

Anti-eavesdropping and interference-resistant unmanned aerial vehicle - MEC system robustness task offloading mechanism

Jianbin Xue¹[0000-0002-4645-0803], Han Zhang²(✉)[0000-0001-8765-9251]

¹ Modern Industry College of Microelectronics, Lanzhou University of Technology, Lanzhou City 730050, China

² College of Computer and Artificial Intelligence, Lanzhou University of Technology, Lanzhou City 730050, China
hanshuail1@yeah.net

Abstract. With the rapid growth of intelligent wireless applications, secure task offloading in mobile edge computing (MEC) systems has become increasingly important. This paper investigates a UAV-assisted MEC framework in the presence of potential eavesdroppers. A three-layer architecture consisting of mobile users, UAV-mounted MEC servers, and cloud servers is developed to support flexible edge computing services. To improve transmission security and task continuity, a task segmentation strategy is introduced to divide large tasks into smaller sub-tasks during user mobility. In addition, a differential privacy-based distance perturbation mechanism is designed to conceal user location information and reduce inference attacks. A joint optimization framework is further proposed to determine task allocation and offloading decisions with the objective of minimizing system delay while improving communication security. Simulation results show that the proposed method effectively reduces privacy leakage risk and improves secure task processing performance under dynamic wireless conditions.

Keywords: Communication Security, Mobile Edge Computing, Data Offloading, Wireless Communication.

1 Introduction

The rapid development of intelligent applications has greatly increased the demand for low-latency and computation-intensive services [1]. Although cloud computing provides strong processing capability, remote transmission often introduces excessive delay and network congestion [2]. Mobile edge computing (MEC) addresses this issue by enabling computation near end users [3,4].

Recently, UAV-assisted MEC systems have attracted significant attention because UAVs can dynamically provide edge services in mobile or infrastructure-limited environments [5–7]. However, wireless task transmission in UAV-assisted MEC systems remains vulnerable to eavesdropping and privacy leakage [8–11]. Existing

studies mainly improve security through interference control, trajectory optimization, or resource allocation methods [12–15]. Some works also apply federated learning, reinforcement learning, or blockchain techniques to improve offloading efficiency and secure communication [16–20]. Nevertheless, user location privacy and stable task execution under mobility are still insufficiently addressed.

To solve these issues, this paper proposes a secure task offloading mechanism for UAV-assisted MEC systems. First, computation tasks are divided into multiple partitions to support continuous execution during user mobility. Second, a differential privacy-based distance perturbation strategy is introduced to protect user location information during task offloading. Finally, a joint optimization framework is developed to reduce system delay while improving communication security. The main contributions are summarized as follows:

- A segmented task offloading mechanism is proposed for mobile UAV-assisted MEC systems.
- A differential privacy-based distance perturbation method is designed to protect user location privacy.
- A joint optimization model is developed to improve both transmission security and task processing efficiency.

2 Related work

Secure transmission and privacy protection in MEC systems have been widely studied in recent years. Existing works mainly focus on physical-layer security, intelligent task offloading, and privacy-preserving communication.

Several studies improve communication security through cooperative interference, UAV trajectory optimization, and transmission power control [12–15]. Although these methods enhance resistance against eavesdropping, they may introduce additional system overhead. Other studies investigate task offloading optimization using reinforcement learning, Markov decision processes, and resource scheduling strategies [16–20]. Meanwhile, federated learning, blockchain, and differential privacy techniques have also been introduced to reduce privacy leakage risks. However, most existing approaches mainly emphasize latency or energy efficiency while paying limited attention to location privacy in dynamic UAV-assisted MEC environments.

Different from previous studies, this paper jointly considers secure communication, user mobility, and location privacy protection. By combining task segmentation with differential privacy-based distance perturbation, the proposed method improves secure task execution while reducing user privacy leakage risks.

3 System Model

Multiple wireless access nodes are distributed around mobile users in the considered MEC environment. Fig. 1 presents the architecture of the proposed UAV-assisted MEC system. As the user begins to move, their position changes when they move to the next location, and the coverage range of edge servers around the user is also limited due to

the range of the drone, resulting in an inability to guarantee the quality of service provided. Meanwhile, wireless transmission may suffer from eavesdropping and privacy leakage risks.

3.1 System Model

The proposed framework considers mobile users generating computation-intensive tasks within UAV-assisted MEC coverage areas.

