Resource allocation method based on mobile edge computing in smart grid

Ningli Qin¹, Bo Li, Da Li, Xiaosong Jing, Changyu Du, Chunyi Wan
Beijing Fibrlink Communications Co., Ltd, Beijing, 100070, China
¹qinningli@sgitg.sgcc.com.cn

Abstract: Mobile edge computing (MEC) refers to offloading the collected data to the mobile edge server, which can calculate data efficiently, further improve the operating efficiency of the smart grid and reduce energy consumption. In the face of increasing data, the spectrum overhead and energy consumption of the network are becoming increasingly severe. Based on this, this paper proposes to use massive multiple input multiple output (MIMO) technology to improve the spectrum and energy efficiency of the system, and proposes a massive MIMO-MEC smart grid system framework. In addition, considering that it is easy to be eavesdropped in the process of offloading data, we propose to use physical layer security technology to ensure user information security. In order to minimize the energy consumption of applications such as smart meters, this paper proposes a sequential iterative optimization algorithm to jointly optimize the offloading rate and transmission power. The simulation results prove that as the number of antennas increases, the transmission rate of the system increases, which reduces the total energy consumption of the system.

1. Introduction
With the continuous development of society, green energy-saving development is increasingly advocated, and electric energy is widely used as a highly efficient green energy source. In order to meet the demand for electricity from all walks of life in modern cities, energy-saving electricity consumption has become one of the necessary measures for green and environmental protection. The existing smart grid mainly realizes information collection and monitoring by deploying a large number of sensors and advanced metering infrastructure (AMI) equipment, and offloading the collected data to a cloud server to realize real-time demand side management of resources. However, in the face of the increasing number of smart devices (such as smart meters, sensors, AMI) and other devices, the data that needs to be collected and monitored will increase significantly, which will bring great energy costs to the entire power system. Secondly, offloading the collected data to the cloud will also cause a certain burden on the network's spectrum resources.

With the advent of the 5G era, many advanced technologies, such as mobile edge computing, massive multiple input multiple output (MIMO) can be effectively introduced into the smart grid to further realize the effective management of electric energy resources. Specifically, mobile edge computing (MEC), as an advanced technology that effectively improves computing power and reduces latency, can sink computing power to the edge of the network. In addition, some devices such as smart meters offload the collected data to the mobile edge server, which greatly saves the spectrum cost and energy cost of the network.

In recent years, considering the many advantages of MEC, some progress has been made in introducing MEC into the smart grid. Reference [1] proposed a new mobile edge smart grid
architecture. Reference [2] defines a three-layer hierarchical intelligent grid communication structure based on fog computing. Although the above work satisfies the needs of the smart grid through fog computing, the privacy of users is not considered. In order to improve the security performance of information, Reference [3] proposed an efficient and privacy-protected smart grid communication aggregation scheme EPPA. In [4], in order to prevent the user's energy consumption information may leak the user's private information. A linkable anonymous certificate protocol based on Camenisch Lysyanskaya (CL) signature is constructed. On this basis, a privacy protection smart metering scheme based on linkable anonymous certificates is proposed. Reference [5] proposed another smart grid communication based on the additive ElGamal cryptographic system. However, the decryption of additive cryptosystems requires the calculation of discrete logarithms, which leads to the low efficiency of the scheme. Therefore, this paper proposes to use physical layer security technology to realize the secure communication of smart grid communication.

In addition, the increasing number of smart meters or other smart gateways in the future will occupy a large amount of spectrum resources and consume a large amount of energy. Therefore, we consider using massive MIMO technology to increase spectrum efficiency and energy efficiency [6-7] to achieve stable operation of smart grids. There have been articles considering the use of massive MIMO to improve the spectrum efficiency and energy efficiency of MEC. Literature [8] in a large-scale antenna heterogeneous MEC network, jointly optimize the unloading ratio, calculation frequency and offloading time to minimize the energy consumption of the system; Literature [9] use data partitioning to improve the energy efficiency of massive MIMO-MEC.

