IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON EMERGING APPROACHES TO MOBILE COOPERATIVE SENSING AND ITS APPLICATIONS IN SMART ENVIRONMENTS

Received August 4, 2020, accepted August 10, 2020, date of publication August 14, 2020, date of current version August 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3016764

Mobile Cooperative Sensing Based Secure Communication Strategy of Edge Computational Networks for Smart Cities

YING SUN[1], ZHIPENG SU[1], YING ZHAO[1], DAN DENG[2], (Member, IEEE), FUSHENG ZHU[3], AND JUNJUAN XIA[4], (Member, IEEE)

[1]Guangzhou Power Supply Bureau of Guangdong Power Grid Company, Ltd., Guangzhou 518000, China
[2]School of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou 511483, China
[3]Guangdong New Generation Communication and Network Innovative Institute (GDCNi), Guangzhou 510700, China
[4]School of Computer Science, Guangzhou University, Guangzhou 510006, China

Corresponding authors: Ying Sun (fjsunying@foxmail.com), Dan Deng (dengdan@ustc.edu), Fusheng Zhu (zhufusheng@gdcni.cn), and Junjuan Xia (xiajunjuan@gzhu.edu.cn)

This work was supported in part by the Science and Technology Projects of China Southern Power Gird under Grant GZHKJXM20190101, in part by the Science and Technology Program of Guangzhou under Grant 201807010103, in part by the research program of Guangzhou University under Grant YK2020008, in part by the International Science and Technology Cooperation Projects of Guangdong Province under Grant 2020A0505100060, in part by the Natural Science Foundation of Guangdong Province under Grant 2018A030313736, in part by the Scientific Research Project of Education Department of Guangdong under Grant 2019GZDXM002, in part by the Project of Technology Development Foundation of Guangdong under Grant 706049150203, in part by the Application Technology Collaborative Innovation Center of GZPYP under Grant 2020ZX01, and in part by the Yangcheng scholar, scientific research project of Guangzhou Education Bureau under Grant 202032761.

ABSTRACT With the development of smart cities, lots of mobile cooperative sensing based nodes have emerged. However, due to the open nature of wireless transmission, attackers in the networks can use some intelligent radio devices to deteriorate the secure transmission, which imposes a severe issue of information leakage. In this paper, we consider the transmitter has some computational tasks to be computed, under the environments of intelligent attacker. Due to the limited computational capability, the sender needs to offload some tasks to the receiver. To address this problem, we propose a power allocation algorithm based on combining the technology of reinforcement learning and game theory, in order to achieve an optimal secure data rate and meanwhile reduce the whole task latency of the transmission and computation with Q learning and Nash equilibrium. Then, the Nash equilibrium and its existence conditions are derived and proven mathematically. Finally, we perform some simulations under Matlab platform, and the results show that the proposed algorithm can effectively improve the secrecy data rate and reduce the whole system latency.

INDEX TERMS Mobile cooperative sensing, secure communication, smart environments.

I. INTRODUCTION

In recent years, there has been a great progress in the development of smart cities, and many wireless techniques have been proposed to support the system development. Among these techniques, the mobile cooperative sensing is one of the most promising techniques, which can support the deployment and application of smart cities very efficiently [1]–[3]. In particular, compressive cooperative sensing and cooperative and active sensing have been proposed to apply in the mobile sensor network to enhance the system performance [4]–[7]. On the other hand, with the rapid development of wireless technology, the traffic of mobile devices increases sharply [8]. However, due to the limited computational resources and performance, how to make reasonable use of the limited computational resources on the edge nodes becomes an important issue, which needs to be solved urgently [9], [10]. In order to deal with the problems mentioned above, such as insufficient processing capability and limited resources, many researchers have introduced the concept of computational offloading into mobile edge computing (MEC) networks [11]–[13]. In the MEC networks,

The associate editor coordinating the review of this manuscript and approving it for publication was Mu Zhou.

user terminal (UE) offloads some computational tasks to edge nodes, in order to solve the shortcomings of equipment in resource storage, computational performance and energy efficiency [14]–[16].

The process of computational offloading generally refers to the reasonable allocation of computationally-heavy tasks to the edge nodes with sufficiently computational resources for processing, and then the feedback of the calculated results from the edge server [17], [18]. This process is often affected by a number of practical factors, such as radio communication channels, the performance of the mobile devices, and so on [19]–[21]. Therefore, the key to realize computational offloading lies in specifying an appropriate offloading decision [22]–[25]. The offloading strategy affects the latency and energy consumption of both communication and computation, and it is basically an important method to utilize the computational resources of edge nodes, at the cost of wireless transmission. Hence, the offloading strategy can be viewed as a trade-off between the communication and computation. Generally speaking, the decision about computational offloading can be classified into the following three categories:

- Local computation: The entire computational task is completed locally.
- Full offloading: The entire computational task is allocated to the edge nodes for processing.
- Partial offloading: A part of the computational task is left for the local processing, while the other part is offloaded to the edge nodes for processing.

There are some existing works on the study of offloading strategy for the MEC networks [26]. In [27], [28], the authors proposed a deep Q-network which is based on the Q-learning algorithm to optimize the system offloading strategy of MEC networks, in order to reduce the network latency and energy consumption. In addition, the authors in [29] employed the ant colony optimization (ACO) algorithm to optimize the offloading strategy and used the relay selection technique, in order to reduce the system cost measured by a linear combination of both latency and energy consumption. Moreover, the authors in [30], [31] considered price mechanism in the MEC networks, and studied the impact of price on the system offloading strategy. In further, the authors in [32] proposed a novel framework to optimize the offloading strategy as well as the relay selection and wireless bandwidth allocation, in order to enhance the network performance in terms of latency and energy consumption. All these works clearly indicate that the offloading strategy plays a significant role in the system design for the MEC networks.

Another key challenge in the MEC networks is the attack from the smart attackers in the networks. The smart attackers can operate in spoofing, jamming or eavesdropping mode, which severely affects the system secrecy performance. Hence, it is of vital importance to suppress the smart attackers in order to safeguard the secrecy performance of MEC networks. In this viewpoint, the recent unmanned aerial vehicle (UAV) technique can be used to assist the secure transmission, based on the interference alignment [33], [34]. Moreover, the non-orthogonal multiple access (NOMA) technique can be implemented to enhance the network security, where the secrecy data rate can be significantly increased [35]. In further, caching technique can be exploited into the wireless networks, in order to enhance the network security, through increasing the dimension of communication resources at the cost of storage [36], [37].