Fig. 1 illustrates the overall architecture of the considered UAV-assisted MEC framework. The considered MEC architecture consists of three collaborative layers, namely the cloud layer, the edge cloud layer composed of drones equipped with MEC servers, and the user layer. The user layer contains mobile users together with potential eavesdroppers. The user mobility trajectory is represented by a sequence of connected path segments, which represent $\{l_1, l_2, \dots, l_n\}$ through the set L . Adjacent communication regions are considered independent with limited overlap. The communication coverage radius is denoted by r , and there exists a set of radii $R = \{r_1, r_2, \dots, r_n\}$, where drones equipped with MEC servers with computing and storage capabilities are placed in each small unit. Each communication region is assumed to contain one UAV-mounted MEC server, so there exists a set $N = \{n_1, n_2, \dots, n_n\}$ representing the MEC server and $M = \{m_1, m_2, \dots, m_m\}$ representing the ground user group.

Mobile users continuously generate computation tasks during movement. Since user tasks have different computational requirements, we use u_k to represent the task size of user k , s_k to represent the input data bit size of task calculation, and w_k denotes the required CPU cycles for task execution, $w_k = \omega * s_k$ where ω is determined by the computational complexity of the user task.

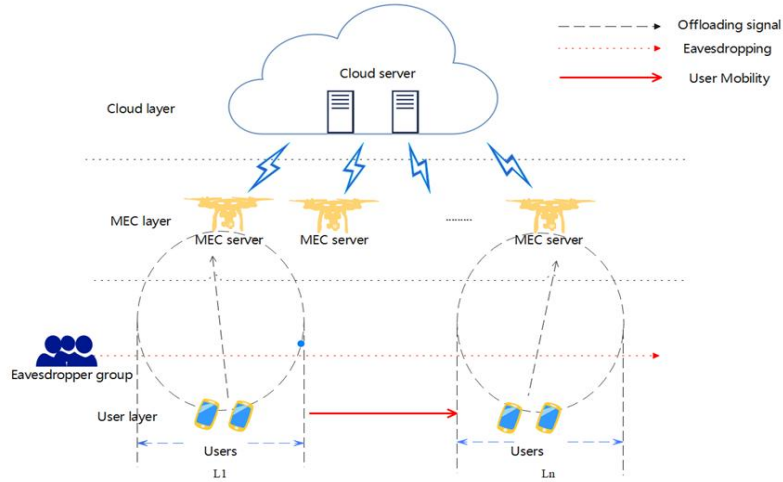


Fig. 1. System model.

We represent the computing power of local users as f_i , the total computing power of MEC servers as C , where f_j represents the computing power allocated by edge server j to local users themselves. Therefore, for the computing task u_k of mobile users, the processing time locally is w_k/f_i , and the processing time on edge servers is

$$w_k/f_j.$$

To improve transmission reliability and execution continuity, each computation task is divided into multiple smaller partitions. Individual partitions can either be processed locally or offloaded to the current MEC server. If communication interruption occurs because the user moves outside the coverage region, only the unfinished partition requires retransmission instead of restarting the entire task. At the same time, each task partition can choose to process tasks locally or uninstall them to the current MEC server for processing. In this paper, if the task execution process is interrupted because the user moves out of the communication coverage area, you do not need to re-upload the calculation task, you only need to re-partition the interrupted task, and then continue to upload the re-partitioned task. This article considers that if the size of each task unit is I_0 bits, then the total number of partition blocks for the mobile user's task is

$$N_q = \left\lceil \frac{S_k}{I_0} \right\rceil \text{ (Take the upper limit).}$$

3.2 Offloading Model

When a user moves to change location, they may be covered within the range of different MEC servers. Direct server selection may lead to communication congestion and unbalanced resource utilization. To reduce offloading latency and improve resource utilization, we need to consider how to choose a suitable MEC server for users to offload tasks. We assume that the task upload rate has a maximum value $R_{\max}$, which is limited by bandwidth. If the maximum uplink rate assigned to user i is r_i , then r_i can be obtained as follows:

$$r_i = B \log_2 \left(1 + \frac{p_k h_{i,k}}{\delta^2} \right) \quad (1)$$

Among them, $h_{i,k}$ represents the channel gain between ground mobile user k and MEC server i , p_k represents the transmission power of ground mobile user, B represents the channel bandwidth, and δ^2 represents noise. In the proposed framework, Local execution is also allowed to reduce MEC workload. Due to the mobility of users and the distance between users and MEC, security issues have also become prominent.

We consider T_1 representing the queuing delay of computing tasks on the MEC server, and T_2 representing the communication delay from ground users to the MEC

server:

$$T_2 = \beta \cdot Z^* \quad (2)$$

Among them, Z^* represents the distance from the i -th ground user to the j -th MEC server (i.e. the distance Z^* after disturbance in the subsequent 3.4.). We assume that if the task does not choose to unload to a nearby MEC server, T_2 is 0.

