This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2019.2959579, IEEE Wireless Communications Letters

Offloading Optimization for Low-Latency Secure Mobile Edge Computing Systems

Yi Zhou, Phee Lep Yeoh, Cunhua Pan, Kezhi Wang, Maged Elkashlan, Zhongfeng Wang, Branka Vucetic, and Yonghui Li

***Abstract*—This paper proposes a low-latency secure mobile edge computing (MEC) system where multiple users offload computing tasks to a base station in the presence of an eavesdropper. We jointly optimize the users' transmit power, computing capacity allocation, and user association to minimize the computing and transmission latencies over all users subject to security and computing resource constraints. Numerical results show that our proposed algorithm outperforms baseline strategies. Furthermore, we highlight a novel trade-off between the latency and security of MEC systems.**

I. Introduction

With the imminent deployment of 5G networks, a wide-range of advanced applications such as mobile gaming and virtual reality are rapidly emerging [1], [2]. A major challenge in realizing these computing-intensive immersive applications is the low computing capability of user devices. To alleviate computing capacity constraints and reduce latency, mobile edge computing (MEC) has emerged as a promising platform for users to offload computing tasks via high-speed wireless links to nearby macro base stations (MBS) equipped with high-capacity computing resources [3], [4]. In [5], the offloading latency of a multi-user MEC system was minimized by jointly optimizing the time slot and computing capacity. In [6], an energy-minimization framework focused on the computing capacity was developed for a two-tier MEC system.

Due to the open nature of wireless links, the security performance is another important consideration in wireless communication networks [7], [8]. To address this, physical layer security (PLS) techniques have been proposed to protect legitimate transmissions in MEC systems from being overheard by an eavesdropper. Recently in [9], the sum-energy of the computing tasks was minimized subject to a secrecy offloading rate and computation latency constraints.

In this paper, to achieve a low-latency secure MEC system, we jointly optimizing the users' transmit power, computing capacity allocation, and user association where only a subset of users offload to the MBS. We consider the users that are not associated with the MBS can execute their tasks locally with perfect security but may suffer from higher latency due to their limited computing capacity compared with the MBS. This results in a fundamental trade-off which is the main focus of this paper. We summarize our contributions as follows:

- We formulate a latency minimization problem of an MEC system by jointly optimizing the users' transmit power, computing capacity allocation, and user association subject to security and computing resource constraints.
- We design a low-complexity algorithm to solve this optimization problem by applying the block coordinate descent (BCD), successive convex approximation (SCA), and branch-and-cut methods.
- We show that our proposed algorithm outperforms baseline strategies and highlight a fundamental trade-off between latency and security via numerical results.

The rest of this paper is organized as follows. Section II introduces the system model. In Section III, we formulate the optimization problem and propose an algorithm to solve it. Section VI shows the simulation results and Section V concludes the paper.

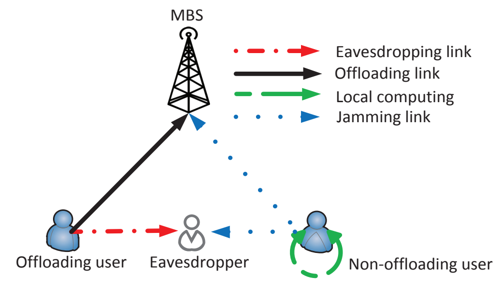

Fig. 1. System model.

II. System Model

We consider an MEC system with N users, one MBS and one eavesdropper, where the set of users is defined as $\mathcal{N}$. We consider the users can either process their tasks locally or offload their tasks via uplink channels to the MBS in the presence of an eavesdropper. To satisfy a given security constraint, we assume that the non-offloading users transmit jamming signals to interfere the eavesdropper.

