UAV-Aided Energy-Efficient Edge Computing Networks: Security Offloading Optimization

Xiaohui Gu, Guoan Zhang, *Member, IEEE*, Mingxing Wang, Wei Duan, Miaowen Wen, *Senior Member, IEEE*, and Pin-Han Ho, *Fellow, IEEE*

***Abstract*—Unmanned aerial vehicles (UAVs) are widely applied for service provisioning in many domains, such as topographic mapping and traffic monitoring. These applications are complicated with huge computational resources and extremely low-latency requirements. However, the moderate computational capability and limited energy restrict the local data processing for the UAV. Fortunately, this impediment may be mitigated by utilizing wireless power transfer (WPT) and employing the multiaccess edge computing (MEC) paradigm for offloading demanding computational tasks from the UAV via wireless communications. Particularly, the offloaded information may become compromising by the eavesdropper (Eve) when UAVs offload the computational tasks to MEC servers. To address this issue, a UAV-MEC (UMEC) system with energy harvesting (EH) is studied, where the full-duplex protocol is considered to realize simultaneously receiving confidential data from the UAV and broadcasting the control instructions. It is worth noting that in our proposed scheme, these control instructions also serve as the artificial interference to confuse the Eve. To improve the energy efficiency for offloading, the computational communication resource allocation is optimized to minimize the energy consumption for UAV with the consumed and harvested energy. Specially, the worst case secrecy offloading rate and computation-latency constraint are considered, to further enhance the reliability and security of the proposed system. Since the objective optimization problem is nonconvex, we convert it into a convex one by analytical means. The semiclosed form expressions of the offloading time, offloading data size, and transmit power are, respectively, derived. Moreover, the conditions of nonoffloading, partial, and full offloading are also discussed from a physical perspective. With the specific conditions of activating the above-mentioned three offloading options, numerical results verify the performance of our proposed offloading strategy in various scenarios and show the superiority of our offloading strategy with the existing works in terms of the offloading capacity and energy efficiency.**

Manuscript received April 27, 2021; revised June 10, 2021 and July 13, 2021; accepted August 2, 2021. Date of publication August 9, 2021; date of current version March 7, 2022. This work was supported by the National Natural Science Foundation of China under Grant 61971245 and Grant 61801249. *(Corresponding author: Wei Duan.)*

Xiaohui Gu is with the School of Information Science and Technology, Nantong University, Nantong 226019, China, and also with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: 17110013@yjs.ntu.edu.cn).

Guoan Zhang, Mingxing Wang, and Wei Duan are with the School of Information Science and Technology, Nantong University, Nantong 226019, China (e-mail: gzhang@ntu.edu.cn; 2010310022@stmail.ntu.edu.cn; sinder@ntu.edu.cn).

Miaowen Wen is with the School of Electronics and Information, Nantong University, Nantong 226019, China, and also with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510640, China (e-mail: eemwwen@scut.edu.cn).

Pin-Han Ho is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: p4ho@uwaterloo.ca).

Digital Object Identifier 10.1109/JIOT.2021.3103391

***Index Terms*—Computation offloading, multiaccess edge computing (MEC), physical-layer security (PLS), resource allocation, unmanned aerial vehicle (UAV).**

I. Introduction

TO OVERCOME the computing and power limitations of unmanned aerial vehicles (UAVs), computationally expensive tasks generated from UAV applications can be processed by employing multiaccess edge computing (MEC) paradigm for computation offloading. On the other hand, wireless power transfer (WPT) is the promising technique to further prolong the lifetime of UAV's battery. During computation offloading, the security issues can be mitigated through the physical-layer security (PLS)-based solutions.

A. Background and Motivation

With the growth of the fifth-generation (5G) cellular systems, UAVs have found widespread use in environmental monitoring, disaster management, intelligent transportation systems (ITSs) [1], and high security military applications [2]. However, there exist some challenges relevant to the employment of UAV networks and its applications, i.e., trajectory planning, energy resources management [3], and security. In particular, the inherent disadvantages of UAVs lie in their limited computing capacities due to constraints of the weight, size, battery life, and heat dissipation. As a result, computation-intensive applications are difficult to be successfully executed, for UAVs using their local resources.

As a means of extending intelligence to the edge of the network along with higher processing and storage capabilities [4], mobile-edge computing (MEC) was introduced by the European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG) [5]. From 2017, the ETSI industry group renamed it to multiaccess edge computing, due to its benefits of providing cloud-computing capabilities at the edge of access networks, reached into Wi-Fi and fixed access technologies (e.g., fiber) [6]–[8]. Offloading computation-intensive tasks from UAVs to MEC servers have great potentials to economize on the response time, prolong the battery lifetime, and ultimately enhance the mission success. Basically, a decision on computation offloading may result in binary and partial offloading, which are related to the application model/type. For a highly integrated or relatively simple task, it should be executed as a whole being locally at the

mobile device or offloading to the MEC server, named as binary offloading. In practice, many mobile applications are composed of multiple procedures/components, making it possible to partition the program into two parts: one executed at the mobile device and the other offloaded for edge execution, so-called partial offloading. Although the former one is easier to implement, for a very large data set, the partial offloading characterized by parallel computing has advantages on reducing the latency and energy consumption on the local devices more flexibly and effectively [9].

On the other hand, WPT provides low-power mobile devices with sustainable and cost-effective energy supply by using radio-frequency (RF) signals [10]. Specifically, it facilitates a perpetual operation and enables users to have a high Quality of Experience (QoE), especially, in the case that mobile devices do not have sufficient battery energy for offloading task or supporting the service. Therefore, enabling UAVs to harvest energy from surroundings has been considered as an emerging solution, to effectively extend the operation time for energy-constrained UAVs. Moreover, if WPT technique is implemented for UAV when offloading computation tasks to MEC, the QoE of UAV will be further improved.

Despite the advantages of MEC and WPT, the security issue of UAV-ground communication has to be considered. It is known that communications between UAVs and ground users can be readily overheard by nearby malicious attackers, due to the broadcast nature of wireless transmissions. To address this issue, a viable solution of PLS techniques has been considered to perfectly protect wireless communications from eavesdroppers (Eves) attack, as long as legitimate users grasp (partial) channel state information (CSI) of Eves [11]. From the perspective of ensuring PLS, the principal design objective is to maximize the secrecy capacity [12], which is defined as the difference between the channel capacity of the main link and that of the wiretap link. If the secrecy capacity falls below 0, the transmissions from the source to the destination become insecure, and Eve would become capable of intercepting the source transmissions.

In this background, a PLS-aided energy-efficient computational offloading scheme for the UAV-MEC (UMEC) system with energy harvesting (EH) is proposed in this article. With the advantages of the full-duplex protocol, the access point (AP) plays a role of a gateway for edge nodes to receive computational tasks offloaded from the UAV, in addition to acting as a jammer to impose artificial noise (AN) to Eves. Moreover, the signals transmitted from the AP can also be harvested by the UAV in a cost-effective way. In this manner, we provide the optimal solution to the energy-efficiency problems satisfying both the offloading and security requirements to address the following three issues: 1) what is the volume of the computational tasks to be offloaded? 2) what is the suitable duration of offloading? and 3) how much power should be allocated to the offloaded signal?

B. Related Works

1) Computation Offloaded to UAVs: The new setup by utilizing a UAV equipped with an MEC server to serve a number of terminal devices, poses new opportunities to solve the challenges in communication and computation design, and several prior related works have been done for this [13]–[17]. Specifically, the work in [13] studied the Pareto-optimal solution to balance the tradeoff between UAV energy consumption and completion time, considering the energy budget of users. The power allocation for users, the computation load allocation and UAV trajectory planning for UAV were jointly optimized in [14], with the aim to maximize the ratio between overall offloaded bits and UAV energy consumption. In [15], the UAV was employed to not only power ground users but provide computing resources, and the weighted sum of UAV energy consumption for computing, powering, and flying was minimized. To further improve the Quality of Service (QoS) for users, the UAV served as not only a computing platform but also a decode-and-forward relay in [16] and [17]. In this way, the computation bits can be computed locally, offloaded to the UAV for computing or transmitted to a terrestrial AP [16] or cloud [17] via UAV relaying.

2) Computation Offloading From UAVs: Many studies have been proposed to bridge the gap between the characteristics of resource-intensive applications and limited resources on UAVs. For example, Yang *et al.* [18] considered a UAV offloading a portion of tasks to a MEC server for target tracking. They proposed a hierarchical machine learning tasks distribution framework for the UAV tracking system, where the UAV and MEC server were, respectively, embedded with lower and higher layers of the convolutional neural network (CNN) model. Messous *et al.* [19]–[21] focused on a scenario, where a set of capacity-limited UAVs has to offload computation-intensive tasks to a nearby base station (BS) via WiFi or offload to a an edge server via cellular links. They formulated the offloading problem as a noncooperative theoretical game with N players as UAVs and three pure strategies as local computing, offloading to the BS or edge server, and the objective was to minimized the system utility in terms of energy consumption and task experienced delay. The Nash equilibrium point was finally, derived in [21], for the best possible tradeoff between energy consumption, delay, and computation cost. Recently, Liu *et al.* [22] studied a UAV-edge–cloud computing system, where the UAV with limited onboard resources offloaded partial computation bits to edge servers or cloud for processing, with the help of neighboring UAVs. However, the above-mentioned works focused on the achievable energy efficiency through resources allocation and offloading decision optimization, while the security issues was not covered.

3) WPT in UAV-Ground Communications: For UAV relay networks, the power splitting (PS) scheme was applied to simultaneously perform EH and information decoding, and the UAV as an aerial mobile relay could be powered with WPT [23], [24] to prolong the battery lifetime and extend the working period in the air. Specially, multiple UAV relays with WPT were selected to minimize the end-to-end outage probability [25] or maximize the secrecy capacity [26]. For the UAV-assisted MEC networks investigated in [15] and [27]–[29], UAVs were employed as edge servers for processing computational bits offloaded from terrestrial users, and simultaneously

acted as energy sources for powering users. With the perspective of improving QoE for UAV, we enable the UAV to harvest energy from connected AP during the computation offloading duration.

