

Jammer Selection for Energy Harvesting-aided Non-Orthogonal Multiple Access: Performance Analysis


Khuong Ho-Van (✉ hvkhuong@hcmut.edu.vn)
Ho Chi Minh City University of Technology

Research Article

Keywords: Performance analysis, non-orthogonal multiple access, jammer selection, nonlinear energy harvesting

Posted Date: June 7th, 2023

DOI: <https://doi.org/10.21203/rs.3.rs-3010011/v1>

License:  This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Peer-to-Peer Networking and Applications on August 18th, 2023. See the published version at <https://doi.org/10.1007/s12083-023-01542-5>.

Jammer Selection for Energy Harvesting-aided Non-Orthogonal Multiple Access: Performance Analysis

Khuong Ho-Van

Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam

Email: hvkhuong@hcmut.edu.vn

Abstract

Energy harvesting-aided non-orthogonal multiple access (NOMA) meets critical requirements of modern wireless networks in terms of spectral efficiency, communication reliability, and energy efficiency. However, information security for it has not received greatly attentions from both industry and academia. This paper proposes jammer selection to meliorate its security performance. To promptly assess the efficacy of the proposed jammer selection, we propose explicit formulas of connection/secretcy throughput and outage probability for both far and near users accounting for non-linear feature of energy harvesters. These formulas are corroborated by Monte-Carlo simulations and quickly generate innumerable results to reveal a significant/slight influence of energy harvesting nonlinearity on communications reliability/information security. In addition, there exist limits on target data/secretcy rates to avoid complete connection outage (i.e. connection outage probability is one) and achieve complete security (i.e. secretcy outage probability is one). Additionally, the proposed (NOMA-and-proposed jammer selection) scheme significantly outperforms its counterparts (NOMA-and-random jammer selection and orthogonal multiple access-and-proposed jammer selection) in terms of both security and reliability. Nevertheless, there is a trade-off between reliability and security. Notably, the proposed scheme obtains optimum security/reliability performance with proper selection of time/power splitting coefficient.

Index Terms

Performance analysis; non-orthogonal multiple access; jammer selection; nonlinear energy harvesting.

I. INTRODUCTION

A. Backgrounds

Modern wireless networks, namely Fifth/Sixth Generation (5G/6G), offer various wireless services for a tremendous quantity of users. Nevertheless, such massive services and a huge quantity of users impose enormous burden on communications infrastructure, particularly in current circumstance of spectrum scarcity and energy deficiency, in accommodating power and bandwidth sufficiently for such users [1]–[3]. Further, securing transmissions for a vast quantity of users in 5G/6G networks against eavesdroppers faces up to severe challenges [4]. Consequently, solutions meliorating security-and-reliability performances and spectral-and-energy efficiencies become more and more principal.

One of feasible solutions to meliorate spectral efficiency is non-orthogonal multiple access (NOMA) that is proposed for beyond 5G networks [5]–[7]. NOMA can be implemented by distributing distinct power levels to different users. Relied on distinct power levels, NOMA can decode user information with successive interference cancellation, which promises to improve reliability performance further. Additionally, energy efficiency can be enhanced with harvesting radio frequency (RF) energy inherently available in wireless signals surrounding RF transmitters. Currently, cheap energy harvesting (EH) circuits are integrated successfully in 5G/6G users [8]–[10]. Nonetheless, EH has been modelled to be linear for tractability in most performance analyses [11]–[14]. Realistically, EH circuits are composed of nonlinear components such as transistors, inductors, capacitors. Therefore, modelling EH should take nonlinearity of circuit components into account. So far, the literature (e.g. [7], [15]–[20]) has proposed various nonlinear energy harvesting (NLEH) models. Further, physical layer security (PLS) that makes use of propagation natures of wireless channels has proved to be an efficient solution to ameliorate security performance [21]–[25]. Consequently, PLS for EH-aided NOMA has attracted considerable interests from both industry and academia in order to meet concurrently principal demands of high security-and-security performances and energy-and-spectral efficiencies for next generation wireless networks. One of efficient PLS techniques to warrant secure transmission is jamming, which impairs purposely the wire-tapping of eavesdroppers but not harm transmissions of desired users [26], [27].

Jammer selection for EH-aided NOMA (JSEHNOMA), e.g. Figure 1, offers concurrent communications from the NOMA transmitter (S) to two NOMA receivers (N and F) for high spectral

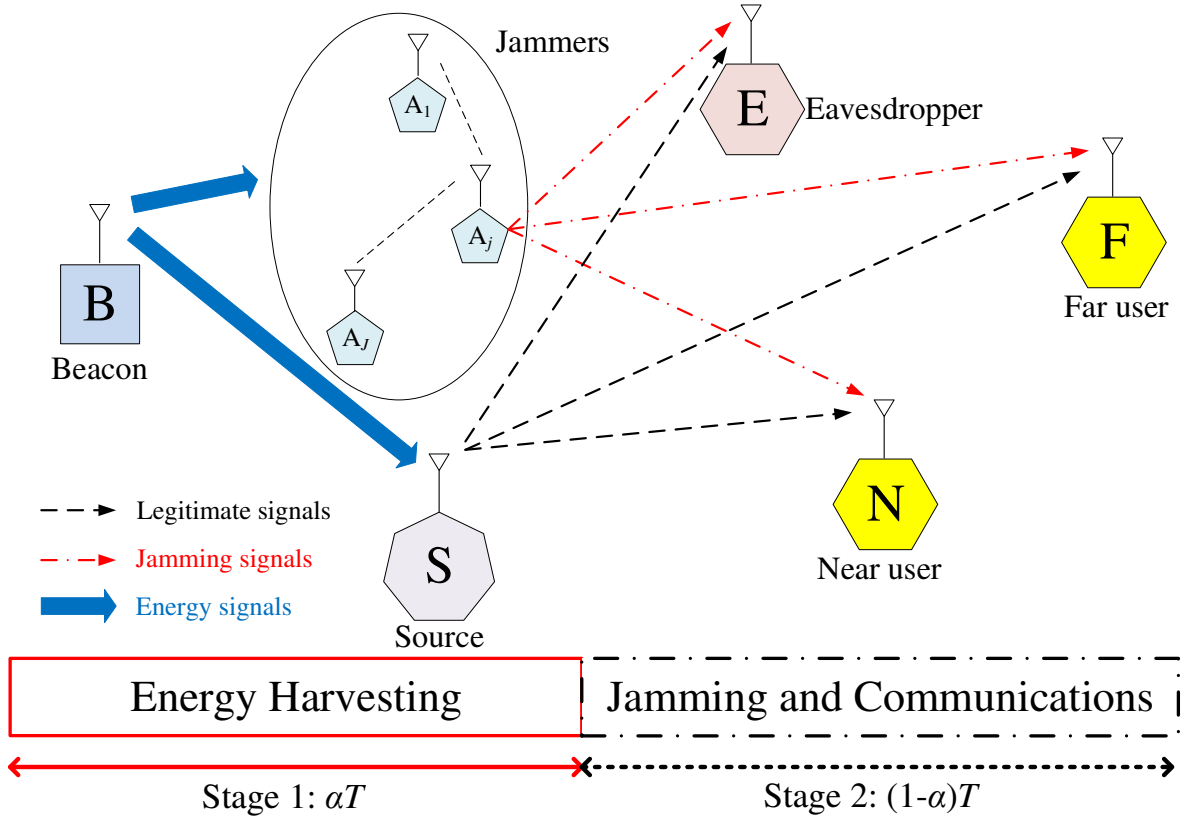


Fig. 1: Jammer selection in EH-aided NOMA

efficiency whilst the jammer A_j selected from a group of J jammers interrupts the wire-tapping of the eavesdropper (E) for high security performance. S and A_j self-power their operations by scavenging energy from a power beacon (B) which can be radio/television broadcasting stations having stable and high transmit power to improve the energy efficiency. Briefly, JSEHNOMA unveils advantages of high reliability-and-security performances and spectral-and-energy efficiencies. Accordingly, the performance analysis of JSEHNOMA, especially in the realistic scenario of NLEH, is crucial to verify whether JSEHNOMA attains such advantages. Our pioneering work proposes such security/reliability analyses.

B. Previous works

Uplink communications in EH-aided NOMA (UcEHNOMA) was researched in [7] in which numerous NOMA users, who send their data to the same receiver (S), experience two stages as demonstrated in Figure 1. NOMA users scavenge RF energy from a stable power beacon (B) with

nonlinear energy harvesters in Stage 1 whilst they send data to S with scavenged energy in Stage 2. Moreover, [7] optimized duration of each stage. Notwithstanding, [7] did not analyze average secrecy outage probability (SOP) in closed-form. A special case of [7] with two NOMA users was investigated in [28] which proposed countermeasures to maximize the energy efficiency and implement user grouping for NLEH. Additionally, [28] analyzed connection outage probability (COP) but only in approximated-form.

The works in [29]–[31] studied downlink communications in EH-aided NOMA (DcEHNOMA) where S sends NOMA signals simultaneously to two NOMA users (N and F). Subsequently, [32] extended [29]–[31] to the context of multiple NOMA users. The COP and connection throughput (CTP) formulas in approximated-form were proposed in [29]–[32]. Moreover, [32] proposed a solution to the sum-rate maximization problem. Notwithstanding, S scavenges RF energy from a NOMA user with linear energy harvester (LEH) that is not realistic [29], [30], [32]. Furthermore, F harvests RF energy from S with NLEH yet what harvested energy is for was not explained explicitly in [31]. Additionally, [31] proposed three distinct communications modes with divergent utilization degrees of feedback information.

DcEHNOMA with two NOMA users (N and F) was studied where communications to F is aided by N in [33]–[37] or by a relay in [38]–[40], who harvests energy from a NOMA sender. [33] and [40] presented the approximated COP analysis for NLEH at the relay. In the meantime, [38] found a solution to the sum-rate maximization problem for LEH while [35] and [36] maximized data rate of F and optimized both the energy efficiency and the total transmit power for NLEH, correspondingly. [41] and [42] extended [40] to a multiplicity of relays and proposed the relay selection to support NOMA communications from S to both N and F. Additionally, [43] extended [40] by employing two relays who exchange their roles to assist F. Moreover, [43] presented the average CTP yet not in closed-form. In lieu of utilizing several relays as in [41] and [42], the authors in [44] take advantage of multiple near NOMA users and proposed to adopt merely one near NOMA user to assist the far NOMA user. [45] and [46] continues expanding [40] by studying several NOMA receivers. Notwithstanding, [34], [37], [39], [41]–[46] researched LEH in performance analysis. As an alternative countermeasure, intelligent reflecting surface was employed to substitute the relay in forwarding data from S to N and F [47]–[49]. The sum-rate (or throughput) was maximized for NLEH in [47] and LEH in [48] and [49], correspondingly. Nevertheless, [35], [36], [38], [47]–[49] did not analyze the system performance.

In summary, the previous works relevant for performance analysis for EH-aided NOMA in [7], [28]–[34], [37], [39]–[46] researched a trivial system model in which jamming was not exploited for enhanced security performance in [7] and the security problem was ignored in [28]–[34], [37], [39]–[46]. Thence, the security/reliability analyses for the system model in Figure 1, which takes NLEH into account, have not been researched in the current literature. This paper pioneers in proposing such analyses which are useful in assessing quickly and optimizing the security/reliability performances before realistic implementation.

C. Contributions

We contribute the following:

- We propose JSEHNOMA in Figure 1 to ameliorate the security/reliability performances and the spectral-and-energy efficiencies. Moreover, we propose the deployment of the extensively-accepted NLEH model in [16] at S and A_j to characterize appropriately non-linear circuit components in energy scavengers.
- We propose the CTP/secrecy throughput (STP) and the SOP/COP analyses for the proposed JSEHNOMA, which takes NLEH into account, to evaluate the reliability/security performances quickly.
- We estimate and optimize the security/reliability performances in different realistic settings. Multifarious results reveal that EH nonlinearity impacts drastically the reliability performance yet slightly the security performance. Additionally, the target data/secrecy rates are limited to prevent complete connection outage (i.e. the COP is one) and attain the complete security (i.e. the SOP is one). Further, the proposed (NOMA-and-proposed jammer selection) scheme drastically outperforms two reference schemes (NOMA-and-random jammer selection and orthogonal multiple access (OMA)-and-proposed jammer selection) in terms of both the security and the reliability. Nonetheless, there is a trade-off between the reliability and the security. Notably, the proposed scheme attains optimum security/reliability performance with proper selection of time/power splitting coefficient.

D. Organization

Section II describes the proposed JSEHNOMA. Next, Section III presents the COP/SOP/CTP/STP analyses. Then, Section IV provides analytical/simulated results in divergent realistic settings. Ultimately, Section V closes the paper. Table I tabulates frequently-used notations.

