Secure Mobile Edge Computing Networks in the Presence of Multiple Eavesdroppers

Xiazhi Lai, Lisheng Fan, Xianfu Lei, Yansha Deng, George K. Karagiannidis, *Fellow, IEEE* and Arumugam Nallanathan, *Fellow, IEEE*

Abstract

In this paper, we investigate a secure mobile edge computing (MEC) network in the presence of multiple eavesdroppers, where multiple users can offload parts of their tasks to the computational access point (CAP). The multiple eavesdroppers may overhear the confidential task offloading, which leads to information leakage. In order to address this issue, we present the minimization problem of the secrecy outage probability (SOP), by jointly taking into account the constraints from the latency and energy consumption. With the aim to improve the system secrecy performance, we then introduce three user selection criteria to choose the best user among multiple ones. Specifically, *criterion I* maximizes the locally computational capacity, while *criterion II* and *III* maximize the secrecy capacity and data rate of main links, respectively. For these criteria, we further analyze the system secrecy performance by deriving analytical and asymptotic expressions for the SOP, from which we can conclude important insights for the system design. Finally, simulation and analytical results are provided to verify the proposed analysis. The results show that the three criteria can efficiently safeguard the MEC networks, compared to the traditional local computing and fully offloading, especially with a large value of user number.

X. Lai and L. Fan are with the School of Computer Science and Cyber Engineering, Guangzhou University, China (e-mail: lsfan@gzhu.edu.cn).

X. Lei is with the School of Information Science and Technology, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu 610031, China (e-mail: xflei@home.swjtu.edu.cn).

Y. Deng is with the Department of Informatics, King's College London, London WC2R 2LS, UK (e-mail: yansha.deng@kcl.ac.uk).

G. K. Karagiannidis is with the Wireless Communications and Information Processing (WCIP) Group, Electrical and Computer Engineering Dept., Aristotle University of Thessaloniki, Thessaloniki 54 124, Greece (e-mail: geokarag@auth.gr).

A. Nallanathan is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London, U.K (e-mail: a.nallanathan@qmul.ac.uk).

Index Terms

Secure communication, mobile edge computing, user selection, latency, energy consumption, secrecy outage probability.

I. Introduction

The development and deployment of the fifth-generation (5G) wireless networks and the roadmap towards the sixth-generation (6G) have enabled the research community to investigate new methods for high-speed data rate, ultra-low latency and ubiquitous access, in order to launch intelligent applications, such as autonomous driving and smart healthcare [1]–[4]. One major characteristic of these new applications is the need for intensive computation, which clearly shows the evolution from traditional *communication-oriented* to *computation-oriented* systems. In the computational-oriented systems, the performance metrics of interest have extended from those related to traditional communication quality, such as the data rate and bit error rate, to latency, energy consumption, etc [5], [6]. To support these new applications with the need of intensive computation load, one solution is to compute the tasks in the cloud server, which however, imposes a huge burden on the communication and may cause a large latency and energy consumption. To alleviate this, mobile edge computing (MEC) has been proposed, which exploits the computational capability of near-by devices through offloading some parts of the users' tasks [7]–[9]. It has been widely shown in the literature that MEC can reduce the system latency and energy consumption, and so, it can be efficiently used to support applications of 5G and 6G networks [10]–[13].

A. Literature

In MEC networks, offloading is a key method to improve the system performance, by reducing the latency and energy consumption. The offloading policy determines how many parts of tasks will be computed by the computational access points (CAPs) [14]–[18]. In this direction, the authors in [19] investigated a joint offloading and computing optimization for MEC networks, where an optimal resource allocation scheme was developed to minimize the energy consumption at the CAP. Specifically, for the unmanned aerial vehicle (UAV)-enabled MEC networks, partial or binary computation offloading mode can be used to maximize the computation rate [20].

Later, the system computation efficiency of the wireless-powered MEC networks was effectively enhanced by jointly devising the offloading strategy and the local computing frequency [21]. Furthermore, the impact of energy and task causality on the MEC networks was investigated, where task offloading and local computing along with the energy beamforming were jointly optimized to minimize the system energy consumption [22]. Finally, the authors in [23] proposed an offloading strategy for MEC networks with multiple CAPs, where both selection and switch-and-stay combining protocols were employed to reduce the system latency and energy consumption.

Due to the nature of broadcasting, wireless offloading may be overheard by eavesdroppers in MEC networks. This leads to information leakage, and thus, it is of vital importance to safeguard the wireless offloading process from the physical to application layers. Compared with the encryption based secure methods, a physical-layer based security method has lower complexity and attracts increasing attention from the researchers [24]. Physical-layer security of wireless transmission can be improved by exploiting the system resources, such as signal, user and relays. In this direction, the authors in [2], [25] developed a secure transmission scheme, based on the signal constellation overlapping, where an experimental platform was implemented to secure the transmission over a two-way untrusted relaying system. For relaying networks with multiple antennas, the system secrecy data rate can be maximized by using beamforming, which exploits the signal fluctuation among multiple antennas [26]. Moreover, relaying or user selection could be applied to wireless communication systems with multiple relays or users, where the channel fluctuation among them was exploited to improve the secrecy data rate and secrecy outage probability (SOP) [27], [28]. Furthermore, for the cache-aided relaying networks, the system secure transmission could be secured by exploiting the caching resources, where several caching strategies were investigated for the secure transmission through providing the asymptotic SOP expressions in the high regime of signal-to-noise ratio (SNR) and main-to-eavesdropper ratio (MER) [29]. Besides the eavesdropping mode in the above works, some other attack modes such as jamming and spoofing were investigated in [30]–[32], where intelligent learning based algorithms such as Q-learning algorithm were employed to prevent the intelligent attackers. Although the existing works have extensively studied the physical-layer security of wireless transmission, there has been little work on the secure transmission of MEC networks, which motivates the work in this paper.

B. Contribution

In this paper, we study a secure MEC network in the presence of multiple eavesdroppers, where multiple users can offload some parts of task to the CAP. The task offloading may be overheard by the multiple eavesdroppers in the network, which causes the severe issue of information leakage. We start with the critical question: *"How to optimize the secrecy outage probability in the secure MEC networks?"*. To answer this question, we firstly present the minimization problem of the secrecy outage probability (SOP), by jointly taking into account the constraints from the latency and energy consumption. In order to improve the network secrecy performance, we then employ three user selection criteria to choose one best user among multiple ones to be assisted by the CAP. Specifically, *criterion I* maximizes the locally computational capacity, while *criterion II* and *III* maximize the secrecy capacity and data rate of main links, respectively.

We proceed with the following important question: *"What is the effect of the system parameters on the secure MEC networks design?"*. To tackle this problem, we study the system secrecy performance of the secure MEC networks, by deriving analytical and asymptotic expressions for the SOP of the three user selection criteria. We further analyze how the system SOP is related to the network parameters, from which we obtain important insights for the system design. Simulations and numerical results are finally presented to verify the proposed analysis. In particular, the simulation results show that the three criteria can efficiently safeguard the MEC networks, compared to the traditional local computing and fully offloading, especially with a large value of user number.

The main contributions of this work are summarized as follows:

- We investigate a secure MEC network in the presence of multiple eavesdroppers, and present the SOP minimization problem by jointly taking into account the constraints from the latency and energy consumption.
- To improve the system secrecy performance, we provide three user selection criteria to choose the best user among multiple ones, based on the computational capability and channel parameters, respectively.
- For the three user selection criteria, we analyze the system secrecy performance by deriving analytical SOP expressions, in order to evaluate the impact of network parameters on the secrecy performance in the entire MER regime.

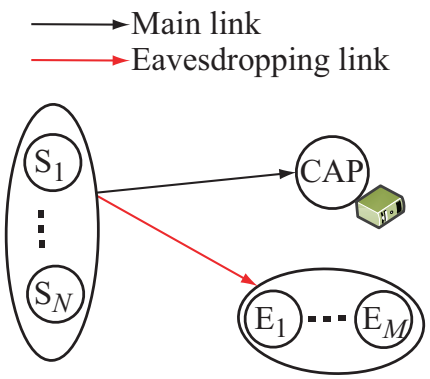

Fig. 1. Secure MEC networks in the presence of multiple eavesdroppers.

- For the three criteria, we also derive asymptotic SOP expressions in the high MER regime, to determine the key factors, that govern the network secrecy performance. From the asymptotic expressions, we can find that the three criteria can efficiently safeguard the MEC networks, compared to the traditional local computing and fully offloading, especially with a large value of user number.

C. Structure

The organization of this paper is as follows. After the introduction, Section II describes the system model of the secure MEC networks, while Section III presents the SOP minimization problem and provides three user selection criteria for the considered secure MEC networks. In further, Section IV provides an analysis for the SOP, by deriving analytical and asymptotic expressions. Finally, Section V presents numerical and simulation results and Section VI concludes this paper.

II. System Model

Fig. 1 presents the system model of the MEC network under Rayleigh fading, with N users $\{S_n|1 \leq n \leq N\}$ and one CAP, where the users have some confidential tasks to be computed with the help of the CAP. This system can be applied to a single-cell network, or multi-cell network with cell planning or Gaussian distributed interference. The users have limited computational capability, denoted by the local CPU-cycle frequency set $\{g_n|1 \leq n \leq N\}$. Moreover, g_n may vary in practice, due to many factors such as the dynamic tasks and processes in the user terminal.

Without loss of generality, we assume that g_n follows the uniform distribution [14]–[16], within the interval of $[g_{min}, g_{max}]$[1]. To alleviate the computational burden at users, the CAP with a much more powerful computational capability can help users compute the tasks, through the wireless transmission from the users to the CAP, subject to Rayleigh fading. As the existing M eavesdroppers in the network can overhear the transmission of the confidential task, the severe issue of information leakage may be caused. All nodes in the network have a single antenna due to the size limitation, and the links in the network experience Rayleigh fading[2], without loss of generality.

Besides the single-cell network, the considered system model can be applied to the multi-cell network, in the following several folds. Firstly, the considered system model in this paper is applicable to the multi-cell network with cell planning, where different cells use some orthogonal frequency spectrums, and the network degenerates into multiple single-cell networks. Secondly, the considered system model in this paper is still applicable for the multi-cell network with reuse of frequency spectrums, as the interference among cells can be suppressed by some methods such as beamforming, and the residual interference can be modeled by the Gaussian noise, through some design techniques such as random pilot design [33], which can be found in the 4G LTE and 5G new radio networks. Thirdly, even for the multi-cell network with interference which may not be modeled by the Gaussian noise, the work in this paper is still meaningful, as it can provide an important reference for the system design.