In this paper, we consider an MEC network where the transmitter has some computational tasks to be computed, under the environments of intelligent attacker. Due to the limited computational capability, the sender needs to offload some tasks to the receiver. By combining the technology of reinforcement learning and game theory, this paper proposes a power allocation algorithm, in order to achieve an optimal secure data rate and reduce the whole task latency of both communication and computation with Q learning and Nash equilibrium. Then, the Nash equilibrium and its existence conditions are derived and proven mathematically. Finally, we perform some simulations under Matlab platform, and the results show that the proposed algorithm can effectively improve the secrecy data rate and reduce the whole system latency.

The organization of this paper is given as follows. After the introduction, Section II describes the model of MEC networks with under intelligent attack, and then details the communication and computation process. Section III presents the transmission game based on the system latency for the transmitter and attacker, and Section IV provides an effective power allocation algorithm for the transmitter in the networks. Simulation results are provided in Section V to offer valuable insights into the system performance, and finally, conclusions are drawn in Section VI.

Notations: Let $\mathcal{CN}(0, \beta)$ be a random variable (RV) with zero mean and variance β, subject to circularly symmetric complex Gaussian. In addition, we use $f_X(\cdot)$ to denote the probability density function (PDF) of the RV X, and the operation $\Pr(\cdot)$ returns probability.

II. SYSTEM MODEL

As shown in Fig. 1, Alice sends some secure messages to Bob through the main link and there is an attacker Eve in the network. Alice has a computational task, but due to the lack of computational capability, she needs to offload a part of the computational task to Bob. Alice has the flexibility to adjust her transmit power P_A. Eve has the option of keeping silent, eavesdropping, jamming, and spoofing as its mode of attack.

- Eve chooses to keep silent: In this case, Alice sends a normalized signal x_a to Bob, and then Bob receives a signal y_0,

$$y_0 = h_{AB}x_a + n_b, \tag{1}$$

where $h_{AB} \sim \mathcal{CN}(0, \sigma_{ab}^2)$ is the channel parameter of the main link and $n_b \sim \mathcal{CN}(0, \sigma_n^2)$ is the additive white Gaussian noise (AWGN) at Bob.

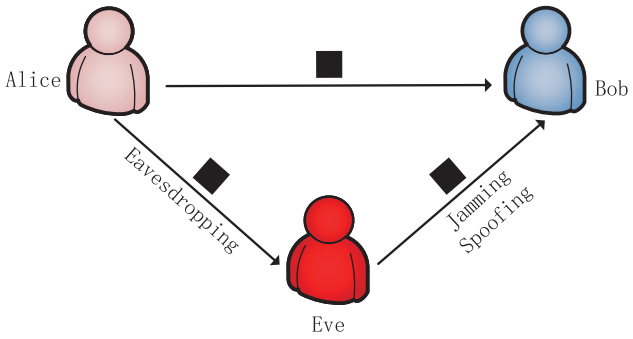

FIGURE 1. A secure communication of an edge computational network under intelligent attack.

According to the Shannon's theorem [38], the system secrecy data rate R_0 can be described as

$$R_0 = W_B \left[\log_2 \left(1 + \frac{P_A |h_{AB}|^2}{\sigma_n^2} \right) \right], \tag{2}$$

where W_B is the wireless bandwidth and σ_n^2 is the noise power.

The local latency to compute the local task can be written as [27], [28]

$$t_{local} = \frac{(1-\rho)L\eta}{f_A}, \tag{3}$$

where ρ is the proportion of task offloading, and L represents the task size. We use η to denote the number of CPU cycles required for one-bit task and the computational capability of the CPU at the Alice is represented by f_A. In particualr, ρ represents the proportion of the task to be calculated by the Bob, while $1-\rho$ represents the proportion of the task to be computed by the Alice itself.

The transmission latency of offloading, t_1, is given by

$$t_1 = \frac{\rho L}{R_0}. \tag{4}$$

The computational latency at the Bob, t_2, can be written as

$$t_2 = \frac{\rho L\eta}{f_B}, \tag{5}$$

where f_B represents the computational capability of the CPU at the Bob.

Therefore, the whole latency is $t_{local} + t_1 + t_2$.

- Eve chooses to overhear the message: In this case, the Alice sends Bob the secure message x_a, and then Eve receives a signal y_1,

$$y_1 = h_{AE}x_a + n_e, \tag{6}$$

where $h_{AE} \sim \mathcal{CN}(0, \sigma_{ae}^2)$ is the channel parameter of the Alice-Eve link and $n_e \sim \mathcal{CN}(0, \sigma_n^2)$ is the additive white Gaussian noise (AWGN) at Eve.

Similarly, the system secrecy data rate under eavesdropping attack can be written as

$$R_1 = W_B \left[\log_2 \left(1 + \frac{P_A |h_{AB}|^2}{\sigma_n^2} \right) - \log_2 \left(1 + \frac{P_A |h_{AE}|^2}{\sigma_n^2} \right) \right]^+, \tag{7}$$

where $[x]^+$ returns x if x is positive, or zero otherwise. From (7), the secure transmission latency t_1 becomes

$$t_1 = \frac{\rho L}{R_1}. \tag{8}$$

- If Eve chooses to send a jamming signal x_J with jamming power P_J to obstruct transmission of information: In this case, Bob will receive a signal y_2 as

$$y_2 = h_{AB}x_a + h_{BE}x_J + n_b, \tag{9}$$

where $h_{BE} \sim \mathcal{CN}(0, \sigma_{be}^2)$ is the channel parameter of the Bob-Eve link.

