Secure Communications for UAV-Enabled Mobile Edge Computing Systems

Yi Zhou, Cunhua Pan, Phee Lep Yeoh, *Member, IEEE*, Kezhi Wang, Maged Elkashlan, Branka Vucetic, *Fellow, IEEE*, and Yonghui Li, *Fellow, IEEE*

***Abstract*— In this paper, we propose a secure unmanned aerial vehicle (UAV) mobile edge computing (MEC) system where multiple ground users offload large computing tasks to a nearby legitimate UAV in the presence of multiple eavesdropping UAVs with imperfect locations. To enhance security, jamming signals are transmitted from both the full-duplex legitimate UAV and non-offloading ground users. For this system, we design a low-complexity iterative algorithm to maximize the minimum secrecy capacity subject to latency, minimum offloading and total power constraints. Specifically, we jointly optimize the UAV location, users' transmit power, UAV jamming power, offloading ratio, UAV computing capacity, and offloading user association. Numerical results show that our proposed algorithm significantly outperforms baseline strategies over a wide range of UAV self-interference (SI) efficiencies, locations and packet sizes of ground users. Furthermore, we show that there exists a fundamental tradeoff between the security and latency of UAV-enabled MEC systems which depends on the UAV SI efficiency and total UAV power constraints.**

***Index Terms*— Physical layer security, mobile edge computing, UAV communication, secrecy capacity.**

I. Introduction

UNMANNED aerial vehicles (UAVs) are promising for on-demand deployment in wireless networks due to their mobility and flexibility [1], [2]. The strong line-of-sight (LoS) characteristics of UAV air-to-ground communications have also attracted significant commercial interest for delivering high-quality aerial services. Owing to these advantages, much research effort have been devoted to developing a range of UAV-enabled wireless platforms, such as aerial base stations and relays [3]–[5]. In [3], the optimal UAV base station deployment, antenna beamwidth and bandwidth allocation were jointly investigated to minimize the sum uplink power subject to minimal rate constraints. In [4], the optimal UAV deployment was investigated to maximize the number of ground users served by a UAV base station subject to quality-of-service (QoS) constraints. The authors in [5] studied the joint blocklength and location optimization for ultra-reliable and low-latency UAV relay communications.

Given the broadcast nature of wireless transmissions, it is important to consider the security performance of UAV-enabled platforms where the communication between ground users and the UAV can be readily overheard by nearby eavesdroppers [6]. To tackle this issue, some physical layer security (PLS) techniques have been considered such as UAV aerial base station [7], [8], cooperative UAV relays [9] and UAV friendly jamming [10]–[14]. In [7], the authors proposed a secrecy capacity maximization algorithm in a UAV-assisted downlink network. In [8], the security performance of both the uplink and the downlink communications has been addressed. In [9], the authors jointly optimized the trajectory and power allocation of a UAV relay to minimize the outage probability. In [10], the UAV deployment and jamming power allocation were jointly optimized to improve the secrecy performance of a wireless network with unknown eavesdropper locations. In [11], the secrecy rate of the ground wiretap channel has been maximized by jointly optimizing the UAV trajectory and jamming power. In [12] and [13], the minimum average secrecy rate was maximized by jointly optimizing the trajectories and transmit powers of both the UAV base station and UAV jammer with time division multiple access (TDMA) and frequency division multiple access (FDMA), respectively. In [14], by considering the location uncertainty of eavesdropper, the authors proposed an efficient iterative algorithm to maximize the worst-case secrecy capacity.

Another considerations in wireless systems are the computing capacity and latency performance of users [15]. To alleviate computing capacity constraints and reduce transmission and computing latencies, mobile edge computing (MEC) has emerged as a promising platform for providing high-capacity computing resources at the network edge [16]–[18]. In [16], a total energy consumption minimization problem was studied by jointly optimizing the energy transmit beamforming, offloading ratio and time allocation subject to the computing latency requirements in a MEC-enabled wireless power

Manuscript received March 16, 2019; revised July 3, 2019 and August 28, 2019; accepted October 8, 2019. Date of publication October 17, 2019; date of current version January 15, 2020. The work of P. L. Yeoh was supported in part by ARC under Grant DP190100770. The work of Y. Li was supported by ARC under Grant DP150104019 and DP190101988. The work of B. Vucetic was supported in part by ARC Laureate Fellowship under Grant FL160100032. The associate editor coordinating the review of this article and approving it for publication was H. Zhang. *(Corresponding author: Yonghui Li.)*

Y. Zhou, P. L. Yeoh, B. Vucetic, and Y. Li are with the School of Electrical and Information Engineering, The University of Sydney, Sydney, NSW 2006, Australia (e-mail: yi.zhou@sydney.edu.au; phee.yeoh@sydney.edu.au; branka.vucetic@sydney.edu.au; yonghui.li@sydney.edu.au).

C. Pan and M. Elkashlan are with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K. (e-mail: c.pan@qmul.ac.uk; maged.elkashlan@qmul.ac.uk).

K. Wang is with the Department of Computer and Information Sciences, Northumbria University, Newcastle NE2 1XE, U.K. (e-mail: kezhi.wang@northumbria.ac.uk).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2019.2947921

transfer network. In [17], the computing resource allocation between MEC servers and mobile users was investigated through a game-theoretic approach. In [18], a low-complexity algorithm was proposed to minimize the overall energy consumption in a two-tier computing offloading MEC network.

Due to its flexible and rapid deployment capabilities, UAV is an ideal MEC platform for performing computing intensive tasks for the ground users. We envision potential applications for such UAV-enabled MEC platforms include the need for fast deployment in emergency response scenarios, such as large-scale energy outages in smart energy grids and major traffic disruptions in intelligent transport systems. Several papers have considered the performance of UAV-enabled MEC systems [19]–[21]. In [19], the authors developed an algorithm to minimize the sum of the maximum latency among all ground users served by a UAV-enabled MEC base station by jointly optimizing the UAV trajectory, user association and user offloading ratio. In [20], the UAV trajectory, bandwidth allocation and user association are jointly optimized to maximize the minimum throughput of all mobile users served by a MEC-UAV. The authors in [21] jointly optimized the task offloading decision, bit allocation and UAV trajectory aiming at minimizing the overall energy consumption in a UAV-aided edge computing network.

Though providing a general security framework for the power and trajectory optimization in UAV-assisted network, these interesting existing studies in [7]–[14] only focused on the UAV without considering the mobile edge computing. The offloading performance has not been jointly addressed in these works. For the UAV-enabled MEC systems, although several significant concerns such as latency and throughput have been optimized, the security issue that is one major concern in UAV-enabled MEC system has not been investigated in [19]–[21]. Motivated by this background, in this paper, we present a novel framework aiming at maximizing the security performance of a UAV-enabled MEC system where one full-duplex legitimate UAV with computing resource is capable of receiving and processing the offloaded packets from multiple ground users and transmitting the jamming signal to interfere with multiple eavesdropping UAVs with imperfect locations. Specifically, we consider that a number of ground users offload large computing tasks to the legitimate UAV due to strict latency requirements. To further enhance the security, non-offloading users also transmit jamming signals to interfere with the eavesdropping UAVs. To the best of our knowledge, this is the first paper to jointly consider the security, latency and offloading performance in UAV-enabled MEC systems. Moreover, to satisfy the latency requirement, the users with large tasks to be executed have to associate with the legitimate UAV due to the limited computing resource equipped on them, while such offloading transmission might be overheard by the eavesdropping UAVs, which results in a degraded security performance. We highlight the fundamental tradeoff between the security and latency of UAV-enabled MEC system which has not been previously analyzed in existing works.

A key challenge in this paper is to efficiently maximize the minimum secrecy capacity by jointly optimizing the UAV location, users' transmit power, UAV jamming power, offloading ratio, UAV computing capacity, and offloading user association subject to MEC constraints of latency, total power and minimum offloading requirements. Such a joint optimization problem is valuable and meaningful due to the importance of providing secure communications in future wireless systems. First, by optimizing the UAV location, we can not only reduce the transmission latency for the offloading users significantly, but also enhance the secrecy capacity for each offloading link. We further consider the impact of the UAV jamming power and users' transmit power on the secrecy capacity. Lastly, we optimize the offloading ratio, UAV computing capacity, and offloading user association to satisfy the latency requirement, which also indirectly impact on the secrecy capacity. Due to the coupling effects between the UAV location, users' transmit power, UAV jamming power, offloading ratio, UAV computing capacity, and offloading user association, this optimization problem is non-convex and very challenging to solve.

To overcome this challenge, we apply a number of efficient mathematical techniques including block coordinate descent (BCD) method, successive convex approximation (SCA), alternating approximation, and branch-and-cut method to obtain a high-quality solution for our joint optimization problem. First, we adopt a bounded eavesdropper location error model to discuss the location uncertainty of the eavesdropping UAVs and derive a mathematically tractable expression of lower bound secrecy capacity. To convexify the approximated objective function, slack variables are introduced. Next, we decompose the original optimization problem into five subproblems by employing the BCD method and propose a low-complexity iterative algorithm to solve each subproblem. We solve the first three subproblems of UAV location, users' transmit power and UAV jamming power by applying an SCA technique on the secrecy capacity. Then, we formulate the offloading ratio and UAV computing capacity as convex functions that can be jointly optimized in a single subproblem. Finally, we apply a branch-and-cut method to solve the offloading user association as a binary linear problem. Numerical results show that our proposed algorithm significantly outperforms baseline strategies over a wide range of UAV self-interference (SI) efficiencies, locations and packet sizes of ground users. Furthermore, we show that there exists a fundamental tradeoff between the security and latency of UAV-enabled MEC systems which depends on the UAV SI efficiency and total UAV power constraints.

The rest of this paper is organized as follows. Section II introduces the secure UAV-enabled MEC system model and formulates the joint optimization problem. In Section III, we propose an efficient iterative algorithm to maximize the minimum secrecy capacity by means of a number of convex optimization techniques. The effectiveness of our proposed solution is shown through simulation results in Section VI. Finally, we conclude the paper in Section V.

