Energy-Efficient Computation Offloading for Secure UAV-Edge-Computing Systems

Tong Bai, *Member, IEEE*, Jingjing Wang, *Student Member, IEEE*,
Yong Ren, *Senior Member, IEEE*, and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—Characterized by their ease of deployment and bird's-eye view, unmanned aerial vehicles (UAVs) may be widely deployed both in surveillance and traffic management. However, the moderate computational capability and the short battery life restrict the local data processing at the UAV side. Fortunately, this impediment may be mitigated by employing the mobile-edge computing (MEC) paradigm for offloading demanding computational tasks from the UAV through a wireless transmission link. However, the offloaded information may become compromised by eavesdroppers. To address this issue, we conceive an energy-efficient computation offloading technique for UAV-MEC systems, with an emphasis on physical-layer security. We formulate a number of energy-efficiency problems for secure UAV-MEC systems, which are then transformed to convex problems. Finally, their optimal solutions are found for both active and passive eavesdroppers. Furthermore, the conditions of zero, partial and full offloading are analyzed from a physical perspective. The numerical results highlight the specific conditions of activating the above three offloading options and quantify the performance of our proposed offloading strategy in various scenarios.**

***Index Terms*—UAV, mobile-edge computing, physical-layer security and energy-efficient offloading.**

I. Introduction

A. Motivation and Scope

Given the advantages of prompt deployment and their bird's-eye perspective, unmanned aerial vehicles (UAVs) have been widely invoked for environmental monitoring and data collection [1]–[3], in the fields of agriculture [4], disaster sensing [5], emergency management [6], border control [7], intelligent transportation systems [8] and crowd surveillance [9]. However, the decision-making applications relying on real-time video streaming and image processing tend to exceed the local data processing capability of low-cost UAVs or may excessively prolong the time required for executing their actions [10].

To address this issue, mobile-edge computing (MEC) [11] may benefically cooperate with UAVs [8], [9] for facilitating computational offloading from the UAV to the edge nodes. The cooperation between UAVs and MEC systems can be exemplified by crowd surveillance [9]. More explicitly, UAV-mounted high-resolution cameras are capable of streaming real-time video, which facilitates the detection of criminals using face recognition. However, both the moderate computational capability and limited power supply of UAVs stifle the aforementioned real-time recognition on board. To tackle this challenges, the assistance of MEC systems can be invoked for offloading a number of computational tasks for improving the face recognition performance in a timely manner. To be specific, the data collected are partitioned into two segments, one to be computed at the UAV and the other to be offloaded to the edge node through a gateway or access point (AP). Specific to the part to be offloaded, the data may also be valuable to a third party, hence it is under a risk of being intercepted, which jeopardizes data security and privacy [12]. To overcome this security risk of the MEC, extensive work has been carried out in [13]–[16]. However, the current state-of-the-art is focused on improving the cyber-security, whilst there is a paucity of contributions on their physical-layer security (PLS) at the time of writing.

Against this background, we conceive a PLS-aided energy-efficient computational offloading scheme for UAV-MEC systems (UMEC) operating in the presence of an eavesdropper. Specifically, with the advent of an advanced full-duplex mechanism, the AP acts as a gateway for the edge nodes to receive the computational tasks offloaded from the UAV, but also plays the role of a jamming source in order to impose artificial noise on the eavesdroppers. Moreover, depending on the availability of the eavesdropper's channel state information (CSI) and location information (LI), we consider three different types of eavesdroppers [17], namely, active eavesdroppers for which we have both CSI and LI knowledge, passive eavesdroppers for whom the LI is known but the CSI is not, and passive eavesdroppers at a random location for whom we have no CSI or LI. In this context, we provide the optimal solution to the energy-efficiency problems satisfying both the offloading and security requirements by answering the following three questions: 1) What is the volume of the computational tasks to be offloaded? 2) What is the suitable duration of offloading? 3) How much power should be assigned to the offloaded signal?

B. Related Work

1) Computational Offloading in Mobile-Edge Computing: In order to support efficient mobile edge computing, three

T. Bai did this work in University of Southampton, Southampton, SO17 1BJ, U.K. He is now with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K. (e-mail: t.bai@qmul.ac.uk). J. Wang and Y. Ren are with the Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China. (e-mail: chinaeephd@gmail.com; reny@tsinghua.edu.cn). L. Hanzo is with the School of Electronics and Computer science, University of Southampton, Southampton, SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk).

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/Noo4558/1, EP/PO34284/1, COALESCE, of the Royal Society's Global Challenges Research Fund Grant as well as of the European Research Council's Advanced Fellow Grant QuantCom.

challenges have to be carefully tackled: 1) How should we decide whether to process the computational task locally or to offload it to remote edge-cloud nodes? 2) How should we determine the transmit power and choose the most appropriate channel for offloading? 3) How should we allocate computational resources to meet the multi-user latency requirements? Extensive related work has been carried out to deal with these problems [10], [11], [18]–[22]. As for single-user MEC systems, for instance, the transmission energy minimization problem is formulated under specific latency constraints in [10], [11]. Furthermore, the effect of dynamic voltage scaling on the computational speed, as well as the joint optimization of the local computational speed, offloading transmit power and offloading ratio was addressed in [18], while aiming for energy-efficient and low-latency MEC. In terms of multi-user (MU) MEC systems, for example, Sardellitti *et al.* [19] designed the transmitter's precoding matrix and optimized the computational resources for meeting the requirements of different users in a multi-cell scenario. Chen *et al.* [20] conceived a game-theoretic approach for allocating both the transmission resources and mobile-edge computational resources. You *et al.* [21] designed an energy-efficient offloading policy, for determining the offloading data volume, the offloading duration and the transmission resources of each user. Recently, Wang *et al.* [22] incorporated the concept of non-orthogonal-multiple-access (NOMA) into multi-user MEC offloading for improving the spectral efficiency attained. Apart from the above general problems, computational offloading is also investigated in specific MEC applications, such as energy harvesting [23] and medical cyber-physical systems [24].

2) Security in Mobile-Edge Computing: The current state-of-the-art richly deals with security issues in MEC, mainly from three perspectives [13]: trust and authentication mechanisms, secure networking, as well as secure computation. More explicitly, trust and authentication mechanisms are introduced for examining whether the received messange is tampered with during the transmission and identify the entity that the system is interacting with [14]. As for networking security, typically cryptographic attributes are utilized as credentials for exchanging session keys [15]. Secure computation typically relies on encryption algorithms [16]. However, the computation offloading process is also subject to the risk of being compromised at the physical layer, which has not been investigated at the time of writing.

3) Security of UAV Communication Links: Security issues arise both in the control and data links of UAV communications both due to active (e.g. jamming and spoofing) as well as passive attacks (e.g. eavesdropping) [25]. The classic cryptographic techniques have been widely invoked for protecting the data stream of UAVs in the upper layers, while the emerging solutions based on PLS also increase the difficulty for attackers to decipher the message [26]. The data transmission links may become intercepted by eavesdroppers, when the UAV acts as a surveillance node [8], a relay [27], a small base station [28] or a member of a cooperative UAV group [29]. In order to mitigate these risks, sophisticated strategies have been conceived for optimizing the UAV's flight trajectory and transmit power [12] as well as speed [30]. Furthermore, the UAV can also be invoked as a source of jamming signals for imposing artificial noise on the eavesdroppers for improving the PLS of the legimate users. For example, Lee *et al.* [31] investigated UAV-enabled secure communication systems, where a UAV is employed for transmitting confidential signals to ground users, while a cooperative UAV is deployed for sending jamming signals to the eavesdroppers. Zou *et al.* [32] exploited relay-selection for improving the security-reliability trade-off in cognitive radio systems.

C. Contributions and Organizations

Our main contribution is to conceive a secure computational offloading strategy for UMEC relying on PLS, detailed as follows.

- *Energy-efficiency problem formulation for secure UMEC*: We establish a secure model including a UAV, an AP as well as an eavesdropper, and formulate an energy-efficient computation offloading problem, subject to both time-duration and security constraints, in the presence of an active eavesdropper, a passive eavesdropper at a fixed location and a passive eavesdropper at a random location.
- *Problem transformation and optimal solution*: Owing to the presence of multiple variables, the initially formulated problems cannot be directly solved. To overcome this problem, we transform the original problems into convex problems having a single variable, through a series of mathematical manipulations accompanied by their strict proofs and then provide the corresponding (asymptotically) optimal offloading solutions within the feasible sets.
- *Physical analysis of offloading options*: The optimized offloading scenarios, when the UAV offloads no computational tasks, or a fraction of the tasks or alternatively all tasks are respectively referred to as zero, partial and full offloading. We investigate the conditions of these scenarios from a physical perspective.
- *Numerical validations and evaluations*: Our numerical results verify the accuracy of the proposed optimal solutions for the three offloading scenarios, and quantify the performance of the secure UMEC in terms of both the maximum computational loads that can be processed and the total energy consumption, given a certain volume of computational loads in diverse scenarios.

The rest of the paper is organized as follows. The system model is elaborated on in Section II, and the energy-efficient computation offloading problem of UMEC is formulated in Section III. Section IV transforms the original problems into convex problems and provides the optimal offloading strategy, whilst Section V presents the conditions for the three offloading options from a physical perspective. Our numerical results are discussed in Section VI, while our conclusions are offered in Section VII.

II. System Model

As shown in Fig. 1, we consider a hovering single-antenna UAV capable of offloading computational tasks to an edge

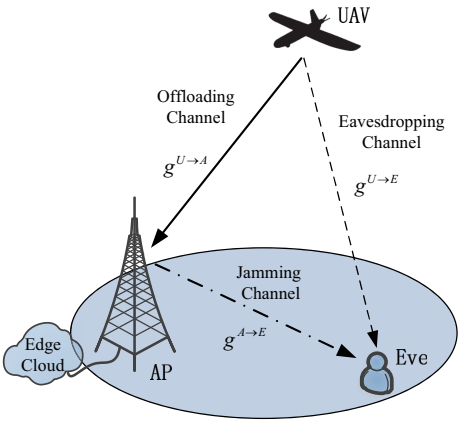

Figure 1: Illustration of the secure UAV-edge hyrbrid system model.

computing node via an AP on the ground through the wireless transmission link, which is intercepted by a single-antenna eavesdropper (Eve) on the ground. In order to combat eavesdropping, the AP relying on full-duplex techniques [33] imposes artificial noise for degrading Eve's reception quality. Since the transmitted artificial noise is known by the AP and the CSI between the AP's transmit and receive antennas is known, we invoke the idealized simplifying assumption that the self-interference of the AP is canceled.