A. Communication Model

Define $a_i = \{0, 1\}, i \in \mathcal{N}$ as the offloading user association variable where $a_i = 1$ when the i-th user offloads its computing task to the MBS, while $a_i = 0$ when the i-th user executes the computing task locally. We further define

This work was supported in part by ARC under Grant DP190100770, Grant DP150104019 and Grant DP190101988, in part by ARC Laureate Fellowship under Grant FL160100032.

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

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

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

Z. Wang is with the Key Laboratory of Networked Control Systems, Shenyang Institute of Automation, Chinese Academy of Sciences, China. (e-mail: wzf@sia.cn).

$\mathcal{N}_{as} = \{i|a_i = 1, \forall i \in \mathcal{N}\}$ as the set of associated users and h_{im} as the channel power gain between the i-th user and the MBS, which is perfectly known at each user. If the i-th user is associated with the MBS, the data rate of the uplink transmission is given by

$$r_{im} = \log_2\left(1 + \frac{p_i h_{im}}{\sum_{k\in\mathcal{N},k\neq i} p_k h_{km} + \sigma^2}\right), \forall i \in \mathcal{N}_{as}, \quad (1)$$

where p_i is the transmit power at the i-th user, σ^2 is the noise power, and $\sum_{k\in\mathcal{N},k\neq i} p_k h_{km}$ is the interference from all the other users except i.

We denote h_{ie} as the channel power gain between the i-th user and the eavesdropper, which can be imperfectly estimated from the local oscillator power leaked from the eavesdropper's front end [9]. To do so, we consider a bounded channel power gain uncertainty model given by $h_{ie} \in \mathcal{H}_{ie} \triangleq \{|h_{ie} - \tilde{h_{ie}}| \leq \delta\}$, where $\tilde{h_{ie}}$ is the corresponding estimated channel power gain and δ is the maximum estimation error. The data rate at the eavesdropper for eavesdropping the i-th offloading user can be written as

$$r_{ie} = \log_2\left(1 + \frac{p_i h_{ie}}{\sum_{k\in\mathcal{N},k\neq i} p_k h_{ke} + \sigma^2}\right), \forall i \in \mathcal{N}_{as}. \quad (2)$$

Based on (1) and (2), the secrecy capacity of the i-th offloading user associated with the MBS is given by

$$C_i = [r_{im} - r_{ie}]^+, \forall i \in \mathcal{N}_{as}, \quad (3)$$

where $[x]^+ \triangleq \max(x, 0)$. We note that the uncertainty of the eavesdropper's channel power gains makes it challenging to obtain a mathematically tractable expression of secrecy capacity in (3). To do so, we consider the eavesdropper's channel gains that result in the worst-case lower bound on the secrecy capacity of the i-th offloading user, which is given by

$$C_i^{lb} = \left[r_{im} - \underbrace{\log_2\left(1 + \frac{p_i h_{ie}^{max}}{\sum_{k\in\mathcal{N},k\neq i} p_k h_{ke}^{min} + \sigma^2}\right)}_{r_{ie}^{ub}} \right]^+, \quad (4)$$

where r_{ie}^{ub} is the upper bound of r_{ie} which can be achieved by satisfying $h_{ie}^{max} = \tilde{h_{ie}} + \delta$ and $h_{ke}^{min} = \tilde{h_{ke}} - \delta$.

B. Offloading Model

We denote D_i as the task size and F_i as the number of CPU cycles required to compute each bit of task D_i. In the following, we define the latency for local computing or offloading of task D_i at the i-th user.

