Computer Communications 194 (2022) 180–188

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Physical-layer security based mobile edge computing for emerging cyber physical systems

Lunyuan Chen [a], Shunpu Tang [b], Venki Balasubramanian [c,*], Junjuan Xia [b,*], Fasheng Zhou [a], Lisheng Fan [b,*]

[a] School of Electronics and Communication Engineering, Guangzhou University, Guangzhou 510006, China
[b] School of Computer Science, Guangzhou University, Guangzhou 510006, China
[c] School of Science, Engineering and Information Technology, Federation University, Mount Helen VIC 3350, Australia

ARTICLE INFO

Keywords:
Cyber physical systems
Mobile edge computing
Secure communication
Eavesdropping

ABSTRACT

This paper studies a secure mobile edge computing (MEC) for emerging cyber physical systems (CPS), where there exist K eavesdroppers in the network, which can threaten the task offloading. These K eavesdroppers can work either in a colluding mode where they cooperate to decode the secret message, or in a non-colluding mode where the eavesdroppers decode the message individually. For both eavesdropping nodes, we design the secure MEC system by devising a computation offloading ratio, transmit power and computational capability allocation to optimize the system performance mainly measured by the latency. In particular, a novel deep reinforcement learning (DRL) together with convex optimization (DRCO) is proposed, where the DRL is used to find a proper solution to the offloading ratio, while the convex optimization is implemented to solve the allocation of transmission power and computational capability. Simulation results show that the proposed DRCO method is superior to other conventional methods, and can provide a guaranteed secrecy and latency.

1. Introduction

Recent years have witnessed the emergence of advanced perceptive technologies and communication protocols [1–3], more and more devices have abilities of environmental awareness, information processing, and data transmission [4–6], promoting the emergency of a novel platform named cyber–physical systems (CPS). CPS consists of kinds of wireless sensors, mobile devices, and control systems, which aim to provide intelligence services by combining the technologies of computing, communication, and control [7–10].

This facilitates the progress of intelligent transportation, smart cities, building automation, emergency management, and such applications [11]. However, how to process the massive data generated at the edge of the CPS still faces some challenges due to the decentralized characteristic of data, limited computational power, and vulnerable wireless channel. On the one hand, on-device computing leads to a large computational latency and energy consumption, which is incompatible with the latency-sensitive applications and devices powered by batteries. On the other hand, it is arduous to transfer data and computing operations to the cloud server through wireless networks. Although this strategy can obtain abundant computational resources, there is a phenomenon that the communication latency is dominant in the system latency, and even exceeds the latency of on-device computing [12,13]. Besides, the cloud server has to suffer a lot of stress, due to massive communication and computation.

Fortunately, mobile edge computing (MEC) was presented as a novel computational paradigm to address this issue, which aims to achieve faster response and lower on-device energy consumption than the conventional schemes by deploying computational access points (CAPs) as close to the data sources as possible [14]. Moreover, the local devices can transfer a part of their computational tasks to the close CAPs by reasonable offloading decisions. Many previous works have made the breakthrough in this topic [15].

For example, in [16], the authors investigated mobile edge computing aided vehicular networks, and proposed a collaborative computation offloading and resource allocation optimization scheme. In [17], a MEC framework in the presence of co-channel interference was investigated, where some analytical and asymptotic expressions of system outage probability were derived the characterize the rate and latency. The federated edge learning was studied in a MEC network, where the system has jointly optimized the computational capability and wireless bandwidth based on deep reinforcement learning (DRL) [18,19].

However, The heterogeneity and complexity of CPS components have provided substantial challenges for the security and privacy preservation of CPS, especially in the scenarios of MEC with CPS. The

* Corresponding authors.
E-mail addresses: 2112019037@e.gzhu.edu.cn (L. Chen), tangshunpu@e.gzhu.edu.cn (S. Tang), v.balasubramanian@federation.edu.au (V. Balasubramanian), xiajunjuan@gzhu.edu.cn (J. Xia), zhoufs@gzhu.edu.cn (F. Zhou), lsfan@gzhu.edu.cn (L. Fan).

https://doi.org/10.1016/j.comcom.2022.07.037
Received 10 November 2021; Received in revised form 30 June 2022; Accepted 20 July 2022
Available online 25 July 2022
0140-3664/

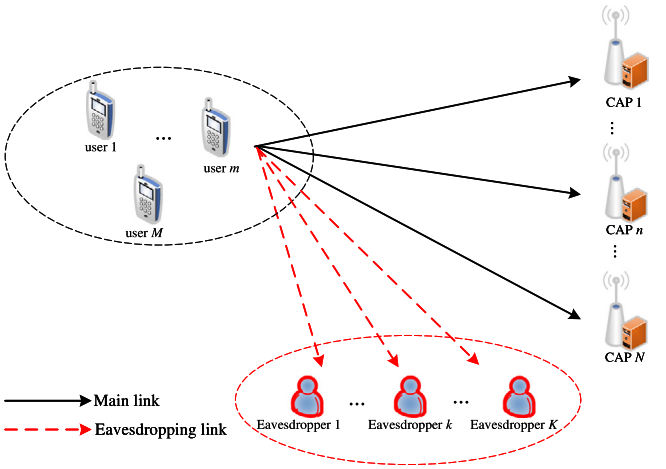


Fig. 1. Secure multi-access MEC network with multiple eavesdroppers.

physical-layer attacks, including jamming and eavesdropping, would seriously threaten the security of wireless communication in MEC, leading to a lower secure data transmission rate [20]. To tackle this physical-layer security problem, the authors in [21] investigated a secure MEC framework amongst a large number of eavesdroppers, where an analytically optimal offloading strategy was investigated as a method to enhance the transmission security. In [22], the authors studied the MEC system under imperfect channel state information of the eavesdroppers, and they jointly optimized the offloading ratio and subcarriers allocation to reduce the total energy consumption for the whole user set, under the limitations of secure transmission rate and computation latency.

In this paper, we study a secure MEC for emerging CPS, where there exist K eavesdroppers in the network, which can threaten the task offloading. These K eavesdroppers can work either in a colluding mode where they cooperate to decode the secret message, or in a non-colluding mode where the eavesdroppers decode the message individually. For both eavesdropping nodes, we design the secure MEC system by devising an offloading strategy and resource allocation so as to optimize the system latency. In particular, a novel DRL combined with convex optimization (DRCO) is proposed, where DRL is used to find a proper solution to the offloading ratio, while the convex optimization is implemented to solve the allocation of transmission power and computational capability. The following are the paper's major contributions:

- We study a secure MEC for CPS in the case of K malicious eavesdroppers, in which multiple eavesdroppers work either in a colluding mode where they cooperate to decode the secret message, or in a non-colluding mode where the eavesdroppers decode the message individually.
- To ensure secure and efficient MEC, we formulate an optimization objective function by jointly optimizing the offloading decision and resource allocation of the MEC network.
- We propose a DRL combined with convex optimization method to minimize the system latency, where the DRL is used to find a proper solution to the offloading ratio, while the convex optimization is implemented to solve the allocation of transmission power and computational capability.
- Simulations show that the DRCO method can outperform other approaches that are commonly used, and can decrease the latency of the MEC system by 32.5% even under up to 15 colluding eavesdroppers, which verifies the validity of the proposed method.

This paper's remaining sections are arranged as follows. Section 2 summarized some more related works and existing works about computation offloading and physical-layer security. Section 3 proposed the secure multi-access MEC system model for emerging CPS and gave its problem formulation. Section 4 presents the proposed DRL combined with convex optimization method for task offloading and resource allocation. The simulation results and discussions of DRCO and other methods are presented in Section 5, and in Section 6, we came to the conclusion.