3.3 Task Segmentation

Considering user mobility and task complexity, computation tasks are divided into multiple partitions. When a mobile user enters a communication region of unit l_s , the time that the mobile user stays in that unit can be calculated first:

$$T_3 = \frac{r_s}{v_1} \quad (3)$$

where v_1 represents the speed at which the mobile user moves within that unit. Accordingly, the maximum local execution delay can be estimated as:

$$T_3 = \frac{r_s}{v_1} T_{st} = \frac{\omega N_{qloc,max} I_0}{f_i} \quad (4)$$

Due to the limited number of task partition blocks that users can offload to the MEC server for processing, $N_{qoff,max}$ represents the maximum number of task partition blocks that can be offloaded in a unit. Its value is determined by the duration of stay in the unit, channel conditions, and the computing power of the MEC server. In this article, we consider using the average uplink rate of all ground users in the unit to represent the data transmission rate in the unit:

$$r_1 = \frac{1}{m} \sum_{i=1}^m B \log_2 \left(1 + \frac{p_k h_{i,k}}{\delta^2} \right) \quad (5)$$

Meanwhile, we consider calculating the average computing power of all MEC servers in the unit using the following equation:

$$f_m = \frac{1}{n} \sum_{j=1}^n f_m^j \quad (6)$$

Due to changes in the coverage range of MEC servers during user movement, in order to avoid interruptions during task execution, the execution time of unloading to MEC servers cannot exceed the maximum time the user stays in the unit. Therefore, we can derive constraint conditions:

$$\frac{N_{qoff,max} I_0}{r_1} + \frac{\omega N_{qoff,max} I_0}{f_m} \leq T_{max} \quad (7)$$

From the previous settings in this article, it can be concluded that the total number of task partitions calculated includes the maximum number that local devices can execute and the total number of task partitions offloaded to MEC servers for execution. Therefore:

$$N_{q,max} = N_{qloc,max} + N_{qoff,max} \quad (8)$$

We have set an adjustment factor ϕ , $\phi \in [0,1]$, which depends on the quality of the channel and the workload of the unit. When the channel quality of the user's unit is worse or the communication load is larger, the value of ϕ is smaller. Therefore, we can determine the number of task partition blocks that can be completed in the unit:

$$N_q = \lfloor \phi N_{q,max} \rfloor \quad (9)$$

We can obtain the pre assigned set of tasks in each unit, represented as:

$$N_q = \{N_q^1, N_q^2, \dots\} \quad (10)$$

3.4 Security Policy

Let Z denote the actual distance between a mobile user and the MEC server. meanwhile the perturbed distance is Z^* . We let Z_{max} represent the maximum coverage radius of the MEC server, Z_1 and Z_2 represent the upper and lower bounds of the range of the user's perturbed distance, respectively, $\Delta Z = Z_2 - Z_1$, $Z_1 < Z_2$, $Z_1, Z_2 \in [0, Z_{max}]$.

After defining the perturbation interval, a differential privacy mechanism is introduced to interfere with the distance of the ground mobile user to the MEC. Direct application of Laplace perturbation in MEC task offloading is challenging due to the constrained transmission distance in wireless environments. To guarantee probability normalization within the perturbation interval, we have designed a Probability Density Function (PDF), which is:

$$Pdf(Z^*|Z) = \begin{cases} \frac{\theta}{2\Delta Z} e^{-\frac{\theta|Z^*-Z|}{\Delta Z} + e^{\frac{\theta(Z_1-Z)}{\Delta Z} + e^{\frac{\theta(Z_2-Z)}{\Delta Z}}}} & \text{if } Z^* \in [Z_1, Z_2] \\ 0 & \text{otherwise} \end{cases} \quad (11)$$

The perturbation process masks the actual user location information. Since task offloading is performed based on the perturbed distance, eavesdroppers can only infer a distorted user location from the offloading ratio. The inherent randomness of

differential privacy further prevents accurate location inference, thereby protecting user data privacy.

To balance privacy protection and communication efficiency, the perturbation interval is dynamically adjusted according to wireless channel conditions and user privacy requirements. A larger perturbation range provides stronger location privacy but may increase transmission overhead and task latency. Therefore, the proposed mechanism selects an adaptive perturbation interval to achieve a tradeoff between communication performance and privacy preservation..