II. System Model and Problem Formulation

Fig. 1 depicts our proposed UAV-enabled MEC system with N ground users, one legitimate UAV and E non-colluding

TABLE I
TABLE OF NOTATIONS

Notation	Description
$\mathcal{N}, \mathcal{N}_{as}, \mathcal{E}$	The set of ground users, associated ground users and eavesdropping UAVs
a_i	The user association variable
p_i	The transmit power at the i-th user
p_{jam}	The jamming power at the legitimate UAV
γ	The self-interference efficiency
σ^2	The noise power
β_1, β_2	The reference channel power gain of ground-to-air link and air-to-air link
$\mathbf{y}$, $\mathbf{w}_i$, $\mathbf{v}_e$	The horizontal location of the legitimate UAV, the i-th ground user, the e-th eavesdropping UAV
$\tilde{\mathbf{v}}_e$	The estimated horizontal location of the e-th eavesdropping UAV
χ	The maximum estimation error
H_u, H_e	The altitude of the legitimate UAV and the e-th eavesdropping UAV
r_{iu}	The uplink data rate from the i-th user
r_{ie}	The rate for eavesdropping the i-th offloading signal at the e-th eavesdropping UAV
C_i	The secrecy capacity at the i-th user
D_i	The task data size of the i-th user
F_i	The CPU cycles for computing task D_i
T	The latency constraint
η_i	The offloading ratio of the i-th user
f_0, f_{iu}	The local computing capacity and the computing capacity of the legitimate UAV assigned to the i-th user

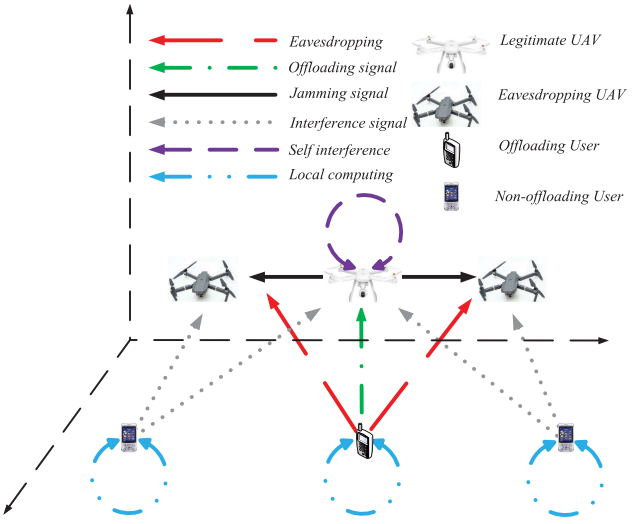


Fig. 1. System model for full-duplex UAV-enabled mobile edge computing systems.

eavesdropping UAVs, where the sets of ground users and eavesdropping UAVs are defined as $\mathcal{N}$ and $\mathcal{E}$, respectively. It is assumed that the legitimate UAV knows the perfect locations of ground users and the imperfect locations of eavesdropping UAVs [14]. We consider that each user has a set of tasks to process. Due to limited local computing capability and latency requirements, the users can either process their tasks locally or offload some of their tasks to the legitimate UAV. In the presence of eavesdropping UAVs, the legitimate UAV operating in full-duplex mode is equipped with two antennas where one receive antenna is used for receiving the offloading signals from the offloading users and one transmit antenna is used for transmitting the jamming signal to the eavesdropping UAVs. The ground users and the eavesdropping UAVs are equipped with a single antenna for transmission and eavesdropping, respectively. To further enhance the security, the non-offloading users can transmit jamming signals to interfere with the eavesdropping UAVs. We consider a multiple access channel where all ground users can transmit their signals simultaneously using the same channel [17], [22]. At the legitimate UAV and eavesdropping UAVs, the desired user's signal is decoded by regarding all other users' signals as co-channel interference. The descriptions of some notations used in this paper are summarized in Table I.

A. Communication Model

The coordinate of the i-th user is denoted as $\mathbf{w}_i = (x_i, y_i)^T \in \mathbb{R}^{2\times 1}, \forall i \in \mathcal{N}$. The legitimate UAV is fixed at altitude H_u above ground and the horizontal location of UAV is denoted by $\mathbf{y} = (x_u, y_u)^T \in \mathbb{R}^{2\times 1}$. For air-to-ground channel, since the propagation conditions between the UAV and ground users can be approximated as free space when the UAV is placed above a certain altitude and the LoS probability is close to one, we adopt a simple channel model where the channel gains are dominated by the LoS links [1]. Then, the channel power gain between the i-th user and the legitimate UAV can be written as

$$h_{iu} = \frac{\beta_1}{H_u^2 + ||\mathbf{y} - \mathbf{w}_i||^2}, \quad \forall i \in \mathcal{N}, \tag{1}$$

where $\beta_1 = g_t g_r \left(\frac{\lambda}{4\pi d_0}\right)^2$ denotes the channel power gain of ground-to-air link at the reference distance $d_0 = 1$ m, with g_t and g_r being the antenna power gains of the ground users and UAVs, respectively, and λ is the wavelength. We note that more antennas at both the ground users and UAVs can increase the antenna array gains [22], i.e., g_t and g_r.

Define $a_i = \{0, 1\}, i \in \mathcal{N}$ as the offloading user association variable where $a_i = 1$ means that the i-th user is associated with the legitimate UAV and part of its task will be offloaded to the UAV, while $a_i = 0$ represents that this user will execute the whole computing task locally. If the i-th user is associated with the legitimate UAV, the data rate of the uplink transmission is given as

$$r_{iu} = \log_2 \left(1 + \frac{p_i h_{iu}}{\sum\limits_{k \in \mathcal{N}, k \neq i} p_k h_{ku} + \gamma p_{jam} + \sigma^2}\right), \quad \forall i \in \mathcal{N}_{as}, \tag{2}$$

where p_i is the transmit power at the i-th user, $\mathcal{N}_{as} = \{i | a_i = 1, \forall i \in \mathcal{N}\}$ is the set of associated users, $\sum\limits_{k \in \mathcal{N}, k \neq i} p_k h_{ku}$ is the interference from all other users except i and σ^2 is the noise power. Moreover, p_{jam} denotes the transmit power of the jamming signal from the legitimate UAV to the eavesdropping UAVs which results in a residual self-interference (SI) power of γp_{jam} where γ is the SI efficiency of the full-duplex transmitter [23].

We assume that the e-th eavesdropping UAV is located at a fixed altitude of H_e with horizontal coordinates $\mathbf{v}_e = (x_e, y_e)^T \in \mathbb{R}^{2\times 1}, \forall e \in \mathcal{E}$ which are imperfectly known at the legitimate UAV. Similar to [12], we consider a bounded eavesdropper location error model given by $\mathbf{v}_e \in \Theta_e \triangleq \{||\tilde{\mathbf{v}}_e - \mathbf{v}_e|| \leq \chi\}$ where $\tilde{\mathbf{v}}_e$ is the estimated horizontal location and χ is the maximum estimation error. The channel power gain between the i-th user and the e-th eavesdropping UAV can be given as

$$h_{ie} = \frac{\beta_1}{H_e^2 + ||\mathbf{w}_i - \mathbf{v}_e||^2}, \quad \forall i \in \mathcal{N}, \ \forall e \in \mathcal{E}. \tag{3}$$

We note that the channel power gains between different UAVs are mainly dominated by the LoS links [24]. Hence, the channel power gain between the e-th eavesdropping UAV and the legitimate UAV is given by

$$h_{eu} = \frac{\beta_2}{(H_u - H_e)^2 + ||\mathbf{y} - \mathbf{v}_e||^2}, \quad \forall e \in \mathcal{E}, \tag{4}$$

where β_2 denotes the channel power gain of the air-to-air link at a reference distance $d_0 = 1$ m and can be written as $\beta_2 = g_r g_r \left(\frac{\lambda}{4\pi d_0}\right)^2$.

The data rate for the e-th eavesdropping UAV to eavesdrop the signal from the i-th associated user can be given as

$$r_{ie} = \log_2 \left(1 + \frac{p_i h_{ie}}{\sum\limits_{k \in \mathcal{N}, k \neq i} p_k h_{ke} + p_{jam} h_{eu} + \sigma^2}\right), \quad \forall i \in \mathcal{N}_{as}, \quad \forall e \in \mathcal{E}. \tag{5}$$

The secrecy capacity is given by [25]–[27]

$$C_i = \left[r_{iu} - \max_{e \in \mathcal{E}}(r_{ie})\right]^+, \quad \forall i \in \mathcal{N}_{as}, \tag{6}$$

where $[x]^+ \triangleq \max(x, 0)$. Note that if users are not associated with the legitimate UAV and execute the whole task locally, there is no security issue involved.

B. Computing Model

We assume that each user has a task U_i to be executed which is characterized as [28]

$$U_i = (D_i, F_i, T), \quad \forall i \in \mathcal{N}, \tag{7}$$

where D_i denotes the data size of this task and F_i describes the number of CPU cycles for computing one bit of task D_i. Moreover, T is the latency requirement for this task. Without loss of generality, we assume that all the tasks have the same time requirement T.

Note that since there is a delay-sensitive task to be executed at each user, the users with large packet size to be processed are not able to locally compute the whole task due to the latency limitation. We consider the case that each task can be divided into two parts. One part is offloaded to the associated UAV and the other part is self-executed. Define $\eta_i \in [0, 1]$ as the offloading ratio where $D_i \eta_i$ is processed by the UAV and the rest $D_i(1 - \eta_i)$ will be computed locally.

1) Local Computing: For local computing, $D_i(1 - \eta_i)$ bits will be self-executed at the i-th user. The computing time for local computing T_i^L can be expressed as [18]

$$T_i^L = \frac{D_i(1 - \eta_i) F_i}{f_0}, \quad \forall i \in \mathcal{N}, \tag{8}$$

where f_0 is the computing capacity at each user. The power consumption for self-execution is given by

$$P_i^L = \kappa_i (f_0)^3, \tag{9}$$

where $\kappa_i \geq 0$ is the effective switched capacitance.