Similarly, the system secrecy data rate under jamming attack mode, R_2, is denoted by

$$R_2 = W_B \log_2 \left(1 + \frac{P_A |h_{AB}|^2}{\sigma_n^2 + P_J |h_{BE}|^2} \right). \tag{10}$$

From (10), the secure transmission latency t_1 is given by

$$t_1 = \frac{\rho L}{R_2}. \tag{11}$$

- Eve chooses to send a spoofing signal x_S with a spoofing power P_S to deceive Bob: In this case, the Bob will receive a signal y_3, denoted by

$$y_3 = h_{BE}x_S + n_b. \tag{12}$$

Similarly, the system secrecy data rate under the spoofing attack is denoted by

$$R_3 = W_B \left[\log_2 \left(1 + \frac{P_A |h_{AB}|^2}{\sigma_n^2} \right) - \gamma \log_2 \left(1 + \frac{P_A |h_{AE}|^2}{\sigma_n^2} \right) \right], \tag{13}$$

where γ represents an influence factor on the spoofing signal. From (13), the secure transmission latency, t_1, becomes

$$t_1 = \frac{\rho L}{R_3}. \tag{14}$$

III. TRANSMISSION GAME BASED ON SYSTEM LATENCY

According to the game theory, the interaction between the Alice and Eve can be viewed as a non-cooperative game. The action set of Alice is $[0, P_{max}]$, i.e., Alice can choose a proper power P_A from the range $[0, P_{max}]$ as its transmit power, where P_{max} is the maximum transmit power that Alice can choose. The action set of Eve is $[0, 1, 2, 3]$, i.e., Eve

can choose one attack mode q from these attack modes, where $q = 0, 1, 2$ and 3 correspond to four modes of keep silent, eavesdropping, jamming and spoofing, respectively. The purpose of Alice is to reduce the whole latency of the system as much as possible, while the purpose of Eve is to increase the whole latency of the system as much as possible. In order to achieve the goal of optimizing the system latency, we set the benefit function of Alice u_A as

$$u_A = -\left(t_{local} + t_1 + t_2\right) - C_A P_A, \tag{15}$$

where C_A is the cost coefficient of transmit power. From (15), we can find that the benefit of the Alice becomes worse when the latency becomes larger or an increased transmit power is used. Hence, the Alice tends to use a smaller transmit power and achieve a smaller latency in the whole secure transmission process.

On the contrary, the benefit function of Eve u_E is denoted by

$$u_E = t_{local} + t_1 + t_2 - C(q), \tag{16}$$

in which $C(q)$ represents the cost of Eve launching a specific attack mode with $C(1) = 0, C(2) = \theta_E, C(3) = \theta_J$ and $C(4) = \theta_S$.

From the definition of Nash equilibrium, the Nash equilibrium $(P_A{}^*, q^*)$ of the game can be obtained from the following two inequalities,

$$u_A\left(P_A^*, q^*\right) \geq u_A\left(P_A, q^*\right), \tag{17}$$
$$u_E\left(P_A^*, q^*\right) \geq u_E\left(P_A^*, q\right). \tag{18}$$

It can be seen from (17) and (18) that the strategies of Alice and Eve in Nash equilibrium are better than other strategies in the same environment, that is, both sides reach a balance. In this condition, the system balance is achieved by both the Alice and Eve.

Lemma 1: When inequalities (20a)-(23d) are satisfied, there exists a Nash equilibrium $(P_A{}^*, 0)$ in the game, and $P_A{}^*$ is given by (19),

$$\begin{cases} \dfrac{\rho L}{\left(R_0^*\right)^2} \dfrac{W_B \left|h_{AB}\right|^2}{\left(P_A^* \left|h_{AB}\right|^2 + \sigma_n^2\right) \ln 2} = C_A, & \text{(19a)} \\ 0 \leq P_A{}^* \leq P_{max}. & \text{(19b)} \end{cases}$$

If

$$\begin{cases} \theta_E \geq \dfrac{\rho L\left(R_0^* - R_1^*\right)}{R_0^* R_1^*}, & \text{(20a)} \\ \theta_J \geq \dfrac{\rho L\left(R_0^* - R_2^*\right)}{R_0^* R_2^*}, & \text{(20b)} \\ \theta_S \geq \dfrac{\rho L\left(R_0^* - R_3^*\right)}{R_0^* R_3^*}, & \text{(20c)} \\ \dfrac{\rho L}{\left(R_0^m\right)^2} \dfrac{W_B \left|h_{AB}\right|^2}{\left(P_{\max} \left|h_{AB}\right|^2 + \sigma_n^2\right) \ln 2} < C_A, & \text{(20d)} \end{cases}$$

where the superscript * in R_0^*, R_1^*, R_2^* and R_3^* represent that P_A is $P_A{}^*$ in R_0, R_1, R_2 and R_3, respectively. Similarly, the superscript m in R_0^m represents that P_A is P_{max} in R_0.

Proof 1: If (20a)-(20c) hold, from (16), we have

$$u_E\left(P_A^*, 0\right) - u_E\left(P_A^*, 1\right) = \frac{\rho L}{R_0^*} - \left(\frac{\rho L}{R_1^*} - \theta_E\right) \geq 0,$$
$$u_E\left(P_A^*, 0\right) - u_E\left(P_A^*, 2\right) = \frac{\rho L}{R_0^*} - \left(\frac{\rho L}{R_2^*} - \theta_J\right) \geq 0,$$
$$u_E\left(P_A^*, 0\right) - u_E\left(P_A^*, 3\right) = \frac{\rho L}{R_0^*} - \left(\frac{\rho L}{R_3^*} - \theta_S\right) \geq 0.$$

Thus, (17) holds for $(P_A{}^*, 0)$. From (15), we have

$$\begin{aligned} \frac{\partial u_A\left(P_A, 0\right)}{\partial P_A} &= \frac{\rho L}{R_0^2} \frac{W_B \left|h_{AB}\right|^2}{\left(P_A \left|h_{AB}\right|^2 + \sigma_n^2\right) \ln 2} - C_A, \\ \frac{\partial u_A^2\left(P_A, 0\right)}{\partial P_A^2} &= -\frac{W_B \rho L \left|h_{AB}\right|^2}{\left[R_0^2\left(\sigma_n^2 + P_A \left|h_{AB}\right|^2\right)\right]^2 \ln 2} \\ &\quad \times \left[R_0^2 \left|h_{AB}\right|^2 + 2\, R_0 \frac{W_B \left|h_{AB}\right|^2}{\ln 2}\right] \\ &\leq 0, \end{aligned}$$

which indicates that $\partial u_A\left(P_A, 0\right)/\partial P_A$ monotonically decreases with respect to P_A. Moreover, we can have

$$\lim_{P_A \to 0^+} \left[\frac{\rho L}{R_0^2} \frac{W_B \left|h_{AB}\right|^2}{\left(P_A \left|h_{AB}\right|^2 + \sigma_n^2\right) \ln 2}\right] \to +\infty.$$

Therefore, when $P_A \to 0^+$ holds, we can have $\partial u_A\left(P_A, 0\right)/\partial P_A > 0$.

