On Secrecy Analysis of UAV-Enabled Relaying NOMA Systems with RF Energy Harvesting

Anh-Nhat Nguyen[1(✉)], Dac-Binh Ha[2], Van-Truong Truong[2], Chakchai So-In[1], Phet Aimtongkham[1], Chinapat Sakunrasrisuay[1], and Chatchai Punriboon[1]

[1] Department of Computer Science, Khon Kaen University, Khon Kaen 40002, Thailand
{nguyenanhnhat,chinapat.s,chatchai}@kkumail.com, {chakso,phetim}@kku.ac.th
[2] Faculty of Electrical-Electronics Engineering, Duy Tan University, Danang 550000, Vietnam
hadacbinh@duytan.edu.vn, truongvantruong@dtu.edu.vn

Abstract. This paper investigates the physical-layer security (PLS) for the Internet of Things (IoT) using nonorthogonal multiple access (NOMA) with an unmanned aerial vehicle (UAV)-enabled relaying (UR) cluster in an urban environment. Consider a scenario where two energy-limited IoT device (ID) clusters can use radio frequency (RF) energy harvesting (EH) to send messages to a destination with the help of a UR cluster in the presence of a passive eavesdropper. We propose a UR and ID selection scheme, as well as the usage of artificial noise (AN), to increase the PLS performance of system. As a result, closed-form closed-form secrecy outage probability (SOP) expressions are derived. The effects of network parameters on secrecy performance are also investigated to better understand the NOMA UR system with NOMA UR. Finally, the accuracy of our analysis is verified by Monte-Carlo simulation results.

Keywords: Internet of Things · Unmanned aerial vehicles · Radio frequency energy harvesting · Nonorthogonal multiple access · Physical layer security

1 Introduction

Unmanned aerial vehicles (UAVs) can provide advanced services for edge-enabled Internet of Things (IoT) applications, such as communication relays for ubiquitous connectivity to ground IDs, due to their advantages of controllable mobility, flexible deployment, and strong Line-of-Sight (LoS) channels [1–3]. For example, the authors of [2] proposed a UAV-enabled relaying (UR) network with a UAV acting as a decode-and-forward (DF) relay. In [3], Liang *et al.* studied an amplify-and-forward (AF) UR network with the channels between the UR and ground devices modeled as LoS propagation.

N.-S. Vo et al. (Eds.): INISCOM 2022, LNICST 444, pp. 267–281, 2022.
https://doi.org/10.1007/978-3-031-08878-0_19

IDs often use rechargeable batteries to keep networks connected. Batteries must be recharged regularly to ensure continuous operation. For energy-limited devices, a new technology is known as radio frequency (RF) energy harvesting [4,5] has emerged to extend and increase battery life [6]. Because of their mobility and adaptability, UR provides wireless power transfer (WPT) to ID while also collecting and transmitting data to the target [7,8]. In [7] investigated UR use DF scheme in IoT network network, in which UR first power many IDs via WPT, and then IDs harvest energy to transmit data to UR. Similar to the model in [7,8] employed both DF and AF schemes to UR.

Recently, nonorthogonal multiple access (NOMA) has much potential to improve IDs' transmission efficiency and connectivity [9]. Through superposition coding and successive interference cancellation (SIC), NOMA improves system throughput and spectral efficiency by enabling multi-user spectrum sharing [10]. NOMA has been applied in several scenarios, with UAV-assisted NOMA being a promising IoT solution [11]. Jiang *et al.* employ a NOMA DF UR to ferry data from a remote base station (BS) to multiple ground IDs. Moreover, in [12] analyzed the performance of a NOMA DF UR-assisted WPT network, where the UR is used as RF power transmitter and as a communication relay between EH IDs and a BS.

In addition, the communication between the UAV and IDs may be eavesdropped on by nearby eavesdroppers, and the communication links may be attacked due to wireless signal propagation characteristics. Thus, the secrecy of UAV-based communication is a significant aspect affecting system performance [13]. In this context, PLS can protect wireless data transmissions without requiring secret keys or sophisticated algorithms, making it more suited for low cost IDs [14]. For example, Wang *et al.* suggested a mobile relaying strategy with four nodes: source, destination, UR, and eavesdropper [15]. In [16], the secrecy performance of simultaneous wireless information and power transfer UR system was studied using both AF and DF schemes.

Motivated by the above discussion, the secrecy performance for IoT systems deploying RF EH NOMA UR over Rayleigh fading channels is studied in this paper. In addition, we consider the probability of LoS and non-LoS (NLoS) for UR-ground device wireless channels. Furthermore, we consider the imperfect SIC (iSIC) component to ensure that the model is as close to reality. The following are our paper's main contributions:

- We propose the UR-ID selection scheme to improve system secrecy performance by using the (AN) generated by the selected UR to enhance the PLS.
- We derive closed-form expressions of SOP for each ID cluster and the entire system.
- The system secrecy performance is examined by numerical results to verify the efficiency of our system.

The remainder of this paper is organized as follows. In Section 2, the system model, the communication protocol are introduced. In Sect. 3, the SOPs are analyzed. In Sect. 4, numerical results are presented and discussed. Finally, conclusions are presented in Sect. 5.

2 System Model and Communication Protocol

2.1 System and Channel Model

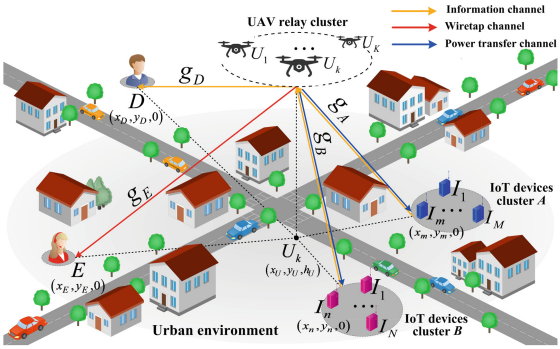

Fig. 1. System model for an RF EH NOMA UR system.