Let us denote the channel between the UAV and the AP as well as the channel between the UAV and Eve by $g^{U\to A}$ and $g^{U\to E}$ respectively, which are assumed to be dominated by the Line-of-Sight (LoS) path, yielding

$$g^{U\to A(E)} = \kappa_1 d_1^{-\eta_1}, \tag{1}$$

where d_1 denotes the hovering altitude of the UAV [1], while κ_1 corresponds to the unity channel gain at the reference distance of $d_1 = 1$ m and η_1 represents the path loss exponent of the LoS path. Moreover, the channel between the AP and Eve consists of both the large-scale path loss and small-scale fading, i.e. $g^{A\to E} = \xi h^{A\to E}$. As for the large scale fading, it is modeled as

$$\xi = \kappa_2 d_2^{-\eta_2}, \tag{2}$$

where d_2 denotes the distance between Eve and the AP, while κ_2 corresponds to the unity channel gain at the reference distance of $d_2 = 1$ m and η_2 represents the path loss exponent of the NLoS component. Finally, the small-scale fading envelope is assumed to obey quasi-static Rayleigh distribution and hence the Cumulative Density Function (CDF) of $h^{A\to E}$ obeys

$$F_{h^{A\to E}}(x) = 1 - e^{-\lambda x}, \tag{3}$$

where $\lambda^{-1} = \mathbb{E}\big[h^{A\to E}\big]$.

A. Local-Computing Model

We use L and ℓ to denote the total number of bits to be processed and the number of bits to be offloaded to the edge node, respectively. In this case, the number of locally computed bits is $L-\ell$. Moreover, as for the local computing at the UAV, C_U corresponds to the number of central processing unit (CPU) cycles required for processing 1-bit of input data, while P_U represents the energy consumption of each CPU cycle. In this case, the energy consumption of the local computation is expressed as $E_{\text{loc}} = C_U P_U (L-\ell)$. Furthermore, assuming that the UAV has a computational capability of D_U quantified in terms of the number of CPU cycles per second, the time required for carrying out the local computation is expressed as $C_U(L-\ell)/D_U$.

B. Jamming Model

Various jamming schemes have been proposed for PLS based on various strategies [35], such as nonself-cooperative [36] versus self-cooperative [37], omni-directional [38] versus directional scenarios [39], relying on either perfect or imperfect eavesdropper CSI [35]. Since the design of the jamming scheme is not within our main focus in this paper, the self-cooperative jamming strategy using an omnidirectional antenna [35] is invoked at the AP side for simplicity. Accordingly, given a jamming power of p_J, the artificial noise received by Eve is given by $N_J^E = p_J g^{A\to E}$.

C. Secure-Offloading Model

Let us denote the power of the natural noise at the AP and Eve by N_0^A and N_0^E, respectively. As for a wiretap channel, the secrecy capacity denoted by S can be obtained as the difference between the main channel's and the wiretap channel's capacity [40]. Specifically, given the offloading power of p_O and the jamming power of p_J, $S(p_O, p_J)$ in the system considered is formulated as [40]

$$S(p_O,p_J) = B\log_2\left(1+\frac{p_O g^{U\to A}}{N_0^A}\right) - B\log_2\left(1+\frac{p_O g^{U\to E}}{N_0^E+N_J^E}\right), \tag{4}$$

where B refers to the bandwidth of the channel. Another metric quantifying the quality-of-service (QoS) is the secrecy outage probability (SOP), which corresponds to the probability that the secrecy capacity fails to meet the secure transmission rate required. Given the offloading power of p_O, jamming power of p_J, ℓ offloaded bits and the offloading transmit duration of t, the SOP is formulated as [40]

$$P_{\text{out}}^S(p_O,p_J,\ell,t) = 1 - \Pr\left[S(p_O,p_J) \geq \frac{\ell}{t}\right]. \tag{5}$$

Moreover, the energy consumption of offloading from the UAV is given by $E_{\text{off}} = p_O t$.

D. Edge-Computing Model

As for edge computing, we use D_E and C_E to represent the computational capability quantified in terms of the number of CPU cycles per second and the number of CPU cycles required for processing one bit of input data, respectively. Taking advantage of parallelism [41], the computational loads can be partitioned into tasks of minimal volume, hence the edge computing node is capable of executing the computations along with all the receiver's tasks. Then, the time-duration required for edge computing is formulated as $C_E\ell/D_E$.

[1]The drone may potentially be laser-charged as detailed in [34] for supporting sustained operations.

III. Energy-Efficient Resource Allocation Problem Formulation for Secure UMEC

The total energy consumption of UAVs is constituted by the sum of the local computation-related and computation offloading-based dissipation as well as that of the propulsion. As for the scenario where the UAV acts as a flying base station [42] and as a floating relay [43], the flight trajectory and the placement of the UAV can be optimized for improving the communication performance, respectively. By contrast, the mobility of the UAVs used for environmental monitoring and surveillance is controlled by a specific user instead of a communication service provider. Therefore, we have to exclude the propulsion-related energy-optimization in our problem formulation. Specifically, the total energy is calculated as $E_{\text{tot}} = E_{\text{loc}} + E_{\text{off}}$. We note that E_{off} substantially depends on the availability of the eavesdropper's CSI, as we will demonstrate by considering both active and passive eavesdroppers. More explicitly, the active eavesdropper (i.e. listening and transmitting) may be a user being served by the AP, hence the CSI between the AP and Eve can be estimated in a near-instantaneous manner. By contrast, the passive eavesdropper is listening but not transmitting. Hence, its CSI cannot be extracted. Therefore, at best we can assume the knowledge of statistical information of the channel between the AP and Eve.

Furthermore, both the total volume of computational loads and the computing-related energy per bit on the UAV's board are assumed to be signalled by the AP using its feedback link. Based on the above information, the small-cell cloud manager [44] of the AP aims for determining both the UAV's offloading data volume of ℓ, as well as the offloading transmit power of p_O and the offloading duration of t, for maintaining both a high energy efficiency and high transmission secrecy. In the rest of this section, our energy-efficient computation offloading problems are formulated in the presence of both an active and a passive eavesdropper, one after the other.

A. Problem 1: Active Eavesdropper

1) Constraints: Our energy-efficient computation offloading problem is formulated in the presence of an active eavesdropper under the following constraints:

- Latency constraint: the computation has to be executed within a maximum tolerable latency, which is denoted by T. Then, the temporal constraints of the local and of the edge computing can be formulated as $C_U(L-\ell)/D_U \leq T$ and $C_E\ell/D_E \leq T$, respectively; Moreover, assuming that the offloading duration is t, it should not exceed the latency constraint, i.e. $0 \leq t \leq T$;
- Offloaded data volume constraint: the volume of data offloaded to the AP is naturally a non-negative integer and does not exceed the total computational loads, i.e. $\ell \in \{0, 1, \cdots, L\}$;
- Power consumption constraint: the UAV has a maximum transmission power limit of $p_O^{\max}$, i.e. $0 \leq p_O \leq p_O^{\max}$;
- Secrecy constraint: Provided that the instantaneous CSI of Eve is known, the AP is able to ensure that the received power of artificial noise remains constant by forcing $p_J = \overline{p}_J/g^{A\to E}$. In order to support secure offloading in the presence of an eavesdropper, the secrecy capacity should not be lower than the offloading rate, given the offloading duration of t, i.e. $S(p_O, p_J) \geq \ell/t$.

2) Problem Formulation: The computational offloading problem is formulated for minimizing the energy consumption of the UAV's data processing in the secure UMEC intercepted by an active eavesdropper as

$$\begin{aligned}
\mathcal{P}1: \arg\min_{\ell, p_O, t}\ & C_U P_U (L-\ell) + p_O t \\
\text{s.t.}\ & \frac{C_U(L-\ell)}{D_U} \leq T, && \text{(6a)}\\
& \frac{C_E \ell}{D_E} \leq T, && \text{(6b)}\\
& S(p_O, p_J) \geq \frac{\ell}{t}, && \text{(6c)}\\
& \ell \in \{0, 1, \cdots, L\}, && \text{(6d)}\\
& 0 \leq p_O \leq p_O^{\max}, && \text{(6e)}\\
& 0 \leq t \leq T, && \text{(6f)}
\end{aligned}$$

where the first and second term of the objective function (OF) correspond to the energy consumption of the local computation and the computation offloading, respectively. As for the constraints, (6a), (6b) and (6f) ensure the latency requirement to be met. Furthermore, (6c) guarantees the secure offloading, while (6d) and (6e) restrict the feasible sets of ℓ and p_O.

B. Problem 2: Passive Eavesdropper

1) Constraints: The constraints of the energy-efficient computation offloading problem in the presence of a passive eavesdropper are elaborated on as follows.

- The latency, the offloaded data volume and the power consumption constraints are the same as those in the presence of an active eavesdropper;
- Secrecy constraint: since the instantaneous CSI is unknown in this case, the secrecy capacity cannot be always ensured for supporting the secure target offloading rate in the face of the channel's fluctuation. Therefore, we impose a SOP requirement of ϵ on the offloading transmission, i.e. $P_{\text{out}}^S(p_O, p_J, \ell, t) \leq \epsilon$.

2) Problem Formation: The energy-efficient computing offloading problem is formulated for the UMEC intercepted by a passive eavesdropper as

$$\begin{aligned}
\mathcal{P}2: \arg\min_{\ell, p_O, t}\ & C_U P_U (L-\ell) + p_O t \\
\text{s.t.}\ & \frac{C_U(L-\ell)}{D_U} \leq T, && \text{(7a)}\\
& \frac{C_E \ell}{D_E} \leq T, && \text{(7b)}\\
& P_{\text{out}}^S(p_O, p_J, \ell, t) \leq \epsilon, && \text{(7c)}\\
& \ell \in \{0, 1, \cdots, L\}, && \text{(7d)}\\
& 0 \leq p_O \leq p_O^{\max}, && \text{(7e)}\\
& 0 \leq t \leq T, && \text{(7f)}
\end{aligned}$$

where (7a), (7b) and (7f) correspond to the latency constraint. Moreover, (7c) ensures the SOP requirement to be satisfied, whilst (7d) and (7e) restrict the feasible set of ℓ and p_O, respectively.