If (25d) holds, we have

$$\begin{aligned} \frac{\partial u_A\left(P_A, 0\right)}{\partial P_A}\Big|_{P=P_{\max}} &= \frac{\rho L}{\left(R_0^m\right)^2} \frac{W_B \left|h_{AB}\right|^2}{\left(P_{\max} \left|h_{AB}\right|^2 + \sigma_n^2\right) \ln 2} - C_A \\ &< 0. \end{aligned}$$

Therefore, we know that there is only one solution which satisfies $\partial u_A\left(P_A, 0\right)/\partial P_A = 0$, and the solution is given by (19). From the above derivation, we can see the monotonicity of the function $u_A\left(P_A, 0\right)$ with respect to P_A. Thus, $u_A\left(P_A, 0\right)$ achieves the maximum value at $P = P_A{}^*$, i.e., (17) also holds for $(P_A{}^*, 0)$. In this way, we have completed the proof of Lemma 1.

In the following Lemma 2, we provide an NE $(P_{max}, 0)$ result.

Lemma 2: The game has an NE $(P_{max}, 0)$, if

$$\begin{cases} \theta_E \geq \dfrac{\rho L\left(R_0^m - R_1^m\right)}{R_0^m R_1^m}, & \text{(21a)} \\ \theta_J \geq \dfrac{\rho L\left(R_0^m - R_2^m\right)}{R_0^m R_2^m}, & \text{(21b)} \\ \theta_S \geq \dfrac{\rho L\left(R_0^m - R_3^m\right)}{R_0^m R_3^m}, & \text{(21c)} \\ C_A \leq \dfrac{\rho L}{\left(R_0^m\right)^2} \dfrac{\left|h_{AB}\right|^2}{\left(P_{\max} \left|h_{AB}\right|^2 + \sigma_n^2\right) \ln 2}, & \text{(21d)} \end{cases}$$

where the superscript m in R_0^m, R_1^m, R_2^m and R_3^m represents that P_A is P_{max} in R_0, R_1, R_2 and R_3, respectively.

Algorithm 1: Q-Learning Based Power Allocation Algorithm

1: Initialize all parameters
2: **for** each time slot n **do**
3: Update the system state $\boldsymbol{s^n} = [q^{n-1}]$
4: Choose a transmit power P_n using the ε-greedy policy
5: Choose the proportion ρ of tasks to compute in local
6: Observe the attack types $\boldsymbol{q_n}$ and the utility of Alice u_A
7: Update the Q function:
$Q(\boldsymbol{s^n}, {P_A}^n) = (1-\alpha)Q(\boldsymbol{s^n}, {P_A}^n) + \alpha(u_A(\boldsymbol{s^n}, {P_A}^n) + \delta V(\boldsymbol{s^{nC1}}))$
8: Find the optimal value function:
$V(\boldsymbol{s^n}) = \max_{0 \le P_A \le P_{max}} Q(\boldsymbol{s^n}, P_A)$
9: **end for**

Proof 2: Similar to the proof of Lemma 1, if (21d) holds, we have

$$\left.\frac{\partial u_A\left(P_A, 0\right)}{\partial P_A}\right|_{P=P_{\max}} = \frac{\rho L}{\left(R_0^m\right)^2} \frac{W_B \left|h_{AB}\right|^2}{\left(P_{\max}\left|h_{AB}\right|^2 + \sigma_n^2\right) \ln 2} - C_A \geq 0.$$

As $\partial u_A\left(P_A, 0\right)/\partial P_A$ decreases monotonically with respect to P_A, we can find that $u_A\left(P_A, 0\right)$ is increasing monotonically, and it can achieve the maximum value at $P_A = P_{max}$. i.e., (17) holds for $(P_{max}, 0)$.

If (21a)-(21c) hold, from (16), we have

$$u_E\left(P_{\max}, 0\right) - u_E\left(P_{\max}, 1\right) = \frac{\rho L}{R_0^m} - \left(\frac{\rho L}{R_1^m} - \theta_E\right) \geq 0,$$
$$u_E\left(P_{\max}, 0\right) - u_E\left(P_{\max}, 2\right) = \frac{\rho L}{R_0^m} - \left(\frac{\rho L}{R_2^m} - \theta_J\right) \geq 0,$$
$$u_E\left(P_{\max}, 0\right) - u_E\left(P_{\max}, 3\right) = \frac{\rho L}{R_0^m} - \left(\frac{\rho L}{R_3^m} - \theta_S\right) \geq 0.$$

Thus, (18) also holds for $(P_{max}, 0)$. In this way, we have completed the proof of Lemma 2.

IV. POWER ALLOCATION ALGORITHM

In this paper, we describe the power allocation algorithm for the Alice, which is of vital importance for the system benefits of both Alice and Eve. Specifically, the parameters are firstly initialized, and then Alice uses a ε-greedy strategy to select the transmit power as her current action strategy. After that, Eve selects an attack mode as its behavioral strategy. The Q function $Q(s, P_A)$ is related to the system state s as well as the power P_A, and the system state s on time slot t is the attack mode of Eve on time slot $t-1$. The value function $V(s)$ records the optimal value of the Q function $Q(s, P_A)$. We set the learning rate to $\alpha \in [0, 1]$, and the discount factor to $\delta \in [0, 1]$. Finally, through repeated learning, a solution of the power allocation for the Alice can be achieved. The whole procedure of the power allocation algorithm can be summarized in Algorithm 1.

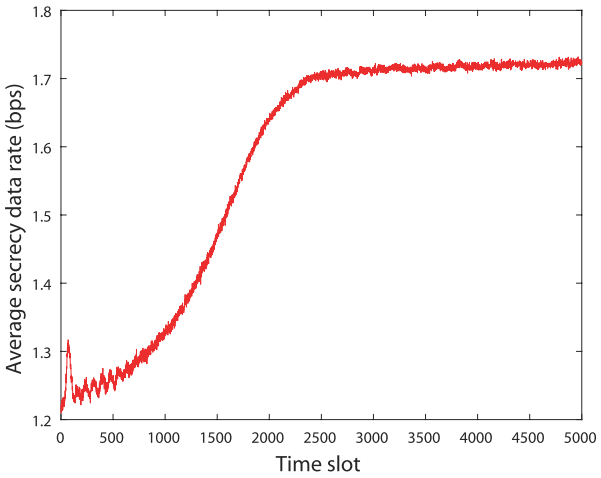

FIGURE 2. Average secrecy data rate of the MEC networks versus the time slot: $\rho = 0.1$.