As illustrated in Fig. 1, we consider an RF EH NOMA UR system in which two clusters of energy-limited ID (i.e. cluster A has M high-priority devices, denoted by $I_m, 1 \leq m \leq M$ and cluster B has N low-priority devices, denoted by $I_n, 1 \leq n \leq N$) wish to send confidential information to a ground destination D through a UR cluster of K elements, denoted by $U_k, 1 \leq k \leq K$, in the presence of a passive eavesdropper E. There are no direct links between the IDs and D because of the presence of barriers in the urban environment. We assume that all devices with a single antenna operate in half-duplex mode and that the URs use the DF scheme [17]. The Rayleigh distribution is used to characterize the small-scale fading of the channel coefficient h_{ab}, i.e., the channel power gain $|h_{ab}|^2$ is a random variable (RV) that follows an exponential distribution with parameter λ_{ab}, where ab is the link $a \rightarrow b$, $ab \in \{I_m U_k, I_n U_k, U_k D, U_k E\}$. For clarity, we define the notations adopted throughout the remainder of this paper in Table 1.

Without loss of generality, we use a three-dimensional Cartesian coordinate system where D, E, and $I_i, i \in (m, n)$ are on the ground with coordinates $D\,(x_D, y_D, 0)$, $E\,(x_E, x_E, 0)$, and $I_i\,(x_i, x_i, 0)$, respectively. The U_k is fixed at $H_{U_k} > 0$ [13], and its location is $U_k\,(x_{U_k}, y_{U_k}, H_{U_k})$. Assume that the large-scale fading of the channel between the UAV and ground devices is based on the probabilistic LoS and NLoS model [18], which is influenced by building density and distance between the U_k and ground devices. The likelihood of devices seeing a LoS link is expressed as [18]

$$\begin{cases} P_{LoS}\,(ab) & = \dfrac{1}{1 + \nu \exp\left(-\upsilon\left[\theta_{ab} - \nu\right]\right)}, \\ P_{NLoS}\,(ab) & = 1 - P_{LoS}\,(ab)\,, \end{cases} \tag{1}$$

Table 1. Notation

Notation	Meaning	Notation	Meaning
M	Number of IDs in cluster A	I_A^*	The best ID in cluster A
N	Number of IDs in cluster B	I_B^*	The best ID in cluster B
K	Number of URs in cluster UR	U^*	The best UR in cluster UR
T	Transmission block time	α	Time switching ratio (TSR)
P_U	Transmit power of UR	η	Energy conversion efficiency
ρ_0, $1-\rho_0$	Power allocation coefficient for transmitted signal from I_A^* and I_B^* to U^*	ρ_A, ρ_B, ρ_J	Power allocation coefficient for signal x_A, signal x_B, and AN from U^* to D
ϵ_0	The cancellation error factor with iSIC at UR	ϵ_1	The cancellation error factor with iSIC at D
γ_U, γ_E	Average transmit SNR at U^* and E	$\bar{L}_{(.)}$	The mean path loss

where ν and υ are constant values that vary according to the surrounding environment (such as suburban, urban, dense-urban) [19], the elevation angle $\theta_{ab} = \frac{180}{\pi} \arcsin\left(\frac{H_U}{d_{ab}}\right)$, and the distance between the UR and the ground device $d_{ab} = \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2 + {H_U}^2}$. We were using the path-loss model in [18] to accurately present the air-to-ground channels of UR networks, which takes LoS and NLoS of $a \to b$ channels into consideration. The expressions are as follows [13]:

$$L_l(ab) = \kappa_l^{-1} d_{ab}^{-\sigma}, \tag{2}$$

where $l \in \{LoS, NLoS\}$, κ_l is parameters depend on environment and carrier frequency, which can be expressed as $\kappa_l = \xi_l (4\pi f_c / c)^2$. f_c is the carrier frequency, c is the speed of light, and ξ_l is the excessive path losses of the LoS and NLoS propagation, and σ is the path-loss exponent. The mean path loss, taking into account the probability of both LoS and NLoS linkages from the UAV to the ground devices is thus calculated as [18]

$$\bar{L}_{ab} = P_{LoS}(ab) L_{LoS}(ab) + P_{NLoS}(ab) L_{NLoS}(ab). \tag{3}$$

In this work, the URs first send their pilot signals to the D simultaneously. Once the signal-to-noise ratios (SNRs) of all U_k to D channels have been estimated [11], the D selects the best UR, denoted by the symbol U^*, which is the one with the highest received SNR at the D. Thus, the indices and channel power gain of a selected UAV U^* in a UR cluster are represented as follow:

$$U^* = \arg \max_{1 \le k \le K} \left\{ |h_{U_k D}|^2 \right\}, \tag{4}$$

$$|h_D|^2 = \max_{1 \le k \le K} \left\{ |h_{U_k D}|^2 \right\}. \tag{5}$$

Next, the IDs concurrently transmit pilot signals to the selected UAV. U^* estimates the SNRs of all transmission channels from two clusters and then selects the best ID in cluster A, denoted I_A^*, and the best ID in cluster B, denoted I_B^*, as the ones with the greatest received SNRs at the selected UAV terminal. Therefore, the indices and channel power gains of the selected ID in clusters A and B are as follows:

$$I_O^* = \arg \max_{i \in (m,n)} \left\{ \left| h_{I_i U^*} \right|^2 \right\}, \tag{6}$$

$$\left| h_O \right|^2 = \max_{i \in (m,n)} \left\{ \left| h_{I_i U^*} \right|^2 \right\}, \tag{7}$$

where $O \in (A, B)$.

2.2 Communication Protocol

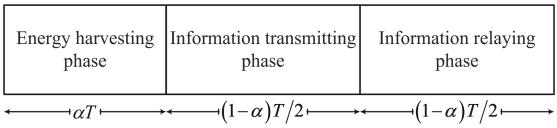

Fig. 2. Time flowchart of the considered RF EH NOMA UR network.