In summary, most of the existing massive MIMO-MEC system researches focus on energy efficiency issues, but currently they have not addressed intelligent Grid mobile edge computing have been researched. In addition, no one has used physical layer security technology to achieve the information security of grid data in response to this problem.

2. System model

In a single cell, assuming that the number of smart meters for the requested service is K, there is an MEC server and a malicious eavesdropping provider, which can steal data offloaded by some users' smart meters (SM) and log in its inherent server performs calculations to achieve the purpose of stealing information. The MEC server is deployed on the base station (BS), and M antennas are configured at the base station, and the number of antennas for malicious eavesdroppers is N.

2.1. Communication model

We consider performing information statistics every fixed duration T to realize real-time processing of grid data. Each smart meter has $s_k$ input bits, and the information must be offloaded within this time. In this article, we assume that the base station and the malicious user have collected all the smart meters in the cell to the BS and the perfect channel state information of the malicious user, denoted as $g_k$ and $g^e_k$ respectively, where $g_k = h_k \sqrt{\beta_k}$ is the uplink channel gain matrix of $SM_k$, $g^e_k = h^e_k \sqrt{\beta^e_k}$ is the channel gain matrix between $SM_k$ and the eavesdropping user, $h_k \sim CN_{M \times 1}(0_{M \times 1}, I_M)$ and $\beta_k$ represent the small-scale and large-scale fading between $SM_k$ and the BS, $h^e_k \sim CN_{N \times 1}(0_{N \times 1}, I_N)$ and $\beta^e_k$ represent the small-scale and large-scale fading between $SM_k$ and the eavesdropper. The corresponding achievable rate is

$$r_k = B \log_2 \left(1 + \frac{p_k M \beta_k^2}{p_k \beta^2_k + \sum_{j \neq k, i \neq 1} p_i \beta_i + \beta_k \sigma_k^2}\right)$$

where, $p_k$ is the transmission power of $SM_k$, $\sigma_k^2$ is the variance of an additive white Gaussian noise at $SM_k$. We assume that the total spectrum bandwidth is $B$ Hz. Similarly, the transmission rate of eavesdropping users is expressed as
\[ r_k^e = B \log_2 \left(1 + \frac{p_i \beta_{k,e}^2}{p_i \beta_{k,e}^2 + \sum_{i \neq k, i \neq 1} p_i \beta_{k,e} \beta_{i,e} + \beta_{k,e} \sigma_i^2} \right) \]  \hspace{1cm} (2)

Therefore, the corresponding security rate is 

\[ r_k = \left[ r_k^b - r_k^e \right]^+ \]  \hspace{1cm} \text{where,} \hspace{1cm} [x]^+ = \max(x,0)

2.2. Computing model

The edge server is equipped with a computing server with a computing capacity of \( C \) (calculated in the number of CPU cycles per second). \( f_m \) is the total CPU frequency of the server. Assuming that the MEC server has high computing power and uses virtualized parallel computing to realize the independent calculation of each group of data, the energy consumption of offloading all smart meters is expressed as:

\[ E_{\text{off}} = \sum_{k=1}^{K} \mu_k \left( p_k + p_r \right) \frac{s_k}{R_k} \]  \hspace{1cm} (3)

where, \( \mu_k \) is the amplification factor of the power amplifier, and \( p_r \) is the circuit power loss during transmission. \( R_k \) is the transfer rate during offloading. \( s_k \) is the number of bits offloaded from \( SM_k \) to MEC. The energy consumption calculated on the MEC server is expressed as

\[ E_{\text{MC}} = \sum_{k=1}^{K} \mu_{m,k} f_{m,k}^2 C_s_k \]  \hspace{1cm} (4)

The CPU frequency \( f_{m,k} \) is the computational rate assigned to the \( SM_k \) task by the MEC, and \( \mu_{m,k} \) is a hardware dependent constant of the MEC server. In order to minimize the energy consumption of edge server computing, MEC server adopt dynamic voltage and frequency scaling (DVFS) technology. The MEC server can dynamically allocate a reasonable computing frequency according to the delay limit and offloading data. The time required for the user to calculate the task in MEC is \( t_k^c = \frac{C_s_k}{f_{m,k}} \), the offloading delay is \( t_k^\text{off} = \frac{s_k}{R_k} \). The optimal calculation frequency is \( f_{m,k} = \frac{C_s_k}{C_s_k / (T - \frac{s_k}{R_k})} \). In addition, we assume that the calculation result is small and negligible.

