The Research of NOMA-MEC Network based on Untrusted Relay-Assisted Transmission in Power Internet of Things

Da Li*, Bo Li, Ningli Qin, Xiaosong Jing, Changyu Du and Chunyi Wan
Beijing Fibrlink Communications Co., Ltd, Beijing, 100070, China
*lda@sgitg.sgcc.com.cn

Abstract: Mobile edge computing provides a promising architecture for the computing of power Internet of Things terminal equipment, which can effectively solve the problems of insufficient computing power and energy-limitation of terminal equipment. In addition, relay-assisted transmission is adopted because the equipment may be far away from the MEC server. However, relay may be attacked by malicious users and become untrusted relay. Therefore, destination-assisted jamming is proposed to improve the security performance of offload computing. In order to improve spectrum utilization, non-orthogonal multiple access technology is used to transmission. An alternate iterative algorithm is proposed to jointly optimize the power allocation and offloading time to maximize security energy efficiency. The simulation results verify the effectiveness of the proposed method.

1. Introduction
Power Internet of Things is a product of Internet of Things technology applied to power systems. Although the current power grid has gradually developed in the direction of the power Internet of Things, many important operations still use manual control methods, but their low efficiency and high cost can no longer meet the needs of future development. With the development of 5G communication technology, it provides a strong guarantee for the further realization of the power Internet of Things. Many advanced technologies (such as mobile edge computing (MEC), non-orthogonal multiple access technology (NOMA)) can be effectively introduced into the power Internet of Things to further realize the effective management of power resources.

Previously, literature [1] proposed MEC technology for the Internet of Power Distribution Internet of Things, provided a standard architecture for edge computing in the Internet of Power Distribution Internet of Things. A hierarchical adaptive autonomous CPS control model based on edge computing is constructed in [2]. Literature [3]-[4] considered that the traditional calculation model can not meet the real-time requirements of data processing and the time synchronization accuracy, proposed the use of MEC to improve implementation and time synchronization. Literature [5] improved the timeliness of services by offloading computing tasks to MEC servers, and rationally allocated resources and balanced workloads in power Internet of Things architecture.

NOMA plays an important role in improving spectrum efficiency, providing a large number of connections, and reducing latency [6]. Literature [7] showed that applying NOMA technology to MEC system can effectively reduce the delay and energy consumption of MEC offloading.

However, the security of information in the power Internet of Things is also very important. [8] proposed a security management and control architecture for the Universal Power Internet of Things based on edge cloud computing collaboration technology. In [9], a linkable anonymous credential
protocol was studied to protect the privacy of user. A lightweight privacy-preserving electricity consumption aggregation scheme was proposed in [10], which guaranteed the consumers privacy, messages authenticity and integrity.

In addition, relay-assisted transmission is adopted because the equipment may be far away from the MEC server. However, relay may be attacked by malicious users and become untrusted relay. Therefore, destination-assisted jamming is proposed. Based on this, this article considers the physical layer of information transmission in the power Internet of Things safe question, uses reasonable resource allocation to maximize the security of information transmission. Theoretical analysis and simulation practice show: (1)NOMA transmission can effectively improve security energy efficiency; (2)The proposed active jamming method greatly improves the offloading security performance.

2. System model

In this paper, The system model is a three-node model including relay, collector and MEC server. The collector offload the data to the MEC through direct transmission and relay-assisted transmission.

2.1 Task offloading slot

In the first slot, the data that needs to be processed by the collector is offloaded to the MEC server. The power-domain NOMA technology is considered. The collector transmits the information to the MEC and the relay simultaneously, the signal is expressed as: $x = \sqrt{p_1}s_1 + \sqrt{p_2}s_2$, where $p_1$ and $p_2$ are the power allocated to the relay and MEC server respectively, which satisfied $p_2 \geq p_1 \geq 0$. In this part, the energy consumption of the collector is $e_{\text{off}} = (p_1 + p_2)t_1$.

The received signal on the server side is expressed as: $y_m = h_{\text{mm}}x + n_m$, where $n_m$ is the noise with power $N_0$. Then the signal-to-noise ratio (SNR) received by the MEC is: $\gamma_m = \frac{|h_{\text{mm}}|^2 p_2}{|h_{\text{mm}}|^2 p_1 + N_0}$.