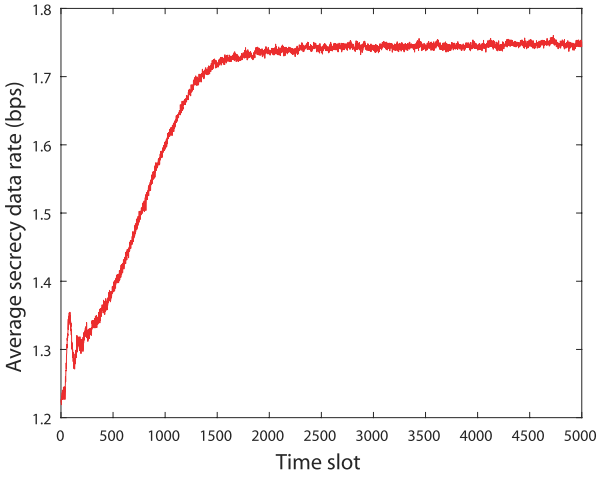

FIGURE 3. Average secrecy data rate of the MEC networks versus the time slot: $\rho = 0.5$.

V. SIMULATION RESULTS

In this part, we perform some simulation experiments by using Matlab to verify the effectiveness of the proposed secure communication strategy. The main parameters are set as follows. The average channel gain of the main channel, σ_{ab}^2, is set to 1.2; the average channel gain of the eavesdropping link, σ_{ae}^2, is set to 0.2; and the average channel gain of the jamming and spoofing link, σ_{be}^2, is set to 0.6 [39], [40]. The noise power is set to 1, and the wireless bandwidth W_B is set to 100MHz. The task size L is set to 100Mbit, and CPU cycle required for one-bit, η, is set to 10. Moreover, we set $f_A = 1$GHz, and $f_B = 20$GHz. The cost coefficient of the transmit power at the Alice, C_A, is set to 0.1, and the influence coefficient of the spoofing, γ, is set to 0.6. In further, the eavesdropping attack cost θ_E is se to 2.6, the jamming attack cost θ_J is set to 2.8, and the spoofing attack cost θ_S is set to 3.

Figs. 2-4 demonstrate the variation of the secrecy data rate versus the time slot, where several values of the offloading ratio ρ are used. Specifically, Fig. 2, Fig. 3 and Fig. 4

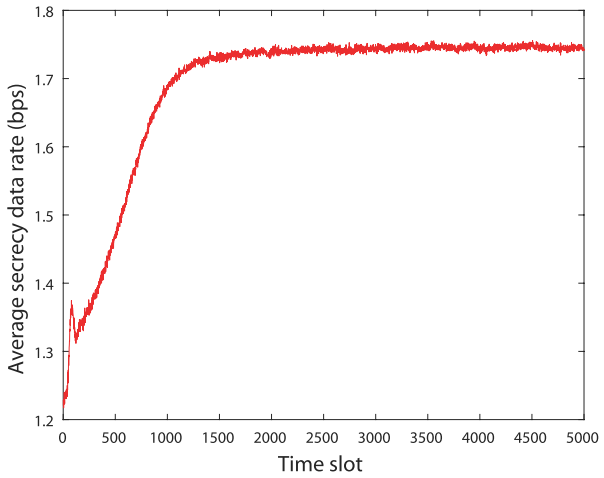

FIGURE 4. Average secrecy data rate of the MEC networks versus the time slot: $\rho = 0.8$.

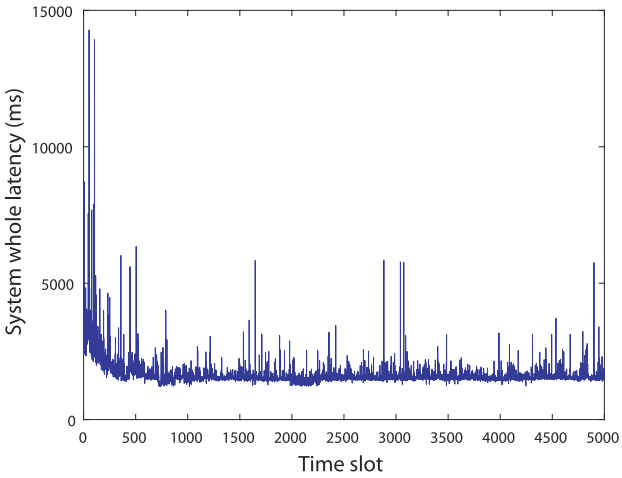

FIGURE 6. The system latency of the MEC networks versus the time slot: $\rho = 0.5$.

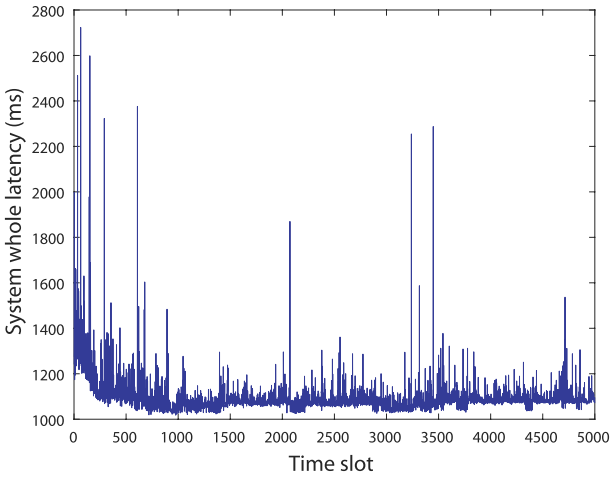

FIGURE 5. The system latency of the MEC networks versus the time slot: $\rho = 0.1$.