4) Security of UAV Communication Links: Compared to terrestrial wireless communication systems, it requires fewer efforts for Eves to attack the UAV air-to-ground communications, which brings great security challenges. Recently, many works have enabled the UAV serving as a helper node to impose jamming noise on the Eve, to improve the PLS of legitimate communication links. For example, [30] and [31] deployed a cooperative UAV imposing jamming signals on Eves on the ground, when other UAVs transmitted confidential signals to ground users. In [32], one UAV with the best CSI was selected from multiple UAV relay nodes, and others were operated as jammers. The secure UMEC system was studied in [33], where the UAV can access multiple ground BSs to offload partial computation bits. The total energy consumption for local computation, communication transmission, and flight propulsion was minimized in [33], via jointly optimizing UAV trajectory, computation task allocation, BSs selection, and transmit power allocation. Different from [33] and to further improve the system performance, we conceive the terrestrial AP to help improve the PLS for UAV, through imposing AN on Eve, besides, the jamming noise is simultaneously harvested by the UAV to prolong the service time.

C. Contributions and Organizations

This work designs the energy-efficient computation offloading scheme for UAV with EH, while the communication security is simultaneously guaranteed. The main contributions of our works are summarized as follows.

1) A novel secure and energy-efficient computational offloading model is investigated, in which the secrecy of UAV computational offloading is enhanced by the AP imposing AN on Eve, and the energy limitation problem for the UAV is simultaneously mitigated by the harvesting energy from AP.
2) Considering both situations that the UAV's battery is *draining* or *charging*, and to prolong the UAV's service time, the gap between the consumed and harvested energy is minimized, subject to the worst secure offloading rate constraint and latency constraint under the partial offloading mode. The formulated problem can be effectively converted into a convex one with a single variable. The semiclosed-form expressions for the optimal transmit power, offloading time, as well as offloading data size for UAV are rigorously derived.
3) The optimized offloading options, i.e., the UAV offloading without computational bits, or a fraction of the task loads, alternatively all task loads, respectively, referring to nonoffloading, partial, and full offloading, are performed according to various communications and computation conditions. We discuss the corresponding conditions for above described decisions from a physical perspective.
4) The numerical results show that the computation performance obtained by the proposed resource allocation scheme is better than that of the ones achieved by nonoffloading, full offloading, and partial offloading without AN schemes. Moreover, we quantify the maximum offloading load for our proposed offloading scheme, with the certain volume of computational loads in diverse communication conditions.

The remainder of this article is organized as follows. Section II presents the system model. Section III formulates the resource allocation problem under the partial offloading mode, accompanied by the analysis of binary offloading conditions. In Section IV, simulation results and discussions are presented. Finally, Section V concludes this article.

II. System Model

A UMEC system is considered in Fig. 1, where a single-antenna is implemented in the UAV and capable of offloading computational tasks to MEC servers. The UAV accesses the AP on the ground through wireless transmission links, which can be overheard by the Eve on the ground. Based on the full-duplex protocol, the AP simultaneously communicates with the UAV and imposes AN on the Eve, to protect the UAV from interception.

Without loss of generality, the different locations of UAV are considered. The solid lines in Fig. 1 illustrate that the UAV is close to AP but far away from Eve, in this case, the UAV is less likely to be overheard, and more energy can be harvested from AP. On the other hand, the dashed lines denote that the UAV locates far away from AP but near Eve, in this case, to improve the security performance, more transmit power should be considered for offloading.

A. Computing Model

In this article, we focus on data partitioned oriented applications. For such applications, the input data are known beforehand and can be arbitrarily partitioned for parallel processing due to the bitwise independence. Particularly, the application is abstracted into a profile with two parameters, i.e., (L, T) [34], where L and T represent the amount of computation input data bits and the application-dependent latency requirement, respectively. Denoting ℓ as the offloading data size, and letting C_U as task complexity (the number of CPU cycles required to compute each bit of input data), the latency and energy consumption for the local computing at the UAV or offloading to the edge can be, respectively, defined as follows.

1) Local Computing: Denote D_U as the computing capacity (i.e., the clock frequency of CPU chip) of UAV. The local computing time T_{loc} consumed by the UAV processing $(L-\ell)$ bits is given by

$$T_{\text{loc}} = \frac{C_U(L-\ell)}{D_U} \tag{1}$$

meanwhile that the energy consumption for local computing E_{loc} is given by

$$E_{\text{loc}} = C_U P_U (L-\ell) \tag{2}$$

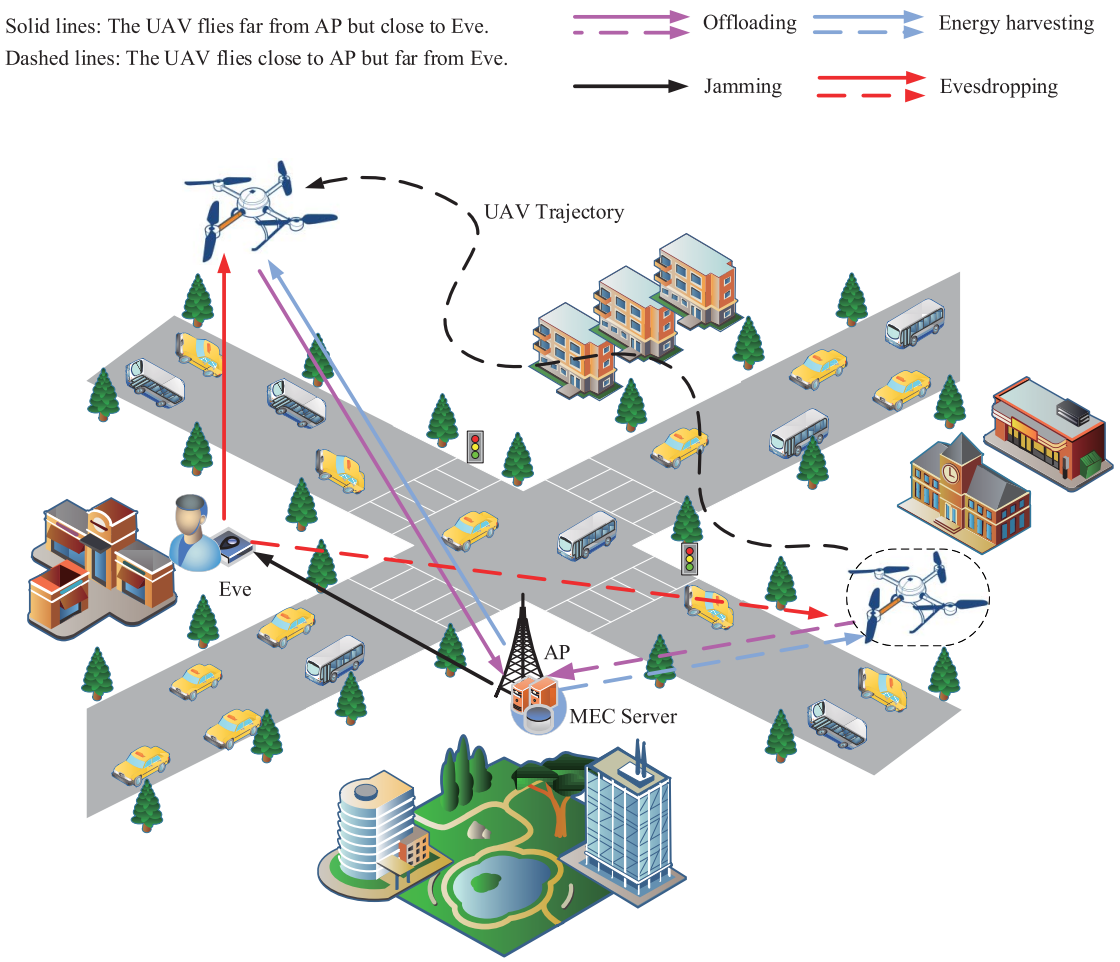


Fig. 1. Proposed UAV-aided energy-efficient edge computing system.

where P_U denotes the energy consumption for UAV running each CPU cycle.

2) Edge Computing: When ℓ bits data are offloaded to MEC, the offloading time duration T_{up} for the UAV can be obtained from

$$T_{\text{up}} = \frac{\ell}{\mathcal{R}_{UA}(P_t)} \tag{3}$$

where $\mathcal{R}_{UA}$ in bits-per-second (b/s) denotes the offloading rate from the UAV to AP for computing, and $\mathcal{R}_{UA}(P_t)$ represents the offloading rate as function of transmit power P_t. In addition, the energy consumption for UAV secure offloading E_{off} can be written as

$$E_{\text{off}} = P_t T_{\text{up}}. \tag{4}$$

In those works studying UAV-assisted edge computing networks, i.e., [13]–[17], the time and energy for remote computing at the MEC server and downloading computational results from the AP have been ignored, since that MEC servers are usually with powerful computing capacity, and the data size of results is relatively smaller than that of the input data. In this article, we investigate the partial offloading problem for data partitioned oriented applications with large task size and high computation complexity. Subjecting to the computing capacity and computation-latency constraints, the UAV can offload a portion of tasks to the MEC server for processing, while the other part will be executed by local computing. Besides, the AP/BS is powerful for forwarding results back; therefore, the downloading time will be much smaller compared with the offloading time. In other words, the offloading time domains the transmission time in the whole process of computation offloading. Therefore, in this article, negligible time duration for downloading the computed results is acceptable and considered.

Finally, the consumed energy consumption E_c for the UAV completing its computational tasks can be presented as

$$E_c = E_{\text{loc}} + E_{\text{off}} = C_U P_U (L - \ell) + P_t T_{\text{up}}. \tag{5}$$

B. Communication Models

Actually, due to the short-term data transmission and latency constraint, we assume the UAV hovering at a certain altitude to perform task offloading. Moreover, for the efficient and stable EH, it would be beneficial if the UAV keeps stationary during WPT. Optimizing the trajectory for UAV to further improve the system efficiency is left for our future work. Similar to [33], considering that the channel between the AP and UAV, denoted by h_{UA}, is the LoS path, yielding

$$h_{UA} = \rho_0 d_0^{-\eta_0} \tag{6}$$

where d_0 denotes the hovering altitude of UAV, ρ_0 represents channel power gain at the reference distance of $d_{\text{ref}} = 1$ m and η_0 is the path-loss exponent of LoS. Denoting $P_t \geq 0$ as the transmit power for task offloading, and B as the bandwidth of the channel, the data rate (b/s) of uplink transmission can be represented as

$$\mathcal{R}_{UA}(P_t) = B\log_2\left(1 + \frac{P_t h_{UA}}{\sigma^2}\right) \tag{7}$$

where σ is the variance of the independent and identically distributed (i.i.d.) additive white Gaussian noise (AWGN) with zero mean.

