Security Energy Efficiency Maximization for Untrusted Relay Assisted NOMA-MEC Network With WPT

PINFANG ZHAO, WEI ZHAO, (Member, IEEE), HUI BAO, AND BAOGANG LI, (Member, IEEE)

Department of Electronic and Communication Engineering, North China Electric Power University, Baoding 071003, China

Corresponding author: Wei Zhao (andyzhaoster@163.com)

This work was supported in part by the Natural Science Foundation of China under Project 61971190 and Project 61501185, in part by the Natural Science Foundation of Hebei under Project F2016502062, and in part by the Fundamental Research Funds for the Central Universities under Project 2019MS089 and Project 2015MS95.

ABSTRACT Relay assisted transmission can effectively improve the range of coverage and offloading efficiency of non-orthogonal multiple access-mobile edge computing (NOMA-MEC) system. However, the relay will become untrusted relay when it is attacked by malicious users, resulting in the leakage of information. To solve this problem, this article uses destination-assisted jamming to prevent the leakage of information during the offloading process. Under the condition of time delay and energy consumption, we jointly optimize the transmission power allocated to relay, central processing unit (CPU) frequency and offloading time to maximize the security energy efficiency of the user (UE). Since it is a non-convex multi-objective optimization problem, it is decomposed into several suboptimal single-objective sub-problems, and the single-objective sub-problems are transformed into convex problems by Taylor approximation method, then be solved by Lagrange dual method. Besides, the multi-objective iterative algorithm (MOIA) is further proposed to achieve joint optimal solution. The simulation results show that the proposed method can effectively improve the security offloading performance and security energy efficiency compared with other relay assisted offloading methods.

INDEX TERMS Non-orthogonal multiple access-mobile edge computing, untrusted relay, offloading, destination-assisted jamming, security energy efficiency.

I. INTRODUCTION

With the development of the Internet of Things (IoT) and the popularization of multimedia applications, Internet traffic has increased 17 times in the past five years, and explosive growth in the future is inevitable [1]. The ensuing demand for emerging business continues to grow. For example, a large scale fast-growing data generated in intelligent transportation systems (ITS) has become a ponderous burden on the coordination of heterogeneous transportation networks, which makes the traditional cloud-centric storage architecture no longer satisfy new data analytics requirements [2]. Mobile edge computing (MEC) has been considered a key technology to meet the stringent computation latency requirements of emerging business. It sinks the computing ability to the edge, which can significantly improve the computing efficiency of mobile users [3], [4]. Non-orthogonal multiple access (NOMA) plays an important role in improving spectrum efficiency, providing a large number of connections, and reducing latency [5]. Power multiplexing technology assigns different power to the signals of different users, and superimposes coding at the transmitter. The receiver with successive interference cancellation (SIC) detects multiuser interference imposed by other users [6], [7]. Wireless power transmission (WPT) can effectively solve the energy limitation of IoT devices [8].

Applying NOMA technology to the MEC network is an important innovation that takes advantage of the utilization of both NOMA’s spectrum and MEC’s computing resources. Literature [9] studied the influence of NOMA on the uplink and downlink transmission of MEC offloading, the results showed that the use of NOMA can effectively reduce the
delay and energy consumption of users offloading. In the case of ensuring that the transmission quality of the far user is not inferior to that of orthogonal multiple access (OMA) transmission, the authors in [10] optimized the transmission power of near users in different time slots to minimize delay according to the discussion of the near-user energy level. Reference [11] minimized the energy consumption of offloading by jointly optimizing power and time allocation. The optimal user NOMA pairing method was proposed in [12]. Reference [13] proved that NOMA has better delay performance than time-division multiple access (TDMA) in MEC system.

The above literatures do not take into account the terminal energy-limited devices in wireless network system. For this problem, wireless power transmission (WPT) technology was considered to be applied to MEC systems [14], [15]. In this regard, literature [16] combined WPT, NOMA, and MEC technologies to jointly optimize energy harvesting time, local CPU frequency, operation mode selection, offloading time, and power to improve system computing efficiency. In the same scenario, the rate adaptive computing task is considered to maximize the total computing speed of all users in [17]. In order to further improve the energy efficiency, a full-duplex multi-cluster NOMA-MEC system based on WPT was proposed in [18], which significantly reduced the overall energy consumption of the system through power control, time scheduling and offload data distribution.

However, distance is also an important factor affecting energy consumption and delay due to the offloading process in the MEC system. For smart devices, long distance will directly reduce the transmission rate and quality of information, thus affecting the energy consumption and delay of transmission. Relay can effectively improve the coverage of IoT, assist users in offloading and performing energy capture. Literature [19] considered that the relay has the function of computing and transmission, in which the users computed and exchanged the calculation results with the help of relay. Reference [20] used the time slot computing method to allow relay to perform cooperative computing and transmission in different time slots, which effectively improved the system offloading delay and total energy consumption. Two-way relay performed collaborative communication and collaborative computing was studied in [21], which optimized the proportion of offloading data to minimize the energy consumption of the system under conditions of limited latency. In the MEC system considered WPT, far user utilized near user for coordinated power collection and coordinated offloading, optimized transmission power and offloading strategies by two-phase method to minimize the access point (AP) node energy consumption [22]. On this basis, literature [23] considered that there is no direct link between the user and the edge server, and jointly optimized the offload task volume, offload time, and WPT time to reduce offloading time and energy costs.

The deployment of relays can take many advantages, but it also increases the risk of information leakage. Reference [24] considered that the energy-limited relay node is untrusted and assists malicious users to eavesdrop information. At the destination node, the cooperative jamming method was used to optimize the secrecy outage probability and the ergodic secrecy rate of the system, then got the optimal transmission method. In [25], a downlink single-input single-output non-orthogonal multiple access setting was considered, in which two relay working modes of amplify-and-forward and compress-and-forward were adopted. The users transmitted a cooperative jamming signal simultaneously, which improved the secure rate of downlink transmission of the system. However, the studies of untrusted relay do not consider the impact on the MEC system. So it is critical to solve the security offloading problem of untrusted relay assisted non-orthogonal multiple access-mobile edge computing (NOMA-MEC) system for the information security of the system.

The research of physical layer security in MEC has become one of the key issues. Literature [26] adopted the method of jointly optimizing local offloading, transmission power and subcarrier allocation to realize the security offloading of multi-user multi-carrier systems and minimize the energy consumption of the system under the condition of limited delay and secrecy offloading rate. A novel physical-layer security method was proposed to prevent eavesdropping users stealing offloading information, in which the jamming signals is considered [27]. On this basis, the joint optimization of the security offloading rate and power distribution was used to effectively improve the physical layer security performance in the NOMA-MEC system [28]. Literature [29] proposed a novel iteration algorithm, in which the CPU frequency and transmission power are jointly optimized to maximize secure computation efficiency of NOMA-MEC network, and the simulation results proved the effectiveness of the proposed method. But these studies did not consider the cooperative computing and communication of relay.

In this article, an untrusted relay assisted NOMA-MEC system is considered. Specifically, considering the leakage of information at the relay, the destination-assisted jamming is proposed to improve the security by interfering untrusted relay and reducing the received signal-to-noise ratio at relay. Furthermore, the security energy efficiency is considered as the object function to evaluate the security of offloading. As far as we know, the physical-layer security of untrusted relay assisted MEC to offload by NOMA transmission has not been studied.

