Hindawi
Journal of Function Spaces
Volume 2023, Article ID 9767396, 1 page
https://doi.org/10.1155/2023/9767396

Retraction

Retracted: Certificateless Batch Authentication Scheme and Intrusion Detection Model Based on the Mobile Edge Computing Technology NDN-IoT Environment

Journal of Function Spaces

Received 15 August 2023; Accepted 15 August 2023; Published 16 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Sun, "Certificateless Batch Authentication Scheme and Intrusion Detection Model Based on the Mobile Edge Computing Technology NDN-IoT Environment," *Journal of Function Spaces*, vol. 2022, Article ID 5926792, 9 pages, 2022.

Hindawi
Journal of Function Spaces
Volume 2022, Article ID 5926792, 9 pages
https://doi.org/10.1155/2022/5926792

Research Article

Certificateless Batch Authentication Scheme and Intrusion Detection Model Based on the Mobile Edge Computing Technology NDN-IoT Environment

Jianzhao Sun

School of Computer Engineering, Henan Institute of Economics and Trade, Zhengzhou 450018, China

Correspondence should be addressed to Jianzhao Sun; jzsun@henetc.edu.cn

Received 27 May 2022; Revised 5 July 2022; Accepted 8 July 2022; Published 22 July 2022

Academic Editor: Miaochao Chen

With the rapid development of mobile communication technology, the data transmission rate of mobile communication has been significantly improved and emerging Internet of things applications need a lot of computing resources to meet their own computing needs. However, the existing intelligent terminals have limited computing power and cannot meet the low-latency computing requirements with limited energy consumption. Mobile edge computing technology is considered to be one of the technical solutions that can efficiently solve this problem. Through mobile edge computing technology, intelligent terminals can actively divert some computing tasks to the computing servers deployed in edge network nodes and return the computing results to intelligent terminals after the edge computing servers have finished computing, thus greatly reducing the computing delay of users. In this paper, aiming at multiple edge server networks, combined with dual-connection technology, based on the research of a single edge computing server network, it is further extended to two edge computing servers and a joint optimization problem of computing task allocation and security performance requirements of intelligent terminals and edge computing servers is proposed, so as to minimize the global time delay for completing the computing tasks of intelligent terminals. By layering the problem, this paper proposes a corresponding algorithm, which can efficiently obtain the optimal solution of the initial problem. Compared with the linear search algorithm, the algorithm proposed in this paper can significantly reduce the computation time.

1. Introduction

With the wide application of the computer network and information confidentiality and authentication, network security and protection have attracted more and more attention from all walks of life. A password is a key technology in information security and plays a very important role in information security [1]. The certificateless signcryption scheme combines the advantages of certificateless cryptosystem and signcryption, which can not only complete the functions of signing and encrypting messages in the same logical step at a lower communication cost but also avoid the storage problem of the public key certificate in the public key infrastructure and the key escrow problem in the identity-based cryptosystem. Huge digital data are stored in computer databases and then transmitted between cumbersome communication networks. Without the protection of security technology, these data will be easily intercepted in the transmission process, which will lead to the leakage of secrets and the risk of data being extracted or copied in storage [2]. Cryptography is the key technology to ensure information security and network security and plays an important role in the field of information security.

Firstly, this paper deeply studies the mobile edge computing service deployment and information interaction mode in the multiterminal multi-intelligent base station environment and designs the system architecture and resource management algorithm based on multibase station cooperation.

The characteristics of all kinds of mobile terminal tasks are abstracted as ordered vectors, and the characteristics and signal transmission rate of each component of the system are quantified. The optimization problem of overall task processing delay is decomposed into two parts: calculating delay and transmission delay, which are modeled separately. The optimization algorithm based on the genetic algorithm is combined with the resource management algorithm based on multibase station cooperation. Further considering the scenario of multiple intelligent terminals and a single edge server, how does the edge server choose intelligent terminals to provide computing services with limited energy resources [3]? Aiming at the abovementioned problems, this paper proposes an accurate and effective algorithm to find the optimal intelligent terminal selection scheme and a large number of simulation results prove the accuracy of the proposed algorithm [4]. By layering the problem, this paper proposes a corresponding algorithm, which can efficiently obtain the optimal solution of the initial problem. Compared with the linear search algorithm, the algorithm proposed in this paper can significantly reduce the computation time.