2. Related works

Various types of computation offloading difficulties have been addressed in the existing literature. Specifically, some existing works investigated the full computation offloading problem, while other recent works, such as [13,22], addressed the partial computation offloading problem. These studies often focus on the partial computation offloading of a single-CAP system. For example, the authors in [23,24] studied how to devise an analytical solution to the offloading and resource allocation for the MEC networks. However, they did not consider the physical-layer attack, which would seriously threaten wireless communication security in MEC. Compared to these existing works, our work considers partial offloading for multiple users and multiple CAPs system under physical-layer attack.

Physical-layer security in MEC networks has received much scholarly attention. For example, the work in [25] presented a mobile offloading system based on reinforcement learning to protect edge computing from jamming and interference. In [26], a physical authentication system is proposed to prevent rogue edge attackers from faking signals to attack MEC networks. There has been more recent work [27] that proposes a method to achieve the optimal beamforming policy against the eavesdropper in a visible light communication channel. However, these works fail to consider multiple eavesdroppers attacking the wireless communication either in a colluding mode or in a non-colluding mode, which would severely deteriorate the system performance. Besides, this paper proposes a new approach to reduce the search space in the reinforcement learning algorithm where the task offloading decision generated in every reinforcement learning step is used to calculate the analytical resource allocation decision as opposed to all using reinforcement learning.

3. System model and problem formulation

According to Fig. 1, we assume a secure multi-access MEC network for emerging CPS with multiple mobile users and multiple CAPs, with the presence of multiple eavesdroppers. Firstly, eavesdropping is one of the most representative attacks in the wireless environment, which can severely deteriorate the system's performance. Secondly, eavesdropping is a passive attack, which has a lower cost and is more difficult to detect compared with other active attacks. Therefore, it is one of the most common attacks in the wireless environment. Thirdly, our research on eavesdropping attacks can provide an important reference for the research of other attack modes. Due to these reasons, we choose to study eavesdropping mode in the considered MEC networks. $\mathcal{M} \triangleq \{1, 2, \ldots, M\}$ is the user set, where the number of the users is M, and $\mathcal{N} \triangleq \{1, 2, \ldots, N\}$ is CAP set, where the number of the CAPs is N. In this multi-access MEC system, each user $m \in \mathcal{M}$ has a computation-intensive and latency-sensitive task I_m with a corresponding task size of $|I_m|$ to compute. Therefore, each user can conduct both local computing with its limited computational capability and choose to partially offload its task to different CAPs with more powerful computational capability to perform a faster computation. Specifically, we consider that mobile user m can offload the subtasks to various CAPs through frequency division multiple access (FDMA) simultaneously. At the same time, there are K eavesdroppers in the network, collecting the radio signals from each user, threatening the security of task offloading. Note that the

above system model can be applied to different application scenarios. Specifically, for the application scenarios such as smart healthcare and smart home in the presence of malicious unmanned aircraft vehicle (UAV) eavesdropping the personal privacy information, the considered MEC networks can be used to protect data security and ensure rapid service. Moreover, the considered MEC system can also be applied in mobile cellular networks based video transmission and navigation in the presence of eavesdroppers to provide secure and rapid service. The following subsections will be discussed about the local computation model and multi-access offloading model, respectively, and we will give the formulation of the task offloading and resource allocation optimization problem for the considered MEC in CPS.

3.1. Local computation model

For the local computation model, we use $\alpha_{m,0}$ to denote the local computational ratio of mobile user m. Therefore, the corresponding local computation latency of user m is given by

$$T_m^{\text{local}} = \frac{\alpha_{m,0} l_i \omega}{f_m}, \tag{1}$$

where f_m denotes the fixed local processing capability of user m, as measured by the local CPU cycle frequency, and ω is the needed CPU cycles to process one bit of task.

3.2. Multi-access offloading model

In this subsection, we introduce the multi-access task offloading under malicious attacks of multiple eavesdroppers, which includes the data transmission part and the edge processing part. Specifically, In the data transmission part, mobile user m will offload parts of its task to several CAPs while suffering eavesdroppers' overhearing. In order to perform secure offloading, we use physical-layer secure method to guarantee secure wireless communication against malicious eavesdropping. According to the principle of physical-layer security, the achievable secure data rate without information leakage is called secure data transmission rate, which can be given by

$$R_{m,n}^{\text{sce}} = W \left(\log_2 \left(1 + \frac{P_{m,n}|h_{m,n}|^2}{\sigma^2} \right) - \log_2 \left(1 + \frac{P_{m,n}|h_{m,e}|^2}{\sigma^2} \right) \right)^+, \tag{2}$$

where W denotes the communication bandwidth of the link between mobile client m and CAP $n \in \mathcal{N}$, $h_{m,n} \in \mathbb{C}$ denotes the corresponding instantaneous channel parameter, $h_{m,e} \in \mathbb{C}$ is the channel parameter of the eavesdropping link, and $P_{m,n}$ denotes the transmission power allocated to the channel between mobile client m and CAP n. What is more, σ^2 is the variance of additive white Gaussian noise (AWGN) received at the CAPs and eavesdroppers, where the noise effect on the wireless communication system [28–30]. We can see from (2) that the existence of eavesdropping affects the original wireless transmission rate and therefore deteriorates the performance of the MEC system. According to the model of multiple eavesdroppers, these K eavesdroppers can work either in a colluding mode where they cooperate to decode the secrecy message and maximize the eavesdropped ratio of the task, or in a non-colluding mode, where they decode the message individually without sharing the received information. Notably, the above model is able to cover the case with only one eavesdropper. Specifically, for the non-colluding eavesdropping scenarios, the equivalent channel gain of user m's eavesdropping links is given by

$$|h_{m,e}|^2 = \max\{|h_{m,e_1}|^2, |h_{m,e_2}|^2 \dots, |h_{m,e_K}|^2\}, \tag{3}$$

where $h_{m,e_k} \in \mathbb{C}$ denotes the channel parameter between the kth eavesdropper and user m. In contrast, for the colluding eavesdropping scenarios, the equivalent channel gain of user m's eavesdropping link can be given by

$$|h_{m,e}|^2 = \sum_{k=1}^{K} |h_{m,e_k}|^2. \tag{4}$$

Then, the latency of user m securely transmitting $\alpha_{m,n}$ part of l_m to CAP n can written as

$$T_{m,n}^{\text{tran}} = \frac{\alpha_{m,n} l_m}{R_{m,n}^{\text{sce}}}. \tag{5}$$

Upon receiving the offloading $\alpha_{m,n}$ part of the task, CAP n computes the subtasks with a more significant computational capability, and we consider the computation resources at the CAP can be allocated to the subtasks from different users. Thus, the corresponding execution latency at the CAP can be written as

$$T_{m,n}^{\text{Cap}} = \frac{\alpha_{m,n} l_m \omega}{F_{m,n}}, \tag{6}$$

where $F_{m,n}$ is the computational capability allocated to user m's $\alpha_{m,n}$ part of the task at CAP n, which should meet the constraint $\sum_{m=1}^{M} F_{m,n} \le F_n^{\text{total}}, \forall n \in \mathcal{N}$, where F_n^{total} is the total computational capability of CAP n.