3. Optimization problem formulation

In order to better meet the needs of \( SM \) and realize the secure transmission of data. This article uses physical layer security technology, that is, to prevent eavesdropping by strictly satisfying that the offload rate cannot exceed the minimum security rate. On this basis, the \( SM \) transmit power and maximum offloading rate are combined to minimize the system's total energy consumption under the time delay constraint. The optimization problem is formulated as follows:

\[ \min_{p,R} E = \sum_{k=1}^{K} \left( \mu_k (p_k + p_r) \frac{s_k}{R_k} + \mu_{m,k} f_{m,k}^2 C_s_k \right) \]  \hspace{1cm} (5)

\( C1: t_k^c + t_k^\text{off} \leq T \), \hspace{1cm} \( C2: 0 \leq p_k \leq p_k^{\text{max}} \), \hspace{1cm} \( C3: \left[ r_k^b - r_k^e \right]^+ \geq R_k \), \hspace{1cm} \( C4: \sum_{k=1}^{K} f_{m,k} \leq f_m \)

C1 represents the limit of offloading time, C2 represents the constraint of transmission power, and C3 represents the constraint of secure rate. Taking into account the actual scene in reality, the eavesdropper is generally far away from the base station in the smaller area. Through formulas (1) and (2), we can know that \( r_k^b \geq r_k^e \). Thus, C3 can be reduced to \( r_k^b - r_k^e \geq R_k \).

For problem (5), considering that the constraint C3 is a non-convex function, it can be seen from
formulas (1) and (2) that \( r_k \) and \( r_k \) are a concave function, and it is difficult to directly solve the problem through convex optimization. Therefore, we set the constraint C3 Simplify.

\[
C5: r_k^* - r_k^* \geq R_k
\]

\[
2 \log (p_k M \beta_k^2 + a) b, \quad r_k^* = B \log_2(p_k N \beta_k^2 + b) a
\]

where, \( a = p_k \beta_k^2 + \sum_{i \neq k, j=1}^{K} p_i \beta_i \beta_j + \beta_i \sigma_k^2 \) \( b = p_k \beta_k^2 + \sum_{i \neq k, j=1}^{K} p_i \beta_i \beta_j + \beta_i \sigma_k^2 \).

Since in inequality (6), the left side is the subtraction of two concave functions, it is a non-convex function, so \( r_k^* \) can be approximated as an affine function for solving.

\[
r_k^* - [r_k^* + (\nabla p_k \beta_k^2 / p_k - p_i) \gamma (p - p_i)] \geq R_k
\]

For any given \( p_1 \), the first expression of (7) is a concave function, and the second expression is an affine function, so the constraint function (7) is a concave function. Therefore, we can find the maximum value of the secure rate through a sequential iterative optimization algorithm.

Algorithm1 The power control and offloading rate algorithm based on sequential iterative optimization algorithm.

1. Initialize tolerant thresholds \( \delta_s = 1 \), a group of feasible values \( p^0 \), and the number of iterations \( n = 0 \). 2. While \( \delta_s \geq 0.01 \), Do \( n = n + 1 \); 3. Bring \( p^n \) into C5 to get the maximum \( R_k^* \); 4. Calculate \( t^{\text{on}}_k \) and \( t^{\text{off}}_k \) respectively; 5. If \( t^{\text{on}}_k + t^{\text{off}}_k \geq T \), break; else Calculation formula (5) minimum E. end

6. Calculation \( \delta_s = \max \left[ \frac{p_k^n - P_k^{n-1}}{P_k^{n-1}} \right] \) Calculate the optimal \( p_k^n, R_k^* \), and \( E^{\text{opt}} \).