In the considered system, we use a time switching (TS) communication protocol as shown in Fig. 2. This communication protocol is described as follows:

- In the first phase, during the duration of αT, I_O^* harvests energy from U^*, where α $(0 < \alpha < 1)$ indicates the TSR [20], and T represents transmission block time. Thus, the energy harvested at I_O^* can be expressed as follows:

$$E_O = \frac{\eta P_U g_O \alpha T}{\bar{L}_O}, \tag{8}$$

  where, η is the EH efficiency coefficient, which depends on the rectification $(0 < \eta < 1)$, P_U is the transmit power of U^*, $g_O = \left| h_O \right|^2$. Noted that all harvested energies are used for their transmission.
- In the second phase, I_O^* sends their own messages to U^* during the period of $(1 - \alpha) T/2$. Thus, the received signal at U^* is written as

$$y_U = \sqrt{\frac{P_A}{\bar{L}_A} \rho_0} g_A x_A + \sqrt{\frac{P_B}{\bar{L}_B} (1 - \rho_0)} g_B x_B + n_U, \tag{9}$$

  where $P_A = \frac{E_A}{(1-\alpha)T/2} = \frac{\beta P_U g_A}{\bar{L}_A}$, $P_B = \frac{E_B}{(1-\alpha)T/2} = \frac{\beta P_U g_B}{\bar{L}_B}$, $\beta = \frac{2\eta\alpha}{(1-\alpha)}$, ρ_0 denotes the power allocation coefficient for transmitted signal from I_A^* to U^* and $n_U \sim \mathcal{CN}(0, N_0)$ is additive white Gaussian noise (AWGN) at U^* [11]. Because the UR uses the DF transmission scheme, U^* must first

decode both x_A and x_B before forwarding. U^* decodes x_A first by treating the signal corresponding to x_B as interference. After successfully decoding x_A, U^* decodes x_B by canceling the known x_A using the SIC method [10]. The signal-to-interference-plus-noise ratio (SINR) for detect x_A at U^* is given by

$$\gamma_U^{x_A} = \frac{\beta\gamma_U\rho_0 {g_A}^2 \bar{L}_B^2}{\left[(1-\rho_0)\,\beta\gamma_U {g_B}^2 + \bar{L}_B^2\right]\bar{L}_A^2}, \tag{10}$$

where $\gamma_U = P_U/N_0$. The SIC principle states that x_B is decoded by subtracting x_A from $\gamma_U^{x_A}$; the SIC is perfect when x_A is totally deleted. Otherwise, x_B will be decoded in the presence of residual interference due to iSIC [21]. We investigate the scenario of iSIC in this paper, therefore SINR at U^* to detect x_B is given by

$$\gamma_U^{x_B} = \frac{(1-\rho_0)\,\beta\gamma_U {g_B}^2 \bar{L}_A^2}{\bar{L}_B^2\left(\epsilon_0\beta\gamma_U\rho_0 {g_A}^2 + \bar{L}_A^2\right)}, \tag{11}$$

where ϵ_0 represents the residual interference due to iSIC, $0 \le \epsilon_0 \le 1$, and ϵ_0 refer to perfect SIC (pSIC).

– In the third phase, U^* uses the downlink NOMA technique to forward the correctly decoded messages to destination D. Because the channel state information (CSI) of E is unknown, the AN is used for relaying communication in order to increase information security [22]. It is a strategy that permits the usable signals and the AN to transmit at the same time in order to degrade the received signal of E while without impairing that of D. As a result, the message sent from U^* takes the following form:

$$x_U = \sqrt{\rho_A}x_A + \sqrt{\rho_B}x_B + \sqrt{\rho_J}x_J, \tag{12}$$

where ρ_A, ρ_B, and ρ_J ($\rho_A+\rho_B+\rho_J = 1$ and $\rho_A > \rho_B$) are the power allocation coefficient for messages x_A, x_B, and AN x_J, respectively. Thus, the received signal at D is as follows:

$$y_D = \sqrt{\frac{\rho_A P_U}{\bar{L}_D}}g_D x_A + \sqrt{\frac{\rho_B P_U}{\bar{L}_D}}g_D x_B + \sqrt{\frac{\rho_J P_U}{\bar{L}_D}}g_D x_J + n_D, \tag{13}$$

where $g_D = |h_D|^2$ and $n_D \sim \mathcal{CN}(0, N_0)$ is AWGN at D. Assuming the AN can be removed at D [23]. Thus, the SINR to detect x_A and x_B at D are expressed as follows:

$$\gamma_D^{x_A} = \frac{\rho_A\gamma_U g_D}{\rho_B\gamma_U g_D + \bar{L}_U}, \tag{14}$$

$$\gamma_D^{x_B} = \frac{\rho_B\gamma_U g_D}{\epsilon_1\rho_A\gamma_U g_D + \bar{L}_U}, \tag{15}$$

where ϵ_1 represents residual interference due to the iSIC at the D. Similarly, the expression of signal received at E is as follows:

$$y_E = \sqrt{\frac{\rho_A P_U}{\bar{L}_E}}g_E x_A + \sqrt{\frac{\rho_B P_U}{\bar{L}_E}}g_E x_B + \sqrt{\frac{\rho_J P_U}{\bar{L}_E}}g_E x_J + n_E, \tag{16}$$

where $g_E = |h_E|^2$ and $n_E \sim \mathcal{CN}(0, N_0)$ is AWGN at E. We suppose E is a low-capacity passive eavesdropping device, so E can only eavesdrop on the communication from U^* to D. Assuming the AN cannot be removed at E [22]. The SINR to detect x_A and x_B at E is given by

$$\gamma_E^{x_A} = \frac{\rho_A \gamma_E g_E}{(\rho_B + \rho_J)\gamma_E g_E + \bar{L}_E}, \tag{17}$$

$$\gamma_E^{x_B} = \frac{\rho_B \gamma_E g_E}{(\rho_A + \rho_J)\gamma_E g_E + \bar{L}_E}, \tag{18}$$

where $\gamma_E = P_U/N_0$.