Note that the size of the computational result is much smaller than the original task, we dismiss the time needed for users' downloading the result from the CAPs. Thus, we can get the offloading latency by jointly considering the subtasks offloading and CAP's computation, given by

$$T_{m,n}^{\text{offl}} = T_{m,n}^{\text{tran}} + T_{m,n}^{\text{Cap}}. \tag{7}$$

By using FDMA for offloading and computational capability allocation, multiple subtasks can be offloaded and computed simultaneously, and thus the total computational latency for user m can be given by [31]

$$T_m^{\text{total}} = \max\{T_m^{\text{local}}, T_{m,1}^{\text{offl}}, T_{m,2}^{\text{offl}}, \dots, T_{m,N}^{\text{offl}}\}. \tag{8}$$

For the secure multi-access MEC network, the total system latency can be decided by the last user who finishes its task, given by

$$T^{\text{total}} = \max\{T_1^{\text{total}}, T_2^{\text{total}}, \dots, T_M^{\text{total}}\}. \tag{9}$$

3.3. Problem formulation

In this paper, we jointly formulate an optimization of users' task offloading decision, transmission power allocation, and CAPs' computational capability allocation, and our objective is to minimize the total system latency while ensuring secure and successful task computing in the multi-access MEC network, given by

$$(\text{P1}): \min_{\{\alpha,P,F\}} T^{\text{total}}, \tag{10a}$$

$$\text{s.t.} \quad C_1: \alpha_{m,n} \in \left\{ \frac{i}{L_s} \right\}, 0 \le i \le L_s, \quad \forall m \in \mathcal{M}, n \in \mathcal{N}, \tag{10b}$$

$$C_2: \sum_{n=0}^{N} \alpha_{m,n} = 1, \forall m \in \mathcal{M}, \tag{10c}$$

$$C_3: \sum_{n=1}^{N} P_{m,n} \le P_m^{\text{total}}, \forall m \in \mathcal{M}, \tag{10d}$$

$$C_4: \sum_{m=1}^{M} F_{m,n} \le F_n^{\text{total}}, \forall n \in \mathcal{N}, \tag{10e}$$

where constraint C_1 represents that each user's task can be divided into L_s subtasks, and each user chooses integer multiple of a subtask as the offloading ratio to offload to several CAPs. Constraint C_2 denotes that the cumulative offloading ratio of all users would equal 1. Note that the transmission power at each user is limited, and constraint C_3 makes sure that the transmission power allocated to different channels will not exceed the total transmission power. Analogously, constraint C_4 ensures

that the computational resources at each CAP are limited. Due to the discrete offloading ratio and other complicated operations, the problem (P1) is a non-convex optimization problem that is generally difficult to be solved by conventional optimization methods, such as convex optimization. It is reasonable to use DRL to solve the multi-access problem, but joint optimization of offloading strategy and resource allocation will significantly increase the state space and action space of DRL algorithm, leading to a massive number of training steps and a long time taken to converge. To deal with this issue, we introduce a novel DRL combined with convex optimization (DRCO) in the next section.

4. Offloading decision and resource allocation

The implementation details of the proposed DRCO method for the considered system, which can be described in the following two stages is presented in this section. We firstly exert DRL algorithm to obtain the offloading decision at each time slot. After that, a convex optimization method well be utilized to get the closed-form solution of the transmission power and computational capability for the given offloading decision.

4.1. DRL based offloading strategy

In recent years, many intelligent algorithms have been proposed to solve the problem of system resource allocation in wireless networks [32,33]. As a typical intelligent algorithm, the DRL is used to solve the task offloading decision for the considered multi-access system, where we use a Markov decision process (MDP) to form the formulation of the process. We define $S = \{\mathbf{L}_t, \mathbf{P}_t, \mathbf{F}_t, \boldsymbol{\alpha}_t\}$, where $\mathbf{L}_t = [l_1(t), l_2(t), \dots, l_M(t)]$ is the task size vector of M users, $\mathbf{P}_t = [P_1(t), P_2(t), \dots, P_M(t)]$ is the transmission power vector of M users, $\mathbf{F}_t = [F_1(t), F_2(t), \dots, F_N(t)]$ is the computational capability vector of N CAPs, and $\boldsymbol{\alpha}_t = [\alpha_{1,0}(t), \alpha_{1,1}(t), \dots, \alpha_{M,N}(t)]$ denotes the partial offloading rate. Aiming to represent the offloading decision, we define $A = \{\rho^m_{n,n^*} | m \in \mathcal{M}, n, n^* \in \{0, \mathcal{N}\}\}$, where ρ^m_{n,n^*} denotes the action of reducing user m's offloading ratio to CAP n by β and increasing offloading ratio by β to CAP n^*, where β is the ratio of one subtask. In particular, if the action causes an offloading rate violating the constraints C_1 and C_2, the agent will choose another action instead of executing this illegal one. Since we intend to jointly optimize the total latency, the corresponding reward r_t in MDP can be defined by

$$r_t = \begin{cases} \eta_1, & \text{if } T^{\text{total}}(t) < T^{\text{total}}(t-1), \\ -\eta_2, & \text{if } T^{\text{total}}(t) = T^{\text{total}}(t-1), \\ -\eta_3, & \text{if } T^{\text{total}}(t) > T^{\text{total}}(t-1), \end{cases} \tag{11}$$

where $T^{\text{total}}(t)$ is the total system latency at time slot t while $T^{\text{total}}(t-1)$ represents the total system latency at time slot $t-1$. η_1, η_2 and η_3 are three positive values. Specifically, The reward function shows that if the action of changing offloading ratio leads to lower system latency, the DRL agent will receive a positive reward η_1. In contrast, if the total system latency remains unchanged, the agent achieves a negative reward $-\eta_2$, and if the total system latency gets worse, the agent gets a more negative reward $-\eta_3$.

Under such setting, we can formulate the Q function $Q(s, a)$ used to evaluate the expected cumulative rewards with a specific policy π, and we can define the optimal one as $Q^*(s, a)$. Therefore, we get the optimal offloading policy by [34,35]

$$\pi^* = \arg\max_{\pi} Q^*(s, a), \tag{12}$$

Notably, in practical reinforcement learning, an action will be made based on the exploration using ϵ-greedy policy to gather more information and avoid getting into the local optimum, shown by [36–38]

$$a^* = \begin{cases} \arg\max_{\pi} Q^*(s, a), & \epsilon \\ \text{Randomly choose from } A, & \text{otherwise} \end{cases} \tag{13}$$

Due to the curse of dimensionality, Q table based reinforcement learning such as Q learning may not be able to handle a large number of environment states and actions. Therefore, we turn to use deep Q-Networks (DQN) [39], since it can deal with the case with a large number of environment states.

In further, we use the temporal-difference (TD) method to help approximate the Q function after every time slot, which can be written as

$$Q(s_t, a_t; \theta) = r_t + \gamma \max_{a_{t+1}}(Q(s_{t+1}, a_{t+1}; \theta)), \tag{14}$$

where θ is the evaluation Q network parameter, and γ is the coefficient indicating the relevance of cumulative reward. In general, the DQN's loss is to calculate the loss between the optimal value and the evaluated value. So a duplicate network is deployed to compute the TD target, called the target network. It is worth noting that we will synchronize these two networks on a regular basis after a set period of time, so the target network will be replaced every certain rounds. Therefore, we can give the loss function as follows:

$$Loss_t = (r_t + \gamma \max_{a_{t+1}}(\hat{Q}(s_{t+1}, a_{t+1}; \hat{\theta})) - Q(s_t, a_t; \theta))^2, \tag{15}$$

where $\hat{Q}$ denotes the target network's Q function and $\hat{\theta}$ denotes its parameter. The target Q value of executing action a_{t+1} at state s_{t+1} is denoted by the notation $\hat{Q}$, which is evaluated by the target Q network. Furthermore, the DQN contains an experience replay buffer E, allowing us to pick training samples at random to reduce the data correlation and so speed up convergence.

In this paper, we only use DQN for offloading strategy making, although it is achievable to jointly optimize offloading strategy and resource allocation, as the extra action space it brings would slow down the convergence speed. So we turn to use convex optimization to give a closed-form solution for the allocation of transmission power and computational capability after getting a specific offloading ratio from the DQN.