A. MOTIVATION AND CONTRIBUTIONS

With the advent of the 5G era [30], reasonable resource allocation becomes particularly important. MEC technology can solve the business computing problem of energy-limited and resource-limited IoT devices, and has become one of the key technologies of 5G. Furthermore, it has been found that applying NOMA technology to MEC system can effectively reduce the delay and energy consumption of MEC offloading. However, due to the offloading process in the MEC system, distance is also an important factor affecting energy
consumption and delay. For smart devices, long distance will directly reduce the transmission rate and quality of information, thus affecting the energy consumption and delay of transmission. Relay can effectively improve the coverage of IoT, assist users in offloading and performing energy capture. The deployment of relays brings many advantages, but it also increases the risk of information leakage. Especially when it is attacked by malicious users and becomes an untrusted relay, the offloading security of the MEC system becomes particularly important. Motivated by this, an untrusted relay assisted NOMA-MEC network with WPT is considered. To prevent the leakage of offloading information at the relay, this article uses destination-assisted jamming to prevent the leakage of information during the offloading process. As far as we know, the physical-layer security of untrusted relay assisted MEC to offload by NOMA transmission has not been studied. In this article, the security energy efficiency maximization for untrusted relay assisted NOMA-MEC network with WPT is considered under the condition of time delay and energy consumption.

The physical-layer security has been studied in [26] and [28], but the security of system only be considered as a constraint, not as an important performance index. Different from others, in this article, we take the security energy efficiency as the object function, in which the security offloading rate and the energy consumption of user are considered comprehensively. We jointly optimize the user’s transmission power, CPU frequency and offloading time to maximize the security energy efficiency of the user under the condition of time delay and energy consumption. Since it is a non-convex multi-objective optimization problem, it is decomposed into several suboptimal single-objective sub-problems, and the single-objective sub-problems are transformed into convex problems by Taylor approximation method, then solved by Lagrange dual method. Alternative iterative algorithm is proposed to jointly optimize the transmission power, CPU frequency and offloading time, which aim to maximize the security energy efficiency.

As far as we know, NOMA transmission has not been used in the relay assisted MEC system compared with literature [19]–[23], literature [24], [25] studied the traditional three-node communication model, namely the source node, untrusted relay, and destination node. However, the studies of untrusted relay do not consider the impact on the MEC system. The physical-layer security has been studied in [26] and [28], but the security of system only be considered as a constraint, not as an important performance index. Different from others, in this article, we take the security energy efficiency as the object function, and the security energy efficiency is defined as the ratio of security offloading rate to energy consumption, in which the security offloading rate and the energy consumption of user are considered comprehensively. And we use the security energy efficiency to evaluate the reliability of the message which are offloaded by relay under normalized frequency spectrum and given delay constraints. The greater the security energy efficiency value, the higher the reliability of the message which are offloaded by relay. As far as we know, the physical-layer security of untrusted relay assisted MEC to offload by NOMA transmission has not been studied. So this article consider the security energy efficiency of untrusted relay assisted MEC to offload by NOMA transmission.

The contributions of our work are as follows:

- In the relay-assisted MEC system, NOMA transmission is considered to improve offloading performance.
- Considering that when the relay is attacked by a malicious eavesdropper and becomes an untrusted relay, we study the security performance of the NOMA-MEC system. And destination-assisted jamming is considered to prevent the leakage of information during the offloading process.
- The security offloading rate and the energy consumption of user are considered comprehensively. We jointly optimize the user’s transmission power, CPU frequency and offloading time to maximize the security energy efficiency of the user under the condition of time delay and energy consumption.
- Since the object function is a non-convex multi-objective optimization problem, it is decomposed into several suboptimal single-objective sub-problems, and the single-objective sub-problems are transformed into convex problems by Taylor approximation method, then solved by Lagrange dual method. Alternative iterative algorithm is proposed to jointly optimize single objective optimal solution to maximize the security energy efficiency.
- The simulation results show that the relay can achieve security transmission after taking destination-assisted jamming and the security energy efficiency of taking destination-assisted jamming is significantly better than that without taking destination-assisted jamming. It also shows that the security energy efficiency of NOMA transmission is better than OMA transmission.

B. ORGANIZATION

The remainder of this article is organized as follows. The system model is presented in Section II. We formulate the optimization problem in detail and describe its solutions in Section III. Simulation results are presented in Section IV. Finally, we draw our conclusions in Section V.

II. SYSTEM MODEL

As shown in figure 1, the untrusted relay assisted NOMA-MEC system model is considered, which consists of a user (UE), a mobile edge computing (MEC) server, an untrusted relay, UE transmits the data to be offloaded through the downlink power-domain NOMA technology. The untrusted relay and MEC server form a set of NOMA pairs, and the relay is closer to the UE. Therefore, the data offloaded to the relay is transmitted by using the power-domain NOMA with no extra spectrum overhead compared with only offloading to MEC server directly. In addition, the energy consumption of UE to offload data to the relay is expressed as
Since the relay is an untrusted relay, the destination-assisted jamming is adopted to achieve security transmission, which means the MEC server acts as a jamming node to jam the received signal of the relay. The relay received signal is expressed as:

$$y_r = h_{ur}x + h_{mr} \sqrt{p_3} s_3 + n_r$$

where $h_{ur}$ represents the channel gain between the UE and the relay, $h_{mr}$ denotes the channel gain between the UE and the MEC server, and $|h_{ur}|^2 \leq |h_{ur}|^2$. $n_r$ represents the channel gain between the relay and the MEC server, $p_3$ represents the power allocated to relay.
the transmission power of the jamming signal $s_3$ from the server to the relay when the server jamming the relay, and $n_r$ represents the noise of the relay with power $N_0$.

Because the power-domain NOMA is used for transmission, the relay may attempt to decode the message $s_1$, the signal-to-noise ratio (SNR) of the signal received at the relay is expressed as:

$$\gamma_r^1 = \frac{p_1|h_{ur}|^2}{p_3|h_{mr}|^2 + N_0}$$  \hspace{1cm} (6)

The signal received by the server is expressed as:

$$y_m = h_{um}x + n_m$$  \hspace{1cm} (7)

where $n_m$ represents the additive white Gaussian noise received during the relay receiving process with power $N_0$. On the MEC server side, $s_1$ is directly used as noise to decode $s_2$, and the signal-to-noise ratio is:

$$\gamma_m^2 = \frac{|h_{um}|^2 p_2}{|h_{um}|^2 p_1 + N_0}$$  \hspace{1cm} (8)

### C. RELAY FORWARDING TIME SLOT

The relay amplifies and forwards the information to the MEC server for cooperative computing. The signal forwarded after being amplified by the relay is expressed as:

$$y_r^\gamma = \alpha y_r = \sqrt{\frac{p_4}{p_1|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0}} y_r$$  \hspace{1cm} (9)