TABLE I: Frequently-used notations

Notation	Meaning
Δ_v	Connection Outage Probability (COP)
$\bar{F}_V(\cdot)$	Complementary Cumulative Distribution Function (CCDF) of V
$\mathcal{E}\{\cdot\}$	Expectation operator
$\mathcal{N}(0, \varkappa)$	Zero-mean and \varkappa -variance complex Gaussian random variable
$\Pr\{\cdot\}$	Probability operator
$\mathbf{C}_n^m = \frac{n!}{m!(n-m)!}$	Binomial coefficient
T	Transmission block time
J	Number of jammers
Υ_v	Secrecy Outage Probability (SOP)
g_{kl}	Channel gain
h_{kl}	Channel coefficient
φ_{kl}	Fading power
χ	Power saturation threshold
P_u	Transmit power
E_u	Harvested energy
α	Time splitting coefficient
β	Energy converting efficiency
$f_V(\cdot)$	Probability Density Function (PDF) of V
P	Transmit power of beacon
δ	Power splitting coefficient
x_v	Transmit information
y_v	Received signal
ε_v	Additive noise
R_b	Target data rate
R_s	Target secrecy rate
\mathbb{T}_v	Connection Throughput (CTP)
\mathbb{S}_v	Secrecy Throughput (STP)
$F_V(\cdot)$	Cumulative Distribution Function (CDF) of V

II. JAMMER SELECTION FOR EH-AIDED NOMA

Figure 1 shows the proposed system model of JSEHNOMA¹ with B, S, N, F, E and A_j , $j = 1, \dots, J$. Such a JSEHNOMA can stand for downlink communications in mobile com-

¹We study NOMA for each cluster of two users owing to the extensively-acknowledged reality that accreting a quantity of users in each cluster is complex and inefficient [50], [51]. Additionally, the two-user NOMA case was recommended for the 3GPP-LTE-A [52], [53]. Notwithstanding, how to cluster two users is outside the scope of our work (please refer to [6], [28], [35], [41], [54] for deep comprehension on NOMA user grouping).

munications networks. As energy-constrained users, S and A_j self-power their operations by scavenging energy from B which may be an available power beacon (e.g. radio broadcasting stations, television broadcasting stations). For the proposed JSEHNOMA, B transfers energy to S and A_j in a time fraction α of transmission block T , viz. Stage 1, while S implements NOMA downlink communications to N and F and the selected jammer A_j among J jammers jams the eavesdropping of E in the remaining of T , viz. Stage 2.

We denote g_{bs} , g_{sn} , g_{sf} , and g_{se} as channel gains between B and S, S and N, S and F, S and E, respectively whilst g_{bj} , g_{jn} , g_{jf} , g_{je} as channel gains between B and A_j , A_j and N, A_j and F, A_j and E, correspondingly. We also suppose flat block Rayleigh fading channels. Therefore, g_{kl} with $kl = \{bs, sn, sf, se, bj, jn, jf, je\}$ is exponentially distributed with the mean of $\varphi_{kl} = \mathcal{E}\{g_{kl}\}$. To account for path loss, φ_{kl} is modelled as $\varepsilon d_{kl}^{-\nu}$ wherein ε is the fading power at the reference distance of 1 meter (m), d_{kl} is the corresponding transmitter-to-receiver distance and ν is the path-loss exponent [18]. Moreover, the PDF, the CDF, and the CCDF of g_{kl} are correspondingly expressed to be $f_{g_{kl}}(a) = e^{-a/\varphi_{kl}}/\varphi_{kl}$, $F_{g_{kl}}(a) = 1 - e^{-a/\varphi_{kl}}$, and $\bar{F}_{g_{kl}}(a) = e^{-a/\varphi_{kl}}$. It is noted that the following denotes $g_{kl} = |h_{kl}|^2$ where h_{kl} is the channel coefficient.

In Stage 1, B transfers energy wirelessly to S and A_j . Consequently, S and A_j accumulate the amount of energy as $E_u = \alpha T \beta P g_{bu}$ where P is the power of B and $\beta \in (0, 1)$ represents the energy converting efficiency; $u = \{s, j\}$. Since Stage 2 lasts $(1 - \alpha)T$, the power for communications in Stage 2 transformed from E_u is $\frac{E_u}{(1-\alpha)T}$. In accordance with NLEH in [16], the power of S and A_j consumed in Stage 2 is

$$P_u = \begin{cases} \frac{\beta\alpha P}{1-\alpha} g_{bu} & , \alpha P g_{bu} \leq \chi \\ \frac{\beta\alpha\chi}{1-\alpha} & , \alpha P g_{bu} > \chi \end{cases} = \begin{cases} A g_{bu} & , g_{bu} \leq B \\ C & , g_{bu} > B \end{cases} \quad (1)$$

where $A = \frac{\beta\alpha P}{1-\alpha}$, $C = \frac{\beta\alpha\chi}{1-\alpha}$, $B = \frac{\chi}{\alpha P}$, and χ is the power saturation threshold.

It is worth noticing that NLEH is evidently featured by (1). To be more specific, NLEH outputs the power of $A g_{bu}$, which is proportional linearly to the input power as it subceeds χ ; otherwise, its output power is saturated at χ . Additionally, NLEH reduces to LEH as χ is large ($\chi \rightarrow \infty$).

In Stage 2, the NOMA downlink communications and the jamming operation are executed simultaneously, viz. S sends concurrently the symbols (x_n and x_f) with transmit power P_s in the NOMA representation of $\sqrt{\delta P_s} x_n + \sqrt{(1-\delta) P_s} x_f$ to N and F while the selected jammer, namely A_j , sends the jamming signal x_j to interfere the wire-tapping of E with transmit power P_j where $\mathcal{E}\{|x_n|^2\} = \mathcal{E}\{|x_f|^2\} = \mathcal{E}\{|x_j|^2\} = 1$, x_n and x_f are the desired symbols intended

to N and F, respectively. In agreement with the NOMA mechanism, N is allocated less power than F and thence, $\delta < 0.5$. Consequently, $\{N, F, E\}$ receives the signal to be

$$y_v = h_{sv} \left(\sqrt{\delta P_s} x_n + \sqrt{(1-\delta) P_s} x_f \right) + h_{jv} \sqrt{P_j} x_j + \varepsilon_v, \quad (2)$$

wherein $\varepsilon_v \sim \mathcal{N}(0, \sigma_v)$ is additive noise at v with $v = \{n, f, e\}$.

This paper selects the jammer A_j such that it causes the most interference among all jammers to E. This means the index j is expressed as $j = \max_{i \in [1, J]} g_{ie} P_i$. The selection of A_j can be implemented in numerous ways. For example, each jammer A_i can set its timer independently with the threshold inversely proportional to $g_{ie} P_i$. Then, A_j is the jammer whose timer expires earliest².

1) *Detection at N and F:* Because A_j creates the jamming message x_j to interfere deliberately only E without harming communications of N and F, the desired receivers (N and F) can predict accurately this jamming signal, which can be interpreted as being transmitted through the null space to N and F [55]–[60]. Accordingly, N and F can completely suppress the jamming signal out of y_d , ultimately producing the no-jamming signal as $\tilde{y}_d = h_{sd} \left(\sqrt{\delta P_s} x_n + \sqrt{(1-\delta) P_s} x_f \right) + \varepsilon_d$ with $d = \{n, f\}$.

Conditioned on \tilde{y}_d , N and F detect x_n and x_f in accordance with the NOMA-based detection principle. Because $\delta < 0.5$, N detects x_f first by behaving x_n as the interference. Subsequently, N detects x_f from \tilde{y}_n with signal-to-interference plus noise ratio (SINR) as

$$\Phi_n^f = \frac{(1-\delta) P_s g_{sn}}{g_{sn} \delta P_s + \sigma_n}. \quad (3)$$

By suppressing the interference³ created by x_f , N keeps restoring x_n from $\hat{y}_n = \tilde{y}_n - h_{sn} \sqrt{(1-\delta) P_s} x_f = h_{sn} \sqrt{\delta P_s} x_n + \varepsilon_n$. Consequently, conditioned on \hat{y}_n , N restores x_n with the signal-to-noise ratio (SNR) as

$$\Phi_n^n = \frac{g_{sn} \delta P_s}{\sigma_n}. \quad (4)$$

²Although that all jammers jam E simultaneously generates higher amount of jamming power to secure better the desired communications, the current paper does not consider this scenario. This is because of the increasing complexity. Indeed, in order to cancel all jamming signals from J jammers from the desired signals at N and F, they need to synchronize these jamming signals. As such, the higher J , the more complex the synchronization. Accordingly, the jammer selection proposed in this paper reduces the complexity of the synchronization significantly.

³This paper researches the case that N implements the detection of x_n solely if N has restored x_f accurately. The condition to specify whether N has detected x_f exactly will be presented in the sequel. Consequently, the interference remained after suppressing x_f out of \tilde{y}_n is neglected.

In the meanwhile, F detects x_f by behaving x_n as the interference. Accordingly, F detects x_f directly from \tilde{y}_f with the SINR to be

$$\Phi_f^f = \frac{(1 - \delta) P_s g_{sf}}{g_{sf} \delta P_s + \sigma_f}. \quad (5)$$

2) *Detection at E*: The eavesdropper is blind with the jamming information x_j . Thence, conditioned on (2), E performs the detection of x_n and x_f conforming to the NOMA-based detection principle. Since $\delta < 0.5$, E detects x_f first by behaving x_n as the interference. Subsequently, E detects x_f from $y_e = h_{se} \left(\sqrt{\delta P_s} x_n + \sqrt{(1 - \delta) P_s} x_f \right) + h_{je} \sqrt{P_j} x_j + \varepsilon_e$ with the SINR to be

$$\Phi_e^f = \frac{(1 - \delta) P_s g_{se}}{g_{se} \delta P_s + g_{je} P_j + \sigma_e}. \quad (6)$$

By suppressing the interference induced by x_f , E keeps detecting x_n from $\hat{y}_e = y_e - h_{se} \sqrt{(1 - \delta) P_s} x_f = h_{se} \sqrt{\delta P_s} x_n + h_{je} \sqrt{P_j} x_j + \varepsilon_e$. Accordingly, conforming to \hat{y}_e , E detects x_n with the SINR to be

$$\Phi_e^n = \frac{g_{se} \delta P_s}{g_{je} P_j + \sigma_e}. \quad (7)$$

One sees from (6)-(7) that A_j impairs E by the quantity of jamming power to be $g_{je} P_j$, which drastically mitigates the probability of successful detection of x_n and x_f at E and thence, ameliorating dramatically the security performance.

III. PERFORMANCE ANALYSIS FOR JSEHNOMA

At first, this section analyzes the COP/SOP of JSEHNOMA. The COP is determined as the possibility that the achieved channel capacity at the desired receiver subceeds the target data rate R_b . In the meantime, the SOP is determined as the likelihood that the obtained channel capacity at the eavesdropper subceeds the redundant secrecy rate $(R_b - R_s)$ reserved against eavesdropping where R_s is the target secrecy rate. Therefore, the COP/SOP represents the reliability/security of information transmission. Subsequently, the proposed COP/SOP analyses are extended to the CTP/STP analyses. Those analyses facilitate the quick COP/SOP/CTP/STP evaluation without exhaustive simulations.

A. Reliability analysis

The reliability performance is characterized by the COP at N and F. As a result, the lower the COP at N and F, the higher the reliability performance.

1) *The COP at F*: The COP at F is represented as

$$\Delta_f = \Pr \left\{ (1 - \alpha) \log_2 \left(1 + \Phi_f^f \right) \leq R_b \right\} = \Pr \left\{ \Phi_f^f \leq \Phi_b \right\}, \quad (8)$$

where $\Phi_b = 2^{R_b/(1-\alpha)} - 1$. The factor of $(1 - \alpha)$ before the logarithm in (8) is because Stage 2 lasts $(1 - \alpha)T$.

Invoking Φ_f^f in (5), one obtains

$$\begin{aligned} \Delta_f &= \Pr \left\{ \frac{(1 - \delta) P_s g_{sf}}{g_{sf} \delta P_s + \sigma_f} \leq \Phi_b \right\} \\ &= \begin{cases} \mathcal{B} \left(\frac{\sigma_f \Phi_b}{1 - \delta - \delta \Phi_b}, \varphi_{bs}, \varphi_{sf} \right), & \frac{1 - \delta}{\delta} > \Phi_b \\ 1, & \frac{1 - \delta}{\delta} \leq \Phi_b \end{cases} \end{aligned} \quad (9)$$

where

$$\mathcal{B}(x, \varphi_{bu}, \varphi_{ud}) = \mathcal{E}_{P_u} \left\{ F_{g_{ud}} \left(\frac{x}{P_u} \right) \right\}. \quad (10)$$

Conditioned on P_u in (1), $\mathcal{B}(x, \varphi_{bu}, \varphi_{ud})$ is expressed in closed-form as

$$\begin{aligned} \mathcal{B}(x, \varphi_{bu}, \varphi_{ud}) &= \int_0^B F_{g_{ud}} \left(\frac{x}{Ay} \right) \mathfrak{f}_{g_{bu}}(y) dy + \int_B^\infty F_{g_{ud}} \left(\frac{x}{C} \right) \mathfrak{f}_{g_{bu}}(y) dy \\ &\approx \sum_{m=1}^I \frac{\pi B}{2I} \sqrt{1 - \vartheta_m^2} F_{g_{ud}} \left(\frac{x}{A \zeta_m} \right) \mathfrak{f}_{g_{bu}}(\zeta_m) + F_{g_{ud}} \left(\frac{x}{C} \right) \bar{\mathfrak{F}}_{g_{bu}}(B) \\ &= \sum_{m=1}^I \frac{\pi B}{2I} \sqrt{1 - \vartheta_m^2} \mathfrak{f}_{g_{bu}}(\zeta_m) \left(1 - e^{-\frac{x}{A \zeta_m \varphi_{ud}}} \right) + \left(1 - e^{-\frac{x}{C \varphi_{ud}}} \right) \bar{\mathfrak{F}}_{g_{bu}}(B), \end{aligned} \quad (11)$$

where $\vartheta_m = \cos \left(\frac{2m-1}{2I} \pi \right)$, $\zeta_m = \frac{B}{2} (\vartheta_m + 1)$, and I stands for the complexity-accuracy trade-off of the Gaussian-Chebyshev quadrature in [61] which is used to approximate the first integral in (11). Section IV adopts $I = 50$ which guarantees a very high preciseness.