Although the mobile edge computing technology has all the abovementioned advantages, due to the data transmission between the intelligent terminal and the edge server, it is necessary to jointly optimize the wireless resource allocation and computing resource allocation in order to obtain an effective computing diversion scheme. In view of the scarcity of wireless network resources and the problems of application efficiency, the importance of network resource allocation utility can be improved. Further solve the scenario limitations of existing wireless network resource allocation methods. On this basis, the general efficient wireless network resource allocation architecture adopts the utility-based resource allocation strategy algorithm, which has strong scenario adaptability and high utility. This paper further considers the security problems in edge computing while considering the uplink and downlink transmission and indirectly reflects the security degree of computing diversion data by quantifying the security overflow probability defined in the physical layer security. Through three scenarios, the amount of uploaded data, and energy distribution of intelligent terminals, the overall delay is divided into two parts: edge server processing delay and local computing delay, in which the server processing computing time is equal to the sum of uplink and downlink transmission delay and computing delay. By jointly optimizing the flow scheduling and energy distribution of intelligent terminals, the total delay consumed by intelligent terminals in completing computing tasks is minimized [5]. Although the joint optimization problem in this scenario is a nonconvex optimization problem, by exploring and utilizing the convex optimization characteristics of the energy allocation subproblem, this paper decomposes the joint optimization problem into the bottom-level problem and the top-level problem to be optimized and solved, respectively. Compared with the heuristic algorithm, the accuracy of the algorithm proposed in this paper is verified. Through a large number of data tests and simulations, the effectiveness of the algorithm proposed in this paper is verified.

2. Related Work

At present, the research on mobile edge computing is relatively scarce and mainly focuses on computing migration. However, it has been widely regarded as the development direction of mobile cloud services and has initially laid a foundation for the implementation of subsequent projects. The edge computing technology can not only reduce the computing delay of intelligent terminals and improve the utilization rate of resources but also meet the requirements of large-scale device access in the 5G era, and the business sinks to the edge to relieve the pressure of the core network [6].

Li et al. studied binary computing diversion of a single user in a random wireless channel. A decentralized binary computing distributary game method is proposed [7]. Zhao studied the joint optimization of multiuser binary computing diversion decision and resource optimization [8]. Zhu et al. studied the problem of maximizing the computing rate of binary computing with wireless power supply. This paper analyzes the energy delay dynamic shunting balance of mobile edge computing technology with energy collection devices and proposes an incentive compatible auction mechanism for resource transactions between mobile devices and cloud base stations to stimulate binary computing shunting [9]. Wen-He et al. proposed a strategic computing diversion algorithm based on the deep Q network, which is used to learn the optimal binary computing diversion strategy in a superdense network [10]. Chu and Leng used the dynamic voltage scale to study partial calculation shunt. An energy-efficient resource allocation scheme is proposed based on the edge calculation part to calculate the diversion. Considering the application with limited resources, the energy-saving part of wireless resources and computing resources is jointly optimized to calculate the shunting method, through wireless energy transmission [11]. Wang et al. proposed a joint optimization scheme of the edge computing system based on full-duplex relay wireless power supply and proposed a joint optimization method of energy consumption and delay based on fog computing [12]. Yang et al. put forward a strategy called PRIMAL, which selectively migrates computing tasks to their best location, considers the benefits and costs of migrating users' tasks to the appropriate mobile edge cloud according to their location, and optimizes the tradeoff between migration benefits and migration costs. However, this document designs a real-time model to calculate each computing task separately, which will bring a lot of overall task processing delay [13]. Li et al. introduced mobile edge computing into blockchain, taking edge computing as the network startup factor of mobile blockchain. Literature has exhausted the resource management and pricing of mobile edge computing to support the application of mobile blockchain. Among them, the mining process of miners can be migrated to edge computing service providers [14]. Alferaidi et al. have optimized the algorithm overhead. In order to reduce the transmission time of the program status on the system network, the mobile edge cloud is designed as a tree hierarchy of geographic distribution servers. Firstly, the scenario that each