All the N users can simultaneously communicate with the CAP, or one user is selected to communicate with the CAP. As the former mode may cause interference among users and asks for a very complicated receiver structure at the CAP, the user selection technique is adopted in this work, in which one user is selected among N to communicate with the CAP. We assume that the n-th user S_n is selected to compute the task, which contains L bits and the offloading ratio is $\rho \in [0, 1]$. In other words, the $(1-\rho)$ part of the task is computed locally, while the rest

[1]When the local CPU frequency follows some other kinds of distribution, such as normal distribution or exponential distribution, the results in this work will be changed accordingly, whereas the analysis method in this work can be easily extended.

[2]Rayleigh fading model is suitable for wireless communications in urban and indoor areas, where the prorogation of radio signals are usually scattered by buildings and no light-of-sight wireless channels is available. Thus, flat Rayleigh fading environment has been widely studied in the literature such as the works in [18], [19], [23]. The results in this work can be easily extended to other fading model, such as Nakagami-m fading.

ρ part is computed by the CAP.

If the task is completely computed locally with $\rho = 0$, the local latency T_0 and energy consumption E_0 are given by

$$T_0 = \frac{L\eta}{g_n}, \tag{1}$$

$$E_0 = \frac{P_0 L\eta}{g_n}, \tag{2}$$

where η is the number of CPU cycles required by one bit of the computational task, and P_0 is the locally computational power.

When the task offloading occurs with $\rho > 0$, the data is transmitted through the wireless link from S_n to the CAP. Let $h_n \sim \mathcal{CN}(0, \alpha)$ and $h^e_{n,m} \sim \mathcal{CN}(0, \beta)$ denote the instantaneous channel parameters from S_n to the CAP and eavesdropper E_m, respectively. When the eavesdroppers overhear in a non-colluding mode, the system secrecy data rate is given by

$$C_{n,s} = W_B \Big[\log_2 \Big(1 + \frac{P_S}{\sigma^2}|h_n|^2\Big) - \log_2 \Big(1 + \frac{P_S}{\sigma^2}|h^e_n|^2\Big) \Big]^+, \tag{3}$$

where W_B is the wireless bandwidth, P_S is the transmit power at users, σ^2 is the variance of the additional white Gaussian noise (AWGN) and residual interference at the receiver, and $|h^e_n|^2 = \max_{1\le n\le N} |h^e_{n,m}|^2$ is the largest channel gain of the eavesdropping links. In practice, $C_{n,s}$ is varying and it is difficult for the system to transmit at the secrecy data rate of $C_{n,s}$. Accordingly, the communication system turns to transmit at a given secrecy data rate C_t, which is easily implemented in practice. In this case, the transmission latency T_S and energy consumption E_S with $\rho = 1$ are given by

$$T_S = \frac{L}{C_t}, \tag{4}$$

$$E_S = \frac{P_S L}{C_t}. \tag{5}$$

The associated computational latency T_C and energy consumption E_C at the CAP with $\rho = 1$ are given by

$$T_C = \frac{L\eta}{g_c}, \tag{6}$$

$$E_C = \frac{P_C L\eta}{g_c}, \tag{7}$$

where g_c is the CPU-cycle frequency of the CAP. By summarizing the above latency and energy consumption, and incorporating the offloading ratio ρ, we can obtain the system latency $t_{n,A}$ and energy consumption $E_{n,A}$ associated with user S_n as

$$t_{n,A} = \max\left[(1-\rho)T_0, \rho T_S + \rho T_C\right], \tag{8}$$

$$E_{n,A} = (1-\rho)E_0 + \rho E_S + \rho E_C, \tag{9}$$

where the max operation is used in (8), since the local computing and the offloading of confidential data as well as the edge computing can be executed in parallel. Hence, the system latency is the maximum value between the latency of local computing and the latency of offloading as well as the edge computing. In contrast, to fulfill the computational task, the procedures including local computing, offloading and edge computing consume energy. Hence, the sum operation is used in the calculation of energy consumption in (9).

III. SOP Minimization Problem and User Selection Criteria

In the traditional physical-layer security theory, the outage probability is defined as the probability that the instantaneous secrecy data rate $C_{n,s}$ falls below the target secrecy data rate C_t. In the secure MEC networks, except from the secrecy data rate, the constraints from the latency and energy consumption should be also taken into account in the minimization problem of the secrecy outage probability. In particular, the latency is important for the real-time control systems, while the energy consumption is of vital importance for the limited-battery scenarios. By jointly taking into account the impact from the latency and energy consumption, we aim to minimize the secrecy outage probability for the secure MEC networks under the constraints from the latency and energy consumption, which can be formulated as

$$\min_{\rho} \quad P_{n,out} = \Pr(C_{n,s} < C_t), \tag{10a}$$

$$s.t. \quad t_{n,A} \leq \gamma_T, \tag{10b}$$

$$E_{n,A} \leq \gamma_E, \tag{10c}$$

where γ_T and γ_E are the thresholds of the latency and energy consumption, respectively. We can observe from (10) that the system secrecy outage event occurs when the secrecy data rate $C_{n,s}$ is below the target secrecy data rate C_t, and the setting of the offloading ratio should meet the requirements from the latency and energy consumption.

In further, we propose several user selection criteria to choose one best user S_{n^*} among N ones, in order to enhance the system SOP performance, through exploiting the computational and communication resources. In the following, we present three selection criteria based on the computational capability, the instantaneous CSI of both main and eavesdropping links, and the instantaneous CSI of main link only, respectively.

A. *Criterion I*

In this criterion, we choose the best user S_{n^*} which has the most powerful computational capacity, given by

$$n^* = \arg \max_{1 \le n \le N} g_n, \tag{10}$$

which leads to the largest CPU-cycle frequency of users. To implement this criterion, the CAP can firstly collect the CPU-cycle frequencies of N users, and then perform the user selection. After that, the selection result is notified to the users through some dedicated feedback links.

B. *Criterion II*

If the instantaneous CSI of both the main and eavesdropping links is known, we can select the best user S_{n^*} through maximizing the secrecy data rate $C_{n,s}$,

$$n^* = \arg \max_{1 \le n \le N} \left(\frac{1 + \frac{P_S}{\sigma^2} |h_n|^2}{1 + \frac{P_S}{\sigma^2} |h_n^e|^2} \right). \tag{11}$$

To implement this criterion, the CAP and eavesdroppers can firstly estimate the channel parameters of the links to the users, through the help of some pilot signals from the users. Then, the CAP can gather the required channel information and perform the user selection. If only a part of eavesdroppers are willing to feedback the channel information, i.e., the instantaneous channel information from only a part of eavesdroppers is known, criterion II will change from (11) to

$$n^* = \arg \max_{n \in \Omega} \left(\frac{1 + \frac{P_S}{\sigma^2} |h_n|^2}{1 + \frac{P_S}{\sigma^2} |h_n^e|^2} \right), \tag{12}$$

where Ω denotes the set of eavesdroppers whose instantaneous channel information is known.

If none of the eavesdroppers is willing to feedback the channel information, the following criterion III will be used instead.

C. Criterion III

If the instantaneous CSI of the eavesdropping links is hard to obtain, we can perform the user selection through maximizing the data rate of the main links,

$$n^* = \arg \max_{1 \le n \le N} |h_n|^2, \tag{13}$$

which leads to the largest received signal-to-noise-plus-interference ratio (SINR) at the CAP. To implement this criterion, the CAP can firstly estimate the channel parameters of the links with users, aided by the pilot signals from the users. Then, the CAP can gather these channel information and perform the user selection. In particular, criterion III can be regarded as a degenerated version of criterion II with statistical channel information of eavesdropping links [3].

Overall, the above three user selection criteria provide a flexible choice for the system design of the considered secure MEC networks. Specifically, if the system is sensitive to the computational capability, criterion I tends to be used to achieve the fastest CPU-cycle frequency. On the other hand, if the system is sensitive to the wireless channels, criterion II and III can be used to choose the best user. In particular, criterion II should be used to implement the user selection if the instantaneous channel information of eavesdropping links is known. If the instantaneous channel information of eavesdropping links is unknown, i.e., only the statistical channel information of eavesdropping links is known or even no channel information of eavesdropping links is known, we should turn to use criterion I or III to perform the user selection. In particular, criterion III can be regarded as a degenerated version of criterion II with statistical channel information of eavesdropping links. In a word, we can flexibly choose one user selection criterion according to the specific requirement on the computation and communication.

IV. Analysis of the Secrecy Outage Probability

In this part, we investigate the system secrecy performance by providing analytical and analytical expressions for the SOP, under the constraints of both latency and energy consumption.

[3]If only statistical channel information of eavesdropping links is known, criterion II should be devised as $n^* = \arg\max_{1\le n\le N}\left(\frac{1+\frac{P_S}{\sigma^2}|h_n|^2}{1+\frac{P_S}{\sigma^2}E\{|h_n^e|^2\}}\right)$, where the operation $E\{\dot{}\}$ denotes the statistical average. When the users form a cluster which has the same distance to the eavesdropper, $E\{|h_n^e|^2\}$ will be the same for the users, and the selection criterion of $n^* = \arg\max_{1\le n\le N}\left(\frac{1+\frac{P_S}{\sigma^2}|h_n|^2}{1+\frac{P_S}{\sigma^2}E\{|h_n^e|^2\}}\right)$ will degenerate into $n^* = \arg\max_{1\le n\le N}|h_n|^2$.