Additionally, since the large-scale path loss is a component of $g^{A\to E}$, the fact whether the passive eavesdropper's LI is acknowledged by the AP influences the distribution of $g^{A\to E}$ and hence further influences the $P_{\text{out}}^{S}(p_O, p_J, \ell, t)$ in (7c). In this paper, therefore, we consider two types of passive eavesdroppers - i.e. one at a fixed location whose LI is acknowledged by the AP while the other at a random location whose LI is unknown to the AP - and the corresponding problems are denoted by $\mathcal{P}2$-1 and $\mathcal{P}2$-2, respectively.

IV. Optimal Solution of the Energy-Efficient Secure UMEC Problem

In this section, we present the optimal solution to the problems for both the active and for the passive eavesdropper at a fixed location as well as the asymptotically optimal solution to the problem, where the passive eavesdropper is at a random location. In short, the problems are solved in three steps: 1) Having multiple variables, Problem $\mathcal{P}1$, $\mathcal{P}2$-1 and $\mathcal{P}2$-2 cannot be solved directly and here we transform them into problems having a single variable; 2) We prove the convexity of the problems; 3) The optimal solutions are conceived for the three problems considered.

A. Case 1: Active Eavesdropper

1) Transformation of Problem $\mathcal{P}1$: Problem $\mathcal{P}1$ is transformed to Problem $\mathcal{P}1$-E having a single variable as follows.

Proposition 1. *Constraint* (6c) *is strictly binding for the optimal solution of Problem $\mathcal{P}1$, i.e. the secrecy capacity of S to satisfy*

$$S(p_O, p_J) = \frac{\ell}{t}. \tag{8}$$

Proof: It may be readily seen that $S(p_O, p_J)$ in (4) is monotonically increasing with p_O in our considered case where the SNR at the AP is higher than that at the eavesdropper. Assuming that the constraint of (6c) is slack at the optimal solution of Problem $\mathcal{P}1$, we can then reduce p_O for reducing the objective function values, without violating any constraints. This completes the proof. ∎

Theorem 1. *Given ℓ number of bits to be offloaded,, the offloading duration yields $t = T$ for the optimal solution to Problem $\mathcal{P}1$.*

Proof: Defining $\gamma^{U\to A} = g^{U\to A}/N_0^A$ and $\gamma^{U\to E} = g^{U\to E}/(N_0^E + p_J g^{A\to E})$, and substituting (4) into (8), p_O can be expressed as a function of ℓ as

$$p_O(\ell) = \frac{1 - 2^{-\frac{\ell}{Bt}}}{\gamma^{U\to A} 2^{-\frac{\ell}{Bt}} - \gamma^{U\to E}}. \tag{9}$$

Then, E_{off} can be formulated as

$$E_{\text{off}} = p_O(\ell) t = \frac{(1 - 2^{-\frac{\ell}{Bt}})t}{\gamma^{U\to A} 2^{-\frac{\ell}{Bt}} - \gamma^{U\to E}}. \tag{10}$$

It can be observed that the denominator in (10) increases with t. In this case, if the numerator in (10) decreases with t, the offloading energy can be shown to be monotonically decreasing along with t. Taking the partial derivative of the numerator of t, we have

$$\frac{\partial\left(2^{\frac{\ell}{Bt}} - 1\right)\cdot t}{\partial t} = \left(1 - \frac{\ln(2)\cdot \ell}{Bt}\right) 2^{\frac{\ell}{Bt}} - 1, \tag{11}$$

whose polarity is still difficult to observe. Defining $\psi = \ell/Bt$, where $\psi \geq 0$, and denoting (11) by Ψ, the derivative of $\Psi(\psi)$ with respect to ψ is expressed as

$$\frac{\mathrm{d}\Psi(\psi)}{\mathrm{d}\psi} = -\big[\ln(2)\big]^2 \psi 2^{\psi}, \tag{12}$$

which is non-positive and hence $\Psi(\psi)$ is monotonically decreasing with ψ. In other words, when $\psi = 0$, $\Psi(\psi)$ reaches its maximum that is equal to 0. In this way, the partial derivative of the numerator of (10) with respect to t is non-positive and hence E_{off} has been shown to monotonically decrease in $t \in [0, T]$. ∎

With the aid of Theorem 1 and (9), Problem $\mathcal{P}1$ can then be reformulated to Problem $\mathcal{P}1$-E as follows

$$\mathcal{P}1\text{-}E: \arg\min_{\ell}\ C_U P_U (L - \ell) + \frac{T(1 - 2^{-\frac{\ell}{BT}})}{\gamma^{U\to A} 2^{-\frac{\ell}{BT}} - \gamma^{U\to E}}$$

$$\text{s.t. } \ell \geq L - \frac{TD_U}{C_U}, \tag{13a}$$

$$\ell \leq \frac{TD_E}{C_E}, \tag{13b}$$

$$\ell \leq -BT \log_2\left(\frac{1 + p_O^{\max}\gamma^{U\to E}}{1 + p_O^{\max}\gamma^{U\to A}}\right), \tag{13c}$$

$$0 \leq \ell \leq L. \tag{13d}$$

Here (13a), (13b) and (13c) are reformulated by taking into account (6a), (6b) and (6d), respectively, whilst (13d) is obtained by relaxing the integer programming constraint of (6d) to a continuous constraint.

2) Convexity of Problem $\mathcal{P}1$-E: Problem $\mathcal{P}1$-E is proved to be a convex problem in the following proposition.

Proposition 2. *Problem $\mathcal{P}1$-E is a convex problem.*

Proof: Denoting the first derivative of the objective function of Problem $\mathcal{P}1$-E by $\Phi_1(\ell)$, we have

$$\Phi_1(\ell) = -C_U P_U + \frac{\frac{\ln(2)}{B}(\gamma^{U\to A} - \gamma^{U\to E}) 2^{-\frac{\ell}{BT}}}{\left(\gamma^{U\to A} 2^{-\frac{\ell}{BT}} - \gamma^{U\to E}\right)^2}. \tag{14}$$

It can be readily observed that the increase of ℓ results in an increased $\Phi_1(\ell)$ and hence the objective function of Problem $\mathcal{P}1$-E is a convex function. Moreover, the constraint functions of (13a), (13b), (13c) and (13d) are all of linear forms. In this way, Problem $\mathcal{P}1$-E is shown to be a strictly convex problem. ∎

B. Case 2-1: Passive Eavesdropper at a Fixed Location

1) Transformation of Problem $\mathcal{P}2$: Similar to the process of solving Problem $\mathcal{P}1$ in Section IV-A, Problem $\mathcal{P}2$-1 is herein transformed to Problem $\mathcal{P}2$-1-E having a single variable. In short, the method is to link the SOP of (5) with the CDF of

$h^{A\to E}$ in (3). Specifically, substituting (4) into $S(p_O,p_J)\geq \ell/t$ in (5), we have

$$\frac{p_O g^{U\to E}}{N_0^E+p_J\xi h^{A\to E}}\leq 2^{-\frac{\ell}{Bt}}\left(1+\frac{p_O g^{U\to A}}{N_0^A}\right)-1, \quad (15)$$

where ξ is known by the AP for the case of the eavesdropper at a fixed location. In order to obtain the feasible set of $h^{A\to E}$ satisfying $S(p_O,p_J)\geq \ell/t$, firstly the polarity of the right side of (15) has to be clarified. Particularly, under the condition of $S(p_O,p_J)\geq \ell/t$, we have $1+p_O g^{U\to A}/N_0^A\geq 2^{\ell/Bt}$ based on the observation of (4) and hence the right side of (15) is proved to be positive. Then, the range of $h^{A\to E}$ can be obtained by reformulating (15) as

$$h^{A\to E}\geq \frac{p_O g^{U\to E}}{\xi p_J\left[2^{-\frac{\ell}{Bt}}\left(1+\frac{p_O g^{U\to A}}{N_0^A}\right)-1\right]}-\frac{N_0^E}{\xi p_J}. \quad (16)$$

Upon denoting the right side of (16) by $h_{\text{req}}^{A\to E}(p_O,p_J,\ell,t)$, (7c) becomes equivalent to

$$F_{h^{A\to E}}\left[h_{\text{req}}^{A\to E}(p_O,p_J,\ell,t)\right]\leq \epsilon, \quad (17)$$

where $F_{h^{A\to E}}(x)$ corresponds to the CDF of $h^{A\to E}$ as illustrated in (3). In this way, under the given values of ℓ, t and p_J, the required p_O attaining the targeted SOP of ϵ can be obtained by substituting (3) and (16) into (17), as

$$p_O\geq \frac{\left[-\frac{\xi p_J\ln(1-\epsilon)}{\lambda}+N_0^E\right]\left[1-2^{-\frac{\ell}{Bt}}\right]}{\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\left[-\frac{\xi p_J\ln(1-\epsilon)}{\lambda}+N_0^E\right]-g^{U\to E}}. \quad (18)$$

Again, the polarity of the denominator of (18) is clarified in the following proposition.

Proposition 3. *The denominator of* (18) *can be proved to be positive under the condition of* $P_{out}^S\leq\epsilon$.

Proof: Since $\log_2(x)$ is a monotonically increasing function of x, we have

$$B\log_2\left(\frac{\frac{p_O g^{U\to A}}{N_0^A}}{\frac{p_O g^{U\to E}}{N_0^E+p_J g^{A\to E}}}\right)>B\log_2\left(\frac{1+\frac{p_O g^{U\to A}}{N_0^A}}{1+\frac{p_O g^{U\to E}}{N_0^E+p_J g^{A\to E}}}\right). \quad (19)$$

Then, with the aid of (7c), we have

$$\Pr\left[B\log_2\left(\frac{\frac{p_O g^{U\to A}}{N_0^A}}{\frac{p_O g^{U\to E}}{N_0^E+p_J g^{A\to E}}}\right)\leq\frac{\ell}{t}\right]<\Pr\left[S(p_O,p_J)\leq\frac{\ell}{t}\right]\leq\epsilon. \quad (20)$$

The left side of above equation can be reformulated as

$$\Pr\left(h^{A\to E}\leq\frac{g^{U\to E}\cdot N_0^A}{\xi p_J g^{U\to A}}2^{\frac{\ell}{Bt}}-\frac{N_0^E}{\xi p_J}\right)<\epsilon. \quad (21)$$

Then, replacing the left side of (21) by $h^{A\to E}$'s CDF of (3), the denominator of (18) can be proved to be positive under the condition of $P_{\text{out}}^S\leq\epsilon$. ∎

Then, p_O can be expressed as a function of ℓ through the following proposition.

