec},x_p(m)}$ must exceed the predefined threshold $\overline{R}_\tau$. The power allocation is still governed by the factor η, however, in the multiple-user case, η is dynamically adjusted based on the number of SRs. Specifically, the power weighting coefficient η_τ corresponding to $\overline{R}_\tau$ is recalculated to accommodate the additional SRs while ensuring the PR's QoS is met. η is dynamically adjusted according to

$$\eta_n = \max\left(\eta - 5\left(n-2\right), \eta_\tau\right)/100. \tag{44}$$

Conversely, for the SRs, we implemented a decremental factor μ to allocate power among them. This factor is determined by the remaining power after allocating a portion for the PR's signal and the number of SRs n. This is governed by the expression

$$\alpha_{s,a} = \max\left(\frac{1-\alpha_{in}}{n-1} - \mu\left(a-1\right), 0\right). \tag{45}$$

The details of this dynamic power allocation algorithm are elaborated in Algorithm 1.

Algorithm 1 Power allocation

```
Input: $n$ (number of users), $p_{st}$ (Transmit power), $\overline{R}_\tau$ (ESR threshold), $\eta$ (Power allocation in two-user scenario), $\eta_\tau$ (Allocated power for $\overline{R}_\tau$), $a$ (specific SR)
Output: $\alpha_p$ (Power allocation for primary user), $\alpha_{s,a}$ (Power allocation for secondary user)
Begin
Initialize $\alpha_p$, $\alpha_{s,a}$
if $n = 1$ then
    Set $\alpha_p = \eta p_{st}$ & $\alpha_s = p_{st}\left(1-\eta\right)$
else
    Calculate $\eta_n$ using $\eta_n = \max\left(\eta - 5\left(n-2\right), \eta_\tau\right)/100$
    Set $\alpha_p = \eta_n p_{st}$ & $\sum_{i=1}^{n} \alpha_{s,i} = p_{st}\left(1-\eta_n\right)$
    Initialize array for $\alpha_{s,a}$
    Set initial factor $\alpha_{in} = \frac{(1-\eta_n)}{n-1}$ & $\mu = \frac{\alpha_{in}}{2(n-1)}$
    for $i = 1$ to $n-1$ do
        Update $\alpha_{s,i} = \max\left(\frac{1-\alpha_{in}}{n-1} - \mu\left(i-1\right), 0\right)$
        Set $\alpha_{s,a} = \alpha_{s,i}$
        Decrease $\alpha_{s,a}$ by $\mu$
        if $\alpha_{s,a} < 0$ then
            Set $\alpha_{s,a} = 0$
        end if
    end for
end if
Determine $\alpha_p$ & $\alpha_{s,a}$
Calculate $\sum_{i=a+1}^{n} \alpha_{s,i}$ for users after $a^{th}$ user
End
```

VI. Results and Discussion

In this section, we present and discuss the analytical and simulation results. All the results were obtained using Matlab. During the Monte-Carlo simulations, gamma-distributed random variables were generated by adjusting the fading and gain parameters through the 'gamrnd' function. We then obtained the square roots of these values to create Nakagami-m distributed random variables for all channel coefficients. For all the simulations, the total number of channel samples utilized was 10^5. For the presented results, unless specified otherwise, the parameters are set as follows: $p_{pt} = 40$ dBm, $p_{st} = 50$ dBm[6], $\alpha_p = 0.7$, $\alpha_s = 0.3$, $\delta = 0$, $\Omega_{pt,st} = \Omega_{pr,st} = \Omega_{st,sr} = \Omega_{sr,pr} = 1$, $\Omega_{st,pr} = 2$, $m_{pt,st} = m_{pr,st} = m_{st,pr} = m_{sr,pr} = m_{st,sr} = 3$, and $\sigma_{st}^2 = \sigma_{pr}^2 = \sigma_{sr}^2 = 30$ dBm. Additionally, this section includes a comparative analysis with two benchmark schemes. First, we

[6] We allocate more power to the ST than to the PT to reflect the ST's role as a broadcaster to both the PR and SR.

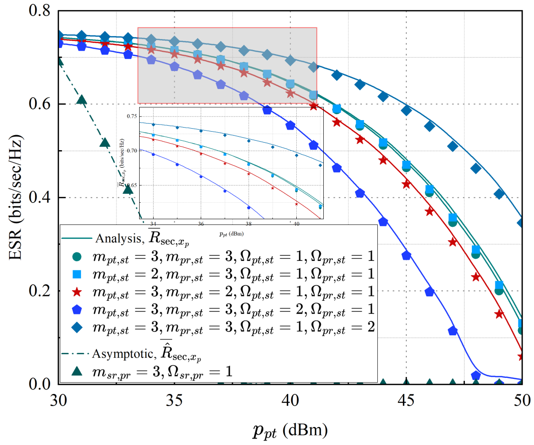

Fig. 2. ESR for the primary network versus p_{pt}.