For the selected user S_{n^*}, from (8), we can know that the latency constraint $t_{n^*,A} \leq \gamma_T$ is equivalent to

$$\begin{cases} \rho \geq \rho_1^*, \\ T_S \leq \frac{\gamma_T}{\rho} - T_C, \end{cases} \tag{14}$$

with

$$\rho_1^* = 1 - \frac{\gamma_T}{T_0}. \tag{15}$$

From (9), the constraint of energy consumption of $E_{n^*,A} \leq \gamma_E$ is equivalent to

$$T_S \leq \frac{E_0 - E_C}{P_S} - \frac{E_0 - \gamma_E}{P_S \rho}. \tag{16}$$

By applying the constraint transformation in (14) and (16), we can re-write P_{out} as

$$P_{out} = 1 - \Pr(T_S \leq d(g_{n^*}), C_{n^*,s} \geq C_t) \tag{17}$$

where

$$d(g_{n^*}) = \min\left(\frac{\gamma_T}{\rho} - T_C, \frac{1}{P_S}\left(E_0 - E_C - \frac{E_0 - \gamma_E}{\rho}\right)\right). \tag{18}$$

Through the relationship of $T_S = \frac{L}{C_t}$ and $T_S \leq d(g_{n^*})$, we can further write P_{out} as

$$P_{out} = 1 - \Pr\left(C_{n^*,s} \geq \frac{L}{d(g_{n^*})}\right) \tag{19}$$

$$= \int_0^\infty F_{C_{n^*,s}}\left(\frac{L}{d(v)}\right) f_{g_{n^*}}(v) dv, \tag{20}$$

where $F_{C_{n^*,s}}(x)$ is the CDF of the secrecy data rate[4], and $f_{g_{n^*}}(v)$ is the PDF of the computational capability of user S_{n^*}.

A. *Analysis on the offloading ratio*

From (20), we can find that the system SOP improves with the increased value of $d(v)$. Hence, we can obtain the optimal offloading ratio ρ^* in the following proposition,

[4]The subsequent analysis of this paper considers the Rayleigh fading. If some other kinds of channel fading are used such as Nakagami-m fading, we can easily obtain the analytical results, through replacing the CDF of (20) by the CDF under the other channel fading models.

Proposition 1: The optimal offloading ratio ρ^* of the considered secure MEC networks is given by,

$$\rho^* = \begin{cases} 1, & \text{If } \rho_2^* > 1 \\ \rho_2^*, & \text{If } \rho_1^* \leq \rho_2^* \leq 1 \\ \rho_1^*, & \text{If } \rho_2^* < \rho_1^* \end{cases} \tag{21}$$

where ρ_1^* is given in (15) and ρ_2^* is

$$\rho_2^* = \frac{E_0 - \gamma_E + P_S\gamma_T}{E_0 - E_C + P_S T_C}. \tag{22}$$

Proof: See Appendix A. ■

From the optimal offloading ratio ρ^* in Proposition 1, we can obtain the optimal value of $d(g_{n^*})$ as

$$d^*(g_{n^*}) = \begin{cases} \frac{\gamma_E - E_C}{P_S}, & \text{If } P_S > \gamma_P \\ \psi_1(g_{n^*}), & \text{If } P_C \leq P_S \leq \gamma_P \\ \psi_2(g_{n^*}), & \text{If } P_S < \min(P_C, \gamma_P),\ g_{n^*} \geq \gamma_f \\ \psi_1(g_{n^*}), & \text{If } P_S < \min(P_C, \gamma_P),\ g_{n^*} < \gamma_f \end{cases}, \tag{23}$$

where

$$\psi_1(g_{n^*}) = \frac{\gamma_T P_0 L\eta - \gamma_T(E_C - P_S T_C)g_{n^*}}{P_0 L\eta - (\gamma_E - P_S\gamma_T)g_{n^*}} - T_C, \tag{24}$$

$$\psi_2(g_{n^*}) = \frac{\gamma_T L\eta}{L\eta - \gamma_T g_{n^*}} - T_C, \tag{25}$$

$$\gamma_f = \frac{L\eta(E_C + \gamma_T P_0 + P_S\gamma_T - T_C P_S - \gamma_E)}{\gamma_T T_C(P_0 - P_S)}, \tag{26}$$

$$\gamma_P = \frac{\gamma_E - E_C}{\gamma_T - T_C}. \tag{27}$$

From Proposition 1, we can see that the optimization of the offloading ratio needs to know the local information on the CPU-cycle frequency of the selected user S_{n^*}. In addition, we can obtain the following insights on the system,

- When the transmit power is large with $P_S > \gamma_P$, the system SOP is irrelative to the latency threshold γ_T, and it only depends on the energy consumption threshold γ_E. This

is because that the transmission latency becomes negligible and the energy consumption becomes dominant in the outage event.

- When the transmit power is small with $P_S \leq \gamma_P$, both the latency threshold γ_T and energy consumption threshold γ_E will affect the system SOP, as the transmission latency cannot be ignored when the transmit power is not high.
- As $d^*(g_{n^*})$ is a decreasing function with respect to L, an increased size of the computational task will deteriorate the secrecy outage probability.

From the maximum value of $d^*(g_{n^*})$ in (23), we can write the system SOP of the considered secure MEC networks with the optimal offloading ratio as

$$P_{out} = \int_0^\infty F_{C_{n^*,s}}\Big(\frac{L}{d^*(v)}\Big) f_{g_{n^*}}(v) dv. \tag{28}$$

In the following, we will derive the analytical and asymptotic expressions of SOP for the three user selection criteria.

B. Secure Outage Probability of Criterion I

1) Analytical secrecy outage probability of criterion I: To compute the analytical SOP for criterion I, we need to firstly calculate the CDF of $C_{n^*,s}$, which is given by the following theorem,

Theorem 1: The CDF of $C_{n^*,s}$ for criterion I is given by

$$F_{C_{n^*,s},I}(x) = 1 - \sum_{m=0}^{M-1} \frac{(-1)^m \binom{M-1}{m} \alpha M}{\alpha(m+1) + 2^{\frac{x}{W_B}}\beta} \exp\Big(-\frac{2^{\frac{x}{W_B}} - 1}{\alpha P_S/\sigma^2}\Big). \tag{29}$$

Proof: See Appendix B. ■

Then, we turn to compute the PDF of g_{n^*}. Note that the RV g_n follows the uniform distribution, and its PDF is given by

$$f_{g_n}(v) = \begin{cases} \dfrac{1}{g_{max} - g_{min}}, & \text{If } v \in [g_{min}, g_{max}] \\ 0, & \text{Else} \end{cases}. \tag{30}$$

From the order theory [34], we can obtain the PDF of RV $g_{n^*} = \max_{1 \leq n \leq N} g_n$ as

$$f_{g_{n^*}}(v) = \begin{cases} \dfrac{N(v - g_{min})^{N-1}}{(g_{max} - g_{min})^N}, & \text{If } v \in [g_{min}, g_{max}] \\ 0, & \text{Else} \end{cases}. \tag{31}$$

Applying the results of (31) and Theorem 1, we can write the SOP of criterion I as

$$P_{out,I} = 1 - \sum_{m=0}^{M-1} \frac{(-1)^m \binom{M-1}{m} \alpha N M}{(g_{max} - g_{min})^N} \int_{g_{min}}^{g_{max}} \left(\alpha(m+1) + 2^{\frac{L}{d^*(v)W_B}} \beta\right)^{-1}$$
$$\times \exp\left(-\frac{2^{\frac{L}{d^*(v)W_B}} - 1}{\alpha P_S/\sigma^2}\right)(v - g_{min})^{N-1} dv. \tag{32}$$

As it is difficult to directly solve the above integral, we turn to use the widely used Gaussian-Chebyshev approximation [35]. We firstly apply the variable substitution of $v = \frac{g_{max}-g_{min}}{2} w + \frac{g_{max}+g_{min}}{2}$ into (32), and then compute the analytical expression of $P_{out,I}$ as

$$P_{out,I} = 1 - \sum_{m=0}^{M-1} \frac{(-1)^m \binom{M-1}{m} \alpha N M}{2(g_{max} - g_{min})^{N-1}} \int_{-1}^{1} \left(\alpha(m+1) + 2^{\frac{L}{d^*(w)W_B}} \beta\right)^{-1}$$
$$\times \exp\left(-\frac{2^{\frac{L}{d^*(w)W_B}} - 1}{\alpha P_S/\sigma^2}\right)(w - g_{min})^{N-1} dw \tag{33}$$
$$\approx 1 - \sum_{m=0}^{M-1} \sum_{k=1}^{K} \frac{(-1)^m \binom{M-1}{m} \alpha N M}{2(g_{max} - g_{min})^{N-1}} \left(\alpha(m+1) + 2^{\frac{L}{d^*(u_k)W_B}} \beta\right)^{-1}$$
$$\times \exp\left(-\frac{2^{\frac{L}{d^*(u_k)W_B}} - 1}{\alpha P_S/\sigma^2}\right)(u_k - g_{min})^{N-1} \sqrt{1 - w_k^2}, \tag{34}$$

where K is a complexity-vs-accuracy tradeoff parameter, and

$$w_k = \cos\left(\frac{(2k-1)\pi}{2K}\right), \tag{35}$$
$$u_k = \frac{g_{max} - g_{min}}{2} w_k + \frac{g_{max} + g_{min}}{2}. \tag{36}$$

Note that the Gaussian-Chebyshev approximation in (34) can provide an exact result with an infinite value of K, which has been pointed out by the literature such as the work in [35]. By setting K to a relatively large number, (34) can provide a highly accurate approximation of SOP for criterion I.

As $d^*(g_{n^*})$ in (23) has several forms, we can further specify the analytical form of $P_{out,I}$ by applying (23) into (33) through using the relationship of P_S and γ_P. In this way, we can obtain the analytical form of SOP of criterion I for the considered MEC networks, which consists of elementary functions only and hence is readily to be evaluated.