2) Offloading to UAV: For task offloading, $D_i \eta_i$ bits will be offloaded to the associated UAV. Then, the transmission time for offloading for the i-th associated user is given by [18]

$$T_i^{Tr} = \frac{D_i \eta_i}{B r_{iu}}, \quad \forall i \in \mathcal{N}_{as}, \tag{10}$$

where B is the bandwidth. Denote f_{iu} as the computing capacity of the UAV assigned to the i-th associated user, the computing time for processing each offloading task at the UAV is expressed as

$$T_i^O = \frac{F_i D_i \eta_i}{f_{iu}}, \quad i \in \mathcal{N}_{as}. \tag{11}$$

Note that for non-offloading user, i.e., $i \in \mathcal{N}/\mathcal{N}_{as}$, $T_i^{Tr} = T_i^O = 0$ since it executes the whole task locally and $\eta_i = 0$. Moreover, the CPU power consumption at the UAV for executing the task for the i-th associated user is expressed as [19]

$$P_i^O = \epsilon f_{iu}^3, \quad \forall i \in \mathcal{N}_{as}, \tag{12}$$

where ϵ denotes the power consumption coefficient depending on the chip architecture of the UAV.

C. Offloading, Latency and Power Constraints

The total computing resource allocated to the associated users should be bounded by the maximum UAV computing capacity f_{max}^{UAV} such that

$$\sum_{i=1}^{N} a_i f_{iu} \leq f_{max}^{UAV}. \tag{13}$$

In order to utilize the UAV computing resource more effectively and efficiently, we also impose a minimum offloading requirement D_{min} at the UAV such that

$$\sum_{i=1}^{N} a_i D_i \eta_i \geq D_{min}. \tag{14}$$

Note that each task can be self-executed and processed at the UAV simultaneously. To satisfy the latency requirement, the completion time of this task at the i-th user should be constrained by

$$\max\{T_i^L, (T_i^{Tr} + T_i^O)\} \leq T, \quad \forall i \in \mathcal{N}. \tag{15}$$

Specifically, if the i-th user cannot compute the whole task locally under the latency limitation, i.e., $\frac{D_i F_i}{f_0} \geq T$. Then, it must offload some part of this task to the UAV to reduce the execution time, this intrinsic constraint can be given as

$$(1 - a_i)\frac{D_i F_i}{f_0} \leq T, \quad \forall i \in \mathcal{N}. \tag{16}$$

According to (16), if the i-th user is able to execute the whole task locally within the latency requirement, it can be associated with the UAV or not. Otherwise, the user must be associated with the UAV and a_i must be equal to one to release the constraint.

From the power consumption perspective, for each user, the power is divided into two parts. One part is used for locally computing the task and the other part is used for transmitting. Then the total power consumption constraint at each user can be formulated as

$$P_i^L + p_i \leq P_{max}^{ue}, \quad \forall i \in \mathcal{N}. \tag{17}$$

Moreover, the UAV power consumption which consists of jamming power and CPU processing power should be bounded by a maximal budget P_{max}^{UAV}, which is given by

$$p_{jam} + \sum_{i=1}^{N} a_i P_i^O \leq P_{max}^{UAV}. \tag{18}$$

D. Problem Formulation

In this paper, we seek to optimize six key variables impacting on the security, latency, and offloading performance, namely the UAV location $\mathbf{y} = (x_u, y_u)^T$, users' transmit power $\mathcal{P}^{ue} \triangleq \{p_i, \forall i \in \mathcal{N}\}$, UAV jamming power p_{jam}, offloading ratio $\eta \triangleq \{\eta_i, \forall i \in \mathcal{N}\}$, UAV computing capacity $\mathcal{F} \triangleq \{f_{iu}, \forall i \in \mathcal{N}\}$ and offloading user association $\mathcal{A} \triangleq \{a_i, \forall i \in \mathcal{N}\}$. The objective is to maximize the minimum secrecy capacity among all offloading ground users while guaranteeing the latency, total power and minimum offloading requirements. The optimization problem can be formulated as

$$\max_{\mathbf{y}, \mathcal{P}^{ue}, p_{jam}, \eta, \mathcal{F}, \mathcal{A}} \ \min_{i \in \mathcal{N}_{as}} \ C_i \tag{19a}$$

$$\text{s.t.} \ \sum_{i=1}^{N} a_i f_{iu} \leq f_{max}^{UAV} \tag{19b}$$

$$\sum_{i=1}^{N} a_i D_i \eta_i \geq D_{min} \tag{19c}$$

$$T_i^L \leq T, \quad \forall i \in \mathcal{N} \tag{19d}$$

$$T_i^{Tr} + T_i^O \leq T, \quad \forall i \in \mathcal{N}_{as} \tag{19e}$$

$$(1 - a_i)\frac{D_i F_i}{f_0} \leq T, \quad \forall i \in \mathcal{N} \tag{19f}$$

$$P_i^L + p_i \leq P_{max}^{ue}, \quad \forall i \in \mathcal{N} \tag{19g}$$

$$p_{jam} + \sum_{i=1}^{N} a_i P_i^O \leq P_{max}^{UAV} \tag{19h}$$

$$a_i = \{0, 1\}, \quad \forall i \in \mathcal{N} \tag{19i}$$

$$\eta_i \in [0, 1], \quad \forall i \in \mathcal{N}. \tag{19j}$$

We note that the location uncertainty of the eavesdropping UAVs makes it challenging to obtain a mathematically tractable expression of the objective function in (19). To do so, we consider the eavesdropper location that results in the worst-case lower bound on the secrecy capacity of the i-th offloading user, which is given by

$$\begin{aligned} C_i &= \left[r_{iu} - \max_{e \in \mathcal{E}} \left(\log_2 \left(1 + \frac{p_i h_{ie}}{\sum\limits_{k \in \mathcal{N}, k \neq i} p_k h_{ke} + p_{jam} h_{eu} + \sigma^2} \right) \right) \right]^+ \\ &\geq \left[r_{iu} - \max_{e \in \mathcal{E}} r_{ie}^{ub} \right]^+ = C_i^{lb}, \end{aligned}$$

with

$$r_{ie}^{ub} = \log_2 \left(1 + \frac{p_i h_{ie}^{max}}{\sum\limits_{k \in \mathcal{N}, k \neq i} p_k h_{ke}^{min} + p_{jam} h_{eu}^{min} + \sigma^2} \right), \tag{20}$$

where we consider the UAV location within the uncertainty bound corresponding to the upper bound of eavesdropping rate r_{ie}^{ub} between the i-th user and the e-th eavesdropping UAV. This eavesdropping UAV horizontal location $\mathbf{v}_e$ corresponds to the location satisfying $h_{ie}^{max} = \max\limits_{\mathbf{v}_e \in \Theta_e} h_{ie} = \frac{\beta_1}{H_e^2 + (||\mathbf{w}_i - \tilde{\mathbf{v}}_e|| - \chi)^2}$ when $\mathbf{v}_e = \tilde{\mathbf{v}}_e + \frac{\mathbf{w}_i - \tilde{\mathbf{v}}_e}{||\mathbf{w}_i - \tilde{\mathbf{v}}_e||}\chi$, $h_{ke}^{min} = \min\limits_{\mathbf{v}_e \in \Theta_e} h_{ke} = \frac{\beta_1}{H_e^2 + (||\mathbf{w}_k - \tilde{\mathbf{v}}_e|| + \chi)^2}$ when $\mathbf{v}_e = \tilde{\mathbf{v}}_e - \frac{\mathbf{w}_k - \tilde{\mathbf{v}}_e}{||\mathbf{w}_k - \tilde{\mathbf{v}}_e||}\chi$, and $h_{eu}^{min} = \min\limits_{\mathbf{v}_e \in \Theta_e} h_{eu} = \frac{\beta_2}{(H_u - H_e)^2 + (||\mathbf{y} - \tilde{\mathbf{v}}_e|| + \chi)^2}$ when $\mathbf{v}_e = \tilde{\mathbf{v}}_e - \frac{\mathbf{y} - \tilde{\mathbf{v}}_e}{||\mathbf{y} - \tilde{\mathbf{v}}_e||}\chi$.

Therefore, to make (19) more tractable, we have transformed the objective function to maximize the minimum lower

bound secrecy capacity $\min_{i\in\mathcal{N}_{as}} C_i^{lb}$. Since the joint optimization always results in a non-negative secrecy capacity according to [8] and [14], the $[\cdot]^+$ operator on the objective function can be omitted without affecting the solution. Moreover, we note that even with an explicit expression, the approximated objective function $\max \min_{i\in\mathcal{N}_{as}} C_i^{lb}$ is non-convex due to the $\max(\cdot)$ and $\min(\cdot)$ operations. To convexify the objective function, we further introduce two auxiliary variables C_0 and r_0 [12], which yields the following problem

$$\max_{\mathbf{y},\mathcal{P}^{ue},p_{jam},\eta,\mathcal{F},\mathcal{A},C_0,r_0} C_0 \tag{21a}$$

$$\text{s.t. } r_{iu} - r_0 \geq C_0, \quad \forall i \in \mathcal{N}_{as} \tag{21b}$$

$$r_{ie}^{ub} \leq r_0, \forall i \in \mathcal{N}_{as}, \quad \forall e \in \mathcal{E} \tag{21c}$$

$$(19b) - (19j),$$

where r_0 represents the highest r_{ie}^{ub} among all eavesdropping UAVs and C_0 corresponds to the minimum C_i^{lb} among all offloading users. Although relaxed, problem (21) is still a non-convex optimization problem due to the binary variable $\mathcal{A}$ and non-convex constraints related to the legitimate UAV and upper bound eavesdropper rates in (21b), (21c) and (19e).

III. Proposed Security Maximization Algorithm for UAV-Enabled MEC Systems

In this section, we detail our proposed security maximization algorithm for UAV-enabled MEC systems. To solve the optimization in (21), we apply the BCD method [1] and decouple the original problem into five subproblems. We solve the first three subproblems of optimizing UAV location, users' transmit power and UAV jamming power by applying an SCA technique [1] based on the first-order Taylor expansion of the secrecy capacity. Next, the offloading ratio and UAV computing capacity are jointly optimized in a single convex subproblem based on maximizing the total offloaded packets. Finally, we apply a branch-and-cut method to solve the binary linear offloading user association problem.