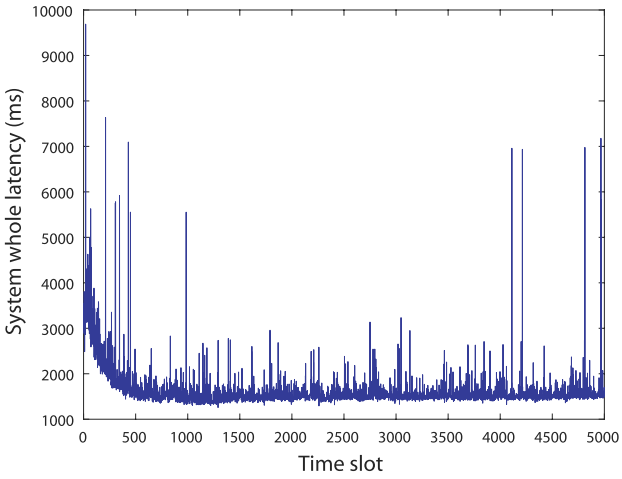

FIGURE 7. The system latency of the MEC networks versus the time slot: $\rho = 0.8$.

correspond to $\rho = 0.1$, $\rho = 0.5$ and $\rho = 0.8$, respectively. We can observe from Figs. 2-4 that after some trials, a stable secrecy data rate can be achieved for different values of the offloading ratio. In particular, a stable secrecy data rate of 1.72 bps/Hz can be achieved after 2300 times of trial when $\rho = 0.1$; a stable secrecy data rate of 1.74 bps/Hz can be achieved after 1500 times of trial when $\rho = 0.5$; and a stable secrecy data rate of 1.75 bps/Hz can be achieved after 1200 times of trial when $\rho = 0.8$. These results clearly indicate that a stable secrecy performance can be achieved for the MEC networks after some trials for different values of ρ, which verifies the effectiveness of the proposed power allocation scheme.

Figs. 5-7 illustrate the variation of the system whole latency of the considered MEC networks versus the time slot, where several values of the offloading ratio ρ are used. In particular, Fig. 5, Fig. 6 and Fig. 7 are associated with $\rho = 0.1$, $\rho = 0.5$ and $\rho = 0.8$, respectively. We can find from Figs. 5-7 that after some trials, a stable latency performance can be achieved for different values of the offloading ratio. In particular, a stable latency of 1.1s can be achieved after 1000 times of trial when $\rho = 0.1$; a stable latency of 1.5s can be achieved after 800 times of trial when $\rho = 0.5$; and a stable latency of 1.6s can be achieved after 500 times of trial when $\rho = 0.8$. These results clearly indicate that a stable latency performance can be achieved for the MEC networks after some trials for different values of ρ, which further verifies the effectiveness of the proposed power allocation scheme.

Figs. 8-10 demonstrate the variation of the attack rate versus the time slot, where several values of the offloading ratio ρ are used. Specifically, Fig. 8, Fig. 9 and Fig. 10 correspond to $\rho = 0.1$, $\rho = 0.5$ and $\rho = 0.8$, respectively. We can observe from Figs. 8-10 that after some trials, a stable attack rate can be achieved for different values of the offloading ratio. In particular, a stable attack rate of 0.138 can be achieved after 2500 times of trial when $\rho = 0.1$; a stable attack rate of 0.136 can be achieved after 2000 times of trial when $\rho = 0.5$; and a stable attack rate of 0.140 can be achieved

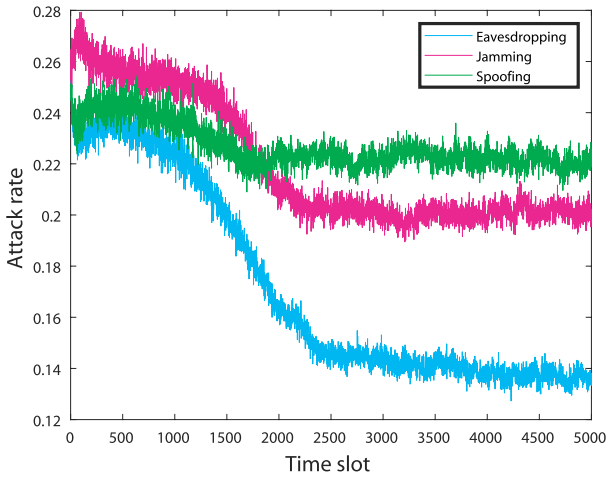

FIGURE 8. The attack rate of the MEC networks versus the time slot: $\rho = 0.1$.

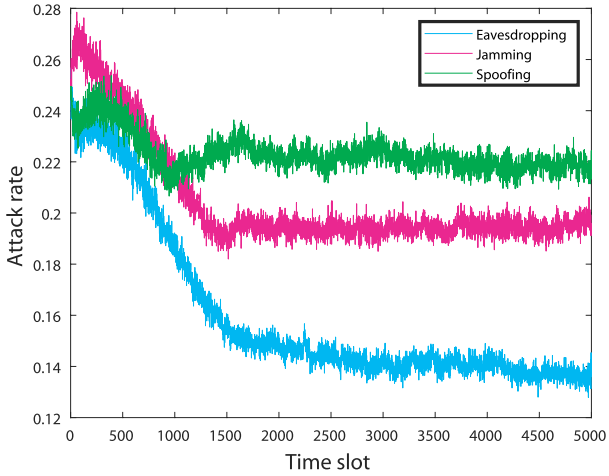

FIGURE 9. The attack rate of the MEC networks versus the time slot: $\rho = 0.5$.

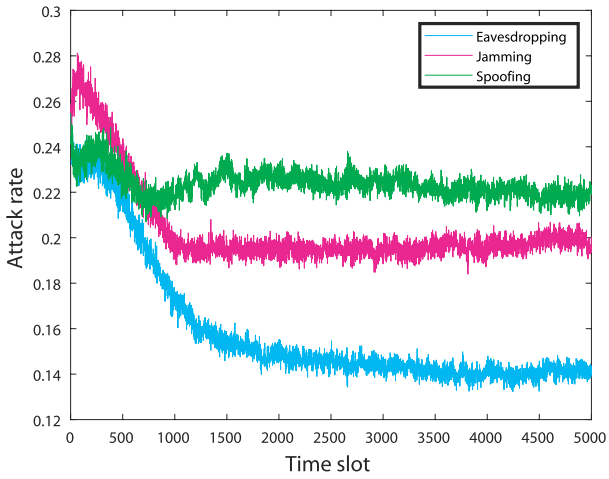

FIGURE 10. The attack rate of the MEC networks versus the time slot: $\rho = 0.8$.

after 2000 times of trial when $\rho = 0.8$. These results clearly indicate that a stable attack rate can be achieved for the MEC networks after some trials for different values of ρ, which verifies the effectiveness of the proposed power allocation scheme furthermore.