4.2. Allocation of transmission power and computational capability

With the given offloading ratio after every time slot of DQN algorithm, we can reduce the original problem (P1) into the following resource allocation problem:

$$(\text{P2}): \min_{\{P,F\}} T^{\text{total}}, \tag{16a}$$

$$\text{s.t. } C_3: \sum_{n=1}^{N} P_{m,n} \le P_m^{\text{total}}, \forall m \in \mathcal{M}, \tag{16b}$$

$$C_4: \sum_{m=1}^{M} F_{m,n} \le F_n^{\text{total}}, \forall n \in \mathcal{N}. \tag{16c}$$

We can observe new problem (P2) to be a convex optimization problem, thus we can use convex optimization tools to get a solution over multiple iterations. However, due to too many variables and max operations, it is hard to get a reasonable solution at a low computational complexity. To reduce the computational complexity, we intend to find a closed-form solution without iteration, so we turn to solve the resource allocation problem of latency sum to simplify the problem, given by

$$(\text{P3}): \min_{\{P,F\}} \sum_{m=1}^{M} \sum_{n=1}^{N} T_{m,n}^{\text{offl}}, \tag{17a}$$

$$\text{s.t. } C_3: \sum_{n=1}^{N} P_{m,n} \le P_m^{\text{total}}, \forall m \in \mathcal{M}, \tag{17b}$$

$$C_4: \sum_{m=1}^{M} F_{m,n} \le F_n^{\text{total}}, \forall n \in \mathcal{N}. \tag{17c}$$

It is worth noting that the solution of problem (P3) is a reasonable and closed approximate result, for it is a tight upper bound of the

problem (P2). We can see from problem (P3) that the system latency is monotonically decreases with both the two inequality constraints C_3 and C_4, which means the optimal resource allocation appears in equality constraints of the allocation of transmit power, and computational power at CAPs. Therefore, we can use Lagrange Multiplier Method to derive the closed-form optimal solution of problem (P3). Let $\lambda_m \leq 0, m \in \mathcal{M}$ and $\mu_n \leq 0, n \in \mathcal{N}$ denote the dual variables associated with the constraints C_3 and C_4, respectively. The Lagrangian of problem (P3) is given by

$$\begin{aligned}\mathcal{L}(P, F, \lambda_m, \mu_n) = &\sum_{m=1}^{M}\sum_{n=1}^{N} T_{m,n}^{\text{offl}} \\ &+ \sum_{m=1}^{M} \lambda_m \left(\sum_{n=1}^{N} P_{m,n} - P_m^{\text{total}} \right) \\ &+ \sum_{n=1}^{N} \mu_n \left(\sum_{m=1}^{M} F_{m,n} - F_n^{\text{total}} \right).\end{aligned} \tag{18}$$

We consider a practical scenario where the SNR is high, so an approximation is used to simplify the calculation by expanding Eq. (2) to Taylor Series, by using the first item to approximate, and we get

$$R_{m,n}^{\text{sce}} \simeq W \left(\log_2 \frac{|h_{m,n}|^2}{|h_{m,e}|^2} - \frac{\sigma^2}{\ln 2 \cdot P_{m,n}} \frac{|h_{m,n}|^2 - |h_{m,e}|^2}{|h_{m,n}|^2 |h_{m,e}|^2} \right)^+. \tag{19}$$

For convenience, we denote $b_{m,n} = \log_2(|h_{m,n}|^2/|h_{m,e}|^2)$ and $\upsilon_{m,n} = (|h_{m,n}|^2 - |h_{m,e}|^2)/(|h_{m,n}|^2|h_{m,e}|^2)$. Then we take the partial derivative of $\mathcal{L}$ with respect to $P_{m,n}$, given by

$$\frac{\partial \mathcal{L}}{\partial P_{m,n}} = \lambda_m - \frac{\ln 2 \cdot \alpha_{m,n} l_m \upsilon_{m,n} P_{m,n} \sigma^2}{W_m (\ln 2 \cdot b_{m,n} P_{m,n} - \sigma^2 \upsilon_{m,n})^2}. \tag{20}$$

Similarly, the partial derivative of $\mathcal{L}$ with respect to $F_{m,n}$ can given by

$$\frac{\partial \mathcal{L}}{\partial F_{m,n}} = \mu_n - \frac{\alpha_{m,n} l_m \omega}{F_{m,n}^2}. \tag{21}$$

By setting the above two derivatives equal to 0, we can obtain the analytical results of λ_m and μ_n as

$$\lambda_m = \left(\frac{\sum_{n=1}^{N} \frac{\sqrt{\alpha_{m,n} l_m \upsilon_{m,n}} \cdot \prod_{n=1}^{N} b_{m,n}}{b_{m,n}}}{P_m^{\text{total}} \prod_{n=1}^{N} b_{m,n} - \sum_{n=1}^{N} \frac{\upsilon_{m,n} \cdot \prod_{n=1}^{N} b_{m,n}}{b_{m,n}}} \right)^2, \tag{22}$$

$$\mu_n = \left(\frac{\sum_{m=1}^{M} \sqrt{\alpha_{m,n} l_m}}{F_n^{\text{total}}} \right)^2. \tag{23}$$

Accordingly, the transmission power allocation is given by,

$$P_{m,n} = \frac{\sqrt{\frac{\alpha_{m,n} l_m \upsilon_{m,n}}{\lambda m}} + \upsilon_{m,n}}{b_{m,n}}. \tag{24}$$

The computational capability allocation is given by,

$$F_{m,n} = \sqrt{\frac{\alpha_{m,n} l_m}{\mu_n}}. \tag{25}$$

With the allocation problem of transmission power and computational capability solved, these results can be applied in (2) and (6) after the DQN network outputs an action for every time slot to calculate the corresponding total system latency T^{total}. This completes the system offloading design and resource allocation. The proposed task offloading and resource allocation method DRCO can be summarized in Algorithm 1. We also provide an example of our DRCO method to more clearly describe how the proposed method works in Fig. 2. Specifically, the reinforcement learning agent first receive all the state information from the environment, and chooses the offloading decision action from the evaluation network and the ϵ-greedy policy. The given offloading decision is then used to calculate the resource allocation of the transmission power and computational capability via (24) and (25). By executing the task offloading decision, transmission power allocation decision, and CAPs' computational capability allocation decision, the MEC network can store the transition sample in the reply memory for the reinforcement learning' training.

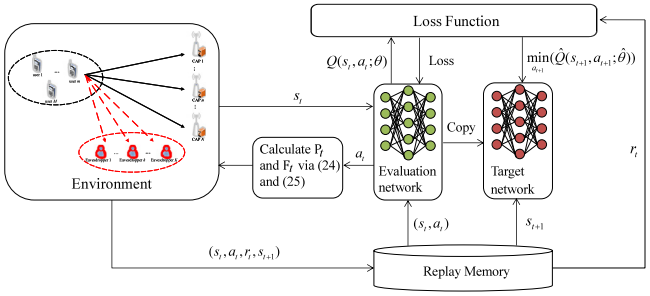


Fig. 2. An example of the DRCO method.

Algorithm 1 Deep reinforcement learning combined with convex optimization

Require: the tasks $\mathbf{L}_t$ requested by users, the transmission power $\mathbf{P}_t$ and computational capability $\mathbf{F}_t$
Ensure: Offloading ratio $\boldsymbol{\alpha}$

```
Initialize the reply buffer E
Randomly initialize θ and θ̂
for episode=1,...,Z do
    Initialize s_0 ∈ S
    for t=1,...,T do
        With probability ϵ select a random action a_t ∈ A
        Execute action a_t to get the offloading ratio, perform convex
        optimization to calculate the allocation of transmission power
        and computational capability via (24) and (25) and get the
        reward r_t and the state s_{t+1}
        Store (s_t, a_t, r_t, s_{t+1}) in E
        Sample a batch of reply buffer from E
        Calculate Loss_t = (r_t + γ max_{a_{t+1}}(Q̂(s_{t+1}, a_{t+1}; θ̂))
        −Q(s_t, a_t; θ))^2
        Execute gradient decent to the loss function with respect to θ;
        Every 100 steps reset Q̂ = Q
    end for
end for
```

4.3. Computational complexity

The complexity of the proposed DRCO algorithm is lower than that of using DQN to find both the offloading decision and resource allocation due to the using of convex optimization method. Moreover, the DRCO algorithm is based on the DQN algorithm, for one step of the DQN, the computational complexity is $O(J)$, The DRCO algorithm calculates one resource allocation closed-form solution for every step of DQN, and the convex optimization operation needs $O(G)$, thus, the complexity of DRCO for one episode is $O(T(J+G))$. The computational complexity of DRCO for all Z episodes is $O(ZT(J+G))$.