1) Local Computing: Denote f_0 as the computing capacity at each user. If the i-th user executes its task locally, the local computing time T_i^L can be expressed as [6]

$$T_i^L = \frac{D_i F_i}{f_0}, \forall i \in \mathcal{N}/\mathcal{N}_{as}. \quad (5)$$

2) Offloading to MBS: For task offloading, the offloading transmission time for the i-th associated user is given by [6]

$$T_i^{Tr} = \frac{D_i}{B r_{im}}, \forall i \in \mathcal{N}_{as}, \quad (6)$$

where B is a fixed bandwidth and r_{im} is given in (1). Let f_{im} denotes the MBS computing capacity assigned to the i-th associated user. The computing time for the i-th offloading task at the MBS can be expressed as

$$T_i^O = \frac{D_i F_i}{f_{im}}, \forall i \in \mathcal{N}_{as}. \quad (7)$$

Finally, based on (5)-(7), the latency for executing the task of the i-th user is defined as

$$T_i = (1 - a_i)T_i^L + a_i(T_i^{Tr} + T_i^O), \forall i \in \mathcal{N}. \quad (8)$$

Similar to [9], we ignore the time required for transmitting the computation results from the MBS to the users.

III. Problem Formulation and Proposed Solution

Our aim is to minimize the overall latency consumption among all users by jointly optimizing the users' transmit power $\mathcal{P} \triangleq \{p_i, \forall i \in \mathcal{N}\}$, computing capacity allocation $\mathcal{F} \triangleq \{f_{im}, \forall i \in \mathcal{N}_{as}\}$, and user association $\mathcal{A} \triangleq \{a_i, \forall i \in \mathcal{N}\}$ subject to a minimum security constraint C_{min} for all associated users and a maximum computing requirement f_{max} for the MBS. By introducing a set of auxiliary variables $\hat{T} \triangleq \{\hat{T}_i, \forall i \in \mathcal{N}\}$, the optimization problem can be formulated as

$$\min_{\mathcal{P},\mathcal{F},\mathcal{A},\hat{T}} \sum_{i=1}^{N} \hat{T}_i \quad (9a)$$

$$\text{s.t.} \quad (1 - a_i)T_i^L + a_i(T_i^{Tr} + T_i^O) \leq \hat{T}_i, \forall i \in \mathcal{N} \quad (9b)$$

$$C_i^{lb} \geq C_{min}, \forall i \in \mathcal{N}_{as} \quad (9c)$$

$$\sum_{i=1}^{N} a_i f_{im} \leq f_{max} \quad (9d)$$

$$a_i = \{0, 1\}, \forall i \in \mathcal{N}. \quad (9e)$$

We note that problem (9) is non-convex and the non-convexity arises from the binary user association variables $\mathcal{A}$ and the non-convex constraints with respect to $\mathcal{P}$ in (9b) and (9c). To solve (9), we apply the BCD method [10] and decouple problem (9) into three subproblems to iteratively solve $\mathcal{P}, \mathcal{F}$, and $\mathcal{A}$.

A. Users' Transmit Power Subproblem

For any given $\mathcal{F}$ and $\mathcal{A}$, the users' transmit power of problem (9) can be optimized by solving

$$\min_{\mathcal{P},\hat{T}} \sum_{i=1}^{N} \hat{T}_i \quad (10a)$$

$$\text{s.t.} \; \underbrace{\log_2\left(\frac{\sum_{i\in\mathcal{N}} p_i h_{im} + \sigma^2}{\sum_{k\in\mathcal{N},k\neq i} p_k h_{km} + \sigma^2}\right)}_{r_{im}} \geq \frac{D_i}{B(\hat{T}_i - T_i^O)}, \forall i \in \mathcal{N}_{as} \quad (10b)$$

$$r_{im} - \underbrace{\log_2\left(\frac{p_i h_{ie}^{max} + \sum\limits_{k\in\mathcal{N},k\neq i} p_k h_{ke}^{min} + \sigma^2}{\sum_{k\in\mathcal{N},k\neq i} p_k h_{ke}^{min} + \sigma^2}\right)}_{r_{ie}^{ub}} \geq C_{min}, \forall i \in \mathcal{N}_{as}, \quad (10c)$$

where the constraints (10b) and (10c) correspond to (9b) and (9c), respectively. Due to the non-convexity of r_{im} and r_{ie}^{ub}, problem (10) is non-convex. In the following, we apply the SCA solution to solve (10). We begin by re-expressing r_{im} as

$$r_{im} = \underbrace{\log_2(\sum_{i\in\mathcal{N}} p_i h_{im} + \sigma^2)}_{\mathcal{L}} - \underbrace{\log_2(\sum_{k\in\mathcal{N},k\neq i} p_k h_{km} + \sigma^2)}_{\mathcal{I}_i}, \quad (11)$$

where both $\mathcal{L}$ and $\mathcal{I}_i$ are concave in terms of $\mathcal{P}$. Recall that any concave function is upper-bounded by its first-order Taylor