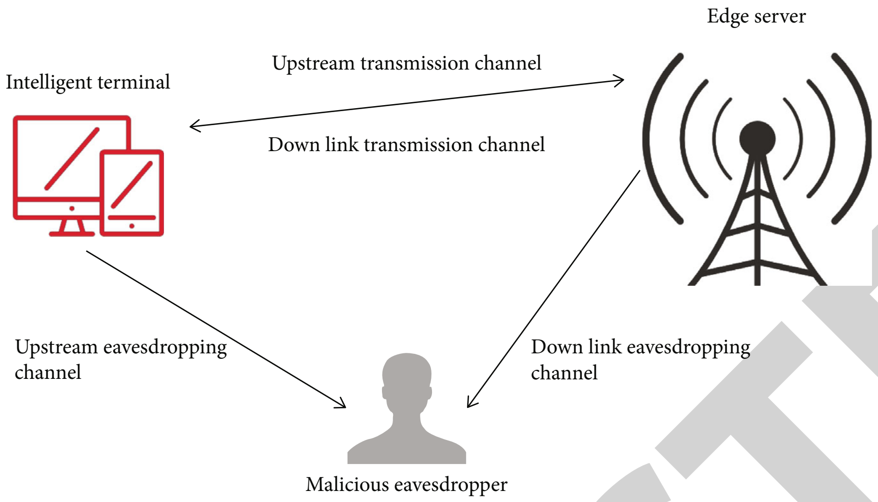
Edge server
Upstream transmission channel
Intelligent terminal
Down link transmission channel
Upstream eavesdropping channel
Down link eavesdropping channel
Malicious eavesdropper

Figure 1: Downlink transmission system model.

layer of the mobile edge cloud has only one server is considered, and then, the workload placement decisions of different mobile edge cloud servers are summarized together. At the same time, a workload allocation algorithm is proposed, which determines which mobile edge cloud service the mobile program is placed on and how much computing power is provided for it. However, despite the optimization of the algorithm overhead, the running process of these algorithms still needs to take up a certain amount of computing time for mobile applications. If large-scale user migration or large-scale computing tasks occur, the overhead of real-time algorithms will be one of the main obstacles to the development of delay-sensitive mobile applications [15]. Koo and Lim proposed an implementation scheme of block flow application, which can remotely retrieve the application from the server as required and run it locally on the Internet of things device. In particular, after investigation, it is found that the design of computing diversion based on edge computing is closely related to mobile data diversion based on the wireless network [16]. Song et al. put forward a method to find the best diversion strategy based on learning by using the energy collection system to supply power to data. The new paradigm based on Hong Jizhan double-join technology is applied to efficient data streaming [17]. Wang and Xu provide a scheme for data distribution in the Internet of vehicles to use edge computing servers for effective storage [18].

However, none of the abovementioned studies have considered the problems existing in wireless transmission. Based on this problem, this paper decomposes the joint optimization problem into the bottom-level problem and the top-level problem and optimizes them. Compared with the heuristic algorithm, the accuracy of the algorithm proposed in this paper is verified.

3. Multireceiver Signcryption without a Certificate

3.1. Bilinear Pair. A bilinear pair is also called bilinear mapping, and its predecessor is the Weil pair and Tate pair on the algebraic curve. They are mainly used in cryptography to attack the elliptic curve or hyperelliptic curve cryptosystems. It is mainly used to provide a higher access rate for users. Cooperative networking of base stations can not only increase the coverage of base stations but also facilitate the concentration of base station resources, thus serving more users. Double-connection technology mainly involves two different base stations covered by two different cells, macro cell and smaller cell [19]. The downlink transmission system model is shown in Figure 1.