Proposition 4. (18) *is strictly binding for the optimal solution to Problem* $\mathcal{P}2$-1*, i.e.*

$$p_O(\ell)=\frac{\left[-\frac{\xi p_J\ln(1-\epsilon)}{\lambda}+N_0^E\right]\left[1-2^{-\frac{\ell}{Bt}}\right]}{\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\left[-\frac{\xi p_J\ln(1-\epsilon)}{\lambda}+N_0^E\right]-g^{U\to E}}. \quad (22)$$

Proof: Similar to the proof of Proposition 1. ∎

The optimal offloading duration of t is obtained from the following theorem.

Theorem 2. *Given* ℓ *number of bits to be offloaded, the offloading duration becomes* $t=T$ *for the optimal solution to Problem* $\mathcal{P}2$-1 *for the eavesdropper at a fixed location.*

Proof: Upon introducing $\alpha=-\frac{\xi p_J\ln(1-\epsilon)}{\lambda}+N_0^E$, the energy consumed by computation offloading in the presence of a passive eavesdropper at a fixed location, may be expressed with the aid of (22), as

$$E_{\text{off}}(t)=\frac{\alpha\left[1-2^{-\frac{\ell}{Bt}}\right]t}{\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha-g^{U\to E}}. \quad (24)$$

Then, the derivative of $E_{\text{off}}(t)$ with respect to t can be obtained as (23), where the inequality of $1-2^{-\frac{\ell}{Bt}}-\ln(2)\frac{\ell}{Bt}\leq 0$ can be proved in the feasible set of $\ell/Bt\in[0,+\infty)$. In this way, the energy consumption of computation offloading $E_{\text{off}}(t)$ is monotonically decreasing along with t and hence $t=T$ yields the optimal solution to Problem $\mathcal{P}2$-1. ∎

With the aid of Proposition 4 and Theorem 2, Problem $\mathcal{P}2$-1 can be reformulated to a single-variable problem for the passive eavesdropper at a fixed location, i.e.

$$\mathcal{P}2\text{-}1\text{-}E: \arg\min_{\ell} C_U P_U(L-\ell) + \frac{\alpha\left[1-2^{-\frac{\ell}{BT}}\right]T}{\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{BT}}\alpha-g^{U\to E}}$$

$$\text{s.t.} \quad (13a),(13b),(13d)$$

$$\ell\leq -BT(1-\epsilon)\log_2\left[\frac{\alpha+p_O^{\max}g^{U\to E}}{\alpha+\frac{p_O^{\max}\alpha g^{U\to A}}{N_0^A}}\right]. \quad (25a)$$

Herein the constraints of (7a) and (7b) in Problem $\mathcal{P}2$ are transformed to (13a) and (13b), respectively. Moreover, (13d) is obtained by relaxing (7d) to a continuous constraint, whilst (7e) is rewritten as in (25a).

2) Convexity of Problem $\mathcal{P}2$-1-E*:* The convexity of Problem $\mathcal{P}2$-1-E is discussed in the following proposition.

Proposition 5. *Problem* $\mathcal{P}2$-1-E *is a convex problem.*

Proof: Denoting the first derivative of the objective function of Problem $\mathcal{P}2$-1-E with respect to ℓ by $\Phi_2(\ell)$, we have

$$\Phi_2(\ell)=-C_U P_U+\frac{\frac{\alpha\ln(2)}{B}2^{-\frac{\ell}{BT}}\left(\frac{g^{U\to A}}{N_0^A}\alpha-g^{U\to E}\right)}{\left[\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha-g^{U\to E}\right]^2}. \quad (26)$$

It can be readily observed that the increase of ℓ results in the increase of $\Phi_2(\ell)$ and hence the objective function of Problem

$$\frac{\mathrm{d}E_{\text{off}}(t)}{\mathrm{d}t} = \frac{\alpha\left(\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha - g^{U\to E}\right) + \alpha 2^{-\frac{\ell}{Bt}}\left(g^{U\to E} - \frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha\right) + \alpha\ln(2)\frac{\ell}{Bt}\left(g^{U\to E}2^{-\frac{\ell}{Bt}} - \frac{g^{U\to A}}{n_0^A}2^{-\frac{\ell}{Bt}}\alpha\right)}{\left[\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha - g^{U\to E}\right]^2}$$
$$\leq \frac{\alpha\left(\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha - g^{U\to E}\right) + \alpha 2^{-\frac{\ell}{Bt}}\left(g^{U\to E} - \frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha\right) + \alpha\ln(2)\frac{\ell}{Bt}\left(g^{U\to E} - \frac{g^{U\to A}}{n_0^A}2^{-\frac{\ell}{Bt}}\alpha\right)}{\left[\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha - g^{U\to E}\right]^2}$$
$$= \frac{\alpha\left(\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha - g^{U\to E}\right)\left(1 - 2^{-\frac{\ell}{Bt}} - \ln(2)\frac{\ell}{Bt}\right)}{\left[\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt}}\alpha - g^{U\to E}\right]^2}. \tag{23}$$

$\mathcal{P}2$-1-E is a convex function. Moreover, the constraint functions of (13a), (13b), (13d), and (25a) are all of linear form. In this way, Problem $\mathcal{P}2$-1-E is proved to be a strictly convex one. ■

C. Case 2-2: Passive Eavesdropper at a Random Location

In this section, we consider the case of a passive eavesdropper at a random location, which is assumed to obey uniform distribution within the circle having a radius of R served by the AP.

1) Transformation of Problem $\mathcal{P}2$: The transformation process is similar to that in Section IV-A1, with the only difference being that of linking the SOP constraint of (7c) to the CDF of $g^{A\to E}$. More explicitly, given the values of p_O, p_J, ℓ and t, the specific range of $g^{A\to E}$ satisfying $S(p_O, p_J) \geq \ell/t$ can be obtained by reformulating (15) as

$$g^{A\to E} \geq \frac{p_O g^{U\to E}}{p_J\left[2^{-\frac{\ell}{Bt}}\left(1 + \frac{p_O g^{U\to A}}{N_0^A}\right) - 1\right]} - \frac{N_0^E}{p_J}. \tag{27}$$

Then, denoting the left side of (27) by $g_{\text{req}}^{A\to E}(p_O, p_J, \ell, t)$, (7c) becomes equivalent to

$$F_{g^{U\to A}}\left[g_{\text{req}}^{A\to E}(p_O, p_J, \ell, t)\right] \leq \epsilon, \tag{28}$$

where $F_{g^{U\to A}}(\cdot)$ corresponds to the CDF of $g^{U\to A}$, which is obtained in Appendix A. Substituting (41) into (28), the feasible set of p_O satisfying $S \geq \ell/t$ can be obtained after further mathematical manipulations as

$$p_O > \frac{(p_J\theta + N_0^E)\left[1 - 2^{-\frac{\ell}{Bt(1-\epsilon)}}\right]}{\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt(1-\epsilon)}}(p_J\theta + N_0^E) - g^{U\to E}}, \tag{29}$$

where θ yields

$$\theta = \frac{\frac{2}{2+\eta_2} - \sqrt{\frac{4}{(2+\eta_2)^2} - \frac{2\epsilon}{1+\eta_2}}}{\frac{1}{1+\eta_2}\frac{\lambda R^{\eta_2}}{\kappa_2}}. \tag{30}$$

Here the polarity of the denominator of (29) is clarified in the following proposition.

Proposition 6. *The denominator of* (29) *can be proved to be positive under the condition of $P_{out}^S \leq \epsilon$.*

Proof: Similar to the Proof of Proposition 3, with the aid of (19) and (20), the left side of (20) can be reformulated as

$$\Pr\left(g^{A\to E} \leq \frac{g^{U\to E}\cdot N_0^A}{p_J g^{U\to A}}2^{\frac{\ell}{Bt}} - \frac{N_0^E}{p_J}\right) < \epsilon. \tag{31}$$

Rewriting (31) with the aid of the CDF function of (41) and after some further mathematical manipulations, we have

$$\frac{g^{U\to E}\cdot N_0^A}{p_J g^{U\to A}}2^{\frac{\ell}{Bt}} - \frac{N_0^E}{p_J} < \theta. \tag{32}$$

Then the denominator of (29) can be proved to be larger than 0 by reformulating (32) and hence Proposition 6 is proved. ■

Here p_O can be expressed as a function of ℓ in the following proposition.

Proposition 7. *The optimal p_O approximates the minimum value obtained in* (29)*, yielding*

$$p_O(\ell) \to \frac{(p_J\theta + N_0^E)\left[1 - 2^{-\frac{\ell}{Bt(1-\epsilon)}}\right]}{\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{Bt(1-\epsilon)}}(p_J\theta + N_0^E) - g^{U\to E}}, \tag{33}$$

under the condition defined in Appendix A.

Proof: The relationship $>$ in (29) is asymptotically close to $\geq$, under the condition defined in Appendix A. Then, the rest of the proof is similar to the proof of Proposition I. ■

The optimal offloading duration of t is obtained by the following theorem.