Because the relay is an untrusted relay, the MEC server sends an auxiliary jamming signal $s_3$ to jam with the effective received signal of the relay. The received signal at the relay end is: $y_r = h_{\text{mr}}x + h_{\text{mm}}\sqrt{p_1}s_3 + n_r$, where $h_{\text{mr}}$ and $h_{\text{mm}}$ denote the channel gain between collector and relay and between relay and MEC respectively. $p_1$ denotes the jamming power of $s_3$. $n_r$ is the noise in relay. The received SNR of signal $s_1$ at the relay is: $\gamma_r = p_1|h_{\text{mr}}|^2 / (p_1|h_{\text{mr}}|^2 + N_0)$.

2.2 Relay forwarding slot

In this time slot, the signal received by the relay is amplified and then forwarded to the MEC server, and the received signal by MEC server can be expressed as:

\[
y_r' = \sqrt{\frac{p_4}{p_1|h_{\text{mr}}|^2 + p_3|h_{\text{mr}}|^2 + N_0}}h_{\text{mr}}x + \sqrt{\frac{p_4}{p_1|h_{\text{mr}}|^2 + p_3|h_{\text{mr}}|^2 + N_0}}h_{\text{mr}}n_r + n_m.
\]

The second and third terms can be regarded as noise, and the SNR of valid signal is:

\[
\gamma_{\text{rm}} = \frac{p_4|h_{\text{mr}}|^2|h_{\text{mr}}|^2 p_1}{(p_4 |h_{\text{mr}}|^2 + p_1|h_{\text{mr}}|^2 + p_3|h_{\text{mr}}|^2)N_0 + N_0^2}.
\]

2.3 MEC server and local computing

Due to the powerful calculation function of MEC, we think the calculation delay of MEC is $t_s = 0$. The amount of locally computed data and offloading data are $d_i = Tf / b$, $d_i = B \log_2(1 + \gamma_{\text{rm}})t_2$, $d_2 = B \log_2(1 + \gamma_m) t_1$, and the energy consumption is $e_i = \xi T f^3$.
2.4 Problem formulation

In this paper, we use the collector-side security energy efficiency as the objective function to evaluate the performance of MEC offloading. Task offloading time and relay forwarding time are considered the same. The sum of secure offloading transmission rate can be expressed as:

$$R_{sec} = R_{sec} + R_{sec}^{2} = B \log_{2}(1 + \gamma_{m}) - B \log_{2}(1 + \gamma_{m}^{2}) + B \log_{2}(1 + \gamma_{m}^{2})$$

(3)

The actual energy consumption of the collector is expressed as: $E = (p_{1} + p_{2})t_{i} + \xi TF^{3}$. The optimization problem in this paper can be expressed as:

$$\max \frac{\eta}{p_{1}} = \frac{R_{sec}}{E}$$

(4)

$$C1: B \log_{2}(1 + \gamma_{m})t_{i} + B \log_{2}(1 + \gamma_{m})t_{i} + \frac{TF}{b} \geq D; \quad C2: t_{i} + t_{s} \leq T; \quad C3: p_{1} + p_{2} = p_{r}$$

$$C4: e - \xi TF^{3} - (p_{1} + p_{2})t_{i} \geq 0; \quad C5: R_{1} = B \log_{2}(1 + \gamma_{m}) \geq r_{th}; \quad C6: R_{2} = B \log_{2}(1 + \gamma_{m}) \geq r_{th}$$

$C1$ is the computing data volume constraint, $C2$ is the delay constraint, $C3$ is the power constrain, $C4$ is the energy constraints on the collector, $C5$ and $C6$ are the transmission rate constraint. Since the objective function is in fractional form, it is difficult to solve it, so the Dinkelback’s method is used to transform it into an equation optimization problem. which can be rephrased as: $\max \eta = R_{sec} - \mu E$.