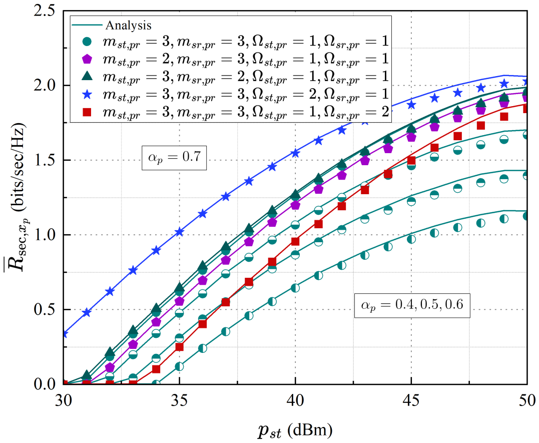

Fig. 3. ESR for the primary network versus p_{st}.

compare our approach with a conventional wireless system that does not employ jamming, to underscore the advantages of the proposed CADP-CJ method. Second, we compare our system with an OMA-based cognitive system, a widely used model in wireless communications. This comparison offers insights into the balance between enhancing secrecy and ensuring fairness in the system, with orthogonal frequency division multiple access serving as the reference scheme in our study. Notably, the strong correlation observed between the analytical and simulation results across all metrics underscores the accuracy of our analysis.

Figs. 2 and 3 demonstrate the effects of transmit power and channel fading on the ESR of the primary network. Fig. 2 shows the relationship between p_{pt} and $\overline{R}_{\text{sec},x_p}$, revealing that $\overline{R}sec, x_p$ decreases with an increase in p_{pt}. This trend is attributed to the increased likelihood of the ST successfully decoding x_p and countering the jamming as the PT transmits more power to the ST. Furthermore, the ESR is significantly influenced by variations in the Nakagami fading severity parameter and the second moment of the distribution. A reduced fading on the PR-ST jamming link and increased fading on the PT-ST link enhance the $\overline{R}_{\text{sec},x_p}$. This effect is further highlighted in the zoomed portion of Fig. 2. The impact of changing the second moment is more pronounced. Notably, a substantial improvement in $\overline{R}_{\text{sec},x_p}$ is observed when $\Omega_{pr,st}$ is increased to 2. Conversely, $\overline{R}_{\text{sec},x_p}$ significantly decreases, approaching nearly zero at $p_{pt} = 50$ dBm, when $\Omega_{st,pt}$ is set to 2. The influence of p_{pt} is also evident in the AESR, where $\overline{\hat{R}}_{\text{sec},x_p}$ drops to zero for $p_{pt} > 36$ dBm. This negative effect arises because $\overline{\hat{R}}_{\text{sec},x_p}$ depends solely on p_{pt}. Given that the ratio of α_p to α_s is constant, $\overline{\hat{R}}_{\text{sec},x_p}$ is heavily influenced by p_{pt}. In Fig. 3, $\overline{R}_{\text{sec},x_p}$ is plotted against p_{st} and α_p. It is evident that $\overline{R}_{\text{sec},x_p}$ significantly improves with an increase in p_{st}. The power weighting coefficient α_p also plays a crucial role in influencing $\overline{R}_{\text{sec},x_p}$, with higher values of $\overline{R}_{\text{sec},x_p}$ achieved when $\alpha p > 0.5$. Additionally, a reduction in $m_{st,pr}$ leads to a slight decrease in $\overline{R}_{\text{sec},x_p}$. Conversely, a reduction in $m_{sr,pr}$ results in a slight increase in $\overline{R}_{\text{sec},x_p}$. Notably, an increase in $\Omega_{st,pr}$ to 2 causes a noticeable rise in $\overline{R}_{\text{sec},x_p}$, while a similar increase in $\Omega_{sr,pr}$ results in a significant decrease. This effect can be attributed to the channel between SR and PR acting as a jamming channel, which introduces interference at the primary receiving end.

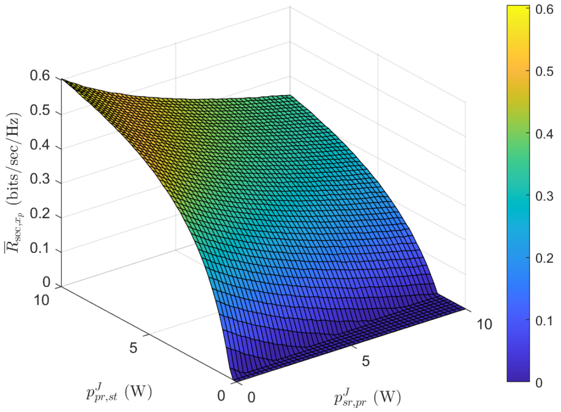

Fig. 4. ESR for the primary network versus $p^J_{sr,pr}$ and $p^J_{pr,st}$.

The surface plot in Fig. 4 demonstrates the effect of CADP-CJ on $\overline{R}_{\text{sec},x_p}$. This figure confirms that $\overline{R}_{\text{sec},x_p} = 0$ for the first benchmark scheme, where no jamming occurs, meaning both $p^J_{sr,pr}$ and $p^J_{pr,st}$ are set to zero. A notable impact of $p^J_{pr,st}$ on $\overline{R}_{\text{sec},x_p}$ is observed. The maximum $\overline{R}_{\text{sec},x_p}$ is attained when $p^J_{pr,st}$ is 10 W. Conversely, $p^J_{sr,pr}$ is found to have a negative effect on $\overline{R}_{\text{sec},x_p}$. This is because the jamming signal sent from the SR to the PR is interpreted as interference during the decoding of x_p. Notably, positive secrecy is not achieved until $p^J_{pr,st}$ reaches 1.6 W when $p^J_{sr,pr}$ is at 10 W. When both $p^J_{sr,pr}$ and $p^J_{pr,st}$ are set to 10 W, the primary network achieves an ESR of 0.345 bits/sec/Hz.