The transmission signal of the relay received by the MEC server is expressed as:

$$y_r = h_{rm}y_r^\gamma + n_m$$

$$= \alpha(h_{ur}x + h_{mr}\sqrt{p_3 s_3} + n_r)h_{rm}x + n_m$$

$$= \alpha h_{ur}h_{rm}x + \alpha \sqrt{p_3} h_{mr}h_{rm} s_3 + \alpha h_{mn} n_r + n_m$$  \hspace{1cm} (10)

where $n_m$ represents server-side noise, which is additive white Gaussian noise with power $N_0$. Since $s_3$ is the jamming signal sent by the MEC server itself to the relay in the second time slot, the MEC server can remove the term $\alpha \sqrt{p_3} h_{mr}h_{rm} s_3$ from (9) and decode the source information from the rest of the received signal. Thus, the resultant received signal at the MEC server becomes:

$$y_r' = \alpha h_{ur}h_{rm}x + \alpha h_{mn} n_r + n_m$$  \hspace{1cm} (11)

where $\alpha = \sqrt{\frac{p_4}{p_1|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0}}$, then the received signal at the MEC server is:

$$y_r' = \sqrt{\frac{p_4}{p_1|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0}} h_{ur}h_{rm}x$$

$$= \sqrt{\frac{p_4}{p_1|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0}} h_{mn} n_r + n_m$$  \hspace{1cm} (12)

The first term on the right-hand side of (12) represents the useful signal, whereas the second and third terms correspond to the total received noise at the MEC server. Then, the SNR at the destination can be written as:

$$\gamma_m = \frac{p_4|h_{ur}|^2|h_{rm}|^2 p_1}{(p_4|h_{rm}|^2+p_1|h_{ur}|^2+p_3|h_{mr}|^2)N_0 + N_0}$$  \hspace{1cm} (13)

The communication security rate obtained through untrusted relay is expressed as:

$$R_{r \text{ sec}} = B \log_2(1 + \gamma_{rm}) - B \log_2(1 + \gamma_r^1)$$  \hspace{1cm} (14)

Then the overall security transmission rate of the system can be expressed as:

$$R_{\text{sec}} = R_{r \text{ sec}} + B \log_2(1 + \gamma_m^2)$$  \hspace{1cm} (15)

In this process, the total amount of information transmitted by the system is expressed as:

$$d_{off} = d_1 + d_2$$  \hspace{1cm} (16)

$$d_1 = B \log_2(1 + \gamma_{rm} n_1)$$  \hspace{1cm} (17)

$$d_2 = B \log_2(1 + \gamma_m^2 n_2)$$  \hspace{1cm} (18)

### D. MEC SERVER AND LOCAL COMPUTING

The computing delay of MEC server can be expressed as:

$$t_4 = \frac{(d_1 + d_2) b_{MEC}}{f_{MEC}}$$  \hspace{1cm} (19)

where $b_{MEC}$ denotes the number of CPU cycles required by the MEC to compute 1-bit data, $f_{MEC}$ denotes the CPU frequency of server. Considering that the MEC sever has the powerful computation function and the amount of result data returned is small, then the computing delay and the result return delay at the MEC are ignored in subsequent analysis.

In the whole computing cycle, UE can perform local computation, and the amount of data computed locally by UE is expressed as:

$$d_l = \frac{T_f c}{c}$$  \hspace{1cm} (20)

The energy consumed by the local computing is expressed as:

$$e_l = \xi T_f f^3$$  \hspace{1cm} (21)

### III. PROBLEM FORMULATION

In this article, we consider the MEC computation offloading in the presence of untrusted relay, and evaluate the system performance through the UE’s security energy efficiency. We jointly optimize the UE’s transmission power, CPU frequency and offloading time to maximize the security energy efficiency of the UE under the constraint of time delay, data and energy consumption. Without loss of generality, the task offloading time and relay forwarding time are considered the same [23]. The security energy efficiency of the UE is defined as the ratio of total security transmission rate to the energy consumption of the UE. The sum of security transmission can be expressed by:

$$R_{\text{sec}} = R_{r \text{ sec}} + R_m^2$$

$$= B \log_2(1 + \gamma_{rm}) - B \log_2(1 + \gamma_r^1)$$

$$+ B \log_2(1 + \frac{|h_{um}|^2 p_2}{|h_{um}|^2 p_1 + N_0})$$  \hspace{1cm} (22)
The actual energy consumption of the user is expressed by:

\[ Q_E = (p_1 + p_2)t_2 + \frac{\xi T f^3}{c} - \mu((h_{um}|^2 p_m)|h_{um}|^2 p_{mt1}) \]  

(23)

Our goal is to maximize the energy efficiency of UE by optimizing the transmission power, CPU frequency and offloading time. Then the problem P1 is formulated as:

\[
\max_{p_1, f, t_2} \eta = \frac{R_{sec}}{Q_E} 
\]  

(24)

\[
\text{s.t.} \quad \text{Blog}_2(1 + \gamma_{um})t_3 + \text{Blog}_2(1 + \gamma_{um}^2)p_2 + \frac{T f^3}{c} \geq D 
\]  

(24a)

\[
t_1 + t_2 + t_3 = T \quad \text{(24b)}
\]

\[
p_1 + p_2 = p_r \quad \text{(24c)}
\]

\[
e + \mu((h_{um}|^2 p_m)|h_{um}|^2 p_{mt1}) - \xi T f^3(p_1 + p_2)t_2 \geq 0 
\]  

(24d)

\[
R_1 = \text{Blog}_2(1 + \gamma_{um}) \geq r_{th} \quad \text{(24e)}
\]

\[
R_2 = \text{Blog}_2(1 + \gamma_{um}^2) \geq r_{th} \quad \text{(24f)}
\]

\[
R_1 = \text{Blog}_2(1 + \gamma_{um}) = \frac{p_4|h_{ur}|^2|h_{rm}|^2 p_1}{(p_4|h_{rm}|^2 + p_1|h_{ur}|^2 + p_3|h_{mr}|^2)|N_0 + N_0|^2} 
\]  

(25)

\[
R_2 = \text{Blog}_2(1 + \gamma_{um}^2) = \text{Blog}_2(1 + \frac{|h_{um}|^2 p_2}{|h_{um}|^2 p_1 + N_0}) 
\]  

(26)

The constraint (24a) is the offloading data, the constraint (24b) is the limit of time delay, the constraint (24c) is the power constraint, the constraint in (24d) denotes the energy constraint of the UE. the \(r_{th}\) in (24e) and (24f) denotes the minimum transmission rate.

It is difficult to find the optimal solution of the problem due to the fractional form of the objective function, for which the close-form solution of the energy efficiency can hardly be derived, so the Dinkelbach’s method [34] is used to transform it into an equation optimization problem. By using the Dinkelbach’s method, the object function can be transformed into a maximize problem with parameter \(\lambda\).

It can be expressed by \(F(\Pi, \lambda) = R_{sec} - \lambda Q_E\), where \(\Pi\) denotes the collection of \(p_1, f\) and \(t_2\), we regulate the function \(h(\lambda) = \max(\Pi, \lambda)\), for the given \(p_1, f\) and \(t_2\), we can get the optimal \(\lambda^*\) when \(h(\lambda) = 0\), which can be exploited by the following theorem.

**Theorem 1:** \(h(\lambda)\) is convex continuous and decreasing function of \(\lambda\), then we can get the optimal solution of problem P2 when \(F(\Pi, \lambda) = 0\). The proof is given by Appendix.