KL divergence is adopted to evaluate the similarity between real and perturbed distance distributions and those who do not when the true distance between the user and the MEC server is Z . Assuming that $Q(Z^*|Z)$ represents the probability distribution of users unloading tasks at the true distance without privacy protection mechanisms, and $P(Z^*|Z)$ represents the probability distribution of users perturbing at the true distance with privacy protection mechanisms, the degree of fit between the two is:

$$D_{KL}(P\|Q) = \int_{Z_1}^{Z_2} Q(Z^*|Z) \log \frac{Q(Z^*|Z)}{P(Z^*|Z)} dZ^* \quad (12)$$

According to the KL divergence property, we can conclude that if the value of $D_{KL}(P\|Q)$ is smaller, the degree of fit is higher, a higher probability of leakage of true distance information between users and MEC servers, and a lower degree of protection for user privacy data. Therefore, if we assume that the true distance between the ground mobile user and the MEC is Z , the degree of data information leakage of the ground mobile user can be expressed as the opposite of the above equation:

$$PZ_{Z_1, Z_2} = - \int_{Z_1}^{Z_2} Q(Z^*|Z) \log \frac{Q(Z^*|Z)}{P(Z^*|Z)} dZ^* \quad (13)$$

In summary, this article mainly provides a new differential privacy based denoising method for the true distance between ground users and MEC servers, in order to protect the privacy of user data information. However, before unloading tasks based on this false distance, we need to determine the specific values of Z_1 , Z_2 .

In this article, in order to protect user data information while minimizing energy consumption and latency during task offloading, users in each MEC system should adaptively add noise based on their wireless channel situation with the MEC server, thereby perturbing the true distance. When channel quality becomes stable, in most cases, the false distance formed after interference will be relatively close. Offloading strategies are determined according to perturbed distance information can ground users ensure that they will offload more tasks to MEC servers, thereby reducing their resource consumption in real locations. Similarly, to ensure the utility of the task offloading

decisions made by ground users based on the false distance Z^* , we maximize the utility when false distance $Z^* = Z$. Therefore, in this article, it is necessary to ensure that the false distance Z^* lies on the left and right sides that are close to the true distance Z , in order to obtain the disturbance range $Z_1 \leq Z \leq Z_2$. Moreover, the closer Z_1 , Z_2 and Z are, the better the effectiveness of the task unloading decision under the false distance.

Overall, when the range ΔZ between Z_1 and Z_2 is reduced, although task offloading decisions based on false distances can reduce the user's energy consumption and latency at the real distance, the program that leaks user information and data privacy will increase. To balance privacy preservation and communication efficiency, the perturbation interval is adaptively adjusted according to user privacy requirements and wireless channel conditions. Larger perturbation ranges provide stronger privacy protection but may increase transmission overhead and task latency.

We use the formula to adjust the disturbance range as follows:

$$\min_{Z_1, Z_2} E + D + \mathfrak{U} \cdot PZ \quad (14)$$

Among them, E is the user's energy consumption, D is the user's computational delay cost, and $\mathfrak{U}$, as an influencing element, it shows the degree of importance that ground users attach to their data information leakage. The more privacy is valued, the greater $\mathfrak{U}$, and vice versa.

4 Problem Formulation

The overall system delay mainly includes: (1) the time for ground users to upload the required offloading tasks; (2) Communication latency after applying security policies; (3) The time it takes for the MEC server to process the completed task data. The offloading ratio is defined as α , $\alpha \in [0, 1]$. When $\alpha = 0$, all task data partition blocks are processed and calculated locally. Otherwise, all data needs to be unloaded to the MEC server for processing and calculation.

In the previous section 3.2. setting, the maximum uplink rate of user i is r_1 . Therefore, the transmission delay for all offloading tasks that ground mobile users need to complete within their respective units is:

$$T_c = \frac{\alpha N_q I_0}{r_1} \quad (15)$$

The binary decision variable is defined as $x_{i,k} \in [0, 1]$, where $x_{i,k} = 1$ represents ground user k unloading data, and vice versa represents task processing performed locally. Accordingly, the offloading strategy is represented as $x_k = (x_{1,k}, x_{2,k}, \dots, x_{m,k})$,

and $\sum_{i \in M} x_{i,k} = 1$. Define the task partition block offloading selection variable as $y_{j,k} \in \{0,1\}$, where $y_{j,k} = 0$ indicates that the user chooses not to offload the task partition block to the j -th MEC server. Otherwise, they choose to offload to the j -th MEC server. Because the MEC selection strategy is represented as $y_k = (y_{1,k}, y_{2,k}, \dots, y_{n,k})$, and $\sum_{j \in N} y_{j,k} = 1$.

Thus, the time for processing task partition blocks locally can be expressed as:

$$T_l = \frac{\omega \alpha N_q I_0}{f_i} \quad (16)$$

When the user moves within their unit, the time it takes to offload a block of data to the MEC server for processing can be expressed as:

$$T_m = \frac{\omega \alpha N_q I_0}{f_j} \quad (17)$$

Based on the delay analysis above, we can obtain the total delay function of the entire unloading process of the task partition block:

$$T_x = T_m + T_c + T_l + T_2 \quad (18)$$

The task completion delay is defined as T_k^s :

$$T_k^s = \max\{T_l, T_x\} \quad (19)$$

The problem of minimizing delay can be expressed as:

$$\begin{aligned} \min T_k^s &= \min \sum_{i \in M} \sum_{j \in N} \max\{T_l, T_x\} \\ &= \min \sum_{i \in M} \sum_{j \in N} \max \left\{ \begin{aligned} &T_l, y_{i,k} T_m + x_{i,k} T_c + \\ &y_{i,k} T_1 + x_{i,k} y_{i,k} T_2 \end{aligned} \right\} \end{aligned} \quad (20)$$