The analysis of the ESR for the secondary network is presented in Figs. 5 and 6. Fig. 5 highlights the effects of varying p_{st} and channel parameters on $\overline{R}_{\text{sec},x_s}$. It is clear that $\overline{R}_{\text{sec},x_s}$ significantly improves with an increase in p_{st}. Moreover, stronger ST-SR and SR-PR links contribute positively to $\overline{R}_{\text{sec},x_s}$, in contrast to the negative impact of a stronger ST-PR link. The influence of the ST-PR link on $\overline{\hat{R}}_{\text{sec},x_s}$ is notably more pronounced than other links. The maximum

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2025.3606837

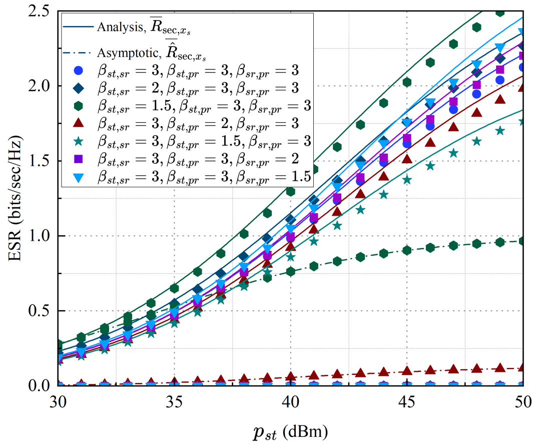

Fig. 5. ESR for the secondary network versus p_{st}.

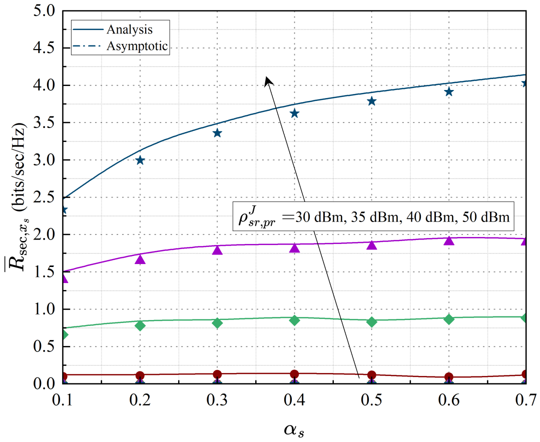

Fig. 6. ESR for the secondary network versus α_s.

$\hat{\overline{R}}_{\mathrm{sec},x_s}$, reaching 0.97 bits/sec/Hz, occurs at $p_{st} = 50$ dBm and $\Omega_{st,pr} = 2$. Additionally, Fig. 6 explores the impact of α_s and $p^J_{sr,pr}$. A substantial improvement in $\overline{R}_{\mathrm{sec},x_s}$ is observed with higher $p^J_{sr,pr}$ levels, underscoring the effectiveness of the CADP-CJ strategy. It's noteworthy that $\hat{\overline{R}}_{\mathrm{sec},x_s}$ approaches nearly zero at $p^J_{sr,pr} = 30$ dBm. While $\hat{\overline{R}}_{\mathrm{sec},x_s}$ enhances with an increase in α_s, this improvement tends to plateau for $\alpha s > 0.4$. Furthermore, we can gain insights into the optimal jamming powers from Figs. 4 and 6, considering the trade-offs in ESRs based on their dependency on jamming powers. While $p^J_{pr,st}$ has little to no effect on $\hat{\overline{R}}_{\mathrm{sec},x_s}$, it significantly positively affects $\hat{\overline{R}}_{\mathrm{sec},x_p}$. Conversely, although $p^J_{sr,pr}$ can be significantly increased, it negatively impacts $\hat{\overline{R}}_{\mathrm{sec},x_p}$. To strike a balance in choosing the optimal jamming powers, we can preserve the primary network's QoS. For instance, if we aim for $\overline{R}_\tau = 0.4$ bits/sec/Hz, we can set $p^J_{pr,st} = 40$ dBm and $p^J_{sr,pr} = 34.8$ dBm to maintain $\overline{R}_\tau$. By doing so, we can optimally achieve an approximate $\hat{\overline{R}}_{\mathrm{sec},x_p} = 1.6$ bits/sec/Hz.

Moreover, Fig. 7 illustrates the comparison of ESR between our proposed scheme and the second benchmark OMA-based scheme. It is evident that our proposed scheme surpasses the OMA-based scheme in terms of ESR for both primary and secondary networks. This superiority primarily stems from our scheme's ability to allocate full bandwidth to users, albeit with a minor reduction in transmit power, as opposed to the bandwidth segmentation characteristic of the OMA scheme. In both networks, the OMA-based scheme demonstrates a marginally higher ESR at low p_{st}s, a detail highlighted in the zoomed-in section of Fig. 7. This slight advantage is attributed to the lower power transmission by the ST at smaller p_{st} values, which impacts the ESR. However, in the primary network, a significant improvement in ESR is observed when $p_{st} > 32$ dBm for $p^J_{sr,pr} = 40$ dBm, and when $p_{st} > 38$ dBm for $p^J_{sr,pr} = 50$ dBm. Similarly, for the secondary network, a notable enhancement in ESR is seen when $p_{st} > 37$ dBm for $p^J_{sr,pr} = 40$ dBm, and for $p_{st} > 38$ dBm for $p^J_{sr,pr} = 50$ dBm, respectively. Especially, at $p^J_{pr,st} = p^J_{sr,pr} = 50$ dBm, the primary and secondary networks achieve an approximate improvement of 86% and 64%.