When the \(\lambda\) is given, then the object function can be rephrased as P2:

\[
P2: \quad \max_{p_1, f, t_2} \eta = R_{sec} - \lambda Q_E 
\]  

(27)

### A. OPTIMIZATION OF TRANSMISSION POWER

We consider the transmission power allocated to relay with given CPU frequency \(f\) and offloading time \(t_2\) now, the objective function can be written as:

\[
P2.1: \quad \max_{p_1} \eta = R_{sec} - \lambda Q_E 
\]  

(28)

The secure rate \(R_{sec}\) causes the objective function (28) to be a non-convex problem. It is approximated as an affine function by using the expansion method of the first-order Taylor series, then the problem is approximated as a convex optimization problem. The \(R_{sec}\) is given by:

\[
R_{sec} = \text{Blog}_2[p_4|h_{rm}|^2 + p_1|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0]|N_0 
\]

\[
+ p_4|h_{ur}|^2|h_{rm}|^2 + 2p_2|h_{mt}|^2 + p_1|p_{mt1}|^2 + |N_0 + N_0|^2 
\]

(29)

The first-order Taylor series expansion of the second term at \(p_0\) in equation (29) can be expressed as:

\[
\text{Blog}_2[p_4|h_{rm}|^2 + p_1|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0]|N_0 
\]

\[
- B|h_{ur}|^2N_0(p_1 - p_0) 
\]

\[
+ \ln[2(|p_4|h_{rm}|^2 + p_0|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0)|N_0] 
\]

\[
+ \phi_1 
\]  

(30)

In the same way, the third and sixth terms are expanded in order according to the second term

\[
\text{Blog}_2[p_4|h_{rm}|^2 + p_1|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0]|N_0 
\]

\[
- B|h_{ur}|^2N_0(p_1 - p_0) 
\]

\[
+ \ln[2(|p_4|h_{rm}|^2 + p_0|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0)|N_0] 
\]

\[
+ \phi_2 
\]  

(31)

Then the transformed secure rate is expressed as:

\[
R^*_{sec} = \text{Blog}_2[p_4|h_{rm}|^2 + p_1|h_{ur}|^2 + p_3|h_{mr}|^2]|N_0 
\]

\[
+ N_0^2 + p_4|h_{ur}|^2|h_{rm}|^2|p_1|^2 
\]

\[
- B|h_{ur}|^2N_0(p_1 - p_0) 
\]

\[
+ \ln[2(|p_4|h_{rm}|^2 + p_0|h_{ur}|^2 + p_3|h_{mr}|^2)|N_0 + N_0^2] 
\]

\[
- B|h_{ur}|^2N_0(p_1 - p_0) 
\]

\[
+ \ln[2(|p_4|h_{rm}|^2 + p_0|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0)|N_0] 
\]

\[
+ \phi 
\]  

(33)

The \(\phi\) in equation (33) be written as:

\[
\phi = \text{Blog}_2[p_3|h_{mr}|^2 + N_0] 
\]

\[
+ \text{Blog}_2[|h_{um}|^2(p_1 + p_2) + N_0] 
\]

\[
+ B|h_{ur}|^2N_0(p_0) 
\]

\[
+ \ln[2(|p_4|h_{rm}|^2 + p_0|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0)|N_0] 
\]
\[ -B \log_2[(p_4|h_{rm}|^2 + p_0|h_{ur}|^2 + p_3|h_{mr}|^2 + N_0)N_0] + B|h_{ur}|^2p_0/\ln 2(p_3|h_{mr}|^2 + p_0|h_{ur}|^2 + N_0) \]
\[ -B \log_2(p_3|h_{mr}|^2 + p_0|h_{ur}|^2 + N_0) + B|h_{um}|^2p_0/\ln 2(h_{um}|^2p_0 + N_0) \]
\[ -B \log_2((h_{um}|^2p_0 + N_0) - \varphi_1 - \varphi_2 - \varphi_3 \quad (34) \]

The first-order Taylor expansion of \( R_1 \) is expressed as:
\[ R_1^* = B \log_2((p_4|h_{rm}|^2 + p_1|h_{ur}|^2 + p_3|h_{mr}|^2)N_0 + N_0^2 + p_4|h_{ur}|^2|h_{rm}|^2p_1] \]
\[ + B|h_{ur}|^2N_0p_1 - \ln 2(|p_4|h_{rm}|^2 + p_0|h_{ur}|^2 + p_3|h_{mr}|^2)N_0 + N_0^2] + \theta_1 \quad (35) \]

The first-order Taylor expansion of \( R_2 \) is expressed as:
\[ R_2^* = B \log_2(|h_{um}|^2(p_1 + p_2) + N_0) \]
\[ - B|h_{um}|^2p_1/\ln 2(|h_{um}|^2p_0 + N_0) + \theta_2 \quad (36) \]

In the equation (35), (36):
\[
\begin{align*}
\theta_1 &= \frac{B|h_{ur}|^2N_0p_0}{\ln 2(|p_4|h_{rm}|^2 + p_0|h_{ur}|^2 + p_3|h_{mr}|^2)N_0 + N_0^2} - B \log_2[p_4|h_{rm}|^2 + p_0|h_{ur}|^2 + p_3|h_{mr}|^2)N_0 + N_0^2] - \varphi_1 \\
\theta_2 &= \frac{B|h_{um}|^2p_0}{\ln 2(|h_{um}|^2p_0 + N_0)} - B \log_2(|h_{um}|^2p_0 + N_0) - \varphi_3 \quad (37) \end{align*}
\]

The \( \varphi_1, \varphi_2, \varphi_3 \) in equation (30) (31) (32) (34) (37) denote the Taylor expansion error. When \( p_0 \) is given, \( \phi, \theta_1 \) and \( \theta_2 \) are the constants.

Then we can get the constraint (24a) can be written as \( R_1^*t_3 + R_2^*t_2 + \frac{Tf}{c} \geq D \), and the object function is expressed as:
\[ \max_{p_1} \eta = R_{sec}^* - \lambda Q_E \quad (38) \]
\[ \text{s.t. } R_1^*t_3 + R_2^*t_2 + \frac{Tf}{c} \geq D \quad (38a) \]
\[ p_1 + p_2 = p_r \quad (38b) \]
\[ R_1^* \geq r_{th} \quad (38c) \]
\[ R_2^* \geq r_{th} \quad (38d) \]

The standard form of the convex optimization problem is that both the objective function and the constraint function are convex functions, so problem (38) is approximately a convex optimization problem. And the Lagrange dual method is used to find the optimal solution to the transmit power. It can be expressed as:
\[ \min_{p_1 \geq 0, p_2 \geq 0, p_3 \geq 0} \{ \max L(p_1, \gamma_1, \gamma_2, \gamma_3) \} \quad (39) \]

The problem (38) is convex and satisfies the Slater’s condition [35], the strong dual relationship is established, the dual gap is zero between problem (38) and (39), so solving problem (39) is equivalent to solving problem (38). The Lagrangian function in equation (39) is written as:
\[
L(p_1, \gamma_1, \gamma_2, \gamma_3) = R_{sec}^* - \lambda[p_r t_2 + \xi(t_2 + t_3) + \mu p_m|h_{um}|^2t_1] + \gamma_1[(R_1^*(p_1) + R_2^*(p_2))t_2 + \frac{Tf}{c} - D] + \gamma_2[R_1^*(p_1) - r_{th}] + \gamma_3(R_2^*(p_2) - r_{th}) \quad (40)
\]

where \( \gamma_1, \gamma_2 \) and \( \gamma_3 \) are dual variables associated with constraints with (38a), (38c) and (38d), respectively. Extremum points \( p_1^*, \gamma_1^*, \gamma_2^* \) and \( \gamma_3^* \) can be obtained by the first-order partial of (41).
\[
\begin{align*}
\frac{\partial L}{\partial p_1} &= 0 \\
\frac{\partial L}{\partial \gamma_1} &= 0 \\
\frac{\partial L}{\partial \gamma_2} &= 0 \\
\frac{\partial L}{\partial \gamma_3} &= 0
\end{align*}
\]

According to the constraints of (38a), (38b), (38c) and (38d), the value range of \( p_1^* \) is obtained by \( P_u = \{ \max(x_1, a_1) \leq p_1^* \leq (x_2, b_1, \frac{c}{Tf}) \} \).