A. UAV Location Subproblem

For any given $\mathcal{P}^{ue}, p_{jam}, \eta, \mathcal{F}$ and $\mathcal{A}$, the UAV location of problem (21) can be optimized by solving the following problem

$$\max_{\mathbf{y},C_0,r_0} C_0 \tag{22a}$$

$$\text{s.t. } \underbrace{\log_2\left(\frac{\sum_{i\in\mathcal{N}} \frac{\beta_1 p_i}{H_u^2+||\mathbf{y}-\mathbf{w}_i||^2}+\rho}{\sum_{k\in\mathcal{N},k\neq i} \frac{\beta_1 p_k}{H_u^2+||\mathbf{y}-\mathbf{w}_k||^2}+\rho}\right)}_{r_{iu}} - r_0 \geq C_0,$$

$$\forall i \in \mathcal{N}_{as} \tag{22b}$$

$$\underbrace{\log_2\left(\frac{\frac{\beta_2\ p_{jam}}{(H_u-H_e)^2+(||\mathbf{y}-\tilde{\mathbf{v}}_e||+\chi)^2}+\zeta_{i,e}}{\frac{\beta_2\ p_{jam}}{(H_u-H_e)^2+(||\mathbf{y}-\tilde{\mathbf{v}}_e||+\chi)^2}+\epsilon_{i,e}}\right)}_{r_{ie}^{ub}} \leq r_0,$$

$$\forall i \in \mathcal{N}_{as}, \quad \forall e \in \mathcal{E} \tag{22c}$$

$$\underbrace{\log_2\left(\frac{\sum_{i\in\mathcal{N}} \frac{\beta_1 p_i}{H_u^2+||\mathbf{y}-\mathbf{w}_i||^2}+\rho}{\sum_{k\in\mathcal{N},k\neq i} \frac{\beta_1 p_k}{H_u^2+||\mathbf{y}-\mathbf{w}_k||^2}+\rho}\right)}_{r_{iu}} \geq \iota_i,$$

$$\forall i \in \mathcal{N}_{as}, \tag{22d}$$

where the constraints (22b), (22c), and (22d) correspond to (21b), (21c) and (19e), respectively, and all other constraints in (21) are not applicable. In (22), we define $\rho = \gamma p_{jam} + \sigma^2$, $\zeta_{i,e} = p_i h_{ie}^{max} + \sum_{k\in\mathcal{N},k\neq i} p_k h_{ke}^{min} + \sigma^2$, $\epsilon_{i,e} = \sum_{k\in\mathcal{N},k\neq i} p_k h_{ke}^{min} + \sigma^2$ and $\iota_i = \frac{D_i\eta_i}{B(T-T_i^O)}$. Note that (22) is a non-convex optimization problem due to the non-convexity of the logarithm terms in r_{iu} and r_{ie}^{ub}.

In the following, we adopt the SCA technique [1] to re-express r_{iu} as

$$r_{iu} = \mathcal{I}_1 - \underbrace{\log_2\left(\sum_{k\in\mathcal{N},k\neq i} \frac{\beta_1 p_k}{H_u^2+||\mathbf{y}-\mathbf{w}_k||^2}+\rho\right)}_{\mathcal{I}_2}, \tag{23}$$

where $\mathcal{I}_1$ is a concave lower bound expression based on the first-order Taylor expansion at the UAV location in the m-th iteration, $\mathbf{y}[m]$, given by

$$\mathcal{I}_1 = \log_2\left(\sum_{i\in\mathcal{N}} \frac{\beta_1 p_i}{H_u^2+||\mathbf{y}[m]-\mathbf{w}_i||^2}+\rho\right) - \frac{\sum_{i\in\mathcal{N}} \frac{\beta_1 p_i}{(H_u^2+||\mathbf{y}[m]-\mathbf{w}_i||^2)^2}\left(||\mathbf{y}-\mathbf{w}_i||^2 - ||\mathbf{y}[m]-\mathbf{w}_i||^2\right)}{\left(\sum_{i\in\mathcal{N}} \frac{\beta_1 p_i}{H_u^2+||\mathbf{y}[m]-\mathbf{w}_i||^2}+\rho\right)\ln 2}. \tag{24}$$

To convexify $\mathcal{I}_2$, we define an auxiliary variable $s_k \leq ||\mathbf{y}-\mathbf{w}_k||^2$ and apply a Taylor expansion at $\mathbf{y}[m]$ which results in

$$\mathcal{I}_2 = \log_2\left(\sum_{k\in\mathcal{N},k\neq i} \frac{\beta_1 p_k}{H_u^2+s_k}+\rho\right), \tag{25}$$

where

$$s_k \leq ||\mathbf{y}[m]-\mathbf{w}_k||^2 + 2(\mathbf{y}[m]-\mathbf{w}_k)^T(\mathbf{y}-\mathbf{y}[m]), \quad \forall k \in \mathcal{N}, \quad k \neq i. \tag{26}$$

Based on (24) and (25), the legitimate UAV rate r_{iu} is now concave and the corresponding constraints (22b) and (22d) are convex.

Applying the SCA approach to (22c), r_{ie}^{ub} can be rewritten as

$$r_{ie}^{ub} = \log_2\left(\frac{\beta_2\ p_{jam}}{(H_u-H_e)^2+t_e}+\zeta_{i,e}\right) - \mathcal{I}_3, \tag{27}$$

where

$$\mathcal{I}_3 = \log_2\left(\frac{\beta_2 p_{jam}}{(H_u-H_e)^2+(||\mathbf{y}[m]-\tilde{\mathbf{v}}_e||+\chi)^2}+\epsilon_{i,e}\right) - \frac{\vartheta_e((||\mathbf{y}-\tilde{\mathbf{v}}_e||+\chi)^2 - (||\mathbf{y}[m]-\tilde{\mathbf{v}}_e||+\chi)^2)}{\left(\frac{\beta_2 p_{jam}}{(H_u-H_e)^2+(||\mathbf{y}[m]-\tilde{\mathbf{v}}_e||+\chi)^2}+\epsilon_{i,e}\right)\ln 2}, \tag{28}$$

with $\vartheta_e = \frac{\beta_2\ p_{jam}}{((H_u-H_e)^2+(||\mathbf{y}[m]-\tilde{\mathbf{v}}_e||+\chi)^2)^2}$ and

$$t_e \leq (||\mathbf{y}[m]-\tilde{\mathbf{v}}_e||+\chi)^2 + 2(||\mathbf{y}[m]-\tilde{\mathbf{v}}_e||+\chi)\frac{(\mathbf{y}[m]-\tilde{\mathbf{v}}_e)^T}{||\mathbf{y}[m]-\tilde{\mathbf{v}}_e||}(\mathbf{y}-\mathbf{y}[m]), \quad \forall e \in \mathcal{E}. \tag{29}$$

Finally, the UAV location subproblem can be solved as

$$\max_{\mathbf{y},C_0,r_0,\mathcal{S},\mathcal{T}} C_0 \tag{30a}$$
$$\text{s.t. } \mathcal{I}_1 - \mathcal{I}_2 - r_0 \geq C_0, \quad \forall i \in \mathcal{N}_{as} \tag{30b}$$
$$\log_2\left(\frac{\beta_2\ p_{jam}}{(H_u-H_e)^2+t_e}+\zeta_{i,e}\right) - \mathcal{I}_3 \leq r_0, \quad \forall i \in \mathcal{N}_{as},\ \forall e \in \mathcal{E} \tag{30c}$$
$$\mathcal{I}_1 - \mathcal{I}_2 \geq \iota_i, \quad \forall i \in \mathcal{N}_{as} \tag{30d}$$
$$(26),\ (29),$$

where $\mathcal{S} \triangleq \{s_k, \forall k \in \mathcal{N}, k \neq i\}$ and $\mathcal{T} \triangleq \{t_e, \forall e \in \mathcal{E}\}$. Due to the convexity of (30), it can be efficiently solved by utilizing convex optimization software [29].

B. Users' Transmit Power Subproblem

For any given $\mathbf{y}, p_{jam}, \eta, \mathcal{F}$ and $\mathcal{A}$, the users' transmit power of problem (21) can be optimized by solving the following problem

$$\max_{P^{ue},C_0,r_0} C_0 \tag{31a}$$
$$\text{s.t. } r_{iu} - r_0 \geq C_0, \quad \forall i \in \mathcal{N}_{as} \tag{31b}$$
$$r_{ie}^{ub} \leq r_0, \forall i \in \mathcal{N}_{as}, \quad \forall e \in \mathcal{E} \tag{31c}$$
$$r_{iu} \geq \iota_i, \quad \forall i \in \mathcal{N}_{as} \tag{31d}$$
$$p_i \leq P_{max}^{ue} - P_i^L, \quad \forall i \in \mathcal{N}, \tag{31e}$$

where the constraints (31b), (31c), (31d), and (31e) correspond to (21b), (21c), (19e) and (19g), respectively, and all other constraints in (21) are not applicable. Note that problem (31) is a non-convex optimization problem due to the non-convexity of r_{iu} and r_{ie}^{ub}. In the following, we adopt the SCA technique to solve this problem.