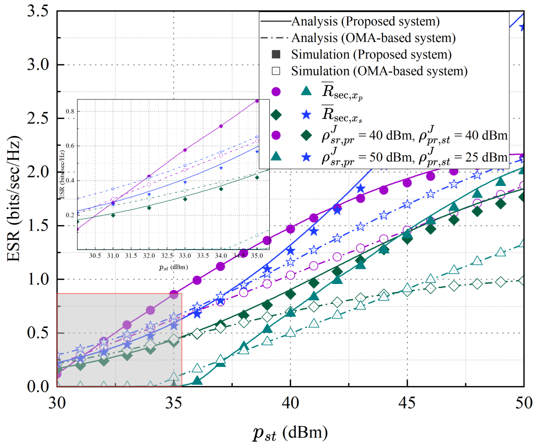

Fig. 7. ESR comparison between the proposed system and the OMA-based system.

To determine the ESR in the multiple-user case, we set the channel parameters as follows: $\Omega_{pt,st} = \Omega_{pr,st} = \Omega_{st,sr} = \Omega_{sr,pr_b} = 2$, $\Omega_{st,pr} = 1$, and $\sigma^2_{st} = \sigma^2_{pr} = \sigma^2_{sr} = 30$ dBm. We employed a one-dimensional increment to generate the channel variables for the ST-SR links. The power allocation is performed based on Algorithm 1, where η is set to 0.7. Fig. 8 illustrates the ESR for both primary and secondary networks in scenarios involving multiple SRs. The results were obtained by incrementing n to 100 and considering $p^J_{sr_b,pr}$ at 40 and 50 dBm. $\overline{R}_{\mathrm{sec},x_p(m)}$ was determined with p_{pt} set to 40 dBm and p_{st} to 50 dBm. It is observed that as α_p decreases with an increasing n, $\overline{R}_{\mathrm{sec},x_p(m)}$ declines drastically. The highest $\overline{R}_{\mathrm{sec},x_p(m)}$ is achieved at $n = 1$ and $p^J_{sr_b,pr} = 40$ dBm. Conversely, the ESR for the secondary network is analyzed for the n^{th}, $(n-5)^{th}$, and $(n-15)^{th}$ users. In all cases, $\overline{R}_{\mathrm{sec},x_{s,n}}$ is highest due to the largest power allocation. However, as n increases, there is a significant decrease in ESR. Nonetheless, positive secrecy is maintained in every scenario. According to the proposed algorithm, the decrease in ESR stabilizes for $n > 15$. All three SRs achieve an ESR of approximately 0.05 bits/sec/Hz when $n = 100$. The data suggests that the ESR can be notably enhanced by increasing $p^J_{sr_b,pr}$, as demonstrated in Fig. 8.

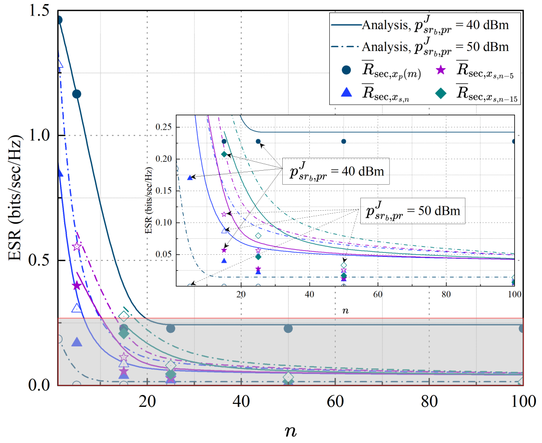

Fig. 8. ESR vs n in the case of multiple SRs.

It is worth noting that the proposed CADP-CJ scheme is designed for low-complexity implementation. The power allocation strategy in Algorithm 1 involves a linear scan over secondary users. This results in an overall computational complexity of $\mathcal{O}(n)$, where n is the number of SRs. Additionally, the reverse SIC and jamming phases are statically structured, and all channel-aware operations rely on closed-form expressions evaluated using the available CSI. As such, the scheme does not require convex solvers or convergence loops, which makes it well-suited for real-time execution in resource-constrained environments, including UAV-assisted cognitive networks.

VII. Conclusions

In this paper, we introduce privacy designs for a NOMA-based purely antagonistic overlay cognitive network, utilizing a UAV as a DF relay. We addressed two primary system-wide privacy challenges and proposed a CADP-CJ strategy to improve the data privacy of both primary and secondary users. Additionally, we integrated reverse SIC and a dynamic top-down power allocation approach into our privacy framework. We derived closed-form expressions for the ESR and AESR for both primary and secondary networks applying Taylor-McLaurin expansions and Gaussian-Chebyshev quadrature, under the assumption that all channels experience Nakagami-m fading in both single and multiple-user scenarios. The precision of our analysis was confirmed through Monte-Carlo simulations, which demonstrated that our proposed system consistently achieves a positive ESR. We further explored the influence of various channel fading parameters on the ESR and AESR and provided insights about optimal jamming power. Our findings indicate that the ESR is predominantly impacted by the channel's second moment, whereas the AESR is significantly affected by all channel parameters except for the jamming channel. Comparative analyses revealed that our proposed system outperforms benchmark strategies. Notably, while the ESR was marginally lower compared to the OMA-based scheme, it showed substantial improvement at higher transmit powers.