Furthermore, denote $\tilde{h}_{UE}$ as the channel between UAV and Eve, and $\tilde{h}_{AE}$ as the channel between AP and Eve, respectively. We assume that the AP perfectly knows the CSI of h_{UA} and computation profiles of the UAV. In practice, the CSI of $\tilde{h}_{UE}$ and $\tilde{h}_{AE}$ cannot be perfectly estimated.[1] Moreover, the uncertainty of $\tilde{h}_{UE}$ and $\tilde{h}_{AE}$ makes it challenging to obtain a mathematically tractable expression of secrecy capacity.

To achieve robust transmission with imperfect CSI, this article adopts the CSI uncertainty model [35], in which the CSI errors are assumed to be within a bounded set. Specifically, we consider the deterministic CSI uncertainty model for $\tilde{h}_{UE}$ and $\tilde{h}_{AE}$, respectively, where $|\tilde{h}_{UE} - h_{UE}| \leq \varepsilon$ and $|\tilde{h}_{AE} - h_{AE}| \leq \delta$ with $\tilde{h}_{UE}$ and $\tilde{h}_{AE}$ as the estimated CSI of $\tilde{h}_{UE}$ and $\tilde{h}_{AE}$, respectively, and ε and δ as the estimated error. Therefore, the estimated channel can be, respectively, expressed as

$$h_{UE} = \rho_1 d_1^{-\eta_1} \tag{8}$$

$$h_{AE} = \rho_2 d_2^{-\eta_2}\zeta \tag{9}$$

where d_1 represents the distance between UAV and Eve, and d_2 is the distance between AP and Eve, respectively, while ρ_1 and ρ_2 denote the channel power gain at the reference distance of $d_{\text{ref}} = 1$ m, η_1 and η_2 represent the path-loss exponent of the LoS and NLoS paths, ζ stands for the small-scale fading envelope, which is assumed to be i.i.d. Rayleigh fading with zero mean and unit variance [36].

In this article, we consider a simple jamming model, where the AP with an omnidirectional antenna imposes the artificial/jamming noise $P_J\tilde{h}_{AE}$ on the Eve with P_J as the jamming power. Therefore, the data rate (b/s) at Eve for overhearing the UAV offloading channel can be written as

$$\mathcal{R}_{UE} = B\log_2\left(1 + \frac{P_t\tilde{h}_{UE}}{P_J\tilde{h}_{AE} + \sigma^2}\right) \tag{10}$$

where B represents the bandwidth of the channel and P_J is the jamming power of AP.

C. EH Model

As those works [15] and [24]–[28] investigating UAV-assisted communications, we assume an ideal linear EH model for a tractable optimization and analysis; nonlinear EH models can be incorporated with respect to the realistic performance in a certain region, which is beyond our scope in this article and is reserved as a future study. Under the linear EH model, the RF-to-direct current (DC) energy conversion efficiency λ is a constant. Accordingly, the harvested energy at the UAV is defined as

$$E_h = \lambda T_{\text{up}} P_J h_{UA} \tag{11}$$

where $\lambda \in (0, 1]$ denotes the energy conversion efficiency, P_J is the transmit power of AP, h_{UA} denotes the channel gain between UAV and AP, and T_{up} is the offloading time duration. The physical meaning of (11) is the jamming power transmitted by the AP during the offloading time duration, which can be harvested by the UAV.

D. Secure-Communication Model

Under the CSI uncertainty model, we consider the Eve's channel gain that results in the worst-case achievable secrecy capacity (b/s), which is given by

$$\mathcal{R}_{\text{sec}}(P_t) = [\mathcal{R}_{UA}(P_t) - \max \mathcal{R}_{UE}(P_t)]^+ \tag{12}$$

$$= \left[\mathcal{R}_{UA}(P_t) - \mathcal{R}_{UE}^{ub}\right]^+ \tag{13}$$

where $[x]^+ \triangleq \max(x, 0)$, and the upper bound of $\mathcal{R}_{UE}$ denoted by $\mathcal{R}_{UE}^{ub}$ can be written as

$$\mathcal{R}_{UE}^{ub} = B\log_2\left(1 + \frac{P_t\tilde{h}_{UE}^{\max}}{P_J h_{AE}^{\min} + \sigma^2}\right). \tag{14}$$

With the maximum estimation error ε and δ, $\tilde{h}_{UE}^{\max}$ and $\tilde{h}_{AE}^{\min}$ can be, respectively, obtained as

$$\tilde{h}_{UE}^{\max} = h_{UE}(1 + \varepsilon) \tag{15}$$

$$\tilde{h}_{AE}^{\min} = h_{AE}(1 - \delta). \tag{16}$$

One can observe from (12) that there exists a threshold value of P_{J}^{th}, as $\mathcal{R}_{\text{sec}}(P_t) > 0$

$$P_{\text{J}}^{\text{th}} = \frac{\sigma^2}{h_{AE}}\left(\frac{\tilde{h}_{UE}^{\max}}{\tilde{h}_{AE}^{\min} - 1}\right). \tag{17}$$

From (17), it is clear that the value of P_J is highly related to the channel conditions of h_{UA} and h_{UE} with LoS characteristics. Therefore, the jamming power transmitted by AP can be mainly determined by the distance form UAV to AP and Eve.

III. Joint Optimization of the Communication and Computation Resources

In this section, the computational offloading scheme will be determined. Since we aim to obtain an energy-efficient and secure offloading scheme for the UAV intercepted by an Eve in the secure UMEC system, the corresponding optimization problem is first provided, and then converted into a convex problem with a single-one variable analytically. Finally, the optimal solution under different communication conditions and computing profiles is effectively obtained.

[1]For cases that the Eve is active or passive, the UAV and AP can detect Eve's potential transmission to estimate the corresponding $\tilde{h}_{UE}$ and $\tilde{h}_{AE}$, from Eve's active transmission or Eve's local oscillator power leaked from its RF front end. In this way, the UAV and AP can eventually obtain partial information of $\tilde{h}_{UE}$ and $\tilde{h}_{AE}$.

A. Optimization Formulation

1) Constraints:

a) Latency constraint: Under the partial offloading model, local computing and computation offloading process simultaneously. With this assumption, the local computing time and computation offloading time should be lower than the maximum tolerable latency T, i.e., $T_{\text{loc}} \leq T$ and $T_{\text{up}} \leq T$.

b) Secrecy constraint: To make sure that the offloaded data are not overheard by Eve, the secure offloading rate should satisfy the constraint of $\mathcal{R}_{\text{sec}}(P_t) \geq (\ell/T_{\text{up}})$.

c) Offloaded data volume constraint: $0 \leq \ell \leq L$.

d) Power consumption constraint: $0 \leq P_t \leq P_t^{\max}$.

2) Problem Formulation: The gap between the consumption and conservation of the energy E_τ is defined as

$$E_\tau = E_c - E_h \tag{18}$$

$$= C_U P_U (L - \ell) + P_t T_{\text{up}} - \lambda T_{\text{up}} P_J h_{UA}. \tag{19}$$

Here, we consider two types of energy: 1) the consumed energy E_c for completing tasks and anti-eavesdropping and 2) the harvested energy E_h from AP. Clearly, when the value of E_τ is nonnegative, the battery of UAV is *draining*; otherwise, the harvested energy is larger than the consumed energy, leading to a *charging* battery. In the former case, the AP should enlarge its transmit power for the purpose of jamming Eve and prolonging UAV's battery life.

Our goal is to minimize the energy consumption and maximize the energy storage of the UAV by jointly optimizing offloading data size ℓ, offloading time duration T_{up}, and transmit power P_t, subject to above constraints. The secure computation offloading problem can be formulated as

$$\begin{aligned} \mathcal{Q}1: \min_{l, T_{\text{up}}, P_t} \quad & C_U P_U (L - \ell) + P_t T_{\text{up}} - \lambda T_{\text{up}} P_J h_{UA} \\ \text{s.t.} \quad & C1: T_{\text{loc}} \leq T \\ & C2: T_{\text{up}} \leq T \\ & C3: \mathcal{R}_{\text{sec}}(P_t) \geq \frac{\ell}{T_{\text{up}}} \\ & C4: 0 \leq \ell \leq L \\ & C5: 0 \leq P_t \leq P_t^{\max}. \end{aligned} \tag{20}$$

Without loss of generality, two situations corresponding to the positive and negative values of E_τ are both considered in problem $\mathcal{Q}1$, which are detailed as follows.

- Case 1: The value of consumed energy E_c is larger than that of the harvested energy E_h, resulting in a positive value of the objective function in $\mathcal{Q}1$. In this case, the battery of UAV is *draining*, and the purpose of problem $\mathcal{Q}1$ is to minimize the total energy consumption;
- Case 2: The value of harvested energy E_h is larger than that of the consumed energy E_c, corresponding to the negative value of E_τ. In this situation, the UAV's battery is *charging*, and we should maximize the energy stored in UAV's battery, i.e., $\max |E_c - E_h|$. Therefore, with the negative value of E_τ, we have

$$\max |E_c - E_h| \Rightarrow \min E_c - E_h. \tag{21}$$

Hence, the energy storage maximization can also be achieved by problem $\mathcal{Q}1$.

After all, the objective of problem $\mathcal{Q}1$ is to prolong the service time of UAV, through jointly optimizing resources allocation and EH.

By substituting (3) and (7) into (19), E_τ can be re-expressed as

$$E_\tau(\ell, P_t) = \frac{\ell(P_t - \lambda P_J h_{UA})}{B \log_2\left(1 + \frac{P_t h_{UA}}{\sigma^2}\right)} + C_U P_U (L - \ell) \tag{22}$$

which is a function with $\ell \geq 0$ and $P_t \geq 0$. Clearly, (22) is a linear function with respect to ℓ, and its Hessian matrix is given as

$$\nabla^2 E_\tau(\ell, P_t) = \begin{bmatrix} \frac{\partial E_\tau}{\partial \ell^2} & \frac{\partial E_\tau}{\partial \ell \partial P_t} \\ \frac{\partial E_\tau}{\partial P_t \partial \ell} & \frac{\partial E_\tau}{\partial P_t^2} \end{bmatrix} = -\left(\frac{\partial E_\tau}{\partial \ell \partial P_t}\right)^2 \leq 0. \tag{23}$$

Then, the function $E_\tau(\ell, P_t)$ is characterized by a negative semidefinite Hessian matrix. Therefore, the objective function in $\mathcal{Q}1$ is nonconvex [37, Ch. 3].