Under Rayleigh fading [14], the corresponding cumulative distribution function (CDF) and probability density function (PDF) of channel power gains, g_X, $(X \in \{A, B, D\})$ are respectively given by

$$F_{g_X}(x) = \left(1 - e^{-\frac{x}{\lambda_X}}\right)^{\Psi} = \sum_{\psi=0}^{\Psi} \binom{\Psi}{\psi} (-1)^{\psi} e^{-\frac{\psi x}{\lambda_X}}, \tag{19}$$

$$f_{g_X}(x) = \sum_{\psi=1}^{\Psi} \binom{\Psi}{\psi} \frac{(-1)^{\psi+1}\psi}{\lambda_X} e^{-\frac{\psi x}{\lambda_X}}, \tag{20}$$

where $\Psi \in \{K, M, N\}$.

The CDF and PDF of channel power gains g_E are respectively expressed as

$$F_{g_E}(x) = 1 - e^{-\frac{x}{\lambda_E}}, \tag{21}$$

$$f_{g_E}(x) = \frac{1}{\lambda_E} e^{-\frac{x}{\lambda_E}}. \tag{22}$$

According to the above results, the CDFs of $\gamma_D^{x_A}$ and $\gamma_D^{x_B}$ are determined as follows:

$$F_{\gamma_D^{x_A}}(x) = \begin{cases} 1, & x \geq {}^{\rho_A}/_{\rho_B} \\ \sum\limits_{l=0}^{K} \binom{K}{l} (-1)^l e^{-\frac{x l \bar{L}_U}{\lambda_D(\rho_A - \rho_B x)\gamma_U}}, & x < {}^{\rho_A}/_{\rho_B} \end{cases}, \tag{23}$$

$$F_{\gamma_D^{x_B}}(x) = \begin{cases} 1, & x \geq {}^{\rho_B}/_{\epsilon_1 \rho_A} \\ \sum\limits_{l=0}^{K} \binom{K}{l} (-1)^l e^{-\frac{x l \bar{L}_U}{\lambda_D \gamma_U (\rho_B - \epsilon_1 \rho_A x)}}, & x < {}^{\rho_B}/_{\epsilon_1 \rho_A} \end{cases}. \tag{24}$$

The CDFs and PDFs of $\gamma_E^{x_A}$ and $\gamma_E^{x_B}$ are respectively given by:

$$F_{\gamma_E^{x_A}}(x) = \begin{cases} 1, & x \geq {}^{\rho_A}/_{\rho_B+\rho_J} \\ 1 - e^{-\frac{x\bar{L}_E}{\lambda_E[\rho_A-(\rho_B+\rho_J)x]\gamma_E}}, & x < {}^{\rho_A}/_{\rho_B+\rho_J} \end{cases}, \tag{25}$$

$$f_{\gamma_E^{x_A}}(x) = \begin{cases} 0, & x \geq {}^{\rho_A}/_{\rho_B+\rho_J} \\ \frac{\rho_A\bar{L}_E}{\lambda_E\gamma_E[\rho_A-(\rho_B+\rho_J)x]^2} e^{-\frac{x\bar{L}_E}{\lambda_E\gamma_E[\rho_A-(\rho_B+\rho_J)x]}}, & x < {}^{\rho_A}/_{\rho_B+\rho_J} \end{cases}, \tag{26}$$

$$F_{\gamma_E^{x_B}}(x) = \begin{cases} 1, & x \geq {}^{\rho_B}/_{\rho_A+\rho_J} \\ 1 - e^{-\frac{x\bar{L}_E}{\lambda_E\gamma_E[\rho_B-(\rho_A+\rho_J)x]}}, & x < {}^{\rho_B}/_{\rho_A+\rho_J} \end{cases}, \tag{27}$$

$$f_{\gamma_E^{x_B}}(x) = \begin{cases} 0, & x \geq {}^{\rho_B}/_{\rho_A+\rho_J} \\ \frac{\rho_B\bar{L}_E}{\lambda_E\gamma_E[\rho_B-(\rho_A+\rho_J)x]^2} e^{-\frac{x\bar{L}_E}{\lambda_E\gamma_E[\rho_B-(\rho_A+\rho_J)x]}}, & x < {}^{\rho_B}/_{\rho_A+\rho_J} \end{cases}. \tag{28}$$

3 Secrecy Performance Analysis

In this section, we derive the expressions for the SOPs to evaluate the secrecy performance of the considered system. It is possible for the proposed system to experience a security outage event if the instantaneous secrecy capacity, denoted by $C_S^{x_O}$, falls below a preset secrecy rate threshold, denoted by C_{th}^O, which is expressed as

$$\mathbb{S}_O = \Pr\left(C_S^{x_O} < C_{th}^O\right), \tag{29}$$

where $C_S^{x_O}$ is expressed as follows [14]:

$$C_S^{x_O} = [C_D^{x_O} - C_E^{x_O}]^+ = \begin{cases} \frac{(1-\alpha)}{2} W \log_2\left(\frac{1+\gamma_D^{x_O}}{1+\gamma_E^{x_O}}\right), & \gamma_D^{x_O} > \gamma_E^{x_O} \\ 0, & \gamma_D^{x_O} \leq \gamma_E^{x_O} \end{cases}, \tag{30}$$

where W is the system bandwidth, $C_D^{x_O}$ and $C_E^{x_O}$ are the capacities of D and E to detect x_O. The following lemmas are provided to characterize the secrecy performance of an RF EH NOMA UR system.