4. Simulation results

In this section, we will provide numerical results to verify the performance of the proposed massive MIMO-MEC scheme. The specific simulation parameters are set as follows: we assume that the number of Smart meters currently requesting service is \( K = 20 \), the number of antennas of the eavesdropper is \( N = 32 \), the number of CPU cycles per MEC 500 cycles/bit , the CPU cycle frequency of the MEC server is \( f_{\text{m}} = 3.4 \text{GHz} \) [9].

Figure 1 shows the total energy consumption of offloading data to MEC through massive MIMO. It can be seen that as the number of antennas increases, the energy consumed during transmission gradually decreases. It’s not difficult to understand that with the increase in the number of antennas, the secure transmission rate increases greatly, which increases the offload efficiency and greatly reduces the energy consumed by the smart meter. Although the energy consumption reduction in the figure is relatively small, when users expand the amount of data to the entire smart grid, the energy consumption saved is undoubtedly huge.
Figure 2 shows the energy consumption of MEC calculation tasks under the condition of time delay limitation. Because this article considers the lowest energy-saving scheme, dynamic voltage and frequency scaling (DVFS) technology is adopted, so that the calculation frequency of the CPU in the MEC can change with the delay limit and the dynamic change of the task volume. It can be seen from the figure that as the delay requirement is relaxed, the CPU frequency per unit time is greatly reduced, and the computational energy consumption of the MEC is reduced. In addition, it proved that as the amount of offloaded data increased, the amount of tasks consumed by MEC increased substantially.

5. Conclusion
This paper considers using massive MIMO technology in smart grids and setting up massive antennas on the base station side, which can greatly improve energy efficiency and transmission rate, and meet the requirements of low latency and low energy consumption in the smart grid system. In addition, this article also considers the security threat of eavesdroppers stealing information, and proposes the use of physical layer security technology to prevent eavesdropping, and fully guarantee the secure and energy saving of smart grids. Finally, simulations prove that under this new massive MIMO-MEC secure edge computing system model, on the basis of ensuring information security, as the number of antennas increases, the energy consumption of the system is significantly reduced.

References
[1] Stojmenovic I, and Wen S, (2014) The fog computing paradigm: Scenarios and security issues, in Proc. FedCSIS, Warsaw, Poland, pp. 1-8.
[2] Okay F Y and Ozdemir S, (2016) A fog computing based smart grid model, in Proc. ISNCC, pp. 1-6.
[3] Lu R, Liang X, Li X, Lin X, and Shen X, (2012) EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications, IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621-1631.
[4] Diao F, Zhang F, and Cheng X, (2015) A privacy-preserving smart metering scheme using linkable anonymous credential, IEEE Trans. Smart Grid, vol. 6, no. 1, pp. 461-467.
[5] Busom N, Petrlic R, Sebe F, Sorge C, Valls M, (2016) Efficient smart metering based on homomorphic encryption, Comput.Commun., vol. 82, pp. 95-101.
[6] Gizlenmistir Y, (2018) Massive MIMO in LTE systems: Energy and spectral efficiency," 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, pp. 1-4.
[7] Xiong J, You L, Zappone A, Wang W and Gao X, (2019) Energy- and Spectral-Efficiency Tradeoff in Beam Domain Massive MIMO Downlink with Statistical CSIT, 2019 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Ottawa, ON, Canada, pp. 1-5.
[8] Hao Y, Ni Q, Li H and Hou S, (2019) Energy-Efficient Multi-User Mobile-Edge Computation Offloading in Massive MIMO Enabled HetNets, IEEE International Conference on Communications, Shanghai, China, pp. 1-6.
[9] Malik R, Vu M, (2020) Energy-Efficient Offloading in Delay-Constrained Massive MIMO Enabled Edge Network Using Data Partitioning, arXiv:2001.08259. [Online]. Available: http://arxiv.org/abs/2001.08259.