According to the nature of univariate functions, in order to obtain the maximum value of the problem, the optimal value of \( p_1 \) should be obtained at the boundary point of the domain and the extreme point of the objective function. Then the optimal value of \( p_1 \) can be written as:
\[
\begin{align*}
p_1^* &= \max\{ x_1 \mid p_1^* \leq \min(x_2, b_1, \frac{p_r}{2}) \} \\
&= \max\{ a_1 \mid p_1^* \leq \min(x_2, b_1, \frac{p_r}{2}) \} \\
&= \max\{ x_2 \mid \min(x_1, a_1) \leq \min(p_1^*, x_2, b_1, \frac{p_r}{2}) \} \\
&= \max\{ b_1 \mid \min(x_1, a_1) \leq \min(p_1^*, x_2, b_1, \frac{p_r}{2}) \}
\end{align*}
\]

In the equation (42):
\[
\begin{align*}
x_1 &= (v_1 - \sqrt{v_2 - v_3})/2g_3|h_{ur}|^2|h_{um}|^2 \\
a_1 &= a_1 = (p_4|h_{rm}|^2 + N_0 - 2\alpha/h_0 N_0)|h_{ur}|^2 \\
x_2 &= (v_1 + \sqrt{v_2 - v_3})/2g_3|h_{ur}|^2|h_{um}|^2 \\
b_1 &= (|h_{um}|^2p_r + N_0 - 2\alpha/h_0 N_0)|h_{ur}|^2 \\
\end{align*}
\]

where \( v_1, v_2 \) and \( v_3 \) in equation (43) are expressed as:
\[
\begin{align*}
v_1 &= g_2(N_0 + p_4|h_{rm}|^2)|h_{ur}|^2 \\
&- g_1|g_3|h_{um}|^2 - g_3|h_{ur}|^2N_0^2 \\
v_2 &= g_3(g_1|h_{um}|^2 + |h_{ur}|^2N_0^2) \\
&+ g_2(N_0 + p_4|h_{rm}|^2)|h_{ur}|^4 \\
v_3 &= 2g_3(g_1|h_{um}|^2 + |h_{ur}|^2N_0^2)N_0 + p_4|h_{rm}|^2|h_{ur}|^2
\end{align*}
\]

where \( v_1, v_2 \) and \( v_3 \) in equation (43) are expressed as:
\[
\begin{align*}
v_1 &= g_2(N_0 + p_4|h_{rm}|^2)|h_{ur}|^2 \\
&- g_1|g_3|h_{um}|^2 - g_3|h_{ur}|^2N_0^2 \\
v_2 &= g_3(g_1|h_{um}|^2 + |h_{ur}|^2N_0^2) \\
&+ g_2(N_0 + p_4|h_{rm}|^2)|h_{ur}|^4 \\
v_3 &= 2g_3(g_1|h_{um}|^2 + |h_{ur}|^2N_0^2)N_0 + p_4|h_{rm}|^2|h_{ur}|^2
\end{align*}
\]
In the equation (44), \( g_1, g_2 \) and \( g_3 \) can be written as:

\[
\begin{align*}
g_1 &= (p_4|h_{um}|^2 + p_3|h_{ar}|^2 + N_0)N_0 \\
g_2 &= p_f|h_{um}|^2 + N_0 \\
g_3 &= 2(D - Tf/c)/Bt_2
\end{align*}
\] (45)

B. OPTIMIZATION OF CALCULATION FREQUENCY

We consider the CPU frequency of UE with given \( p_1 \) and \( t_2 \) in this section, the problem can be formulated as:

\[
P.2.2: \max_{f} \eta = R_{sec}
\]

\[-\lambda[p_target + T_f^3 - \mu(|h_{um}|^2p_m)|h_{um}|^2p_m t_1]
\]

s.t. \( t_1 + t_2 + t_3 = T \)

\[
R_{1}t_3 + R_{2}t_2 + \frac{T_f}{c} \geq D
\] (46a)

\[
e + \mu(|h_{um}|^2p_m)|h_{um}|^2p_m t_1 - \xi T_f^3 - (p_1 + p_2)t_2 \geq 0
\] (46c)

Differentiate the question about \( f \), we can get the expression as follows:

\[
\eta'(f) = -3\lambda \xi T_f^2
\] (47)

Since the variable \( f \) is a positive number, it can be seen that the function is a monotone decreasing function with respect to \( f \), and the range of \( f \) can be obtained by the constraints as follows:

\[
\frac{(D - R_{1}t_3 + R_{2}t_2)c}{T} \leq f \leq \Gamma
\]

\[
\Gamma = \sqrt{e + \mu(|h_{um}|^2p_m)|h_{um}|^2p_m(T - 2t_3) - (p_1 + p_2)t_2}
\]

Then we can get the optimal value of \( f \):

\[
f^* = \frac{(D - R_{1}t_3 + R_{2}t_2)c}{T}
\] (49)

C. OPTIMIZATION OF OFFLOADING TIME

To optimize the UE’s transmission delay, the problem is expressed as follows:

\[
P.2.3: \max_{t_2} \eta = \frac{R_{sec}}{p_s t_2 + \xi T_f^3 - \mu(|h_{um}|^2p_m)|h_{um}|^2p_m t_1}
\]

s.t. \( R_{1}t_3 + R_{2}t_2 + \frac{T_f}{c} \geq D \)

\[
t_1 + t_2 + t_3 = T
\] (50a)

\[
e + \mu(|h_{um}|^2p_m)|h_{um}|^2p_m t_1 - \xi T_f^3 - (p_1 + p_2)t_2 \geq 0
\] (50c)

Based on the constrains of (50a), (50b) and (50c), the range of \( t_2 \) can be written as:

\[
\Xi_1 \leq t_2 \leq \Xi_2
\]

\[
\Xi_1 = \frac{D - Tf/c}{B\log_2(1 + \Theta) + B\log_2(\frac{|h_{um}|^2p_s + N_0}{|h_{um}|^2p_s + N_0})}
\]

\[
\Xi_2 = \frac{e + \mu(|h_{um}|^2p_m)|h_{um}|^2p_m T - \xi T_f^3}{2\mu(|h_{um}|^2p_m)|h_{um}|^2p_m + p_r}
\] (52)

D. ALTERNATE ITERATION ALGORITHM FOR JOINT OPTIMIZATION

This article jointly optimizes the transmission power allocated to relay \( p_1 \), CPU frequency \( f \) and offloading time \( t_2 \) to maximize the security energy efficiency of the UE. For this problem, we proposed an alternate iterative algorithm, which was shown in TABLE 1. Initialize \( n = 1 \), the transmission power allocated to relay \( p_1 \), the minimum transmission rate \( r_{th} \), calculation data \( D \), UE’s initial energy \( e \). In the algorithm 2, \( p_1(n) \), \( f(n) \) and \( t_2(n) \) will be updated in turn in each iteration, the power allocated to relay \( p_1(n) \) will be updated with the fixed \( f(n-1) \) and \( t_2(n-1) \). The CPU frequency \( f(n) \) can be available with \( p_1(n) \) and \( t_2(n-1) \) given. The offloading time \( t_2(n) \) is available with \( p_1(n) \) and \( f(n) \) given. The iteration is terminated when the condition \( |\eta(n) - \eta(n-1)| < \epsilon \) is met.