5. Simulation results and discussions

In this section, some simulations have been conducted to evaluate the proposed deep reinforcement learning combined with convex optimization based offloading scheme. We let the MEC system consist of $M = 3$ mobile users and $N = 2$ CAPs, in which each user can execute multi-access offloading to CAPs in the presence of $K = 6$ passive eavesdroppers. The bandwidth for each communication link is 2 MHz, all links in this system experience Rayleigh flat fading channels [40,41], with the average channel gain of users to CAPs to be unit, and the

Table 1
Parameter setting.

Parameter	Value
Number of users M	3
Number of CAPs N	2
Bandwidth of each link W	2 MHz
Average channel gain of $\|h_{m,n}\|^2$	1
Average channel gain of $\|h_{m,e}\|^2$	0.04
Variance of the AWGN at the CAPs σ^2	0.01
Variance of the AWGN at the eavesdroppers σ^2	0.01
Users' transmission power P	{2, 3, 2} W
Distribution of tasks size	$l_1 \sim \mathcal{U}(10, 15)$ Mb, $l_2 \sim \mathcal{U}(40, 45)$ Mb, $l_3 \sim \mathcal{U}(70, 75)$ Mb
User m' distribution of computational capability f_m	$\mathcal{U}(0.2 \times 10^8, 2 \times 10^8)$ cycle/s
CAP n's computational capability F_n	{3*10^8, 10*10^8} cycle/s
Subtask number L_s of each task	100
Ratio of one subtask β	0.01

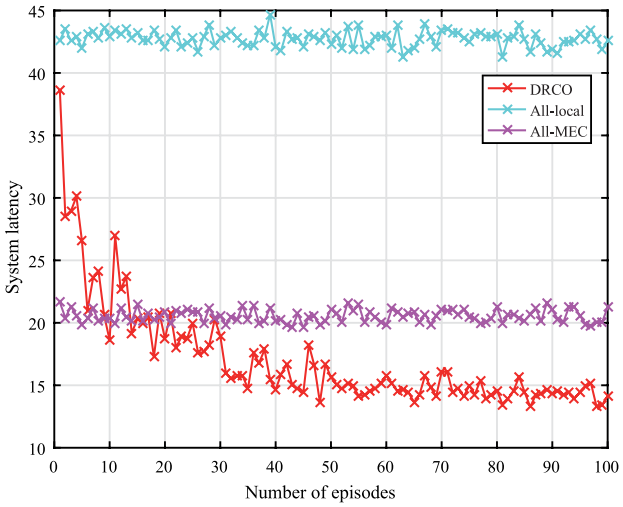
average eavesdropping channel gain is set to be 0.04. The three mobile users have different data sizes of the computational tasks, following the uniform distribution of $l_1 \sim \mathcal{U}(10, 15)$, $l_2 \sim \mathcal{U}(40, 45)$ and $l_3 \sim \mathcal{U}(70, 75)$ Mb. Each of the tasks can be divided into $X = 100$ subtasks to execute locally with a smaller computational capability of $f_m \sim \mathcal{U}(0.2 \times 10^8, 2 \times 10^8)$ cycle/sec or partially offloading to more computation powerful CAPs with computational capability ranging from 3×10^8 to 10×10^8 cycle/s. Moreover, the total transmission power at users are set as $\{P_1^{\text{total}}, P_2^{\text{total}}, P_3^{\text{total}}\} = \{2, 3, 2\}$ W. The full list of simulation parameter setting is provided in Table 1.

In the simulation, for the proposed DRCO method, the evaluation network and the target network have three hidden layers with 64, 256, and 64 neurons, respectively, and have one output layer as well. When training, the evaluation network updates its network parameters every 5 steps after the first 200 steps, and the target network duplicates the evaluation network's parameters every 100 steps.

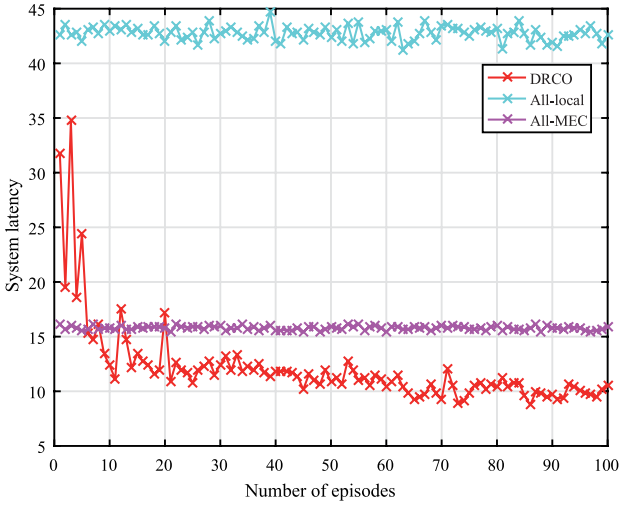
Besides the proposed DRCO method, we consider another three benchmarks for comparison:

- All-MEC: All the M users evenly offload all of their tasks to all N CAPs, and use (24) and (25) to allocate transmission power and computational capability at CAPs.
- All-local: All the M users calculate all of their tasks locally.
- DQN-average: All the M users use DQN to find an offloading strategy with transmission power evenly allocated to each link and computational capability evenly allocated to each user's workload.

Fig. 3 shows the impact of the episode number on the overall latency of the DRCO approach that has been proposed, where the user number $M = 3$, CAP number $N = 2$, eavesdropper number $K = 6$, wireless bandwidth $W = 2$ MHz and the number of episodes ranges from 0 to 100. Specifically, Fig. 3(a) represents the scenario of multiple eavesdroppers attacking the offloading scheme in a colluding way, while Fig. 3(b) is associated with the scenario of multiple eavesdroppers working in a non-colluding way. From this figure, we can find that for All-local and All-MEC methods, the total system latency changes little over episodes, which is caused by different task sizes and channel parameters for different episodes. Moreover, the total system latency of the proposed DRCO method falls down with the increase of the number of episodes, and converges to about 15 s and 10 s after about 50 episodes for colluding and non-colluding eavesdropping scenarios, respectively, which shows that DRCO can find a suitable offloading and resource allocation strategy after an acceptable number of training episodes. In further, the proposed DRCO method outperforms All-local and All-MEC methods for either non-colluding or colluding eavesdroppers in terms of the convergent value, which indicate its effectiveness in reducing the system latency.



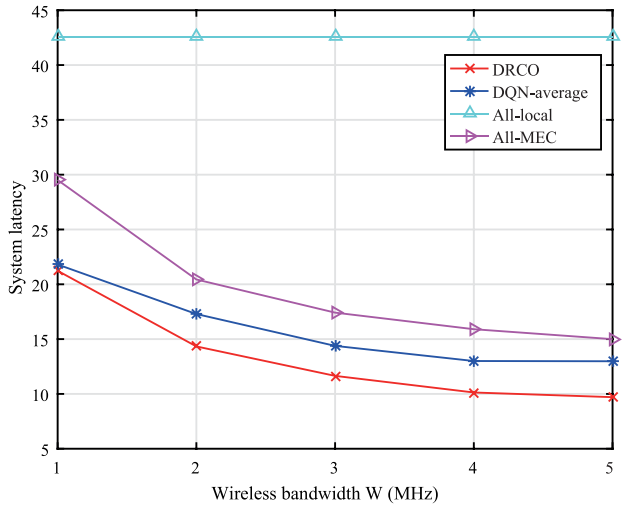
(a) Colluding eavesdroppers.