Theorem 3. *Given ℓ number of bits to be offloaded, the offloading duration is $t = T$ for the optimal solution of Problem $\mathcal{P}2$-2.*

Proof: Upon introducing $\beta = p_J\theta + N_0^E$, this theorem can be proved by replacing α in (23) by β. ■

With the aid of Proposition 7 and Theorem 3, Problem $\mathcal{P}2$-2 can be reformulated as a single-variable problem for the case of a passive eavesdropper at a uniformly distributed location, i.e.

$$\mathcal{P}2\text{-}2\text{-}E: \arg\min_{\ell} C_U P_U(L-\ell) + \frac{\beta\left[1 - 2^{-\frac{\ell}{BT}}\right]T}{\frac{g^{U\to A}}{N_0^A}2^{-\frac{\ell}{BT}}\beta - g^{U\to E}}$$

s.t. (13a), (13b), (13d)

$$\ell \leq -BT(1-\epsilon)\log_2\left[\frac{\beta + p_O^{\max} g^{U\to E}}{\beta + \frac{p_O^{\max}\beta g^{U\to A}}{N_0^A}}\right]. \tag{34a}$$

Herein the constraints of (7a), (7b) and (7d) in Problem $\mathcal{P}2$ are transformed to (13a), (13b) and (13d), respectively, whilst (34a) is rewritten by (7e).

2) Convexity of Problem $\mathcal{P}2$-2-E: The convexity of Problem $\mathcal{P}2$-2-E is discussed in the following proposition.

Proposition 8. *Problem $\mathcal{P}2$-2-E is a convex problem.*

Proof: The process is similar to the proof of Proposition 5 by replacing α in (26) by β. ■

D. Optimal Offloading Strategy for the Secure UMEC

As illustrated in Section IV, Problem $\mathcal{P}1$-E, $\mathcal{P}2$-1-E and $\mathcal{P}2$-2-E are proved to be convex and hence there exist optimal solutions to the problems. Let us use $\mathcal{I} = \{1, 2\text{-}1, 2\text{-}2\}$ to represent the Problems $\mathcal{P}1$, $\mathcal{P}2$-1 and $\mathcal{P}2$-2, respectively, and $\bullet_i$, where $i \in \mathcal{I}$, to represent the variable of $\bullet$ in Problem i. Then, the optimal offloading strategy for the secure UMEC is formulated as follows.

- Offloading duration: According to Theorem 1, 2 and 3, the offloading duration is $t_i^{\text{opt}} = T$, where $i \in \mathcal{I}$, for the optimal solutions;
- Offloading computational load size: let us denote the feasible set of ℓ by $\ell \in [\ell_i^{\min}, \ell_i^{\max}]$, which is determined by the constraint functions of (13a), (13b), (13c) and (13d) for Problem $\mathcal{P}1$-E, (13a), (13b), (25a) and (13d) for Problem $\mathcal{P}2$-1-E, and (13a), (13b), (34a) and (13d) for Problem $\mathcal{P}2$-2-E. Moreover, we denote the solution to $\Phi_1(\ell) = 0$ by $\hat{\ell}_1^{\text{opt}}$, the solution to $\Phi_2(\ell) = 0$ by $\hat{\ell}_{2\text{-}1}^{\text{opt}}$ and the solution to $\Phi_2(\ell) = 0$, where α is replaced by β by $\hat{\ell}_{2\text{-}2}^{\text{opt}}$, which can be obtained from (35), (36) and (36), where α is replaced by β, respectively. Then, the optimal offloading data volume of ℓ_i^{opt} can be obtained differently in three specific cases:
  - If $\hat{\ell}_i^{\text{opt}} < \ell_i^{\min}$, then we have[2] $\ell_i^{\text{opt}} = \lceil \ell_i^{\min} \rceil$, where $i \in \mathcal{I}$;
  - If $\hat{\ell}_i^{\text{opt}} \in [\ell_i^{\min}, \ell_i^{\max}]$, then we have $\ell_i^{\text{opt}} = \underset{\ell_i^{\text{opt}} \in \{\lceil \hat{\ell}_i^{\text{opt}} \rceil, \lfloor \hat{\ell}_i^{\text{opt}} \rfloor\}}{\arg\min} E_{\text{tot}}\big(p_O(\ell_i^{\text{opt}}), \ell_i^{\text{opt}}, T\big)$, where $i \in \mathcal{I}$;
  - If $\hat{\ell}_i^{\text{opt}} > \ell_i^{\max}$, then we have $\ell_i^{\text{opt}} = \lfloor \ell_i^{\max} \rfloor$, where $i \in \mathcal{I}$.
- Offloading transmit power: the optimal offloading power of ${p_O}_i^{\text{opt}}$ can be obtained from (9) and (22) for $i = 1, 2\text{-}1$, respectively, while the asymptotically optimal power of ${p_O}_{2\text{-}2}^{\text{opt}}$ is obtained from (33), by substituting the values of p_J, t_i^{opt} and ℓ_i^{opt}.

V. Analysis of Zero, Full and Partial Offloading As Well As Overloaded Computation

In Section IV, we have provided the optimal solutions to the secure computation offloading problems from a mathematical perspective with the aid of strict proofs. To further augment our understanding, additional physically tangible insights are offered in this section. Specifically, we refer to the results obtained from the optimization in Section IV-D for $\ell = 0$, $\ell = L$ and $0 < \ell < L$ as the zero, full and partial offloading, respectively. Moreover, we use the terminology of computational overload to refer to the event, when the problems formulated in Section III cannot be solved owing to the UAV's limited hardware capability. In the following, the conditions both of selecting one of the three offloading options and of the computational overload event are explicitly detailed.

[2]Here we use $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$ to represent the floor and ceil operations, respectively.

A. Zero Offloading

The zero offloading scenario requires the following necessary condition and one of the following optional conditions to be simultaneously satisfied:

- Necessary condition: the UAV is capable of executing all the computational tasks subject to the latency constraint, i.e. we have $C_U L / D_U \leq T$, which corresponds to $\ell \geq 0$ in (13a).
- Optional conditions:
  - (a) the edge node is unable to carry out a bit calculation within the temporal constraint, i.e. $C_E / D_E > T$, which corresponds to $\ell < 1$ in (13b);
  - (b) the offloading is unable to transmit a bit within the maximum tolerable time interval subject to our specific security constraint, corresponding to $\ell < 1$ in (13c), (25a) and (34a);
  - (c) the edge node is capable of computing a bit and the offloading link is secure, and simultaneously the energy consumption of computing a bit at the UAV is lower than the energy cost of offloading a bit, i.e. we have:

$$C_U P_U \leq p_O(1) T, \tag{37}$$

where $p_O(1)$ can be obtained by substituting $\ell = 1$ into (9), (22) and (33) for Problems $\mathcal{P}1$, $\mathcal{P}2$-1 and $\mathcal{P}2$-2, respectively. The associated reason is explained as follows. When the energy consumption of offloading a bit is lower than that of computing it locally, the UAV would definitely offload the bit to the edge node. Hence zero offloading is not a valid option in this scenario.

B. Full Offloading

The activation of full offloading requires the necessary condition and one of the optional conditions to be simultaneously accommodated as follows:

- Necessary conditions: the edge node is capable of completing all the computational tasks subject to the latency constraint, i.e. $C_E L / D_E \leq T$, whilst L bits can be transmitted to the AP within the same time interval subject to the specific security constraints, which correspond to $\ell \leq L$ in (13b) and $\ell \leq L$ in (13c), (25a) and (34a), respectively.
- Optional conditions:
  - (a) the UAV is incapable of computing a bit within the temporal constraint, i.e. $C_U / D_U > T$, corresponding to $\ell \geq L$ in (13a);

$$\hat{\ell}^{\text{opt}} = -BT\log_2\left[\frac{2C_UP_U\gamma^{U\to A}\gamma^{U\to E}+\frac{\ln(2)}{B}\left(\gamma^{U\to A}-\gamma^{U\to E}\right)}{2C_UP_U\left(\gamma^{U\to A}\right)^2}\right.$$
$$\left.+\frac{\sqrt{\frac{4\ln(2)}{B}C_UP_U\gamma^{U\to A}\gamma^{U\to E}\left(\gamma^{U\to A}-\gamma^{U\to E}\right)+\frac{\ln^2(2)}{B^2}\left(\gamma^{U\to A}-\gamma^{U\to E}\right)^2}}{2C_UP_U\left(\gamma^{U\to A}\right)^2}\right]. \tag{35}$$

$$\hat{\ell}^{\text{opt}} = -BT\log_2\left[\frac{\frac{2C_UP_U\alpha g^{U\to A}g^{U\to E}}{N_0^A}+\frac{\alpha\ln(2)}{B}\left(\frac{g^{U\to A}}{N_0^A}\alpha-g^{U\to E}\right)}{\frac{2C_UP_U\alpha^2(g^{U\to A})^2}{(N_0^A)^2}}\right.$$
$$\left.+\frac{\sqrt{\frac{4C_UP_U\alpha g^{U\to A}g^{U\to E}}{N_0^A}\frac{\alpha\ln(2)}{B}\left(\frac{g^{U\to A}}{N_0^A}\alpha-g^{U\to E}\right)+\frac{\alpha^2\ln^2(2)}{B^2}\left(\frac{g^{U\to A}}{N_0^A}\alpha-g^{U\to E}\right)^2}}{\frac{2C_UP_U\alpha^2(g^{U\to A})^2}{(N_0^A)^2}}\right]. \tag{36}$$

– (b) the average energy consumption per bit of offloading all bits is lower than that of the combination of offloading $(L-1)$ bits and locally computing a bit, i.e.

$$\frac{C_UP_U+p_O(L-1)T}{L} > \frac{p_O(L)T}{L}, \tag{38}$$

where $p_O(\cdot)$ can be obtained from (9), (22) and (33) for Problem $\mathcal{P}1$, $\mathcal{P}2$-1 and $\mathcal{P}2$-2, respectively, and the associated reason is explained as follows. When the average energy consumption per bit for offloading all bits is higher than that for the combination of offloading $(L-1)$ bits and locally computing a bit, the associated bit would be processed at the UAV side and hence full-offloading cannot be achieved in this scenario.

