*Journal of Computer Science and Cybernetics, V.41, N.x (2025), 1–*
DOI no. 10.15625/1813-9663/21772

# SECURE NOMA COMMUNICATION EAVESDROPPED BY ENERGY HARVESTING-CAPABLE RECEIVER WITH JAMMING

PHAM THI DAN NGOC[1], VO QUE SON[2], DO DAC THIEM[3,*], PHAM NGOC SON[4]

[1]*Posts and Telecommunications Institute of Technology, 11 Nguyen Dinh Chieu Street, Sai Gon Ward, Ho Chi Minh City, Viet Nam*
[2]*Ho Chi Minh City University of Technology (HCMUT), VNU-HCM, 268 Ly Thuong Kiet Street, Dien Hong Ward, Ho Chi Minh City, Viet Nam*
[3]*Thu Dau Mot University, 6 Tran Van On Street, Phu Loi Ward, Ho Chi Minh City, Viet Nam*
[4]*Ho Chi Minh City University of Technology and Education, 1 Vo Van Ngan Street, Thu Duc Ward, Ho Chi Minh City, Viet Nam*



**Abstract.** Non-orthogonal multiple access (NOMA) facilitates simultaneous transmissions of a huge quantity of wireless users on the same system resources (time, frequency, space), significantly improving spectral efficiency. Also, harvesting radio frequency energy for wireless communication not only saves energy resources but also makes communication greener. However, an energy harvesting-capable eavesdropper can be one of the NOMA receivers, threatening the security of NOMA communication. This paper secures NOMA communication eavesdropped by the energy harvesting-capable receiver by utilizing a jammer. The secrecy performance of the proposed system model is analyzed thoroughly and corroborated by computer simulations. Moreover, its secrecy performance is demonstrated to be superior to three different reference models. Furthermore, we secure the proposed system model at best by properly configuring critical system parameters.

**Keywords.** Secrecy performance, energy harvesting, jammer, non-orthogonal multiple access.

## 1. INTRODUCTION

5G/6G systems support a multitude of new wireless services, designed to satisfy critical transmission demands of a massive quantity of connected users [1,2]. Although these systems promise high data rate and ultra-low latency, they also impose difficulties, particularly in power allocation and bandwidth management as user density increases. Furthermore, ensuring reliable and secure transmission in such advanced systems is a pivotal target for system designers. To address these issues, it becomes crucial to develop mechanisms that simultaneously meliorate energy and spectral efficiencies while guaranteeing reliable and secure communication.

NOMA is deemed an effective mechanism for enhancing spectral efficiency in wireless communication [3]. NOMA can utilize spectrum efficiently by allotting various power degrees to different NOMA users and exploiting successive interference cancellation (SIC).

*Corresponding author.
*E-mail addresses*: ngocptd@ptit.edu.vn (P.T.D. Ngoc); sonvq@hcmut.edu.vn (V.Q. Son); thiemdd@tdmu.edu.vn (D.D. Thiem); sonpndtvt@hcmute.edu.vn (P.N. Son).

Thereby, NOMA is standardized for deployment in 5G and beyond, emphasizing its significance in advanced wireless communication systems wherein efficient spectrum usage is essential. Furthermore, wireless users can harvest energy from neighbouring users, leading to improved energy efficiency [4].

In [5], NOMA communication in secondary and primary systems in the context of cognitive radio was secured by artificial noise (AN) against eavesdropping of energy harvesting (EH)-capable users. The practical nonlinear EH circuits were used to demonstrate the secrecy performance of the proposed AN-injecting mechanism. However, the performance analysis of this mechanism was overlooked in [5]. Similar to [5], the authors in [6] exploited AN in securing NOMA communication, but applicable to the context of non-cognitive radio. This AN is also against the eavesdropping of EH-capable users. Moreover, the same practical nonlinear EH circuits as used in [5] were deployed in [6] to minimize the power of the proposed AN-injecting mechanism. Furthermore, [6] overlooked the performance analysis of this mechanism. Instead of considering multiple NOMA receivers and a single-antenna NOMA transmitter as in [6], the authors in [7] studied an alternative system model of two NOMA receivers and a multi-antenna NOMA transmitter. Other investigated conditions, such as EH-capable eavesdroppers, practical nonlinear EH models, no performance analysis, and non-cognitive radio context, are under the same concerns for both [6] and [7]. The authors in [8] secured NOMA communication by an active intelligent reflecting surface. Different from [5–7], the work in [8] evaluated the secrecy performance with linear EH circuits. Nonetheless, the authors in [8] also investigated the same conditions as studied in [6] and [7], such as EH-capable eavesdroppers, no performance analysis, and non-cognitive radio context. Different from [5–8] wherein the eavesdroppers are EH-capable NOMA receivers, the authors in [9] studied the scenario wherein the NOMA transmitter is capable of EH, while the eavesdropper is just an ordinary receiver without the capability of EH. The NOMA transmitter in [9] scavenges energy from a power beacon that also functions as a jammer to transmit AN to corrupt the eavesdropper for the improved secrecy performance. The performance analysis in [9] showed the advantages of the proposed system model. Recently, [10] improved the spectral efficiency of [9] by deploying full-duplex operation at the NOMA transmitter. Moreover, [10] analysed the system performance under more pivotal operation conditions than [9], such as erroneous channel estimation, imperfect hardware, and erroneous propagation in SIC. Furthermore, the results in [10] showed the superiority of the proposed NOMA communication to the traditional orthogonal multiple access (OMA) in a multitude of simulation settings.

In this paper, we secure NOMA communication against eavesdropping of EH-capable users as deemed in [5–8]. However, we deploy a dedicated jammer to transmit AN instead of transmitting AN by the NOMA transmitter as in [5–8]. This jammer can jam better than the NOMA transmitter, leading to improved secrecy performance. Furthermore, our performance analysis is valid for Nakagami-$m$ fading, which is more general than Rayleigh fading inherently deemed in [5–8]. Both analytical and simulated results demonstrate the superiority of our proposed system model to other three reference models, including [9].

The subsequent section depicts the proposed system model. Afterwards, its performance analysis is executed in Section 3. After that, Section 4. demonstrates numerous results for performance comparison and evaluation. Eventually, the paper is finalized with conclusions in Section 5.