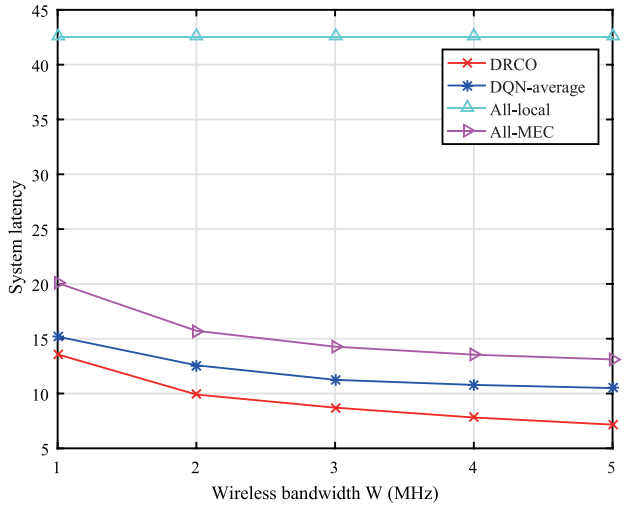
(b) Non-colluding eavesdroppers.

Fig. 3. Convergence of the proposed DRCO methods.

Fig. 4 illustrates the impact of wireless bandwidth W for each link on the system total latency of several offloading and resource allocation methods, where the user number $M = 3$, CAP number $N = 2$, eavesdropper number $K = 6$, and the wireless bandwidth of each link varies from 1 to 5 MHz. Specifically, Figs. 4(a) and 4(b) depict the scenarios of colluding and non-colluding eavesdroppers, respectively. According to Fig. 4, for either colluding or non-colluding eavesdroppers, the overall system latencies of DRCO, DQN-average, and All-MEC decrease as wireless bandwidth increases. However, the system latency of All-local remains constant across bandwidths, which is due to the fact that the system transmission latency can be reduced along with the increasing bandwidth. Moreover, the system latencies of DRCO, DQN-average, and All-MEC under the colluding eavesdropping scenario are smaller than that under the non-colluding eavesdropping scenario for various wireless bandwidths, as colluding eavesdroppers would seriously affect the secure transmission rate. Furthermore, the DRCO method outperforms the other benchmarks, including All-local, All-MEC, and DQN with averaged resource allocation, which proves DRCO's ability to provide offloading and resource allocation strategy for the multi-access MEC system.

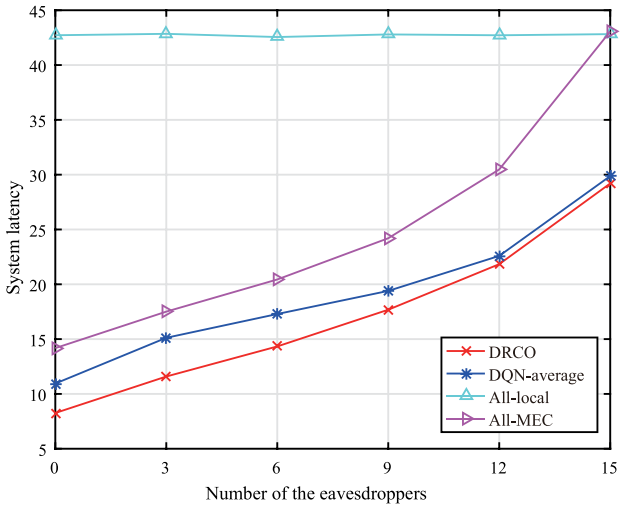


(a) Colluding eavesdroppers.

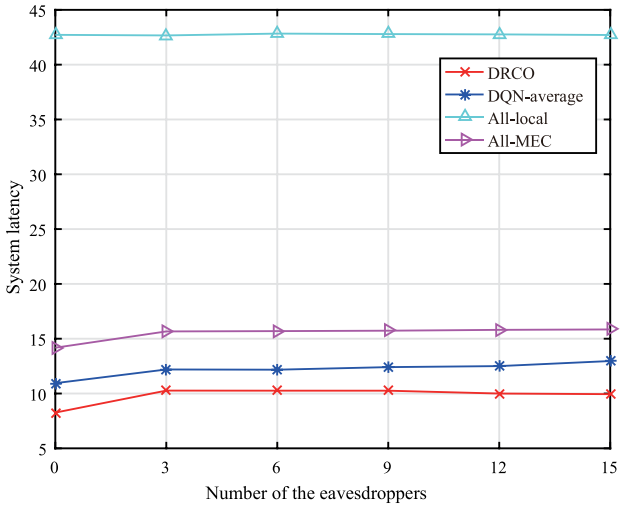


(b) Non-colluding eavesdroppers.

Fig. 4. Total system latency of several offloading and resource allocation strategies versus the wireless bandwidth.



(a) Colluding eavesdroppers.



(b) Non-colluding eavesdroppers.

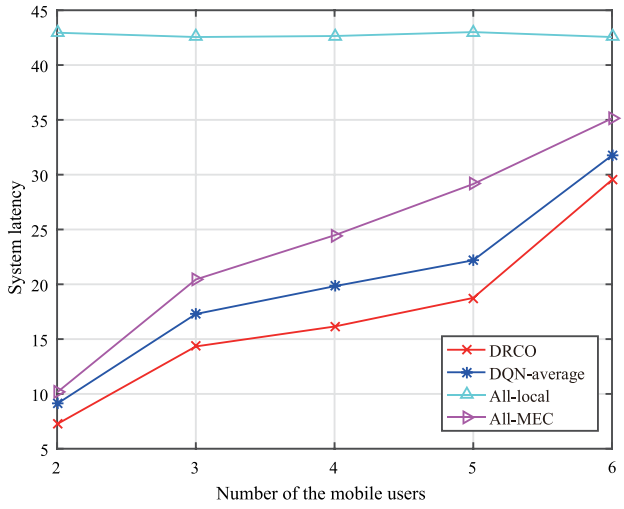
Fig. 5. Total system latency for different number of eavesdroppers for several offloading and resource allocation strategies.

Fig. 5 depicts the effect of the number of eavesdroppers on the system latency of several offloading and resource allocation schemes, where the user number $M = 3$, CAP number $N = 2$, and the number of eavesdroppers K is set to 0, 3, 6, 9, 12 and 15. Figs. 5(a) and 5(b) correspond to the scenario with colluding and non-colluding eavesdroppers, respectively. We can observe from Fig. 5(a) that for the DRCO, DQN-average, and All-MEC schemes, the system latency deteriorates with an increase in the number of the eavesdroppers, as more colluding eavesdroppers would impose a more serious threat to the security of task offloading. Moreover, for the colluding eavesdropping scenarios, the DRCO and DQN-average methods can get a lower system latency even under the effect of up to 15 eavesdroppers where both All-local and All-MEC perform badly. In further, for the non-colluding eavesdropping scenarios, the change of different numbers of eavesdroppers have a marginal impact on the system latency, as the eavesdroppers work individually without sharing the received information. Furthermore, compared with the scenarios without eavesdroppers, the system performance degrades when eavesdroppers exist for both colluding and non-colluding eavesdroppers, for the existence of eavesdropping affects the original wireless transmission rate and therefore deteriorates the performance of the MEC system.