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2019.2959579, IEEE Wireless Communications Letters

expansion at any point. Thus, for $\mathcal{I}_i$, with the fixed users' transmit power in the m-th iteration, $p_k[m]$, we adopt the first-order Taylor expansion and derive the corresponding convex upper bound $\mathcal{I}_i^{ub}$ as

$$\mathcal{I}_i^{ub} = \log_2\Big(\sum_{k\in\mathcal{N},k\neq i} p_k[m]h_{km} + \sigma^2\Big) + \frac{\sum_{k\in\mathcal{N},k\neq i} h_{km}(p_k - p_k[m])}{(\sum_{k\in\mathcal{N},k\neq i} p_k[m]h_{km} + \sigma^2)\ln 2}. \tag{12}$$

Next, we reexpress r_{ie}^{ub} as

$$r_{ie}^{ub} = \underbrace{\log_2\Big(p_i h_{ie}^{max} + \sum_{k\in\mathcal{N},k\neq i} p_k h_{ke}^{min} + \sigma^2\Big)}_{\mathcal{S}_i} - \mathcal{W}_i, \tag{13}$$

where $\mathcal{W}_i = \log_2(\sum_{k\in\mathcal{N},k\neq i} p_k h_{ke}^{min} + \sigma^2)$. For $\mathcal{S}_i$, we apply similar approach to derive its convex upper bound $\mathcal{S}_i^{ub}$ as

$$\mathcal{S}_i^{ub} = \log_2\Big(p_i[m]h_{ie}^{max} + \sum_{k\in\mathcal{N},k\neq i} p_k[m]h_{ke}^{min} + \sigma^2\Big) + \frac{h_{ie}^{max}(p_i - p_i[m]) + \sum_{k\in\mathcal{N},k\neq i} h_{ke}^{min}(p_k - p_k[m])}{(p_i[m]h_{ie}^{max} + \sum_{k\in\mathcal{N},k\neq i} p_k[m]h_{ke}^{min} + \sigma^2)\ln 2}. \tag{14}$$

According to (12) and (14), the users' transmit power subproblem in the m-th iteration can be approximated as

$$\min_{\mathcal{P},\hat{T}} \sum_{i=1}^{N} \hat{T}_i \tag{15a}$$

$$\text{s.t.}\ \mathcal{L} - \mathcal{I}_i^{ub} \geq \frac{D_i}{B(\hat{T}_i - T_i^{O})}, \forall i \in \mathcal{N}_{as} \tag{15b}$$

$$\mathcal{L} - \mathcal{I}_i^{ub} - \mathcal{S}_i^{ub} + \mathcal{W}_i \geq C_{min}, \forall i \in \mathcal{N}_{as}, \tag{15c}$$

which is now a convex problem that can be efficiently solved by general convex optimization solvers.

B. Computing Capacity Allocation Subproblem

For any given $\mathcal{P}$ and $\mathcal{A}$, the computing capacity allocation can be optimized by solving the following problem

$$\min_{\mathcal{F},\hat{T}} \sum_{i=1}^{N} \hat{T}_i \tag{16a}$$

$$\text{s.t.}\quad f_{im} \geq \frac{D_i F_i}{\hat{T}_i - T_i^{Tr}}, \forall i \in \mathcal{N}_{as} \tag{16b}$$

$$\sum_{i=1}^{N} a_i f_{im} \leq f_{max}, \tag{16c}$$

where the constraint (16b) corresponds to (9b). We note that (16) is a convex optimization problem which can be efficiently solved by general convex optimizer.