3. Maximum security energy efficiency

3.1 Optimization of transmission power

After fixing offloading time, the optimization problem is expressed as:

$$P3.1: \max \frac{\eta}{p_{1}} = \frac{R_{sec}}{E} - \mu E$$

(5)

the expansion method of the first-order Taylor series is used to approximate as a convex optimization problem, and the transformed $R_{sec}$ is expressed as: $R_{sec}^{*} = R_{sec}^{*} - R_{sec}^{*} + R_{sec}^{*}$.

$$R_{sec}^{*} = B \log_{2}((p_{1} h_{m} + p_{1} h_{w} + p_{3} h_{w} + N_{0} + p_{4} h_{m} + p_{1})$$

$$-B h_{m} h_{w} p_{1} / \ln 2(p_{1} h_{m} + p_{1} h_{w} + p_{3} h_{w} + N_{0}) + \delta_{l})$$

$$R_{sec}^{*} = B \log_{2}(h_{m} - p_{3} + N_{0}) - B h_{m} h_{w} p_{1} / \ln 2(h_{m} + p_{0} + N_{0} + \delta_{l})$$

$$R_{sec}^{*} = B \log_{2}(p_{3} h_{m} + N_{0} - B \log_{2}(p_{3} h_{m}^{2} + N_{0} + p_{0} h_{w}^{2} + N_{0}) - \frac{B h_{m}^{2} (p_{1} - p_{0})}{\ln 2(p_{0} h_{w}^{2} + p_{0} h_{w}^{2} + N_{0})} - \sigma_{2}$$

After the above approximation, the optimization problem can be expressed as:

$$\max \eta = R_{sec}^{*} - \mu E \text{ (subject to D1: } R_{1}^{*} t_{1} + R_{2}^{*} t_{1} + \frac{TF}{b} t_{1} \geq D; \quad D2: \ p_{1} + p_{2} = p_{r}; \quad D3: \ R_{1}^{*} \geq r_{th}; \quad D4: \ R_{2}^{*} \geq r_{th})$$

(6)

In this section, the Lagrangian dual algorithm is applied to solve this problem. The optimized Lagrangian function can be expressed as: $L(p_{1}, \beta_{1}, \beta_{2}, \beta_{3}) = \max \{L(p_{1}, \beta_{1}, \beta_{2}, \beta_{3})\}$.

$$L(p_{1}, \beta_{1}, \beta_{2}, \beta_{3}) = \frac{R_{sec}^{*} - \mu[p_{1} t_{1} + \xi TF^{3}] + \beta_{1} [R_{1}^{*} + R_{2}^{*}] t_{1} + \frac{TF}{b} - D] + \beta_{2} (R_{1}^{*} r_{th}) + \beta_{3} (R_{2}^{*} r_{th})$$

(7)

where $\beta_{1}, \beta_{2}, \beta_{3}$ are the Lagrangian multipliers of constraints $D1, D3, D4$, and we can get the corresponding extreme point $p_{1}^{*}$ by finding the first-order partial derivative of formula (7). It can be obtained that the optimal value of $p_{1}$ can be expressed as:
3.2 Optimization of offloading time

In this section, we solve the optimal offloading time with given $p_i$.

$$P3.2: \quad \max_{\eta_i} \eta = \frac{R_{\text{sec}}}{\langle p_i t_i + \xi Tf^{3}\rangle}$$

It is subject to $C1, C2, C4$, Based on constraints of $C1, C2, C4$, the range of $t_i$ is:

$$\Psi \leq t_i \leq \min(T / 2, (e - \xi T f^{3}) / p_i)$$

where

$$\Psi = \frac{D - Tf / b}{B \log_2 (1 + \Upsilon) + B \log_2 \left( \frac{h_{\text{ru}}}{p_i + N_0} \right)}$$

$$\Upsilon = \frac{p_d h_{\text{ru}}}{(p_i h_{\text{ru}} + N_0)^2} \left( p_i h_{\text{ru}} + p_i h_{\text{ru}} + p_i h_{\text{ru}} + N_0 \right) N_0$$

It is easy to know that the function decreases as $t_i$ increases, so the optimal of $t_i$ is $\Psi$.