The intelligent terminal uploads some computing tasks to the edge computing server for computing, and during the transmission, it is eavesdropped by a potential malicious eavesdropper. Dual connection (DC) means that the mobile phone can simultaneously use the wireless resources of at least two different base stations (divided into the master station and slave station) in the connected state. The dual connection introduces the concept of “shunting bearer,” that is, the data is shunted to two base stations at the PDCP layer. The PDCP layer of the master station user interface is responsible for PDU numbering, data shunting, and aggregation between master and slave stations. Through the dual-connection technology, the intelligent terminal can transmit data with Hong Jizhan and a small base station at the same time, so it is particularly important to divide the data between Hong Jizhan and a small base station reasonably according to its own location, channel condition, and security performance requirements [20].

According to the principle of physical layer security, the security throughput that the terminal can upload to the edge server is shown in formula (1).

$$C_{iB}^{\mathrm{sec}} = \left(W_b \log_2 \left(2 \frac{p_{ib} g_{ib}}{n_b} \right) - W_B \log_2 \left(2 \frac{p_{ib} g_{iE}}{n_E} \right) \right). \quad (1)$$

W_B is the bandwidth of the edge server, and p_{ib} represents the channel gain from the intelligent terminal to the edge server and eavesdropper. Because of the randomness

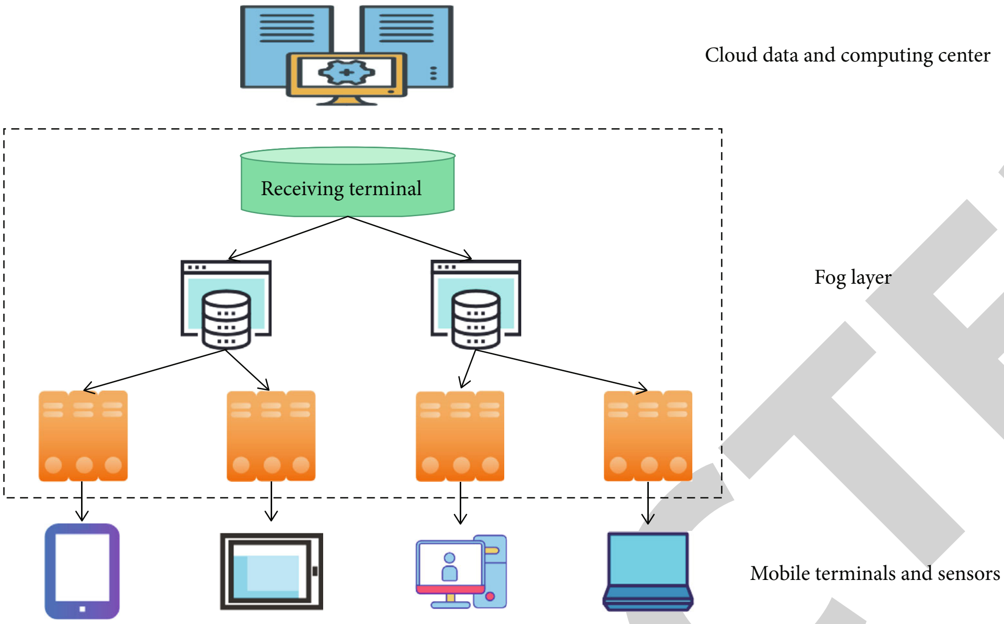

Figure 2: Schematic diagram of the fog computing structure.

and uncertainty of the eavesdropper's location, we cannot get the exact value of its channel gain. Assuming that the channel gain from the intelligent terminal to the eavesdropper obeys the exponential distribution with a constant mean value and given a fixed shunting rate from the intelligent terminal to the eavesdropper, the throughput of uplink transmission can be obtained as shown in formula (2).

$$x_{iB} = W_B \log_2\left(1 - \frac{p_{ib}}{g_{ib}}\left(1 + e^{g_{ib}/g_{ie}}\right)\right),$$
$$P_{\text{out}} = pr\left\{\left(x_{iB} \middle| W_B \log_2\right)\left(1 - \frac{p_{ib}}{g_{ib}}\right) + W_B \log_2\left(1 + \frac{p_{ib}}{g_{iE}}\right)\right\}. \tag{2}$$