Moreover, constraint C1 jointly connects the offloading data size ℓ and maximum tolerable latency T, while constraints C2 and C3 are coupled by the variable T_{up} with the upper bound as T. As a result, the nonconvex problem $\mathcal{Q}1$ is difficult to be solved directly. In what follows, we first convert the formulated problem into a more tractable one and then derive the optimal solution.

B. Problem Transformation

Assertion 1: It is certain, when the objective function of $\mathcal{Q}1$ achieves the minimum, the constraint C3 would be tightened from

$$\mathcal{R}_{\text{sec}}(P_t) = \frac{\ell}{T_{\text{up}}}. \tag{24}$$

Proof: With our assumption that the SNR at AP is higher than that of the one at Eve, both the objective function and secrecy capacity $\mathcal{R}_{\text{sec}}(P_t)$ in (12) are monotonically increasing with P_t. Assume that $(\ell^*, T_{\text{up}}^*, P_t^*)$ are the optimal solutions of $\mathcal{Q}1$ with the relaxed constraint C3. Clearly, with a decreased P_t^*, and considering other constraints established in $\mathcal{Q}1$, the objective function will accordingly decrease. This contradicts the assumption that $(\ell^*, T_{\text{up}}^*, P_t^*)$ are the optimal solutions. Hence, for $\mathcal{Q}1$ with binding constraint (24), constraint (24) should be active in an optimum form. ■

Lemma 1: Given the offloading data size ℓ, the offloading time duration yields $T_{\text{up}}^* = T$ for the optimal solution to Problem $\mathcal{Q}1$.

Proof: See Appendix A. ■

As a result, $\mathcal{Q}1$ can be equivalently converted into the following problem:

$$\begin{aligned} \mathcal{Q}2: \min_{\ell} \quad & C_U P_U (L - \ell) + \frac{\left(1 - 2^{-\frac{\ell}{BT}}\right) T}{\gamma_{UA} 2^{-\frac{\ell}{BT}} - \gamma_{UE}} - \lambda T P_J h_{UA} \\ \text{s.t.} \quad & C6: L - \frac{T D_U}{C_U} \leq l \\ & C7: \ell \leq -BT \log_2\left(\frac{1 + P_t^{\max} \gamma_{UE}}{1 + P_t^{\max} \gamma_{UA}}\right) \\ & \text{and C4.} \end{aligned} \tag{25}$$

In $\mathcal{Q}2$, constraints C6 and C7 correspond to constraints C1 and C3, respectively.

Assertion 2: Problem $\mathcal{Q}2$ is a convex problem.

Proof: Letting $\phi_1(\ell)$ and $\phi_2(\ell)$ denote the first-order and the second-order derivatives of the objective function of $\mathcal{Q}2$, we have

$$\phi_1(\ell) = -C_U P_U + \frac{\ln 2(\gamma_{UA} - \gamma_{UE})2^{-\frac{\ell}{BT}}}{B\left(\gamma_{UA}2^{-\frac{\ell}{BT}} - \gamma_{UE}\right)^2} \tag{26}$$

and

$$\phi_2(\ell) = \frac{(\ln 2)^2 2^{-\frac{\ell}{BT}}(\gamma_{UA} - \gamma_{UE})\left(\gamma_{UA}2^{-\frac{\ell}{BT}} - \gamma_{UE}\right)}{B^2 T\left(\gamma_{UA}2^{-\frac{\ell}{BT}} - \gamma_{UE}\right)^3}. \tag{27}$$

From (27), the second-order derivative of the objective function of $\mathcal{Q}2$ is nonnegative, concluding that the objective function of $\mathcal{Q}2$ is convex. In addition, constraints C4, C6, and C7 are all linear with respect to ℓ. This completes the proof. ∎

Let $\ell \in [\ell_{\min}, \ell_{\max}]$ denote the feasible set of ℓ, where $\ell_{\min} = \max\{0, L - (TD_U/C_U)\}$ is determined by the latency constraint and UAV's computing capacity, $\ell_{\max} = \min\{L, OL_{\max}\}$ is determined by secure offloading rate and transmit power associated with constraints C4, C6, and C7. The maximum secure offloading load $OL_{\max}$ is given by

$$OL_{\max} = -BT\log_2\left(\frac{1 + P_t^{\max}\gamma_{UE}}{1 + P_t^{\max}\gamma_{UA}}\right). \tag{28}$$

Lemma 2: The optimal solution to $\mathcal{Q}2$ is given by

$$\ell^* = \begin{cases} \ell_{\min}, & \text{if } \hat{\ell} < \ell_{\min} \\ \hat{\ell}, & \text{if } \ell_{\min} \le \hat{\ell} \le \ell_{\max} \\ \ell_{\max}, & \text{if } \ell_{\max} < \hat{\ell} \end{cases} \tag{29}$$

where $\hat{\ell}$ denotes the root of equation $\phi_1(\ell) = 0$.

Proof: See Appendix B. ∎

C. Optimal Offloading Strategy for the Secure UMEC

As illustrated in the above section, the formulated problem $\mathcal{Q}1$ is mathematically converted into a convex problem and, hence, there exists an optimal solution to the objective problem. The optimal offloading strategy for the secure UMEC is summarized as follows.

1) *Offloading Time Duration:* According to Lemma 1, the optimal offloading time duration is $T_{\text{up}}^* = T$.
2) *Offloading Data Size:* According to Lemma 2, the optimal offloading data volume ℓ^* is given by

$$\ell^* = \begin{cases} \ell_{\min}, & \text{if } \hat{\ell} < \ell_{\min} \\ \hat{\ell}, & \text{if } \ell_{\min} \le \hat{\ell} \le \ell_{\max} \\ \ell_{\max}, & \text{if } \ell_{\max} < \hat{\ell}. \end{cases} \tag{30}$$

3) *Transmit Power:* The optimal transmit power P_t^* can be determined from (34), by substituting the values of P_J, T_{up}^*, and ℓ^*.

The proposed algorithm to obtain the optimal offloading strategy is shown in Algorithm 1. Benefiting from our semiclosed forms of optimal solutions, the computational complexity of Algorithm 1 is determined by the bisection algorithm, with the maximal complexity of $\mathcal{O}(\log L)$.

Algorithm 1 Proposed Algorithm for Secure Offloading

Input:
$\{L, C_U, T\}$: task profile;
$\{d_0, d_1, d_2\}$: distances;
$\{P_U, P_t^{\max}\}$: UAV capacity;
$\{\epsilon, \delta\}$: maximum estimation error;
σ: an infinitesimal number;
Output:
$\{T_{\text{up}}^*, l^*, P_t^*\}$: optimal offloading strategy;

```
/*Offloading time duration*/
T*_up = T;
Initialize:
a ← 0, b ← L, x_0 ← (a + b)/2, iteration index k ← 1;
/*Solving φ_1 = 0 with the bisection method*/
if φ_1(x_0) = 0 then
    l̂ = x_0;
else
    while |x_0(k + 1) − x_0(k)| < σ do
        if φ_1(x_0) * φ_1(b) < 0 then
            a = x_0;
        else
            b = x_0;
        end if
        x_0(k + 1) = (a + b)/2;
        k = k + 1;
    end while
    l̂ = x_0;
end if
/*Offloading data size */
if l̂ < l_min then
    l* = l_min;
else
    if l_max < l̂ then
        l* = l_max;
    else
        l* = l̂;
    end if
end if
/*Transmit power*/
Calculate P*_t by Eq. (34);
```

D. Special Cases of Full Offloading and Nonoffloading

In this section, we analyze the special cases of the optimization problem $\mathcal{Q}2$, to determine under what condition binary decisions of full offloading or nonoffloading should be performed.

1) Optimality of Full Offloading: First, we investigate the conditions where the energy gap E_τ can be minimized by offloading all task bits to the MEC server, i.e., $\ell^* = L$. The condition is twofold: 1) $\ell^* = L$ should be feasible and 2) $\phi_1(\ell) \le 0\ \forall \ell_{\min} \le \ell \le \ell_{\max}$.

The first condition holds when the UAV is capable of offloading ℓ bits to AP without violating latency and specific security constraints, i.e., $P_t(L)T \ge L$ and $OL_{\max} \ge L$.

Then, recalling the definition of $\phi_1(\ell)$ in (26), the sufficient condition 2) indicates that the average energy consumption per

TABLE I
OPTIMAL OFFLOADING DECISIONS

Energy-efficiency \ Latency	$\frac{C_U L}{D_U} \leq T$	$P_t(L)T \geq L \ \& \ OL_{\max} \geq L$	$\frac{C_U(L-\ell)}{D_U} \leq T \ \& \ P_t(\ell)T \leq \ell \ \& \ OL_{\max} \geq l$
$C_U P_U \leq P_t(1)T$	Non-offloading	-	-
$\frac{P_t(L)T}{L} \leq \frac{C_U P_U + P_t(L-1)T}{L}$	-	Full offloading	-
$P_t(1)T < C_U P_U < P_t(L)T - P_t(L-1)T$	-	-	Partial offloading

TABLE II
DEFAULT SIMULATION PARAMETERS

Description	Parameter and Value
UAV hovering altitude [38]	$d_0 \in [100, 500]$m, $d_1 \in [100, 500]$m
The location of Eve [36]	$d_2 \in [0, 200]$m
UAV-to-ground channel [39]	$\rho_0 = \rho_1 = 1.42 \times 10^{-4}$ $\eta_0 = \eta_1 = 2$
AP-to-Eve channel [39]	$\rho_2 = 1.42 \times 10^{-4}$, $\eta_2 = 3.5$
Transmission bandwidth [40]	$B = 1$MHz
Noise power [39]	$\sigma^2 = 1.99 \times 10^{-10}$mW
Task profile [41, 42]	$L \in [0, 2]$Mbits $C_U = [500, 1500]$cycles/bit
Temporal constraint	$T = [0.4, 0.8]$s
Energy conversion efficiency [27]	$\lambda = 0.9$
UAV capacity [41]	$D_U = 2.0$GHz $P_U = [0, 10 \times 10^{-12}]$J/cycle $P_t^{\max} \in [0.1, 1.0]$mW
Jamming power [39]	$P_J \in [0, 3.5]$mW
Maximum estimation error [40]	$\varepsilon = 0.1$, $\delta = 0.1$

bit for full offloading is lower than that of the combination of offloading $(L-1)$ bits and locally computing a bit

$$\frac{P_t(L)T}{L} \leq \frac{C_U P_U + P_t(L-1)T}{L} \tag{31}$$

where $P_t(\cdot)$ can be obtained from (34).

