A Secrecy Offloading in Radio Frequency Energy Harvesting NOMA Heterogeneous Mobile Edge Computing Network

Van-Truong Truong[1,2(✉)], Dac-Binh Ha[1,2], and Minh-Thong Vo[1,2]

[1] Faculty of Electrical-Electronic Engineering, Duy Tan University, Da Nang 550000, Vietnam
{truongvantruong,vominhthong}@dtu.edu.vn, hadacbinh@duytan.edu.vn
[2] Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam

Abstract. This paper studies a security offloading scheme in radio frequency energy harvesting (RF EH) non-orthogonal multiple access (NOMA) enabled heterogeneous mobile edge computing (Het-MEC) network over Rayleigh fading channel. Specifically, we investigate the model of a single mobile user (MU) offloading tasks to Het-MEC servers located at neighboring access points (APs) in the presence of a passive eavesdropper. In addition, the MU collects radio energy from a power station to ensure power throughout the offloading process. Accordingly, a four-phase energy-secrecy-offloading scheme is proposed under latency constraint, namely NOLES. We derive the exact close-form secrecy successful computation probability (SSCP) to evaluate the system performance. Numerical results under the Monte-Carlo simulation demonstrate the effective performance of our proposed framework.

Keywords: mobile edge computing · non-orthogonal multiple access · secrecy successful computation probability · security offloading · radio frequency energy harvesting

1 Introduction

The rapid development of applications in next-generation networks, such as virtual/augmented reality (VR/AR), autonomous driving, and tactile Internet of Things, has increased the demand for mobile data traffic explosively [1]. Additionally, each application is deployed with a massive user, requiring a large amount of computation, low latency, and some other security or power requirements. However, the path to effectively deploy such applications is still far, given that mobile terminals (MDs) have minimal computing capability and power for

N.-S. Vo and H.-A. Tran (Eds.): INISCOM 2023, LNICST 531, pp. 275–286, 2023.
https://doi.org/10.1007/978-3-031-47359-3_20

operation [2]. Furthermore, the valuable resources in a wireless network can be heterogeneous, leading to challenges in implementing operational protocols [3].

In order to effectively solve the above challenges, non-orthogonal multiple access (NOMA) and mobile edge computing (MEC) are proposed to be applied in 5G and 6G telecommunications networks. In the MEC-architectured system, MEC servers (MES) are set up at the network edge, which is close to the MDs to support them in computing services. In other words, MEC is the next generation of cloud computing, allowing it to support real-time applications more efficiently [4]. Meanwhile, NOMA uses advanced techniques in modulation and decoding to support better MDs in terms of spectrum efficiency, data rate, and user fairness. Thus, many studies have been carried out to clarify the NOMA-MEC system performance [5–7]. For instance, Ha *et al.* [6] examined a downlink NOMA MEC network under a Rayleigh channel, where one MD offloads the task to two neighboring APs under a tolerance constraint. The results demonstrate the effectiveness of the combination of NOMA and MEC and open up many exciting research directions for this model. However, the energy problem of MD has not been entirely solved by these studies.

Different from these prior works that only focus on investigating the time performance of the NOMA MEC system, many studies have proposed frameworks to solve the energy problem for MD [8,9]. One solution that has proven effective in solving the above problem is to deploy radio energy harvesting techniques. It is a technique that allows MDs to use specialized hardware to collect power from hybrid access points [10] or power stations [11,12]. One example is the wirelessly powered NOMA MEC IoT system proposed by Do *et al.* [12]. The study clarified the system performance regarding spectrum efficiency and significantly improved the MD lifetime.

However, NOMA-MEC-based networks still have an inherent risk because of the broadcast nature of wireless communication, which is the risk of information leakage [13]. Offloaded tasks from MD to MES can be eavesdropped by active or passive eavesdroppers, leading to an urgent need to pay attention to security issues for the success of the NOMA-MEC system. Accordingly, physical layer security (PLS) has been widely studied as a very effective wireless information security technique [14,15]. In the study [14], the authors investigated PLS-based MEC system with hybrid successive interference cancellation (SIC) technique deployed. The results show that the system performance outperforms the traditional OMA models.