C. Partial Offloading

The occurrence of partial offloading requires the necessary condition and one of the optional conditions to be simultaneously met, detailed as follows:

- Necessary condition: the joint computational ability of the UAV and of the edge node exceeds the total computational requirement of processing all L bits, subject to the latency constraint, i.e. $C_U(L-\ell)/D_U \le T$ and $C_E\ell/D_U \le T$, for an $\ell \in (0,L)$, whilst ℓ bits can be offloaded subjected to the security constraint. This condition corresponds to the situation, when there exists an intersection between $\{$(13a), (13b), (13d)$\}$ and (13c), (25a) and (34a) for Problem $\mathcal{P}1$, $\mathcal{P}2$-1 and $\mathcal{P}2$-2, respectively.
- Optional conditions:
  – (a) the UAV and the edge computing are incapable of completing the computational tasks satisfying the temporal constraint, respectively, i.e. we have $C_UL/D_U > T$ and $C_EL/D_E > T$, which indicates that $0 < \ell < L$ for (13a) and (13b);
  – (b) the energy consumption of locally computing a bit falls in the supplementary set of (37) and (38), i.e.

$$p_O(1)T < C_UP_U \le p_O(L)T - p_O(L-1)T, \tag{39}$$

where $p_O(\cdot)$ can be obtained from (9), (22) and (33) for the Problems $\mathcal{P}1$, $\mathcal{P}2$-1 and $\mathcal{P}2$-2, respectively.

D. Computational Overload

A computational overload may occur due to either of the following two conditions:

- The joint computational capability of both the UAV and the edge does not meet the requirement of computing all the bits within the latency constraint, i.e. $C_U(L-\ell)/D_U > T$ or $C_E\ell/D_U > T$, for any $\ell \in [0,L]$, which corresponds to the situation that there is no intersection between (13a) and (13b).
- The UAV is incapable of executing all the computational tasks within the temporal requirement, i.e. $C_UL/D_U > T$, whilst the offloading fails to transmit $L - TD_U/C_U$ bits within the maximum tolerable time interval subject to the security constraint, which corresponds to the situation that there is no intersection between (13a) and (13c).

VI. Numerical Results

In this section, we evaluate the performance of the proposed energy-efficient computation offloading strategy conceived for secure UMEC, by answering the following questions: 1) Which offloading option should be selected for optimal offloading? 2) What is the impact of different secrecy requirements on both the maximum number of bits that can be processed and the total energy consumption in UMEC? 3) What is the influence of the UAV's altitude and of the eavesdropper's location on the performance of total energy consumption and of the maximum number of bits that can be proceeded? The parameters are selected according to the existing industrial data sheets and standards. Their default values are listed in Table I.

A. Selection of Offloading Options

One of the three offloading options (i.e. zero offloading, partial offloading and full offloading) is selected for the non-overloaded computational scenarios after carrying out the proposed optimization as discussed in Section V. In this subsection, we aim for investigating the selection of these

Table I: Simulation Parameters

Description	Parameter and Value
AP Coverage Radius	$R = 100$ m
UAV Hovering Altitude	$d_1 \in [200, 400]$ m
The Location of Eve	$d_2 \in [0, R]$ m
Bandwidth	$B = 50$ MHz
UAV-to-Ground Channel [45]	$\kappa_1 = 1.42 \times 10^{-4}$ $\eta_1 = 2$
AP-to-Eve Channel [45]	$\kappa_2 = 1.42 \times 10^{-4}$ $\eta_2 = 3.5$ $\lambda = 1$
Noise [46]	$N_0^A = 1.99 \times 10^{-10}$ mW $N_0^E = 1.99 \times 10^{-10}$ mW
UAV Computation [21]	$L \in [0, 20]$ MB $D_U = 2.0$ GHz $P_U \in [0, 20 \times 10^{-11}]$ J/cycle $C_U = 500$ cycle/bit
Edge Computation	$D_E = 200$ GHz $C_E = 500$ cycle/bit
Power Consumption	$p_J \in [0, 3.5]$ W $p_O^{\max} = 250$ mW, $p_O^{\min} = 0$ mW
Temporal Constraint [21]	$T = 100$ ms
Secrecy Constraint [47]	$\epsilon \in [0.001, 0.1]$

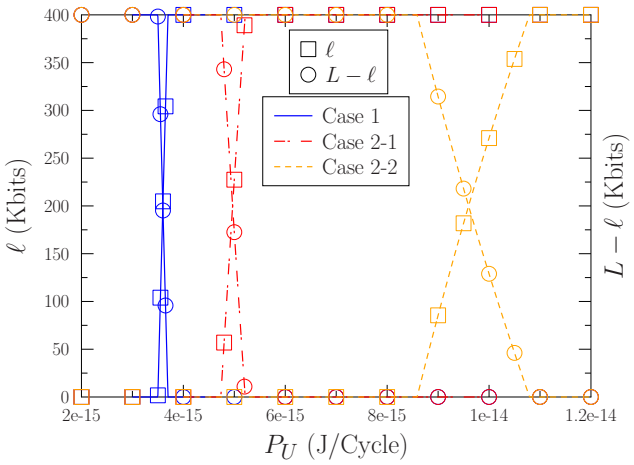

Figure 2: Locally computed number of bits ℓ and offloaded bit volume of $L-\ell$ versus the energy consumption for each CPU cycle of P_U, in Case 1, Case 2-1 and Case 2-2. The results are obtained according to the proposed strategy in Section IV-D. The parameters are set as follows; $L = 400$ Kbits; $p_J(\overline{p}_J) = 3.5$ W; $d_1 = 300$ m; $d_2 = 50$ m for Case 1 and 2-1; $\epsilon = 10^{-3}$ for Case 2-1 and 2-2. The remaining parameters are listed in Table I.

three offloading options under various numerical relationships between the local computation and the offloading in terms of the energy consumption per bit, whilst relying on the numerical results.

Fig. 2 depicts the results of our offloading strategy proposed in Section IV for the three considered scenarios [3] under various values of P_U, where the total number of bits to be computed is equal to the maximum number of bits that can be processed within the maximum tolerable time interval of T at the UAV, but below that in the edge node. It can be observed that zero offloading (i.e. $\ell = 0$) is selected when P_U is of a small value, which corresponds to the optional condition (b)

[3]Here $\overline{p}_J$ refers to the averaged jamming power for Case 1 while p_J refers to the constant jamming power for Case 2-1 and 2-2. In the following, we use p_J to represent both p_J and $\overline{p}_J$.

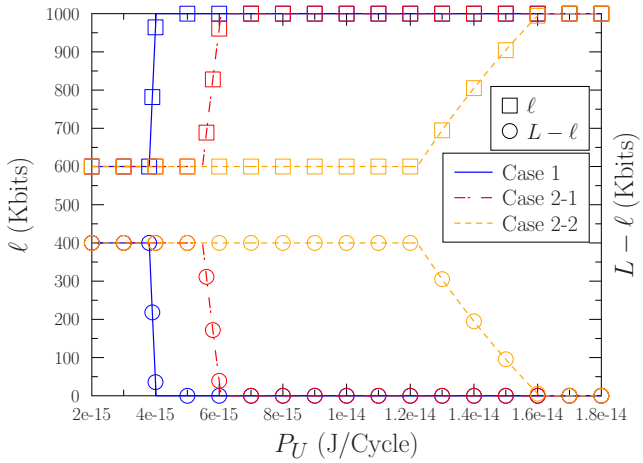

Figure 3: Locally computed number of bits ℓ and offloaded bit volume of $L-\ell$ versus the energy consumption for each CPU cycle of P_U, in Case 1, Case 2-1 and Case 2-2. The results are obtained according to the proposed strategy in Section IV-D. The parameters are set as follows: $L = 1000$ Kbits; $p_J = 3.5$ W; $d_1 = 300$ m; $d_2 = 50$ m for Case 1 and 2-1; $\epsilon = 10^{-3}$ for Case 2-1 and 2-2. The remaining parameters are listed in Table I.

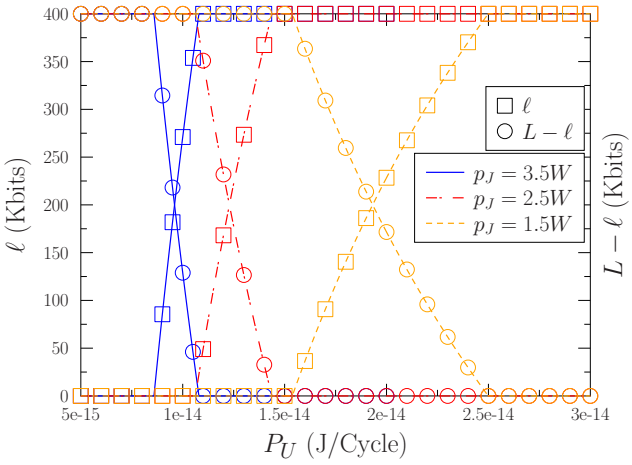

Figure 4: Locally computed number of bits ℓ and offloaded bit volume of $L-\ell$ versus the energy consumption for each CPU cycle of P_U parameterized by different jamming power of p_J in Case 2-2. The results are obtained according to the proposed strategy in Section IV-D. The parameters are set as follows: $L = 400$ Kbits; $d_1 = 300$ m; $\epsilon = 10^{-3}$. The remaining parameters are listed in Table I.

of Section V-A. When P_U increases, the computational tasks start to become offloaded to the edge node (i.e. $0 < \ell < L$, corresponding to the optional condition (b) of Section V-C), until reaching full offloading (i.e. $\ell = L$, corresponding to the condition (b) of Section V-B). Numerically, the cut-off values of P_U for zero, partial and full offloading reflected from Fig. 2 are also consistent with the analysis of (37), (39) and (38) in Section V, respectively. Moreover, it can be seen that partial and full offloading occur in conjunction with a smaller value of P_U in Case 1, compared to Case 2-1 and 2-2, which is because the AP is capable of exploiting the knowledge of the channel between itself and the eavesdropper in Case 1. Furthermore, Case 2-1 has a similar advantage over Case 2-2,

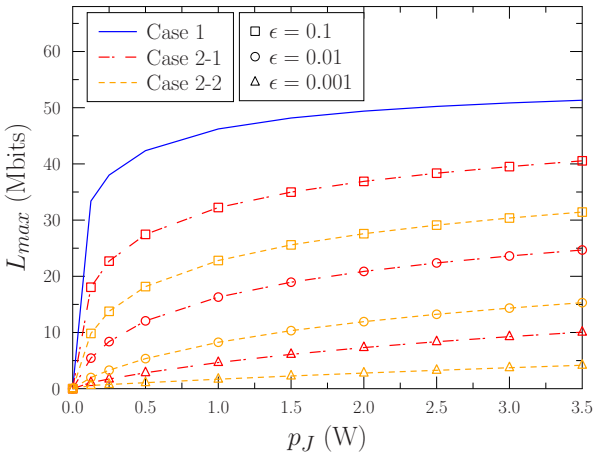

Figure 5: Simulation results of maximum computational load of $L_{\max}$ versus jamming power of p_J parameterized by different values of SOP requirement of ϵ in Case 1, Case 2-1 and Case 2-2. The parameters are set as follows: $P_U = 10 \times 10^{-11}$ J/Cycle; $d_1 = 300$ m; $d_2 = 50$ for Case 1 and 2-1. The remaining parameters are listed in Table I.