## 2. SYSTEM MODEL

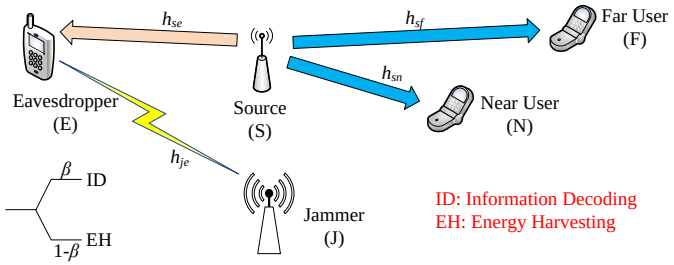



Figure 1: NOMA communication eavesdropped by an energy harvesting-capable receiver

The system model demonstrated in Figure 1 exposes a specific scenario of NOMA communication eavesdropped by an energy harvesting-capable receiver (E), but secured by a jammer (J). In the sequel, we refer to the proposed system model as NOMAwJ. It encompasses a source (S), a nearby receiver (N), and a far receiver (F), where S transmits a NOMA signal $x_s = \sqrt{\theta}x_f + \sqrt{1-\theta}x_n$ simultaneously to N and F with $x_n$ and $x_f$ being information signals purposely reserved for N and F, respectively, and $\theta$ being the NOMA-related power splitting parameter. Since F is a far (or weak) user, $\theta$ is set to be greater than 0.5 but less than 1 in according to NOMA communication. The broadcast nature of wireless propagation exposes $x_s$ to E. Therefore, to secure $x_s$ against E, J is utilized to transmit interference signals towards E. In this paper, E can be one of the NOMA receivers and can harvest radio frequency energy from S and J for its operation. E applies the power-splitting protocol not only to decode $x_n$ and $x_f$ but also to harvest energy for its own usage. More specifically, E uses $\beta$ $(0 < \beta < 1)$ percentage of its received power for decoding and the rest for energy harvesting.

Figure 1 denotes $h_{ca}$, $ca = \{sf, sn, se, je\}$, as a channel gain. This research assumes independent block frequency non-selective channels to experience Nakagami-$m$ fading with $m$ being a real number for generality. Thereby, the cumulative distribution function (CDF) and probability density function (PDF) of the power gain $g_{ca} = |h_{ca}|^2$ are respectively described to be

$$F_{g_{ca}}(z) = \frac{\gamma(m_{ca}, \kappa_{ca} z)}{\Gamma(m_{ca})} \quad \text{and} \quad f_{g_{ca}}(z) = \frac{\kappa_{ca}^{m_{ca}}}{\Gamma(m_{ca})} z^{m_{ca}-1} e^{-\kappa_{ca} z}, \tag{1}$$

wherein $\kappa_{ca} = \frac{m_{ca}}{\vartheta_{ca}}$ with $m_{ca}$ and $\vartheta_{ca} = \Xi\{g_{ca}\}$ being the fading severity and power of the Nakagami-$m$ distribution. Also, $\Xi\{\cdot\}$ and $\gamma(\cdot,\cdot)$ are the expectation operator and lower incomplete Gamma function [11]. The fading power is modelled as $\vartheta_{ca} = \varphi d_{ca}^{-\tau}$ on account of path loss with $d_{ca}$ being the transceiver separation, $\tau$ being the path loss exponent, and $\varphi$ being the reference fading power [12].

Similar to [13–17], the jamming signal $x_j$ transmitted by J is mainly to corrupt E without affecting the signal reception quality at F and N. Thereby, F and N can accurately know $x_j$. This exact prediction is supported by the fact that $x_j$ is viewed as a pseudo-random signal whose seed is known in advance at F and N. On account of $x_j$ known at F and N, the processing at F and N merely eliminates the impact of $x_j$ from the received signals at F and

N. Therefore, Figure 1 overlooks the channels from J to F and N. Briefly, F and N receive signals, respectively expressed as

$$y_f = h_{sf}\sqrt{P_s}x_s + \varepsilon_f \quad \text{and} \quad y_n = h_{sn}\sqrt{P_s}x_s + \varepsilon_n, \tag{2}$$

wherein $P_s$ is the transmission power of S (i.e., $\Xi\left\{|x_s|^2\right\} = \Xi\left\{|x_f|^2\right\} = \Xi\left\{|x_n|^2\right\} = 1$); $\varepsilon_f \sim \mathsf{CN}(0, \sigma_f)$ and $\varepsilon_n \sim \mathsf{CN}(0, \sigma_n)$ are additive noises at F and N.

On the incapability of removing the jamming signal $x_j$, E receives the signals transmitted by S and jammed by J as

$$y_e = h_{se}\sqrt{P_s}x_s + h_{je}\sqrt{P_j}x_j + \varepsilon_e, \tag{3}$$

wherein $P_j$ is the transmission power of J (i.e., $\Xi\left\{|x_j|^2\right\} = 1$) and $\varepsilon_e \sim \mathsf{CN}(0, \sigma_e)$ is additive noise at E.

The decoding process at F and N involves restoring their private information $x_f$ and $x_n$ based on the received signals $y_f$ and $y_n$. More particularly, a far user (F) utilizes a NOMA-relied decoding principle to recover its own information $x_f$ directly from $y_f$ without recovering $x_n$. This is on account of power allocation ($\theta > 0.5$), which warrants $x_f$ to be allotted more power than $x_n$. Thereby, SINR[1] for F to recover $x_f$ is computed from $y_f$ to be

$$\gamma_f^f = \frac{g_{sf}\theta P_s}{g_{sf}(1-\theta)P_s + \sigma_f}. \tag{4}$$

On account of the power allocation ($\theta > 0.5$), N first restores F's information $x_f$ while deeming $x_n$ as interference and afterwards cancels the interference posed by $x_f$ before recovering N's information $x_n$. Thereby, N decodes $x_f$ with SINR, calculated from $y_n$, as

$$\gamma_n^f = \frac{g_{sn}\theta P_s}{g_{sn}(1-\theta)P_s + \sigma_n}. \tag{5}$$