To this end, r_{iu} can be rewritten as

$$r_{iu} = \log_2\left(\sum_{i\in\mathcal{N}} p_i h_{iu} + \rho\right) - \underbrace{\log_2\left(\sum_{k\in\mathcal{N},k\neq i} p_k h_{ku} + \rho\right)}_{\mathcal{I}_4}. \tag{32}$$

We apply the similar approach as mentioned in Subsection III-A and successively approximate $\mathcal{I}_4$ into convex term with respect to the users' transmit power in the m-th iteration, $p_k[m]$, which is reexpressed as

$$\mathcal{I}_4 = \log_2\left(\sum_{k\in\mathcal{N},k\neq i} p_k[m]h_{ku} + \rho\right) + \frac{\sum_{k\in\mathcal{N},k\neq i} h_{ku}(p_k - p_k[m])}{\left(\sum_{k\in\mathcal{N},k\neq i} p_k[m]h_{ku} + \rho\right)\ln 2}. \tag{33}$$

To convexify (31c), we apply similar approach to r_{ie}^{ub} and reformulate it as

$$r_{ie}^{ub} = \mathcal{I}_5 - \log_2\left(\sum_{k\in\mathcal{N},k\neq i} p_k h_{ke}^{min} + \omega_e\right), \tag{34}$$

where $\omega_e = p_{jam}h_{eu}^{min} + \sigma^2$ and $\mathcal{I}_5$ is a convex upper bound expression based on the first-order Taylor expansion in terms of the users' transmit power in the m-th iteration, which is given by

$$\mathcal{I}_5 = \log_2\left(p_i[m]h_{ie}^{max} + \sum_{k\in\mathcal{N},k\neq i} p_k[m]h_{ke}^{min} + \omega_e\right) + \frac{h_{ie}^{max}(p_i - p_i[m]) + \sum_{k\in\mathcal{N},k\neq i} h_{ke}^{min}(p_k - p_k[m])}{\left(p_i[m]h_{ie}^{max} + \sum_{k\in\mathcal{N},k\neq i} p_k[m]h_{ke}^{min} + \omega_e\right)\ln 2}. \tag{35}$$

Based on (33) and (35), the users' transmit power subproblem can be efficiently solved using general convex optimization solvers by re-expressing the constraints in (31) as

$$\max_{P^{ue},C_0,r_0} C_0 \tag{36a}$$
$$\text{s.t. } \log_2\left(\sum_{i\in\mathcal{N}} p_i h_{iu} + \rho\right) - \mathcal{I}_4 - r_0 \geq C_0, \quad \forall i \in \mathcal{N}_{as} \tag{36b}$$
$$\mathcal{I}_5 - \log_2\left(\sum_{k\in\mathcal{N},k\neq i} p_k h_{ke}^{min} + \omega_e\right) \leq r_0, \quad \forall i \in \mathcal{N}_{as},\ \forall e \in \mathcal{E} \tag{36c}$$
$$\log_2\left(\sum_{i\in\mathcal{N}} p_i h_{iu} + \rho\right) - \mathcal{I}_4 \geq \iota_i, \quad \forall i \in \mathcal{N}_{as} \tag{36d}$$
$$(31e).$$

C. UAV Jamming Power Subproblem

For any given $\mathbf{y}, \mathcal{P}^{ue}, \eta, \mathcal{F}$ and $\mathcal{A}$, the UAV jamming power of problem (21) can be optimized by solving

$$\max_{p_{jam},C_0,r_0} C_0 \tag{37a}$$
$$\text{s.t. } r_{iu} - r_0 \geq C_0, \quad \forall i \in \mathcal{N}_{as} \tag{37b}$$
$$r_{ie}^{ub} \leq r_0, \quad \forall i \in \mathcal{N}_{as},\ \forall e \in \mathcal{E} \tag{37c}$$
$$r_{iu} \geq \iota_i, \quad \forall i \in \mathcal{N}_{as} \tag{37d}$$
$$p_{jam} \leq (P_{max}^{UAV} - \sum_{i=1}^{N} a_i P_i^O), \tag{37e}$$

where the constraints (37b), (37c), (37d), and (37e) correspond to (21b), (21c), (19e) and (19h), respectively, and all other constraints in (21) are not applicable. Note that problem (37) is non-convex and the non-convexity arises from (37b) and (37d).

Specifically, the first term of (37b), i.e., r_{iu}, can be written as the difference of two concave functions in terms of p_{jam} as

$$r_{iu} = \log_2\left(\sum_{i\in\mathcal{N}} p_i h_{iu} + \gamma p_{jam} + \sigma^2\right) - \mathcal{I}_6, \quad (38)$$

where $\mathcal{I}_6$ is a convex upper bound expression based on the first-order Taylor expansion in terms of the UAV jamming power in the m-th iteration, $p_{jam}[m]$, given by

$$\mathcal{I}_6 = \log_2\left(\sum_{k\in\mathcal{N},k\neq i} p_k h_{ku} + \gamma p_{jam}[m] + \sigma^2\right) + \frac{\gamma(p_{jam} - p_{jam}[m])}{(\sum_{k\in\mathcal{N},k\neq i} p_k h_{ku} + \gamma p_{jam}[m] + \sigma^2)\ln 2}. \quad (39)$$

According to (39), the UAV jamming power subproblem can be solved as

$$\max_{p_{jam},C_0,r_0} \; C_0 \quad (40a)$$

$$\text{s.t. } \log_2\left(\sum_{i\in\mathcal{N}} p_i h_{iu} + \gamma p_{jam} + \sigma^2\right) - \mathcal{I}_6 - r_0 \geq C_0, \quad \forall i \in \mathcal{N}_{as} \quad (40b)$$

$$\log_2\left(\sum_{i\in\mathcal{N}} p_i h_{iu} + \gamma p_{jam} + \sigma^2\right) - \mathcal{I}_6 \geq \iota_i, \quad \forall i \in \mathcal{N}_{as} \quad (40c)$$

$$(37c),\ (37e).$$

We note that (40) is a convex optimization problem and can be efficiently solved by convex optimization software.

D. Offloading Ratio and UAV Computing Capacity Subproblems

According to (2), (5) and (21), we note that the offloading ratio and UAV computing capacity variables do not directly appear in the secrecy objective function. However, to satisfy the latency and offloading constraints, we observe that the total offloaded packets from the users to the UAV is determined by the offloading ratio, the selection of user offloading ratio will directly impact the user association solution, which affects the max-min secrecy capacity. Therefore, we proceed to maximize the total offloaded packets by optimizing the offloading ratio while satisfying the latency requirements for any given $\mathbf{y}, \mathcal{P}^{ue}, p_{jam}, \mathcal{F}$ and $\mathcal{A}$, which is given by

$$\max_{\eta} \sum_{i\in\mathcal{N}_{as}} D_i\eta_i$$
$$\text{s.t. } (19d),\ (19e),\ (19j). \quad (41a)$$

We note that maximizing the total offloaded packets is equivalent to maximizing $\eta_i, i \in \mathcal{N}_{as}$ for any given user association. Therefore, the optimal offloading ratio can be derived in closed-form by setting the constraint (19e) with equality, which is given by

$$\eta_i = \min\left(\frac{T r_{iu} f_{iu} B}{D_i f_{iu} + F_i D_i B r_{iu}}, 1\right), \quad \forall i \in \mathcal{N}_{as}. \quad (42)$$

Note that problem (41) is feasible if and only if

$$\eta_i \geq \max\left(1 - \frac{T f_0}{D_i F_i}, 0\right), \quad \forall i \in \mathcal{N}_{as}. \quad (43)$$

Moreover, the relation between the UAV computing capacity and user offloading ratio can be seen from (11) where for a given latency requirement, the UAV computing capacity is proportional to the user offloading ratio. Therefore, in order to maximize the minimum computing capacity that the UAV allocates to each associated user, the UAV computing capacity problem of (21) for any given $\mathbf{y}, \mathcal{P}^{ue}, p_{jam}, \eta$ and $\mathcal{A}$ can be optimized by solving the following problem

$$\max_{\mathcal{F},f_{min}} \; f_{min} \quad (44a)$$

$$\text{s.t. } f_{min} \leq f_{iu}, \quad \forall i \in \mathcal{N}_{as} \quad (44b)$$

$$(19b),\ (19e),\ (19h),$$

where f_{min} is the minimum computing capacity that UAV allocates to associated users. Problem (44) is a convex optimization problem since all constraints are convex, therefore, it can be solved with general convex optimizer.

E. User Association Subproblem

For any given $\mathbf{y}, \mathcal{P}^{ue}, p_{jam}, \eta$ and $\mathcal{F}$, the user association variables can be optimized by solving the following problem

$$\max_{\mathcal{A},C_0} \; C_0 \quad (45a)$$

$$\text{s.t. } a_i\xi_i + (1 - a_i)M \geq C_0, \quad \forall i \in \mathcal{N} \quad (45b)$$

$$(19b),\ (19c),\ (19e),\ (19f),\ (19h),\ (19i),$$

where $\xi_i = r_{iu} - \max_{e\in\mathcal{E}} r_{ie}^{ub}$ and M is a sufficiently large number which is greater than the upper bound of C_0 to ensure that the objective function C_0 is non-zero when $a_i = 0$. Due to the binary variable a_i, problem (45) is non-convex. However, due to the linear constraints, the user association subproblem is a binary integer linear problem with linear constraints which can be solved by using the branch-and-cut method.

F. Proposed Iterative Algorithm

Based on the aforementioned analysis, we describe our proposed iterative algorithm in Algorithm 1 where the UAV location $\mathbf{y}$, the users' transmit power $\mathcal{P}^{ue}$, the UAV jamming power p_{jam}, the offloading ratios η, the UAV computing capacity $\mathcal{F}$ and user association $\mathcal{A}$ are successively optimized by solving problems (30), (36), (40), (42), (44) and (45) respectively, while keeping the other variables fixed. Moreover, the derived solution in each iteration will be applied as the input for the next iteration. We note that similar convergence analysis from step 3 to step 5 of Algorithm 1 for UAV location, users' transmit power and UAV jamming power subproblems which are solved by SCA technique has been proved in [1] and thus it is omitted here for brevity. According to [1], we have $C_0(\mathbf{y}[m], \mathcal{P}_{ue}[m], p_{jam}[m], \eta[m], \mathcal{F}[m], \mathcal{A}[m]) \leq C_0(\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m], \mathcal{F}[m], \mathcal{A}[m])$.