2) *The COP at N*: Two events cause N to be in a connection outage as follows:

- The first event happens as N decodes x_f unsuccessfully (namely, $(1 - \alpha) \log_2 (1 + \Phi_n^f) \leq R_b$).
- The second event occurs as N decodes x_f successfully (namely, $(1 - \alpha) \log_2 (1 + \Phi_n^f) > R_b$) yet restores x_n unsuccessfully (namely, $(1 - \alpha) \log_2 (1 + \Phi_n^n) \leq R_b$).

In accordance with the total probability law, the COP at N is represented as

$$\begin{aligned} \Delta_n &= \Pr \left\{ (1 - \alpha) \log_2 (1 + \Phi_n^f) \leq R_b \right\} \\ &\quad + \Pr \left\{ (1 - \alpha) \log_2 (1 + \Phi_n^f) > R_b, (1 - \alpha) \log_2 (1 + \Phi_n^n) \leq R_b \right\} \\ &= 1 - \Pr \left\{ \Phi_n^f \geq \Phi_b, \Phi_n^n \geq \Phi_b \right\}. \end{aligned} \quad (12)$$

Invoking Φ_n^f in (3) and Φ_n^n in (4), one obtains

$$\begin{aligned}
\Delta_n &= 1 - \Pr \left\{ \frac{(1-\delta)P_s g_{sn}}{g_{sn}\delta P_s + \sigma_n} \geq \Phi_b, \frac{g_{sn}\delta P_s}{\sigma_n} \geq \Phi_b \right\} \\
&= 1 - \Pr \left\{ (1-\delta-\delta\Phi_b)P_s g_{sn} \geq \sigma_n \Phi_b, g_{sn} \geq \frac{\Phi_b \sigma_n}{\delta P_s} \right\} \\
&= \begin{cases} \bar{\Delta}_n & , \frac{1-\delta}{\delta} > \Phi_b \\ 1 & , \frac{1-\delta}{\delta} \leq \Phi_b \end{cases}
\end{aligned} \tag{13}$$

where

$$\begin{aligned}
\bar{\Delta}_n &= 1 - \Pr \left\{ g_{sn} \geq \frac{\sigma_n \Phi_b}{(1-\delta-\delta\Phi_b)P_s}, g_{sn} \geq \frac{\Phi_b \sigma_n}{\delta P_s} \right\} \\
&= 1 - \Pr \left\{ g_{sn} \geq \frac{D}{P_s} \right\} \\
&= \Pr \left\{ g_{sn} < \frac{D}{P_s} \right\} \\
&= \mathcal{B}(D, \varphi_{bs}, \varphi_{sn})
\end{aligned} \tag{14}$$

with $D = \max\left(\frac{\Phi_b \sigma_n}{1-\delta-\delta\Phi_b}, \frac{\Phi_b \sigma_n}{\delta}\right)$.

Remark 1: (9) and (13) indicate that since $\Phi_b = 2^{R_b/(1-\alpha)} - 1$, adopting the combination $\{R_b, \delta, \alpha\}$ leads to $\frac{1-\delta}{\delta} > \Phi_b$ or $\frac{1-\delta}{\delta} \leq \Phi_b$, inducing Δ_f and Δ_n to accept divergent values and finally causing distinct COP degrees for F and N. More specifically, F and N suffer a complete connection outage if $\frac{1-\delta}{\delta} \leq \Phi_b$ (or $R_b \geq -(1-\alpha)\log_2\delta$); otherwise, a complete connection outage does not happen at F and N. This implies that the system designer must set the limit for the target data rate R_b such that $R_b < -(1-\alpha)\log_2\delta$ to prevent the complete connection outage at F and N.

Remark 2: Both Δ_f and Δ_n depend on parameters $(R_b, \alpha, P, \delta, \chi, \beta)$, meaning that N and F can attain the desired reliability by establishing properly these parameters.

3) *Asymptotic reliability analysis:* The following finds the upper-bound on the communications reliability of JSEHNOMA in the regime of high transmit power, namely $P \rightarrow \infty$. It is recalled that NLEH is completely saturated as $P \rightarrow \infty$. Therefore, $P_u \rightarrow C$ as $P \rightarrow \infty$. Following the analysis in Subsections III-A1 and III-A2 yields the COPs at F and N, respectively, as

$$\Delta_f^\infty = \begin{cases} \mathbb{F}_{g_{sf}} \left(\frac{\sigma_f \Phi_b}{[1-\delta-\delta\Phi_b]C} \right) & , \frac{1-\delta}{\delta} > \Phi_b \\ 1 & , \frac{1-\delta}{\delta} \leq \Phi_b \end{cases} \tag{15}$$

and

$$\Delta_n^\infty = \begin{cases} F_{g_{sn}} \left(\frac{D}{C} \right) & , \frac{1-\delta}{\delta} > \Phi_b \\ 1 & , \frac{1-\delta}{\delta} \leq \Phi_b \end{cases} \quad (16)$$

4) *Connection throughput*: For JSEHNOMA with delay-limited communications, the CTPs of N and F are expressed to be

$$\mathbb{T}_n = (1 - \alpha)R_b(1 - \Delta_n) \quad \mathbb{T}_f = (1 - \alpha)R_b(1 - \Delta_f). \quad (17)$$

It is recalled that the higher the CTP, the higher the reliability performance. Moreover, (17) indicates that the CTPs of N and F are also jointly determined by a specification set $(R_b, \alpha, P, \delta, \chi, \beta)$ since this set influences Δ_n and Δ_f . Consequently, the desired CTPs are accomplished by establishing flexibly and properly this set conditioned on its preset value range.

B. Security analysis

The security performance is represented by the SOP at E. Accordingly, the lower the SOP at E, the lower the security performance. Additionally, the SOP at E is defined in the same manner as the COP at N and F. As such, the SOPs of F and N are respectively given by

$$\Upsilon_f = \Pr \left\{ (1 - \alpha) \log_2 (1 + \Phi_e^f) \leq R_b - R_s \right\} = \Pr \left\{ \Phi_e^f \leq \Phi_s \right\}, \quad (18)$$

and

$$\begin{aligned} \Upsilon_n &= \Pr \left\{ (1 - \alpha) \log_2 (1 + \Phi_e^f) \leq R_b - R_s \right\} \\ &+ \Pr \left\{ (1 - \alpha) \log_2 (1 + \Phi_e^f) > R_b - R_s, (1 - \alpha) \log_2 (1 + \Phi_e^n) \leq R_b - R_s \right\} \\ &= 1 - \Pr \left\{ \Phi_e^f \geq \Phi_s, \Phi_e^n \geq \Phi_s \right\}, \end{aligned} \quad (19)$$

where $\Phi_s = 2^{(R_b - R_s)/(1 - \alpha)} - 1$.

1) *Derivation of Υ_f* : Inserting Φ_e^f in (6) into (18), one obtains

$$\Upsilon_f = \Pr \left\{ \frac{(1 - \delta) P_s g_{se}}{g_{se} \delta P_s + g_{je} P_j + \sigma_e} \leq \Phi_s \right\}. \quad (20)$$

Based on the proposed jammer selection, (20) is further simplified as

$$\begin{aligned} \Upsilon_f &= \sum_{j=1}^J \Pr \left\{ \frac{(1 - \delta) q_{se}}{\delta q_{se} + q_{je} + \sigma_e} \leq \Phi_s, A_j \text{ is selected} \right\} \\ &= \sum_{j=1}^J \Pr \left\{ \frac{(1 - \delta) q_{se}}{\delta q_{se} + q_{je} + \sigma_e} \leq \Phi_s, \bigcap_{k \in [1, J] \setminus j} \{q_{je} > q_{ke}\} \right\}, \end{aligned} \quad (21)$$

where $q_{se} = P_s g_{se}$, $q_{ke} = P_k g_{ke}$, and $q_{je} = P_j g_{je}$.

For notation simplicity, we assume that all jammers are close enough in order for average statistics from S to all jammers and from all jammers to E to be identical, i.e. $\varphi_{bj} = \varphi_b$ and $\varphi_{je} = \varphi_e$ for all $j \in [1, J]$. Then, all the terms inside the summation in (21) are also identical and thence,

$$\begin{aligned}
\Upsilon_f &= J \Pr \left\{ \frac{(1-\delta)q_{se}}{\delta q_{se} + q_{je} + \sigma_e} \leq \Phi_s, \bigcap_{k \in [1, J] \setminus j} \{q_{je} > q_{ke}\} \right\} \\
&= J \mathcal{E}_{q_{je}} \left\{ \Pr \left\{ (1-\delta - \Phi_s \delta) q_{se} \leq \Phi_s q_{je} + \Phi_s \sigma_e, \bigcap_{k \in [1, J] \setminus j} \{q_{je} > q_{ke}\} \middle| q_{je} \right\} \right\} \\
&= \begin{cases} J \mathcal{E}_{q_{je}} \left\{ \Pr \left\{ q_{se} \leq \frac{\Phi_s q_{je} + \Phi_s \sigma_e}{1 - \delta - \Phi_s \delta}, \bigcap_{k \in [1, J] \setminus j} \{q_{je} > q_{ke}\} \middle| q_{je} \right\} \right\}, & \frac{1-\delta}{\delta} > \Phi_s \\ J \mathcal{E}_{q_{je}} \left\{ \Pr \left\{ \bigcap_{k \in [1, J] \setminus j} \{q_{je} > q_{ke}\} \middle| q_{je} \right\} \right\}, & \frac{1-\delta}{\delta} \leq \Phi_s \end{cases} \quad (22) \\
&= \begin{cases} J \bar{\Upsilon}_f, & \frac{1-\delta}{\delta} > \Phi_s \\ J \tilde{\Upsilon}_f, & \frac{1-\delta}{\delta} \leq \Phi_s \end{cases}
\end{aligned}$$

where

$$\bar{\Upsilon}_f = \mathcal{E}_{q_{je}} \left\{ \underbrace{\mathbb{F}_{q_{se}} \left(\frac{\Phi_s q_{je} + \Phi_s \sigma_e}{1 - \delta - \Phi_s \delta} \right)}_{\mathcal{L}} \prod_{k \in [1, J] \setminus j} \underbrace{\mathbb{F}_{q_{ke}}(q_{je})}_{\mathcal{G}} \right\}, \quad (23)$$

$$\tilde{\Upsilon}_f = \mathcal{E}_{q_{je}} \{ \mathcal{G} \}. \quad (24)$$

To complete the derivation of (22), one needs the CDF and the PDF of $q_{ue} = P_u g_{ue}$ with $u \in \{s, k, j\}$. Towards this end, we follow the steps in deriving $\mathcal{B}(\cdot, \cdot, \cdot)$ in (11) as

$$\begin{aligned}
\mathbb{F}_{q_{ue}}(x) &= \Pr \{ P_u g_{ue} \leq x \} \\
&= \mathcal{E}_{P_u} \left\{ \mathbb{F}_{g_{ue}} \left(\frac{x}{P_u} \right) \right\} \\
&= \mathcal{B}(x, \varphi_{bu}, \varphi_{ue}) \\
&= \sum_{m=1}^I \frac{\pi B}{2I} \sqrt{1 - \vartheta_m^2} \mathbb{f}_{g_{bu}}(\zeta_m) \left(1 - e^{-\frac{x}{A \zeta_m \varphi_{ue}}} \right) + \left(1 - e^{-\frac{x}{C \varphi_{ue}}} \right) \bar{\mathbb{F}}_{g_{bu}}(B).
\end{aligned} \quad (25)$$

Taking the derivative of $F_{q_{ue}}(x)$ with respect to x yields the PDF of q_{ue} to be

$$\begin{aligned} f_{q_{ue}}(x) &= \sum_{m=1}^I \frac{\pi B}{2I} \sqrt{1 - \vartheta_m^2} \frac{f_{g_{bu}}(\zeta_m)}{A\zeta_m \varphi_{ue}} e^{-\frac{x}{A\zeta_m \varphi_{ue}}} + \frac{\bar{F}_{g_{bu}}(B)}{C\varphi_{ue}} e^{-\frac{x}{C\varphi_{ue}}} \\ &= \sum_{m=0}^I T_{mu} e^{-K_{mu}x}, \end{aligned} \quad (26)$$

where $T_{0u} = \frac{\bar{F}_{g_{bu}}(B)}{C\varphi_{ue}}$, $K_{0u} = \frac{1}{C\varphi_{ue}}$, $T_{tu} = \frac{\pi B}{2I} \sqrt{1 - \vartheta_t^2} \frac{f_{g_{bu}}(\zeta_t)}{A\zeta_t \varphi_{ue}}$, and $K_{tu} = \frac{1}{A\zeta_t \varphi_{ue}}$ with $t \geq 1$.