There are two key parameters in the abovementioned formula, one is the security overflow probability of intelligent terminal, and the other is the strength of the eavesdropping channel. With the increase of throughput, the overflow probability decreases, which means that it is a relatively relaxed security protection environment. The security overflow probability of intelligent terminals increases with the decrease of overflow probability, which means that the ability to withstand eavesdropping is stronger at this time [21]. The time taken to upload the computing task to the edge server in this paper represents the uploading speed of the intelligent terminal, as shown in formula (3).

$$P_{iB} = \frac{x_{iB}\left(1 + c_{ib}\right)t_i}{g_{ib} - 2W_B\left(1 - c_{ib}\right)}. \tag{3}$$

After calculating the task distributed by the intelligent terminal, the edge server returns the calculation result to the intelligent terminal. In this model, it is assumed that the intelligent terminal will compress the data of the calculation task. In this model, the downstream security throughput can be expressed as shown in formula (4).

$$C_{Bi}^{\text{sec}} = \left(W_B \log_2\left(1 + \frac{p_{ib}}{g_{ib}}\right)\right). \tag{4}$$

We set the safe overflow probability as shown in formula (5).

$$x_{Bi} = W_B \log_2\left(1 - \left(1 - e^{g_{ib}/\alpha_{\text{sec}}}\right)\left(1 + \alpha_{\text{sec}}\right)\right). \tag{5}$$

Next, this paper models the global delay of the intelligent terminal. The overall time includes two parts: calculation delay and transmission delay. The downlink transmission power of the edge server is shown in formula (6).

$$P_{Bi} = \frac{n_E 2^{s_i n^E / W_B}}{G_{B_i} - n_E 2^{s_i n^E / W_B}}. \tag{6}$$

3.2. Fog Computing and Cloud Computing. Mobile edge computing allows the data needed by mobile terminal computing tasks to be processed at the edge of the mobile network without further migration to mobile cloud. The components of the mobile edge network mainly include the following: mobile terminal equipment, mobile edge equipment, mobile edge computing server, and mobile edge computing intelligent base station. These components need to have corresponding computing power and storage capacity to support mobile edge computing. In a word, mobile edge computing does not need the active assistance service of the cloud and it focuses more energy on the edge of mobile cloud. Mobile cloud integrates all the advantages of mobile computing, cloud computing, and mobile Internet, while mobile cloud can provide corresponding resources for mobile terminals according to their needs. In the MCC infrastructure, the centralized cloud server cluster is far away from the mobile terminal equipment, so the computing efficiency of MCC is low in the environment with high computing pressure. Fog computing can support most common connection devices on the market [22]. The structure diagram of fog computing is shown in Figure 2.

Fog computing is characterized by its distributed architecture, in which data are collected and processed by distributed fog computing devices from different sensors. Compared with cloud computing far away from mobile terminal users, fog computing greatly reduces system latency. However, FOG computing has certain limitations because of its dependence on wireless connection. In order to ensure the execution of complex operations, wireless connection has high requirements for real time. However, in the mobile edge computing environment, the intelligent computing, communication capability, and data processing capability are node based, rather than the hierarchical network of fog computing, so the development trend of mobile edge computing in 4G and future 5G networks is on the rise. The radio resources in MEC resource management mainly include power and subchannels. The power refers to the uplink transmission power of the terminal equipment when the user unloads the task data. The uplink transmission energy consumption is calculated as the product of uplink transmission power and uplink transmission delay, and the uplink transmission delay is also affected by uplink transmission power, so the uplink transmission power affects the uplink transmission energy consumption. Subchannels are obtained by evenly dividing the system bandwidth, which can be understood as different frequency bands. The bandwidth of the subchannel affects the uplink transmission rate and then affects the uplink transmission delay and the uplink transmission energy consumption. In addition, when considering the MEC system with multiple base stations, intercell interference should be considered, that is, users occupying the same subchannel in different cells will interfere with each other. Interference will reduce the uplink transmission rate and increase the transmission delay and energy consumption. Therefore, it is necessary to allocate channels reasonably for users and reduce intercell interference.