2) Asymptotic secrecy outage probability of criterion I: In order to obtain some insights on the system, we now extend to provide the asymptotic expression of SOP of criterion I, where the SINR P_S/σ^2 is high and the MER $\lambda = \frac{\alpha}{\beta}$ is large. By using the approximations of $e^x \simeq 1 + x$

and $(1+x)^{-1} \simeq 1-x$ for a small value of $|x|$, we can obtain the asymptotic CDF of $C_{n^*,s}$ for criterion I as

$$F_{C_{n^*,s},I}(x) \simeq \frac{\phi_1}{\lambda} 2^{\frac{x}{W_B}}, \tag{37}$$

with

$$\phi_1 = M \sum_{m=0}^{M-1} \binom{M-1}{m} (-1)^m (m+1)^{-2}. \tag{38}$$

From the asymptotic $F_{C_{n^*,s},I}(x)$, we can obtain the asymptotic expression of $P_{out,I}$ in the following theorem,

Theorem 2: The asymptotic secrecy outage probability of criterion I is given by

$$P_{out,I} \simeq \frac{\Phi_1 \phi_1}{\lambda}, \tag{39}$$

where Φ_1 is

$$\Phi_1 \simeq \begin{cases} 2^{\frac{LP_S}{(\gamma_E - E_C)W_B}}, & \text{If } P_S > \gamma_P \\ \Psi_N(g_{min}, g_{max}, \xi_1, \xi_2, \xi_3, \xi_4), & \text{If } P_C \leq P_S \leq \gamma_P \\ \Psi_N(g_{min}, \gamma_f, \xi_1, \xi_2, \xi_3, \xi_4) + \Psi_N(\gamma_f, g_{max}, \xi_5, \xi_6, \xi_7, \xi_8), & \text{If } P_S < \min(P_C, \gamma_P) \end{cases}, \tag{40}$$

in which

$$\xi_1 = \frac{P_0 L^2 \eta}{W_B},\ \xi_2 = \frac{L(\gamma_E - P_S \gamma_T)}{W_B}, \tag{41}$$

$$\xi_3 = (\gamma_T - T_C) P_0 L \eta,\ \xi_4 = \gamma_E T_C - \gamma_T E_C, \tag{42}$$

$$\xi_5 = \frac{L^2 \eta}{W_B},\ \xi_6 = \frac{L \gamma_T}{W_B}, \tag{43}$$

$$\xi_7 = (\gamma_T - T_C) L \eta,\ \xi_8 = T_C \gamma_T, \tag{44}$$

and $\Psi_N(g_1, g_2, \theta_1, \theta_2, \theta_3, \theta_4)$ is

$$\Psi_N(g_1, g_2, \theta_1, \theta_2, \theta_3, \theta_4) = \frac{N 2^{-\frac{\theta_2}{\theta_4}} \ln 2 (\theta_1 + \theta_2 \theta_3/\theta_4)}{(g_{max} - g_{min})^N \theta_4} \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{(-\frac{\theta_3}{\theta_4} - g_{min})^{N-n}}{(n+1)!}$$
$$\times \left(\frac{(\theta_1 + \theta_2 \theta_3/\theta_4) \ln 2}{\theta_4} \right)^n \left(\mathbf{Ei}(\tilde{\zeta}_2) - \mathbf{Ei}(\tilde{\zeta}_1) - \sum_{q=1}^{n+1} \left(\frac{e^{\tilde{\zeta}_2}}{\tilde{\zeta}_2^{n+2-q}} - \frac{e^{\tilde{\zeta}_1}}{\tilde{\zeta}_1^{n+2-q}} \right) (n+1-q)! \right), \tag{45}$$

where ()! denotes the factorial operation, $\mathbf{Ei}(x) = \int_{\infty}^{x} \frac{e^t}{t} dt$ is the exponential integral function and

$$\zeta_1 = \frac{\theta_3 + \theta_4 g_1}{\ln 2}, \ \tilde{\zeta}_1 = \frac{\theta_1 + \theta_2 \theta_3 / \theta_4}{\zeta_1}, \tag{46}$$

$$\zeta_2 = \frac{\theta_3 + \theta_4 g_2}{\ln 2}, \ \tilde{\zeta}_2 = \frac{\theta_1 + \theta_2 \theta_3 / \theta_4}{\zeta_2}. \tag{47}$$

Proof: See Appendix C. ■

From the asymptotic SOP in Theorem 2, we can obtain some insights on the system, as follows,

- The secrecy diversity order of criterion I is unity. This is because that criterion I only exploits the randomness of computational capability, yet fails to exploit the randomness of transmission channels.
- The asymptotic $P_{out,I}$ improves with an increasing N, as more users can provide a more powerful computational capability at users.
- The asymptotic $P_{out,I}$ deteriorates with an increasing M and L, as more eavesdroppers or tasks lead to a more severe secure transmission burden.

C. Secure Outage Probability of Criterion II

1) Analytical secrecy outage probability of criterion II: To obtain the analytical SOP of criterion II for the considered MEC networks, we need to firstly obtain the CDF of $C_{n^*,s}$, which is given by the following theorem,

Theorem 3: The CDF of $C_{n^*,s}$ of criterion II is given by

$$F_{C_{n^*,s},II}(x) = \left(1 - \sum_{m=0}^{M-1} \frac{(-1)^m \binom{M-1}{m} M\alpha}{\alpha(m+1) + 2^{\frac{x}{W_B}}\beta} \exp\left(-\frac{2^{\frac{x}{W_B}} - 1}{\alpha P_S / \sigma^2}\right)\right)^N. \tag{48}$$

Proof: See Appendix C. ■

By applying the result of Theorem 3 into (28), we can obtain the analytical secrecy outage

probability of criterion II as,

$$P_{out,II} = \frac{1}{g_{max}-g_{min}} \int_{g_{min}}^{g_{max}} \left(1 - \sum_{m=0}^{M-1} \frac{(-1)^m \binom{M-1}{m} M\alpha}{\alpha(m+1) + 2^{\frac{L}{d^*(v)W_B}}\beta} \exp\left(-\frac{2^{\frac{L}{d^*(v)W_B}}-1}{\alpha P_S/\sigma^2}\right)\right)^N dv, \tag{49}$$

$$\approx \sum_{k=1}^{K} \frac{\sqrt{1-w_k^2}}{2} \left(1 - \sum_{m=0}^{M-1} \frac{(-1)^m \binom{M-1}{m} M\alpha}{\alpha(m+1) + 2^{\frac{L}{d^*(u_k)W_B}}\beta} \exp\left(-\frac{2^{\frac{L}{d^*(u_k)W_B}}-1}{\alpha P_S/\sigma^2}\right)\right)^N, \tag{50}$$

where the Gaussian-Chebyshev approximation is used in the last approximation. Similarly, by applying several cases of $d^*(g_{n^*})$ shown in (23), we can further specify the analytical form of $P_{out,II}$ by taking into account the relationship of P_S and γ_P. In this way, we can obtain the analytical form of SOP of criterion II for the considered MEC networks, which is composed of elementary functions only and hence is easily to be calculated.

2) Asymptotic secrecy outage probability of criterion II: We further provide the asymptotic expression of secrecy outage probability for criterion II, in the high regime of SINR and MER. By using the approximations of $e^x \simeq 1+x$ and $(1+x)^{-1} \simeq 1-x$ [34], we can firstly approximate the CDF of $C_{n^*,s}$ as

$$F_{C_{n^*,s},II}(x) \simeq \frac{\phi_1^N}{\lambda^N} 2^{\frac{Nx}{W_B}}. \tag{51}$$

Then, by applying the asymptotic $F_{C_{n^*,s}}(x)$ into (28), we can obtain the asymptotic secure outage probability of criterion II as,

$$P_{out,II} \simeq \frac{\phi_1^N}{\lambda^N} \Phi_2, \tag{52}$$

where Φ_2 is defined as

$$\Phi_2 \simeq \begin{cases} 2^{\frac{NLP_S}{(\gamma_E - E_C)W_B}}, & \text{If } P_S > \gamma_P \\ \Psi_1(g_{min}, g_{max}, N\xi_1, N\xi_2, \xi_3, \xi_4), & \text{If } P_C \le P_S \le \gamma_P \\ \Psi_1(g_{min}, \gamma_f, N\xi_1, N\xi_2, \xi_3, \xi_4) + \Psi_1(\gamma_f, g_{max}, N\xi_5, N\xi_6, \xi_7, \xi_8), & \text{If } P_S < \min(P_C, \gamma_P) \end{cases}. \tag{53}$$

From this asymptotic SOP, we can obtain some insights on the system for criterion II as,

- The system secrecy diversity order of criterion II is N, as criterion II exploits the channel diversity of N branches. Accordingly, the system performance can be rapidly enhanced by increasing the number of users.

- The secrecy performance of criterion II deteriorates with a larger M and L, as the transmission latency and energy consumption increase when there are more eavesdroppers and tasks.

D. Secure Outage Probability of Criterion III

1) Analytical secrecy outage probability of criterion III: For criterion III, the associated CDF of $C_{n^*,s}$ is given by the following theorem,

Theorem 4: The CDF of $C_{n^*,s}$ of criterion III is

$$F_{C_{n^*,s},III}(x) = \sum_{m=0}^{M-1}\sum_{n=0}^{N}\binom{N}{n}\binom{M-1}{m}\frac{(-1)^{n+m}M\alpha}{\alpha(m+1)+2^{\frac{x}{W_B}}n\beta}\exp\Big(-\frac{n(2^{\frac{x}{W_B}}-1)}{\alpha P_S/\sigma^2}\Big). \tag{54}$$

Proof: See Appendix D. ■

By applying the result of Theorem 4 into (28), we can obtain the analytical secrecy outage probability of criterion III as,

$$P_{out,III} = \frac{1}{g_{max}-g_{min}}\sum_{m=0}^{M-1}\sum_{n=0}^{N}\binom{N}{n}\binom{M-1}{m}\int_{g_{min}}^{g_{max}}\frac{(-1)^{n+m}M\alpha}{\alpha(m+1)+2^{\frac{L}{d^*(v)W_B}}n\beta}\exp\Big(-\frac{n(2^{\frac{L}{d^*(v)W_B}}-1)}{\alpha P_S/\sigma^2}\Big)dv, \tag{55}$$

$$\approx \sum_{k=1}^{K}\sum_{m=0}^{M-1}\sum_{n=0}^{N}\binom{N}{n}\binom{M-1}{m}\frac{\sqrt{1-w_k^2}}{2}\frac{(-1)^{n+m}M\alpha}{\alpha(m+1)+2^{\frac{L}{d^*(u_k)W_B}}n\beta}\exp\Big(-\frac{n(2^{\frac{L}{d^*(u_k)W_B}}-1)}{\alpha P_S/\sigma^2}\Big), \tag{56}$$

where the Gaussian-Chebyshev approximation is employed in the last approximation. In a similar way, by applying several cases of $d^*(g_{n^*})$ shown in (23), we can further specify the analytical form of $P_{out,III}$ by taking into account the relationship between P_S and γ_P. In this way, we can obtain the analytical form of SOP of criterion III for the considered MEC networks, which consists of elementary functions only and hence is easily to be computed.