We intend to extend this work by considering designing CADP-CJ under partial or outdated CSI scenarios and including additional performance metrics such as secrecy outage probability and energy efficiency. In addition, our extension plan includes a multi-primary and multi-secondary transmitter-receiver scenario, where coordination among STs may be critical for maintaining secrecy. Future work will also include energy-aware secure communication strategies, considering energy harvesting and dynamic power management. Additionally, we plan to investigate hybrid relaying schemes that adaptively switch between DF and AF modes based on energy availability, which potentially offers an effective trade-off between security performance and energy efficiency. Finally, an important extension of this work is to consider the CADP-CJ strategy under MIMO configurations. In such systems, we plan to exploit the spatial degrees of freedom for secrecy enhancement via beamforming, null-space projection, and antenna selection.

References

[1] Z. Li, W. Wang, Q. Wu and X. Wang, "Multi-Operator Dynamic Spectrum Sharing for Wireless Communications: A Consortium Blockchain Enabled Framework," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 1, pp. 3-15, Feb. 2023.

[2] Z. Ding, R. Schober and H. V. Poor, "Design of Downlink Hybrid NOMA Transmission," *IEEE Transactions on Wireless Communications*, vol. 23, no. 12, pp. 19587-19602, Dec. 2024.

[3] L. Mai, H. Luo and Q. Zhang, "Integrated Over-the-Air Computation and Non- Orthogonal Multiple Access Communication in Wireless Uplink Systems," *IEEE Transactions on Wireless Communications*, vol. 23, no. 9, pp. 11433-11443, Sept. 2024.

[4] Z. Cao et al., "Artificial Noise Aided Secure Communications for Cooperative NOMA Networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 2, pp. 946-963, Jun. 2022.

[5] V. Kumar, M. F. Flanagan, D. B. Da Costa and L. -N. Tran, "On the Secrecy Rate of Downlink NOMA in Underlay Spectrum Sharing with Imperfect CSI: Invited Paper," in *Proc. International Conference on Telecommunications (ICT)*, London, United Kingdom, Aug. 2021.

[6] Z. Xiang, W. Yang, G. Pan, Y. Cai, Z. Ding and Y. Zou, "An HARQ Assisted Cognitive NOMA Scheme for Secure Transmission With Imperfect SIC," *IEEE Transactions on Communications*, vol. 69, no. 3, pp. 1930-1946, March 2021.

[7] V. Vikas, K. Deka, S. Sharma and A. Rajesh, "ADMM-Based Detector for Large-Scale MIMO Dense Code-Domain NOMA Systems," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 11, pp. 17024-17040, Nov. 2024.

[8] Y. Liu, C. Zhang, J. Hu, J. Chen and K. Yang, "Low-Complexity MIMO-SCMA Detection for LEO Satellite Communications," *IEEE Transactions on Vehicular Technology,* vol. 74, no. 3, pp. 5253-5258, Mar. 2025.

[9] T. Qin, Z. Yang, J. Liang, K. Han and J. Hu, "Receiver Designs for SC-SCMA Systems Over Frequency Selective Channels,," *in proc. IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, Singapore, Singapore, 2024, pp. 1-5.

[10] X. Liu, K. -Y. Lam, F. Li, J. Zhao, L. Wang, and T. S. Durrani, "Spectrum Sharing for 6G Integrated Satellite-Terrestrial Communication Networks Based on NOMA and CR," *IEEE Network*, vol. 35, no. 4, pp. 28-34, Aug. 2021.

[11] M. K. Hasan, X. Xue, S. Yu and M. Song, "Cooperative NOMA-Based Spectrum Leasing with Multiple Secondary Users," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 11, pp. 14543-14558, Jun. 2023.

[12] V. -H. Dang et al., "Throughput Optimization for Noma Energy Harvesting Cognitive Radio With Multi-UAV-Assisted Relaying Under Security Constraints," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 1, pp. 82-98, Feb. 2023.

[13] Z. Na, C. Ji, B. Lin, and N. Zhang, "Joint Optimization of Trajectory and Resource Allocation in Secure UAV Relaying Communications for Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 16284-16296, Sept. 2022.

[14] X. Liu, Y. Yu, F. Li, and T. S. Durrani, "Throughput Maximization for RIS-UAV Relaying Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19569-19574, Oct. 2022.

[15] V. N. Vo et al., "Outage Probability Minimization in Secure NOMA Cognitive Radio Systems With UAV Relay: A Machine Learning Approach," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 2, pp. 435-451, Apr. 2023.

[16] X. Zheng, J. Zhang and G. Pan, "On Secrecy Analysis of Underlay Cognitive UAV-Aided NOMA Systems With TAS/MRC," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22631-22642, Nov. 2022.

[17] R. Sun, B. Yang, Y. Shen, X. Jiang and T. Taleb, "Covertness and Secrecy Study in Untrusted Relay-Assisted D2D Networks," *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 17-30, Jan. 2023.