3.3. Security Model. The mobile edge computing intelligent base station proposed in this paper has both computing function and storage function, so the intelligent base station needs to schedule computing tasks and data caching tasks according to the current situation of each mobile terminal and its own service. If the control unit receives a computing task request, the function of the control unit is to determine the execution location of the computing task. If the control unit receives the data request required by the task, the function of the control unit is to determine whether the data needs to be cached and where it is cached. In the certificateless cryptosystem, adversaries are divided into type 1 and type 2. According to the types of adversaries, confidentiality and unforgeability games are divided into two types. Therefore, the function of the computing unit is to calculate the computing tasks requested by some mobile terminals covered by the mobile edge computing intelligent base station according to each collaborative resource management algorithm, so as to reduce the pressure of computing load in the mobile cloud. In this paper, the global enumeration method is used to solve the original problem type 1. The computing speed of the intelligent terminal is 120 Mbps, the upper limit of energy consumption is 4 J, the compression rate is 0.25, and the computing power consumption and the computing power consumption of the server are both 0.1.

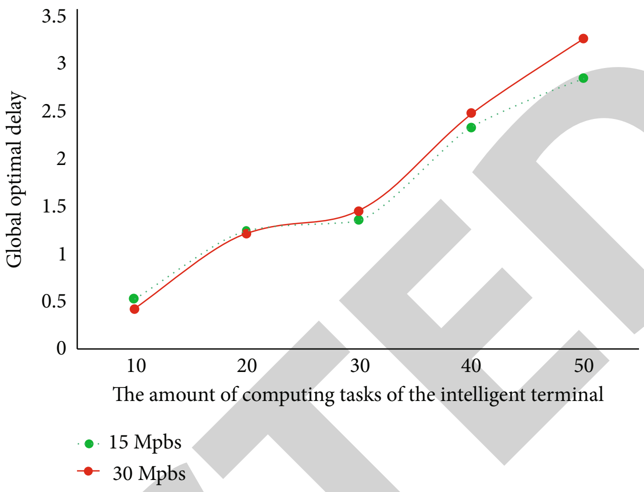

Figure 3: Ratio of global optimal delay.

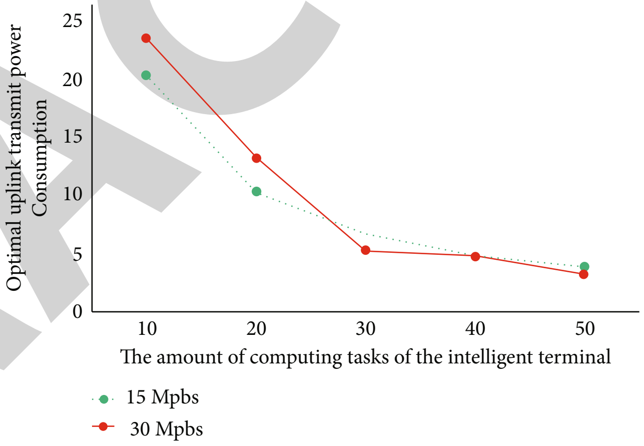

Figure 4: Optimal uplink transmission power consumption.

3.3.1. Simultaneous Comparison. When the local computing speed of the server is different (15 Mpbs and 30 Mpbs), the minimum transmission delay solved by the global enumeration algorithm is shown in Figures 3 and 4.

The comparison is about the optimal uplink transmission power and the change under different calculation tasks. All the abovementioned results show the consistency between our proposed algorithm and enumeration method, which also shows the accuracy of this algorithm from the side. In order to model the problem, this paper considers

Table 1: Comparison of this scheme with other schemes.