After suppressing the interference induced by $x_f$, N conducts the recovery of $x_n$. In this paper, N decodes its own signal $x_n$ only if $x_f$ has been correctly decoded at N. Thereby, $x_n$ is decoded at N with SNR[2], calculated from $y_n - h_{sn}\sqrt{P_s}x_f$, as

$$\gamma_n^n = \frac{g_{sn}(1-\theta)P_s}{\sigma_n}. \tag{6}$$

Since E is an energy harvesting-capable eavesdropper, it utilizes the $\beta$ percentage of the received power in $y_e$ to decode $x_f$ and $x_n$. More specifically, E decodes $x_f$ first from $\sqrt{\beta}y_e + \tilde{\varepsilon}_e$, wherein $\tilde{\varepsilon}_e \sim \mathsf{CN}(0, \tilde{\sigma}_e)$ is noise caused by bandpass-to-baseband conversion at E, with the SINR as

$$\gamma_e^f = \frac{g_{se}\theta P_s}{g_{se}(1-\theta)P_s + g_{je}P_j + \hat{\sigma}_e}, \tag{7}$$

where $\hat{\sigma}_e = \sigma_e + \frac{\tilde{\sigma}_e}{\beta}$.

[1]SINR means signal-to-interference plus noise ratio.

[2]SNR represents signal-to-noise ratio.

After deleting the interference injected by $x_f$, E conducts the recovery of $x_n$ under the condition that E performs this recovery only if it has already decoded $x_f$ correctly. Thereby, E decodes $x_n$ with the SNR computed from $\sqrt{\beta}y_e + \tilde{\varepsilon}_e - h_{se}\sqrt{\beta P_s}x_f$ as

$$\gamma_e^n = \frac{g_{se}\left(1-\theta\right)P_s}{g_{je}P_j + \hat{\sigma}_e}. \tag{8}$$

As seen from (7)-(8), J injects interference to E through jamming. This interference is quantified as $g_{je}P_j$, which contributes considerably to deteriorating the likelihood of successful decoding of $x_f$ and $x_n$ at E, leading to the improved secrecy performance.

## 3. ANALYTICAL RESULTS OF NOMAwJ

This section systematically conducts the reliability and secrecy performance analysis of NOMAwJ, starting with the analysis of secrecy/reliability outage probability (SOP/ROP). SOP and ROP signify the probability that channel capacity accomplished at the eavesdropping receiver (SOP) or the legal receiver (ROP) subceeds the preset data rates ($C_n$ and $C_f$ required by N and F, respectively) [10, 13, 17]. A smaller SOP indicates lower security, whereas a smaller ROP means higher reliability. After the SOP/ROP analysis, this section expands the assessment to cover secrecy/reliability throughput (ST/RT) and secrecy/reliability energy efficiency (SEE/REE).

### 3.1. ROP of F ($\Theta_f^f$)

$\Theta_f^f$ measures the likelihood that F fails to recover its individual message $x_f$. This implies that channel capacity accomplished at F for recovering $x_f$ is less than $C_f$ [10, 13, 17]

$$\Theta_f^f = \Pr\left\{\log_2\left(1+\gamma_f^f\right) < C_f\right\} = \Pr\left\{\gamma_f^f < \bar{\gamma}_f\right\}, \tag{9}$$

where $\bar{\gamma}_f = 2^{C_f} - 1$.

Inserting (4) into (9) results in

$$\Theta_f^f = \Pr\left\{\left[\theta - \bar{\gamma}_f\left(1-\theta\right)\right] g_{sf}P_s < \bar{\gamma}_f\sigma_f\right\}. \tag{10}$$

It is apparent that if $\theta - \bar{\gamma}_f\left(1-\theta\right) \leq 0$ or $\bar{\gamma}_f \geq \frac{\theta}{1-\theta}$ (i.e., complete reliability outage), then $\Theta_f^f = 1$. Otherwise, $\Theta_f^f$ is derived in closed form as

$$\Theta_f^f = F_{g_{sf}}\left(\frac{\sigma_f\bar{\gamma}_f}{\left[\theta - \bar{\gamma}_f\left(1-\theta\right)\right]P_s}\right). \tag{11}$$

### 3.2. ROP of N ($\Theta_n^n$)

It is reminded that N decodes $x_n$ only if $x_f$ has been successfully decoded by it. Thereby, $\Theta_n^n$ measures the complementary probability of the event that N decodes correctly both $x_n$ and $x_f$ [10, 13, 17]

$$\Theta_n^n = 1 - \Pr\left\{\gamma_n^f \geq \bar{\gamma}_f, \gamma_n^n \geq \bar{\gamma}_n\right\}, \tag{12}$$

where $\bar{\gamma}_n = 2^{C_n} - 1$.

Plugging (6) into (12) results in

$$\Theta_n^n = 1 - \Pr\left\{\left[\theta - (1-\theta)\,\bar{\gamma}_f\right] P_s g_{sn} \geq \sigma_n \bar{\gamma}_f, (1-\theta)\, P_s g_{sn} \geq \sigma_n \bar{\gamma}_n\right\}. \tag{13}$$

It is obvious that if $\theta - \bar{\gamma}_f\,(1-\theta) \leq 0$ or $\bar{\gamma}_f \geq \frac{\theta}{1-\theta}$ (i.e., complete reliability outage), then $\Theta_n^n = 1$. Otherwise, $\Theta_n^n$ is derived in closed form as

$$\begin{aligned}\Theta_n^n &= 1 - \Pr\left\{g_{sn} \geq \max\left(\frac{\sigma_n \bar{\gamma}_f}{\left[\theta - \bar{\gamma}_f\,(1-\theta)\right] P_s}, \frac{\sigma_n \bar{\gamma}_n}{(1-\theta)\, P_s}\right)\right\} \\ &= F_{g_{sn}}\left(\frac{\sigma_n}{P_s} \max\left(\frac{\bar{\gamma}_f}{\theta - \bar{\gamma}_f\,(1-\theta)}, \frac{\bar{\gamma}_n}{1-\theta}\right)\right).\end{aligned} \tag{14}$$