Using (25) to simplify \mathcal{L} in (23) as

$$\begin{aligned} \mathcal{L} &= \sum_{m=1}^I \frac{\pi B}{2I} \sqrt{1 - \vartheta_m^2} f_{g_{bs}}(\zeta_m) \left(1 - e^{-\frac{1}{A\zeta_m \varphi_{se}} \frac{\Phi_s x + \Phi_s \sigma_e}{1 - \delta - \Phi_s \delta}}\right) + \left(1 - e^{-\frac{1}{C\varphi_{se}} \frac{\Phi_s x + \Phi_s \sigma_e}{1 - \delta - \Phi_s \delta}}\right) \bar{F}_{g_{bs}}(B) \\ &= \sum_{m=0}^I \Lambda_m (1 - \Psi_m e^{-\Theta_m x}), \end{aligned} \quad (27)$$

where $\Lambda_0 = \bar{F}_{g_{bs}}(B)$, $\Psi_0 = e^{-\frac{\Phi_s \sigma_e}{C\varphi_{se}(1 - \delta - \Phi_s \delta)}}$, $\Theta_0 = \frac{\Phi_s}{C\varphi_{se}(1 - \delta - \Phi_s \delta)}$, $\Lambda_t = \frac{\pi B}{2I} \sqrt{1 - \vartheta_t^2} f_{g_{bs}}(\zeta_t)$, $\Psi_t = e^{-\frac{\Phi_s \sigma_e}{A\zeta_t \varphi_{se}(1 - \delta - \Phi_s \delta)}}$, and $\Theta_t = \frac{\Phi_s}{A\zeta_t \varphi_{se}(1 - \delta - \Phi_s \delta)}$ with $t \geq 1$.

Similarly to (27), one can simplify $F_{q_{ke}}(x)$ as

$$\begin{aligned} F_{q_{ke}}(x) &= \sum_{m=1}^I \frac{\pi B}{2I} \sqrt{1 - \vartheta_m^2} f_{g_{bk}}(\zeta_m) \left(1 - e^{-\frac{x}{A\zeta_m \varphi_{ke}}}\right) + \bar{F}_{g_{bk}}(B) \left(1 - e^{-\frac{x}{C\varphi_{ke}}}\right) \\ &= \sum_{m=0}^I \Omega_m (1 - e^{-\Phi_m x}), \end{aligned} \quad (28)$$

where $\Omega_0 = \bar{F}_{g_{bk}}(B)$, $\Phi_0 = \frac{1}{C\varphi_{ke}}$, $\Omega_t = \frac{\pi B}{2I} \sqrt{1 - \vartheta_t^2} f_{g_{bk}}(\zeta_t)$, and $\Phi_t = \frac{1}{A\zeta_t \varphi_{ke}}$ with $t \geq 1$.

Given (28), one can express \mathcal{G} in (23) after using the multinomial theorem and the closely located jammers as

$$\begin{aligned} \mathcal{G} &= [F_{q_{ke}}(x)]^{J-1} \\ &= \left[\sum_{m=0}^I \Omega_m (1 - e^{-\Phi_m x}) \right]^{J-1} \\ &= \sum_{\sum_{v=0}^I a_v = J-1} \frac{(J-1)!}{\prod_{v=0}^I a_v!} \prod_{t=0}^I [\Omega_t (1 - e^{-\Phi_t x})]^{a_t} \\ &= \sum_{\sim} e^{-xG}, \end{aligned} \quad (29)$$

where $G = \sum_{t=0}^I \Phi_t l_t$ and $\sum_{\sim} = \sum_{\sum_{v=0}^I a_v = J-1} \frac{(J-1)!}{\prod_{v=0}^I a_v!} \left[\prod_{t=0}^I (\Omega_t)^{a_t} \right] \sum_{l_0=0}^{a_0} \cdots \sum_{l_I=0}^{a_I} \left(\prod_{t=0}^I C_{a_t}^{l_t} (-1)^{l_t} \right)$.

Using (26), (27), and (29) to express (23) in closed-form as

$$\begin{aligned}
\bar{\Upsilon}_f &= \int_0^{\infty} \mathcal{L}\mathcal{G}\mathfrak{f}_{q_{je}}(x) dx \\
&= \int_0^{\infty} \left[\sum_{l=0}^I \Lambda_l (1 - \Psi_l e^{-\Theta_l x}) \right] \left[\sum_{\sim} e^{-xG} \right] \left(\sum_{m=0}^I T_{mj} e^{-K_{mj}x} \right) dx \\
&= \sum_{l=0}^I \sum_{\sim} \sum_{m=0}^I \Lambda_l T_{mj} \left(\int_0^{\infty} e^{-(K_{mj}+G)x} dx - \Psi_l \int_0^{\infty} e^{-(K_{mj}+G+\Theta_l)x} dx \right) \\
&= \sum_{l=0}^I \sum_{\sim} \sum_{m=0}^I \Lambda_l T_{mj} \left(\frac{1}{K_{mj} + G} - \frac{\Psi_l}{K_{mj} + G + \Theta_l} \right).
\end{aligned} \tag{30}$$

Similarly, (24) is also expressed in closed-form as

$$\begin{aligned}
\tilde{\Upsilon}_f &= \mathcal{E}_{q_{je}} \left\{ \sum_{\sim} e^{-xG} \right\} \\
&= \int_0^{\infty} \left(\sum_{\sim} e^{-xG} \right) \mathfrak{f}_{q_{je}}(x) dx \\
&= \int_0^{\infty} \left(\sum_{\sim} e^{-xG} \right) \left(\sum_{m=0}^I T_{mj} e^{-K_{mj}x} \right) dx \\
&= \sum_{\sim} \sum_{m=0}^I T_{mj} \int_0^{\infty} e^{-(G+K_{mj})x} dx \\
&= \sum_{\sim} \sum_{m=0}^I \frac{T_{mj}}{G + K_{mj}}.
\end{aligned} \tag{31}$$

Remark 3: Similarly to Remark 1, (22) indicates that selecting $\{R_b, R_s, \alpha, \delta\}$ leads to $\frac{1-\delta}{\delta} > \Phi_s$ or $\frac{1-\delta}{\delta} \leq \Phi_s$, causing Υ_f to accept distinct levels and lastly inducing divergent SOP degrees for F. Therefore, the target data/secretary rates $\{R_b, R_s\}$ should be set appropriately in relation to $\{\alpha, \delta\}$ to achieve the desired security performance for F.

2) *Derivation of Υ_n :* Inserting Φ_e^f in (6) and Φ_e^n in (7) into (19), one obtains

$$\begin{aligned}
\Upsilon_n &= 1 - \Pr \left\{ \frac{(1-\delta) P_s g_{se}}{g_{se} \delta P_s + g_{je} P_j + \sigma_e} \geq \Phi_s, \frac{g_{se} \delta P_s}{g_{je} P_j + \sigma_e} \geq \Phi_s \right\} \\
&= 1 - \Pr \{ (1 - \delta - \delta \Phi_s) q_{se} \geq q_{je} \Phi_s + \sigma_e \Phi_s, q_{se} \delta \geq q_{je} \Phi_s + \sigma_e \Phi_s \} \\
&= \begin{cases} \bar{\Upsilon}_n & , \frac{1-\delta}{\delta} > \Phi_s \\ 1 & , \frac{1-\delta}{\delta} \leq \Phi_s \end{cases}
\end{aligned} \tag{32}$$

where

$$\begin{aligned}\bar{\Upsilon}_n &= 1 - \Pr \left\{ q_{se} \geq \frac{q_{je}\Phi_s + \sigma_e\Phi_s}{1 - \delta - \delta\Phi_s}, q_{se} \geq \frac{q_{je}\Phi_s + \sigma_e\Phi_s}{\delta} \right\} \\ &= \Pr \left\{ q_{se} < \max \left(\frac{q_{je}\Phi_s + \sigma_e\Phi_s}{1 - \delta - \delta\Phi_s}, \frac{q_{je}\Phi_s + \sigma_e\Phi_s}{\delta} \right) \right\}.\end{aligned}\quad (33)$$

Based on the proposed jammer selection and the closely located jammers, (33) is rewritten as

$$\begin{aligned}\bar{\Upsilon}_n &= \sum_{j=1}^J \Pr \left\{ q_{se} < \max \left(\frac{q_{je}\Phi_s + \sigma_e\Phi_s}{1 - \delta - \delta\Phi_s}, \frac{q_{je}\Phi_s + \sigma_e\Phi_s}{\delta} \right), A_j \text{ is selected} \right\} \\ &= \sum_{j=1}^J \Pr \left\{ q_{se} < \max \left(\frac{q_{je}\Phi_s + \sigma_e\Phi_s}{1 - \delta - \delta\Phi_s}, \frac{q_{je}\Phi_s + \sigma_e\Phi_s}{\delta} \right), \bigcap_{k \in [1, J] \setminus j} \{q_{je} > q_{ke}\} \right\} \\ &= J\mathcal{E}_{q_{je}} \left\{ \Pr \left\{ q_{se} < \max \left(\frac{q_{je}\Phi_s + \sigma_e\Phi_s}{1 - \delta - \delta\Phi_s}, \frac{q_{je}\Phi_s + \sigma_e\Phi_s}{\delta} \right), \bigcap_{k \in [1, J] \setminus j} \{q_{je} > q_{ke}\} \middle| q_{je} \right\} \right\} \\ &= J\mathcal{E}_{q_{je}} \left\{ \underbrace{\mathbb{F}_{q_{se}}(\max(Hq_{je} + L, Mx + R))}_{\mathcal{U}} \underbrace{\prod_{k \in [1, J] \setminus j} \mathbb{F}_{q_{ke}}(q_{je})}_{\mathcal{G}} \right\},\end{aligned}\quad (34)$$

where $H = \frac{\Phi_s}{1 - \delta - \delta\Phi_s}$, $L = \frac{\sigma_e\Phi_s}{1 - \delta - \delta\Phi_s}$, $M = \frac{\Phi_s}{\delta}$, and $R = \frac{\sigma_e\Phi_s}{\delta}$.

Before deriving (34), one simplifies \mathcal{U} by invoking (25) as

$$\begin{aligned}\mathcal{U} &= \sum_{m=1}^I \frac{\pi B}{2I} \sqrt{1 - \vartheta_m^2} \mathbb{F}_{g_{bs}}(\zeta_m) \left(1 - e^{-\frac{\max(Hx+L, Mx+R)}{A\zeta_m\varphi_{se}}} \right) + \left(1 - e^{-\frac{\max(Hx+L, Mx+R)}{C\varphi_{se}}} \right) \bar{\mathbb{F}}_{g_{bs}}(B) \\ &= \sum_{m=0}^I \Lambda_m \left(1 - e^{-\max(H_m x + L_m, M_m x + R_m)} \right) \\ &= \begin{cases} \sum_{m=0}^I \Lambda_m \left(1 - e^{-H_m x - L_m} \right) & , \Phi_s > \frac{1-2\delta}{\delta} \\ \sum_{m=0}^I \Lambda_m \left(1 - e^{-M_m x - R_m} \right) & , \Phi_s \leq \frac{1-2\delta}{\delta} \end{cases}\end{aligned}\quad (35)$$

where $H_0 = \frac{H}{C\varphi_{se}}$, $L_0 = \frac{L}{C\varphi_{se}}$, $M_0 = \frac{M}{C\varphi_{se}}$, $R_0 = \frac{R}{C\varphi_{se}}$, $H_t = \frac{H}{A\zeta_t\varphi_{se}}$, $L_t = \frac{L}{A\zeta_t\varphi_{se}}$, $M_t = \frac{M}{A\zeta_t\varphi_{se}}$, and $R_t = \frac{R}{A\zeta_t\varphi_{se}}$ with $t \geq 1$.

Now inserting \mathcal{U} in (35), \mathcal{G} in (29) and $f_{q_{je}}$ in (26) into (34) yields

$$\begin{aligned}
\bar{\Upsilon}_n &= J \int_0^\infty \mathcal{U} \mathcal{G} \mathfrak{f}_{q_{je}}(x) dx \\
&= \begin{cases} J \int_0^\infty \left[\sum_{l=0}^I \Lambda_l (1 - e^{-H_l x - L_l}) \right] \left(\sum_{\sim} e^{-xG} \right) \left(\sum_{m=0}^I T_{mj} e^{-K_{mj} x} \right) dx, & \Phi_s > \frac{1-2\delta}{\delta} \\ J \int_0^\infty \left[\sum_{l=0}^I \Lambda_l (1 - e^{-M_l x - R_l}) \right] \left(\sum_{\sim} e^{-xG} \right) \left(\sum_{m=0}^I T_{mj} e^{-K_{mj} x} \right) dx, & \Phi_s \leq \frac{1-2\delta}{\delta} \end{cases} \quad (36) \\
&= \begin{cases} J \sum_{l=0}^I \sum_{\sim} \sum_{m=0}^I T_{mj} \Lambda_l \left(\frac{1}{K_{mj}+G} - \frac{e^{-L_l}}{K_{mj}+G+H_l} \right), & \Phi_s > \frac{1-2\delta}{\delta} \\ J \sum_{l=0}^I \sum_{\sim} \sum_{m=0}^I T_{mj} \Lambda_l \left(\frac{1}{K_{mj}+G} - \frac{e^{-R_l}}{K_{mj}+G+M_l} \right), & \Phi_s \leq \frac{1-2\delta}{\delta} \end{cases}
\end{aligned}$$

Remark 4: Similarly to Remark 1, (32) indicates that selecting $\{R_b, R_s, \alpha, \delta\}$ leads to $\frac{1-\delta}{\delta} > \Phi_s$ or $\frac{1-\delta}{\delta} \leq \Phi_s$, causing Υ_n to accept different values and finally causing divergent SOP degrees for N. More specifically, N is completely secured ($\Upsilon_n = 1$) if $\frac{1-\delta}{\delta} \leq \Phi_s$ (or $R_b - R_s \geq -(1 - \alpha) \log_2 \delta$); otherwise, N suffers a certain insecurity. This implies that the system designer must set the limit for the target data/secret rates $\{R_b, R_s\}$ such that $R_b - R_s \geq -(1 - \alpha) \log_2 \delta$ to attain the complete security for N.