[18] D. Chen, Y. Cheng, W. Yang, J. Hu and Y. Cai, "Physical Layer Security in Cognitive Untrusted Relay Networks," *IEEE Access*, vol. 6, pp. 7055-7065, Oct. 2018.

[19] Z. Xiang, W. Yang, G. Pan, Y. Cai and X. Sun, "Secure Transmission in Non-Orthogonal Multiple Access Networks With an Untrusted Relay," *IEEE Wireless Communications Letters*, vol. 8, no. 3, pp. 905-908, Jun. 2019.

[20] K. J. K. Liu, A. K. Sadek, W. Su, and A. Kwasinski, *Cooperative communications and networking*, Cambridge University Press, 2009.

[21] Q. Li, R. Q. Hu, Y. Qian, and G. Wu, "Cooperative Communications for Wireless Networks: Techniques and Applications in LTE-Advanced Systems," *IEEE Wireless Communications*, vol. 19, no. 2, p. 22–29, Apr. 2012.

[22] K. Cao, B. Wang, H. Ding, T. Li, J. Tian and F. Gong, "Secure Transmission Designs for NOMA Systems Against Internal and External Eavesdropping," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2930-2943, Mar. 2020.

[23] C. Zhang, F. Jia, Z. Zhang, J. Ge and F. Gong, "Physical Layer Security Designs for 5G NOMA Systems With a Stronger Near-End Internal Eavesdropper," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13005-13017, Nov. 2020.

[24] A. Abushattal, S. Althunibat, M. Qaraqe and H. Arslan, "A Secure Downlink NOMA Scheme Against Unknown Internal Eavesdroppers," *IEEE Wireless Communications Letters*, vol. 10, no. 6, pp. 1281-1285, Jun. 2021.

[25] H. -M. Wang, X. Zhang and J. -C. Jiang, "UAV-Involved Wireless Physical-Layer Secure Communications: Overview and Research Directions," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 32-39, Oct. 2019.

[26] M. K. Hasan, S. Yu and M. Song, "Uplink Secrecy Analysis for UAV-enabled PD-NOMA-based Underlay Spectrum Sharing Networks," *in proc. IEEE Wireless Communications and Networking Conference*, Glasgow, United Kingdom, 2023.

[27] N. Tang, H. Tang, B. Li and X. Yuan, "Cognitive NOMA for UAV-Enabled Secure Communications: Joint 3D Trajectory Design and Power Allocation," *IEEE Access*, vol. 8, pp. 159965-159978, Sept. 2020.

[28] K. Yadav, P. K. Upadhyay, J. M. Moualeu, A. A. F. Osman and P. H. J. Nardelli, "Deep Learning-Based Secrecy Performance of UAV-IRS NOMA Systems With Friendly Jamming," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 4533-4548, 2025.

[29] J. Wang, R. Wang, Z. Zheng, R. Lin, L. Wu and F. Shu, "Physical Layer Security Enhancement in AAV-Assisted Cooperative Jamming for Cognitive Radio Networks: A MAPPO-LSTM Deep Reinforcement Learning Approach," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 3, pp. 4713-4727, Mar. 2025.

[30] T. T. Nguyen, V. T. Hoang, T. T. Huyen Le and X. N. Tran, "Physical Layer Security for UAV-Based Full-Duplex Relay NOMA System," in *proc. International Conference on Advanced Technologies for Communications*, Ha Noi, Vietnam, Nov. 2022.

[31] L. Zhi et al., "Self-powered absorptive reconfigurable intelligent surfaces for securing satellite-terrestrial integrated networks," *China Communications*, vol. 21, no. 9, pp. 276-291, Sept. 2024.

[32] B. Lyu, C. Zhou, S. Gong, D. T. Hoang and Y. -C. Liang, "Robust Secure Transmission for Active RIS Enabled Symbiotic Radio Multicast Communications," *IEEE Transactions on Wireless Communications*, vol. 22, no. 12, pp. 8766-8780, Dec. 2023.

[33] B. Su, W. Yu, H. Liu, A. Chorti and H. V. Poor, "Secure Transmission Design for Cooperative NOMA in the Presence of Internal Eavesdropping," *IEEE Wireless Communications Letters*, vol. 11, no. 5, pp. 878-882, May 2022.

[34] S. Priya Indraganti and S. Vappangi, "Secrecy Performance of Overlay Cognitive Radio Inspired NOMA With Untrusted Secondary User," *IEEE Access*, vol. 12, pp. 194475-194491, 2024.

[35] D. Jiang, Y. Gao, G. Li, N. Sha, X. Bian, and X. Wang, "Enhancing Physical Layer Security of Cooperative Nonorthogonal Multiple Access Networks via Artificial Noise," *Electronics*, vol. 12, no. 10, p. 2224, May 2023.

[36] R. Gao, G. Yan, R. Niu, W. Chang, T. Yan and C. Tang, "A Novel Spectrum Sensing Method for Multiple Unknown Signal Sources Using Frequency Domain Energy Detection and DBSCAN," *IEEE Access*, vol. 13, pp. 76811-76837, 2025.

[37] J. Xie, C. Liu, Y. -C. Liang and J. Fang, "Activity Pattern Aware Spectrum Sensing: A CNN-Based Deep Learning Approach," *IEEE Communications Letters*, vol. 23, no. 6, pp. 1025-1028, Jun. 2019.