According to the above discussion, the remaining problems in the RF EH NOMA Het-MEC network include eavesdropping devices that still need to be studied in depth to clarify. Therefore, in this study, we propose and investigate a secrecy task offloading model in RF EH NOMA Het-MEC networks. The main contributions of our paper are summarized as follows:

– We propose the downlink RF EH NOMA Het-MEC system model over Rayleigh fading channel. We correspondingly propose the energy-secrecy 4-phase offloading protocols based on NOMA.

– We derive the exact close-form expression of the secure successful completion probability (SSCP).
– We evaluate SSCP with essential system parameters, including time switching ratio, power allocation coefficient, task length, bandwidth, secure data rate threshold, and CPU operating frequency, to thoroughly comprehend the system's behavior.

The structure of the paper is presented as follows: Section 2 presents the system model and communication protocol. Section 3 presents the performance analysis. Section 4 describes the numerical results. Section 5 is the conclusion and future scope of the paper.

2 System Model

This study investigates an RF EH NOMA Het-MEC network model consisting of a wireless power station (P), a limited energy and computational resources edge user (U), and two MES deployed at two points access (APs) in the presence of a passive eavesdropper (E), as described in Fig. 1. Specifically, U has to handle an L-bit task, where each bit is independent of the other, for a maximum delay of T. However, U lacks the power and computing to complete the task independently. Therefore, U uses the power service to collect radio energy from P; then it uses all the received energy for offloading tasks to the APs, where AP_1 and AP_2 are denoted for the far and the near AP, respectively. Furthermore, in the AP_2 installation area, an eavesdropping device, denoted by E, intends to steal important information transmitted from U to AP_2.

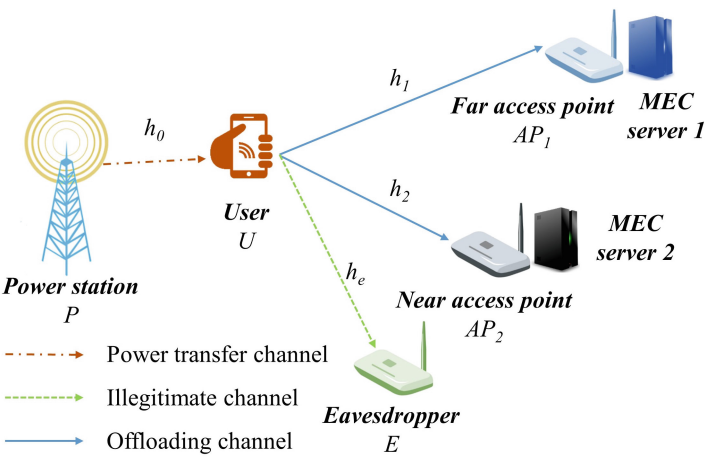

Fig. 1. The secrecy RF EH NOMA MEC system model.

Let h_0, h_1, h_2, and h_e be the channel coefficients from P to U, U to AP_1, U to AP_2, and U to E, respectively. Assume the devices in the proposed system are

equipped with a single antenna, operating in a half-duplex mode under Rayleigh fading channel. Channels are characterized by an average channel gain of λ_Ω ($\Omega \in \{0, 1, 2, e\}$). The system is affected by the additive white Gaussian noise (AWGN). Let g_0, g_1, g_2, and g_e be the channel power gain from P to U and from U to AP_1, AP_2, and E, respectively. Note that $g_\Omega = |h_\Omega|^2$.

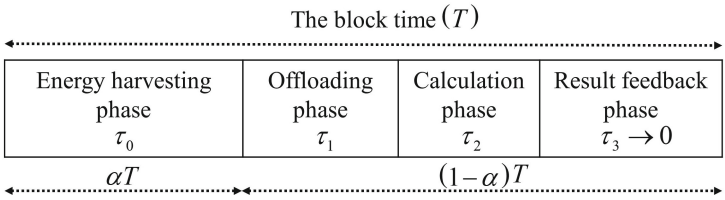

Fig. 2. Time diagram for proposed system.

Based on the proposed system model, we develop a NOMA-based offloading protocol that ensures the system's latency, energy, and security requirements, namely NOLES. Precisely, NOLES which have time diagram at Fig. 2, consists of 4 phases, described in detail as follows:

- Energy harvesting phase: In this phase, the channel parameters are estimated. Then, U collects radio energy from P for $\tau_0 = \alpha T$, where α is the time switching ratio. The formula describing the energy U obtained in this phase is:

$$E_U = \eta P_0 g_0 \alpha T, \tag{1}$$

where η stand for energy conversion efficiency, P_0 is the transmit power of P.