3.3 Multi-objective joint optimization

In this section, we jointly optimize $p_i$ and $t_i$ to maximize the security energy efficiency of the collector. This section proposes an alternate iterative optimization algorithm as shown in Table 1.

| Table 1: Alternating iterative algorithm |
|-----------------------------------------|
| Step 1: initialize variable, constants involved in constraints $D$, $T$, $r_a$, $p_i$, $p_3$, $p_4$, the number of iterations $i = 0$, $t_i^{(0)} = 0.02$, $\eta^{(0)} = -\varepsilon$, $\eta^{(0)} = \eta^{(0)} - \varepsilon$, convergence accuracy $\varepsilon$; |
| Step 2: while $|\eta^{(i)} - \eta^{(i-1)}| \geq \varepsilon$, $i = i + 1$; |
| Step 3: calculate $p_i^{(i)}$ according to formula (8); obtain the offloading time $t_i^{(i)}$ according to $\Psi$; update $\eta^{(i)}$ according to $p_i^{(i)}$, $t_i^{(i)}$ by formula (4); |
| Step 4: end while, output $p_i$ and $t_i$, calculate $\eta$. |

4. Simulation analysis

The proposed offloading system is simulated by MATLAB, and the simulation parameters are set as follows: $p_i = 1w$, $d_{\text{ru}} = 200m$, $d_{\text{ru}} = d_{\text{ru}} = 100m$ channel gain meets $h = d^{-a/2}g$, where $d$ denote the distance and $g \in CN(0,1)$ is the Rayleigh fading channels.

It can be shown from Figure 1 that the security energy efficiency of taking active jamming is significantly better than that without taking active jamming. And as the power allocated by collector to strong users continues to increase, the security energy efficiency of the two transmission modes continues to increase, reaching the optimum at 0.5w. NOMA uses their respective channel gain differences to superimpose multiple users' message signals in the power domain to make its safety and energy efficiency higher than OMA.
Figure 2 describes the curve of security energy efficiency with offloading time under different powers. As the offloading time increases, the security energy efficiency first increases and then decreases. It can be explained that as the increase in the offloading time, the larger the amount of offloaded data, which will increase the transmission energy consumption, resulting in a decrease in security energy efficiency.

![Figure 1: Security energy efficiency under different schemes](image1)

![Figure 2: The curve of security energy efficiency with offloading time under different power](image2)

References

[1] Sun H, Zhang J, Wang P, Lin J, Guo S, Chen L, (2019) Edge Computation Technology Based on Distribution Internet of Things. Power System Technology, vol 43, no 12.

[2] Gong G, Luo A, Chen Z, (2018) Active distribution network information physical system based on edge computing. Power Grid Technology, vol. 42, no. 10, pp. 3128–3135, 2018.

[3] Huo W, Liu F, Wang L, Jin Y, Wang L, (2020) Research on Distributed Power Distribution Fault Detection Based on Edge Computing. IEEE Access, vol. 8, pp. 24643-24652.

[4] Niu X, Shao S, Xin C, Zhou J, Guo S, Chen X, Qi F, (2019) Workload Allocation Mechanism for Minimum Service Delay in Edge Computing-Based Power Internet of Things. IEEE Access, vol. 7, pp. 83771-83784.

[5] Li Y, Li C, Wu G, Zhang C, (2019) Research on High-precision Time Distribution Mechanism of Multi-source Power Grid Based on MEC. In: IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, Beijing, China, pp. 1-5.

[6] Ding Z, Fan P, Poor H V, (2019) Impact of Non-Orthogonal Multiple Access on the Offloading of Mobile Edge Computing. IEEE Transactions on Communications, vol. 67, no. 1, pp. 375-390.

[7] Zhang Z, Sun H, Hu R, (2017) Downlink and Uplink Non-Orthogonal Multiple Access in a Dense Wireless Network. IEEE Journal on Selected Areas in Communications, vol. 35, no. 12, pp. 2771-2784.

[8] Gong Y, Chen C, Liu B, Gong G, Zhou B, Mahato N K, (2019) Research on the Ubiquitous Electric Power Internet of Things Security Management Based on Edge-Cloud Computing Collaboration Technology. In: IEEE Sustainable Power and Energy Conference, Beijing, China, pp. 1997-2002.

[9] Li F, Luo B and Liu P, (2010) Secure Information Aggregation for Smart Grids Using Homomorphic Encryption. In: 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, pp. 327-332.

[10] Abdallah A and Shen X S, (2018) A Lightweight Lattice-Based Homomorphic Privacy-Preserving Data Aggregation Scheme for Smart Grid. IEEE Transactions on Smart Grid, vol. 9, no. 1, pp. 396-405.