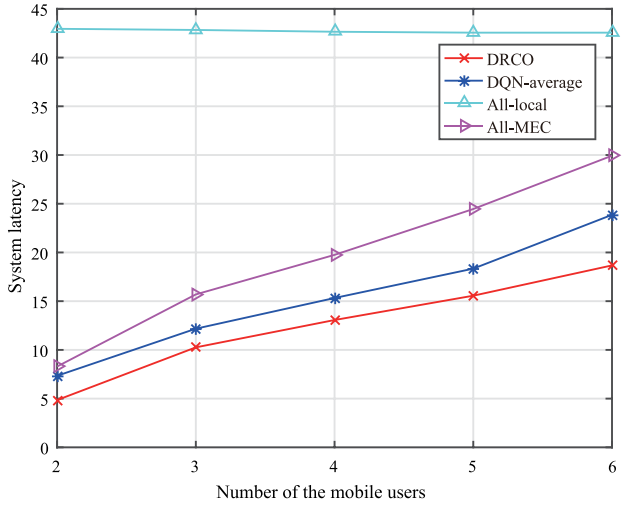
Fig. 6 shows the system latency of the four offloading and resource allocation schemes versus the number of users, where CAP number $N = 2$, the number of eavesdroppers $K = 6$, and the number of users M varies from 2 to 6. Fig. 6(a) and (b) correspond to the scenario with colluding and non-colluding eavesdroppers, respectively. One can easily get that the performance of the DRCO, DQN-average, and All-MEC schemes deteriorates with an increased M, as more users provide more workloads for the task offloading in the MEC system. Moreover, the proposed DRCO method outperforms the other benchmarks, including All-MEC, All-local, and DQN with averaged resource allocation, which proves DRCO's ability to provide offloading and resource allocation strategy under heavy system workloads.

6. Conclusion

This paper studied a secure MEC for emerging CPS, where there exist K eavesdroppers in the network, which can threaten the task offloading. These K eavesdroppers can work either in a colluding mode where they cooperate to decode the secret message, or in a non-colluding mode where the eavesdroppers decode the message individually. For both eavesdropping nodes, we design the secure MEC system by devising an offloading strategy and resource allocation for the purpose of improving the system performance, which is primarily assessed by latency. In particular, a novel deep reinforcement learning



(a) Colluding eavesdroppers.



(b) Non-colluding eavesdroppers.

Fig. 6. Total system latency for different number of users for several offloading and resource allocation strategies.

combined with convex optimization (DRCO) is proposed, where the DRL is used to find a proper solution to the offloading ratio, while the convex optimization is implemented to solve the allocation of transmission power and computational capability.

In future works, we will extend the considered secure MEC networks from eavesdropping attack mode to some more attack modes, such as jamming and spoofing. In addition, we intend to explore some distributed learning methods to solve the resource allocation problems, such as Federated learning.

CRediT authorship contribution statement

Lunyuan Chen: Conceptualization, Methodology, Software, Investigation, Formal analysis, Validation, Writing – original draft. **Shunpu Tang:** Data curation, Software, Writing – original draft. **Venki Balasubramanian:** Conceptualization, Supervision, Writing – review & editing. **Junjuan Xia:** Conceptualization, Supervision, Writing – review & editing. **Fasheng Zhou:** Visualization, Investigation. **Lisheng Fan:** Conceptualization, Funding acquisition, Resources, Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

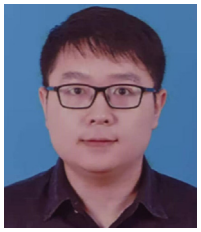
Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (Nos. 61871139/62101145), in part by the International Science and Technology Cooperation Projects of Guangdong Province (No. 2020A0505100060), in part by the Natural Science Foundation of Guangdong Province (No. 2021A1515011392), in part by the Guangdong Basic and Applied Basic Research Foundation (No. 2021A1515011812), and in part by the research program of Guangzhou University (Nos. YK2020008/YJ2021003).

References

[1] B. Wang, F. Gao, S. Jin, H. Lin, G.Y. Li, Spatial- and frequency-wideband effects in millimeter-wave massive MIMO systems, IEEE Trans. Signal Process. 66 (13) (2018) 3393–3406.
[2] X. Hu, C. Zhong, Y. Zhu, X. Chen, Z. Zhang, Programmable metasurface-based multicast systems: Design and analysis, IEEE J. Sel. Areas Commun. 38 (8) (2020) 1763–1776.
[3] Y. Xu, C. Shen, D. Cai, G. Zhu, Latency constrained non-orthogonal packets scheduling with finite blocklength codes, IEEE Trans. Veh. Technol. 69 (10) (2020) 12,312–12,316.
[4] X. Hu, C. Zhong, Y. Zhang, X. Chen, Z. Zhang, Location information aided multiple intelligent reflecting surface systems, IEEE Trans. Commun. 68 (12) (2020) 7948–7962.
[5] X. Li, Y. Zheng, W.U. Khan, M. Zeng, D. Li, G.K. Ragesh, L. Li, Physical layer security of cognitive ambient backscatter communications for green internet-of-things, IEEE Trans. Green Commun. Netw. 5 (3) (2021) 1066–1076.
[6] D. Cai, P. Fan, Q. Zou, Y. Xu, Z. Ding, Z. Liu, Active device detection and performance analysis of massive non-orthogonal transmissions in cellular internet of things, Sci. China Inf. Sci. (99) (2022) 1–17.
[7] X. Hu, J. Wang, C. Zhong, Statistical CSI based design for intelligent reflecting surface assisted MISO systems, Sci. China: Inf. Sci. 63 (12) (2020) 1–10.
[8] P.K. Malik, R. Sharma, R. Singh, A. Gehlot, S.C. Satapathy, W.S. Alnumay, D. Pelusi, U. Ghosh, J. Nayak, Industrial internet of things and its applications in industry 4.0: State of the art, Comput. Commun. 166 (2021) 125–139.
[9] X. Li, J. Li, Y. Liu, Z. Ding, A. Nallanathan, Residual transceiver hardware impairments on cooperative NOMA networks, IEEE Trans. Wirel. Commun. 19 (1) (2020) 680–695.
[10] W. Xu, Z. Yang, D.W.-K. Ng, M. Levorato, Y.C. Eldar, M. Debbah, Edge learning for b5 g networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing, IEEE J. Sel. Top. Sign. Proces. 2022 (2022) 1–10.
[11] P. Singh, A. Nayyar, A. Kaur, U. Ghosh, Blockchain and fog based architecture for internet of everything in smart cities, Future Internet 12 (4) (2020) 61.
[12] Y. Nie, J. Zhao, F. Gao, F.R. Yu, Semi-distributed resource management in UAV-aided MEC systems: A multi-agent federated reinforcement learning approach, IEEE Trans. Veh. Technol. 70 (12) (2021) 13,162–13,173.
[13] L. Chen, Intelligent ubiquitous computing for future UAV-enabled MEC network systems, Cluster Comput. 2021 (25) (2021) 1–10.
[14] J. Zhao, X. Sun, Q. Li, X. Ma, Edge caching and computation management for real-time internet of vehicles: An online and distributed approach, IEEE Trans. Intell. Transp. Syst. 22 (4) (2021) 2183–2197.
[15] S. Tang, L. Chen, Computational intelligence and deep learning for next-generation edge-enabled industrial IoT, IEEE Trans. Netw. Sci. Eng. 9 (3) (2022) 105–117.
[16] J. Zhao, Q. Li, Y. Gong, K. Zhang, Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks, IEEE Trans. Veh. Technol. 68 (8) (2019) 7944–7956.
[17] X. Lai, Outdated access point selection for mobile edge computing with cochannel interference, IEEE Trans. Veh. Tech. 71 (7) (2022) 7445–7455.
[18] Z. Zhao, X. Lei, G.K. Karagiannidis, A. Nallanathan, System optimization of federated learning networks with a constrained latency, IEEE Trans. Veh. Technol. 71 (1) (2022) 1095–1100.
[19] Y. Guo, S. Lai, Distributed machine learning for multiuser mobile edge computing systems, IEEE J. Sel. Top. Signal Process. PP (99) (2021) 1–12.
[20] H. Mughal, M. Bilal, U. Ghosh, G. Srivastava, S.C. Shah, Efficient allocation of resource-intensive mobile cyber–physical social system applications on a heterogeneous mobile ad hoc cloud, IEEE Trans. Netw. Sci. Eng. 9 (3) (2022) 958–969.