- The offloading phase: U uses the energy obtained in the EH phase to send a superimposed signal to APs using the downlink NOMA scheme:

$$\boldsymbol{x} = \sqrt{\rho} x_1 + \sqrt{1-\rho} x_2, \tag{2}$$

where x_1 and x_2 are tasks L_1 and L_2 bits are offloaded to AP_1 and AP_2 respectively; ρ stands for power allocation coefficient. Energy in NOMA-based systems is appropriately allocated to ensure user fairness; thus, the subtask x_1 that intends to offload for AP_1 will be allocated more power [11], i.e., $0.5 < \rho < 1$. During the offload period (τ_1), the signal is broadcast, so E also picks up the superimposed signal and tries to decode the important data at AP_2.

- The computing phase: In this context, the received signal at AP_1, AP_2, and E is as follow:

$$\begin{aligned} \boldsymbol{y}_\Omega &= \sqrt{P_U} h_\Omega \boldsymbol{x} + n_\Omega \\ &= \sqrt{P_U} h_\Omega (\sqrt{\rho} x_1 + \sqrt{1-\rho} x_2) + n_\Omega, \end{aligned} \tag{3}$$

where P_U is the transmit power of U, $P_U = \frac{E_U}{(1-\alpha)T-\tau} = \frac{\eta P_0 g_0 \alpha T}{(1-\alpha)T-\tau} = P_0 g_0 \mu$; $\mu = \frac{\eta \alpha T}{(1-\alpha)T-\tau}$; τ is the maximum computation time of APs, $\tau = \max\left\{\frac{c_1 L_1}{f_1}, \frac{c_2 L_2}{f_2}\right\}$;

c_i and f_i are the number of CPU cycles required to process one input bit, and the operating frequency of the MES located at AP_i, $i \in \{1, 2\}$, respectively; n_Ω is the AWGN has zero mean and variance δ^2, i.e., $n_i \sim \mathcal{CN}(0, \delta^2)$.

According to the NOMA scheme, APs apply SIC to decode the required signal. Since more power is allocated, x_1 is decoded directly. Then x_1 is removed from $\boldsymbol{y}$, and the signal x_2 is decoded later. Therefore, the signal-to-interference-plus-noise ratio (SINR) at AP_1 used for decoding x_1 is as follow:

$$\gamma_1 = \frac{\gamma_0 \mu \rho g_0 g_1}{\gamma_0 \mu \left(1 - \rho\right) g_0 g_1 + 1}, \tag{4}$$

where $\gamma_o = \frac{P_0}{\delta^2}$.

The signal-to-noise ratio (SNR) at AP_2 used for decoding x_2 is:

$$\gamma_2 = \gamma_0 \mu \left(1 - \rho\right) g_0 g_2. \tag{5}$$

Suppose E has the same decoding abilities as AP_2, and it employs SIC to detect the signal received [16]. The SNR at E used to decode signal x_2 is:

$$\gamma_e = \gamma_0 \mu \left(1 - \rho\right) g_0 g_e. \tag{6}$$

- The result feedback phase: During this phase, the resultant calculation information is feedbacked to the U during τ_3. Following [8,11], τ_3 is significantly short compared to τ_0, τ_1 and τ_2, hence it is ignored.

The cumulative distribution function (CDF) and probability density function (PDF) of the channel power gain $g_\Omega, \Omega \in \{1, 2, e\}$ are given as follows [5]:

$$F_{g_\Omega}\left(x\right) = 1 - \exp\left(-\frac{x}{\lambda_\Omega}\right), \tag{7}$$

$$f_{g_\Omega}\left(x\right) = \frac{1}{\lambda_\Omega} \exp\left(-\frac{x}{\lambda_\Omega}\right). \tag{8}$$

3 Performance Analysis

Different from the study [5,6,8], in this paper, we propose to use the secure successful computation probability (SSCP), denoted by ξ, which is the metric to evaluate the performance of the RF EH NOMA Het-MEC system. It is the probability that the security offload event occurs. Simply put, this event occurs when the system latency is lower than the maximum allowed time and the security capacity is above the secure data rate threshold.

$$\xi_S = \Pr\left(\max\left(\tau_1^{(i)} + \tau \leq \left(1 - \alpha\right) T\right), C_{2e} > R\right), \tag{9}$$

where $\tau_1^{(i)}$ is the offloading time for task $\boldsymbol{x}$ to AP_i, $\tau_1^{(i)} = \frac{L}{C_i} = \frac{L}{(1-\alpha) B \log_2(1+\gamma_i)}$; C_{2e} is the secrecy capacity at AP_2, $C_{2e} = \left(1 - \alpha\right) B \log_2\left(\frac{1+\gamma_2}{1+\gamma_e}\right)$; and R is the secure data rate threshold, B is the bandwidth.