2) Asymptotic secrecy outage probability of criterion III: To obtain some insights on the system, we further derive the asymptotic expression of SOP of criterion III for the considered secure MEC networks, in the high region of SINR and MER. Firstly, by using the approximations of $e^x \simeq 1+x$ and $(1+x)^{-1} \simeq 1-x$ [34], we can write the asymptotic $F_{C_{n^*,s},III}(x)$ as

$$F_{C_{n^*,s},III}(x) \simeq \frac{\phi_2}{\lambda^N}2^{\frac{Nx}{W_B}}, \tag{57}$$

with

$$\phi_2 = \sum_{m=0}^{M-1}\sum_{n=0}^{N}\binom{M-1}{m}\binom{N}{n}\frac{(-1)^{n+m+N}Mn^N}{(m+1)^{N+1}}. \tag{58}$$

By applying the asymptotic $F_{C_{n^*,s},III}(x)$ into (28), we can obtain the asymptotic secure outage probability of criterion III as,

$$P_{out,III} \simeq \frac{\Phi_2\phi_2}{\lambda^N}. \tag{59}$$

From this asymptotic SOP, we can obtain some insights on the system for criterion III as,

- The secrecy diversity order of criterion III is also equal to N, as criterion III fully exploits the N branches of main links. Accordingly, the system performance can be also rapidly enhanced by increasing the number of users.
- As $\phi_1^N \leq \phi_2$ holds, we can find that criterion III is poorer than criterion II, since it cannot exploit the eavesdropping links to perform the user selection.
- The secrecy performance of criterion III becomes worse with an increasing M and L, as more eavesdroppers or tasks lead to an increased transmission latency and energy consumption.

V. Simulations and Numerical Results

In this section, we provide some numerical and simulation results to verify the proposed studies. Without loss of generality, we set $P_S = 3$W, $P_0 = 1$W and $P_C = 0.2$W. If not specified, the task length L is 80 Mbits and the bandwidth of wireless transmission is 100MHz. The channels in the network follow Rayleigh flat fading, where the average channel gain of the main links is set to unity. Moreover, the local CPU-cycle frequency is uniformly distributed in the range of [0.1, 1]GHz, while the CPU-cycle frequency at the CAP is set to 10GHz. The number of required CPU-cycles for each bit is 10. In further, we set the outage thresholds of latency and energy consumption to $\gamma_T = 0.3$ s and $\gamma_E = 0.8$ J, respectively[5].

Fig. 2 shows the impact of the parameter K on the secrecy outage probability of the three selection criteria, where $N = M = 3$, SINR is 35dB, MER is 20dB and K varies from 1 to 100.

[5]Similar parameter settings for the MEC networks can be found in the literature, such as the works in [6], [15], [23], where the CAPs are of significantly powerful computational capacity, yet the local CPU-cycle frequency is randomly distributed and smaller than that of CAPs.

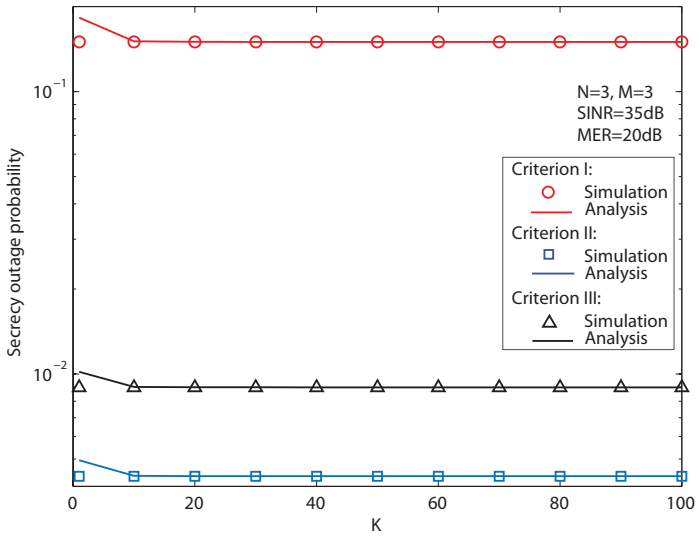

Fig. 2. Impact of parameter K on the secrecy outage probability of the three criteria.

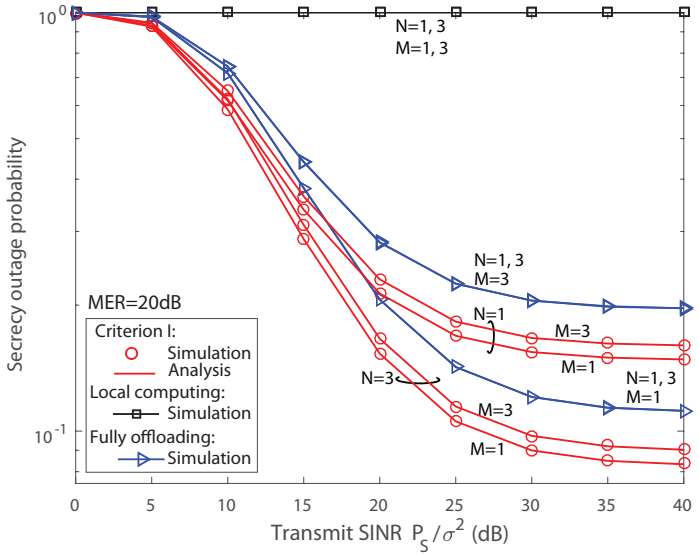

Fig. 3. Secure outage probability versus transmit SINR: Criterion I.

From Fig. 2, we can see that for each criterion, the Gaussian-Chebyshev approximation becomes more accurate with the increased value of K. Moreover, the approximation becomes convergent with a medium value of K, which validates our analysis. By taking into account the tradeoff between the complexity and accuracy, we set the value of K to around 10 in the simulations.

Fig. 3 demonstrates the analytical and simulated secrecy outage probabilities of criterion

I versus the transmit SINR, where MER is set to 20dB and different numbers of users and eavesdroppers are investigated. For comparison, we also plot the results of the local computing with $\rho = 0$ and fully offloading with $\rho = 1$. Accordingly, C_t is set to $\frac{L}{d^*(g_n^*)}$, 0 and $\max\left(\frac{L}{\gamma_T - T_C}, \frac{LP_S}{\gamma_E - E_C}\right)$, corresponding to the proposed criteria, local computing and fully offloading, respectively. As observed from Fig. 3, we can find that the analytical result of criterion I fits well with the simulated one for various values of SINR, which validates the effectiveness of the derived analytical SOP expression for criterion I. Moreover, the system secrecy performance of criterion I improves with a larger value of SINR, due to the increased secrecy data rate. However, in the high regime of SINR, there exhibits an error floor in the secrecy outage probability indicating that the improvement is saturated, as the fixed MER has become the bottleneck of the system performance. In further, the secrecy outage probability improves with a larger N, as more users can provide more computational resources for criterion I. In contrast, the secrecy outage probability of criterion I deteriorates with a larger M, as more eavesdroppers weaken the secrecy transmission quality and hence lead to an increased transmission latency and energy consumption. Furthermore, criterion I outperforms the local computing and fully offloading, as it can jointly utilize the computational resources at both users and CAP. In particular, the secrecy outage probability of local computing is quite poor and remains about unity even in high SINR region, as the computational capability at the users is limited in practice and unable to fulfill the computational task solely. Hence, $\gamma_T \leq T_0$ and $\gamma_E \leq E_0$ hold, and the system requirements on the latency and energy consumption cannot be met in the local computing.

Fig. 4 illustrates the analytical and simulated secrecy outage probabilities of criterion II versus the transmit SINR, where MER is 20dB, $M \in \{1, 3\}$ and $N \in \{1, 3\}$. As observed from Fig. 4, we can find that the analytical result of criterion II matches well with the simulated one, which validates the effectiveness of the derived analytical SOP expression for criterion II. Moreover, the secrecy outage probability of criterion II improves with a larger N, as more users can provide more communications resources for criterion II. In contrast, the secrecy outage probability of criterion II deteriorates with a larger M, as more eavesdroppers decreases the system secrecy data rate and hence cause an increased transmission latency and energy consumption. In further, criterion II outperforms both the local computing and fully offloading, as it can jointly use the communication and computational resources at users and CAP, which further verifies the effectiveness of criterion II.

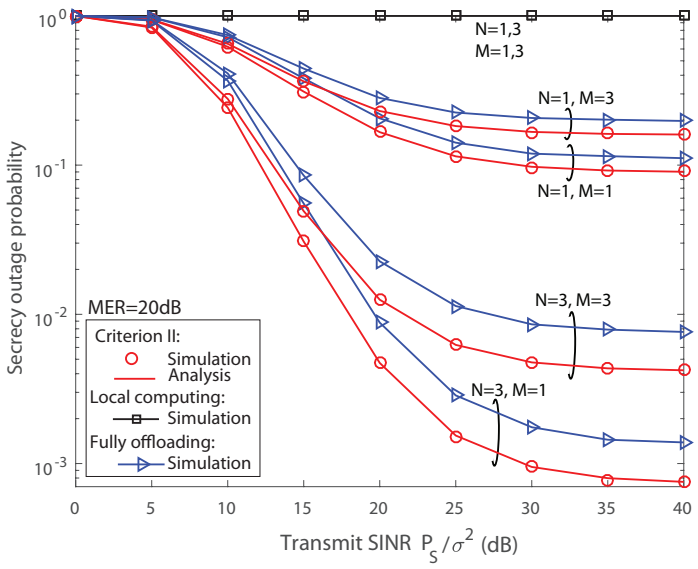

Fig. 4. Secure outage probability versus transmit SINR: Criterion II.