The minimum time required for a ground mobile user to complete their compute offload task is:

$$T_k = \min_s \sum_s T_k^s \quad (21)$$

5 Problem Solving

The optimization model can be formulated as a mixed-integer programming problem, and we need to address issues such as task offloading decisions, offloading methods for task partitioning blocks, and offloading rates. So in the solving process, The task offloading strategy is initialized as $x_k = x_k^*$, and the offloading strategy for the task partition block is $y_k = y_k^*$. This occurs because in section 3.4., the optimization for user task offloading has already been solved. Therefore, this variable can be directly inputted, and the optimization problem can be transformed into a convex optimization problem about task offloading strategy. The function can be transformed:

$$\begin{aligned} f(\alpha) &= \min \sum_{i \in M} \sum_{j \in N} \max \left\{ \begin{aligned} &T_l, y_{i,k} T_m + x_{i,k} T_c \\ &+ y_{i,k} T_1 + x_{i,k} y_{i,k} T_2 \end{aligned} \right\} \\ &= \min \sum_{i \in M} \sum_{j \in N} \max \left\{ \begin{aligned} &\frac{\omega \alpha N_q I_0}{f_i}, y_{i,k} \frac{\omega \alpha N_q I_0}{f_j} + x_{i,k} \frac{\alpha N_q I_0}{r_1} \\ &+ y_{i,k} T_1 + x_{i,k} y_{i,k} \beta^* dis_{k,j} \end{aligned} \right\} \end{aligned} \quad (22)$$

We define $g(\alpha)$ and $\mu(\alpha)$:

$$g(\alpha) = y_{i,k} \frac{\omega \alpha N_q I_0}{f_j} + x_{i,k} \frac{\alpha N_q I_0}{r_1} + y_{i,k} T_1 + x_{i,k} y_{i,k} \beta^* dis_{k,j} \quad (23)$$

$$\mu(\alpha) = \frac{\omega \alpha N_q I_0}{f_i} \quad (24)$$

Then we can introduce:

$$f(\alpha) = \begin{cases} \min \sum_{i \in M} \sum_{j \in N} \mu(\alpha) & g(\alpha) \leq \mu(\alpha) \\ \min \sum_{i \in M} \sum_{j \in N} g(\alpha) & g(\alpha) > \mu(\alpha) \end{cases} \quad (25)$$

From the above equation, we can see that $g(\alpha)$ and $\mu(\alpha)$ are linear functions about α , $g(\alpha)$ is a monotonically increasing function about α , and $\mu(\alpha)$ is a monotonically decreasing function about α . Therefore, when the task offloading strategy $x_k = x_k^*$ and the offloading strategy $y_k = y_k^*$ for the task partition block, we can easily minimize the task execution time based on the task offloading ratio and task offloading decision. Due to the limited number of MEC servers, we can traverse all MEC servers and obtain the optimal solution through comparison.

Algorithm 1:

Algorithm 1. Optimization Algorithm for Task Offloading Decision Using Differential Privacy

- 1: Input:** $Z_{\max}$, Z , Wireless channel condition B between ground and MEC server, Task volume u_k for ground users;
 - 2:** For each possible disturbance range interval $[Z_1, Z_2]$: generate false position Z^* based on the true distance Z and the probability density function formula;
 - 3:** Task offloading decision based on false position Z^* with the goal of minimizing system cost under false position;
 - 4:** Find the appropriate disturbance range $[Z_1, Z_2]$ to balance the system cost and data information exposure at real distances;
 - 5:** For the final determined disturbance range $[Z_1^*, Z_2^*]$, generate false distance Z^* based on the true distance Z and make the optimal task unloading decision x_k^* ;
 - 6: Output:** x_k^*
-

6 Simulation

In this scheme, each edge server's coverage area is divided according to the mobility of ground users, and offloading tasks are partitioned accordingly. As shown in Fig. 2, the number of pre-allocated task partitions within the coverage areas of the first three edge servers decreases as user speed increases. This occurs because higher mobility shortens the user residence time within a coverage area, thereby reducing the available time for task offloading. Hence, the number of task partitions can be dynamically adjusted to adapt to user mobility. This design also helps reduce eavesdropping and attack risks, improving data transmission security.