The convergence analysis: There are three calculation processes need to be performed: the power allocated to relay, CPU frequency of UE, and offloading time. Let \( SEE(p_1(n), f(n), t_2(n)) \) denotes the security energy efficiency calculated by \( p_1(n) \), \( f(n) \) and \( t_2(n) \).Since \( p_1(n) \) is the optimal power allocated to relay by equation (42) with fixed \( f(n-1) \) and \( t_2(n-1) \), the maximum power is \( p_1(n) \). When \( f(n) \) and \( t_2(n-1) \) are fixed, the maximum energy efficiency is \( p_1(n) \). Therefore, the algorithm is convergent.
TABLE 2. Algorithm 2 Alternate iteration algorithm for joint optimization.

1: Initialize $p_0$, $\xi$, $D$, and $\epsilon$
and $t_2^{(n-1)}$, then we can get

$$SEE(p_1^{(n)}, f^{(n-1)}, t_2^{(n-1)}) \geq SEE(p_1^{(n-1)}, f^{(n-1)}, t_2^{(n-1)})$$ (54)

Compared to the initial $f^{(n-1)}$, an optimal CPU frequency $f^{(n)}$ can be given by equation (49) with fixed $p_1^{(n)}$ and $t_2^{(n-1)}$. Then

$$SEE(p_1^{(n)}, f^{(n)}, t_2^{(n)}) \geq SEE(p_1^{(n)}, f^{(n)}, t_2^{(n)})$$ (55)

According to algorithm 1, an optimal offloading time $t_2^{(n)}$ is available with given $p_1^{(n)}$ and $f^{(n)}$. Then the security energy efficiency increases after algorithm 1.

$$SEE(p_1^{(n)}, f^{(n)}, t_2^{(n)}) \geq SEE(p_1^{(n)}, f^{(n)}, t_2^{(n)})$$ (56)

It can be guaranteed that $SEE^{(n)} \geq SEE^{(n-1)}$ from the above analysis, which means that $SEE$ keeps increasing with the number of iterations. When the $p_1^{(n)}$, $f^{(n)}$ and $t_2^{(n)}$ becomes the optimal value, the $SEE$ will remain unchanged, the condition $|\eta^{(n)} - \eta^{(n-1)}| < \epsilon$ is met. Therefore, the algorithm is convergent.

The complexity analysis: There are three calculation processes need to be performed during each iteration. The complexities of computing $p_1^*$ and $f^*$ are $O(1)$, and the complexities of searching $t_2^*$ is $O(\log_2 N)$, where $N$ is the number of iterations of algorithm 1. Then we can get the complexity of algorithm 2 is $O(N_{\text{max}}(1 + 1 + \log_2 N))$, where $N_{\text{max}}$ denotes the maximum iteration number of the while loop in algorithm 2.

IV. NUMERICAL RESULTS

In this section, we will get the numerical results about the security energy efficiency of the UE in our proposed untrusted relay assisted NOMA-MEC system. Without loss of generality, the simulation parameters are shown as follows: The sum transmission power of the UE $p_r = 1w$, the distance from the user to the MEC server is 250m [20], and the distance from the user to the relay and the relay to the MEC server are 125m. Assuming that the channels are modeled as $h = d^{-\alpha/2}g$, where $d$ denotes the distance, and the $g$ is the Rayleigh fading channels with $g \in CN(0, 1)$, $\alpha = 3.5$ denotes the the path loss exponent, the bandwidth $B = 5$ MHz, $\xi = 10^{-28}$J/cycle/cycle is the constant determined by the chip architecture of UE [36]. The noise power $N_0 = 10^{-9}$w, $c = 1 \times 10^3$ cycles/bit denotes the number of CPU cycles required by UE to compute 1-bit data [21], initial energy $e = 0.1$, the number of task need to be computed $D = 4 \times 10^6$bits, the maximum delay $T = 0.1s$ [36], the minimum transmission rate $r_{th} = 1 \times 10^6$bits/s, the power of relay and MEC are $p_m = p_4 = 10w$ [20], [37]. The parameters in energy harvesting heuristic model $m_2 = 1.34, m_1 = 5.2 \times 10^{-5}, m_0 = 1.61 \times 10^{-6}, q_3 = 1, q_2 = 0.0547, q_1 = -0.000318, q_0 = 2.87 \times 10^{-6}$ [33].

Figure 3 shows the relationship between active jamming power and the security rate at relay. In the absence of auxiliary jamming measure, the receiving rate of MEC receiver is lower than the receiving rate of relay when the relay is untrusted, which means that the relay sending part cannot realize security transmission at the physical layer. After taking auxiliary jamming measure, the relay can achieve security transmission, and the security rate continues to improve as the transmission power of the relay increases. In addition, from the comparison of active jamming power, the influence of different jamming power is different.

Figure 4 shows the relationship between active jamming, transmission mode, and power size with security energy efficiency. It can be seen that the security energy efficiency of adopting active jamming is significantly better than that without adopting active jamming whether it is NOMA transmission or OMA transmission, and the security energy efficiency both NOMA transmission and OMA transmission are continuously increasing with the increase of the power allocated to relay, then we can get the optimum power at 0.5w. It also shows that the security energy efficiency of NOMA transmission is 8% better than OMA transmission in the case of active jamming and a certain user power allocation. The...
main reason is that NOMA superimposes the message signals of multiple users in the power-domain by taking advantage of their respective channel gain differences. Using the serial interference cancellation (SIC) at the receiver to eliminate inter-user interference can improve transmission rate and save energy more effectively. In addition, the security energy efficiency of OMA is superior to NOMA in the absence of active jamming, which can be interpreted as the received signal-to-noise ratio of the relay under OMA transmission conditions is relatively poor, and the leakage of information is less than that of NOMA transmission.

Figure 5 illustrates the relationship between the CPU frequency and the security energy efficiency. It can be shown that the security energy efficiency increases first and then decreases as the CPU frequency increases, reaching a maximum value near $0.6 \times 10^9$. It is not difficult to understand that the amount of local computing data increases as the CPU increases. After reaching the optimal value, the increase in local computing data will cause the local computing energy consumption to increase, resulting in a decrease in the security energy efficiency of the UE.

Figure 6 depicts the relationship between offloading time and the security energy efficiency. As can be seen from the figure, along with the offloading time increases, the security energy efficiency increases first and then decreases. This because the offloading data will be increased with the increase of the offloading time, then get the optimal value near 0.028s. After that, the increase of the offloading time will cause the reduction of the energy harvesting time of the terminal, which leads to a decrease in the security energy efficiency of the UE.

Under the previous parameter settings, according to the optimal offloading time $t_2 = 0.028s$, we can get the offloading data is $3.4 \times 10^5$bits, the data offloaded by relay is $2.9 \times 10^5$bits, which is 85% of total offloading data, the offloading data directly is $0.5 \times 10^5$bits, which is 15% of total offloading data, and the data computed locally is $0.6 \times 10^5$bits. The total amount of calculated data is $D = 4 \times 10^5$bits.