VI. CONCLUSION

In this paper, we studied an MEC network where the transmitter had some computational tasks to be computed, under the environments of intelligent attacker. Due to the limited computational capability, the sender needed to offload some tasks to the receiver. By combining the technology of reinforcement learning and game theory, this paper proposed a power allocation algorithm in order to achieve the optimal secure data rate and meanwhile reduce the whole task latency of both the communication and computation with the Q-learning and Nash equilibrium. Then, the Nash equilibrium and its existence conditions were derived and proven mathematically. Finally, some simulations under Matlab platform were demonstrated to show that the proposed algorithm can effectively improve the secrecy data rate and reduce the whole system latency. In future works, we will incorporate some other wireless transmission techniques, such as UAV [41], massive MIMO [42], and deep learning technique [43], [44] into the considered MEC networks, in order to further reduce the system latency and energy consumption.

DATA AVAILABILITY

The data of this work can be available through the request on the corresponding author by e-mail.

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] J. Su, Z. Sheng, A. X. Liu, Z. Fu, and Y. Chen, "A time and energy saving-based frame adjustment strategy (TES-FAS) tag identification algorithm for UHF RFID systems," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 2974–2986, May 2020.

[2] Z. Na, J. Lv, F. Jiang, M. Xiong, and N. Zhao, "Joint subcarrier and subsymbol allocation-based simultaneous wireless information and power transfer for multiuser GFDM in IoT," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5999–6006, Aug. 2019.

[3] J. Su, Y. Chen, Z. Sheng, Z. Huang, and A. X. Liu, "From M-ary query to bit query: A new strategy for efficient large-scale RFID identification," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2381–2393, Apr. 2020.

[4] Y. Mostofi, "Compressive cooperative sensing and mapping in mobile networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 12, pp. 1769–1784, Dec. 2011.

[5] J. Su, A. X. Liu, Z. Sheng, and Y. Chen, "A partitioning approach to RFID identification," *IEEE/ACM Trans. Netw.*, early access, Jul. 10, 2020, doi: 10.1109/TNET.2020.3004852.

[6] D. Zhao, H. Ma, S. Tang, and X.-Y. Li, "COUPON: A cooperative framework for building sensing maps in mobile opportunistic networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 2, pp. 392–402, Feb. 2015.

[7] H. M. La, W. Sheng, and J. Chen, "Cooperative and active sensing in mobile sensor networks for scalar field mapping," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 45, no. 1, pp. 1–12, Jan. 2015.

[8] P. Ockenden, "Over five years, mobile devices have risen from 3% of Web traffic to become the main source," IEEE, New York, NY, USA, Tech. Rep. 2, 2016.

[9] X. Chen, Q. Shi, L. Yang, and J. Xu, "ThriftyEdge: Resource-efficient edge computing for intelligent IoT applications," *IEEE Netw.*, vol. 32, no. 1, pp. 61–65, Jan. 2018.

[10] S. Oueida, Y. Kotb, M. Aloqaily, Y. Jararweh, and T. Baker, "An edge computing based smart healthcare framework for resource management," *Sensors*, vol. 18, no. 12, p. 4307, Dec. 2018.

[11] H. Ching-Hsien, S. Wang, Y. Zhang, and K. Anna, "Mobile edge computing," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–3, Jun. 2018.

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

[13] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, "Collaborative mobile edge computing in 5G networks: New paradigms, scenarios, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 4, pp. 54–61, Apr. 2017.

[14] L. Ji and S. Guo, "Energy-efficient cooperative resource allocation in wireless powered mobile edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4744–4754, Jun. 2019.

[15] J. Su, Z. Sheng, A. X. Liu, Y. Han, and Y. Chen, "A group-based binary splitting algorithm for UHF RFID anti-collision systems," *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 998–1012, Feb. 2020.

[16] C. Li, W. Chen, J. Tang, and Y. Luo, "Radio and computing resource allocation with energy harvesting devices in mobile edge computing environment," *Comput. Commun.*, vol. 145, pp. 193–202, Sep. 2019.

[17] L. Liu, Z. Chang, X. Guo, S. Mao, and T. Ristaniemi, "Multiobjective optimization for computation offloading in fog computing," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 283–294, Feb. 2018.

[18] Z. Wang, Z. Han, L. Yan, and S. Yang, "Cooperative scheduling of multi-core and cloud resources: Multi-thread-based MCC offloading strategy," *IET Commun.*, vol. 13, no. 14, pp. 2146–2154, Aug. 2019.

[19] Z. Jiang and S. Mao, "Energy delay tradeoff in cloud offloading for multi-core mobile devices," *IEEE Access*, vol. 3, pp. 2306–2316, 2015.

[20] M. Zhou, Y. Wang, Y. Liu, and Z. Tian, "An information-theoretic view of WLAN localization error bound in GPS-denied environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4089–4093, Apr. 2019.

[21] *Radio Channel Communication*, M Corp., IEEE, New York, NY, USA, 2015.

[22] K. Li, "A game theoretic approach to computation offloading strategy optimization for non-cooperative users in mobile edge computing," *IEEE Trans. Sustain. Comput.*, early access, Sep. 5, 2018, doi: 10.1109/TSUSC.2018.2868655.

[23] S. Gurun, R. Wolski, C. Krintz, and D. Nurmi, "On the efficacy of computation offloading decision-making strategies," *Int. J. High Perform. Comput. Appl.*, vol. 22, no. 4, pp. 460–479, Nov. 2008.

[24] M. Zhou, Y. Liu, Y. Wang, and Z. Tian, "Anonymous crowdsourcing-based WLAN indoor localization," *Digit. Commun. Netw.*, vol. 5, no. 4, pp. 226–236, Nov. 2019.

[25] M. E. Khoda, M. A. Razzaque, A. Almogren, M. M. Hassan, A. Alamri, and A. Alelaiwi, "Efficient computation offloading decision in mobile cloud computing over 5G network," *Mobile Netw. Appl.*, vol. 21, no. 5, pp. 777–792, Oct. 2016.