*Remark 1*: On the account that $\bar{\gamma}_f = 2^{C_f} - 1$, $\Theta_f^f$ and $\Theta_n^n$ illustrate that F and N suffer various outage degrees on account of the configuration of the preset data rate ($C_f$) and the NOMA-based power splitting parameter ($\theta$). In particular, if $C_f$ and $\theta$ are configured unreasonably to lead to $\bar{\gamma}_f \geq \frac{\theta}{1-\theta}$, F and N incur total outage, i.e., $\Theta_f^f = \Theta_n^n = 1$. Notwithstanding, total outage of F and N can be hindered by appropriately configuring $C_f$ and $\theta$ to lead to $\bar{\gamma}_f < \frac{\theta}{1-\theta}$. Alternatively, NOMAwJ restrains the preset data rate to lead to $C_f < -\log_2(1-\theta)$ in order to cancel total outage for F and N. This restriction warrants that the attainable rate for F remains below the peak allowable rate determined by system parameters, thereby hindering total outage and warranting reliable transmission for F and N. Since N decodes its own information $x_n$ after successfully decoding F's information $x_f$, both total reliability outage events for N and F are only on account of $C_f$.

*Remark 2*: (11) and (14) illustrate that the reliability performance of both F and N in NOMAwJ is impacted by a multitude of specifications, encompassing ($C_f$, $C_n$, $\theta$, $\beta$, $P_s$, $P_j$). Thereby, configuring these specifications allows NOMAwJ to reach preset reliability targets.

### 3.3. SOP at E

#### 3.3.1. SOP for $x_f$

$\Theta_e^f$ measures the likelihood that E fails to restore F's message ($x_f$). This implies the channel capacity attainable at E for decoding $x_f$ is less than $C_f$ [10, 13, 17]

$$\Theta_e^f = \Pr\left\{\log_2\left(1 + \gamma_e^f\right) < C_f\right\} = \Pr\left\{\gamma_e^f < \bar{\gamma}_e^f\right\}. \tag{15}$$

Substituting (7) into (15) yields

$$\Theta_e^f = \Pr\left\{\left[\theta - \bar{\gamma}_f\,(1-\theta)\right] g_{se} P_s < \left(g_{je} P_j + \hat{\sigma}_e\right) \bar{\gamma}_f\right\}. \tag{16}$$

It is definite that if $\theta - \bar{\gamma}_f\,(1-\theta) \leq 0$ or $\bar{\gamma}_f \geq \frac{\theta}{1-\theta}$ (i.e. complete security outage), then $\Theta_e^f = 1$. Otherwise, $\Theta_e^f$ is derived in closed-form as

$$\Theta_e^f = \Pr\left\{g_{se} < \frac{\left(g_{je} P_j + \hat{\sigma}_e\right) \bar{\gamma}_f}{\left[\theta - \bar{\gamma}_f\,(1-\theta)\right] P_s}\right\} = \Psi\left(H_f, K_f\right), \tag{17}$$

where $H_f = \frac{P_j \bar{\gamma}_f}{\left[\theta - \bar{\gamma}_f(1-\theta)\right] P_s}$ and $K_f = \frac{\hat{\sigma}_e \bar{\gamma}_f}{\left[\theta - \bar{\gamma}_f(1-\theta)\right] P_s}$.

The function $\Psi(U,V) = \Pr\{g_{se} < g_{je}U + V\}$ is computed as

$$\Psi(U,V) = \int_0^{\infty} F_{g_{se}}(Uz+V) f_{g_{je}}(z)\, dz. \tag{18}$$

By performing a variable transformation $z = \tan y$, (18) is further written as

$$\Psi(U,V) = \int_0^{\frac{\pi}{2}} F_{g_{se}}(U\tan y + V) f_{g_{je}}(\tan y)(\cos y)^{-2} dy. \tag{19}$$

By applying Gaussian-Chebyshev quadrature in [18] with the factor $L$ indicating the precision-complexity compromise, the tight approximation of (19) is given as

$$\Psi(U,V) = \frac{\pi^2}{4L}\sum_{u=1}^{L}\sqrt{1-\varpi_u^2}(\cos\delta_u)^{-2} F_{g_{se}}(U\tan\delta_u + V) f_{g_{je}}(\tan\delta_u), \tag{20}$$

wherein $\varpi_u = \cos\left(\frac{2u-1}{2L}\pi\right)$ and $\delta_u = \frac{\pi}{4}(\varpi_u + 1)$.

### 3.3.2. SOP for $x_n$

It is reminded that E decodes $x_n$ only if $x_f$ has been successfully decoded by it. Thereby, $\Theta_e^n$ measures the complementary probability of the event that E decodes correctly both $x_n$ and $x_f$ [10, 13, 17]

$$\Theta_e^n = 1 - \Pr\left\{\gamma_e^f \geq \bar{\gamma}_f, \gamma_e^n \geq \bar{\gamma}_n\right\}. \tag{21}$$

Substituting (8) into (21) yields

$$\Theta_e^n = 1 - \Pr\left\{\left[\theta - (1-\theta)\bar{\gamma}_f\right] P_s g_{se} \geq (g_{je}P_j + \hat{\sigma}_e)\bar{\gamma}_f, (1-\theta) P_s g_{se} \geq (g_{je}P_j + \hat{\sigma}_e)\bar{\gamma}_n\right\}. \tag{22}$$

It is apparent that if $\theta - \bar{\gamma}_f(1-\theta) \leq 0$ or $\bar{\gamma}_f \geq \frac{\theta}{1-\theta}$ (i.e., complete security outage), then $\Theta_e^n = 1$. Otherwise, $\Theta_e^n$ is derived in closed form as

$$\Theta_e^n = \Pr\left\{g_{se} < \frac{g_{je}P_j + \hat{\sigma}_e}{P_s}\max\left(\frac{\bar{\gamma}_f}{\theta - \bar{\gamma}_f(1-\theta)}, \frac{\bar{\gamma}_n}{1-\theta}\right)\right\} = \Psi(H_n, K_n), \tag{23}$$

where $H_n = \frac{P_j}{P_s}\max\left(\frac{\bar{\gamma}_f}{\theta-\bar{\gamma}_f(1-\theta)}, \frac{\bar{\gamma}_n}{1-\theta}\right)$ and $K_n = \frac{\hat{\sigma}_e}{P_s}\max\left(\frac{\bar{\gamma}_f}{\theta-\bar{\gamma}_f(1-\theta)}, \frac{\bar{\gamma}_n}{1-\theta}\right)$.