Fig. 3 compares the user cost of the proposed scheme with two benchmark schemes under ideal, moderate, and weak signal-strength conditions. Signal strength is measured in dBm and decreases with propagation loss caused by distance and obstacles. In general, values above -70 dBm indicate ideal signal strength, -70 dBm to -80 dBm indicate moderate strength, and below -80 dBm indicate weak strength. The results show that the proposed scheme achieves the lowest cost under all three network conditions.

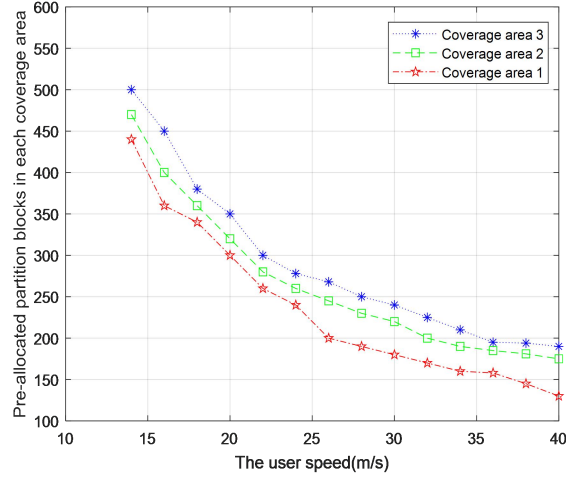


Fig. 2. Effect of user movement speed on pre-assigned unload task blocks.

Fig. 4 shows that as the privacy leakage impact factor of ground mobile users increases, the difference between the confusion ranges Z_1 and Z_2 also shows an increasing trend. This occurs because as the impact factor increases, ground mobile users are more inclined to prevent privacy and information leakage. Therefore, as the value of the confusion range increases, the possibility of privacy and information leakage decreases.

Fig. 5 shows the variation in privacy leakage under different privacy impact factors. From the figure, it can be seen that as the impact factor of privacy leakage increases, the degree of privacy disclosure decreases. This occurs because as the impact factor of privacy disclosure increases, the difference between the confusion ranges Z_1 and Z_2 also shows an increasing trend. When the confusion range is larger, the privacy disclosure is smaller. Therefore, the possibility of ground mobile user information and privacy being attacked and leaked is ultimately reduced, thereby improving the information transmission security of the entire communication link.

In Fig. 6, the abscissa is the distance between the ground mobile user and the mobile edge computing server. It can be seen from Fig. 6 that the difference between the confusion range Z_1 and Z_2 is not obvious as the distance increases. This occurs because although the larger the difference in the confusion interval, the lower the likelihood of user information and privacy leakage, the resulting increase in the user's own expenses. Therefore, we change the confusion interval by centering on the distance between the ground mobile user and the mobile edge computing server, that is, when the distance increases, Z_1 and Z_2 both become larger at the same time with Z as the center, so that the difference between the confusion interval will not change significantly, to maintain the equality of the relationship between user consumption and privacy disclosure.

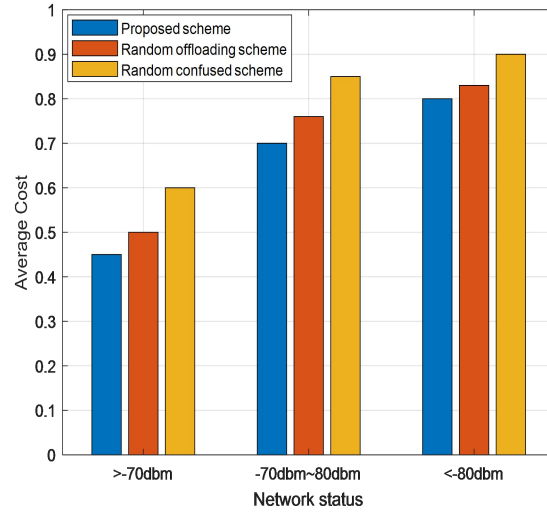


Fig. 3. Comparison of the cost of three schemes in different network states.

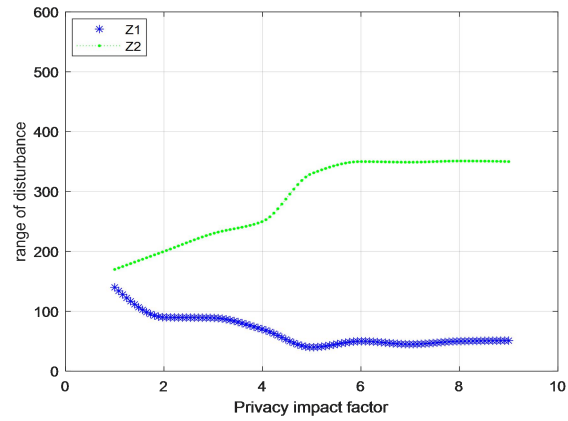


Fig. 4. The influence of privacy disclosure factors on the disturbance range.