2) Optimality of Nonoffloading: Then, we turn to provide the necessary conditions under which $\ell^* = 0$ can be obtained. These conditions are twofold: 1) $\ell^* = 0$ should be feasible and 2) $\phi_1(\ell) > 0 \ \forall \ell_{\min} \leq \ell \leq \ell_{\max}$.

The first condition holds when the UAV is capable of executing all computational bits under the latency constraint, i.e., $(C_U L/D_U) \leq T$.

The sufficient condition 2) indicates that the energy consumption of computing a bit at the UAV is lower than that of offloading a bit, i.e.,

$$C_U P_U \leq P_t(1)T. \tag{32}$$

To summarize results of the above sections, offloading decisions are listed in Table I, in different energy efficiency and latency situations.

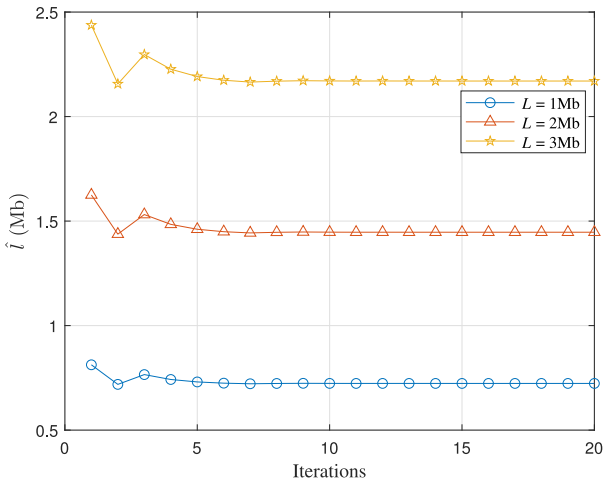


Fig. 2. Convergence of the proposed algorithm.

IV. NUMERICAL RESULTS

In this section, we first evaluate the convergence of the proposed algorithm by numerical analysis. Then, numerical results are provided to evaluate the performance of our proposed *secure partial offloading* scheme in different scenarios, and the corresponding system performance are compared with three benchmark schemes. According to some related works about computation offloading in the context of MEC, simulation settings are summarized in Table II.

A. Nonoffloading

The UAV chooses to compute all computational bits locally. The energy gap E_τ can be obtained by solving problem $\mathcal{Q}1$ with default $\alpha = 0$ and $P_J = 0$.

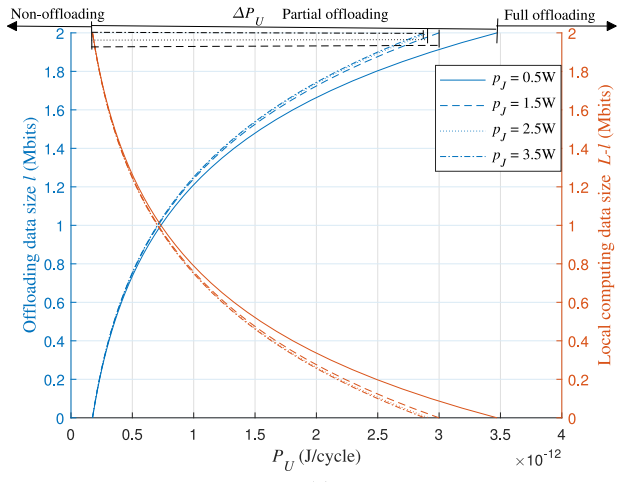
B. Secure Full Offloading

The UAV decides to offload its computational task to AP. In this case, the WPT is not considered, and the energy gap E_τ can be obtained by solving Problem $\mathcal{Q}1$ with $\alpha = 1$.

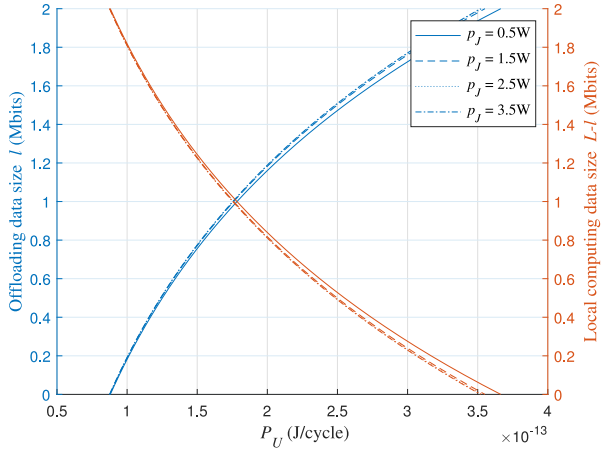
C. Secure Partial Offloading w/o AN [33]

To make a fair comparison, the UAV flight-propulsion energy, as well as trajectory optimization, was not considered, and the subsequent UAV energy consumption minimization corresponds to solving problem $\mathcal{Q}1$ with $P_J = 0$.

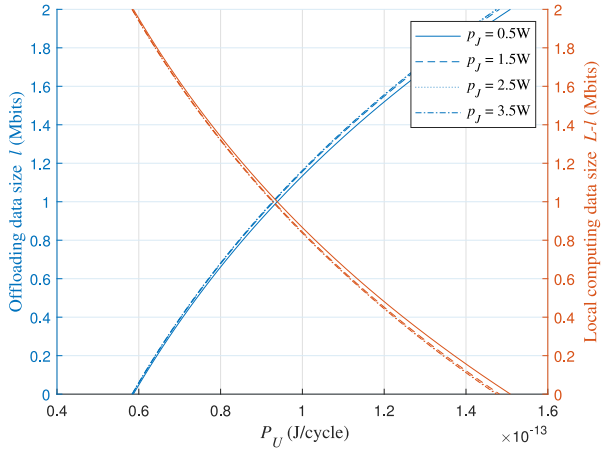
We illustrate the convergence of the proposed algorithm in Fig. 2. It is observed that the root $\hat{l}$ of equation $\phi_1 = 0$ can



(a)



(b)



(c)

Fig. 3. Offloaded data size ℓ and locally computed data size $L - \ell$ versus the energy consumption of UAV for each CPU cycle P_U. ($L = 2$ Mbits; $d_0 = d_1 = 300$ m; $d_2 = 50$ m.) (a) $C = 500$ cycles/bit. (b) $C = 1000$ cycles/bit. (c) $C = 1500$ cycles/bit.

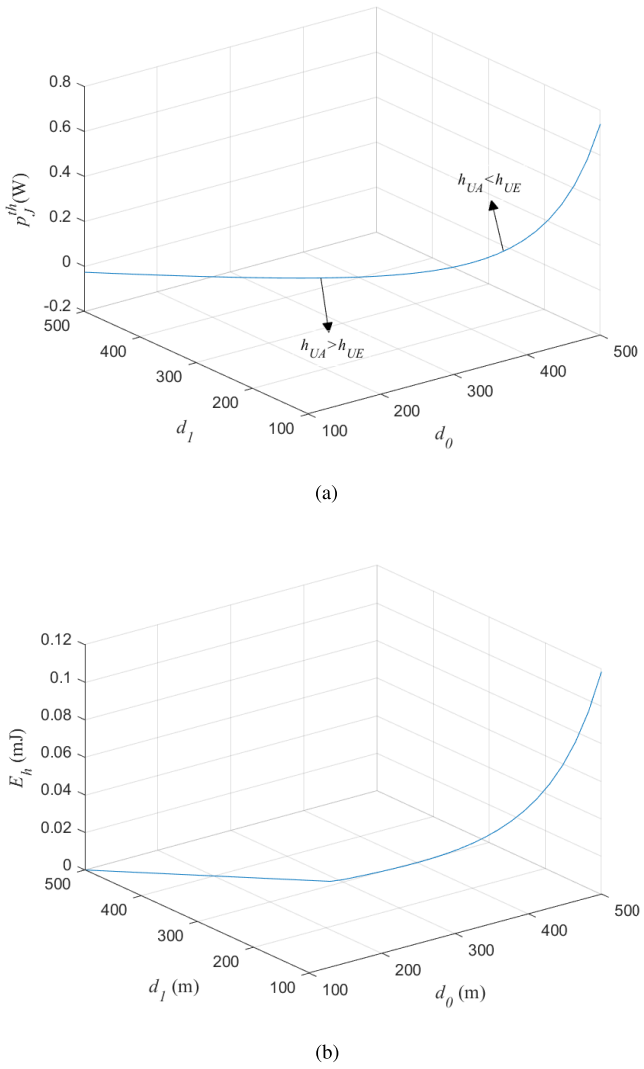
be obtained after several iterations, verifying the efficiency of our proposed algorithm. Note that once $\hat{l}$ is determined, the optimal offloading strategy can be found mathematically.

We assume the data size of computational task is equal to the one that can be computed by the UAV, within the maximum tolerable latency. Fig. 3 depicts the numerical results of the proposed offloading scheme under various values of P_U, as well as AN power P_J. From Fig. 3, we have the following observations.

1) Nonoffloading (i.e., $l = 0$) is performed when the value of P_U is small. In this case, the UAV locally computing a bit consumes less energy than the UAV offloading a bit to MEC. As the value of P_U increases, offloading is becoming more energy efficient; thus, the UAV starts uploading the computational bits to the edge node (i.e., $0 < \ell < L$) until all of which are offloaded (i.e., $l = L$).
2) The cut-off value of P_U [denoted by ΔP_U in Fig. 3(a)] for nonoffloading and full offloading decreases as P_J grows. Since increasing jamming power results in reduced transmit power, for the UAV achieving the same secrecy capacity. Moreover, the curves corresponding to different task complexity show that the cut-off values in the scenario with $P_J = 3.5$ W is smaller than that in scenarios with $P_J = 2.5$ W, $P_J = 1.5$ W, and $P_J = 0.5$ W. Because the offloading security is mainly limited by the jamming power (jamming-power-limited) when P_J is of a small value, in other words, a slight increase in jamming power will lead to a well improvement in secrecy capacity.
3) Finally, the increase in C results in a smaller value of P_U. For the reason that the UAV has to lower transmit power to achieve the same energy efficiency of computational offloading and local computing, when the task characterizes higher complexity. In addition, the cut-off value decreases as C grows, because the energy consumption for local computing is mainly determined by the task complexity and assigned workload. As the task characterizes higher complexity, the value of P_U should slow down to achieve the same energy efficiency gap between nonoffloading and full offloading, i.e., $\Delta P_U = ([P_t(L)T - P_t(L-1)T - P_t(1)T]/C)$.