*Remark 3*: On the account that $\bar{\gamma}_f = 2^{C_f} - 1$, $\Theta_e^f$ and $\Theta_e^n$ expose that E suffers a multitude of secrecy outage degrees when overhearing F's and N's messages on account of the configuration of the preset data rate ($C_f$) and the NOMA-based power splitting parameter ($\theta$). In particular, E experiences total secrecy outage (indicating that N's and F's messages are absolutely secured) if $C_f$ and $\theta$ are configured appropriately to lead to $\bar{\gamma}_f \geq \frac{\theta}{1-\theta}$. Notwithstanding, total secrecy outage does not happen if $C_f$ and $\theta$ are set inappropriately to lead to $\bar{\gamma}_f < \frac{\theta}{1-\theta}$. Alternatively, NOMAwJ warrants a lower bound on the preset data rate to lead to $C_f \geq -\log_2(1-\theta)$ in order to obtain absolute security for N's and F's messages. This lower bound warrants the attainable rate for F to remain above the peak allowable

rate determined by the system parameters, thereby E experiences total secrecy outage and NOMAwJ makes sure to reach absolute security for N's and F's messages. Since E decodes $x_n$ after successfully decoding $x_f$, both total secrecy outage events for E in decoding $x_n$ and $x_f$ are only on account of $C_f$.

*Remark 4*: (17) and (22) reveil that the secrecy performance of both F and N in NOMAwJ is affected by a multitude of specifications, encompassing ($C_f$, $C_n$, $\theta$, $\beta$, $P_s$, $P_j$). Thereby, configuring these specifications allows NOMAwJ to reach preset security targets.

### 3.4. Secrecy/reliability throughput

Under delay restriction, the throughput for NOMAwJ is simply computed from the ROP/SOP as [10]

$$\Delta_u^v = C_v \left(1 - \Theta_u^v\right), \tag{24}$$

where $u = \{e, n, f\}$, $v = \{n, f\}$ and $\Delta_u^v$ is the throughput of $v$ whose information is recovered at $u$. More specifically, $\Delta_e^n$ and $\Delta_e^f$ are respectively STs of N and F, whereas $\Delta_n^n$ and $\Delta_f^f$ are correspondingly RTs of N and F.

Obviously, RT/ST in NOMAwJ, as computed by (24), is jointly influenced by a set of specifications ($C_f$, $C_n$, $\theta$, $\beta$, $P_s$, $P_j$) since this set impacts $\Theta_u^v$. Thereby, accomplishing the preset RT/ST requires properly configuring and flexibly controlling this set.

### 3.5. Secrecy/reliability energy efficiency

Two pivotal metrics which quantify energy utilization efficiency to attain a preset data rate are REE and SEE. They are respectively computed for NOMAwJ as [**?**]

$$\Phi_{rel} = \frac{\Delta_n^n + \Delta_f^f}{P_s + P_j} \quad \text{and} \quad \Phi_{sec} = \frac{\Delta_e^n + \Delta_e^f}{P_s + P_j}. \tag{25}$$

### 3.6. Performance limit

The following lets $P_j = \lambda P_s$. Investigating the performance upper-bound, which represents the best achievable outcome under ideal conditions, confers comprehensive insights into theoretical limits. This subsection examines the performance limit of NOMAwJ in contexts wherein the transmit power $P_s$ of S approaches infinity, i.e., $P_s \to \infty$. As $P_s \to \infty$, the SINRs for decoding $x_f$ at F, $x_f$ at N, $x_n$ at N, $x_f$ at E, and $x_n$ at E, are straightforwardly inferred as $\tilde{\gamma}_f^f = \frac{\theta}{1-\theta}$, $\tilde{\gamma}_n^f = \frac{\theta}{1-\theta}$, $\tilde{\gamma}_n^n = \infty$, $\tilde{\gamma}_e^f = \frac{g_{se}\theta}{g_{se}(1-\theta)+g_{je}\lambda}$, and $\tilde{\gamma}_e^n = \frac{g_{se}(1-\theta)}{g_{je}\lambda}$. By carrying out the procedure in the previous subsections, one obtains the ROPs of N and F as well as the SOP of $x_n$ and $x_f$ as

$$\tilde{\Theta}_f^f = \Pr\left\{\tilde{\gamma}_f^f < \bar{\gamma}_f\right\} = \begin{cases} 0, & \bar{\gamma}_f < \frac{\theta}{1-\theta} \\ 1, & \bar{\gamma}_f \geq \frac{\theta}{1-\theta} \end{cases}, \tag{26}$$

$$\tilde{\Theta}_n^n = 1 - \Pr\left\{\tilde{\gamma}_n^f \geq \bar{\gamma}_f, \tilde{\gamma}_n^n \geq \bar{\gamma}_n\right\} = \begin{cases} 0, & \bar{\gamma}_f < \frac{\theta}{1-\theta} \\ 1, & \bar{\gamma}_f \geq \frac{\theta}{1-\theta} \end{cases}, \tag{27}$$

$$\tilde{\Theta}_e^f = \begin{cases} \Psi\left(\frac{\lambda\bar{\gamma}_f}{\theta - \bar{\gamma}_f(1-\theta)}, 0\right), & \bar{\gamma}_f < \frac{\theta}{1-\theta} \\ 1, & \bar{\gamma}_f \geq \frac{\theta}{1-\theta} \end{cases}, \tag{28}$$

$$\tilde{\Theta}_e^n = \begin{cases} \Psi\left(\lambda \max\left(\frac{\bar{\gamma}_f}{\theta-\bar{\gamma}_f(1-\theta)}, \frac{\bar{\gamma}_n}{1-\theta}\right), 0\right), & \bar{\gamma}_f < \frac{\theta}{1-\theta} \\ 1, & \bar{\gamma}_f \geq \frac{\theta}{1-\theta} \end{cases}. \tag{29}$$