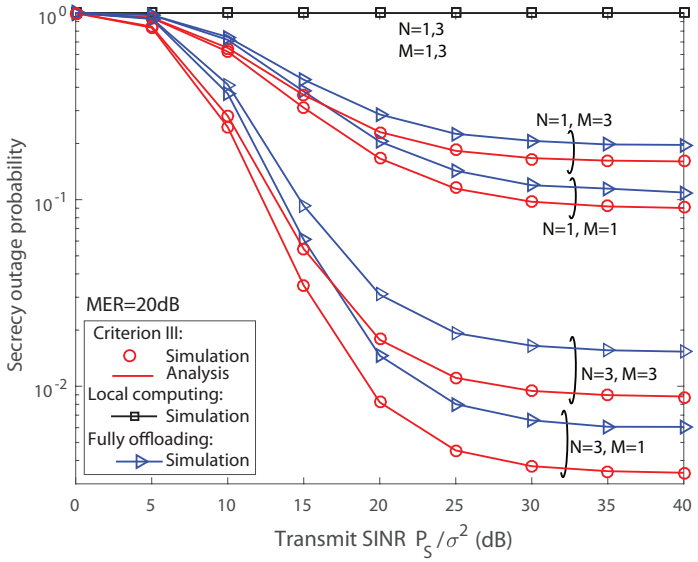

Fig. 5. Secure outage probability versus transmit SINR: Criterion III.

Fig. 5 shows the analytical and simulated secrecy outage probabilities of criterion III versus the transmit SINR, where MER is 20dB, $M \in \{1, 3\}$ and $N \in \{1, 3\}$. We can find from Fig. 5 that the analytical result of criterion III is in good match with the simulated one, which validates the effectiveness of the derived analytical SOP expressions for criterion III. Moreover,

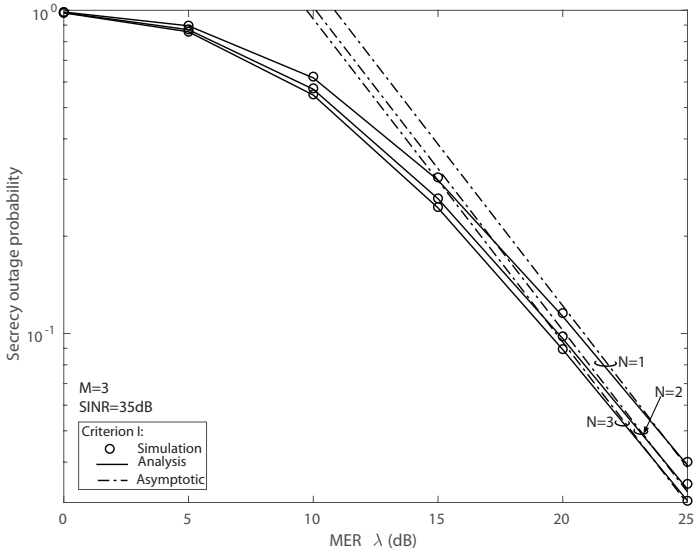

Fig. 6. Effect of MER λ on the secrecy outage probability: Criterion I.

the secrecy outage probability of criterion III improves with a larger N, as more users can provide more communications resources. In contrast, the secrecy outage probability of criterion III deteriorates with a larger M, as more eavesdroppers are harmful to the system secrecy data rate and hence result in an increased transmission latency and energy consumption. In further, criterion III outperforms both the local computing and fully offloading, as it can jointly exploit the communication and computational resources at users and CAP, which further verifies the effectiveness of criterion III. Furthermore, by comparing the results in Figs. 3-5, we can find that the secrecy performances of criterion II and III improve much more profoundly with a larger N than that of criterion I, as criterion I fails to exploit the channel randomness of N branches. In particular, criterion II outperforms criterion III, as the former can suppress the wiretap more effectively by exploiting the eavesdropping information in the user selection.

Figs. 6-8 depict the effect of MER on the secrecy outage probabilities of the three criteria, where $M = 3$, SINR=35dB and the number of users varies from 1 to 3. Specifically, Fig. 6, 7 and 8 correspond to criterion I, II and III, respectively. We can observe from these three figures that for each criterion, the analytical SOP fits well with the simulated one, and the asymptotic result becomes convergent to the exact value in the high regime of MER, which verifies the effectiveness of the derived analytical and asymptotic SOP expressions of the three criteria.

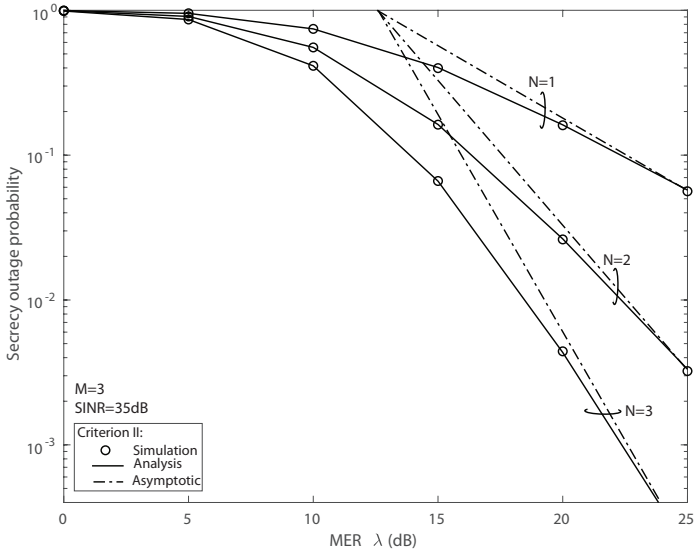

Fig. 7. Effect of MER λ on the secrecy outage probability: Criterion II.

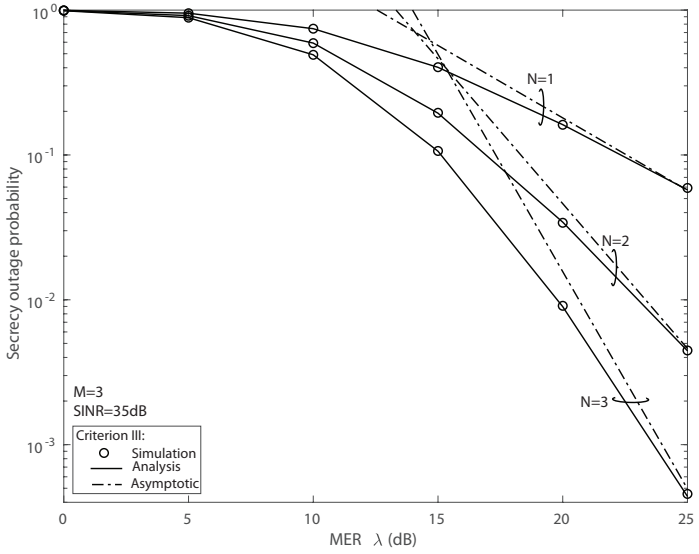

Fig. 8. Effect of MER λ on the secrecy outage probability: Criterion III.

Moreover, the SOP curves with different values of N are in parallel in Fig. 6, indicating that the system secrecy diversity order of criterion I remains unchanged with the number of users. In contrast, the SOP curves of criterion II and III are proportional to the number of users in Figs. 7 and 8, indicating that criteria II and III can achieve the system full secrecy diversity order of N. In further, by comparing the results in Figs. 7-8, we can find that criterion III is worse

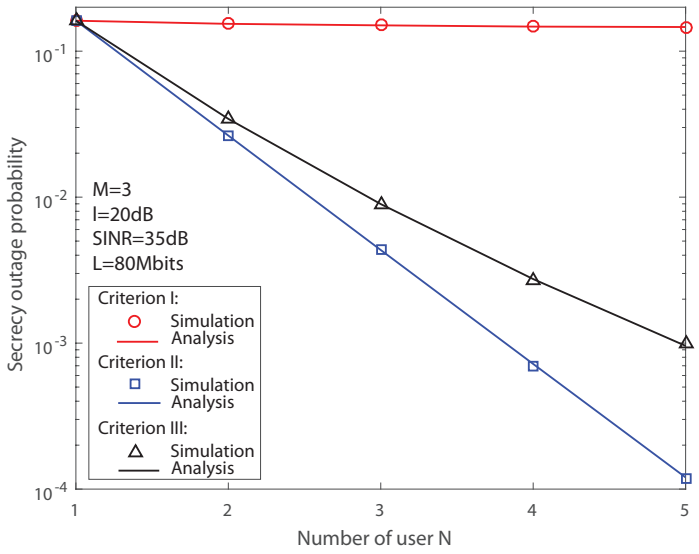

Fig. 9. Secure outage probability versus the number of users N.

than criterion II, since it cannot exploit the eavesdropping information in the process of user selection.

Fig. 9 shows the secrecy outage probabilities of the three criteria versus the number of users and bits, where SINR is 35dB, MER is 20dB, $L = 80$Mbits and N varies from 1 to 5. We can observe from Fig. 9 that for various values of N, the analytical SOP of each criterion is in good match with the simulated one, which further verifies the effectiveness of the derived analytical SOP expressions of the three criteria. Moreover, the SOP performance of each criterion improves with an increased N, as more users provide more communication and computational resources for the system. In particular, the SOP improvement of criterion I from more users is quite marginal, as it exploits the information of CPU-cycle frequency only in the user selection. In contrast, the performances of criterion II and III are enhanced rapidly, and they are not convergent with the increased number of users, as these two criteria employ the dynamic channel information of N branches in the user selection. We can further find that criterion II outperforms criterion III, as it can exploit the channel information of eavesdropping links in the user selection.

Fig. 10 demonstrates the secrecy outage probabilities of the three criteria versus the number of bits, where SINR is 35dB, MER is 20dB, $N = 3$ and L varies from 50Mbits to 100Mbits. We can observe from Fig. 10 that for various values of L, the analytical SOP of each criterion fits

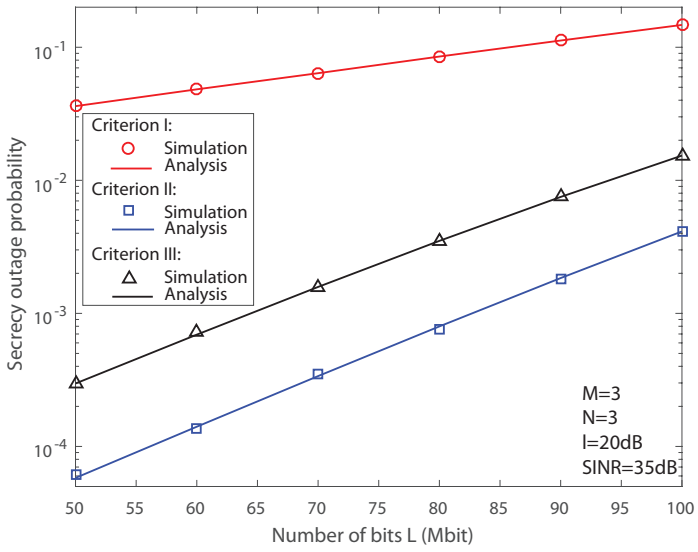

Fig. 10. Secure outage probability versus the task length L.

well with the simulated one, which further verifies the effectiveness of the derived analytical SOP expressions of the three criteria. Moreover, the SOP performance of each criterion deteriorates with an increased L, due to the heavier burden on the communication and computation. In further, we can see that criterion III is outperformed by criterion III, as it fails to exploit the channel information of eavesdropping links in the process of user selection.