The numerical values of $P_{\mathrm{J}}^{\mathrm{th}}$ and the lower bound of harvested energy are illustrated in Fig. 4. It is shown that the channel gain of h_{UA} is better than that of h_{UE} for $d_0 \leq d_1$, thus, UAV is capable of anti-eavesdropping by itself. Meanwhile, there is not any energy that can be harvested from the jamming power for the UAV. Therefore, to extend the working period in the air, the AP should transmit power for WPT of UAV until it is fully charged. On the other hand, in the case $d_0 > d_1$, the security of the offloading channel should be performed by the AP imposing AN on Eve. In this case, the transmit power from AP can be simultaneously harvested by the UAV.

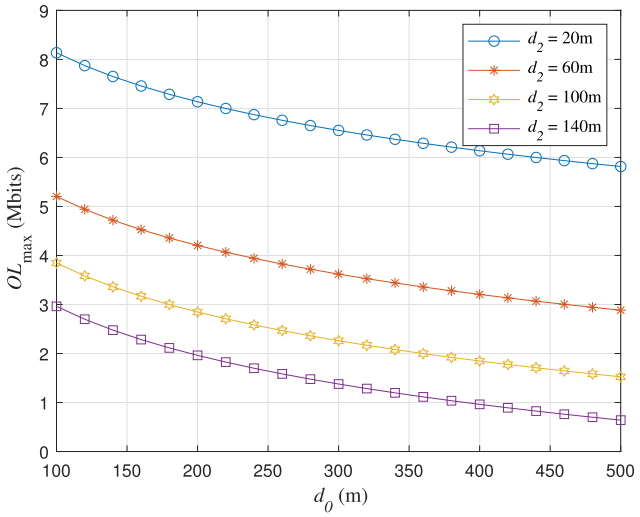
Versus the different UAV's hovering altitude d_0 and distance from UAV to Eve d_2, we characterize the performance of our proposed offloading scheme in Fig. 5, in terms of the maximum achievable offloading load $OL_{\max}$ and consumed energy E_c. It is clear that $OL_{\max}$ and E_c own the opposite growth trend, since the increase of UAV's altitude results in higher path loss between UAV and AP on the ground, which further leads to reduced secrecy capacity. In this condition, given



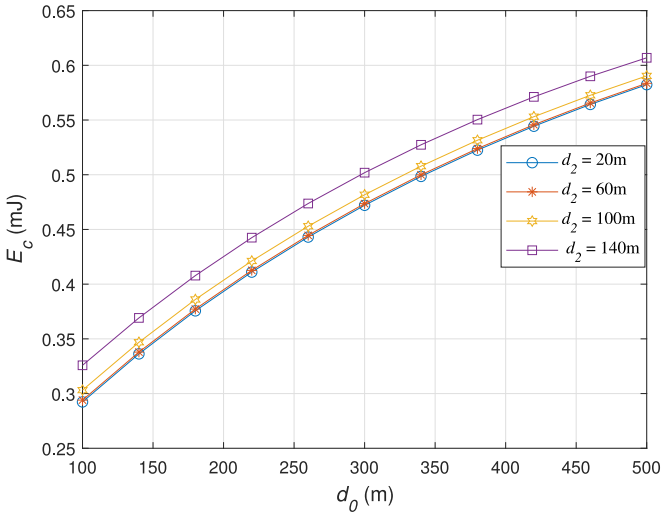
(a)

(b)

Fig. 4. Threshold value of P_J and harvested energy by UAV versus the distance from UAV to AP and Eve ($\lambda = 0.8$; $P_J = \max(P_J^{\text{th}}, 0)^+$; $T_{\text{up}} = 0.5$ s; $d_2 = 100$ m). (a) Threshold value of jamming power. (b) Harvested energy by UAV.



(a)



(b)

Fig. 5. Maximum offloading load $OL_{\max}$ and consumed energy E_c versus UAV's altitude under different Eve's locations d_2 ($C = 500$ cycles/bit; $T = 0.5$ s; $p_U = 7 \times 10^{-13}$ J/cycle; $P_t^{\max} = 0.25$ W; $P_J = 2.5$ W). (a) Maximum offloading load. (b) Consumed energy of UAV.

values of P_J as well as P_t, less computational bits are offloaded and more energy is spent to offload a computational bit. In addition, as the distance between UAV and Eve increases, the changes in $OL_{\max}$ and E_c is opposite, because both the path loss between AP and Eve and the noise power received at Eve reduce. Furthermore, the sharp increase of E_c from $d_2 = 100$ m to $d_2 = 140$ m can be explained by the following. In the case where Eve is far from AP, the security capacity of our offloading scheme is mainly bounded by jamming power; hence, the UAV has to allocate higher transmit power to ensure the security of the offloading channel.

Fig. 6 plots the maximum achievable offloading load $OL_{\max}$, for different values of P_J and $P_t^{\max}$. The numerical results show that increasing jamming power brings a higher value of $OL_{\max}$, since the larger jamming power enhance the secrecy capacity, then more computational bits can be securely offloaded to MEC. Moreover, for a small P_J, $OL_{\max}$ increases drastically, whereas $OL_{\max}$ experiences a slight increase when P_J reaches a certain threshold value. In the former condition, the secrecy performance is mainly bounded by jamming power; while the secrecy performance is mainly limited by the transmit power (transmit-power-limited) in the latter condition. Therefore, when $OL_{\max}$ is offloading-power-limited, the increase in the maximum offloading load is achieved by enhancing UAV's maximum transmit power, as shown in Fig. 6.

With the given the maximum tolerable latency and computational workload, we turn to compute the energy gap E_τ in different scenarios. Moreover, the performance of our proposed offloading scheme is compared with the above-mentioned existing schemes in terms of the energy gap E_τ.

Fig. 7 shows the energy gap E_τ versus task input bits ℓ, in the scenario that of the maximum tolerable latency equals the entire local computing (nonoffloading) time. It is observed

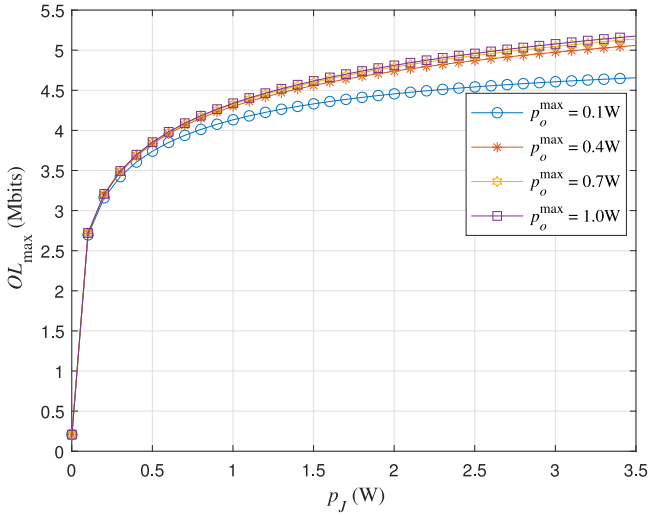


Fig. 6. Maximum offloading load $OL_{\max}$ versus jamming power of P_J under different maximum transmit power $P_t^{\max}$ ($C = 500$ cycles/bit; $T = 0.5$ s; $d_0 = d_1 = 300$ m; $d_2 = 50$ m).

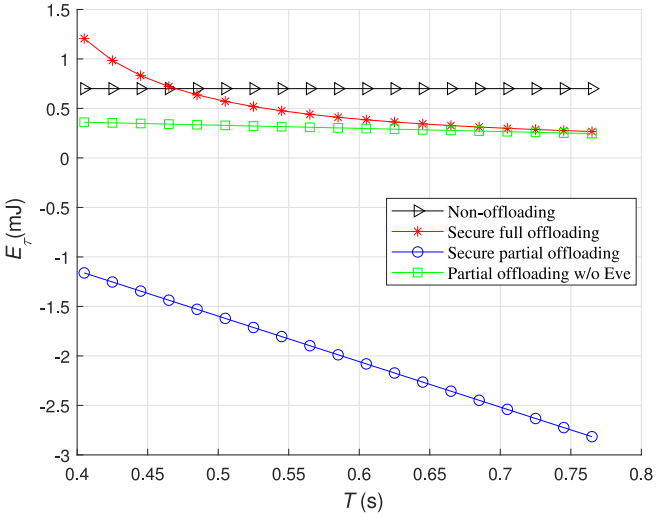


Fig. 8. Energy gap E_τ versus latency T. ($L = 2$ Mbits; $C = 500$ cycles/bit; $P_U = 7 \times 10^{-13}$ J/cycle; $P_J = 2.5$ W; $d_0 = d_1 = 200$ m; $d_2 = 100$ m).

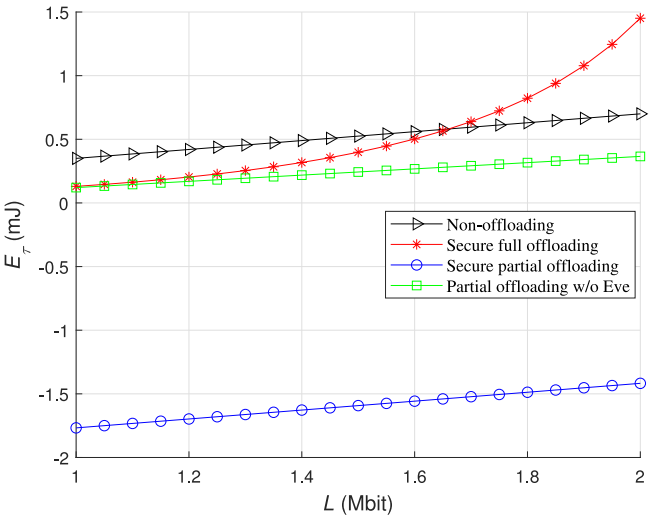


Fig. 7. Energy gap E_τ versus the number of computation input data size ℓ. ($C = 500$ cycles/bit; $T = 0.4$ s; $P_U = 7 \times 10^{-13}$ J/cycle, $P_J = 2.5$ W; $d_0 = d_1 = 200$ m; $d_2 = 100$ m; the transmit power of secure full offloading and partial offloading w/o Eve can be obtained by setting $l = L$ and $P_J = 0$, respectively. The remaining parameters are listed in Table II.)