## 4. DEMONSTRATIVE RESULTS

To produce the results presented in this section, MATLAB software is used even though other software, such as MATHEMATICA, is also used. Moreover, to evaluate the secrecy performance of the proposed model (NOMAwJ), we compare its performance with three reference ones: 1) Model 1 (OMAwJ): OMA with jamming where S sequentially transmits $x_f$ and $x_n$ to F and N, respectively, in two equal-duration phases, each lasting $T/2$; Model 2 (NOMAnJ): NOMA without jamming where J is not available; Model 3 (Ref) in [9]: NOMA with jamming where S plays a dual role by harvesting energy from J in a $T/2$-duration phase and transmitting the NOMA signal to N and F in another $T/2$-duration phase. The function of E is the same in all four models under investigation, where it harvests energy along with eavesdropping on legitimate information, but suffers interference from J. In a fair comparison in terms of total system power ($P_t$), both NOMAwJ and Model 1 set $P_s$ and $P_j$ such that $P_s + P_j = P_t$, whereas NOMAnJ and Ref set $(P_s = P_t, P_j = 0)$ and $(P_s = 0, P_j = P_t)$, respectively.

The throughput gap, represented as $\mathrm{Tg_M}$, is employed as a critical performance metric for comparison among the above models, i.e., M = {NOMAwJ, OMAwJ, NOMAnJ, Ref}. It is the subtraction of the total reliability throughput from the total security throughput, i.e., $\mathrm{Tg_M} = \left(\Delta_n^n + \Delta_f^f\right) - \left(\Delta_e^n + \Delta_e^f\right)$. It behaves in the same manner as secrecy capacity [19]. Thereby, a higher $\mathrm{Tg_M}$ means higher security. The subsequent results in Figures 2-5b demonstrate the consistency between the analytical and simulation results, validating the accuracy of the derived expressions in Section 3. This consistency ensures confidence in the analytical framework and provides insights into the secrecy performance of the proposed model in comparison to its three references under various conditions.

Except as otherwise provided, the parameters used are: S $(0, 0)$, N $(60, 0)$, F $(80, 10)$, E $(70, -20)$, J $(30, -15)$, the reference fading power $\varphi = -20$ dB, the energy converting efficiency of 0.6 for the energy harvester in [9], the path-loss decay $\tau = 2.8$, the preset data rates $C_f = C_n = C = 2$ bps/Hz, the EH-related power splitting parameter $\beta = 0.6$, the power ratio $P_s/P_t = 0.5$ for NOMAwJ and OMAwJ, the noise power $\sigma_n = \sigma_f = \sigma_e = \tilde{\sigma}_e = -90$ dBm, the fading severity $m_{iv} = m = 1.5$ for any $iv$, the NOMA-related power splitting parameter $\theta = 0.9$, and the total system power $P_t = 10$ dBm.

The secrecy performance comparison among the four investigated models (NOMAwJ, OMAwJ, NOMAnJ, and Ref) with respect to (wrt) $P_t$ is shown in Figure 2. We recognize that the proposed model (NOMAwJ) attains a dramatically higher throughput gap than the three reference models (OMAwJ, NOMAnJ, and Ref), showing the superiority of the proposed model in terms of secrecy capability. In addition, the model without jamming (NOMAnJ) has degraded security, whereas the models with jamming (OMAwJ and NOMAwJ) have improved security wrt the increase in $P_t$. In the meantime, Ref, where S harvests energy from J for its operation, has the worst security.

Figure 3 shows the secrecy performance comparison among the four investigated models wrt $\theta$, which represents the fraction of $P_s$ allocated to transmit $x_f$. One sees that the proposed model reaches the peak security when the power allocation in the NOMA transmission

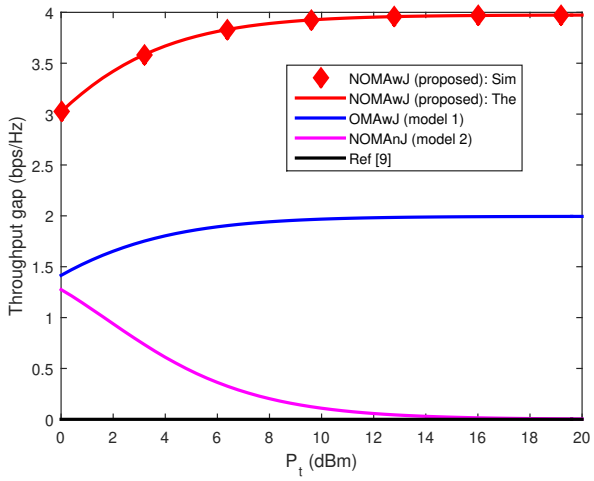



Figure 2: Throughput gap with wrt $P_t$. 'Sim' and 'The' stand for 'Simulation' and 'Theory', respectively, where 'Simulation' is obtained from Monte-Carlo simulations and 'Theory' is attained from expressions derived in Section 3.

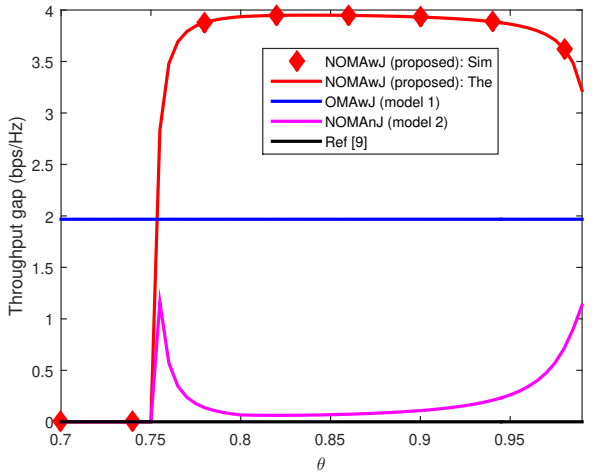
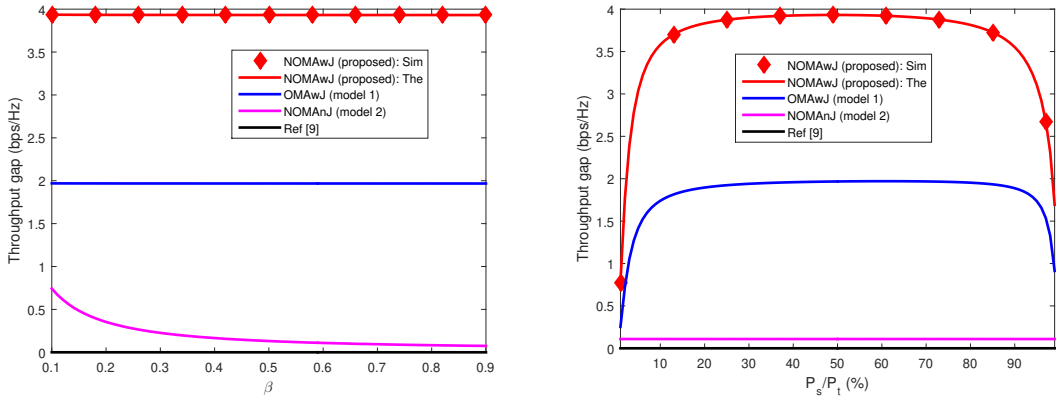