[21] X. Lai, Y. Deng, G.K. Karagiannidis, A. Nallanathan, Secure mobile edge computing networks in the presence of multiple eavesdroppers, IEEE Trans. Commun. 70 (1) (2022) 500–513.
[22] J. Xu, J. Yao, Exploiting physical-layer security for multiuser multicarrier computation offloading, IEEE Wirel. Commun. Lett. 8 (1) (2019) 9–12.
[23] J. Lu, Analytical offloading design for mobile edge computing based smart internet of vehicle, EURASIP J. Adv. Signal Process. 2022 (1) (2022) 44.
[24] L. Zhang, DQN based mobile edge computing for smart internet of vehicle, EURASIP J. Adv. Signal Process. 2022 (1) (2022) 45.
[25] L. Xiao, X. Lu, T. Xu, X. Wan, W. Ji, Y. Zhang, Reinforcement learning-based mobile offloading for edge computing against jamming and interference, IEEE Trans. Commun. 68 (10) (2020) 6114–6126.
[26] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, W. Zhuang, Reinforcement learning based phy authentication for vanets, IEEE Trans. Veh. Tech. 69 (3) (2020) 3068–3079.
[27] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, J. Song, Deep reinforcement learning-enabled secure visible light communication against eavesdropping, IEEE Trans. Commun. 67 (10) (2019) 6994–7005.
[28] K. He, Y. Deng, Efficient memory-bounded optimal detection for GSM-MIMO systems, IEEE Trans. Commun. 70 (7) (2022) 4359–4372.
[29] M. Huang, Y. Liu, V.G. Menon, I/q imbalance aware nonlinear wireless-powered relaying of B5G networks: Security and reliability analysis, IEEE Trans. Netw. Sci. Eng. 8 (4) (2021) 2995–3008.
[30] J. Zhang, Y. Zhang, C. Zhong, Z. Zhang, Robust design for intelligent reflecting surfaces assisted MISO systems, IEEE Commun. Lett. 24 (10) (2020) 2353–2357.
[31] R. Zhao, M. Tang, Profit maximization in cache-aided intelligent computing networks, Phys. Commun. PP (99) (2022) 1–10.
[32] L. He, K. He, Towards optimally efficient search with deep learning for large-scale MIMO systems, IEEE Trans. Commun. 70 (5) (2022) 3157–3168.
[33] S. Tang, Dilated convolution based CSI feedback compression for massive MIMO systems, IEEE Trans. Veh. Technol. 71 (5) (2022) 211–216.
[34] R. Zhao, M. Tang, Impact of direct links on intelligent reflect surface-aided MEC networks, Phys. Commun. PP (99) (2022) 1–10.
[35] L. Zhang, C. Gao, Deep reinforcement learning based IRS-assisted mobile edge computing under physical-layer security, Phys. Commun. PP (99) (2022) 1–10.
[36] J. Lu, M. Tang, Performance analysis for IRS-assisted MEC networks with unit selection, Phys. Commun. PP (99) (2022) 1–10.
[37] Y. Wu, C. Gao, Intelligent task offloading for vehicular edge computing with imperfect CSI: A deep reinforcement approach, Phys. Commun. PP (99) (2022) 1–10.
[38] S. Tang, X. Lei, Collaborative cache-aided relaying networks: Performance evaluation and system optimization, IEEE J. Sel. Areas Commun. PP (99) (2022) 1–12.
[39] V. Mnih, K. Kavukcuoglu, D. Silver, A.A. Rusu, J. Veness, M.G. Bellemare, A. Graves, M.A. Riedmiller, A. Fidjeland, G. Ostrovski, S. Petersen, C. Beattie, A. Sadik, I. Antonoglou, H. King, D. Kumaran, D. Wierstra, S. Legg, D. Hassabis, Human-level control through deep reinforcement learning, Nature 518 (7540) (2015) 529–533.
[40] Y. Zheng, M.D. Alshehri, L. Hai, Cognitive ambc-NOMA IoV-MTS networks with IQI: Reliability and security analysis, IEEE Trans. Intell. Trans. Syst. PP (99) (2021) 1–12.
[41] Q. Tao, J. Wang, C. Zhong, Performance analysis of intelligent reflecting surface aided communication systems, IEEE Commun. Lett. 24 (11) (2020) 2464–2468.



Lunyuan Chen received the bachelor's degree in Communication Engineering from Xidian university in 2019. He is currently pursuing the master's degree with the school of Electronics and Communication Engineering, Guangzhou University. His current research interests focus on statistical machine learning and deep learning.

Shunpu Tang received the B.E. degree in 2020 and he is currently pursuing the master degree, both with the School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou, China. His current research interests include edge intelligence, distributed machine learning.

Venki Balasubramanian received the Ph.D. degree in body area wireless sensor network (BAWSN) for remote healthcare monitoring applications. He is currently with the School of Science, Engineering and Information Technology, Federation University, Mount Helen, VIC, Australia. He is also the Pioneer in building (pilot) remote healthcare monitoring application (rHMA) for pregnant women with the New South Wales Healthcare Department. He also founded Anidra Tech Ventures Pty Ltd., a smart remote patient monitoring. His research establishes a dependability measure to evaluate rHMA that uses BAWSN. His research opens up a new research area in measuring time-critical applications. He contributed immensely to eResearch software research and development that uses cloud-based infrastructure and a core member for the project sponsored by the Nectar Australian Research Cloud Provider. He contributed heavily in the field of healthcare informatics, sensor networks, and cloud computing.

Junjuan Xia received the bachelor degree from the Department of Computer Science, Tianjin University in 2003, and obtained the master degree from the Department of Electronic Engineering, Shantou University in 2015. Now she is working for the School of Computer Science, Guangzhou University. Her current research interests include wireless caching, IoT networks, physical-layer security, and cooperative relaying.

Fasheng Zhou received the Ph.D. degree in information and communication engineering from the South China University of Technology, Guangzhou, China. He received the M. Eng. and B. Eng. degrees both from the University of Science and Technology of China, Hefei, China. Since 2016, Dr. Zhou is with Guangzhou University, Guangzhou. From 2019 to 2020, he was a visiting scholar with the Communications Lab at National University of Singapore. His research interests include mobile edge computing and wireless signal processing.

Lisheng Fan received the bachelor and master degrees from Fudan University and Tsinghua University, China, in 2002 and 2005, respectively, both from the Department of Electronic Engineering. He received the Ph.D. degree from the Department of Communications and Integrated Systems of Tokyo Institute of Technology, Japan, in 2008. He is now a Professor with the School of Computer Science, GuangZhou University. His research interests span in the areas of wireless cooperative communications, physical-layer secure communications, intelligent communications, and system performance evaluation. Lisheng Fan has published many papers in international journals such as IEEE Transactions on Wireless Communications, IEEE Transactions on Communications, IEEE Transactions on Information Theory, as well as papers in conferences such as IEEE ICC, IEEE Globecom, and IEEE WCNC. He is an editor of China Communications, and has served as a guest editor for many journals such as Physical Communication, EURASIP Journal on Wireless Communications and Networking, Wireless Communications and Mobile Computing, and so on. He has been awarded as Exemplary Reviewer by IEEE Transactions on Communications and IEEE Communications Letters.