Remark 5: Both Υ_f and Υ_n depend on parameters $(R_b, R_s, \alpha, P, \delta, \chi, J, \beta)$, meaning that N and F can attain the desired security performances by setting properly these parameters.

3) *Asymptotic security analysis:* The following finds the upper-bound on the information security of JSEHNOMA in the regime of high transmit power, namely $P \rightarrow \infty$. It is recalled that NLEH is completely saturated as $P \rightarrow \infty$. Therefore, $P_u \rightarrow C$ as $P \rightarrow \infty$. Then, $F_{q_{ue}}(x) \rightarrow F_{g_{ue}}\left(\frac{x}{C}\right)$ and $\mathfrak{f}_{q_{ue}}(x) \rightarrow \frac{1}{C} \mathfrak{f}_{g_{ue}}\left(\frac{x}{C}\right)$. Using these results and following the analysis in Subsections III-B2 and III-B1, one attains the SOPs for F and N, respectively, as

$$\Upsilon_f^\infty = \begin{cases} J \bar{\Upsilon}_f^\infty, & \frac{1-\delta}{\delta} > \Phi_s \\ J \tilde{\Upsilon}_f^\infty, & \frac{1-\delta}{\delta} \leq \Phi_s \end{cases} \quad (37)$$

and

$$\Upsilon_n^\infty = \begin{cases} \bar{\Upsilon}_n^\infty, & \frac{1-\delta}{\delta} > \Phi_s \\ 1, & \frac{1-\delta}{\delta} \leq \Phi_s \end{cases} \quad (38)$$

where

$$\begin{aligned}\bar{\Upsilon}_f^\infty &= \int_0^\infty \mathbb{F}_{q_{se}} \left(\frac{\Phi_s x + \Phi_s \sigma_e}{1 - \delta - \Phi_s \delta} \right) [\mathbb{F}_{q_{ke}}(x)]^{J-1} \mathbb{f}_{q_{je}}(x) dx \\ &= \int_0^\infty \mathbb{F}_{g_{se}} \left(\frac{\Phi_s x + \Phi_s \sigma_e}{[1 - \delta - \Phi_s \delta]C} \right) \left[\mathbb{F}_{g_{ke}} \left(\frac{x}{C} \right) \right]^{J-1} \frac{1}{C} \mathbb{f}_{g_{je}} \left(\frac{x}{C} \right) dx\end{aligned}\quad (39)$$

$$\begin{aligned}\tilde{\Upsilon}_f^\infty &= \int_0^\infty [\mathbb{F}_{q_{ke}}(x)]^{J-1} \mathbb{f}_{q_{je}}(x) dx \\ &= \int_0^\infty \left[\mathbb{F}_{g_{ke}} \left(\frac{x}{C} \right) \right]^{J-1} \frac{1}{C} \mathbb{f}_{g_{je}} \left(\frac{x}{C} \right) dx\end{aligned}\quad (40)$$

$$\begin{aligned}\bar{\Upsilon}_n^\infty &= J \int_0^\infty \mathbb{F}_{q_{se}}(\max(Hx + L, Mx + R)) [\mathbb{F}_{q_{ke}}(x)]^{J-1} \mathbb{f}_{q_{je}}(x) dx \\ &= \begin{cases} J \int_0^\infty \mathbb{F}_{q_{se}}(Hx + L) [\mathbb{F}_{q_{ke}}(x)]^{J-1} \mathbb{f}_{q_{je}}(x) dx & , \Phi_s > \frac{1-2\delta}{\delta} \\ J \int_0^\infty \mathbb{F}_{q_{se}}(Mx + R) [\mathbb{F}_{q_{ke}}(x)]^{J-1} \mathbb{f}_{q_{je}}(x) dx & , \Phi_s \leq \frac{1-2\delta}{\delta} \end{cases} \\ &= \begin{cases} J \int_0^\infty \mathbb{F}_{g_{se}} \left(\frac{Hx+L}{C} \right) \left[\mathbb{F}_{g_{ke}} \left(\frac{x}{C} \right) \right]^{J-1} \frac{1}{C} \mathbb{f}_{g_{je}} \left(\frac{x}{C} \right) dx & , \Phi_s > \frac{1-2\delta}{\delta} \\ J \int_0^\infty \mathbb{F}_{g_{se}} \left(\frac{Mx+R}{C} \right) \left[\mathbb{F}_{g_{ke}} \left(\frac{x}{C} \right) \right]^{J-1} \frac{1}{C} \mathbb{f}_{g_{je}} \left(\frac{x}{C} \right) dx & , \Phi_s \leq \frac{1-2\delta}{\delta} \end{cases}\end{aligned}\quad (41)$$

Now we express $\bar{\Upsilon}_f^\infty$, $\tilde{\Upsilon}_f^\infty$, and $\bar{\Upsilon}_n^\infty$ explicitly by using the binomial expansion and the explicit forms of $\mathbb{F}_{g_{ue}}(x)$ and $\mathbb{f}_{g_{ue}}(x)$. Therefore, we obtain

$$\begin{aligned}\bar{\Upsilon}_f^\infty &= \int_0^\infty \left(1 - e^{-\frac{\Phi_s x + \Phi_s \sigma_e}{[1 - \delta - \Phi_s \delta]C\varphi_{se}}} \right) \left(1 - e^{-\frac{x}{C\varphi_e}} \right)^{J-1} \frac{1}{C\varphi_e} e^{-\frac{x}{C\varphi_e}} dx \\ &= \int_0^\infty \left(1 - e^{-\frac{\Phi_s x + \Phi_s \sigma_e}{[1 - \delta - \Phi_s \delta]C\varphi_{se}}} \right) \left[\sum_{i=0}^{J-1} \mathbf{C}_{J-1}^i \left(-e^{-\frac{x}{C\varphi_e}} \right)^{J-1-i} \right] \frac{1}{C\varphi_e} e^{-\frac{x}{C\varphi_e}} dx \\ &= \sum_{i=0}^{J-1} \frac{\mathbf{C}_{J-1}^i (-1)^{J-1-i}}{C\varphi_e} \left[\frac{C\varphi_e}{J-i} - e^{-\frac{\Phi_s \sigma_e}{[1 - \delta - \Phi_s \delta]C\varphi_{se}}} \left(\frac{\Phi_s}{[1 - \delta - \Phi_s \delta]C\varphi_{se}} - \frac{J-i}{C\varphi_e} \right)^{-1} \right]\end{aligned}\quad (42)$$

$$\begin{aligned}
\tilde{\Upsilon}_f^\infty &= \int_0^\infty \left(1 - e^{-\frac{x}{C\varphi_e}}\right)^{J-1} \frac{1}{C\varphi_e} e^{-\frac{x}{C\varphi_e}} dx \\
&= \int_0^\infty \left[\sum_{i=0}^{J-1} \mathbf{C}_{J-1}^i \left(-e^{-\frac{x}{C\varphi_e}}\right)^{J-1-i} \right] \frac{1}{C\varphi_e} e^{-\frac{x}{C\varphi_e}} dx \\
&= \sum_{i=0}^{J-1} \frac{\mathbf{C}_{J-1}^i (-1)^{J-1-i}}{J-i}
\end{aligned} \tag{43}$$

$$\begin{aligned}
\bar{\Upsilon}_n^\infty &= \begin{cases} J \int_0^\infty \left(1 - e^{-\frac{Hx+L}{C\varphi_{se}}}\right) \left(1 - e^{-\frac{x}{C\varphi_e}}\right)^{J-1} \frac{1}{C\varphi_e} e^{-\frac{x}{C\varphi_e}} dx, & \Phi_s > \frac{1-2\delta}{\delta} \\ J \int_0^\infty \left(1 - e^{-\frac{Mx+R}{C\varphi_{se}}}\right) \left(1 - e^{-\frac{x}{C\varphi_e}}\right)^{J-1} \frac{1}{C\varphi_e} e^{-\frac{x}{C\varphi_e}} dx, & \Phi_s \leq \frac{1-2\delta}{\delta} \end{cases} \\
&= \begin{cases} J \sum_{i=0}^{J-1} \frac{\mathbf{C}_{J-1}^i (-1)^{J-1-i}}{C\varphi_e} \left[\frac{C\varphi_e}{J-i} - e^{-\frac{L}{C\varphi_{se}}} \left(\frac{H}{C\varphi_{se}} - \frac{J-i}{C\varphi_e} \right)^{-1} \right], & \Phi_s > \frac{1-2\delta}{\delta} \\ J \sum_{i=0}^{J-1} \frac{\mathbf{C}_{J-1}^i (-1)^{J-1-i}}{C\varphi_e} \left[\frac{C\varphi_e}{J-i} - e^{-\frac{R}{C\varphi_{se}}} \left(\frac{M}{C\varphi_{se}} - \frac{J-i}{C\varphi_e} \right)^{-1} \right], & \Phi_s \leq \frac{1-2\delta}{\delta} \end{cases}
\end{aligned} \tag{44}$$

4) *Secrecy throughput*: For JSEHNOMA with delay-limited communications, the STPs of N and F are given by

$$\mathbb{S}_n = (1 - \alpha)(R_b - R_s)(1 - \Upsilon_n) \quad \mathbb{S}_f = (1 - \alpha)(R_b - R_s)(1 - \Upsilon_f). \tag{45}$$

It is reminded that the higher the STP, the less security N and F attain. Also, (45) indicates that the STPs of N and F are also jointly determined by a specification set $(R_b, R_s, \alpha, P, \delta, \chi, J, \beta)$ since this set influences Υ_n and Υ_f . Therefore, the desired STPs are attained by establishing properly and flexibly this set conditioned on its preset value range.

IV. DEMONSTRATIVE RESULTS

A multiplicity of simulated/analytical results are presented to measure the CTP/STP of N and F in JSEHNOMA in multitudinous specifications in this section. The CTP/STP of N/F is denoted as N/F-Reliability/Security in the subsequent figures. Analytical results are generated by the theoretical expressions in Section III while simulated results are produced by Monte-Carlo simulations. Both simulated and analytical results are then compared to validate the analysis in Section III. For illustration, users are located in a 2D plane. Unless otherwise stated, parameters are adopted in Table II.

For performance comparison, two reference schemes are considered. The reference schemes differ the proposed scheme only in Stage 2. More specifically, in the first reference scheme, a jammer is randomly selected and S implements NOMA. In the second reference scheme, the

TABLE II: Selected parameters unless otherwise stated

Parameter	Value
Power splitting coefficient	$\delta = 0.2$
Energy converting efficiency	$\beta = 0.7$
Position of B	(0, 0) m
Position of S	(10, -10) m
Position of A_j	(10, 5) m
Position of E	(25, 0) m
Position of N	(30, 0) m
Position of F	(45, -10) m
Fading power at the reference distance of 1 m	$\varepsilon = 10^{-2}$
Transmit power of B	$P = 20$ dBW
Noise power	$\sigma_v = -90$ dBm, $v = \{n, f, e\}$
Time splitting coefficient	$\alpha = 0.4$
Power saturation threshold	$\sigma = -20$ dBW
Target data rate	$R_b = 1$ bps/Hz
Target secrecy rate	$R_s = 0.5$ bps/Hz
Quantity of jammers	$J = 5$
Path loss exponent	$v = 2.7$

jammer selection of the proposed scheme is implemented and S carries out OMA by dividing Stage 2 into two equal sub-stages in which S transmits sequentially x_n to N and x_f to F. In the following figures, the proposed scheme, the first and the second reference schemes are respectively denoted as ‘Proposed’, ‘Random’, and ‘OMA’. Therefore, the reliability performances of the proposed and the first reference schemes are similar (denoted as ‘N/F: Proposed & Random’ in the following figures) and the security performances of N and F in the second reference scheme are identical (denoted as ‘F-Security = N-Security’ in the following figures). The security/reliability analyses for two reference schemes are proceeded in the same manner as the proposed scheme and thence, we omitted them for compactness.