C. User Association Subproblem

For any given $\mathcal{P}$ and $\mathcal{F}$, the user association variables can be optimized by solving the following problem

$$\min_{\mathcal{A},\hat{T}} \sum_{i=1}^{N} \hat{T}_i \tag{17a}$$

$$\text{s.t.}\quad a_i\xi_i + (1-a_i)M \geq C_{min}, \forall i \in \mathcal{N} \tag{17b}$$

$$(9b), (9d), (9e), \tag{17c}$$

where $\xi_i = r_{im} - r_{ie}^{ub}$ and M is a sufficiently large number which is greater than C_{min} to ensure that the constraint (17b) is satisfied when $a_i = 0$. Due to the linearity of the objective function and all constraints, problem (17) is a binary linear programming. We note that such problem can be efficiently solved by applying the branch-and-cut method, which combines the branch-and-bound and cutting plane algorithms to branch possible solutions and tight linear programming relaxations, respectively.

D. Proposed Iterative Algorithm

Our proposed algorithm is detailed in Algorithm 1. Denote $T(\mathcal{P},\mathcal{F},\mathcal{A})$ and $T^{up}(\mathcal{P},\mathcal{F},\mathcal{A})$ as the objective values of problem (9) and (15), respectively. The convergence of Algorithm 1 is proved as follows. First, in step 3 of Algorithm 1, since the first-order Taylor expansions in (12) and (14) are tight at the given local points $p_i[m]$ and $p_k[m]$, we have $T(\mathcal{P}[m],\mathcal{F}[m],\mathcal{A}[m]) = T^{ub}(\mathcal{P}[m],\mathcal{F}[m],\mathcal{A}[m])$ in (15). Notice that the users' transmit power solution $\mathcal{P}[m+1]$ for (15) is optimal with given $\{\mathcal{F}[m],\mathcal{A}[m]\}$, then it follows that

$$T^{ub}(\mathcal{P}[m],\mathcal{F}[m],\mathcal{A}[m]) \geq T^{ub}(\mathcal{P}[m+1],\mathcal{F}[m],\mathcal{A}[m]) \geq T(\mathcal{P}[m+1],\mathcal{F}[m],\mathcal{A}[m]), \tag{18}$$

where the last inequality holds since the objective value of (15) is the upper bound of the original problem in (10). Next, since $\mathcal{F}[m+1]$ and $\mathcal{A}[m+1]$ are the globally optimal solutions for (16) and (17), respectively, we have $T(\mathcal{P}[m+1],\mathcal{F}[m],\mathcal{A}[m]) \geq T(\mathcal{P}[m+1],\mathcal{F}[m+1],\mathcal{A}[m]) \geq T(\mathcal{P}[m+1],\mathcal{F}[m+1],\mathcal{A}[m+1])$. Therefore, we can conclude that

$$T(\mathcal{P}[m],\mathcal{F}[m],\mathcal{A}[m]) \geq T(\mathcal{P}[m+1],\mathcal{F}[m+1],\mathcal{A}[m+1]), \tag{19}$$

which shows that the algorithm yields a non-increasing sequence of the objective value. In addition, we see that the objective value is lower bounded by zero. Hence, the proposed algorithm is guaranteed to converge.

Algorithm 1 Proposed Iterative Optimization for Problem (9).

1: initialize $m = 0$, $\mathcal{P}[m], \mathcal{F}[m]$, and $\mathcal{A}[m]$.
2: **repeat**
3: Given $\{\mathcal{F}[m],\mathcal{A}[m]\}$, find the optimal users' transmit power $\mathcal{P}[m+1]$ by solving (15);
4: Given $\{\mathcal{P}[m+1],\mathcal{A}[m]\}$, find the optimal computing capacity allocation $\mathcal{F}[m+1]$ by solving (16);
5: Given $\{\mathcal{P}[m+1],\mathcal{F}[m+1]\}$, find the optimal user association $\mathcal{A}[m+1]$ by solving (17);
6: Update $m = m+1$;
7: **until** convergence.