Moreover, in step 6 and 7 of Algorithm 1, since $\eta[m+1]$ and $\mathcal{F}[m+1]$ are not in the objective function and

Algorithm 1 Proposed Iterative Optimization for Problem (19)

1: initialize $m = 0$, $\mathbf{y}[m], \mathcal{P}_{ue}[m], p_{jam}[m], \eta[m], \mathcal{F}[m]$ and $\mathcal{A}[m]$.
2: **repeat**
3: Given $\{\mathcal{P}_{ue}[m], p_{jam}[m], \eta[m], \mathcal{F}[m], \mathcal{A}[m]\}$, find the optimal UAV location $\mathbf{y}[m+1]$ according to (30);
4: Given $\{\mathbf{y}[m+1], p_{jam}[m], \eta[m], \mathcal{F}[m], \mathcal{A}[m]\}$, find the optimal users' transmit power $\mathcal{P}_{ue}[m+1]$ according to (36);
5: Given $\{\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], \eta[m], \mathcal{F}[m], \mathcal{A}[m], \}$, find the optimal UAV jamming power $p_{jam}[m+1]$ according to (40);
6: Given $\{\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \mathcal{F}[m], \mathcal{A}[m]\}$, find the optimal offloading ratio $\eta[m+1]$ according to (42);
7: Given $\{\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m+1], \mathcal{A}[m]\}$, find the optimal UAV computing capacity $\mathcal{F}[m+1]$ according to (44);
8: Given $\{\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m+1], \mathcal{F}[m+1]\}$, find the optimal user association $\mathcal{A}[m+1]$ according to (45);
9: Update $m = m + 1$;
10: **until** convergence.

the objective value will keep the same in these subproblems, which results in $C_0(\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m], \mathcal{F}[m], \mathcal{A}[m]) = C_0(\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m+1], \mathcal{F}[m], \mathcal{A}[m]) = C_0(\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m+1], \mathcal{F}[m+1], \mathcal{A}[m])$.

Finally, in step 8 of Algorithm 1, since $\mathcal{A}[m+1]$ is the globally optimal solution for (45) with fixed $\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m+1]$ and $\mathcal{F}[m+1]$, we have $C_0(\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m+1], \mathcal{F}[m+1], \mathcal{A}[m]) \leq C_0(\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m+1], \mathcal{F}[m+1], \mathcal{A}[m+1])$.

According to the above analysis, we can conclude that $C_0(\mathbf{y}[m], \mathcal{P}_{ue}[m], p_{jam}[m], \eta[m], \mathcal{F}[m], \mathcal{A}[m]) \leq C_0(\mathbf{y}[m+1], \mathcal{P}_{ue}[m+1], p_{jam}[m+1], \eta[m+1], \mathcal{F}[m+1], \mathcal{A}[m+1])$, which shows that the algorithm yields a non-decreasing sequence of the objective value. In addition, the objective value has upper bound. Hence, the proposed algorithm is guaranteed to converge.

IV. Simulation Results

In this section, we present numerical results to validate our analysis and demonstrate the effectiveness of our proposed algorithm. We consider $N = 8$ users and $E = 2$ eavesdropping UAVs that are randomly and uniformly distributed within a 400 m $\times$ 400 m square area. The legitimate UAV has a fixed altitude of $H_u = 120$ m [5] and the eavesdropping UAVs are operated at the altitudes of 110 m and 130 m, respectively. The maximum estimation error is set as $\chi = 10$ m [14] and the noise power is $\sigma^2 = -110$ dBm. The channel power gains for air-to-ground channel and air-to-air channel are set as $\beta_1 = 10^{-5}$ and $\beta_2 = 10^{-4}$, respectively. We set the power consumption coefficients at the user and UAV as $\kappa_i = \epsilon = 10^{-27}$ [19] and the UAV SI efficiency as $\gamma = 10^{-11}$ [23].

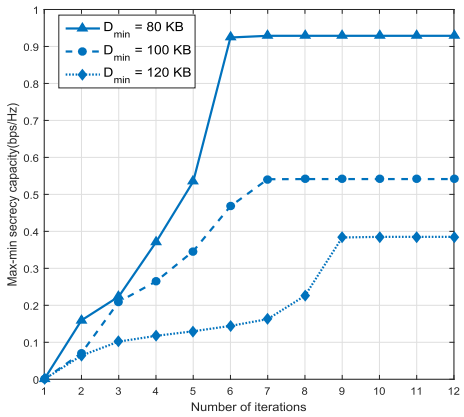


Fig. 2. Max-min secrecy capacity versus number of iterations with different minimum offloading requirements.

We consider the required number of CPU cycles per bit is $F_i = 1000$ cycles/bit. The computing capacity of the legitimate UAV and ground users are set as $f_{max}^{UAV} = 2000$ MHz and $f_0 = 200$ MHz, respectively. The power budgets at the legitimate UAV and ground users are $P_{max}^{UAV} = 1$ W and $P_{max}^{ue} = 0.1$ W, respectively. The transmission bandwidth is set as $B = 1$ MHz. We consider data offloading with large task size D_i which follows a uniform distribution $D_i \sim U[20, 50]$ KB with a latency requirement of $T = 0.2$ s [16].

Fig. 2 shows the convergence of Algorithm 1 with different minimum offloading requirements D_{min}. The plot shows that our proposed algorithm quickly converges within 12 iterations. Furthermore, we find that the max-min secrecy capacity increases as D_{min} decreases. This is because to maximize the minimum secrecy capacity according to (45), users with the highest secrecy capacity will be selected to offload packets to the legitimate UAV to satisfy the minimum offloading requirement. Therefore, with a smaller D_{min}, fewer users will be selected to associate with the legitimate UAV and a larger max-min secrecy capacity is achieved.

In Fig. 3, we highlight the impact of locations of ground users on the max-min secrecy capacity and plot the cumulative distribution function (CDF) of the max-min secrecy capacity for random locations of the ground users. We compare our proposed joint optimization solution in Algorithm 1 with the following four benchmark schemes: 1) Fixed UAV location: We set the UAV location to be at the centroid of all users and all other variables are optimized using Algorithm 1; 2) Fixed users' transmit power: We set $p_i = 0.01$ W, $\forall i \in \mathcal{N}$ and all other variables are optimized using Algorithm 1; 3) No UAV jamming: We set $p_{jam} = 0$ W and all other variables are optimized using Algorithm 1; 4) Fixed offloading variables: We set $\eta_i = 0.5, f_{iu} = f_{max}^{UAV}/N, \forall i \in \mathcal{N}_{as}$ and all other variables are optimized using Algorithm 1. Fig. 3 shows that our proposed joint optimization solution outperforms all other baseline solutions over a wide range of random locations of ground users. Our proposed joint optimization solution achieves a max-min secrecy capacity median of 0.9 bps/Hz, which significantly outperforms the "Fixed UAV location", "Fixed users' transmit power", "No UAV jamming", and "Fixed offloading variables" strategies by at least 243%.

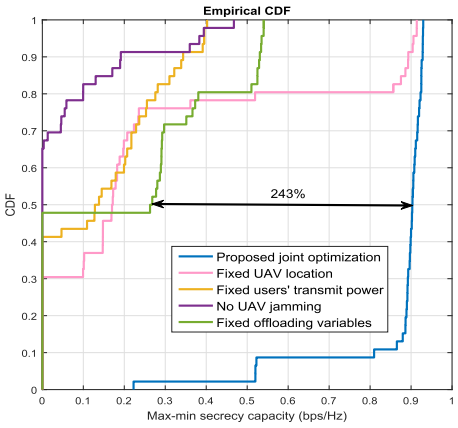


Fig. 3. CDF of max-min secrecy capacity for random locations of ground users when $T = 0.2$ s and $D_{min} = 60$ KB.

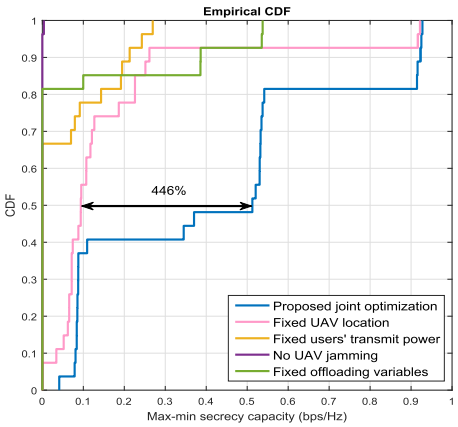


Fig. 4. CDF of max-min secrecy capacity for random packet sizes of ground users when $T = 0.2$ s and $D_{min} = 60$ KB.

Fig. 4 depicts the CDF of the max-min secrecy capacity for random packet sizes of the ground users. It can be seen that our proposed joint optimization solution outperforms all other baseline solutions over a wide range of random packet sizes of ground users. We note that our proposed joint optimization solution achieves a max-min secrecy capacity median of 0.51 bps/Hz, which significantly outperforms the "Fixed UAV location", "Fixed users' transmit power", "No UAV jamming", and "Fixed offloading variables" strategies by at least 446%.

Fig. 5 plots the max-min secrecy capacity as a function of SI efficiency γ when $T = 0.2$ s and $D_{min} = 60$ KB. It shows that our proposed joint optimization solution outperforms all other baseline solutions over a wide range of SI efficiencies. Moreover, we find that the max-min secrecy capacity is independent of γ in "No UAV jamming" scheme due to $p_{jam} = 0$ W, while it keeps decreasing with increasing γ for all other strategies. This is intuitive since a higher γ results in a stronger residual self-interference power at the legitimate UAV, which further reduces the max-min secrecy capacity. Particularly, when SI efficiency γ increases from -120 dB to -100 dB, the max-min secrecy capacity decreases from 0.982 bps/Hz to 0.485 bps/Hz for our proposed joint optimization solution.

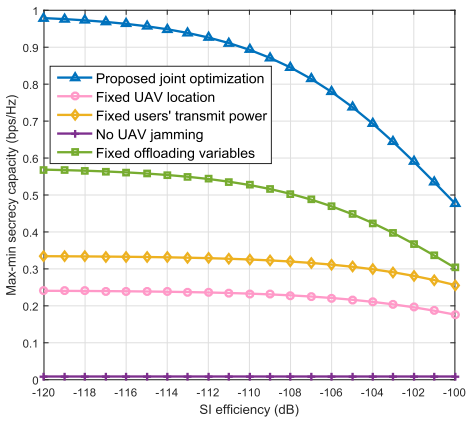


Fig. 5. Max-min secrecy capacity as a function of SI efficiency γ when $T = 0.2$ s and $D_{min} = 60$ KB.