Figure 2 illustrates the CTP/STP versus P . This figure unveils the match between the simulation and the analysis for the proposed scheme, validating the exactness of the analysis in Section III. Also this figure reveals the considerable reliability enhancement (i.e., higher CTP) yet the slight security mitigation (i.e. higher STP) with accreting P for both N and F. This originates from increasing harvested energy. Indeed, the higher harvested energy (i.e., higher transmit power of S) makes N and F receive their desired signals more reliably. However,

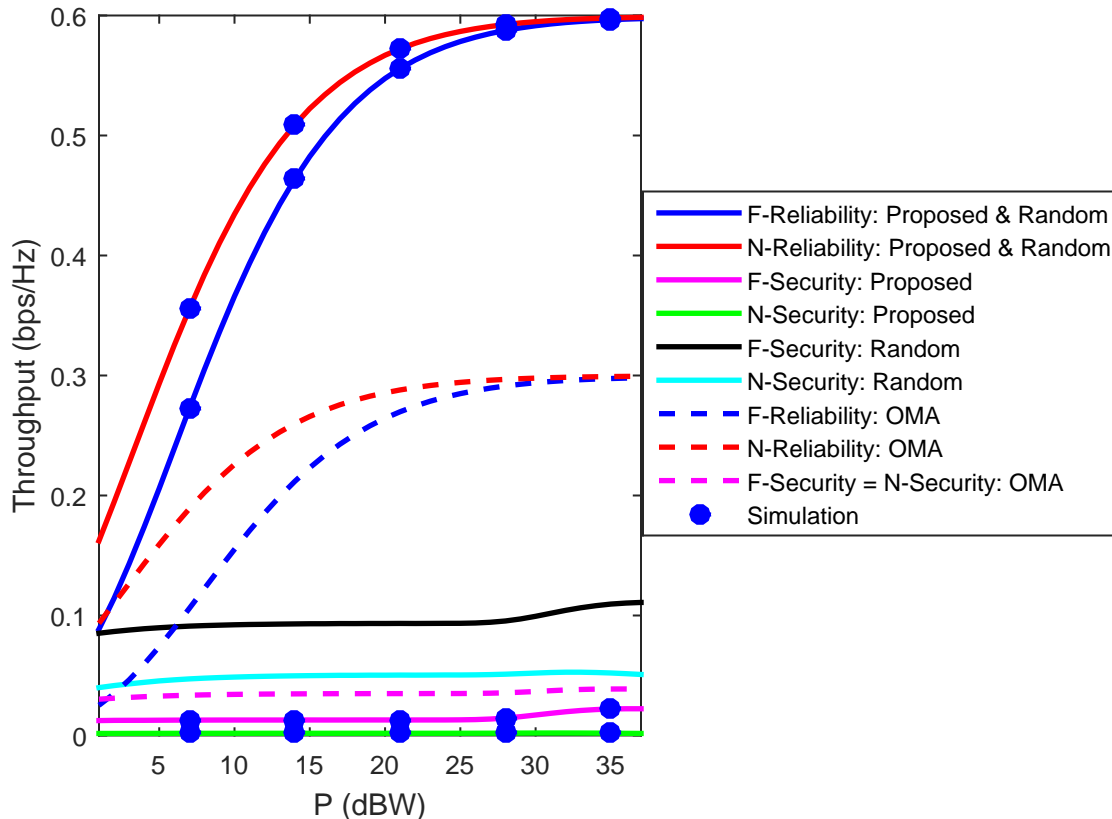


Fig. 2: CTP/STP versus the power of B

the higher harvested energy not only increases the transmit power of S but also accretes the transmit power of A_j , making E receive more both desired signal power and jamming power. Thence, the SINRs for E to decode x_n and x_f increase slightly, eventually degrading slightly the security performance. Moreover, due to the increase of both the CTP and the STP with increasing P , the trade-off between the reliability and the security arises. Nevertheless, that the security is mitigated slightly whilst the reliability is improved significantly with accreting P reveals the efficacy of the jamming operation in remaining communications secured with higher reliability. Furthermore, the security/reliability performance is saturated at high P as analyzed⁴ in Subsections III-A3 and III-B3. Further, the CTP of the proposed (NOMA) scheme is almost double that of the second reference (OMA) scheme as expected, showing the superiority of

⁴Due to the high number of curves in Figure 2, the asymptotic analytical results in Subsections III-A3 and III-B3 are not presented here. Nevertheless, we double-checked the agreement between the asymptotic analytical results and the simulated results at high P , which exposes the precision of the analysis in Subsections III-A3 and III-B3.

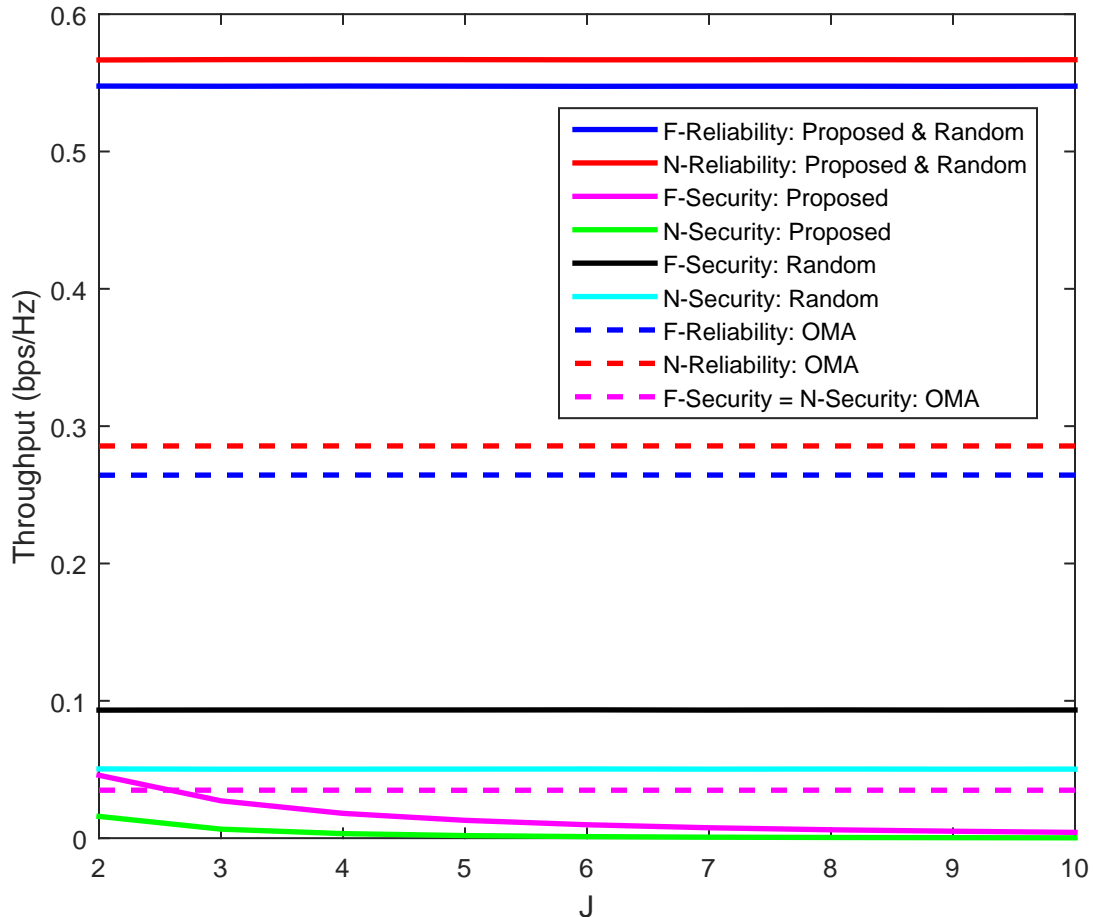


Fig. 3: CTP/STP versus the number of jammers

the proposed scheme in comparison with its OMA counterpart in terms of the reliability. In addition, the STP is in the increasing order for the proposed (NOMA-and-proposed jammer selection) scheme, the second (OMA-and-proposed jammer selection) reference scheme, and the first (NOMA-and-random jammer selection) reference scheme, unveiling the significantly higher security of the proposed scheme as compared to the reference ones. This also exposes the efficacy of the proposed jammer selection and the NOMA in securing communications as compared to the random jammer selection and the OMA. Briefly, the proposed scheme outperforms the reference ones in terms of both the reliability and the security. Owing to the match between the analytical and simulated results of the proposed scheme, the subsequent figures show merely the analytical results to reduce the number of curves, ultimately making the figures readable.

Figure 3 unveils the influence of the number of jammers J on the CTP/STP of N and F.

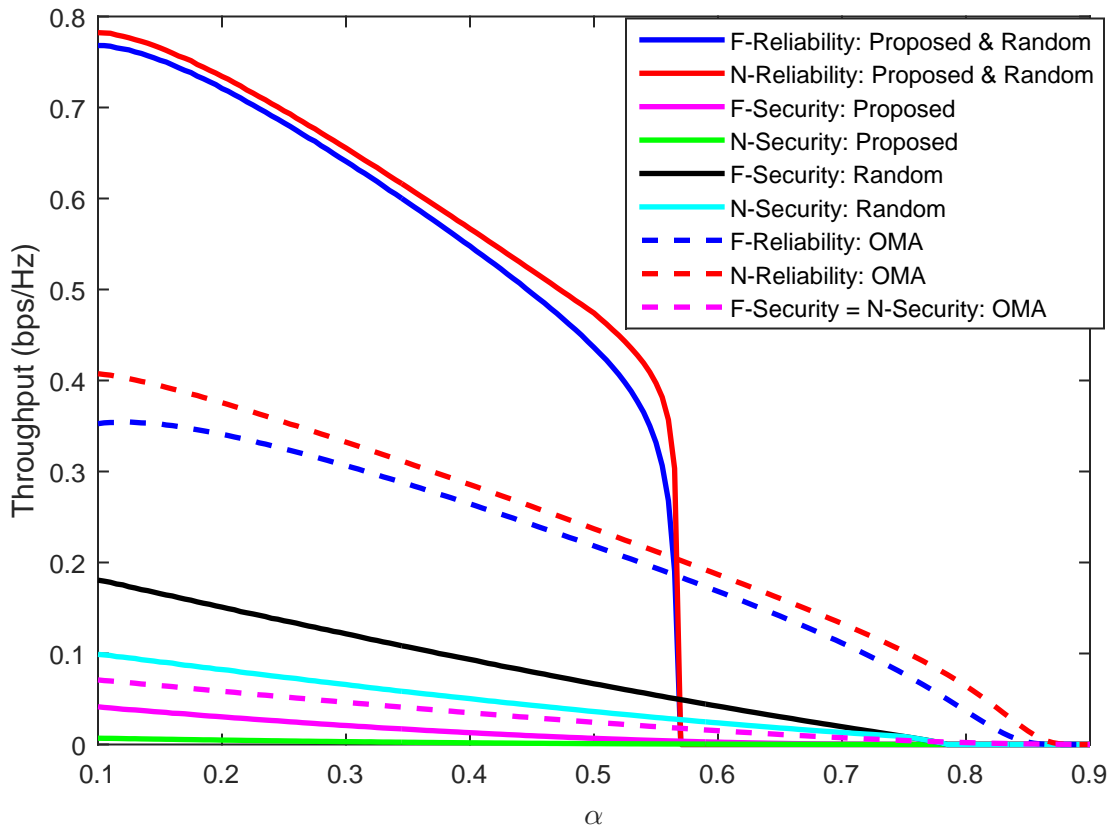


Fig. 4: CTP/STP versus the time splitting coefficient α

As expected, the communications reliability of all the considered schemes and the information security of the first (NOMA-and-random jammer selection) reference scheme are independent of J . Additionally, the CTP of the proposed (NOMA) scheme is twice that of the second (OMA) reference scheme, showing that the proposed scheme outperforms its OMA counterpart in terms of the reliability. Moreover, the proposed scheme is more secure than the reference schemes, exposing the efficacy of the proposed jammer selection in meliorating the information security. Moreover, the security of the proposed scheme is meliorated with increasing J , as expected. Meanwhile, the security of the second (OMA) reference scheme is almost unchanged with increasing J . In summary, the proposed scheme attains higher reliability and security than the reference ones.

Figure 4 illustrates the influence of the time splitting coefficient α on the CTP/STP of N and F. This figure reveals that the reliability performance is deteriorated with increasing α (i.e. the CTP reduces with increasing α). This is because the CTP is inversely proportional to α as seen

in (17). In addition, high α causes the zero CTP, which was already analyzed in Section III. More specifically, Remark 1 indicates the zero CTP (or the complete connection outage) for $R_b \geq -(1 - \alpha) \log_2 \delta$ or $\alpha \geq 1 + \frac{R_b}{\log_2 \delta}$. Given the system parameters ($R_b = 1$ bps/Hz, $\delta = 0.2$) in Table II, it is obvious that the zero CTP of the proposed scheme occurs when $\alpha \geq 0.5693$, which coincides with the results in Figure 4. Additionally, the proposed (NOMA) scheme attains the CTP almost twice that of the second (OMA) reference scheme, showing the efficacy of the NOMA in improving the reliability. Moreover, all the considered schemes have lower STP with increasing α , indicating the security improvement. Therefore, the security-and-reliability trade-off is observed since the reliability is mitigated but the security is meliorated with increasing α . Furthermore, the proposed scheme has the lower STP than two reference schemes, again verifying the efficacy of the proposed jammer selection and the NOMA in improving both the security and the reliability.

Figure 5 illustrates the influence of the energy converting efficiency β on the CTP/STP of N and F. This figure shows that the communications reliability is slightly meliorated with accreting β due to the increasing harvested energy which eventually increases the received power at N and F for decoding x_n and x_f more reliably. However, the security performance is almost unchanged with increasing β . This is because the increasing harvested energy due to increasing β accretes both powers of the desired signal and the jamming signal and thence, the SINR for E to decode x_n and x_f is almost constant. Additionally, the CTP of the proposed (NOMA) scheme is almost double that of the second (OMA) reference scheme, indicating the efficiency of the NOMA in improving the reliability. Further, the proposed scheme is more secure than both reference schemes. In brief, the proposed scheme accomplishes higher reliability and security than the reference ones.