Lemma 1. *The closed-form expression of the (OP) $\mathbb{P}_A$ of the considered system in the second phase to detect x_A is provided by*

$$\mathbb{P}_A = \frac{\pi}{2Q\lambda_B} \sum_{i=0}^{M} \sum_{j=1}^{N} \sum_{q=1}^{Q} \binom{M}{i} \binom{N}{j} \times \frac{(-1)^{i+j+1} j\sqrt{1-\zeta_q{}^2}}{\omega_q \ln^2(\omega_q)} e^{-\frac{i\sqrt{\theta_1 \ln^{-2}(\omega_q)+\theta_2}}{\lambda_A}} \omega_q^{-\frac{j\ln^{-2}(\omega_q)}{\lambda_B}}, \tag{31}$$

where $\theta_1 = \frac{\gamma_{th}\bar{L}_A^2(1-\rho_0)}{\rho_0\bar{L}_B^2}$, $\theta_2 = \frac{\gamma_{th}\bar{L}_A^2}{\beta\gamma_U\rho_0}$, $\zeta_q = \cos\left(\frac{\pi(2q-1)}{2Q}\right)$, $\omega_q = \frac{(\zeta_q+1)}{2}$, $\gamma_{th}^A = 2^{\frac{2R_A}{W(1-\alpha)}} - 1$, *and R_A denote the data rate threshold.*

Proof. See Appendix A.

Lemma 2. *The closed-form expression of the OP $\mathbb{P}_B$ of the considered system in the second phase to detect x_B is provided by*

$$\mathbb{P}_B = \frac{\pi}{2Q\lambda_A}\sum_{i=1}^{M}\sum_{j=0}^{N}\sum_{q=1}^{Q}\binom{M}{i}\binom{N}{j} \times \frac{(-1)^{i+j+1} i\sqrt{1-\zeta_q{}^2}}{\omega_q \ln^2(\omega_q)} e^{-\frac{j\sqrt{\theta_1 \ln^{-2}(\omega_q)+\theta_2}}{\lambda_B}} \omega_q{}^{\frac{i\ln^{-2}(\omega_q)}{\lambda_A}}, \tag{32}$$

where $\theta_3 = \frac{\gamma_{th}^B \epsilon_0 \rho_0 \bar{L}_B^2}{(1-\rho_0)\bar{L}_A^2}$, $\theta_4 = \frac{\gamma_{th}^B \bar{L}_B^2}{(1-\rho_0)\beta\gamma_U}$, $\gamma_{th}^B = 2^{\frac{2R_B}{W(1-\alpha)}} - 1$, and R_B denote the data rate threshold.

Proof. Similar to the proof of Lemma 1.

Lemma 3. *The closed-form expression of the SOP $\mathbb{S}_A$ to detect x_A of the third phase is given by*

$$\mathbb{S}_A = \begin{cases} I_A, & b_1 \geq b_2 \\ I_A + e^{-\frac{b_1 \bar{L}_E}{\lambda_E \gamma_E [\rho_A - (\rho_B + \rho_J) b_1]}}, & b_1 < b_2 \end{cases}, \tag{33}$$

where $I_A = \frac{\pi\tau\rho_A \bar{L}_E}{2Q\lambda_E\gamma_E}\sum_{l=0}^{K}\sum_{q=1}^{Q}\binom{K}{l}\frac{(-1)^l\sqrt{1-\zeta_q{}^2}}{[\rho_A-(\rho_B+\rho_J)b\tau\omega_q]^2} e^{-\frac{[\phi_A(1+\tau\omega_q)-1]l\bar{L}_U}{\lambda_D\gamma_U(\rho_A-\rho_B[\phi_A(1+\tau\omega_q)-1])}} \times e^{-\frac{\tau\omega_q\bar{L}_E}{\lambda_E\gamma_E[\rho_A-(\rho_B+\rho_J)\tau\omega_q]}}$, $\phi_A = 2^{\frac{2C_{th}^A}{W(1-\alpha)}}$, $b_1 = \frac{\rho_A-\rho_B(\phi_A-1)}{\rho_B C_{th}}$, $b_2 = \frac{\rho_A}{\rho_B+\rho_J}$, *and* $\tau = \min(b_1, b_2)$.

Proof. See Appendix B.

Lemma 4. *The closed-form expression of the SOP $\mathbb{S}_B$ to detect x_B of the third phase is given by*

$$\mathbb{S}_B = \begin{cases} I_B, & c_1 \geq c_2 \\ I_B + e^{-\frac{c_1 \bar{L}_E}{\lambda_E \gamma_E [\rho_B - (\rho_A + \rho_J) c_1]}}, & c_1 < c_2 \end{cases},$$

where $I_B = \frac{\pi\mu\rho_B\bar{L}_E}{2Q\lambda_E\gamma_E}\sum_{l=0}^{K}\sum_{q=1}^{Q}\binom{K}{l}\frac{(-1)^l\sqrt{1-\zeta_q{}^2}}{[\rho_B-(\rho_A+\rho_J)\mu\omega_q]^2} e^{-\frac{[\phi_B(1+\mu\omega_q)-1]l\bar{L}_U}{\lambda_D\gamma_U(\rho_B-\epsilon_1\rho_A[\phi_B(1+\mu\omega_q)-1])}} \times e^{-\frac{\mu\omega_q\bar{L}_E}{\lambda_E\gamma_E[\rho_B-(\rho_A+\rho_J)\mu\omega_q]}}$, $\phi_B = 2^{\frac{2C_{th}^B}{W(1-\alpha)}}$, $c_1 = \frac{\rho_B-\epsilon_1\rho_A(C_{th}-1)}{\epsilon_1\rho_A C_{th}}$, $c_2 = \frac{\rho_B}{\rho_A+\rho_J}$, *and* $\mu = \min(c_1, c_2)$.

Proof. Similar to the proof of Lemma 3.