Program	The time of the signcryption process (ms)	The time of the decryption process (ms)
A bilinear pairing operation	$29.63n + 99.425$	232.428
A dot multiplication operation on intrusion detection	$15.62n + 99.384$	$83.86n + 180.362$
Addition operation on an intrusion detection	$23.66n + 88.241$	135.328
An exponentiation on intrusion detection	$26.25n + 76.634$	134.248
Scheme of this paper	$4.26n + 61.265$	118.823

introducing a binary variable to indicate whether the server selects the intelligent terminal for access. In this paper, the problem of maximizing edge server revenue represents the total transmission delay of all intelligent terminals, including uplink transmission delay and downlink transmission delay. The purpose of this problem is to solve the problem of maximizing revenue by reasonably selecting users' access under the limitation of time slot and energy consumption. The efficiency of this scheme is compared with other proposed certificateless multireceiver signcryption schemes, and the comparison results are shown in Table 1.

In the actual network transmission, the communication between devices is very complicated and different intelligent terminals have different security requirements and different energy consumption restrictions, which lead to different data splitting strategies for computing tasks. Because of the coexistence of edge computing technology and dual-connection technology, the resource allocation between the intelligent terminal and a single edge server becomes the resource allocation among multiple computing members, which further increases the difficulty coefficient of the already complicated problems, so it is even more necessary for this paper to allocate computing resources reasonably.

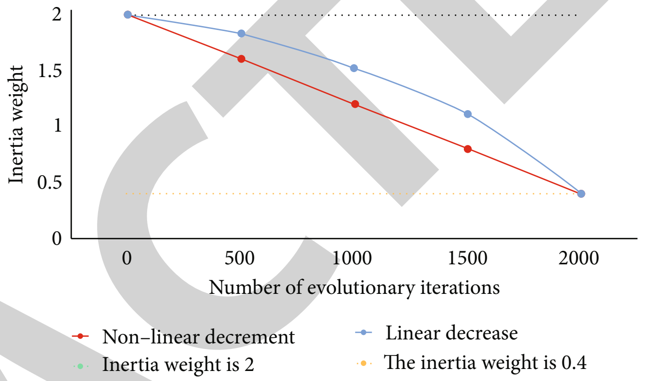

Figure 5: Scheme changes of different inertia weights.

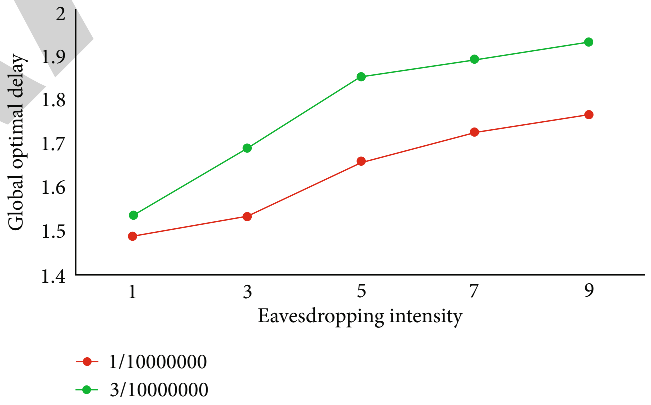

Figure 6: Influence of eavesdropping intensity on global optimal transmission delay.

4. Simulation and Result Analysis

4.1. Unloading Decision Subproblem Analysis. Before the closed expression of the power optimization strategy and computing resource allocation is obtained, this paper adopts the particle swarm optimization algorithm to optimize by iterative search and defines fitness function to evaluate the solution. The algorithm starts iterative search from an initialized population, which contains several particles, and each particle has three attributes, namely position, speed, and fitness value. The position coordinate of each particle is a candidate solution of the problem to be solved, while the velocity of the particle controls the update of the particle position, and the fitness value is used to evaluate the solution. After many iterations, the optimal solution corresponding to the optimal position of all particles is found. The setting of inertia weight plays a key role in the performance of the algorithm. Each particle converges according to its updated speed. When the inertia weight is set larger, the algorithm has better global search ability but the convergence speed will slow down. If the inertia weight is set smaller, the algorithm will have stronger local search ability but this will also lead to the search easily falling into local optimum. The inertia weight of the particle swarm optimization algorithm is closely related to the size of population, spatial dimension, and the decline rate of inertia weight. Through the experimental study of several representative functions, the results show that properly changing the inertia weight can quickly converge, improve the search efficiency, and avoid falling into local optimization. In order to coordinate the ability of global search and local search, this paper uses the nonlinear decreasing adaptive inertia weight scheme and its formula is shown in (7).