Thus, we state **Theorem** 1 describing the SSCP expression as follows.

Theorem 1. *The SSCP of the proposed RF EH NOMA Het-MEC system operating under the NOLES protocol over the Rayleigh fading channel is given by:*

$$\xi_S = \begin{cases} 0, & \rho < 1 - \frac{1}{2^{\Lambda_1}} \\ 2\left[\sqrt{\frac{b_1}{\lambda_0}} K_1\left(2\sqrt{\frac{b_1}{\lambda_0}}\right) - \sqrt{\frac{b_2}{\lambda_0}} K_1\left(2\sqrt{\frac{b_2}{\lambda_0}}\right)\right] & \\ + \frac{2\lambda_2}{\lambda_0\left(\theta\lambda_e + \lambda_2\right)} \sqrt{b_3\lambda_0} K_1\left(2\sqrt{\frac{b_3}{\lambda_0}}\right), & \rho > 1 - \frac{1}{2^{\Lambda_1}} \end{cases} \tag{10}$$

where $b_1 = \frac{\beta_1}{\lambda_1} + \frac{\beta_2}{\lambda_2}$, $b_2 = \frac{\beta_1}{\lambda_1} + \frac{\beta_2}{\lambda_2} + \frac{\beta_3}{\lambda_e}$, $b_3 = \omega_1 + \omega_2 + \frac{\beta_1}{\lambda_1}$, $\omega_1 = \frac{a_1}{\lambda_2}$, $\omega_2 = \beta_3\left(\frac{\theta}{\lambda_2} + \frac{1}{\lambda_e}\right)$, $a_1 = \frac{\theta - 1}{\gamma_0\mu(1-\rho)}$, $\beta_1 = \frac{2^{\Lambda_1} - 1}{\mu\gamma_0\left[2^{\Lambda_1}(1-\rho)+1\right]}$, $\beta_2 = \frac{2^{\Lambda_2} - 1}{\mu\gamma_0(1-\rho)}$, $\beta_3 = \frac{\beta_2 - a_1}{\theta}$, $\theta = 2^{\frac{R}{1-\alpha}}$, $\Lambda_1 = (1-\alpha)\,BT_1$, $\Lambda_2 = (1-\alpha)\,BT_2$, $T_1 = (1-\alpha)\,T - \frac{c_1 L_1}{f_1}$, $T_2 = (1-\alpha)\,T - \frac{c_2 L_2}{f_2}$.

Proof. Please see Appendix A. □

4 Numerical Results and Discussion

This section provides the numerical results regarding the SSCP of the RF EH NOMA Het-MEC downlink system. The Monte-Carlo simulations are employed to confirm the analytical results. Table 1 details the typical values of simulation parameters utilized in our work [5,8].

Table 1. Simulation Parameters.

Parameters	Notation	Typical Values
Environment		Rayleigh
Fading parameter	λ_0,λ_1,λ_2	1
The average transmit SNR	γ_0	0–20 dB
The time switching ratio	α	0.4
The energy conversion efficiency	η	0.75
The power allocation coefficient	ρ	0.7
The CPU-cycle frequency of MES at AP_1, AP_2	f_1, f_2	2 GHz, 1 GHz
The number of CPU cycles for computing each bit of MES at AP_1, AP_2	c_1, c_2	5, 2
Channel bandwidth	B	100 MHz
The threshold of latency	T	0.5 s
The length of sub-task 1, sub-task 2	L_1, L_2	2.5 Mbits
The secure data rate threshold	R	0.1 bps/Hz

In the first experiment, we investigated the impact of the time switching ratio (α) with different values of block time (T) on system performance, as shown in Fig. 3. Note that the smaller T is, the more stringent the real-time constraint corresponds to, and the worse the SSCP. It entirely agrees with the

theoretical analysis presented in Section II. One more observation about the SSCP descriptive curve in this experiment shows that ξ_S is a function with extrema in α, i.e., there is a value $\alpha^\dagger$ such that maximum system performance. Therefore, when implementing the system in the real world, it is required to use strategies to determine $\alpha^\dagger$ so that EH time has a suitable value for U to collect sufficient operating energy and the remaining time is also enough for the process of offloading and computing to be performed.