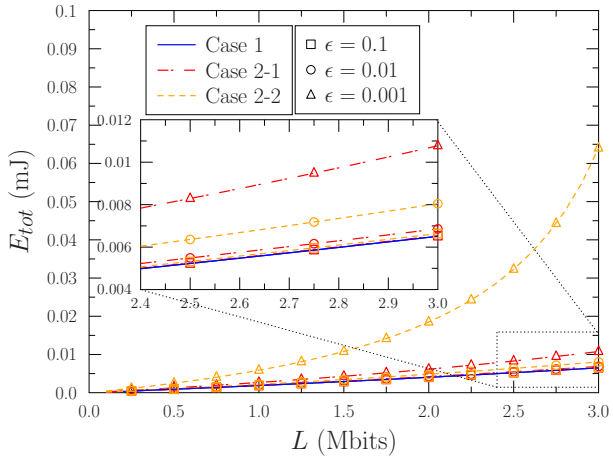

Figure 6: Simulation results of energy consumption of E_{tot} versus the computational load L, parameterized by different SOP requirement of ϵ in Case 1, Case 2-1 and Case 2-2. The parameters are set as follows: $p_J = 3.5$ W; $P_U = 10 \times 10^{-11}$ J/Cycle; $d_1 = 300$ m; $d_2 = 50$ for Case 1 and 2-1. The remaining parameters are listed in Table I.

which is because the eavesdropper has a higher probability to be roaming further away from the AP under the uniform distribution of Case 2-2. Hence the received jamming power at the eavesdropper is likely to be low. In this case, it imposes a higher energy consumption per bit for offloading, whereas partial and full offloading occur only when $C_U P_U$ exceeds the above-mentioned offloading energy consumption.

Fig. 3 presents the results of our offloading strategy proposed in Section IV for the three scenarios considered under various values of P_U, where the total number of bits to be offloaded is beyond the maximum number of bits that can be processed in the UAV, but below the maximum processing limitation of the edge node within the interval of T. It can be observed that zero offloading does not occur, regardless of the value P_U, which corresponds to the optional condition (a) for partial offloading in Section V-C. Moreover, comparing the results in Fig. 2 to those in Fig. 3, we can see that the cut-off value of P_U for full offloading increases along with the total amount of bits to be processed, which is because it requires a higher offloading energy consumption per bit to offload more bits within a certain time interval, while full loading happens only when the energy consumption per bit for local computation is higher than that for offloading.

Fig. 4 characterizes our offloading strategy for Case 2-2 for various values of P_U, where the jamming power of p_J is set differently. It can be observed that increasing p_J results in reduced cut-off values of partial and full offloading, which is because it requires lower offloading power of p_O to achieve the same secrecy capacity, when a higher jamming power is invoked, hence a lower cut-off P_U is obtained. This observation is consistent with the analysis of (38) and (39). Moreover, it can be seen that the difference of the cut-off values of P_U for partial and full offloading between the $p_J = 3.5$ W and $p_J = 2.5$ W scenarios is much smaller than that between $p_J = 2.5$ W and $p_J = 1.5$ W, which is explained as follows. When p_J is of a low value, the performance is jamming-power-limited. In other words, a slight increase on p_J results in a substantial increase of the secrecy offloading capacity defined in (4). By contrast, it requires a substantial increase of p_O to achieve the same secrecy offloading capacity.

B. Impact of SOP Requirements

The attainable computational performance can be characterized both by the maximum computational loads that can be processed within the affordable time interval and by the energy consumption imposed by processing a certain number of bits. These performance metrics are evaluated for our proposed offloading strategies, with a concern on the impact of secrecy capacity and of SOP.

Fig. 5 plots the maximum number of bits L_{max} that can be processed, using our proposed offloading strategy for Case 1, 2-1 and 2-2 for various values of both p_J and SOP requirement of ϵ. Our observations are as follows. Firstly, the advantage of Case 1 over Case 2-1 and 2-2 is an explicit benefit of exploiting the knowledge of the channel between the AP and the eavesdropper, while the advantage of Case 2-1 over Case 2-2 is granted by the fact that the eavesdropper, whose location obeys uniform distribution, has a higher probability of being located more than 50 m away from the AP. Secondly, for Case 2-1 and Case 2-2, a more stringent SOP requirement results in a reduction of L_{max}, because $p_O^{\max}$ is incapable of supporting a high secrecy capacity, whilst meeting the more stringent SOP requirement. Thirdly, the increase of jamming power results in a higher value of L_{max}, because a higher secrecy capacity can be achieved for a higher p_J, facilitating more bits to be offloaded to the edge node. Fourthly, the increase of p_J is capable of drastically increasing L_{max} when p_J is of a small value, whereas the increase of L_{max} becomes smaller when p_J reaches a certain threshold value, because the performance is jamming-power-limited when p_J is of a small value, whereas the performance becomes offloading-power-limited, when p_J reaches a high value.

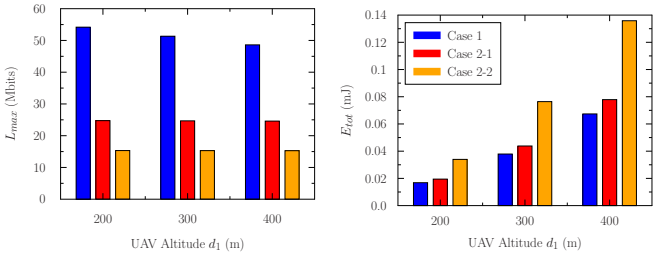

Figure 7: Simulation results of maximum computational load of $L_{\max}$ (left) and total energy consumption of E_{tot} (right) versus the UAV's altitude of d_1 in Case 1, 2-1 and 2-2. The parameters are set as follows: $p_J = 3.5$ W; $d_2 = 50$ m for Case 1 and 2-1; $\epsilon = 0.01$ for Case 2-1 and 2-2; $P_U = 10{\times}10^{-11}$ J/Cycle. For the right, $L = 10$ Mbits. The remaining parameters are listed in Table I.

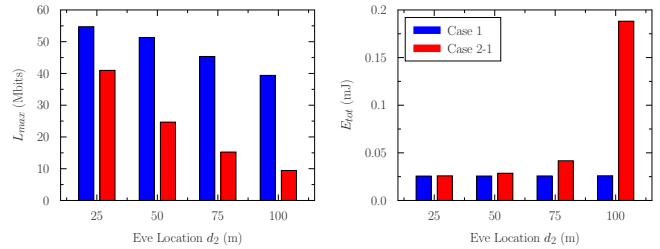

Figure 8: Simulation results of maximum computational load of $L_{\max}$ (left) and total energy consumption of E_{tot} (right) versus the eavesdropper's location of d_2 in Case 1 and 2-1. The parameters are set as follows: $p_J = 3.5$ W. $d_1 = 300$ m for Case 1 and 2-1; $\epsilon = 0.01$ for Case 2-1; $P_U = 10 \times 10^{-11}$ J/Cycle. For the right, $L = 8$ Mbits. The remaining parameters are listed in Table I.

Fig. 6 evaluates the total energy consumption of our proposed offloading strategy for Case 1, 2-1 and 2-2 for various values of computational loads, given a specific value of p_J. The observations are illustrated as follows. Firstly, a more stringent SOP requirement results in an increase of E_{tot}, because it requires higher offloading power to meet more stringent SOP requirements, when offloading a certain volume of computational bits. Secondly, E_{tot} of Case 2-2 exhibits a sharp increase within the L range of $1.5 - 3$ Mbits, which can be explained with the aid of Fig. 5. Explicitly, it is observed in Fig. 5 that when p_J reaches 3.5 W, the $L_{\max}$ value of Case 2-2 having $\epsilon = 10^{-3}$ gradually saturates a little above 3 Mbits, whereas $L_{\max}$ represented by the other curves tend to saturate much higher than 6 Mbits. In general, we require much higher offloading power for approaching the performance limit. Thirdly, the performance tends to degrade in the order of Case 1, 2-1 and 2-2, which is consistent with the trend observed in Fig. 5. Furthermore, The advantage of Case 1 over both Case 2-1 and Case 2-2 in terms of the total energy consumption is marginal when we set L as a small value while the advantage becomes increasingly substantial upon increasing L.

C. Impact of the UAV's Altitude and of the Eavesdropper's Location

Let us now characterize the performance of our proposed offloading strategy for different values of the UAV's altitude with the calibration of both L_{max} and E_{tot} in Fig. 7. It can be observed that the increase of the UAV's altitude results in the reduction of L_{max} and in the increase of E_{tot}, because the path loss between the UAV and the receiver on the ground decreases along with the increase of the UAV's altitude, hence the secrecy capacity is reduced. In this case, less bits can be offloaded given the values of p_J as well as p_O and more energy is expended by offloading a bit.

In Fig. 8, we show the L_{max} and E_{tot} performance of our proposed offloading strategy for different eavesdropper locations. It can be seen that the increase of the distance between the eavesdropper and the AP results in a reduction of L_{max} and the increase of E_{tot}. This is because the increase of d_2 leads to the reduction of the path loss between the AP and the eavesdropper, hence further reduces the jamming power received at the eavesdropper. In this case, the secrecy capacity is degraded. The sharp increase of E_{tot} for Case 2-1 at right of Fig. 8 is because it experiences a jamming-power-limited region when the eavesdropper is located at $d_2 = 100$ m, hence a much higher offloading power is required for processing the computational loads encountered.

VII. Conclusions

A beneficial architecture has been proposed for secure UMEC from the perspective of the PLS. We have formulated an energy-efficient computation offloading problem in the presence of both active and passive eavesdroppers. We then provided the optimal solutions to the problems formulated and analyzed the conditions of both the three offloading options and of the computational overload event from a physical perspective. The numerical results verified the accuracy of our mathematical analysis and quantified the performance of the proposed optimal offloading strategy for the secure UMEC under various scenarios considered.