[38] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed., San Diego, CA: Academic, 2007.

[39] S. Kusaladharma, W. -P. Zhu and W. Ajib, "Outage Performance and Average Rate for Large-Scale Millimeter-Wave NOMA Networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 2, pp. 1280-1291, Feb. 2020.

[40] S. Al-Ahmadi and H. Yanikomeroglu, "On the Use of High-Order Moment Matching to Approximate the Generalized-k Distribution by a Gamma Distribution," *in proc. IEEE Global Telecommunications Conference*, Honolulu, HI, USA, 2009, pp. 1-6.

Appendix A
Proof of Lemma 1

$F_{\gamma_{pr}^{(x_p)}}(x)$ is expanded using (2) and linearity of integration as follows.

$$\begin{aligned} F_{\gamma_{pr}^{(x_p)}}(x) &= \Pr\left(\gamma_{pr}^{(x_p)} \leqslant x\right) \\ &= \Pr\left(\lambda_{st,pr} \leqslant \frac{x\rho_{sr,pr}^{J}\lambda_{sr,pr} + x}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s}\right) \\ &= \int_0^\infty F_{\lambda_{st,pr}}\left(\frac{xy\rho_{sr,pr}^{J} + x}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s}\right) f_{\lambda_{sr,pr}}(y)\,dy \end{aligned} \tag{46}$$

Considering Nakagami-*m* fading, we can further expand the CDF in (46) as follows,

$$\begin{aligned} F_{\gamma_{pr}^{(x_p)}}(x) = 1 - \sum_{i=0}^{m_{st,pr}-1} \frac{\beta_{st,pr}^{i}\left(\frac{xy\rho_{sr,pr}^{J}+x}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s}\right)^{i}}{i!} \\ \times \exp\left(-\frac{\beta_{st,pr}(xy\rho_{sr,pr}^{J} + x)}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s}\right). \end{aligned} \tag{47}$$

By substituting the expansion into (46), we can rewrite $F_{\gamma_{pr}^{(x_p)}}(x) = I_{A_1} - I_{A_2}$, where the integrals are defined as follows.

$$I_{A_1} = \int_0^\infty \frac{\beta_{sr,pr}^{m_{sr,pr}} y^{m_{sr,pr}-1}}{\Gamma\left(m_{sr,pr}\right)} \exp\left(-\beta_{sr,pr}y\right) dy \tag{48}$$

$$\begin{aligned} I_{A_2} = \int_0^\infty \sum_{i=0}^{m_{st,pr}-1} \frac{\beta_{st,pr}^{i}\left(\frac{xy\rho_{sr,pr}^{J}+x}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s}\right)^{i}}{i!} \\ \times \exp\left(-\frac{\beta_{st,pr}(xy\rho_{sr,pr}^{J} + x)}{\rho_{st,pr}\alpha_p - x\rho_{st,pr}\alpha_s}\right) \\ \times \frac{\beta_{sr,pr}^{m_{sr,pr}} y^{m_{sr,pr}-1}}{\Gamma(m_{sr,pr})} \exp(-\beta_{sr,pr}y)\,dy. \end{aligned} \tag{49}$$

By applying the formula $\int_0^\infty x^{\nu-1}\exp\left(-\mu x\right)dx = \mu^{-\nu}\Gamma\left(\nu\right)$, we can straightforwardly deduce that $I_{A_1} = 1$ [

[38], Eqn. (3.381-4)]. However, to solve I_{A_2} we employ the binomial expansion for the term $\left(y\rho^J_{sr,pr}+1\right)^i$ as follows.

$$\left(y\rho^J_{sr,pr}+1\right)^i=\sum_{i_1=0}^{i}\left(\begin{array}{c} i \\ i_1 \end{array}\right)(y)^{i_1}\left(\rho^J_{sr,pr}\right)^{i_1}. \tag{50}$$

Now, using this expansion and after applying Fubini's theorem, I_{A_2} is updated as follows.

$$\begin{aligned} I_{A_2}=&\sum_{i=0}^{m_{st,pr}-1}\frac{\beta^i_{st,pr}\beta^{m_{sr,pr}}_{sr,pr}x^i(\rho_{st,pr}\alpha_p-x\rho_{st,pr}\alpha_s)^{-i}}{i!\Gamma(m_{sr,pr})}\\ &\times\int_0^\infty y^{m_{sr,pr}-1}\sum_{i_1=0}^{i}\binom{i}{i_1}y^{i_1}(\rho^J_{sr,pr})^{i_1}\\ &\times\exp\left(-y\left(\frac{x\beta_{st,pr}\rho^J_{sr,pr}}{\rho_{st,pr}\alpha_p-x\rho_{st,pr}\alpha_s}+\beta_{sr,pr}\right)\right)\\ &\times\exp\left(-\frac{\beta_{st,pr}x}{\rho_{st,pr}\alpha_p-x\rho_{st,pr}\alpha_s}\right)dy, \end{aligned} \tag{51}$$

where the governing integral can be solved using [[38], Eqn. (3.381-4)] as follows.

$$\begin{aligned} &\int_0^\infty y^{m_{sr,pr}+i_1-1}\exp\left(-y\left(\frac{x\beta_{st,pr}\rho^J_{sr,pr}}{\rho_{st,pr}\alpha_p-x\rho_{st,pr}\alpha_s}\right.\right.\\ &\quad\left.\left.+\beta_{sr,pr}\right)\right)dy\\ &=\left(\frac{x\beta_{st,pr}\rho^J_{sr,pr}}{\rho_{st,pr}\alpha_p-x\rho_{st,pr}\alpha_s}+\beta_{sr,pr}\right)^{-(m_{sr,pr}+i_1)}\\ &\quad\times\Gamma\left(m_{sr,pr}+i_1\right), \end{aligned} \tag{52}$$

Now, by substituting the solutions of both I_{A_1} and I_{A_2} into (48), we obtain the closed form of $F_{\gamma^{(xp)}_{pr}}(x)$. Therefore, (8) is proved.