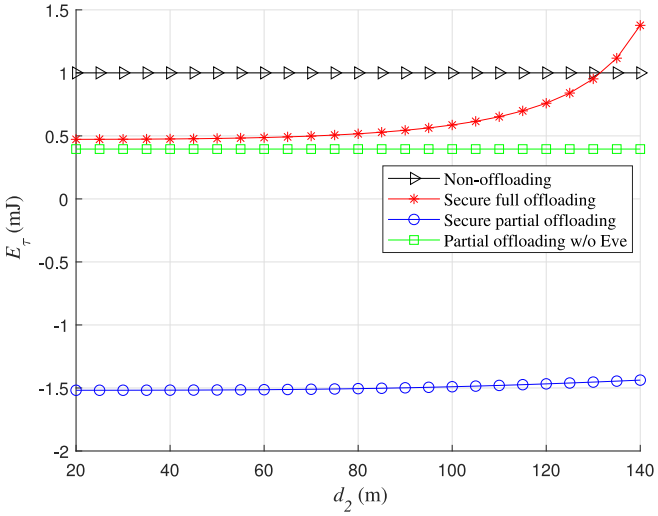


Fig. 9. Energy gap E_τ versus the distance from AP to Eve d_2. ($L = 2$ Mbits; $T = 0.5$ s; $C = 500$ cycles/bit; $P_U = 7 \times 10^{-13}$ J/cycle; $d_0 = d_1 = 200$ m).

that the proposed *secure partial offloading* offloading scheme outperforms *nonoffloading* and *secure full offloading* schemes, which shows the importance of the joint optimization of local computing and secure offloading. It is also revealed that the performance achieved by jointly optimizing communication and computation resources is superior to that of the one obtained by optimizing these resources separately. On the other hand, the performance of the proposed scheme outperforms that of [33], confirming the benefit of imposing AN on Eve. Moreover, it also presents that the harvested energy by UAV is larger than the consumed energy, which ensures sustainable development of the system.

Fig. 8 illustrates the tradeoff between the energy gap E_τ and latency T, in which our proposed *secure partial offloading* scheme outperforms *nonoffloading*, *secure full offloading*, as well as *secure partial offloading w/o AN* [33] schemes, verifying the benefits of WPT in both hard latency deadline and relax latency deadline cases. The performance gap between the proposed scheme and the one of [33] is partly due to the AN implemented in the secure UMEC system. Moreover, we note that E_τ is a decreasing function in terms of T, because the secrecy constraint relieves as the latency constraint relaxes, leading to a transmit power along with energy consumption for offloading decreases. In other words, the improvement in latency can be achieved at the cost of energy. Finally, the energy consumption for the *Nonoffloading* scheme is related to task data size and energy cost for processing a bit at the UAV, whereas it does not change with latency.

Fig. 9 shows the energy gap E_τ of UAV versus the distance from AP to Eve d_2. It is observed that E_τ increases as

d_2, because the channel quality of h_{UE} becomes worse as d_2 increases, and the UAV needs to enlarge its transmit power to ensure the security capacity. Besides, the value of E_τ of *secure full offloading* scheme experiences sharp increase from $d_2 = 100$ m-140 m. Because the performance of the proposed scheme is mainly bounded by jamming power when the Eve locates in a region far from AP; hence, a much higher transmit power is required for securely processing the computational loads encountered. Additionaly, since the AP has no impact on Eve in [33], the performance of the *secure partial offloading w/o AN* scheme dose not respond to the change in d_2.

V. Conclusion

The energy consumption minimization problem was studied in the secure UMEC wireless-powered system, where a UAV is offloading computational bits to MEC under the supervision of Eve. In the cases that the UAV's battery is *draining* or *charging*, the computation and communication resource allocation are optimized to prolong the service time of UAV, through minimizing the gap between the consumed and stored energy, subject to secrecy and latency constraints. The semiclosed form expressions for the optimal solution of offloading time duration, transmit power, and offloading ratio were derived. Moreover, the optimal offloading decision whether the UAV chose to process all computational bits locally or offload them to MEC has been also discussed under binary offloading mode. Through numerical results, it has been shown the correctness of the derivations. Moreover, it has also revealed the superiority of our proposed joint optimization scheme.

The nonlinear EH model and UAV path planning will be investigated in our future work, and the formulated nonconvex problem should be transformed into a more tractable form, through mathematical manipulations, i.e., successive convex approximation (SCA), introducing auxiliary variables. Then, it can be decomposed into a series of subproblems, corresponding to communication and computation resources allocation and trajectory optimization, to be iteratively solved with the block coordinate descent (BCD) method. An iterative algorithm with guaranteed convergence and reasonable complexity should be developed to find the global solution.

Appendix A
Proof of Lemma 1

Since the energy consumption for local computing is fixed, with a given offloading data size, the monotonicity of the objective function is mainly determined by the energy consumption for the offloading bits ℓ.

By substituting (12) into (24), P_t is expressed as a function of ℓ as

$$P_t(\ell) = \frac{1 - 2^{-\frac{\ell}{BT_{\rm up}}}}{\frac{h_{UA}}{\sigma^2} 2^{-\frac{\ell}{BT_{\rm up}}} - \frac{\tilde{h}_{UE}^{\max}}{P_J \tilde{h}_{AE}^{\min} + \sigma^2}}. \tag{33}$$

Denoting $\gamma_{UA} = (h_{UA}/\sigma^2)$ and $\gamma_{UE} = [\tilde{h}_{UE}^{\max}/(P_J \tilde{h}_{AE}^{\min} + \sigma^2)]$, (33) is simplified as

$$P_t(\ell) = \frac{1 - 2^{-\frac{\ell}{BT_{\rm up}}}}{\gamma_{UA} 2^{-\frac{\ell}{BT_{\rm up}}} - \gamma_{UE}}. \tag{34}$$

Thus, $E_{\rm off}$ is re-expressed as

$$E_{\rm off} = P_t(\ell) T_{\rm up} \tag{35}$$

$$= \frac{\left(1 - 2^{-\frac{\ell}{BT_{\rm up}}}\right) T_{\rm up}}{\gamma_{UA} 2^{-\frac{\ell}{BT_{\rm up}}} - \gamma_{UE}} \tag{36}$$

$$= \frac{\left(2^{\frac{\ell}{BT_{\rm up}}} - 1\right) T_{\rm up}}{\gamma_{UA} - \gamma_{UE} 2^{\frac{\ell}{BT_{\rm up}}}}. \tag{37}$$

It is clear that the denominator in (37) increases with $T_{\rm up}$. Next, we will explore the monotonicity of the numerator in (37).

The first derivative of the numerator in (37) of $T_{\rm up}$ is given by

$$\frac{\partial\left(2^{\frac{\ell}{BT_{\rm up}}} - 1\right) T_{\rm up}}{\partial T_{\rm up}} = 2^{\frac{\ell}{BT_{\rm up}}} - \frac{\ell \ln 2}{B T_{\rm up}} 2^{\frac{\ell}{BT_{\rm up}}} - 1. \tag{38}$$

For notational simplicity, let $v = (\ell/BT_{\rm up})$ and $f(v) = 2^v - v2^v \ln 2 - 1$. Hence, (38) can be denoted by $f(v)$. Besides, we have $f(v) = 0$ for $v = 0$, and the partial derive as

$$f'(v) = -(\ln 2)^2 v 2^v. \tag{39}$$

It is clear that $f(v)$ is nonpositive for any $v \geq 0$.

In this way, the first derivative of $E_{\rm off}$ is nonpositive, i.e., $(\partial E_{\rm off}/\partial T_{\rm up}) \leq 0$ for $T_{\rm up} \geq 0$; hence, $E_{\rm off}$ is shown to monotonically decrease in $T_{\rm up} \in [0, T]$. In other words, $E_{\rm off}$ is minimum when $T_{\rm up} = T$. Finally, the optimal offloading time $T_{\rm up}^* = T$ is obtained.

Appendix B
Proof of Lemma 2

Assertion 2 has shown that the objective function of $\mathcal{Q}2$ is strictly convex with respect to ℓ. Thus, equation $\phi_1(\ell) = 0$ has a unique root, denoted as $\hat{\ell}$. If $\hat{\ell} \leq \ell_{\min}$, the objective function increases monotonically in $[\ell_{\min}, \ell_{\max}]$. In this case, $\ell^* = \ell_{\max}$. If $\ell_{\min} \leq \hat{\ell} \leq \ell_{\max}$, the objective function decreases monotonically in $[\ell_{\min}, \hat{\ell}]$ and increases monotonically in $[\hat{\ell}, \ell_{\max}]$. In this case, $\ell^* = \hat{\ell}$. If $\ell_{\max} \leq \hat{\ell}$, the objective function decreases monotonically in the region of $[\ell_{\min}, \ell_{\max}]$. In this case, $\ell^* = \ell_{\max}$. Moreover, note that $\phi_1(\ell) = 0$ is a transcendental equation with respect to ℓ, which can be solved using the bisection search method.

References

[1] O. S. Oubbati, N. Chaib, A. Lakas, P. Lorenz, and A. Rachedi, "UAV-assisted supporting services connectivity in urban VANETs," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3944–3951, Apr. 2019.

[2] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48 572–48 634, Apr. 2019.

[3] A. Bensalem, D. E. Boubiche, F. Zhou, A. Rachedi, and A. Mellouk, "Impact of mobility models on energy consumption in unmanned aerial ad-hoc network," in *Proc. IEEE 45th Local Comput. Netw. Conf. (LCN)*, Nov. 2020, pp. 361–364.

[4] T. Abar, A. Rachedi, A. ben Letaifa, P. Fabian, and S. El Asmi, "FellowMe cache: Fog computing approach to enhance (QoE) in internet of vehicles," *Future Gener. Comp. Syst.*, vol. 113, pp. 170–182, Dec. 2020.

[5] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—a key technology towards 5g," *ETSI white paper*, vol. 11, no. 11, pp. 1–16, 2015.

[6] A. Ebrahimzadeh and M. Maier, "Cooperative computation offloading in FiWi enhanced 4G HetNets using self-organizing MEC," *IEEE Trans.Wireless Commun.*, vol. 19, no. 7, pp. 4480–4493, Apr. 2020.