**V. CONCLUSION**

In this article, an untrusted relay assisted NOMA-MEC system is considered. Specifically, the destination-assisted jamming is proposed to improve the security by jamming untrusted relay and reducing the received signal-to-noise ratio at relay for the leakage of information. Furthermore, downlink NOMA transmission is considered to improve the offloading efficiency, compared with the traditional OMA transmission, the security energy efficiency is significantly
improved. We jointly optimize the user’s transmission power, CPU frequency and offloading time to maximize the security energy efficiency of UE under the condition of time delay and energy consumption. Since it is a non-convex multi-objective optimization problem, it is decomposed into several suboptimal single-objective sub-problems, and the single-objective sub-problems about transmission power allocated to relay and CPU frequency are transformed into convex problems by Taylor approximation method, then be solved by Lagrange dual method. Alternative iterative algorithm is proposed to jointly optimize the transmission power allocated to relay, CPU frequency and offloading time, which aim to maximize the security energy efficiency. The simulation results show that the proposed method can effectively improve the security offloading performance and security energy efficiency compared with other relay assisted offloading methods. In fact, the untrusted relay assisted NOMA-MEC network can be used in some confidential networks, such as national defense, financial or government intelligence networks, in which some users do not have the rights to access some information [38]. Another application scenario is that the relay is attacked by malicious users [39], resulting in the leakage of information. With the development of MEC, the offloading computing in the above-mentioned confidential network is a inevitable trend. Subsequent research will be conducted on untrusted relay assisted NOMA-MEC network with varying jamming power and energy-limited untrusted relay.

APPENDIX

One: According to the $F(\Pi, \lambda)$, we can get

$$\frac{\partial F(\Pi, \lambda)}{\partial \lambda} = -Q\varepsilon$$

$$= \mu(|h_{um}|^2 p_m)|h_{um}|^2 p_{m1}$$

$$- (p_1 + p_2)\tau_2 - \xi Ff^3 < 0$$

(57)

It is easy to know that the function $F(\Pi, \lambda)$ is a decreasing function of $\lambda$ from the above equation. We can get $F(\Pi, \lambda) > F(\Pi, \lambda + \Delta)$ for any $\Delta > 0$.

Then we can express the following equation as:

$$h(\lambda) = \max_{\Pi} F(\Pi, \lambda) \geq F(\Pi, \lambda) > F(\Pi, \lambda + \Delta), \forall \Pi$$

(58)

which can be transformed that

$$h(\lambda) > F(\Pi, \lambda + \Delta) = h(\lambda + \Delta)$$

(59)

Then we can get the conclusion that $h(\lambda)$ is a decreasing function of $\lambda$.

Two: According to equation (24), we can get the following equation

$$F(\Pi, f(\Pi)) = 0$$

(60)

where $f(\Pi) = \frac{R_{\text{sec}}}{(p_1 + p_2)\tau_2 + \xi Ff^3 - \mu(|h_{um}|^2 p_m)|h_{um}|^2 p_{m1}}$

Using $\Pi_{\text{opt}}$ denotes the optimal value of $P2$. Since $f(P_{\text{opt}})$ is the maximum of equation (24), $\lambda = f(\Pi_{\text{opt}})$ is the maximum $\lambda$ that meets the constraints of $F(\Pi, \lambda)$.

We can get the $\lambda^*$ by equation $h(\lambda) = 0$, then we can get $h(\lambda^*) = 0$ and $\Pi^*$, which satisfied $F(\Pi, \lambda^*) = 0$. According to the analysis of step one, when $\lambda_0 > \lambda^*$, we can get

$$h(\lambda_0) = \max_{\Pi} F(\Pi, \lambda_0) < 0$$

(61)

According to the above analysis and equation (61), the $\lambda^*$ is the largest value of $F(\Pi, \lambda)$. And we can get $\lambda^* = f(\Pi_{\text{opt}})$ and $\Pi_{\text{opt}} = \Pi^*$. Thus, the value of $\lambda^*$ that satisfied the equation $h(\lambda) = 0$ is the maximum of the security energy efficiency.

REFERENCES

[1] Z. Zhou, B. Wang, B. Gu, B. Ai, S. Mumtaz, J. Rodriguez, and M. Guizani, “Time-dependent pricing for bandwidth slicing under information asymmetry and price discrimination,” IEEE Trans. Commun., early access, Jun. 9, 2020, doi: 10.1109/TCOMM.2020.3001050.

[2] F. Qiao, J. Wu, J. Li, A. K. Bashar, S. Mumtaz, and U. Tariq, “Trustworthy edge storage orchestration in intelligent transportation systems using reinforcement learning,” IEEE Trans. Intell. Transp. Syst., early access, Jun. 29, 2020, doi: 10.1109/TITS.2020.3003211.

[3] F. Wang, J. Xu, X. Wang, and S. Cui, “Joint offloading and computing optimization in wireless powered mobile-edge computing systems,” IEEE Trans. Wireless Commun., vol. 17, no. 3, pp. 1784–1797, Mar. 2018.

[4] A. Al-Shuwaili and O. Simeone, “Energy-efficient resource allocation for mobile edge computing-based augmented reality applications,” IEEE Wireless Commun. Lett., vol. 6, no. 3, pp. 398–401, Jun. 2017.

[5] K. Chandra, A. S. Marcano, S. Mumtaz, R. V. Prasad, and H. L. Christiansen, “Unveiling capacity gains in ultradense networks: Using mm-wave NOMA,” IEEE Veh. Technol. Mag., vol. 13, no. 2, pp. 75–83, Jun. 2018.

[6] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, “A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends,” IEEE J. Sel. Areas Commun., vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[7] B. Wang, L. Dai, Z. Wang, N. Ge, and S. Zhou, “Spectrum and energy-efficient beamspace MIMO-NOMA for millimeter-wave communications using lens antenna array,” IEEE J. Sel. Areas Commun., vol. 35, no. 10, pp. 2370–2382, Oct. 2017.

[8] 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.

[9] Z. Ding, P. Fan, and H. V. Poor, “Impact of non-orthogonal multiple access on the offloading of mobile edge computing,” IEEE Trans. Commun., vol. 67, no. 1, pp. 375–390, Jan. 2019.

[10] Z. Ding, D. W. K. Ng, R. Schober, and H. V. Poor, “Delay minimization for NOMA-MEC offloading,” IEEE Signal Process. Lett., vol. 25, no. 12, pp. 1875–1879, Dec. 2018.

[11] Z. Ding, J. Xu, O. A. Dobre, and H. V. Poor, “Joint power and time allocation for NOMA–MEC offloading,” IEEE Trans. Veh. Technol., vol. 68, no. 6, pp. 6207–6211, Jun. 2019.

[12] J. Li, F. Wu, K. Zhang, and S. Leng, “Joint dynamic user pairing, computation offloading and power control for NOMA-based MEC system,” in Proc. 11th Int. Conf. Wireless Commun. Signal Process. (WCSP), Oct. 2019, pp. 1–6.

[13] M. Zeng, N.-P. Nguyen, O. A. Dobre, and H. V. Poor, “Delay minimization for NOMA-assisted MEC under power and energy constraints,” IEEE Wireless Commun. Lett., vol. 8, no. 6, pp. 1657–1661, Dec. 2019.