VI. Conclusions

This paper investigated the secure MEC network in the presence of multiple eavesdroppers, where the offloading from the users to the CAP could be overheard by the eavesdroppers, which caused the severe issue of information leakage. To address this issue, we firstly presented the SOP minimization problem, by jointly taking into account the constraints from the latency and energy consumption. We then presented three user selection criteria to enhance the system secrecy performance, based on the locally computational capacity, the secrecy capacity and data rate of main links, respectively. For these three criteria, we further analyzed the system secrecy performance by deriving the analytical and asymptotic expressions of SOP, from which we obtained some important insights on the system design. Simulation and analytical results were finally provided to verify the proposed studies on the secure MEC network. In particular, the three criteria can efficiently safeguard the MEC networks, compared to the traditional local

computing and fully offloading, especially with a large value of user number.

In future works, we will investigate the considered MEC networks in a multi-cell communication scenario, where the interference may not be modeled by the Gaussian distribution. In addition, we will extend the considered MEC networks from the Rayleigh fading to some other kinds of channels, such as Nakagami-m fading.

APPENDIX A
PROOF OF PROPOSITION 1

To prove Proposition 1, we firstly write the first-order derivative of $\frac{\gamma_T}{\rho}-T_C$ and $\frac{1}{P_S}\left(E_0-E_C-\frac{E_0-\gamma_E}{\rho}\right)$ with respect to ρ as,

$$\frac{\partial(\frac{\gamma_T}{\rho}-T_C)}{\partial\rho}=-\frac{\gamma_T}{\rho^2}\leq 0, \tag{A.1}$$

$$\frac{\partial\left[\frac{1}{P_S}\left(E_0-E_C-\frac{E_0-\gamma_E}{\rho}\right)\right]}{\partial\rho}=\frac{E_0-\gamma_E}{P_S\rho^2}\geq 0. \tag{A.2}$$

From these two derivatives, we can find that $\frac{\gamma_T}{\rho}-T_C$ decreases with a larger value of ρ while $\frac{1}{P_S}\left(E_0-E_C-\frac{E_0-\gamma_E}{\rho}\right)$ increases. Then, by setting $\frac{\gamma_T}{\rho}-T_C$ equal to $\frac{1}{P_S}\left(E_0-E_C-\frac{E_0-\gamma_E}{\rho}\right)$, we can obtain one critical value of ρ as

$$\rho=\rho_2^*=\frac{E_0-\gamma_E+P_S\gamma_T}{E_0-E_C+P_ST_C}. \tag{A.3}$$

From (A.3), we can find that $\frac{\gamma_T}{\rho}-T_C$ is larger than $\frac{1}{P_S}\left(E_0-E_C-\frac{E_0-\gamma_E}{\rho}\right)$ when $\rho<\rho_2^*$ and vice versa. Therefore, when $\rho\in(\rho_1^*,1)$ holds, the maximum value of $d(g_{n^*})$ can be obtained by setting $\rho=\rho_2^*$. When $\rho_2^*>1$ holds, which is equivalent to $P_S\geq\frac{\gamma_E-E_C}{\gamma_T-T_C}$, the maximum value of $d(g_{n^*})$ can be obtained by setting $\rho=1$. Similarly, when $\rho_2^*\leq\rho_1^*$ holds, the maximum value of $d(g_{n^*})$ can be obtained by setting $\rho=\rho_1^*$. To summarize, we can obtain the optimal value of $d(g_{n^*})$ with $\rho=\rho^*$ in (21). In this way, we have completed the proof of Proposition 1.

APPENDIX B
PROOF OF THEOREM 1

For criterion I, we can derive the CDF of $C_{n^*,s}$ as

$$F_{C_{n^*,s},I}(x) = \Pr\left(\left[\log_2 \frac{1+\frac{P_S}{\sigma^2}|h_n|^2}{1+\frac{P_S}{\sigma^2}|h_n^e|^2}\right]^+ \leq \frac{x}{W_B}\right), \tag{B.1}$$

$$= \Pr\left(|h_n|^2 \leq \frac{2^{\frac{x}{W_B}}(1+P_S/\sigma^2|h_n^e|^2)-1}{P_S/\sigma^2}\right). \tag{B.2}$$

Applying the PDFs of RVs $|h_n|^2$ and $|h_n^e|^2 = \max_{1\leq m\leq M}|h_{n,m}|^2$, i.e.,

$$f_{|h_n|^2}(y) = \frac{1}{\alpha}e^{-\frac{y}{\alpha}}, \tag{B.3}$$

$$f_{|h_n^e|^2}(z) = \frac{M}{\beta}\sum_{m}^{M-1}\binom{M-1}{m}(-1)^m e^{-\frac{(m+1)z}{\beta}}, \tag{B.4}$$

we can write the CDF of $C_{n^*,s}$ for criterion I as

$$F_{C_{n^*,s},I}(x) = \int_0^\infty \int_0^{\frac{2^{\frac{x}{W_B}}(1+P_S/\sigma^2 z)-1}{P_S/\sigma^2}} f_{|h_n|^2}(y) f_{|h_n^e|^2}(z) dy dz, \tag{B.5}$$

$$= 1 - \sum_{m}^{M-1}\binom{M-1}{m}\frac{(-1)^m \alpha M}{\alpha(m+1)+2^{\frac{x}{W_B}}\beta} e^{-\frac{2^{\frac{x}{W_B}}-1}{\alpha P_S/\sigma^2}}. \tag{B.6}$$

In this way, we have completed the proof of Theorem 1.

APPENDIX C
PROOF OF THEOREM 2

To prove Theorem 2, we firstly apply the results of (31) and (37) into (28), and detail the asymptotic expression of $P_{out,I}$ in the following three cases:

- In the case of $P_S > \gamma_P$, we can write the asymptotic $P_{out,I}$ as

$$P_{out,I} = F_{C_{n^*,s},I}\left(\frac{LP_S}{\gamma_E - E_C}\right) \tag{C.1}$$

$$\simeq 2^{\frac{LP_S}{(\gamma_E - E_C)W_B}}\frac{\phi_1}{\lambda}. \tag{C.2}$$

- In the case of $\min(P_C, \gamma_P) \leq P_S \leq \gamma_P$, we can compute the asymptotic $P_{out,I}$ as

$$P_{out,I} = \int_{g_{min}}^{g_{max}} F_{C_{n^*,s},I}\left(\frac{L}{\psi_1(g_{n^*})}\right)\frac{N(v-g_{min})^{N-1}}{(g_{max}-g_{min})^N}dv \tag{C.3}$$

$$\simeq \int_{g_{min}}^{g_{max}} 2^{\frac{L}{\psi_1(g_{n^*})W_B}}\frac{\phi_1 N(v-g_{min})^{N-1}}{\lambda(g_{max}-g_{min})^N}dv. \tag{C.4}$$

By solving the above integral, we can obtain the asymptotic $P_{out,I}$ as

$$P_{out,I} \simeq \int_{g_{min}}^{g_{max}} 2^{\frac{L^2\eta - L\gamma_T v}{(\gamma_T - T_C)L\eta W_B + T_C\gamma_T W_B v}} \frac{\phi_1 N(v-g_{min})^{N-1}}{\lambda(g_{max}-g_{min})^N} dv \tag{C.5}$$

$$= \Psi_N(g_{min}, g_{max}, \xi_1, \xi_2, \xi_3, \xi_4)\frac{\phi_1}{\lambda}, \tag{C.6}$$

where $\Psi_N(g_1, g_2, \theta_1, \theta_2, \theta_3, \theta_4)$ is given by

$$\Psi_N(g_1, g_2, \theta_1, \theta_2, \theta_3, \theta_4) = \int_{g_1}^{g_2} 2^{\left(\frac{\theta_1 - \theta_2 v}{\theta_3 + \theta_4 v}\right)} \frac{N(v-g_{min})^{N-1}}{(g_{max}-g_{min})^N} dv \tag{C.7}$$

$$= -\frac{N2^{-\frac{\theta_2}{\theta_4}} \ln 2(\theta_1 + \theta_2\theta_3/\theta_4)}{(g_{max}-g_{min})^N \theta_4} \sum_{n}^{N-1} \binom{N-1}{n} (-\frac{\theta_3}{\theta_4} - g_{min})^{N-1-n}$$

$$\times \left(\frac{(\theta_1 + \theta_2\theta_3/\theta_4)\ln 2}{\theta_4}\right)^n \int_{\bar{f}_1}^{\bar{f}_2} e^v v^{-n-2} dv. \tag{C.8}$$

By using the technique of partial integral, we can obtain the analytical form of $\Psi_N(g_1, g_2, \theta_1, \theta_2, \theta_3, \theta_4)$, as shown in (45), which leads to the asymptotic result of $P_{out,I}$.

- In the case of $P_S < \min(P_C, \gamma_P)$, we apply the result of (37), and then obtain the asymptotic $P_{out,I}$ as

$$P_{out,I} \simeq \int_{g_{min}}^{\gamma_f} 2^{\frac{L^2\eta - L\gamma_T v}{(\gamma_T - T_C)L\eta W_B + T_C\gamma_T W_B v}} \frac{\phi_1 N(v-g_{min})^{N-1}}{\lambda(g_{max}-g_{min})^N} dv$$

$$+ \int_{\gamma_f}^{g_{max}} 2^{\frac{L^2 P_0\eta - L(\gamma_E - P_S\gamma_T)v}{(\gamma_T - T_C)P_0 L\eta W_B + (\gamma_E T_C - \gamma_T E_C)W_B v}} \frac{\phi_1 N(v-g_{min})^{N-1}}{\lambda(g_{max}-g_{min})^N} dv \tag{C.9}$$

$$= \Psi_N(g_{min}, \gamma_f, \xi_1, \xi_2, \xi_3, \xi_4) + \Psi_N(\gamma_f, g_{max}, \xi_5, \xi_6, \xi_7, \xi_8). \tag{C.10}$$

By summarizing the above three cases, we obtain the asymptotic expression of $P_{out,I}$, as shown in (39), which has completed the proof of Theorem 2.