Figure 6 demonstrates the influence of the power splitting coefficient δ , which represents the power portion allocated to x_n , on the CTP/STP of N and F. One sees that the reliability performance of the second (OMA) reference scheme is independent of δ as predicted. Moreover, the reliability performance of F for the proposed scheme is mitigated with increasing δ , which is because of less power allocated to transmit x_f and direct decoding of x_f at F. Nevertheless, N in the proposed scheme can attain the highest CTP with the optimal selection of δ (e.g. $\delta = 0.238$ makes the CTP of N the highest in Figure 6). This is because N must decode x_f prior to decoding x_n . Therefore, δ should be selected optimally to balance between the SINR for decoding x_f and the SNR for decoding x_n . In addition, high δ causes the zero CTP, which was already analyzed

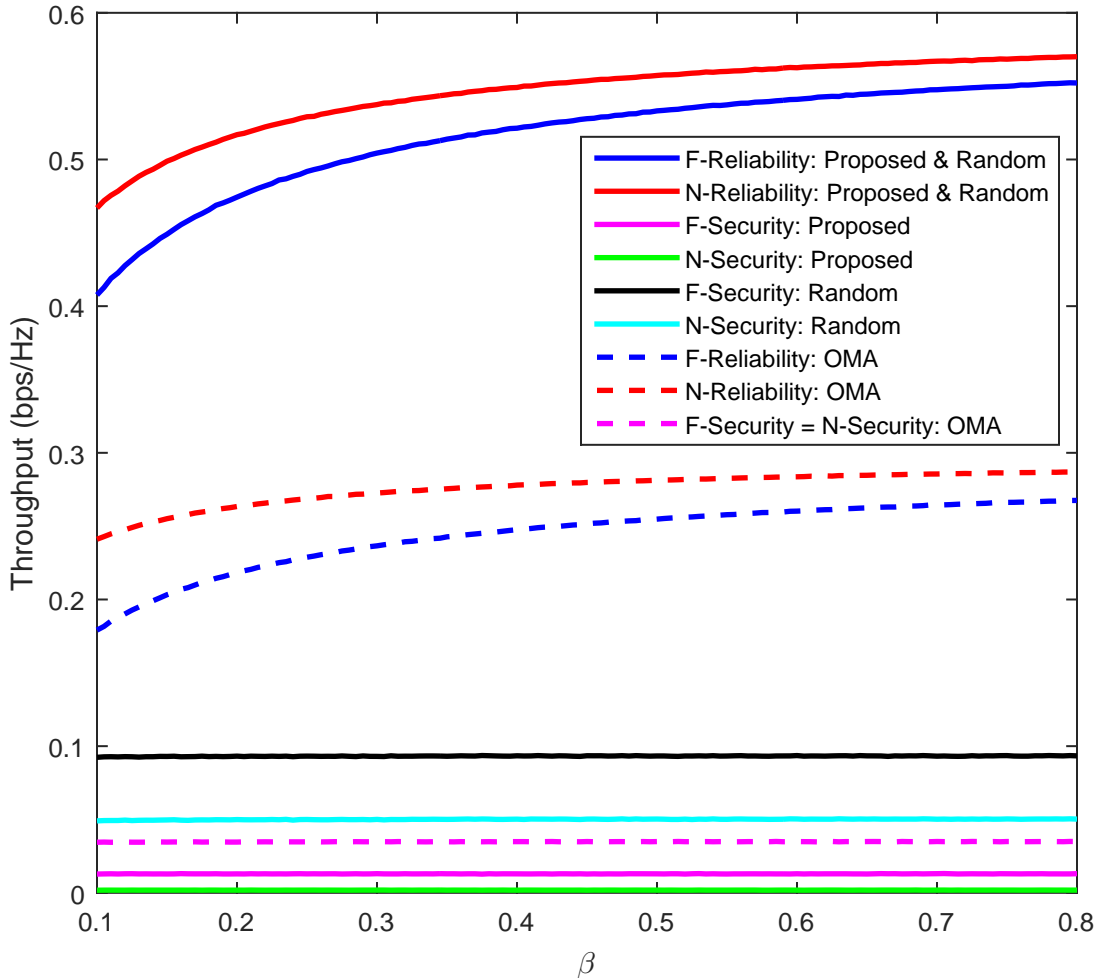


Fig. 5: CTP/STP versus the energy converting efficiency

in Section III. More specifically, Remark 1 indicates the zero CTP (or the complete connection outage) for $R_b \geq -(1 - \alpha) \log_2 \delta$ or $\delta > 2^{-\frac{R_b}{1-\alpha}}$. Given the system parameters ($R_b = 1$ bps/Hz, $\alpha = 0.4$) in Table II, it is obvious that the zero CTP of the proposed scheme occurs when $\delta \geq 0.315$, which coincides with the results in Figure 6. Further, the proposed (NOMA) scheme attains the CTP almost twice that of the second (OMA) reference scheme, showing the efficacy of the NOMA in improving the reliability. Moreover, the proposed scheme has the lower STP than two reference schemes, again verifying the efficacy of the proposed jammer selection and the NOMA in improving both the security and the reliability.

Figure 7 exposes the effect of the power saturation threshold χ on the CTP/STP of N and F. The results show the considerable reliability improvement with accreting χ , which is because

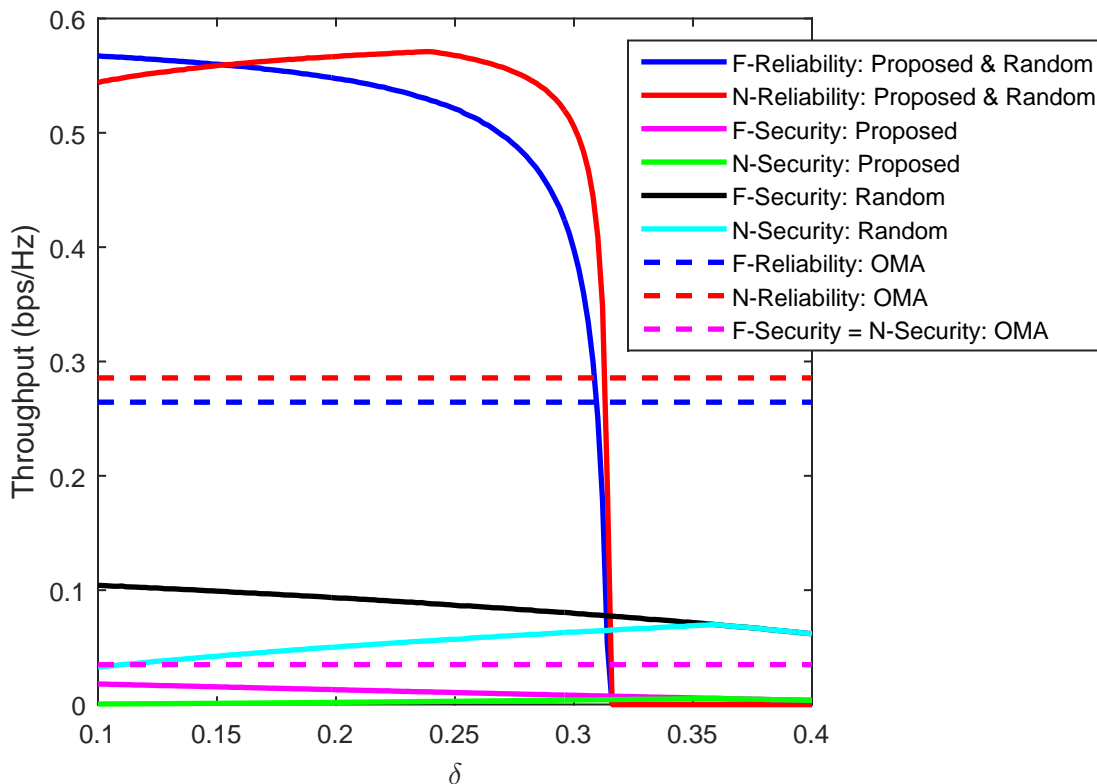


Fig. 6: CTP/STP versus the power splitting coefficient

of the increasing harvested energy. Additionally, the CTP is saturated at high χ because high χ makes the energy harvester linear. In addition, the proposed (NOMA) scheme attains the CTP almost twice that of the second (OMA) reference scheme, showing the efficacy of the NOMA in improving the reliability. Nevertheless, the STP can be optimized with the appropriate selection of χ . This is because increasing χ accretes both powers of the jamming signal and the desired signal. Thence, E can attain the best STP (the worst security for N and F) by balancing between the jamming power and the desired power with the optimal value of χ . Further, the proposed scheme is more secure than two reference schemes, again verifying the efficacy of the proposed jammer selection and the NOMA in meliorating both the reliability and the security.

V. CONCLUSIONS

This paper proposed the jammer selection in EH-aided NOMA to improve the reliability-and-security performances and the spectral-and-energy efficiencies for downlink communications. For prompt security/reliability performance evaluation, this paper proposed the closed-form

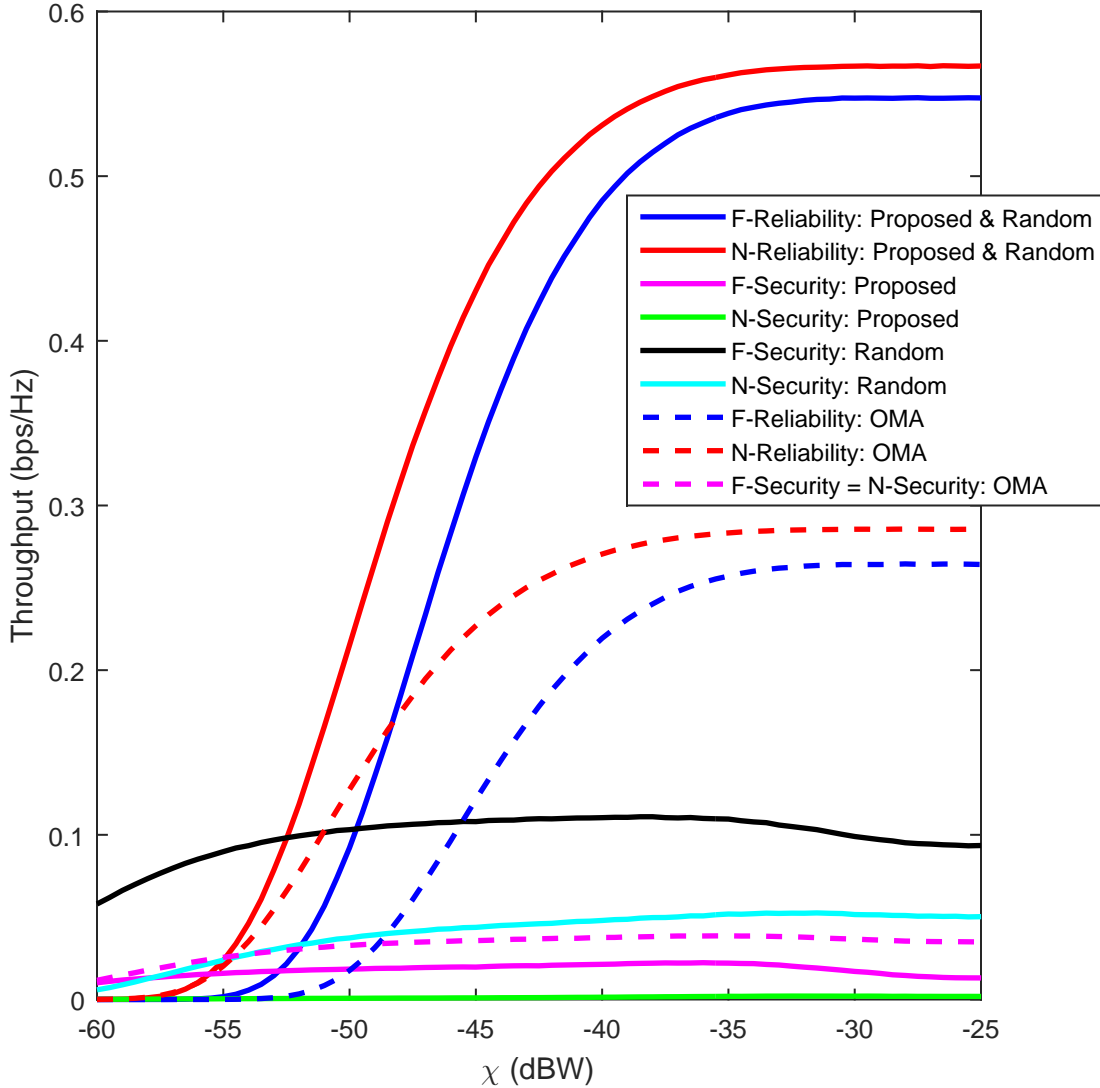


Fig. 7: CTP/STP versus the power saturation threshold

COP/SOP/CTP/STP formulas. Multifarious results corroborated the proposed formulas and reveal that EH nonlinearity, which is characterized by χ , dramatically affects the communications reliability but slightly the information security. In addition, there exists limits on the target data rate R_b and the target secrecy rate R_s to avoid the complete connection outage (i.e. the COP is one) and achieve the complete security (i.e. the SOP is one). Moreover, the proposed (NOMA-and-proposed jammer selection) scheme attains significantly higher security and reliability than its counterparts (NOMA-and-random jammer selection and OMA-and-proposed jammer selection). However, there is a trade-off between the reliability and the security. Remarkably, the proposed

scheme attains the optimum security/reliability performance with the proper selection of δ and χ .

DECLARATIONS

Ethics Approval

Not applicable.

Conflict of Interest

The author declares no conflict of interest.

Data Availability

Data is contained within the article.

Author Contribution

Khuong Ho-Van contributes the whole manuscript.

Funding

No funding.

Consent to publish

Khuong Ho-Van consents to publish this manuscript on Peer-to-Peer Networking and Applications.

REFERENCES

- [1] H. Guo *et al.*, "Multi-UAV Cooperative Task Offloading and Resource Allocation in 5G Advanced and Beyond," *IEEE Trans. Wire. Commun.* To appear.
- [2] M. Fall *et al.*, "Towards Sustainable 5G Networks: A Proposed Coordination Solution for Macro and Pico Cells to Optimize Energy Efficiency," *IEEE Access.* To appear.
- [3] H. Lee *et al.*, "Towards 6G hyper-connectivity: Vision, challenges, and key enabling technologies," *JCN.* To appear.
- [4] Q. T. Ngo *et al.*, "Physical Layer Security in IRS-Assisted Cache-Enabled Satellite Communication Networks," *IEEE Trans. Green Commun. and Netw.* To appear.
- [5] Y. Li *et al.*, "NOMA Assisted Two-Tier VR Content Transmission: A Tile-based Approach for QoE Optimization," *IEEE Trans. Mobi. Comp.* To appear.

