Proceedings of the 2023 International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/34/20230329

# Joint optimization of utility and privacy in mobile edge computing

**Miou Lu**

University of California, Davis, 1 Shields Ave, Davis, CA 95616, the US

miolu@ucdavis.edu

**Abstract.** In mainstream research on Mobile Edge Computing (MEC), considerations for user privacy are often overlooked. This paper introduces Differential Privacy techniques to MEC, which obfuscate specific parameter values when transmitting user data, preventing leakage of sensitive information. Simultaneously, privacy, latency, and energy are incorporated as components of the utility function. We model the task offloading process using a deep reinforcement learning model and propose the use of the Deep Deterministic Policy Gradient (DDPG) algorithm in conjunction with a Laplacian privacy budget for joint optimization of privacy and utility during offloading. After sufficient training, the DDPG model can effectively approximate the optimal solution. Compared to traditional work, the optimized framework gives ample consideration to user privacy needs and outputs the optimal task offloading ratio solution with relatively low time complexity. This approach effectively safeguards user privacy while also considering the efficiency of task offloading.

**Keywords:** mobile edge computing, differential privacy, Deep Deterministic Policy Gradient, task offloading, joint optimization.

## 1. Introduction

Nowadays, with the advent of the 6G era and the explosive growth of Internet applications, such as Chat-GPT, Virtual Reality, Augmented Reality, and Ray Tracing, the massive data generated by mobile users (MUs) during operation has imposed significant pressure on network bandwidth and computing resources [1].

In the traditional centralized cloud computing model, the cloud center is often far away from the MUs, making it difficult to achieve efficient transmission. It also increases the risk of data leakage. Mobile edge computing (MEC), as a new distributed computing model, aims to address this challenge [2]. Its core idea is to deploy computing, storage, network resources, and base stations densely at the network edge. It mainly consists of MUs and surrounding edge servers. MUs offload their computing tasks to the edge for processing, while the cloud center only participates in control and scheduling. This architecture can significantly reduce latency and transmission loss.

However, existing work still has limitations. For example, many studies focus mainly on efficiency, overlooking that user data might be sensitive and require a certain degree of privacy protection [3]. This lack of consideration makes these algorithms difficult to directly implement in practical scenarios. Furthermore, traditional optimization problems often employ mathematical methods for calculating optimal solutions, including linear programming and heuristic algorithms. These methods necessitate extensive matrix operations or recursive iterations at the beginning of each task, exhibiting high time complexity. Such time costs are intolerable in many latency-sensitive applications.

Hence, in view of potential privacy breach risks during the offloading process in edge computing, this paper proposes a joint optimization approach for privacy and utility in MEC. The central idea is to integrate differential privacy (DP) technology into the traditional architecture for data generalization, meeting the privacy needs of MUs. Concurrently, deep reinforcement learning (DRL) methods are utilized for optimal decision-making, selecting the most suitable privacy cost, thereby balancing privacy and utility.

## 2. Key technology

In this section, we focus on introducing two key technologies of the proposed framework: the differential privacy tool for protecting user data privacy, and the deep reinforcement learning algorithm for improving decision efficiency. By combining these two technologies, we try to build a decision model in the MEC that balances utility and privacy costs.

### *2.1. Differential privacy*

Differential Privacy (DP) is an encryption technique utilized to obscure numerical data values [4]. In the context of Mobile Edge Computing (MEC), various services often request users to upload information such as GPS locations, bandwidth, CPU frequencies, and even device models. These data, if not properly handled, could jeopardize users' personal information and privacy. The core principle of DP lies in the inclusion of a certain amount of noise in the actual transmitted data, preventing the precise identification of individual data points and thus reducing the risk of information leakage.

Noise in DP commonly follows a Laplace distribution, within which exists a hyperparameter, $\epsilon$. This parameter is considered the privacy cost or privacy budget in differential privacy. It is employed to adjust the amount of noise added to the original data. A larger privacy budget signifies more noise, further obscuring individual data points to prevent sensitive data leakage. However, it must be noted that enhancing privacy could potentially degrade the quality of service.

By dynamically adjusting this parameter, we can control the level of privacy protection, striking a balance between the safeguarding of privacy and the utility of the service.

### *2.2. Deep reinforcement learning*

Deep Reinforcement Learning (DRL) is an artificial intelligence decision-making algorithm that combines deep learning and reinforcement learning [5]. It leverages the powerful perceptual capabilities of neural networks to address the modeling of policy functions or value functions, and learns from large data sets. Meanwhile, it utilizes the decision-making ability of reinforcement learning to define decision problems and optimize objectives. To some extent, DRL exhibits a form of general intelligence capable of tackling complex issues, possessing the ability to approximate optimal solutions with remarkably low execution time complexity.