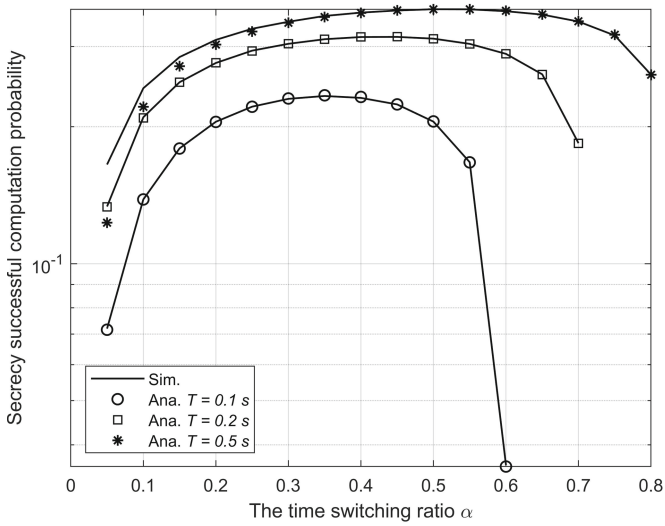

Fig. 3. SSCP vs. the time switching ratio with different values of block time.

In the next experiment, we investigate the impact of average transmit SNR (γ_0) with different bandwidth levels (B) on system performance, as shown in Fig. 4. Specifically, we examine three bandwidth levels, which are 50 MHz, 100 MHz, and 1 GHz. It is effortless to notice that the larger B or/and γ_0, the higher the SSCP. SSCP tends to saturate when γ_0 is greater than 15 dB and tends to saturate faster the larger B is. Therefore, depending on the bandwidth served for each application, we consider designing the transmit power accordingly.

Figure 5 depicts the curve of SSCP versus power allocation coefficient (ρ) with different task division ratios, denoted by ε, $\varepsilon = \frac{L_1}{L}$. We examine three cases, (i) $\varepsilon = 0.4$, (ii) $\varepsilon = 0.6$, and (iii) $\varepsilon = 0.8$. The graphs of all three cases show that the SSCP of the system is a function with extrema in ρ. It confirms that power allocation in a NOMA-based network is important for the best system performance. Furthermore, the correlation between the ε and ρ also gives us an exciting insight into the system behavior. The recommender system works well for case (i) with $0.5 < \rho < 0.65$. Meanwhile, in this range, (ii) makes SSCP low and (iii) makes the system outage. SSCP in (ii) is satisfactory only when

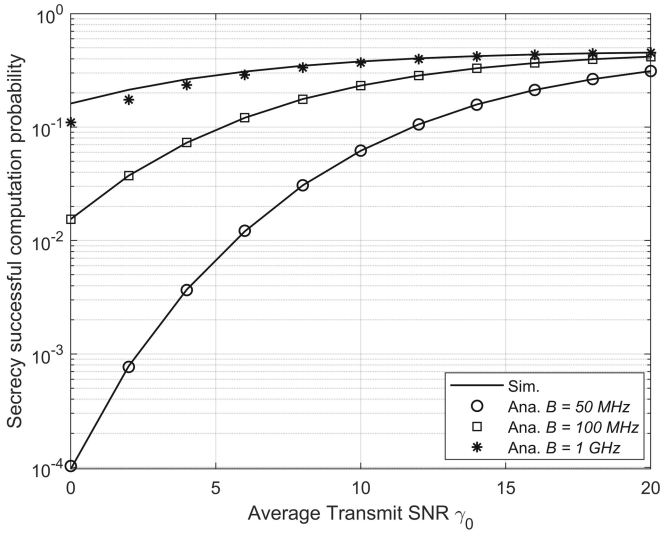

Fig. 4. SSCP vs. the average transmit SNR with different values of bandwidth.