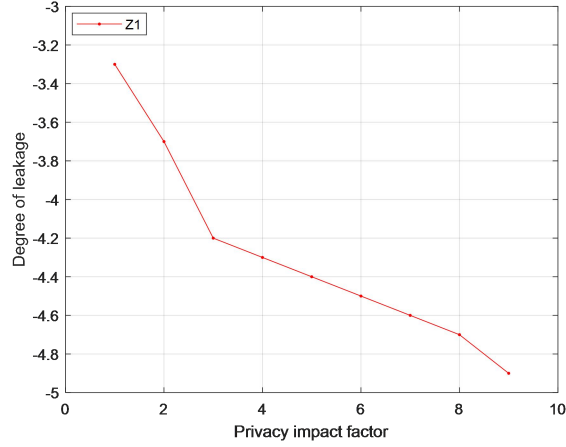


Fig. 5. The influence of privacy disclosure impact factors on the degree of privacy disclosure.

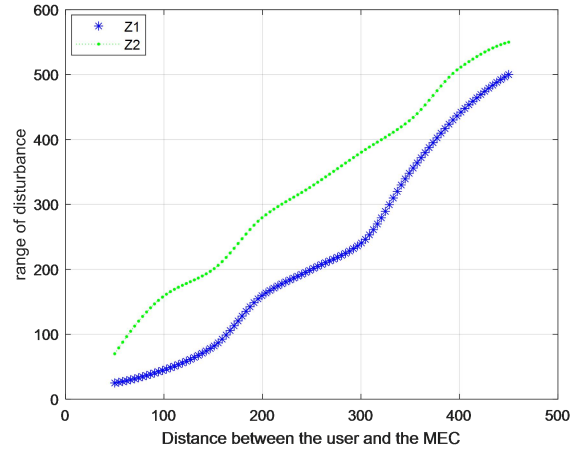


Fig. 6. The influence of distance on the range of disturbance.

Fig. 7 shows that the wireless channel condition deteriorates as the distance between the ground mobile user and the MEC server increases. This is mainly due to longer LoS transmission distance, higher path loss, and increased interference, which reduce transmission efficiency. To improve data security and privacy, the proposed scheme performs more computation locally, leading to a gradual increase in user computation cost.

Fig. 8 illustrates the relationship between user-server distance and privacy leakage. As the distance increases, privacy leakage first decreases and then becomes approximately linear. This occurs because the proposed scheme balances privacy protection and user cost by selecting an appropriate obfuscation distance. As the

difference between the actual and perturbed distances stabilizes, the probability of privacy leakage is reduced, ensuring secure data transmission.

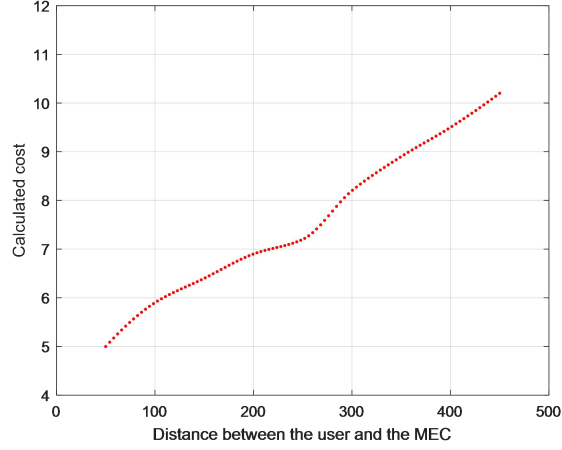


Fig. 7. Cost impact of distance between ground mobile users and edge computing server.

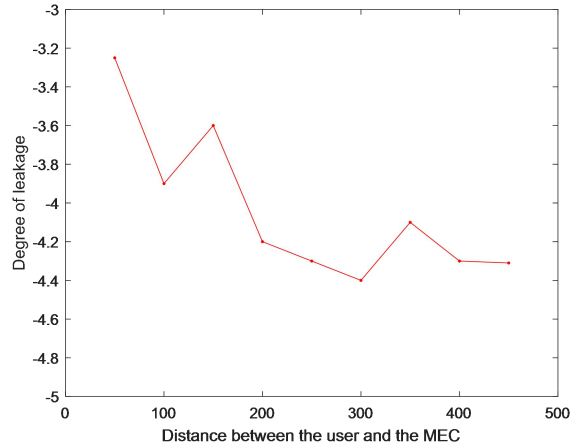


Fig. 8. The influence of distance between ground mobile users and mobile edge computing servers on the degree of user information privacy disclosure.