According to the proposed RF EH NOMA UR system, the system experiences a secrecy outage when the signal x_A or x_B is not successfully decoded at U^* in

phase 2, or when the secrecy rate falls below the predefined threshold. As a result, the SOP for detecting x_O, represented by Θ_O, is derived as

$$\Theta_O = \mathbb{P}_O + (1 - \mathbb{P}_O)\,\mathbb{S}_O. \tag{34}$$

And the SOP of considered system is as follow:

$$\Theta_S = 1 - (1 - \Theta_A)\,(1 - \Theta_B)\,. \tag{35}$$

4 Numerical Result

In this section, we describe the numerical results used to validate the analytical expression of the SOP described in Sect. 3 for the RF EH NOMA UR system. Specifically, we consider the following system parameters in all simulations [18]: transmit SNR $\gamma_U \in (0, 20)$ (dB); $f_c = 2.10^8$ (Hz), $c = 3.10^8$; $\alpha \in (0.1, 0.9)$; $\eta = 0.75$; $\sigma = 2$; $\rho_0 = 0.75$, $\rho_A = 0.5$, $\rho_B = 0.3$, $\rho_E = 0.2$; $\epsilon_0 = \epsilon_1 = 0.3$; the coordinates $D(0, 0, 0)$, $I_A(5, 2, 0)$, $I_B(4, 1, 0)$, $E(1, 3, 0)$, $U(2, 2, H_{U^*})$, where $H_{U^*} \in (0, 20)$ (m); $W = 10^2$ (Hz); $C_{th}^A = C_{th}^B = 0.05$, $R_A = R_B = 0.05$ (bit/s/Hz); $\nu = 0.1581$, $\upsilon = 9.6177$, $\xi_{los} = 1$ and $\xi_{nlos} = 20$.

The impact of the average SNR γ_U and the number of UR (K) on the SOP of the IDs and the entire system is depicted in Fig. 3a. We discover that as γ_U increases, the SOP for each ID and the entire system decreases. In other words, raising the UR's' transmit power can improve the SOP. Furthermore, the figure demonstrates that when K increases, the SOP reduces dramatically. This mean that the more URs that permit signal transfer, the more probable the system is to find the best UR to participate in the communication process.

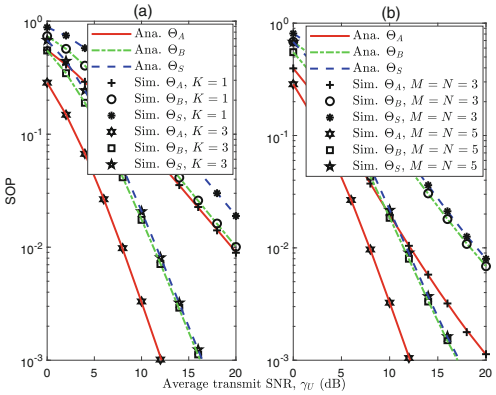

Fig. 3. Impact of average transmit SNR on SOP with different number of UR (K) in (a) and numbers of ID in two clusters (M, N) in (b).

Figure 3b depicts the impact of the number of IDs in two clusters (M, N) on the SOP of the IDs and the entire system. The findings indicate that increasing

the number of IDs can reduce the SOP of each cluster and the entire system. The results show that increasing the number of IDs in clusters can improve the secrecy performance of the selected IDs as well as the entire system. This is due to the fact that the selected IDs have better channel conditions in this scenario.

The influence of height of U^* on the SOP of the IDs and the entire system is depicted in Fig. 4a. As we can see, there appears to be an optimum $H^*_{U^*}$ value for which the SOP value is minimized. This is due to the fact that while the height of U^* is low, the LoS probability is low, whereas the NLoS probability is large; nonetheless, a high H_{U^*} results in a high path loss. As a result, there is a point where the optimum SOP is reached.

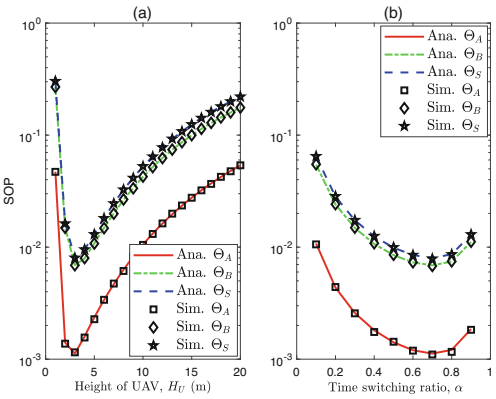

Fig. 4. Impact of height of UR (H_{U^*}) in (a) and time switching ratio (α) in (b) on SOP.

Figure 4b shows the effect of TSR α on the SOP of the IDs and the entire system. The SOP reduces when α increases from 0.5 to 0.8. Then, as α continues to rise, the SOP rises again. Because α is small, less time is spent in the EH phase, resulting in less energy harvested by IDs. When α is larger, IDs can gather more energy, resulting in optimal secrecy performance. However, when α increases, less time is available for phase 2 and phase 3, reducing system reliability and increasing SOP. Based on these findings, we infer that α^* is the ideal value for minimizing SOP.

We investigating a residual interference in Fig. 5a for two cases pSIC and iSIC. The pSIC case $\epsilon_0 = \epsilon_1 = 0$ and the iSIC case $\epsilon_0 = \epsilon_1 = 0.3$. It is clear that ϵ_0 and ϵ_1 harm on system secrecy performance, i.e., when they increase, the higher values of the SOP can be observed. Increasing the values of ϵ_0 and ϵ_1 reduces the SINR for decoding the x_B signal at U^* and D, hence increasing the SOP.

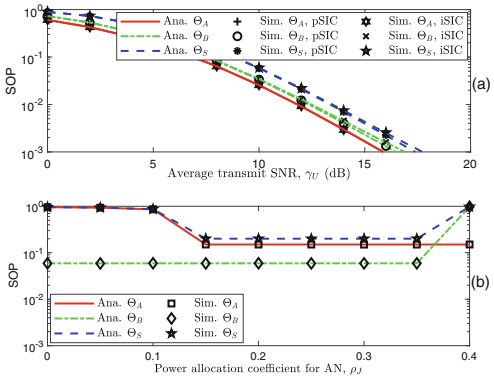

Fig. 5. Impact of the pSIC and iSIC (ϵ_0, ϵ_1) in (a) and the power allocation coefficient for artificial noise in (b) on SOP.