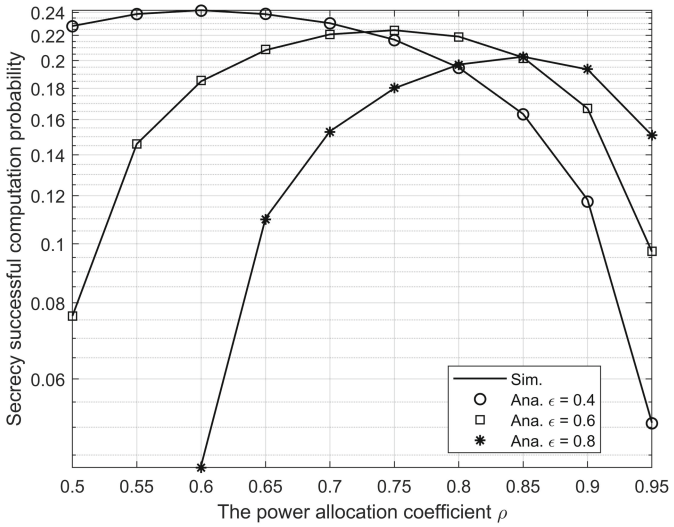

Fig. 5. SSCP vs. the power allocation coefficient with different task division ratios.

$0.7 < \rho < 0.8$, and (iii) is reasonable when $0.85 < \rho < 0.9$. Accordingly, with the Het-MEC network, it is necessary to have an optimal approach to offloading so that the system can achieve the highest performance corresponding to the available resources in the network. To put it succinctly, we need to clarify that tasks must be offloaded in the proper ratios for the system to be optimal.

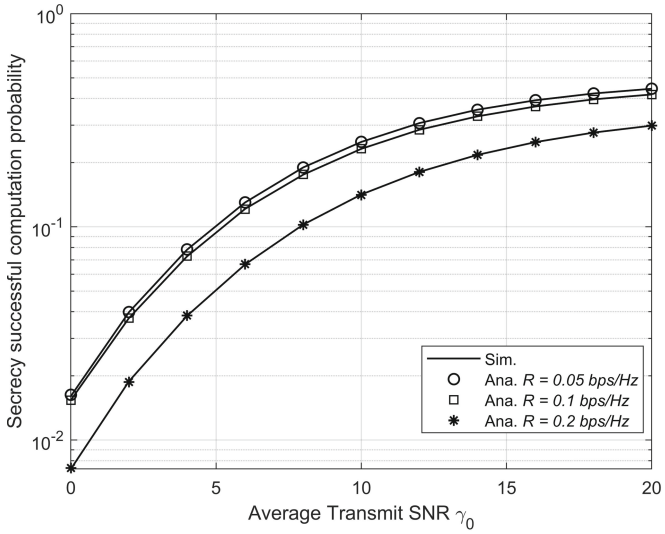

Fig. 6. SSCP vs. secure data rate thresholds.

In the final experiment, we studied the SSCP with different levels of secure data rate thresholds (R), 0.05 bps/Hz, 0.1 bps/Hz, and 0.2 bps/Hz, respectively, as Fig. 6. We conclude that increasing R can decrease SSCP. It is consistent with the definition of SSCP: as R increases, the possibility that the security capacity of the system will not meet the requirements also increases, leading to a decrease in SSCP.

Figure 3 to Fig. 6 all show that the simulated values match the computational theory. That proved the correctness of our study.

5 Conclusion

In this study, we evaluated the downlink RF EH NOMA Het-MEC network with the existence of a passive eavesdropper. Specifically, we consider the edge user to use the radio energy received from the power station to offload the task to two heterogeneous APs using NOMA over the Rayleigh channel. Accordingly, we propose the NOLES protocol for the system, ensuring it satisfies all three basic requirements of NOMA-MEC networks: delay time, energy, and security. We derive the exact closed-form expression of SSCP and perform system performance experiments versus essential system parameters. We give the following recommendations to improve system performance: (a) increase the transmit power of P, (b) increase the bandwidth for the application, (c) determine the optimal time switching ratio and/or power allocation coefficient.

In the next studies, we will deploy the low complexity optimization algorithms to determine the system parameters so that SSCP reaches the maximum value.

Acknowledgment. This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2021.11.