7 Conclusion

This paper studies secure task offloading in MEC systems under wireless environments with eavesdroppers and malicious attackers. We propose a task partitioning strategy that divides offloading tasks into smaller segments, enabling continuous processing while reducing latency and mitigating interception risks. A three-layer architecture is developed, including the ground layer, UAV-assisted edge cloud layer, and cloud layer.

UAVs equipped with MEC servers provide flexible edge computing support, while both legitimate users and potential eavesdroppers reside on the ground. To further enhance security, a distance perturbation mechanism is introduced to obfuscate user location information. By misleading adversaries and reducing information exposure, the proposed approach effectively improves the security and reliability of the task offloading process.

References

1. Zhang, G., Zhang, Q., et al.: Securing UAV communications via joint trajectory and power control. *IEEE Transactions on Wireless Communications* 18(2), 852–863 (2019)
2. Li, X., Wang, X., Wan, P.J., et al.: Hierarchical edge caching in device-to-device aided mobile networks: Modeling, optimization, and design. *IEEE Journal on Selected Areas in Communications* 36(8), 1768–1785 (2018)
3. Xu, K., Zhao, M.M., Cai, Y., et al.: Low-complexity joint power allocation and trajectory design for UAV-enabled secure communications with power splitting. *IEEE Transactions on Communications* 69(3), 1899–1913 (2021)
4. Jeong, S., Simeone, O., Kang, J.: Mobile edge computing via a UAV-mounted cloudlet: Optimization of bit allocation and path planning. *IEEE Transactions on Vehicular Technology* 67(3), 2049–2063 (2018)
5. Yang, W., Yang, et al.: Robust trajectory and communication design for multi-UAV enabled wireless networks in the presence of jammers. *IEEE Transactions on Communications* (to appear, 2024)
6. Li, Z., Chen, M., Pan, C., et al.: Joint trajectory and communication design for secure UAV networks. *IEEE Communications Letters* 23(4), 636–639 (2019)
7. Wang, Q., Chen, Z., Li, H., et al.: Joint power and trajectory design for physical-layer secrecy in the UAV-aided mobile relaying system. *IEEE Access* 6, 67603–67615 (2018)
8. Tran-Dinh, H., Vu, T.X., Chatzinotas, S., et al.: Coarse trajectory design for energy minimization in UAV-enabled wireless communications with latency constraints. *IEEE Transactions on Vehicular Technology* 69(9), 9483–9496 (2020)
9. Tran, D.H., Nguyen, V.D., Gautam, S., et al.: UAV relay-assisted emergency communications in IoT networks: Resource allocation and trajectory optimization. arXiv preprint arXiv:2008.00218 (2020)
10. Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M., Casey, W.: Decision and game theory for security. In: Alpcan, T., et al. (eds.) *Decision and Game Theory for Security*, LNCS, vol. 9996, pp. 1–13. Springer, Cham (2016)
11. He, X., Jin, R., Dai, H.: Physical-layer assisted secure offloading in mobile-edge computing. *IEEE Transactions on Wireless Communications* 19(10), 6777–6791 (2020)
12. Chen, Y., et al.: A comprehensive physical layer security mechanism for mobile edge computing. *IEEE Internet of Things Journal* 10(12), 10500–10513 (2023)
13. Wang, D., et al.: Double-edge computation offloading for secure integrated space-air-aqua networks. *IEEE Internet of Things Journal* 10(15), 13520–13534 (2023)
14. Jiang, G., et al.: Network security strategy based on cloud-edge collaboration in electric power internet of things. In: *Proc. 6th Int. Conf. Information Communication and Signal Processing (ICICSP 2023)*, pp. 1–6. IEEE (2023)
15. Ding, Y., et al.: Online edge learning offloading and resource management for UAV-assisted MEC secure communications. *IEEE Journal of Selected Topics in Signal Processing* 17(1), 54–65 (2023)

16. Zhao, T., Li, F., He, L.: DRL-based secure aggregation and resource orchestration in MEC-enabled hierarchical federated learning. *IEEE Internet of Things Journal* 10(18), 15890–15902 (2023)
17. Wang, Z., et al.: Location privacy-aware task offloading in mobile edge computing. *IEEE Transactions on Mobile Computing* (early access) (2023)
18. Samriya, J.K., Kumar, M., Gill, S.S.: Secured data offloading using reinforcement learning and Markov decision process in mobile edge computing. *International Journal of Network Management* 33(5), e2243 (2023)
19. Tang, Q., et al.: Secure aerial computing: Convergence of mobile edge computing and blockchain for UAV networks. *IEEE Transactions on Vehicular Technology* 71(11), 12073–12087 (2022)
20. Chen, N., et al.: When learning joins edge: Real-time proportional computation offloading via deep reinforcement learning. In: *Proc. IEEE 25th Int. Conf. Parallel and Distributed Systems (ICPADS 2019)*, pp. 1–8. IEEE (2019)