[7] G. Qiao, S. Leng, K. Zhang, and Y. He, "Collaborative task offloading in vehicular edge multi-access networks," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 48–54, Aug. 2018.

[8] Z. Zhou, H. Yu, C. Xu, Z. Chang, S. Mumtaz, and J. Rodriguez, "BEGIN: Big data enabled energy-efficient vehicular edge computing," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 82–89, Nov. 2018.

[9] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1628–1656, Mar. 2017.

[10] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, Nov. 2015.

[11] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensic Secur.*, vol. 6, no. 3, pp. 693–702, Jun. 2011.

[12] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, May 2016.

[13] C. Zhan, H. Hu, X. Sui, Z. Liu, and D. Niyato, "Completion time and energy optimization in the UAV-enabled mobile-edge computing system," *IEEE Internet of Things J.*, vol. 7, no. 8, pp. 7808–7822, May 2020.

[14] M. Li, N. Cheng, J. Gao, Y. Wang, L. Zhao, and X. Shen, "Energy-efficient UAV-assisted mobile edge computing: Resource allocation and trajectory optimization," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3424–3438, Jan. 2020.

[15] Y. Du, K. Yang, K. Wang, G. Zhang, Y. Zhao, and D. Chen, "Joint resources and workflow scheduling in UAV-enabled wirelessly-powered MEC for IoT systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 10 187–10 200, Aug. 2019.

[16] H. Mei, K. Yang, Q. Liu, and K. Wang, "Joint trajectory-resource optimization in UAV-enabled edge-cloud system with virtualized mobile clone," *IEEE Internet of Things J.*, vol. 7, no. 7, pp. 5906–5921, Nov. 2020.

[17] T. Zhang, Y. Xu, J. Loo, D. Yang, and L. Xiao, "Joint computation and communication design for UAV-assisted mobile edge computing in IoT," *IEEE Trans. Ind. Inform.*, vol. 16, no. 8, pp. 5505–5516, Oct. 2020.

[18] B. Yang, H. Wu, X. Cao, X. Li, T. Kroecker, Z. Han, and L. Qian, "Intelli-eye: An UAV tracking system with optimized machine learning tasks offloading," in *Proc. IEEE INFOCOM Workshops*, Apr. 2019, pp. 1–6.

[19] M. Messous, H. Sedjelmaci, N. Houari, and S. Senouci, "Computation offloading game for an UAV network in mobile edge computing," in *Proc. IEEE ICC*, May 2017, pp. 1–6.

[20] M. Messous, A. Arfaoui, A. Alioua, and S. Senouci, "A sequential game approach for computation-offloading in an UAV network," in *Proc. IEEE GLOBOCOM*, Dec. 2017, pp. 1–7.

[21] M. Messous, S. Senouci, H. Sedjelmaci, and S. Cherkaoui, "A game theory based efficient computation offloading in an UAV network," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4964–4974, Feb. 2019.

[22] B. Liu, W. Zhang, W. Chen, H. Huang, and S. Guo, "Online computation offloading and traffic routing for UAV swarms in edge-cloud computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8777–8791, May 2020.

[23] S. Yin, Y. Zhao, L. Li, and F. R. Yu, "UAV-assisted cooperative communications with time-sharing information and power transfer," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1554–1567, Nov. 2020.

[24] W. Lu, S. Fang, Y. Gong, L. Qian, X. Liu, and J. Hua, "Resource allocation for OFDM relaying wireless power transfer based energy-constrained UAV communication network," in *Proc. IEEE ICC Workshops*, May 2018, pp. 1–6.

[25] D. N. K. Jayakody, T. D. P. Perera, A. Ghrayeb, and M. O. Hasna, "Self-energized UAV-assisted scheme for cooperative wireless relay networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 578–592, Nov. 2020.

[26] B. Ji, Y. Li, D. Cao, C. Li, S. Mumtaz, and D. Wang, "Secrecy performance analysis of UAV assisted relay transmission for cognitive network with energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7404–7415, Apr. 2020.

[27] Z. Yang, W. Xu, and M. Shikh-Bahaei, "Energy efficient UAV communication with energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1913–1927, Dec. 2020.

[28] Z. Chen, K. Chi, K. Zheng, G. Dai, and Q. Shao, "Minimization of transmission completion time in UAV-enabled wireless powered communication networks," *IEEE Internet of Things J.*, vol. 7, no. 2, pp. 1245–1259, Nov. 2020.

[29] Y. Liu, K. Xiong, Q. Ni, P. Fan, and K. B. Letaief, "UAV-assisted wireless powered cooperative mobile edge computing: Joint offloading, CPU control, and trajectory optimization," *IEEE Internet of Things J.*, vol. 7, no. 4, pp. 2777–2790, Dec. 2020.

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

[31] 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, Feb. 2019.

[32] T. Shen and H. Ochiai, "A UAV-aided selective relaying with cooperative jammers for secure wireless networks over rician fading channels," in *Proc. IEEE 90th Veh. Technol. Conf.*, Sept. 2019, pp. 1–5.

[33] Z. Lv, J. Hao, and Y. Guo, "Energy minimization for MEC-enabled cellular-connected UAV: Trajectory optimization and resource scheduling," in *Proc. IEEE INFOCOM Workshops*, Jul. 2020, pp. 478–483.

[34] M. Sheng, Y. Wang, X. Wang, and J. Li, "Energy-efficient multiuser partial computation offloading with collaboration of terminals, radio access network, and edge server," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1524–1537, Dec. 2020.

[35] M. R. A. Khandaker, C. Masouros, and K. Wong, "Constructive interference based secure precoding: A new dimension in physical layer security," *IEEE Trans. Inf. Forensic Secur.*, vol. 13, no. 9, pp. 2256–2268, Mar. 2018.

[36] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, "Robust trajectory and transmit power design for secure UAV communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 9042–9046, Jun. 2018.

[37] S. Boyd and L. Vandenberghe, *Convex optimization*.Cambridge university press, 2004.

[38] V. Sharma, M. Bennis, and R. Kumar, "UAV-assisted heterogeneous networks for capacity enhancement," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1207–1210, Apr. 2016.

[39] T. Bai, J. Wang, Y. Ren, and L. Hanzo, "Energy-efficient computation offloading for secure UAV-edge-computing systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 6074–6087, Apr. 2019.

[40] Y. Zhou, P. L. Yeoh, C. Pan, K. Wang, M. Elkashlan, Z. Wang, B. Vucetic, and Y. Li, "Offloading optimization for low-latency secure mobile edge computing systems," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 4, pp. 480–484, Dec. 2020.

[41] C. You, K. Huang, H. Chae, and B. Kim, "Energy-efficient resource allocation for mobile-edge computation offloading," *IEEE Trans. Wirel. Commun.*, vol. 16, no. 3, pp. 1397–1411, Dec. 2017.

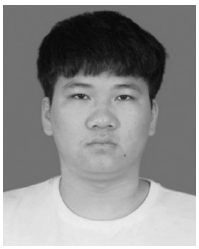
[42] C. You, Y. Zeng, R. Zhang, and K. Huang, "Asynchronous mobile-edge computation offloading: Energy-efficient resource management," *IEEE Trans. Wirel. Commun.*, vol. 17, no. 11, pp. 7590–7605, Sept. 2018.

Xiaohui Gu received the B.E. degree from Nantong University, Nantong, China, in 2017, where she is currently pursuing the Ph.D. degree.

Her main research interests include vehicular networks, edge computing, reconfigurable intelligent surface, and wireless communications.

Guoan Zhang (Member, IEEE) received the B.S. degree in precision instruments, the M.S. degree in automatic instruments and equipment, and the Ph.D. degree in communication and information systems from Southeast University, Nanjing, China, in 1986, 1989, and 2001, respectively.

He is currently a Full Professor with the School of Information Science and Technology, Nantong University, Nantong, China. His current research interests include wireless communications and vehicular networks.



Mingxing Wang is currently pursuing the postgraduate degree in information and communication engineering with Nantong University, Nantong, China.

His main research interest includes nonorthogonal multiple access techniques and wireless communications.

Wei Duan received the Ph.D. degree from Chonbuk National University, Jeonju, South Korea, in 2017.

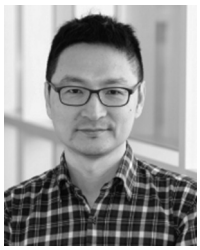
He is currently an Associate Professor with Nantong University, Nantong, China. He had participated in the World Class University, Project, sponsored by the National Research Foundation of Korea Grant funded by the Korean Ministry of Education Science and Technology, as a Vice Head Researcher. He has authored more than 30 journal papers. His research interests include wireless communications and nonorthogonal multiple access techniques.

Dr. Duan served as a Guest Editor for the *China Communications* (Special Issue on New Advances in Nonorthogonal Multiple Access), and a Lead Guest Editor for the *Wireless Communications and Mobile Computing* (Special Issue on Architectures, Challenges and Opportunities within 6G Emerging Technologies), and he is currently serving as an Editor for *Frontiers in Communications and Networks*.

Miaowen Wen (Senior Member, IEEE) received the Ph.D. degree from Peking University, Beijing, China, in 2014.

From 2019 to 2021, he was with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong, as a Postdoctoral Research Fellow. He is currently an Associate Professor with South China University of Technology, Guangzhou, China. He has published two books and more than 130 journal papers. His research interest includes a variety of topics in the areas of wireless and molecular communications.

Dr. Wen was a recipient of the IEEE ComSoc Asia–Pacific Outstanding Young Researcher Award in 2020. He was the Winner in data bakeoff competition (Molecular MIMO) at IEEE Communication Theory Workshop (CTW) 2019, Selfoss, Iceland. He has served as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS and the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING. He is currently serving as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON MOLECULAR, BIOLOGICAL AND MULTI-SCALE COMMUNICATIONS, and the IEEE COMMUNICATIONS LETTERS, and a Guest Editor for the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING (Special Issue on Advanced Signal Processing for Local and Private 5G Networks).



Pin-Han Ho (Fellow, IEEE) received the Ph.D. degree from Queen's University, Kingston, ON, Canada, in 2002.

He is currently a Full Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He has authored/coauthored of over 400 refereed technical papers, several book chapters, and the coauthor of two books on Internet and optical network survivability. His current research interests cover a wide range of topics in broadband wired and wireless communication networks, including wireless transmission techniques, mobile system design and optimization, and network dimensioning and resource allocation.

Prof. Ho is a Professional Engineer Ontario.