Appendix

A. CDF Calculation of $g^{A\to E}$ when the Eavesdropper is at a Random Location

Consider that the location of the eavesdropper obeys the uniform distribution in the cell having a radius of R. Then the probability density function (PDF) of the distance between the AP and the eavesdropper is expressed as [48]

$$f_{d_2}(x) = \frac{2x}{R^2}, \qquad 0 \le x \le R. \tag{40}$$

Given $g^{A\to E}=\xi h^{A\to E}=\kappa_2 d_2^{-\eta_2}h^{A\to E}$, the CDF of $g^{A\to E}$ can be obtained as

$$\begin{aligned}F_{g^{A\to E}}(z)&=\int_0^R f_{d_2}(x)\int_0^{\frac{zx^{\eta_2}}{\kappa_2}} f_{h^{A\to E}}(y)\,\mathrm{d}y\,\mathrm{d}x\\&=\int_0^R f_{d_2}(x)F_{h^{A\to E}}\Big(\frac{zx^{\eta_2}}{\kappa_2}\Big)\,\mathrm{d}x\\&=\int_0^R \frac{2x}{R^2}\Big(1-e^{-\frac{\lambda z}{\kappa_2}x^{\eta_2}}\Big)\,\mathrm{d}x\\&=1-\frac{2\gamma\Big(\frac{2}{\eta_2},\frac{\lambda z R^{\eta_2}}{\kappa_2}\Big)}{R^2\eta_2\big(\frac{\lambda z}{\kappa_2}\big)^{\frac{2}{\eta_2}}}\\&>\frac{\lambda z R^{\eta_2}}{\kappa_2}\frac{2}{2+\eta_2}-\left(\frac{\lambda z R^{\eta_2}}{\kappa_2}\right)^2\frac{1}{2+2\eta_2},\end{aligned}\tag{41}$$

where $\gamma(a,x)=\int_0^x t^{a-1}e^{-t}\,\mathrm{d}t$ corresponds to the lower incomplete gamma function [49] and the inequality approximates the equality in the case of $\frac{\lambda z R^{\eta_2}}{\kappa_2}\le 1$ [50].

REFERENCES

[1] J. Wang, C. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo, "Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones," *IEEE Vehicular Technology Magazine*, vol. 12, pp. 73–82, Mar. 2017.

[2] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint.," *IEEE Communications Surveys and Tutorials*, vol. 18, pp. 2624–2661, Apr. 2016.

[3] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Communications Magazine*, vol. 54, pp. 36–42, May 2016.

[4] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives," *IEEE Internet of Things Journal*, vol. 3, pp. 899–922, June 2016.

[5] C. Luo, J. Nightingale, E. Asemota, and C. Grecos, "A UAV-cloud system for disaster sensing applications," in *Proceeding of 2015 IEEE VTC Spring)*, pp. 1–5, IEEE, 2015.

[6] S. Wan, J. Lu, P. Fan, and K. B. Letaief, "To smart city: Public safety network design for emergency," *IEEE Access*, vol. 6, pp. 1451–1460, 2018.

[7] E. Cusumano, "Emptying the sea with a spoon? Non-governmental providers of migrants search and rescue in the mediterranean," *Marine Policy*, vol. 75, pp. 91–98, 2017.

[8] S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang, "UAV-empowered edge computing environment for cyber-threat detection in smart vehicles," *IEEE Network*, vol. 32, pp. 42–51, Mar. 2018.

[9] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Communications Magazine*, vol. 55, pp. 128–134, Feb. 2017.

[10] O. Munoz, A. Pascual-Iserte, and J. Vidal, "Optimization of radio and computational resources for energy efficiency in latency-constrained application offloading," *IEEE Transactions on Vehicular Technology*, vol. 64, pp. 4738–4755, Oct. 2015.

[11] S. Barbarossa, S. Sardellitti, and P. Di Lorenzo, "Communicating while computing: Distributed mobile cloud computing over 5G heterogeneous networks," *IEEE Signal Processing Magazine*, vol. 31, pp. 45–55, June 2014.

[12] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, "Robust trajectory and transmit power design for secure uav communications," *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 9042–9046, Sep. 2018.

[13] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, pp. 2322–2358, Apr. 2017.

[14] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[15] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust multi-factor authentication for fragile communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, pp. 568–581, June 2014.

[16] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Annual Cryptology Conference*, pp. 465–482, Springer, 2010.

[17] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, pp. 1727–1765, Sep. 2016.

[18] Y. Wang, M. Sheng, X. Wang, L. Wang, and J. Li, "Mobile-edge computing: Partial computation offloading using dynamic voltage scaling," *IEEE Transactions on Communications*, vol. 64, pp. 4268–4282, Oct. 2016.

[19] S. Sardellitti, G. Scutari, and S. Barbarossa, "Joint optimization of radio and computational resources for multicell mobile-edge computing," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 1, pp. 89–103, Feb. 2015.

[20] X. Chen, L. Jiao, W. Li, and X. Fu, "Efficient multi-user computation offloading for mobile-edge cloud computing," *IEEE/ACM Transactions on Networking*, pp. 2795–2808, May 2016.

[21] C. You, K. Huang, H. Chae, and B.-H. Kim, "Energy-efficient resource allocation for mobile-edge computation offloading," *IEEE Transactions on Wireless Communications*, vol. 16, pp. 1397–1411, Mar. 2017.

[22] L. Wang, M. Guan, Y. Ai, Y. Chen, B. Jiao, and L. Hanzo, "Beamforming-aided NOMA expedites collaborative multiuser computational offloading," *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 10027–10032, Oct. 2018.

[23] Y. Mao, J. Zhang, and K. B. Letaief, "Dynamic computation offloading for mobile-edge computing with energy harvesting devices," *IEEE Journal on Selected Areas in Communications*, vol. 34, pp. 3590–3605, Dec. 2016.

[24] L. Gu, D. Zeng, S. Guo, A. Barnawi, and Y. Xiang, "Cost efficient resource management in fog computing supported medical cyber-physical system," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, pp. 108–119, Jan. 2017.

[25] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Communications*, vol. 24, pp. 134–139, Apr. 2017.

[26] Y. Shiu, S. Y. Chang, H. Wu, S. C. . Huang, and H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, pp. 66–74, Apr. 2011.

[27] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmwave networks using Matérn hardcore point processes," *IEEE Journal on Selected Areas in Communications*, vol. 36, pp. 1397–1409, July 2018.

[28] N. Zhao, F. Cheng, F. R. Yu, J. Tang, Y. Chen, G. Gui, and H. Sari, "Caching UAV assisted secure transmission in hyper-dense networks based on interference alignment," *IEEE Transactions on Communications*, vol. 66, pp. 2281–2294, May 2018.

[29] S.-W. Kim and S.-W. Seo, "Cooperative unmanned autonomous vehicle control for spatially secure group communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, pp. 870–882, May 2012.

[30] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Communications Letters*, vol. 6, pp. 310–313, Mar. 2017.

[31] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 9385–9392, Oct. 2018.

[32] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems.," *IEEE Transactions on Communications*, vol. 63, pp. 215–228, Jan. 2015.

[33] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities.," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 1637–1652, Sep. 2014.

[34] Q. Liu, J. Wu, P. Xia, S. Zhao, W. Chen, Y. Yang, and L. Hanzo, "Charging unplugged: Will distributed laser charging for mobile wireless power transfer work?," *IEEE Vehicular Technology Magazine*, vol. 11, pp. 36–45, Apr. 2016.

[35] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, pp. 148–153, Jan. 2018.

[36] C. Wang, H.-M. Wang, X.-G. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry

approach," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 2596–2612, May 2015.

[37] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1728–1740, Sep. 2013.

[38] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Joint transmit beamforming and artificial noise design for QoS discrimination inwireless downlink," in *Proceedings of 2010 IEEE ICASSP*, pp. 2562–2565, IEEE, 2010.

[39] J. Wang, J. Lee, F. Wang, and T. Q. Quek, "Jamming-aided secure communication in massive MIMO rician channels," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 6854–6868, Dec. 2015.

[40] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, pp. 2515–2534, June 2008.

[41] L. Yang, J. Cao, Y. Yuan, T. Li, A. Han, and A. Chan, "A framework for partitioning and execution of data stream applications in mobile cloud computing," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, pp. 23–32, Apr. 2013.

[42] Y. Zeng and R. Zhang, "Energy-efficient UAV communication with trajectory optimization," *IEEE Transactions on Wireless Communications*, vol. 16, pp. 3747–3760, June 2017.

[43] C. Pan, H. Ren, Y. Deng, M. Elkashlan, and A. Nallanathan, "Joint blocklength and location optimization for URLLC-enabled UAV relay systems," *IEEE Communications Letters*, vol. 23, Mar. 2019.

[44] FP7 European Project (2012), "Distributed computing, storage and radio resource allocation over cooperative femtocells (TROPIC)." http://www.ict-tropic.eu. [Online].

[45] H. He, S. Zhang, Y. Zeng, and R. Zhang, "Joint altitude and beamwidth optimization for UAV-enabled multiuser communications," *IEEE Communication Letter*, vol. 22, pp. 344–347, Feb. 2018.

[46] V. Sharma, M. Bennis, and R. Kumar, "UAV-assisted heterogeneous networks for capacity enhancement," *IEEE Communications Letters*, vol. 20, pp. 1207–1210, June 2016.

[47] Y. Wu, K. Guo, J. Huang, and X. S. Shen, "Secrecy-based energy-efficient data offloading via dual connectivity over unlicensed spectrums," *IEEE Journal on Selected Areas in Communications*, vol. 34, pp. 3252–3270, Dec. 2016.

[48] P. Omiyi, H. Haas, and G. Auer, "Analysis of TDD cellular interference mitigation using busy-bursts," *IEEE Transactions on Wireless Communications*, vol. 6, pp. 2721–2731, July 2007.

[49] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[50] G. Jameson, "The incomplete gamma functions," *The Mathematical Gazette*, vol. 100, no. 548, pp. 298–306, 2016.