Appendix B
Proof of Lemma 2

With the help of (1) The CDF $F_{\gamma^{(xp)}_{st}}(x)$ is defined as

$$F_{\gamma^{(xp)}_{st}}(x)=\int_0^\infty F_{\lambda_{pt,st}}\left(\frac{x\rho^J_{pr,st}y+x}{\rho_{pt}}\right)f_{\lambda_{pr,st}}(y)dy \tag{53}$$

Using (6), $F_{\gamma^{(xp)}_{st}}(x)$ is eventually given by

$$F_{\gamma^{(xp)}_{st}}(x)=\underbrace{\int_0^\infty\frac{\beta^{m_{pr,st}}_{pr,st}y^{m_{pr,st}-1}}{\Gamma\left(m_{pr,st}\right)}\exp\left(-\beta_{pr,st}y\right)dy}_{I_{B_1}} \tag{54}$$

$$\begin{aligned} &-\underbrace{\int_0^\infty\sum_{i=0}^{m_{pt,st}-1}\frac{\beta^i_{pt,st}\left(\frac{x\rho^J_{pr,st}y+x}{\rho_{pt}}\right)^i}{i!}\times\exp\left(-\frac{\beta_{pt,st}\left(x\rho^J_{pr,st}y+x\right)}{\rho_{pt}}\right)\times\frac{\beta^{m_{pr,st}}_{pr,st}y^{m_{pr,st}-1}}{\Gamma\left(m_{pr,st}\right)}\exp\left(-\beta_{pr,st}y\right)dy}_{I_{B_2}} \end{aligned} \tag{55}$$

Herein, $I_{B_1}=1$, which is solved using the formula $\int_0^\infty x^{\nu-1}\exp\left(-\mu x\right)dx=\mu^{-\nu}\Gamma\left(\nu\right)$. Furthermore, I_{B_2} can be rewritten after some mathematical manipulation as

$$\begin{aligned} I_{B_2}=&\sum_{i=0}^{m_{pt,st}-1}\frac{\beta^i_{pt,st}\beta^{m_{pr,st}}_{pr,st}x^i(\rho^J_{pr,st})^{i_1}}{\rho^i_{pt}i!\Gamma(m_{pr,st})}\\ &\times\int_0^\infty\sum_{i_1=0}^{i}\binom{i}{i_1}y^{m_{pr,st}+i_1-1}\\ &\times\exp\left(-\frac{\beta_{pt,st}x(\rho^J_{pr,st}y+1)}{\rho_{pt}}-\beta_{pr,st}y\right)dy\\ =&\sum_{i=0}^{m_{pt,st}-1}\sum_{i_1=0}^{i}\binom{i}{i_1}\frac{\beta^i_{pt,st}\beta^{m_{pr,st}}_{pr,st}x^i(\rho^J_{pr,st})^{i_1}}{\rho^i_{pt}i!\Gamma(m_{pr,st})}\\ &\times\exp\left(-\frac{\beta_{pt,st}x}{\rho_{pt}}\right)\left(\frac{\beta_{pt,st}x\rho^J_{pr,st}}{\rho_{pt}}+\beta_{pr,st}\right)^{-(m_{pr,st}+i_1)}\\ &\times\Gamma(m_{pr,st}+i_1). \end{aligned} \tag{56}$$

Subsequently, by inserting the solutions for I_{B_1} and I_{B_2} into (55), we deduce the closed-form expression for $F_{\gamma^{(xp)}_{st}}(x)$, which is presented in (15).

Dr. Moh Khalid Hasan is an Assistant Professor in the Department of Computer Science at James Madison University. He received his Ph.D. degree in Electrical and Electronics Engineering from Stevens Institute of Technology in August 2025. His current research interests include cognitive radio, wireless security, autonomous UAV networks, machine learning, and 6G. Dr. Hasan was awarded the Doctoral Fellowship from Stevens and the Academic Excellence Award from Kookmin University in 2019.

Dr. Shucheng Yu is an Associate Professor of the Graduate Computer Science and Engineering Department at Yeshiva University. His research interests include data security, trustworthy AI, IoT security, applied cryptography, and wireless networking. He is the recipient of the Test of Time Paper Award of IEEE Infocom 2020. He has frequently served on editorial boards or organizing committees for international journals/conferences. He is an IEEE Fellow.

Dr. Min Song is a Professor and Chair in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. Before joining Stevens, he was the David House Professor and Chair of the Computer Science Department at Michigan Tech. Before joining Michigan Tech, Dr. Song served as an NSF Program Director. His research interests include radio spectrum management, cyber-physical systems, machine learning, and wireless communication networks.