PROOF OF THEOREM 1

Based on the definition formula, SSCP is rewritten as follows:

$$\begin{aligned}\xi_S &= \Pr\left(\frac{L}{C_1} \le \underbrace{(1-\alpha)\,T - \frac{c_1 L_1}{f_1}}_{T_1}, \frac{L}{C_2} \le \underbrace{(1-\alpha)\,T - \frac{c_2 L_2}{f_2}}_{T_2}, C_{2e} > R\right) \\ &= \Pr\left(\gamma_1 > 2^{\Lambda_1} - 1, \gamma_2 > 2^{\Lambda_2} - 1, \frac{1+\gamma_2}{1+\gamma_e} > \underbrace{2^{\frac{R}{1-\alpha}}}_{\theta}\right) \\ &= \begin{cases} 0, & \rho < 1 - \frac{1}{2^{\Lambda_1}} \\ \Pr\left(g_1 > \frac{\beta_1}{g_0}, g_2 > \frac{\beta_2}{g_0}, g_2 > \frac{a_1}{g_o} + \theta g_e\right), & \rho > 1 - \frac{1}{2^{\Lambda_1}} \end{cases}\end{aligned} \tag{A-1}$$

where $a_1 = \frac{\theta-1}{\gamma_0\mu(1-\rho)}$, $\beta_1 = \frac{2^{\Lambda_1}-1}{\mu\gamma_0\left[2^{\Lambda_1}(1-\rho)+1\right]}$, $\beta_2 = \frac{2^{\Lambda_2}-1}{\mu\gamma_0(1-\rho)}$, $\Lambda_1 = (1-\alpha)\,BT_1$, $\Lambda_2 = (1-\alpha)\,BT_2$.

We focus the case $\rho > 1 - \frac{1}{2^{\Lambda_1}}$, then the SSCP is:

$$\begin{aligned}\xi_S &= \Pr\left(g_1 > \frac{\beta_1}{g_0}, g_2 > \frac{\beta_2}{g_0}, g_2 > \frac{a_1}{g_0} + \theta g_e\right) \\ &= \underbrace{\Pr\left(g_1 > \frac{\beta_1}{g_0}, g_2 > \frac{\beta_2}{g_0}, \frac{\beta_2}{g_0} > \frac{a_1}{g_0} + \theta g_e\right)}_{I_1} \\ &\quad + \underbrace{\Pr\left(g_1 > \frac{\beta_1}{g_0}, g_2 > \frac{a_1}{g_0} + \theta g_e, \frac{\beta_2}{g_0} < \frac{a_1}{g_0} + \theta g_e\right)}_{I_2}.\end{aligned} \tag{A-2}$$

We continue to present the calculation of I_1 as follows:

$$\begin{aligned}I_1 &= \Pr\left(g_1 > \frac{\beta_1}{g_0}, g_2 > \frac{\beta_2}{g_0}, g_e < \underbrace{\frac{\beta_2 - a_1}{\theta}}_{\beta_3}\frac{1}{g_0}\right) \\ &= \int_0^\infty \left[1 - F_{g_1}\left(\frac{\beta_1}{x}\right)\right]\left[1 - F_{g_2}\left(\frac{\beta_2}{x}\right)\right] F_{g_e}\left(\frac{\beta_3}{x}\right) f_{g_0}(x)\,dx \\ &= 2\left[\sqrt{\frac{b_1}{\lambda_0}} K_1\left(2\sqrt{\frac{b_1}{\lambda_0}}\right) - \sqrt{\frac{b_2}{\lambda_0}} K_1\left(2\sqrt{\frac{b_2}{\lambda_0}}\right)\right],\end{aligned} \tag{A-3}$$

where $b_1 = \frac{\beta_1}{\lambda_1} + \frac{\beta_2}{\lambda_2}$, $b_2 = \frac{\beta_1}{\lambda_1} + \frac{\beta_2}{\lambda_2} + \frac{\beta_3}{\lambda_e}$.

Similarly, I_2 is calculated as follows:

$$\begin{aligned} I_2 &= \Pr\left(g_1 > \frac{\beta_1}{g_0}, g_2 > \frac{a_1}{g_o} + \theta g_e, g_e > \frac{\beta_3}{g_0}\right) \\ &= \int_0^{\infty} \int_{\beta_3/x}^{\infty} \left[1 - F_{g_1}\left(\frac{\beta_1}{x}\right)\right] \left[1 - F_{g_2}\left(\frac{a_1}{x} + \theta t\right)\right] f_{g_0}(x) f_{g_e}(t)\, dxdt \\ &= \frac{2\lambda_2}{\lambda_0(\theta\lambda_e + \lambda_2)} \sqrt{b_3\lambda_0} K_1\left(2\sqrt{\frac{b_3}{\lambda_0}}\right), \end{aligned} \tag{A-4}$$

where $b_3 = \omega_1 + \omega_2 + \frac{\beta_1}{\lambda_1}$, $\omega_1 = \frac{a_1}{\lambda_2}, \omega_2 = \beta_3\left(\frac{\theta}{\lambda_2} + \frac{1}{\lambda_e}\right)$.