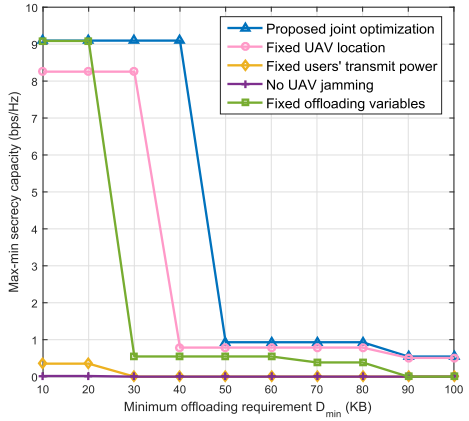
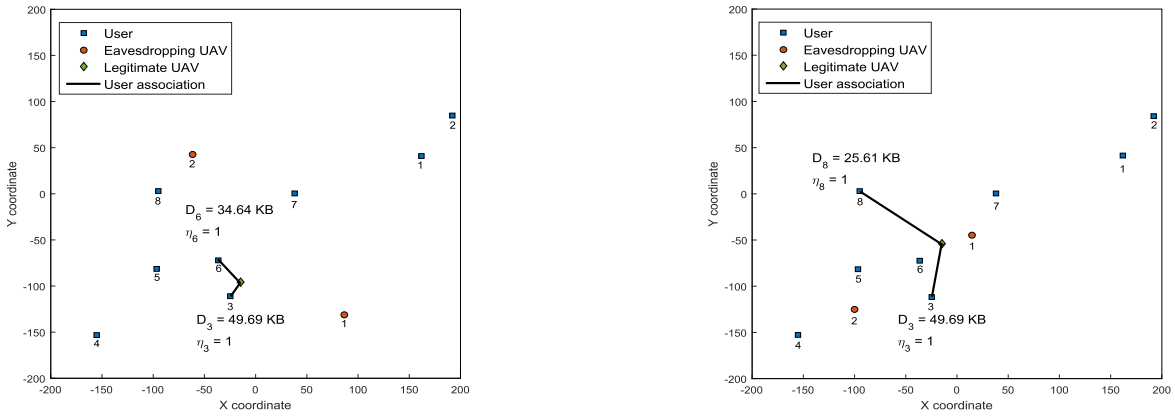


Fig. 6. Max-min secrecy capacity as a function of the minimum offloading requirement D_{min} when $T = 0.2$ s.

Fig. 6 plots the max-min secrecy capacity as a function of the minimum offloading requirement D_{min} when $T = 0.2$ s. We find that the max-min secrecy capacity is a decreasing step function in terms of D_{min}. Each decreasing step change corresponds to an increase in the number of associated users. This is because a low offloading requirement can be easily satisfied by associating with the user with the highest secrecy capacity. Specifically, when the offloading requirement increases from 10 KB to 50 KB, the max-min secrecy capacity decreases from 9.1 bps/Hz to approximately 1 bps/Hz for our proposed joint optimization solution. The figure shows that when D_{min} is less than 20 KB, the fixed offloading variables approach achieves the same performance as our proposed joint optimization solution because the same single user is associated with the UAV. When D_{min} is greater than 20 KB, we find that our proposed joint optimization solution outperforms the other benchmark approaches.

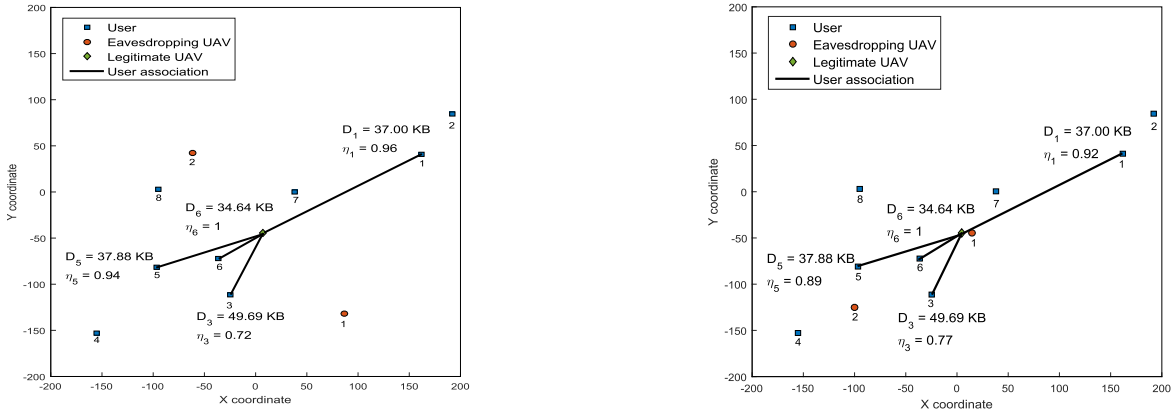
Figs. 7 and 8 demonstrate the impact of estimated locations of eavesdropping UAVs on the max-min secrecy capacity when $T = 0.2$ s and $T = 0.16$ s, respectively. We note that when $T = 0.2$ s, only user 3 must offload some of its large-size task to the legitimate UAV to satisfy the latency constraint. It can be seen from Fig. 7 that in order to improve the secrecy capacity, the legitimate UAV chooses different users to associate with based on different estimated locations of the



(a) The max-min secrecy capacity is 0.930 bps/Hz.

(b) The max-min secrecy capacity is 0.745 bps/Hz.

Fig. 7. The optimal system configuration when $T = 0.2$ s and $D_{min} = 60$ KB for different estimated locations of eavesdropping UAVs.



(a) The max-min secrecy capacity is 0.384 bps/Hz.

(b) The max-min secrecy capacity is 0.347 bps/Hz.

Fig. 8. The optimal system configuration when $T = 0.16$ s and $D_{min} = 60$ KB for different estimated locations of eavesdropping UAVs.

eavesdropping UAVs. Specifically, when the eavesdropping UAVs are located as shown in Fig. 7(a), the users 3 and 6 are associated with the legitimate UAV with a max-min secrecy capacity of 0.930 bps/Hz, whereas only a max-min secrecy capacity of 0.745 bps/Hz can be achieved when the eavesdropping UAVs are located as shown in Fig. 7(b) and the legitimate UAV associates with the users 3 and 8. Moreover, with a strict latency requirement when $T = 0.16$ s, the users 1, 3, 5 and 6 must offload some of their large-size tasks due to the limited local computing resource equipped on them. It can be seen from Fig. 8 that the max-min secrecy capacity decreases from 0.384 bps/Hz to 0.347 bps/Hz when the estimated locations of the eavesdropping UAVs change from Fig. 8(a) to Fig. 8(b) without affecting the user association due to the strict latency requirement. This is intuitive since closer estimated locations of eavesdropping UAVs result in a reduced secrecy performance.

Figs. 7(a) and 8(a) show the impact of latency on the max-min secrecy capacity with the same locations of both the ground users and eavesdropping UAVs. We observe that when the latency requirement decreases from $T = 0.2$ s to $T = 0.16$ s, the max-min secrecy capacity also decreases from 0.930 bps/Hz to 0.384 bps/Hz. According to (8), (10) and (11), we note that the latency affects the objective function from two aspects. On the one hand, for local computing, when the latency requirement is very strict, more users with large packet size cannot meet the latency requirement with local computing. Thus, more users will offload tasks to the UAV and the max-min secrecy capacity is low. On the other hand, for offloading, the offloading ratio η at each associated user should be small to reduce the transmission and offloading time and ensure that the strict latency requirement is guaranteed. This leads to more users associating with the UAV to meet the minimum offloading requirement and reducing the max-min secrecy capacity. This phenomenon is verified in Figs. 7(a) and 8(a) where only user 3 and 6 with $\eta_3 = 1$ and $\eta_6 = 1$ are associated with the legitimate UAV when $T = 0.2$ s, whereas the users 1, 3, 5 and 6 are associated with the legitimate UAV when $T = 0.16$ s with offloading ratios $\eta_1 = 0.96$, $\eta_3 = 0.72$, $\eta_5 = 0.94$ and $\eta_6 = 1$, respectively.

Fig. 9 shows the tradeoff between the max-min secrecy capacity and the actual system latency as a function of the UAV self-interference efficiency γ. We set the γ between -110 dB to -120 dB. The actual system latency is defined as the maximum latency over all users, which is $T_{ac} = \max_{i \in \mathcal{N}} \max\{T_i^L, (T_i^{Tr} + T_i^O)\}$. The plot shows that a higher

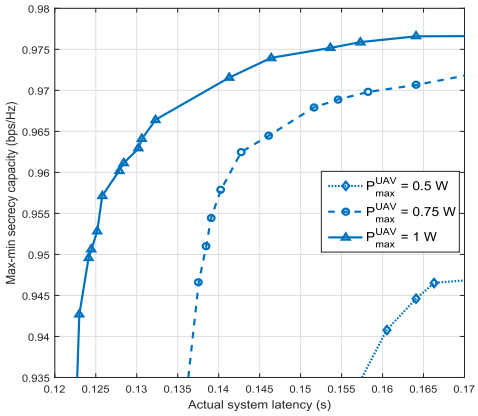


Fig. 9. The tradeoff between the max-min secrecy capacity and actual system latency as a function of γ when $T = 0.2$ s and $D_{min} = 60$ KB.

max-min secrecy capacity is achievable with longer latency. Conversely, a lower latency system design can be achieved by sacrificing the security performance. This is because when γ is small, the self-interference at the legitimate UAV can be effectively cancelled and a higher UAV jamming power is available for the eavesdropping links. To maximize the minimum secrecy capacity, more UAV power is allocated for jamming and less power is used for processing the offloaded packets, which results in an increased system latency. We can see from Fig. 9 that for $P_{max}^{UAV} = 1$ W, the max-min secrecy capacity increases from 0.935 bps/Hz to 0.977 bps/Hz when the actual system latency increases from 0.123 s to 0.170 s. We note that the security-latency feasible region can be increased by increasing the UAV power since more power is available for both jamming and offloading.