Figure 3: Throughput gap wrt $\theta$

is optimal, e.g., $\theta = 0.835$. However, this model also experiences the zero throughput gap when this power allocation is inappropriate, e.g., $\theta \leq 0.75$. This result originates from the analytical result in Section 3 that the SOP/ROP is 1 when $\bar{\gamma}_f \geq \frac{\theta}{1-\theta}$. This inequality yields $\theta \leq 1 - 2^{-C}$. Given the parameters in this section, we straightforwardly infer that $\theta \leq 0.75$ makes the SOP/ROP equal to 1, or the throughput gap is zero. Moreover, OMAwJ is independent of $\theta$ due to the nature of OMA. As such, while the proposed model is significantly more secure than the two reference models (NOMAnJ and Ref) for any $\theta$, it just outperforms OMAwJ for $\theta \geq 0.753$. The range of $\theta \geq 0.753$ is reasonable for the NOMA transmission since the SIC is efficacious when there is a large difference in power allocated to transmit




(a) Throughput gap wrt $\beta$ (b) Throughput gap wrt $P_s/P_t$

Figure 4: Effects of $\beta$ and $P_s/P_t$ on throughput gap

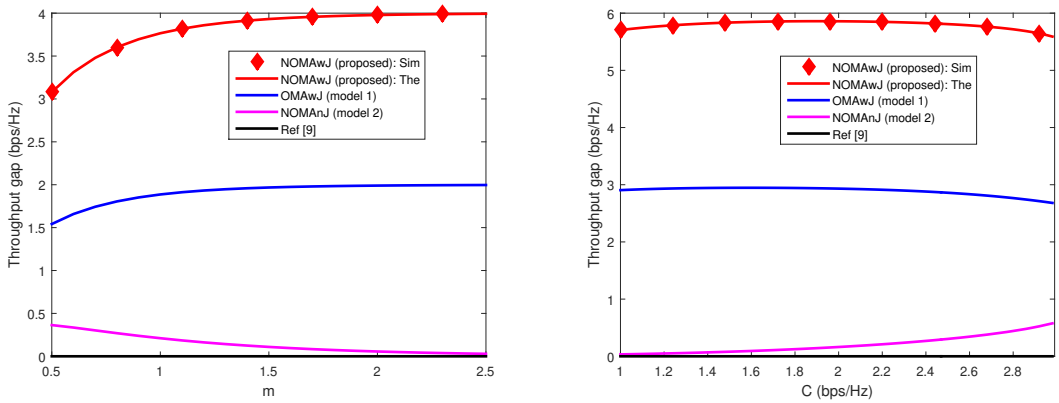
individual NOMA signals ($x_f$ and $x_n$), i.e., $\theta$ must be large. In the meantime, Ref, where S harvests energy from J for its operation, has the worst security.

Figure 4a performs the secrecy performance comparison among the four investigated models wrt $\beta$, which represents the fraction of the power reserved for decoding information at E. We recognize that only the model without jamming (NOMAnJ) has degraded secrecy performance wrt the increase in $\beta$ while other models (NOMAwJ, OMAwJ, and Ref) are almost independent of $\beta$. This result is reasonable since the jamming power almost deteriorates the decoding capability of E irrespective of how much the harvested power is reserved for decoding at E. Furthermore, similar to the previous results, the proposed model attains significantly superior secrecy performance to three reference models for all values of $\beta$. In the meantime, Ref, where S harvests energy from J for its operation, has the worst security.

Figure 4b makes the secrecy performance comparison among the four investigated models wrt $P_s/P_t$, which represents the percentage of the total power allocated to S. We recognize that the secrecy capability of the model without jamming (NOMAnJ) is unchanged wrt the increase of $P_s/P_t$, as expected. Moreover, similar to the previous results, the proposed model has better secrecy performance than the other models (OMAwJ, NOMAnJ, and Ref). Furthermore, the secrecy capability of the models with jamming (OMAwJ and NOMAwJ) can be maximized by properly selecting $P_s/P_t$; for example, Figure 4b shows the peak throughput gap at $P_s/P_t = 49\%$. In the meantime, Ref, where S harvests energy from J for its operation, has the worst security.

The secrecy performance comparison among the four investigated models with respect to (wrt) $m$, which represents the fading severity, is shown in Figure 5a. One sees that the proposed model (NOMAwJ) has considerably higher throughput gap than the three reference models (OMAwJ, NOMAnJ, and Ref), showing the superiority of the proposed model in terms of the secrecy capability. Additionally, the model without jamming (NOMAnJ) has degraded security, whereas the models with jamming (OMAwJ and NOMAwJ) have improved security wrt the increase in $P_t$. In the meantime, Ref, where S harvests energy from J for its operation, has the worst security.

Figure 5b performs the secrecy performance comparison among the four investigated




(a) Throughput gap wrt $m$ (b) Throughput gap wrt $C$

Figure 5: Effects of $m$ and $C$ on throughput gap

models wrt $C$, which means the required spectral efficiency. We recognize that the secrecy capability of the proposed model (NOMAwJ) reaches the peak value when $C$ is configured at 1.9 bps/Hz. In the meantime, OMAwJ has degraded secrecy performance, whereas NOMAnJ has improved secrecy performance wrt the increase of $C$. However, similar to the previous results, the proposed model has a significantly higher secrecy performance than the other reference models (OMAwJ, NOMAnJ, and Ref). Also, Ref, where S harvests energy from J for its operation, still has the worst security.