More specifically, Deep Reinforcement Learning (DRL) learns through interactions by training an agent and modeling the environment as a Markov Decision Process (MDP). It employs a reward function to assess the agent's actions, encouraging beneficial behaviors and penalizing detrimental ones. After extended periods of training, the Deep Learning Neural Network embedded within the agent acquires optimal decision-making capabilities, allowing it to directly predict the optimal action from the input state.

The subsequent part of this paper points out that the decision problem at hand is a continuous variable problem.

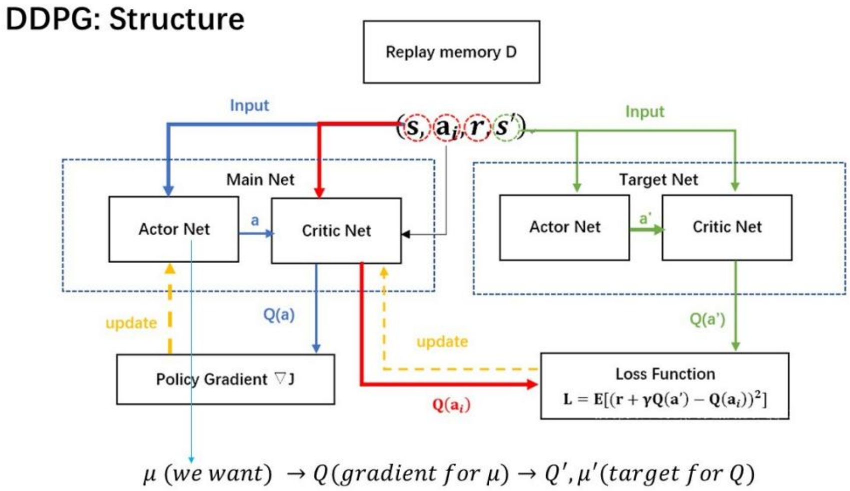

**Figure 1.** DDPG structure.

Therefore, as shown in Figure 1, we employ the Deep Deterministic Policy Gradient (DDPG) as the fundamental DRL architecture [6]. DDPG primarily includes four neural networks: dual Actor networks and dual Critic networks. The Actor network is utilized to evaluate the quality of actions, while the Critic network is used to directly generate optimal actions from the state space. The purpose of employing dual networks is to expedite model convergence. In addition, an experience replay buffer is used to mitigate the correlation between samples. After sufficient interaction and learning with the environment, DDPG can effortlessly acquire an approximation to the optimal solution and outputs it within a time complexity of O(NM), where N and M represent the number of inputs and the number of neural network neurons, respectively, and its value generally not more than 105.

## 3. Joint optimization of utility and privacy in mobile edge computing

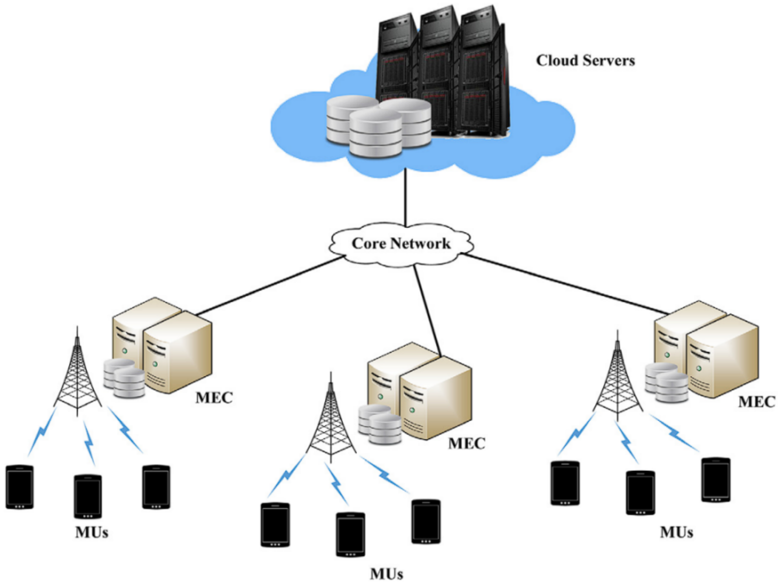

**Figure 2.** The architecture of MEC.

According to Figure 2, in MEC, various underlying services and technologies exist [7]. We primarily focus on joint optimization of utility and privacy in task offloading strategies, which can be defined as a problem of offloading ratio in communication. Users decide the portion of tasks to offload to the edge for computation based on their own parameters (location, task size, privacy requirements) and information broadcasted by the server (location, bandwidth, energy consumption). This is represented by the parameter $\alpha$, denoting the proportion of the task being transferred to the edge.