[14] S. Bi and Y.-J.-A. Zhang, “An ADMM based method for computation rate maximization in wireless powered mobile-edge computing networks,” in Proc. IEEE Int. Conf. Commun. (ICC), May 2018, pp. 1–7.

[15] F. Zhou, Y. Wu, R. Q. Hu, and Y. Qian, “Computation rate maximization in UAV-enabled wireless-powered mobile-edge computing systems,” IEEE J. Sel. Areas Commun., vol. 36, no. 9, pp. 1927–1941, Sep. 2018.

[16] F. Zhou, Y. Wu, R. Q. Hu, and Y. Qian, “Computation efficiency in a wireless-powered mobile edge computing network with NOMA,” in Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWiMOM), Jun. 2019, pp. 1–9.
[18] Z. Yang, J. Hou, and M. Shikh-Bahaei, “Resource allocation in full-duplex mobile-edge computation systems with NOMA and energy harvesting,” in Proc. IEEE Int. Conf. Commun. (ICC), May 2019, pp. 1–6.

[19] X. Chen, Y. Cai, Q. Shi, M. Zhao, B. Champagne, and L. Hanzo, “Efficient resource allocation for relay-assisted computation offloading in mobile-edge computing,” IEEE Internet Things J., vol. 7, no. 3, pp. 2452–2468, Mar. 2020.

[20] X. Cao, F. Wang, J. Xu, R. Zhang, and S. Cui, “Joint computation and communication cooperation for energy-efficient mobile edge computing,” IEEE Internet Things J., vol. 6, no. 3, pp. 4188–4200, Jun. 2019.

[21] B. Xie, Q. Zhang, and J. Qin, “Joint optimization of cooperative communication and computation in two-way relay MEC systems,” IEEE Trans. Veh. Technol., vol. 69, no. 4, pp. 4596–4600, Apr. 2020.

[22] X. Hu, K.-K. Wong, and K. Yang, “Wireless powered cooperation-assisted mobile edge computing,” IEEE Trans. Wireless Commun., vol. 17, no. 4, pp. 2375–2388, Apr. 2018.

[23] B. He, S. Bi, H. Xing, and X. Lin, “Collaborative computation offloading in wireless powered mobile-edge computing systems,” in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2019, pp. 1–7.

[24] S. S. Kalamkar and A. Banerjee, “Secure communication via a wireless energy harvesting untrusted relay,” IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2199–2213, Mar. 2017.

[25] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, “Secure relaying in non-orthogonal multiple access: Trusted and untrusted scenarios,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 210–222, 2020.

[26] J. Xu and J. Yao, “Exploiting physical-layer security for multiuser multicarrier computation offloading,” IEEE Wireless Commun. Lett., vol. 8, no. 1, pp. 9–12, Feb. 2019.

[27] X. He, R. Jin, and H. Dai, “Physical-layer assisted privacy-preserving offloading in mobile-edge computing,” in Proc. IEEE Int. Conf. Commun. (ICC), May 2019, pp. 1–6.

[28] W. Wu, F. Zhou, R. Q. Hu, and B. Wang, “Energy-efficient resource allocation for secure NOMA-enabled mobile edge computing networks,” IEEE Trans. Commun., vol. 68, no. 1, pp. 493–505, Jan. 2020.

[29] H. Lin, Y. Cao, Y. Zhong, and P. Liu, “Secure computation efficiency maximization in NOMA-enabled mobile edge computing networks,” IEEE Access, vol. 7, pp. 87504–87512, 2019.

[30] H. Z. Khan, M. Ali, M. Naeem, I. Rashid, A. M. Siddiqui, M. Imran, and S. Muntaz, “Resource allocation and throughput maximization in decoupled 5G,” in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), May 2020, pp. 1–6.

[31] J.-M. Kang, I.-M. Kim, and D. I. Kim, “Joint tx power allocation and rx power splitting for SWIPT system with multiple nonlinear energy harvesting circuits,” IEEE Wireless Commun. Lett., vol. 8, no. 1, pp. 53–56, Feb. 2019.

[32] G. Ma, J. Xu, Y. Zeng, and M. R. V. Moghadam, “A generic receiver architecture for MIMO wireless power transfer with nonlinear energy harvesting,” IEEE Signal Process. Lett., vol. 26, no. 2, pp. 312–316, Feb. 2019.

[33] L. Shi, L. Zhao, and K. Liang, “Power allocation for wireless powered MIMO transmissions with non-linear RF energy conversion models,” China Commun., vol. 14, no. 2, pp. 57–64, Feb. 2017.

[34] W. Dinkelbach, “On nonlinear fractional programming,” Manage. Sci., vol. 13, no. 7, pp. 492–498, Mar. 1967. [Online]. Available: http://www.jstor.org/stable/2627691

[35] L. V. S. Boyd, Optimization, Cambridge, U.K.: Cambridge Univ. Press, Mar. 2004.

[36] F. Wang, J. Xu, and Z. Ding, “Multi-antenna NOMA for computation offloading in multiuser mobile edge computing systems,” IEEE Trans. Commun., vol. 26, no. 2, pp. 312–316, Feb. 2019.

[37] B. Liu, J. Wang, S. Ma, F. Zhou, Y. Ma, and G. Lu, “Energy-efficient cooperation in mobile edge computing-enabled cognitive radio networks,” IEEE Access, vol. 7, pp. 45382–45394, 2019.

[38] X. He and A. Yener, “Cooperation with an untrusted relay: A secrecy perspective,” IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[39] Y. Zou, J. Zhu, X. Li, and L. Hanzo, “Relay selection for wireless communications against eavesdropping: A security-reliability trade-off perspective,” IEEE Netw., vol. 30, no. 5, pp. 74–79, Sep. 2016.

PINFANG ZHAO received the B.Eng. degree from the North China Institute of Aerospace Engineering, China, in 2017. She is currently pursuing the M.S. degree in communication and information engineering with North China Electric Power University, China. Her research interests include massive MIMO, NOMA, MEC, and energy efficiency of wireless communications, physical layer security, wireless resource management, and optimization technology.

WEI ZHAO (Member, IEEE) received the B.Eng. degree from North China Electric Power University, China, in 2008, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2011. In 2011, he joined the School of Electrical and Electronic Engineering, North China Electric Power University. From 2016 to 2017, he visited the King’s College London, U.K., as a Visiting Scholar. He holds many patents, several EI articles, SCI, and multiple other types of articles. His research interests include wireless security, massive NOMA, MIMO, MEC, and energy efficiency of wireless communications.

HUI BAO is currently a Professor in communication and information engineering with North China Electric Power University, China. She holds many patents, several EI articles, SCI, and multiple other types of articles. Her research interests include full-dimensional multi-antenna, heterogeneous networks, and energy efficiency of wireless communications, NOMA, MEC, physical layer security, wireless resource management, optimization technology, and cognitive radio.

BAOGANG LI (Member, IEEE) received the B.Eng. degree from North China Electric Power University, China, in 2006, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2012. From 2016 to 2017, he visited the Centre for IoT and Telecommunications, The University of Sydney, as a Visiting Scholar. He is currently an Associate Professor with the School of Electrical and Electronic Engineering, North China Electric Power University. His research interests include wireless communication, the industry IoT, and smart grid communication.

* * *