Combining the results from (A-1) to (A-4), we get the result in **Theorem** 1. The proof is completed.

References

1. Parvez, I., Rahmati, A., Guvenc, I., Sarwat, A.I., Dai, H.: A survey on low latency towards 5G: RAN, core network and caching solutions. IEEE Commun. Surv. Tut. **20**(4), 3098–3130 (2018)
2. Siddiqi, M.A., Yu, H., Joung, J.: 5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices. Electronics **8**(9), 981 (2019)
3. Xu, Y., Gui, G., Gacanin, H., Adachi, F.: A survey on resource allocation for 5G heterogeneous networks: current research, future trends, and challenges. IEEE Commun. Surv. Tut. **23**(2), 668–695 (2021)
4. Maray, M., Shuja, J.: Computation offloading in Mobile Cloud Computing and Mobile Edge Computing: survey, taxonomy, and open issues. Mobile Inform. Syst. **2022** (2022)
5. Truong, V.-T., Ha, D.-B., So-In, C., et al.: On the system performance of mobile edge computing in an uplink NOMA WSN with a multiantenna access point over Nakagami-m fading. IEEE/CAA J. Automatica Sinica **9**(4), 668–685 (2022)
6. Ha, D.-B., Truong, V.-T., Ha, D.-H.: A novel secure protocol for mobile edge computing network applied downlink NOMA. In: Vo, N.-S., Hoang, V.-P. (eds.) INISCOM 2020. LNICST, vol. 334, pp. 324–336. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-63083-6_25
7. Ding, Z., Xu, D., Schober, R., Poor, H.V.: Hybrid NOMA offloading in multi-user MEC networks. IEEE Trans. Wireless Commun. (2022)
8. Truong, V.-T., Vo, M.-T., Ha, D.-B.: Performance analysis of mobile edge computing network applied uplink NOMA with RF energy harvesting. In: Vo, N.-S., Hoang, V.-P., Vien, Q.-T. (eds.) INISCOM 2021. LNICST, vol. 379, pp. 57–72. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77424-0_6
9. Qiu, H., Gao, S., Chen, Y., Tu, G.: Energy-efficient rate allocation for NOMA-MEC offloading under outage constraints. IEEE Commun. Lett. **26**(11), 2710–2714 (2022)
10. Pei, L., et al.: Energy-efficient D2D communications underlaying NOMA-based networks with energy harvesting. IEEE Commun. Lett. **22**(5), 914–917 (2018)

11. Truong, V.-T., Ha, D.-B.: Secured scheme for RF energy harvesting Mobile Edge Computing networks based on NOMA and access point selection. In: 7th NAFOSTED Conference on Information and Computer Science (NICS), vol. 2020, pp. 7–12. IEEE (2020)
12. Do, D.-T., Van Nguyen, M.-S., Nguyen, T.N., Li, X., Choi, K.: Enabling multiple power beacons for uplink of NOMA-enabled mobile edge computing in wirelessly powered IoT. IEEE Access **8**, 148892–148905 (2020)
13. Mao, Y., You, C., Zhang, J., Huang, K., Letaief, K.B.: A survey on mobile edge computing: the communication perspective. IEEE Commun. Surveys Tut. **19**(4), 2322–2358 (2017)
14. Wang, K., Li, H., Ding, Z., Xiao, P.: Reinforcement learning based latency minimization in secure NOMA-MEC systems with hybrid SIC. IEEE Trans. Wireless Commun. (2022)
15. Wang, Q., Hu, H., Hu, R.Q., et al.: Secure and energy-efficient offloading and resource allocation in a NOMA-based MEC network. In: IEEE/ACM Symposium on Edge Computing (SEC), vol. 2020, pp. 420–424. IEEE (2020)
16. Xiang, Z., Yang, W., Cai, Y., Ding, Z., Song, Y., Zou, Y.: NOMA-assisted secure short-packet communications in IoT. IEEE Wireless Commun. **27**(4), 8–15 (2020)