- [6] X. Zhang *et al.*, “Generalized Approximate Message Passing Based Bayesian Learning Detectors for Uplink Grant-Free NOMA,” *IEEE Trans. Veh. Tech.* To appear.
- [7] H. G. Srinath *et al.*, “An Efficient NB-IoT Compatible GF-NOMA PHY Mechanism for mMTC,” *IEEE IoT J.* To appear.
- [8] B. Hu *et al.*, “A Self-Powered Rectifier-Less Series-Synchronized Switch Harvesting on Inductor (S-SSHI) Interface Circuit for Flutter-Based Piezoelectric Energy Harvesters,” *IEEE Instrumentation & Measurement Mag.*, vol. 26, no. 3, pp. 5-13, May 2023.
- [9] M. A. Halimi *et al.*, “Rectifier Design Challenges for Wireless Energy Harvesting/Wireless Power Transfer Systems: Broadening Bandwidth and Extended Input Power Range,” *IEEE Micro. Mag.*, vol. 24, no. 6, pp. 54-67, Jun. 2023.
- [10] M. A. Halimi *et al.*, “Rectifier Circuits for RF Energy Harvesting and Wireless Power Transfer Applications: A Comprehensive Review Based on Operating Conditions,” *IEEE Micro. Mag.*, vol. 24, no. 1, pp. 46-61, Jan. 2023.
- [11] N. Pham-Thi-Dan *et al.*, “Security Analysis for Cognitive Radio Network with Energy Scavenging Capable Relay over Nakagami-m Fading Channels,” in *Proc. IEEE ISEE*, Oct. 2019, pp. 68-72.
- [12] D. Wang *et al.*, “Primary Privacy Preserving With Joint Wireless Power and Information Transfer for Cognitive Radio Networks,” *IEEE Trans. Cog. Commun. Netw.*, vol. 6, no. 2, pp. 683-693, Jun. 2020.
- [13] L. Ge *et al.*, “Performance Analysis for Multihop Cognitive Radio Networks With Energy Harvesting by Using Stochastic Geometry,” *IEEE IoT J.*, vol. 7, no. 2, pp. 1154-1163, Feb. 2020.
- [14] M. Bouabdellah *et al.*, “Cooperative Energy Harvesting Cognitive Radio Networks With Spectrum Sharing and Security Constraints,” *IEEE Access*, vol. 7, pp. 173329-173343, Nov. 2019.
- [15] Z. Zhu *et al.*, “Robust Beamforming Designs in Secure MIMO SWIPT IoT Networks With a Nonlinear Channel Model,” *IEEE IoT J.*, vol. 8, no. 3, pp. 1702-1715, Feb. 2021.
- [16] S. Solanki *et al.*, “Performance Analysis of Piece-Wise Linear Model of Energy Harvesting-Based Multiuser Overlay Spectrum Sharing Networks,” *IEEE OJCS*, vol. 1, pp. 1820-1836, Nov. 2020.
- [17] M. Babaei *et al.*, “BER Performance of Full-Duplex Cognitive Radio Network With Nonlinear Energy Harvesting,” *IEEE Trans. Green Commun. Netw.*, vol. 4, no. 2, pp. 448-460, Jun. 2020.
- [18] D. Wang *et al.*, “Performance Analysis and Resource Allocations for a WPCN With a New Nonlinear Energy Harvester Model,” *IEEE OJCOMS*, vol. 1, pp. 1403-1424, Sep. 2020.
- [19] L. Ni *et al.*, “Outage-Constrained Secrecy Energy Efficiency Optimization for CRNs With Non-Linear Energy Harvesting,” *IEEE Access*, vol. 7, pp. 175213-175221, Dec. 2019.
- [20] F. Wang *et al.*, “Secure Resource Allocation for Polarization-Based Non-Linear Energy Harvesting Over 5G Cooperative CRNs,” *IEEE Wire. Commun. Lett.* To appear.
- [21] H. Salman *et al.*, “PLS-IoT Enhancement against Eavesdropping via Spatially Distributed Constellation Obfuscation,” *IEEE Wire. Commun. Lett.* To appear.
- [22] K. Cao *et al.*, “Physical Layer Security for Intelligent Reflecting Surface aided Wireless Powered Communication Systems,” *IEEE IoT J.* To appear.
- [23] M. H. Loukil *et al.*, “Physical Layer Security at a Point-to-Point MIMO System With 1-Bit DACs and ADCs,” *IEEE Wire. Commun. Lett.* To appear.
- [24] Y. Katsuki *et al.*, “Noncoherent Massive MIMO With Embedded One-Way Function Physical Layer Security,” *IEEE Trans. Info. Forensics and Security*, vol. 18, pp. 3158-3170, May 2023.
- [25] C. Amini *et al.*, “Relay-Aided Based Physical Layer Security in VLC System with Improved Noise Model,” *IEEE Trans. Commun.* To appear.
- [26] T. X. Zheng *et al.*, “Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers,” *IEEE Trans. Veh. Tech.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.

- [27] J. Hu *et al.*, "Artificial-noise-aided secure transmission scheme with limited training and feedback overhead," *IEEE Trans. Wire. Commun.*, vol. 16, no. 1, pp. 193–205, Jan. 2017.
- [28] A. Khazali *et al.*, "Energy Efficient Uplink Transmission in Cooperative mmWave NOMA Networks With Wireless Power Transfer," *IEEE Trans. Veh. Tech.*, vol. 71, no. 1, pp. 391-405, Jan. 2022.
- [29] C. K. Singh *et al.*, "Energy Harvesting in Overlay Cognitive NOMA Systems With Hardware Impairments," *IEEE Sys. J.*, vol. 16, no. 2, pp. 2648-2659, Jun. 2022.
- [30] A. K. Shukla *et al.*, "Performance Analysis of Energy Harvesting-Assisted Overlay Cognitive NOMA Systems With Incremental Relaying," *IEEE OJCOMS*, vol. 2, pp. 1558-1576, Jun. 2021.
- [31] Y. Liu *et al.*, "Outage Performance Analysis for SWIPT-Based Incremental Cooperative NOMA Networks With Non-Linear Harvester," *IEEE Commun. Lett.*, vol. 24, no. 2, pp. 287-291, Feb. 2020.
- [32] Q. N. Le *et al.*, "Full-Duplex Non-Orthogonal Multiple Access Cooperative Overlay Spectrum-Sharing Networks With SWIPT," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 1, pp. 322-334, Mar. 2021.
- [33] L. Ma *et al.*, "On the Performance of Full-Duplex Cooperative NOMA With Non-Linear EH," *IEEE Access*, vol. 9, pp. 145968-145976, Oct. 2021.
- [34] V. Aswathi *et al.*, "Outage and Throughput Analysis of Full-Duplex Cooperative NOMA System With Energy Harvesting," *IEEE Trans. Veh. Tech.*, vol. 70, no. 11, pp. 11648-11664, Nov. 2021.
- [35] Q. Si *et al.*, "Cooperative SM-Based NOMA Scheme With SWIPT," *IEEE Trans. Veh. Tech.*, vol. 70, no. 6, pp. 6195-6199, Jun. 2021.
- [36] C. E. Garca *et al.*, "Low-Complexity PSO-Based Resource Allocation Scheme for Cooperative Non-Linear SWIPT-Enabled NOMA," *IEEE Access*, vol. 10, pp. 34207-34220, Mar. 2022.
- [37] T. N. Tran *et al.*, "SWIPT Model Adopting a PS Framework to Aid IoT Networks Inspired by the Emerging Cooperative NOMA Technique," *IEEE Access*, vol. 9, pp. 61489-61512, Apr. 2021.
- [38] X. Liu *et al.*, "Simultaneous Wireless Information and Power Transfer Based on Symbol Allocation for GFDM-NOMA Cooperative Communications," *IEEE Wire. Commun. Lett.*, vol. 11, no. 2, pp. 333-337, Feb. 2022.
- [39] D. T. Do *et al.*, "User Grouping and Energy Harvesting in UAV-NOMA System With AF/DF Relaying," *IEEE Trans. Veh. Tech.*, vol. 70, no. 11, pp. 11855-11868, Nov. 2021.
- [40] K. Agrawal *et al.*, "NOMA With Battery-Assisted Energy Harvesting Full-Duplex Relay," *IEEE Trans. Veh. Tech.*, vol. 69, no. 11, pp. 13952-13957, Nov. 2020.
- [41] X. Li *et al.*, "Cooperative Wireless-Powered NOMA Relaying for B5G IoT Networks With Hardware Impairments and Channel Estimation Errors," *IEEE IoT J.*, vol. 8, no. 7, pp. 5453-5467, April 2021.
- [42] S. Bisen *et al.*, "On Performance of Energy Harvested Cooperative NOMA Under Imperfect CSI and Imperfect SIC," *IEEE Trans. Veh. Tech.*, vol. 70, no. 9, pp. 8993-9005, Sep. 2021.
- [43] C. Zhai *et al.*, "Nonorthogonal Multiple Access With Energy Harvesting-Based Alternate Relaying," *IEEE Sys. J.*, vol. 16, no. 1, pp. 327-338, Mar. 2022.
- [44] R. Lei *et al.*, "Secrecy Outage Performance Analysis of Cooperative NOMA Networks With SWIPT," *IEEE Wire. Commun. Lett.*, vol. 10, no. 7, pp. 1474-1478, Jul. 2021.
- [45] X. Li *et al.*, "Performance Analysis of Impaired SWIPT NOMA Relaying Networks Over Imperfect Weibull Channels," *IEEE Sys. J.*, vol. 14, no. 1, pp. 669-672, Mar. 2020.
- [46] M. Aldababsa *et al.*, "Joint Transmit-and-Receive Antenna Selection System for MIMO-NOMA With Energy Harvesting," *IEEE Sys. J.*, vol. 16, no. 3, pp. 4139-4148, Sep. 2022.
- [47] B. Lyu *et al.*, "IRS-Assisted Downlink and Uplink NOMA in Wireless Powered Communication Networks," *IEEE Trans. Veh. Tech.*, vol. 71, no. 1, pp. 1083-1088, Jan. 2022.

- [48] Q. Wu *et al.*, “IRS-assisted Wireless Powered NOMA: Do We Really Need Different Phase Shifts in DL and UL?” *IEEE Wire. Commun. Lett.*, vol. 10, no. 7, pp. 1493-1497, Jul. 2021.
- [49] D. Zhang *et al.*, “Throughput Maximization for IRS-Assisted Wireless Powered Hybrid NOMA and TDMA,” *IEEE Wire. Commun. Lett.*, vol. 10, no. 9, pp. 1944-1948, Sep. 2021.
- [50] F. D. Ardakani *et al.*, “Joint Device Pairing, Reflection Coefficients, and Power Control for NOMA Backscatter Systems,” *IEEE Trans. Veh. Tech.*, vol. 71, no. 4, pp. 4396-4411, Apr. 2022.
- [51] F. Zhao *et al.*, “Integrated Satellite-Terrestrial Networks With Coordinated C-NOMA and Relay Transmission,” *IEEE Sys. J.*, vol. 16, no. 4, pp. 5270-5280, Dec. 2022.
- [52] Study on Downlink Multiuser Superposition Transmission for LTE, 3GPP, *Shanghai, China*, Mar. 2015.
- [53] G. Chen *et al.*, “On the Performance of Cluster-based MIMO NOMA in Multi-cell Dense Networks,” *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4773-4787, Aug. 2020.
- [54] Z. Ding *et al.*, “Impact of User Pairing on 5G Nonorthogonal Multiple-Access Downlink Transmissions,” *IEEE Trans. Veh. Tech.*, vol. 65, pp. 6010-6023, Aug. 2016.
- [55] B. Fang *et al.*, “Precoding and Artificial Noise Design for Cognitive MIMOME Wiretap Channels,” *IEEE Trans. Veh. Tech.*, vol. 65, no. 8, pp. 6753–6758, Aug. 2016.
- [56] V. D. Nguyen *et al.*, “Joint Information and Jamming Beamforming for Secrecy Rate Maximization in Cognitive Radio Networks,” *IEEE Trans. Infor. Forensics and Security*, vol. 11, no. 11, pp. 2609–2623, Nov. 2016.
- [57] X. Hu *et al.*, “Secure Transmission via Jamming in Cognitive Radio Networks with Possion Spatially Distributed Eavesdroppers,” in *Proc. IEEE PIMRC*, Valencia, Spain, 4-7 Sep. 2016, pp. 1–6.
- [58] Y. Wu *et al.*, “Secure Beamforming for Cognitive Radio Networks with Artificial Noise,” in *Proc. IEEE WCSP*, Nanjing, China, 15-17 Oct. 2015, pp. 1–5.
- [59] Y. Zou, “Physical-Layer Security for Spectrum Sharing Systems,” *IEEE Trans. Wire. Commun.*, vol. 16, no. 2, pp. 1319–1329, Feb. 2017.
- [60] Z. Li *et al.*, “Cooperative Jamming for Secure Communications in MIMO Cooperative Cognitive Radio Networks,” in *Proc. IEEE ICC*, London, UK, 8-12 Jun. 2015, pp. 7609–7614.
- [61] M. Abramowitz *et al.*, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, Tenth printing ed.*, Washington, DC, USA: U.S. Government Printing Office, 1972.