[26] J. Xia, "Opportunistic access point selection for mobile edge computing networks," *IEEE Trans. Wireless Commun.*, no. 99, pp. 1–12, 2020.

[27] R. Zhao, "Deep reinforcement learning based mobile edge computing for intelligent Internet of Things," *Phys. Commun.*, pp. 1–8, 2020.

[28] S. Lai, "Intelligent secure mobile edge computing for beyond 5G wireless networks," *Phys. Commun.*, pp. 1–8, 2020.

[29] Y. Guo, Z. Zhao, R. Zhao, S. Lai, Z. Dan, J. Xia, and L. Fan, "Intelligent offloading strategy design for relaying mobile edge computing networks," *IEEE Access*, vol. 8, pp. 35127–35135, 2020.

[30] Z. Zhao, W. Zhou, D. Deng, J. Xia, and L. Fan, "Intelligent mobile edge computing with pricing in Internet of Things," *IEEE Access*, vol. 8, pp. 37727–37735, 2020.

[31] R. Zhao, "Intelligent physical-layer secure communications for beyond 5G wireless networks," *Phys. Commun.*, pp. 1–8, 2020.

[32] Z. Zhao, R. Zhao, J. Xia, X. Lei, D. Li, C. Yuen, and L. Fan, "A novel framework of three-hierarchical offloading optimization for MEC in industrial IoT networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5424–5434, Aug. 2020.

[33] Y. Cao, N. Zhao, F. R. Yu, M. Jin, Y. Chen, J. Tang, and V. C. M. Leung, "Optimization or alignment: Secure primary transmission assisted by secondary networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 905–917, Apr. 2018.

[34] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, "UAV-relaying-assisted secure transmission with caching," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3140–3153, May 2019.

[35] N. Zhao, Y. Li, S. Zhang, Y. Chen, W. Lu, J. Wang, and X. Wang, "Security enhancement for NOMA-UAV networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 3994–4005, Apr. 2020.

[36] J. Xia, L. Fan, W. Xu, X. Lei, X. Chen, G. K. Karagiannidis, and A. Nallanathan, "Secure cache-aided multi-relay networks in the presence of multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7672–7685, Nov. 2019.

[37] 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 Trans. Commun.*, vol. 66, no. 5, pp. 2281–2294, May 2018.

[38] C. Shannon and W. Weaver, *The Mathematical Theory of Communication*. New Providence, NJ, USA: Bell Lab, 1949.

[39] Z. Na, Y. Liu, J. Shi, C. Liu, and Z. Gao, "UAV-supported clustered NOMA for 6G-enabled Internet of Things: Trajectory planning and resource allocation," *IEEE Internet Things J.*, early access, Jun. 23, 2020, doi: 10.1109/JIOT.2020.3004432.

[40] H. Xie, F. Gao, S. Zhang, and S. Jin, "A unified transmission strategy for TDD/FDD massive MIMO systems with spatial basis expansion model," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3170–3184, Apr. 2017.

[41] Z. Na, J. Wang, C. Liu, M. Guan, and Z. Gao, "Join trajectory optimization and communication design for UAV-enabled OFDM networks," *Ad Hoc Netw.*, vol. 98, Mar. 2020, Art. no. 102031.

[42] B. Wang, F. Gao, S. Jin, H. Lin, and G. Y. Li, "Spatial- and frequency-wideband effects in millimeter-wave massive MIMO systems," *IEEE Trans. Signal Process.*, vol. 66, no. 13, pp. 3393–3406, Jul. 2018.

[43] K. He, "Ultra-reliable MU-MIMO detector based on deep learning for 5G/B5G-enabled IoT," *Phys. Commun.*, pp. 1–8, 2020.

[44] J. Xia, D. Deng, and D. Fan, "A note on implementation methodologies of deep learning-based signal detection for conventional MIMO transmitters," *IEEE Trans. Broadcast.*, early access, Apr. 27, 2020, doi: 10.1109/TBC.2020.2985592.

YING SUN received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Harbin Institute of Technology, Harbin, China, in 2008, 2010, and 2018, respectively. She is currently a Researcher with the Guangzhou Power Supply Bureau of China Southern Power Grid, China. Her research interests include marketing, power big data application, and advanced metering infrastructure (AMI).

ZHIPENG SU received the B.Sc. degree in electrical engineering and automation from the South China University of Technology, Guangzhou, China, in 1991. He is currently the Director with the Guangzhou Power Supply Bureau of China Southern Power Grid, China. His research interests include marketing, power business environment, energy trading, and advanced metering infrastructure (AMI).

YING ZHAO received the B.Sc. degree in information and computing science from the North China University of Water Resources and Electric Power, Zhengzhou, China, in 2005. He is currently a Section Chief with the Guangzhou Power Supply Bureau of China Southern Power Grid, China. His research interests include marketing, power informatization, and advanced metering infrastructure (AMI).

DAN DENG (Member, IEEE) received the bachelor's and Ph.D. degrees from the Department of Electronic Engineering and Information Science, University of Science and Technology of China, in 2003 and 2008, respectively. From 2008 to 2014, he was with Comba Telecom Ltd., Guangzhou, China, as a Director. Since 2014, he has joined Guangzhou Panyu Polytechnic, where he is currently an Associate Professor. His research interests include MIMO communication and physical-layer security in next-generation wireless communication systems. He has published 45 papers in international journals and conferences. Also, he holds 19 patents, and has served as a member of Technical Program Committees for several conferences.

FUSHENG ZHU received the B.E. degree in electronic and information engineering from the Huazhong University of Science and Technology, in 1996, and the M.B.A. degree from Fudan University, in 2011. He was the Chief Engineer of ZTE Wireless, while he was responsible for research and development of ZTE since he joined the company, in 1996. He was appointed as the President of the Guangdong New Generation Communication and Network Innovative Institute (GDCNi), in 2018. His research direction mainly include 6G mobile network and B5G vertical application, and network communication.

JUNJUAN XIA (Member, IEEE) received the bachelor's degree from the Department of Computer Science, Tianjin University, in 2003, and the master's degree from the Department of Electronic Engineering, Shantou University, in 2015. She currently works with the School of Computer Science and Cyber Engineering, Guangzhou University, as a Laboratory Assistant. Her current research interests include wireless caching, physical-layer security, cooperative relaying, and interference modeling.