APPENDIX D
PROOF OF THEOREM 3

In criterion II, the instantaneous CSI of both eavesdropping and main links are known, and we can derive the CDF of $C_{n^*,s}$ as

$$F_{C_{n^*,s},II}(x) = \Pr\left(\max_{1\le n\le N}\left[\log_2\frac{1+\frac{P_S}{\sigma^2}|h_n|^2}{1+\frac{P_S}{\sigma^2}|h_n^e|^2}\right]^+ \le x\right), \tag{D.1}$$

$$= \left(\Pr\left(|h_n|^2 \le \frac{2^x(1+P_S/\sigma^2 \max\limits_{1\le m\le M}|h_{n,m}|^2) - 1}{P_S/\sigma^2}\right)\right)^N, \tag{D.2}$$

where we use the property that the channels of N users are independent and identically distributed, in the last equality. We can further write $F_{C_{n^*,s},II}(x)$ as

$$F_{C_{n^*,s},II}(x) = \left(\int_0^{\infty} \int_0^{\frac{2^x(1+P_S/\sigma^2 z)-1}{P_S/\sigma^2}} f_{|h_n|^2}(y) f_{|h_n^e|^2}(z) dy dz \right)^N, \tag{D.3}$$

By applying the PDFs of RVs $|h_n|^2$ and $|h_n^e|^2$ in (B.3) and (B.4), and then solving the required integral, we can obtain the CDF of $R_{n^*,s}$ for criterion II, as shown in (48). In this way, we have completed the proof of Theorem 3.

APPENDIX E
PROOF OF THEOREM 4

In criterion III, the user selection relies on the channel parameters of main links only. In this case, we can write the CDF of $C_{n^*,s}$ as

$$F_{C_{n^*,s},III}(x) = \Pr\left(\left[\log_2 \frac{1 + \frac{P_S}{\sigma^2} \max\limits_{1\le n\le M} |h_n|^2}{1 + \frac{P_S}{\sigma^2}|h_n^e|^2} \right]^+ \le \frac{x}{W_B} \right) \tag{E.1}$$

$$= \Pr\left(|h_n^*|^2 \le \frac{2^{\frac{x}{W_B}}(1 + P_S/\sigma^2 |h_n^e|^2) - 1}{P_S/\sigma^2} \right) \tag{E.2}$$

$$= \int_0^{\infty} \int_0^{\frac{2^{\frac{x}{W_B}}(1+P_S/\sigma^2 z)-1}{P_S/\sigma^2}} f_{|h_n^*|^2}(y) f_{|h_n^e|^2}(z) dy dz, \tag{E.3}$$

where $|h_{n^*}|^2 = \max_{1\le n\le N} |h_n|^2$ and its PDF is given by

$$f_{|h_{n^*}|^2}(y) = \frac{N}{\alpha}(1 - e^{-\frac{y}{\alpha}})^{N-1} e^{-\frac{y}{\alpha}}. \tag{E.4}$$

Then, by substituting (B.4) and (E.4) into (E.3), and then solving the required integral, we can obtain obtain the CDF of $C_{n^*,s}$ for criterion III, as shown in (54). In this way, we have completed the proof of Theorem 4.

REFERENCES

[1] L. Sun and H. Xu, "Unequal secrecy protection for untrusted two-way relaying systems: Constellation overlapping and noise aggregation," *IEEE Trans. Vehic. Tech.*, vol. 67, no. 10, pp. 9681–9695, 2018.

[2] L. Sun, H. Xu, and Y. Zhang, "Constellation-overlapping-based secure transmission for two-way untrusted relaying: Method, implementation, and experimental results," *IEEE Wirel. Commun. Lett.*, vol. 10, no. 1, pp. 121–125, 2021.

[3] J. Choi, N. Lee, S.-N. Hong, and G. Caire, "Joint user selection, power allocation, and precoding design with imperfect CSIT for multi-cell MU-MIMO downlink systems," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 1, pp. 162–176, 2020.

[4] D. Han and N. Lee, "Distributed precoding using local CSIT for MU-MIMO heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1666–1678, 2021.

[5] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, and M. Guizani, "Security in mobile edge caching with reinforcement learning," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 116–122, 2018.

[6] J. Xu, L. Chen, and P. Zhou, "Joint service caching and task offloading for mobile edge computing in dense networks," in *IEEE Conference on Computer Communications (INFOCOM) Honolulu, HI, USA, April 16-19, 2018*, pp. 207–215.

[7] S. Bi, L. Huang, and Y. A. Zhang, "Joint optimization of service caching placement and computation offloading in mobile edge computing systems," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 7, pp. 4947–4963, 2020.

[8] Y. Zhang, X. Lan, Y. Li, L. Cai, and J. Pan, "Efficient computation resource management in mobile edge-cloud computing," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3455–3466, 2019.

[9] J. Zhao, Q. Li, and Y. Gong, "Computation offloading and resource allocation for mobile edge computing with multiple access points," *IET Commun.*, vol. 13, no. 17, pp. 2668–2677, 2019.

[10] K. He, "Learning based signal detection for MIMO systems with unknown noise statistics," *IEEE Trans. Commun.*, vol. 69, pp. 3025–3038, 2021.

[11] Z. Zhao, "System optimization of federated learning networks with a constrained latency," *IEEE Trans. Vehic. Tech.*, vol. PP, no. 99, pp. 1–5, 2021.

[12] S. Tang, "Dilated convolution based CSI feedback compression for massive MIMO systems," *IEEE Trans. Vehic. Tech.*, vol. PP, no. 99, pp. 1–5, 2021.

[13] S. Lai and Y. Guo, "Distributed machine learning for multiuser mobile edge computing systems," *IEEE J. Sel. Top. Signal Process.*, vol. PP, no. 99, pp. 1–12, 2021.

[14] C. Li, J. Xia, F. Liu, D. Li, L. Fan, G. K. Karagiannidis, and A. Nallanathan, "Dynamic offloading for multiuser muti-CAP MEC networks: A deep reinforcement learning approach," *IEEE Trans. Veh. Tech.*, vol. 70, no. 3, pp. 2922–2927, 2021.

[15] J. Zhao, Q. Li, Y. Gong, and K. Zhang, "Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks," *IEEE Trans. Vehic. Tech.*, vol. 68, no. 8, pp. 7944–7956, 2019.

[16] J. Shi, J. Du, J. Wang, J. Wang, and J. Yuan, "Priority-aware task offloading in vehicular fog computing based on deep reinforcement learning," *IEEE Trans. Veh. Tech.*, vol. 69, no. 12, pp. 16 067–16 081, 2020.

[17] F. Zhou, R. Q. Hu, Z. Li, and Y. Wang, "Mobile edge computing in unmanned aerial vehicle networks," *IEEE Wirel. Commun.*, vol. 27, no. 1, pp. 140–146, 2020.

[18] F. Wang, J. Xu, and Z. Ding, "Multi-antenna NOMA for computation offloading in multiuser mobile edge computing systems," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2450–2463, 2019.

[19] F. Wang, J. Xu, X. Wang, and S. Cui, "Joint offloading and computing optimization in wireless powered mobile-edge computing systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1784–1797, 2018.

[20] F. Zhou, Y. Wu, R. Q. Hu, and Y. Qian, "Computation rate maximization in UAV-enabled wireless-powered mobile-edge computing systems," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 1927–1941, 2018.

[21] F. Zhou and R. Q. Hu, "Computation efficiency maximization in wireless-powered mobile edge computing networks," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 5, pp. 3170–3184, 2020.

[22] F. Wang, H. Xing, and J. Xu, "Real-time resource allocation for wireless powered multiuser mobile edge computing with energy and task causality," *IEEE Trans. Commun.*, vol. 68, no. 11, pp. 7140–7155, 2020.

[23] J. Xia, L. Fan, N. Yang, Y. Deng, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "Opportunistic access point selection for mobile edge computing networks," *IEEE Trans. Wirel. Commun.*, vol. 20, no. 1, pp. 695–709, 2021.

[24] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[25] L. Sun and H. Xu, "Fountain-coding-based secure communications exploiting outage prediction and limited feedback," *IEEE Trans. Vehic. Tech.*, vol. 68, no. 1, pp. 740–753, 2019.

[26] Q. Li and J. Qin, "Joint source and relay secure beamforming for nonregenerative MIMO relay systems with wireless information and power transfer," *IEEE Trans. Vehic. Tech.*, vol. 66, no. 7, pp. 5853–5865, 2017.

[27] L. Fan, R. Zhao, F. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, 2017.

[28] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7599–7603, 2017.

[29] J. Xia, L. Fan, W. Xu, X. Lei, X. Chen, G. K. Karagiannidis, and A. Nallanathan, "Secure cache-aided multi-relay networks in the presence of multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7672–7685, 2019.

[30] L. Xiao, D. Jiang, D. Xu, H. Zhu, Y. Zhang, and H. V. Poor, "Two-dimensional antijamming mobile communication based on reinforcement learning," *IEEE Trans. Vehic. Tech.*, vol. 67, no. 10, pp. 9499–9512, 2018.

[31] L. Xiao, Y. Li, C. Dai, H. Dai, and H. V. Poor, "Reinforcement learning-based NOMA power allocation in the presence of smart jamming," *IEEE Trans. Vehic. Tech.*, vol. 67, no. 4, pp. 3377–3389, 2018.

[32] L. Xiao, J. Liu, Q. Li, N. B. Mandayam, and H. V. Poor, "User-centric view of jamming games in cognitive radio networks," *IEEE Trans. Information Forensics and Security*, vol. 10, no. 12, pp. 2578–2590, 2015.

[33] E. Dahlman, S. Parkvall, and J. Sköld, *5G NR: the Next Generation Wireless Access Technology*, 1st ed. Academic Press, 2018.

[34] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA: Academic, 2007.

[35] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series: More special functions*, 1st ed. CRC, 1990.