Figure 5b depicts the impact of the AN on the SOP of the IDs and the entire system. In this experiment, we set $\rho_J = 0.6$ and investigate the effect of the AN. We can see is that the SOP of the system tends to decrease gradually, reach a minimum, and then grow as ρ_J increases. Because when $\rho_J = 0$, U^* interacts with D without using AN, the probability that E can decode the signal from U^* is high, leading to the high value of the SOP. As the AN power increases, the interference at E increases, hence reducing the SOP. Increasing ρ_J makes it harder for E to eavesdrop, but it reduces the power available for useful signal transmission, increasing the SOP. So, while ρ_J can improve system SOP, it is necessary to find the optimal ρ_J^* value for minimum SOP.

5 Conclusion

In this paper, we investigated the secrecy outage performance of an RF EH NOMA UR system over Rayleigh fading channel. We propose a three-phase system operating protocol based on UR-ID selection, focusing RF EH and AN techniques to increase secrecy outage performance. As a result, we obtain closed-form expressions of SOP for each ID cluster and the entire system. We provided numerical results to verify the proposed system secrecy performance.

Acknowledgment. This work was supported by Thailand Science Research and Innovation (TSRI) and the National Research Council of Thailand (NRCT) via the International Research Network Program (IRN61W0006) and by Khon Kaen University.

A Proof of Lemma 1

Here, we derive the closed-form expression of $\mathbb{P}_A$ as follows

$$\begin{aligned}
\mathbb{P}_A &= \Pr\left(\gamma_{U^*}^{x_A} < \gamma_{th}^{A}\right) \\
&= \int_0^{\infty} F_{g_A}\left(\sqrt{\theta_1 x^2 + \theta_2}\right) f_{g_B}(x)\, dx \\
&= \sum_{i=0}^{M}\sum_{j=1}^{N}\binom{M}{i}\binom{N}{j}\frac{(-1)^{i+j+1} j}{\lambda_B}\int_0^{\infty} e^{-\frac{i\sqrt{\theta_1 x^2+\theta_2}}{\lambda_A} - \frac{jx}{\lambda_B}}\, dx \\
&\overset{(a)}{=} \frac{\pi}{2Q\lambda_B}\sum_{i=0}^{M}\sum_{j=1}^{N}\sum_{q=1}^{Q}\binom{M}{i}\binom{N}{j}\frac{(-1)^{i+j+1} j\sqrt{1-\zeta_q{}^2}}{\omega_q \ln^2(\omega_q)} \\
&\quad \times e^{-\frac{i\sqrt{\theta_1 \ln^{-2}(\omega_q)+\theta_2}}{\lambda_A}} \omega_q^{-\frac{j\ln^{-2}(\omega_q)}{\lambda_B}},
\end{aligned} \tag{36}$$

where $\theta_1 = \frac{\gamma_{th}\bar{L}_A^2(1-\rho_0)}{\rho_0 \bar{L}_B^2}$, $\theta_2 = \frac{\gamma_{th}\bar{L}_A^2}{\beta\gamma_U\rho_0}$, $\zeta_q = \cos\left(\frac{\pi(2q-1)}{2Q}\right)$, and $\omega_q = \frac{(\zeta_q+1)}{2}$. Note that step (a) is obtained by applying the Gaussian-Chebyshev quadrature method with Q is the complexity-vs-accuracy trade-off coefficient. This ends our proof.

B Proof of Lemma 2

From Eq. (29) we derive closed-form expression of the SOP $\mathbb{S}_A$ as follow

$$\begin{aligned}
\mathbb{S}_A &= \int_0^{\infty}\int_0^{\phi_A(1+y)-1} f_{\gamma_D^{x_A}}(x)\, f_{\gamma_E^{x_A}}(y)\, dx dy \\
&= \int_0^{\infty} F_{\gamma_D^{x_A}}\left[\phi_A(1+y)-1\right] f_{\gamma_E^{x_A}}(y)\, dy \\
&= \begin{cases}
\frac{\rho_A\bar{L}_E}{\lambda_E\gamma_E}\sum_{l=0}^{K}\binom{K}{l}(-1)^l \int_0^{b_2} \frac{e^{-\frac{[\phi_A(1+y)-1]l\bar{L}_U}{\lambda_D\gamma_U(\rho_A-\rho_B[\phi_A(1+y)-1])} - \frac{y\bar{L}_E}{\lambda_E\gamma_E[\rho_A-(\rho_B+\rho_J)y]}}}{[\rho_A-(\rho_B+\rho_J)y]^2} dy \\
\qquad\qquad , b_1 \geq b_2 \\
\frac{\rho_A\bar{L}_E}{\lambda_E\gamma_E}\sum_{l=0}^{K}\binom{K}{l}(-1)^l \int_0^{b_1} \frac{e^{-\frac{[\phi_A(1+y)-1]l\bar{L}_U}{\lambda_D\gamma_U(\rho_A-\rho_B[\phi_A(1+y)-1])} - \frac{x\bar{L}_E}{\lambda_E\gamma_E[\rho_A-(\rho_B+\rho_J)x]}}}{[\rho_A-(\rho_B+\rho_J)y]^2} dy \\
\qquad + \int_{b_1}^{b_2} f_{\gamma_E^{x_A}}(y)\, dy \qquad , b_1 < b_2
\end{cases} \\
&= \begin{cases} I_A, & b_1 \geq b_2 \\ I_A + e^{-\frac{b_1\bar{L}_E}{\lambda_E\gamma_E[\rho_A-(\rho_B+\rho_J)b_1]}}, & b_1 < b_2 \end{cases}
\end{aligned} \tag{37}$$

where $I_A \overset{(b)}{=} \frac{\pi\tau\rho_A\bar{L}_E}{2Q\lambda_E\gamma_E}\sum_{l=0}^{K}\sum_{q=1}^{Q}\binom{K}{l}\frac{(-1)^l\sqrt{1-\zeta_q{}^2}}{[\rho_A-(\rho_B+\rho_J)b\tau\omega_q]^2}e^{-\frac{[\phi_A(1+\tau\omega_q)-1]l\bar{L}_U}{\lambda_D\gamma_U(\rho_A-\rho_B[\phi_A(1+\tau\omega_q)-1])}}$ $\times e^{-\frac{\tau\omega_q\bar{L}_E}{\lambda_E\gamma_E[\rho_A-(\rho_B+\rho_J)\tau\omega_q]}}$, $\phi_A = 2^{\frac{2C_{th}^A}{W(1-\alpha)}}$, $b_1 = \frac{\rho_A-\rho_B(\phi_A-1)}{\rho_B C_{th}}$, $b_2 = \frac{\rho_A}{\rho_B+\rho_J}$, and $\tau = \min(b_1, b_2)$. Note that step (b) is obtained by applying the Gaussian-Chebyshev quadrature method with Q is the complexity-vs-accuracy trade-off coefficient. This ends our proof.