IV. Simulation Results

We consider $N = 8$ users and one eavesdropper that are randomly distributed within a 400 m $\times$ 400 m square area. The MBS is fixed at the center of the square. We consider all channels are Rayleigh fading channels and assume that the average channel power gains follow the path loss model $\beta_1(d/d_0)^{-\alpha}$, where d is the distance between nodes, $\alpha = 3$ is the attenuation factor and $\beta_1 = -50$ dB corresponds to the reference path loss at distance of $d_0 = 1$ m. The maximum estimation error δ is set to be 10% of the corresponding path loss [9]. Other simulation parameters are shown in Table I.

Fig. 2 shows the convergence of Algorithm 1 with different local computing capacity f_0. The plot shows that our proposed algorithm quickly converges within six iterations. Furthermore, we find that the latency consumption decreases as f_0 increases. This is due to the fact that with higher local computing capacity at each user, the local computing latency will be reduced and further results in a lower overall latency consumption.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2019.2959579, IEEE Wireless Communications Letters

TABLE I
SIMULATION PARAMETERS [5], [10]

Noise power	$\sigma^2 = -110$ dB
Task size	$D_i \sim U[10, 40]$ KB
CPU cycles per bit	$F_i \sim U[10, 50]$ Kcycles/bit
Maximum MBS computing capacity	$f_{max} = 4$ GHz
User computing capacity	$f_0 = 0.4$ GHz
Minimum secrecy capacity	$C_{min} = 0.1$ bps/Hz
Transmission bandwidth	$B = 1$ MHz

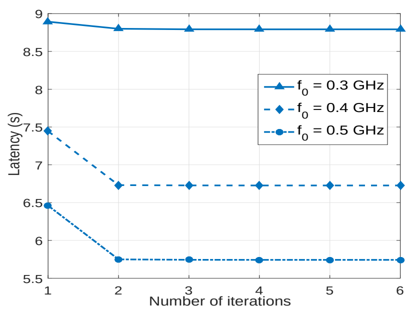

Fig. 2. Latency versus number of iterations with different local computing capacity f_0.

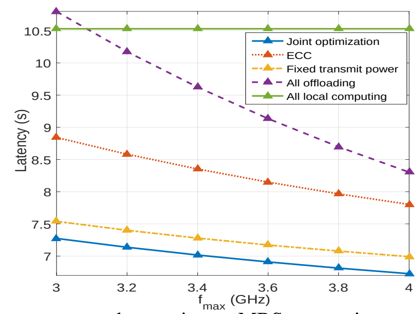

Fig. 3. Latency versus the maximum MBS computing capacity f_{max}.

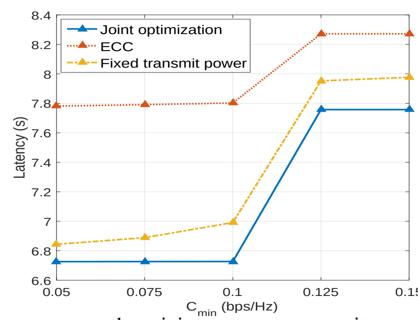

Fig. 4. Latency versus the minimum secrecy capacity requirement C_{min}.