When $\alpha$ tends towards 0, it can be viewed as local computing, where the latency is typically high but the privacy requirement is low, and there's no additional energy expenditure needed. Conversely, when $\alpha$ tends towards 1, it's considered as complete offloading. In this case, there's low latency but it introduces certain privacy demands and increases energy costs. If $\alpha$ falls between 0 and 1, it is referred to as partial offloading. Our optimization objective is to compute the optimal offloading ratio $\alpha$, given the user's parameters and server information.

In our system, we model channel transmission, energy consumption, and privacy costs, which are used to compute the delay, energy expenditure, and privacy overhead of task offloading. For the sake of simplification, we employ the most straightforward models of wireless signal path loss, CPU power calculation, and Laplace privacy budgeting. With the aim of maximizing utility while maintaining an appropriate level of privacy, we formulate this as a Markov Decision Process (MDP). The MDP is realized through training an intelligent agent, whose actions are evaluated according to a predefined reward function.

By leveraging DP and DRL, we can easily quantify the privacy cost and consider it along with latency and energy as components of utility. Next, utilizing the Deep Deterministic Policy Gradient (DDPG) network, we treat the utility as the reward function, continuously training the model. Once the model's loss function tends to smooth out, we consider the model as converged. And then, the trained model is fixed and serves as the actual model in real-world applications. It can swiftly compute the optimal offloading ratio from complex numerical data, maximize utility, and provide MEC users with a more comfortable and convenient service.

## 4. Conclusion

In this paper, we present a privacy-preserving solution for the task offloading problem in MEC, balancing privacy and utility through DRL techniques. Specifically, the solution employs DP to obfuscate user data, preventing parties from inferring sensitive user information. Then, it takes into account the user's privacy cost, energy, and latency in a balanced manner, forming them into a reward function to guide the learning of the agent. This maximizes utility while satisfying certain privacy requirements, balancing latency and energy consumption.

Compared to traditional architectures, this approach is more suitable for real-world scenarios. The proposed algorithm uses Deep Reinforcement Learning as the decision-making model, which comprises two distinct stages: the training phase and the execution phase. These phases operate independently, implying that we only need to undertake one extensive, thorough training period before the model can be fixed. In practical scenarios, the fixed model can be used for decision-making, which typically has a near-constant computing overhead, significantly reducing processing delay and energy consumption. The decision-making system based on Artificial Intelligence (AI) algorithms has lower time complexity. It provides a more applicable task offloading algorithm for MEC, holding the potential to offer better services for future IoT mobile users.

However, this work simplifies certain aspects of the model, such as assuming noiseless channel transmission and infinitely divisible tasks, which may not reflect reality. It also solely presumes a single-user, single-server transmission model, neglecting potential multi-user game theory issues. In complex scenarios, edge servers may need to filter multi-user requests, or there will be wait times due to multiple demands.In future work, we plan to improve mainly in two aspects: the first is to further refine our model to better align with the real world, and the second is that to model and address the optimization problem involving multiple users and services with game theory, employing novel strategies to achieve optimal complex solutions.

## References

[1] Siriwardhana, Y., Porambage, P., Liyanage, M., Ylianttila, M. (2021). AI and 6G security: Opportunities and challenges. In 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), pp. 616-621.

[2] Aslanpour, M. S., Gill, S. S., Toosi, A. N. (2020). Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. Internet of Things, 12, 100273.

[3] Lan, X., Cai, L., Chen, Q. (2019). Execution latency and energy consumption tradeoff in mobile-edge computing systems. In 2019 IEEE/CIC International Conference on Communications in China (ICCC), pp. 123-128.

[4] Dwork, C. (2006). Differential privacy. In International colloquium on automata, languages, and programming. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 1-12.

[5] Li, Y. (2017). Deep reinforcement learning: An overview. arXiv preprint arXiv:1701.07274.

[6] Hou, Y., Liu, L., Wei, Q., Xu, X., & Chen, C. (2017). A novel DDPG method with prioritized experience replay. In 2017 IEEE international conference on systems, man, and cybernetics (SMC), pp. 316-321.

[7] Chen, M., Hao, Y. (2018). Task offloading for mobile edge computing in software defined ultra-dense network. IEEE Journal on Selected Areas in Communications, 36(3), 587-597.