References

1. Li, B., Fei, Z., Zhang, Y.: UAV communications for 5G and beyond: recent advances and future trends. IEEE Internet Things J. **6**(2), 2241–2263 (2019)
2. Zeng, S., Zhang, H., Bian, K., Song, L.: UAV relaying: powerallocation and trajectory optimization using decode-and-forward protocol. In: Proceedings of IEEE ICC, pp. 1–6. Kansas City, MO, USA (2018)
3. Yang, L., Chen, J., Hasna, M.O., Yang, H.: Outage performance of UAV-assisted relaying systems with RF energy harvesting. IEEE Commun. Lett. **22**(12), 2471–2474 (2018)
4. Tam, H.H.M., Tuan, H.D., Nasir, A.A., Duong, T.Q., Poor, H.V.: MIMO energy harvesting in full-duplex multi-user networks. IEEE Trans. Wireless Commun. **16**(5), 3282–3297 (2017)
5. Nguyen, M.-N., Nguyen, L.D., Duong, T.Q., Tuan, H.D.: Real-time optimal resource allocation for embedded UAV communication systems. IEEE Wireless Commun. Lett. **8**(1), 225–228 (2019)
6. Feng, W., Zhao, N., Ao, S., Tang, J., Zhang, X., Fu, Y., So, D.K.C., Wong, K.-K.: Joint 3D trajectory design and time allocation for UAV-enabled wireless power transfer networks. IEEE Trans. Veh. Technol. **69**(9), 9265–9278 (2020)
7. Li, Y., Yang, D., Xu, Y., Xiao, L., Chen, H.: Throughput maximization for UAV-enabled relaying in wireless powered communication networks. Sensors **19**(13) (2019)
8. Jia, H., Wang, Y., Liu, M., Chen, Y.: Sum-rate maximization for UAV aided wireless power transfer in space-air-ground networks. IEEE Access **8**, 216 231–216 244 (2020)
9. Ding, Z., Fan, P., Poor, H.V.: Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions. IEEE Trans. Veh. Technol. **65**(8), 6010–6023 (2016)
10. Vo, V.N., et al.: On security and throughput for energy harvesting untrusted relays in IoT systems using NOMA. IEEE Access **7**, 149 341–149 354 (2019)
11. Nguyen, A.-N., Vo, V.N., So-In, C., Ha, D.: System performance analysis for an energy harvesting IoT system using a DF/AF UAV-enabled relay with downlink NOMA under nakagami-m fading. Sensors **21**(1) (2021)
12. Hadzi-Velkov, Z., Pejoski, S., Zlatanov, N., Schober, R.: UAV-assisted wireless powered relay networks with cyclical NOMA-TDMA. IEEE Wireless Commun. Lett. **9**(12), 2088–2092 (2020)
13. Vo, V.N., So-In, C., Tran, H., Tran, D.-D., Huu, T.P.: Performance analysis of an energy-harvesting IoT system using a UAV friendly jammer and NOMA under cooperative attack. IEEE Access **8**, 221 986–222 000 (2020)
14. Nguyen, A.-N., Vo, V.N., So-In, C., Ha, D., Sanguanpong, S., Baig, Z.A.: On secure wireless sensor networks with cooperative energy harvesting relaying. IEEE Access **7**, 139 212–139 225 (2019)

15. Wang, Q., Chen, Z., Mei, W., Fang, J.: Improving physical layer security using UAV-enabled mobile relaying. IEEE Wireless Commun. Lett. **6**(3), 310–313 (2017)
16. Sun, X., Yang, W., Cai, Y., Ma, R., Tao, L.: Physical layer security in millimeter wave SWIPT UAV-based relay networks. IEEE Access **7**, 35 851–35 862 (2019)
17. Duong, T.-Q., Bao, V.-N.-Q.: Performance analysis of selection decode-and-forward relay networks. Electronics Lett. **44**(12), 1206–1207 (2008)
18. Nguyen, A.-N., Vo, V.N., So-In, C., Ha, D., Truong, V.-T.: Performance analysis in UAV-enabled relay with NOMA under nakagami-m fading considering adaptive power splitting. In: Proceedings, pp. 1–6. Lampang, Thailand, JCSSE (2021)
19. Sohail, M.F., Leow, C.Y., Won, S.: Non-orthogonal multiple access for unmanned aerial vehicle assisted communication. IEEE Access **6**, 22 716–22 727 (2018)
20. Ji, B., Li, Y., Chen, S., Han, C., Li, C., Wen, H.: Secrecy outage analysis of UAV assisted relay and antenna selection for cognitive network under nakagami-m channel. IEEE Trans. Cognitive Commun. Networking **6**(3), 904–914 (2020)
21. Kara, F., Kaya, H.: Improved user fairness in decode-forward relaying non-orthogonal multiple access schemes with imperfect SIC and CSI. IEEE Access **8**, 97 540–97 556 (2020)
22. Nguyen, V.-L., Ha, D.-B., Tran, D.-D., Lee, Y.: Enhancing physical layer security for cooperative non-orthogonal multiple access networks with artificial noise. EAI Endorsed Trans. Indust. Netw. Intellig. Syst. **6**(20) (2019)
23. Liu, Y., Qin, Z., Elkashlan, M., Gao, Y., Hanzo, L.: Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. IEEE Trans. Wireless Commun. **16**(3), 1656–1672 (2017)