Fig. 3 plots the latency versus the maximum computing capacity at MBS f_{max}. We compare our proposed joint optimization in Algorithm 1 with the following four benchmark schemes: 1) Fixed transmit power: We set $p_i = p_i[1], \forall i \in \mathcal{N}$ and all other variables are optimized using Algorithm 1; 2) Equal computing capacity (ECC): We assume that the MBS equally allocates the computing capacity to associated users and all other variables are optimized using Algorithm 1; 3) All offloading: All users offload their tasks to the MBS and other variables are optimized using Algorithm 1; 4) All local computing: All users choose to self-execute their tasks. Fig. 3 shows that our proposed joint optimization algorithm outperforms all other benchmark schemes over a wide range of f_{max}. Moreover, we observe that the latency is independent of f_{max} in "All local computing" scheme, while it keeps decreasing with increasing f_{max} for all other strategies. This is intuitive that with higher computing capacity at MBS, the computing capacity allocated to each associated user will be higher, which reduces the computing latency and results in a lower overall latency. In addition, we note that the secrecy performance in "All offloading" scheme cannot be guaranteed since all users are associated with the MBS even if they have a degraded channel gain compared to eavesdropper.

Fig. 4 shows the trade-off between the latency and the minimum secrecy capacity requirement C_{min}. It shows that our proposed joint optimization algorithm outperforms all other benchmark schemes over a wide range of C_{min}. Moreover, we note that the latency is an increasing function in terms of C_{min} and the remarkable jump, i.e., when $C_{min} = 0.125$ bps/Hz, corresponds to a decrease in the number of associated users. This is because when the secrecy capacity requirement is strict, more users choose to self-execute their packets in order to meet the security constraint, which results in a higher latency consumption due to the limited local computing capacity equipped on them.

V. CONCLUSIONS

We have proposed a new MEC framework to minimize the latency by optimizing the users' transmit power, computing capacity allocation, and user association subject to security and computing resource constraints. Numerical results have shown that our proposed algorithm outperforms baseline schemes and highlighted a trade-off between the latency and security of MEC systems.

REFERENCES

[1] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A Survey on Mobile Edge Computing: The Communication Perspective," in *IEEE Commun. Surveys Tuts,* vol. 19, no. 4, pp. 2322-2358, 4th Quart., 2017.

[2] M. Chen, W. Saad, and C. Yin, "Virtual Reality Over Wireless Networks: Quality-of-Service Model and Learning-Based Resource Management," in *IEEE Trans. Commun.,* vol. 66, no. 11, pp. 5621-5635, Nov. 2018.

[3] X. Tao, K. Ota, M. Dong, H. Qi, and K. Li, "Performance Guaranteed Computation Offloading for Mobile-Edge Cloud Computing," in *IEEE Wireless Commun. Lett.,* vol. 6, no. 6, pp. 774-777, Dec. 2017.

[4] K. Wang, P. Huang, K. Yang, C. Pan, and J. Wang, "Unified Offloading Decision Making and Resource Allocation in ME-RAN," in *IEEE Trans. Veh. Technol.,* vol. 68, no. 8, pp. 8159-8172, Aug. 2019.

[5] J. Ren, G. Yu, Y. Cai, and Y. He, "Latency Optimization for Resource Allocation in Mobile-Edge Computation Offloading," in *IEEE Trans. Wireless Commun.,* vol. 17, no. 8, pp. 5506-5519, Aug. 2018.

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

[7] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "Big Data Analysis-Based Secure Cluster Management for Optimized Control Plane in Software-Defined Networks," in *IEEE Trans. Netw. Service Manag.* vol. 15, no. 1, pp. 27-38, March 2018.

[8] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "FCSS: Fog Computing based Content-Aware Filtering for Security Services in Information Centric Social Networks," in *IEEE Trans. Emerg. Topics Comput.,* vol. PP, no. 99, pp. 11, 2017.

[9] J. Xu and J. Yao, "Exploiting Physical-Layer Security for Multiuser Multicarrier Computation Offloading," in *IEEE Wireless Commun. Lett.,* vol. 8, no. 1, pp. 9-12, Feb. 2019.

[10] Q. Wu, Y. Zeng, and R. Zhang, "Joint Trajectory and Communication Design for Multi-UAV Enabled Wireless Networks," in *IEEE Trans. Wireless Commun.,* vol. 17, no. 3, pp. 2109-2121, March 2018.