## 5. CONCLUSIONS

This paper concentrated on the secrecy analysis of the recommended system model, where the NOMA transmission is secured by the jammer while the eavesdropper is an illegal receiver with the capability of energy harvesting. The proposed analysis is confirmed by a Monte-Carlo simulation. The results unveil the superiority of the proposed system model to the other three reference models. Moreover, the secrecy capability of the proposed model can be optimized with a proper configuration of system parameters.

## ACKNOWLEDGMENTS

This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2023.45.

## REFERENCES

[1] Y. Ahn, J. Kim, S. Kim, S. Kim, and B. Shim, "Sensing and computer vision-aided mobility management for 6g millimeter and terahertz communication systems," *IEEE Transactions on Communications*, vol. 72, no. 10, pp. 6044–6058, 2024, https://doi:10.1109/TCOMM.2024.3392799.

[2] M. Shoaib, G. Husnain, N. Sayed, and S. Lim, "Unveiling the 5g frontier: Navigating challenges, applications, and measurements in channel models and implementations," *IEEE Access*, vol. 12, no. 4, pp. 59 533–59 560, 2024, https://doi:10.1109/ACCESS.2024.3392761.

[3] G. S. Perera, D. Y. Senanayake, V. Basnayake, and D. N. K. Jayakody, "Dynamic spectrum fusion: An adaptive learning approach for hybrid noma/oma in evolving wireless networks," in *International Conference on Advanced Research in Computing (ICARC) Belihuloya, Sri Lanka*, 2024, pp. 253–258, https://doi:0.1109/ICARC61713.2024.10499705.

[4] A. Essa, E. Almajali, R. E. A. S. Mahmoud, S. S. Alja'Afreh, and M. Ikram, "Wireless power transfer for implantable medical devices: Impact of implantable antennas on energy harvesting," *IEEE Open Journal of Antennas and Propagation,*, vol. 5, no. 3, pp. 739–758, 2024, https://doi:10.1109/OJAP.2024.3392160.

[5] F. Zhou, Z. Chu, H. Sun, and V. C. M. Leung, "Resource allocation for secure miso-noma cognitive radios relying on swipt," in *EEE International Conference on Communications (ICC), Kansas City, MO, USA*, 2018, pp. 1–6, https://doi:10.1109/ICC.2018.8422849.

[6] J. Zhou, Y. Sun, Q. Cao, S. Li, Z. Sun, and X. Wang, "Power minimization for secure multi-user miso noma system with energy harvesting," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 10 046–10 058, 2020, https://doi:10.1109/TVT.2020.3005143.

[7] F. Zhou, Z. Chu, H. Sun, and V. C. M. Leung, "Nhancing phy security of MISO NOMA SWIPT systems with a practical non-linear EH model," in *EEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA*, 2018, pp. 1–6, https://doi:10.1109/ICCW.2018.8403565.

[8] . Zhai, L. Dong, Y. Li, and W. Cheng, "Secure communications via active IRS assisted SWIPT NOMA networks," *IEEE Systems Journal*, vol. 18, no. 2, pp. 1032–1043, 2024, https://doi:10.1109/JSYST.2024.3365590.

[9] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, H. Hu, and F. Gong, "Achieving reliable and secure communications in wireless-powered NOMA systems," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1978–1983, 2021.

[10] T. Le-Thanh and K. Ho-Van, "Ecured NOMA full-duplex transmission with energy harvesting," *IEEE Access*, vol. 12, pp. 91 342–91 356, 2024, https://doi:10.1109/ACCESS.2024.3421353.

[11] I. S. Gradshteyn and R. I. M, *Table of Integrals, Series and Products*. San Diego: 7th ed., CA: Academic, 2007, https://doi:10.1016/C2009-0-22516-5.

[12] D. Wang, F. Rezaei, and C. Tellambura, "Performance analysis and resource alloca tions for a WPCN with a new nonlinear energy harvester model," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1403–1424, 2020, https://doi:10.1109/OJCOMS.2020.3022316.

[13] T. Le-Thanh and K. Ho-Van, "Jamming-and-relaying strategy for non-linear energy scavenging networks," *Arabian Journal for Science and Engineering*, vol. 48, no. 11, pp. 14 621–14 638, 2023, https://doi:10.1007/s13369-023-07832-7.

[14] K. Ho-Van and T. Do-Dac, "Joint effects of non-linear energy harvesting, primary interference, and full-duplex destination-assisted jamming on spectrum sharing networks," *Wireless Networks*, vol. 29, no. 1, pp. 221–234, 2023, https://doi:10.1007/s11276-022-03119-1.

[15] M. Li, Y. Huang, H. Yin, Y. Wang, and C. Cai, "Improving the security and spectrum efficiency in overlay cognitive full-duplex wireless networks," *IEEE Access*, vol. 7, pp. 68 359–68 372, 2019, https://doi:10.1109/ACCESS.2019.291861.

[16] K. Agrawal, M. F. Flanagan, and S. Prakriya, "Noma with battery-assisted energy harvesting full-duplex relay," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 952–13 957, 2020, https://doi:10.1109/TVT.2020.3021085.

[17] K. Ho-Van, "Jammer selection for energy harvesting-aided non-orthogonal multiple access: Performance analysis," *Peer-to-Peer Networking and Applications*, vol. 16, no. 5, pp. 2438–2455, 2023, https://doi:10.1007/s12083-023-01542-5.

[18] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. 10th printing ed., Washington, DC, USA: U.S. Government Printing Office: Publishing House for Science and Technology, Vietnam Academy of Science and Technology, 1972.

[19] K. Ho-Van, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, S. K. Yoo, Y. A. Brychkov, O. A. Dobre, and M. Valkama, "Security improvement for energy harvesting based overlay cognitive networks with jamming-assisted full-duplex destinations," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12 232–12 237, 2021.

*Received on October 29, 2024*
*Accepted on September 09, 2025*