V. Conclusion

This paper investigated the security performance of a UAV-enabled MEC system with multiple ground users, one legitimate UAV and multiple eavesdropping UAVs with imperfect locations. To maximize the minimum secrecy capacity, the UAV location, users' transmit power, UAV jamming power, offloading ratio, UAV computing capacity and offloading user association are jointly optimized with the latency, total power and minimum offloading requirements. Moreover, an efficient algorithm is proposed to solve the optimization problem iteratively. Numerical results show that our proposed iterative algorithm outperforms other baseline schemes over a wide range of SI efficiencies, locations and packet sizes of ground users. Furthermore, we show that there exists a fundamental tradeoff between the security and latency of UAV-enabled MEC systems which depends on the full-duplex self-interference efficiency and total UAV power constraints. To further improve the security performance, the extension to multiple legitimate UAVs would be an interesting future research direction which results in a more-complex optimization problem with multiple possible UAVs for user offloading.

References

[1] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-UAV enabled wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 2109–2121, Mar. 2018.

[2] C. She, C. Liu, T. Q. S. Quek, C. Yang, and Y. Li, "Ultra-reliable and low-latency communications in unmanned aerial vehicle communication systems," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3768–3781, May 2019.

[3] Z. Yang *et al.*, "Joint altitude, beamwidth, location, and bandwidth optimization for UAV-enabled communications," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1716–1719, Aug. 2018.

[4] M. Alzenad, A. El-Keyi, and H. Yanikomeroglu, "3-D placement of an unmanned aerial vehicle base station for maximum coverage of users with different QoS requirements," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 38–41, Feb. 2018.

[5] C. Pan, H. Ren, Y. Deng, M. Elkashlan, and A. Nallanathan, "Joint blocklength and location optimization for URLLC-enabled UAV relay systems," *IEEE Commun. Lett.*, vol. 23, no. 3, pp. 498–501, Mar. 2019.

[6] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun.*, to be published.

[7] Z. Li, M. Chen, C. Pan, N. Huang, Z. Yang, and A. Nallanathan, "Joint trajectory and communication design for secure UAV networks," *IEEE Wireless Commun. Lett.*, vol. 23, no. 4, pp. 636–639, Apr. 2019.

[8] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1376–1389, Feb. 2019.

[9] S. Zhang, H. Zhang, Q. He, K. Bian, and L. Song, "Joint trajectory and power optimization for UAV relay networks," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 161–164, Jan. 2018.

[10] Y. Zhou *et al.*, "Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11280–11284, Nov. 2018.

[11] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 181–184, Jan. 2019.

[12] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Trans. Veh. Commun.*, vol. 67, no. 10, pp. 9385–9392, Oct. 2018.

[13] X. Zhou, Q. Wu, S. Yan, F. Shu, and J. Li, "UAV-enabled secure communications: Joint trajectory and transmit power optimization," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4069–4073, Apr. 2019.

[14] C. Zhong, J. Yao, and J. Xu, "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 286–289, Feb. 2019.

[15] H. Chen *et al.*, "Ultra-reliable low latency cellular networks: Use cases, challenges and approaches," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 119–125, Dec. 2018.

[16] 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, Mar. 2018.

[17] X. Chen, L. Jiao, W. Li, and X. Fu, "Efficient multi-user computation offloading for mobile-edge cloud computing," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 2795–2808, Oct. 2016.

[18] Y. Dai, D. Xu, S. Maharjan, and Y. Zhang, "Joint computation offloading and user association in multi-task mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12313–12325, Dec. 2018.

[19] Q. Hu, Y. Cai, G. Yu, Z. Qin, M. Zhao, and G. Y. Li, "Joint offloading and trajectory design for UAV-enabled mobile edge computing systems," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1879–1892, Apr. 2019.

[20] J. Lyu, Y. Zeng, and R. Zhang, "UAV-aided offloading for cellular hotspot," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3988–4001, Jun. 2018.

[21] J. Xiong, H. Guo, and J. Liu, "Task offloading in UAV-aided edge computing: Bit allocation and trajectory optimization," *IEEE Commun. Lett.*, vol. 23, no. 3, pp. 538–541, Mar. 2019.

[22] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[23] H. Ju and R. Zhang, "Optimal resource allocation in full-duplex wireless-powered communication network," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3528–3540, Oct. 2014.

[24] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[25] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[26] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[27] H. Lei *et al.*, "Secrecy outage of Max–Min TAS scheme in MIMO-NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6981–6990, Aug. 2018.
[28] K. Wang, K. Yang, and C. S. Magurawalage, "Joint energy minimization and resource allocation in C-RAN with mobile cloud," *IEEE Trans. Cloud Comput.*, vol. 6, no. 3, pp. 760–770, Jul. 2018.
[29] M. Gao *et al.*, "Heterogeneous computational resource allocation for C-RAN: A contract-theoretic approach," *IEEE Trans. Services Comput.*, to be published.

Yi Zhou is currently pursuing the Ph.D. degree with the School of Engineering and Information Technologies, The University of Sydney, Australia. Her research interests include physical layer security, UAV communications, and 5G related communications. She was a recipient of the Postgraduate Scholarship and the Norman I. Price Scholarship from the Center of Excellence in Telecommunications, School of Electrical and Information Engineering, The University of Sydney.

Cunhua Pan received the B.S. and Ph.D. degrees from the School of Information Science and Engineering, Southeast University, Nanjing, China, in 2010 and 2015, respectively.

From 2015 to 2016, he was a Research Associate with the University of Kent, U.K. He held a post-doctoral position at the Queen Mary University of London, U.K., from 2016 and 2019, where he is currently a Lecturer. His research interests mainly include ultra-dense C-RAN, machine learning, UAV, the Internet of Things, and mobile edge computing. He serves as a TPC member for numerous conferences, such as ICC and GLOBECOM, and the Student Travel Grant Chair for ICC 2019. He also serves as an Editor for IEEE ACCESS.

Phee Lep Yeoh (S'08–M'12) received the B.E. degree (Hons.) and the Ph.D. degree from The University of Sydney, Australia, in 2004 and 2012, respectively. From 2008 to 2012, he was with the Telecommunications Laboratory, The University of Sydney, and the Wireless and Networking Technologies Laboratory, Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia. From 2012 to 2016, he was with the Department of Electrical and Electronic Engineering, University of Melbourne, Australia. In 2016, he joined the School of Electrical and Information Engineering, The University of Sydney. His current research interests include secure wireless communications, ultra-reliable and low-latency communications (URLLC), ultra-dense networks, and multiscale molecular communications.

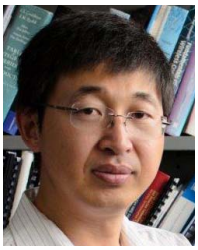
Dr Yeoh was a recipient of the 2017 Alexander von Humboldt Research Fellowship for Experienced Researchers and the 2014 Australian Research Council (ARC) Discovery Early Career Researcher Award (DECRA). He has received best paper awards at IEEE ICC 2014, IEEE VTC-Spring 2013, and AusCTW 2013 and 2019. He has served as a TPC Chair for the 2016 Australian Communications Theory Workshop (AusCTW) and a TPC member for IEEE GLOBECOM, ICC, and VTC conferences.

Kezhi Wang received the B.E. and M.E. degrees from the School of Automation, Chongqing University, China, in 2008 and 2011, respectively, and the Ph.D. degree in engineering from the University of Warwick, U.K. in 2015. He was a Senior Research Officer with the University of Essex, U.K. He is currently a Senior Lecturer with the Department of Computer and Information Sciences, Northumbria University, U.K. His research interests include wireless communication, mobile edge computing, UAV communication, and machine learning.

Maged Elkashlan received the Ph.D. degree in electrical engineering from The University of British Columbia, Canada, in 2006. From 2007 to 2011, he was with the Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia. During this time, he held visiting appointments at the University of New South Wales and the University of Technology Sydney. In 2011, he joined the School of Electronic Engineering and Computer Science, Queen Mary University of London, U.K. His research interests fall into the broad areas of communication theory and statistical signal processing.

Dr. Elkashlan received the best paper awards at the IEEE International Conference on Communications (ICC) in 2016 and 2014, the International Conference on Communications and Networking in China (CHINACOM) in 2014, and the IEEE Vehicular Technology Conference (VTC-Spring) in 2013. He currently serves as an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

Branka Vucetic is currently an ARC Laureate Fellow and the Director of the Centre of Excellence for IoT and Telecommunications, The University of Sydney. Her current work is in the areas of wireless networks and the Internet of Things. In the area of wireless networks, she explores possibilities of millimeter wave (mmWave) frequency bands. In the area of the Internet of things, she works on providing wireless connectivity for mission critical applications. She is a fellow of the Australian Academy of Science, the Australian Academy of Technological Sciences and Engineering, and the Engineers Australia.



Yonghui Li (M'04–SM'09–F'19) received the Ph.D. degree from the Beijing University of Aeronautics and Astronautics in November 2002. From 1999 to 2003, he was with Linkair Communication Inc., where he was a Project Manager with responsibility for the design of physical layer solutions for the LAS-CDMA system. Since 2003, he has been with the Centre of Excellence in Telecommunications, The University of Sydney, Australia, where he is currently a Professor with the School of Electrical and Information Engineering. His current research interests are in the area of wireless communications, with a particular focus on MIMO, millimeter wave communications, machine to machine communications, coding techniques, and cooperative communications. He holds a number of patents granted and pending in these fields.

He was a recipient of the Australian Queen Elizabeth II Fellowship in 2008 and the Australian Future Fellowship in 2012. He received the best paper awards from IEEE International Conference on Communications (ICC) 2014, IEEE PIMRC 2017, and IEEE Wireless Days Conferences (WD) 2014. He is currently an Editor for IEEE TRANSACTIONS ON COMMUNICATIONS and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He also served as a Guest Editor for several special issues of IEEE journals, such as IEEE JSAC SPECIAL ISSUE ON MILLIMETER WAVE COMMUNICATIONS.