$$w(t) = \frac{w_{\text{start}}}{t} - (w_{\text{end}} - w_{\text{start}}). \tag{7}$$

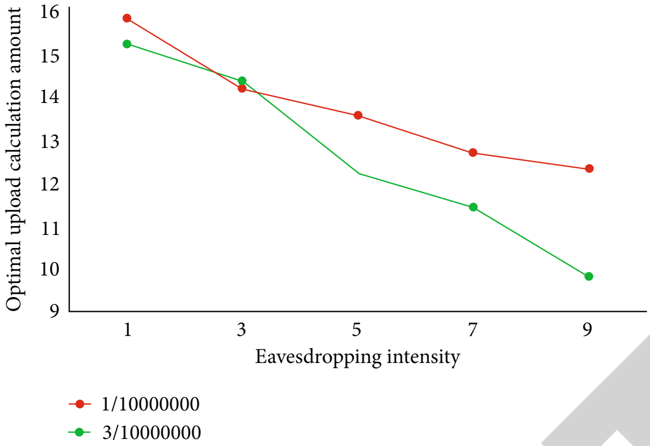

Figure 7: Influence of the change of eavesdropping intensity on the optimal upload calculation.

t represents the current evolution algebra, and w_{start} and w_{end} represent the maximum and minimum inertia weight, respectively.

Inertia weight decreases with the increase of evolution points and decreases slowly in the early stage of iteration and rapidly in the late stage of iteration. This makes the algorithm have a large inertia weight in the early stage of iteration to enhance the global search ability, while in the late stage of iteration, the inertia weight is small and the local search ability is enhanced, which improves the search accuracy and accelerates the convergence speed. As shown in Figure 5.

It can be seen in Figure 5 that the unloading decision variables are binary variables from 0 to 1, so this paper uses the binary particle swarm optimization algorithm to solve the problem, when the global optimal delay decreases and the calculation amount of optimal upload increases. The abovementioned results are reasonable. When the intelligent terminal's own security performance is relatively loose, the intelligent terminal can upload more workload to the server by taking advantage of computing split, and then, the overall optimal delay will decrease.

4.2. Optimal Diversion Scheme for Multiuser Scenarios. Edge computing is a computing facility that deploys data resources outside the data center and close to users. Through this facility, a series of network devices link edge computing devices to users or processes, such as the Internet of things. Therefore, the deployment of edge computing devices does not have the physical security of the data center and cannot adopt the access, network, and data security measures applied by the software or hardware residing therein. The security challenge of edge computing is to provide the additional security required to make the security of edge computing facilities meet the security and compliance of data center standards. In many cases, this means that it is necessary to securely access edge computing devices. Whether it is physical access or through the user interface, some key security measures must be taken. For each intelligent terminal, the binary particle swarm optimization algorithm can be used to solve its optimal security computing diversion strategy. In this section, from the point of view of the edge computing server, this paper mainly studies how the edge computing server selects the access of an intelligent terminal under limited computing resources and a certain time limit and makes use of the edge server to maximize its own revenue under the condition of limited channel time slots and limited energy consumption for transmission and computation.

In order to maximize the revenue, this section will study the influence of eavesdropping intensity on the optimal diversion scheme, setting the eavesdropping intensity at 0.2, and changing it within the interval $[10^{-7}, 9 \times 10^{-7}]$ to verify the minimum transmission delay and the influence of the optimal diversion scheme. By using the method of comparative analysis, two datasets are set as 10^{-7} and 3×10^{-7}. The comparison results are shown in Figure 6.

It can be observed in Figures 6 and 7 that when the eavesdropper's eavesdropping intensity on the user increases, the global optimal transmission delay increases, while the optimal upload workload decreases. This result is reasonable, because as the channel strength of the eavesdropper to the user increases, it means that the eavesdropper's eavesdropping ability is increasing. At this time, the environment in which the intelligent terminal is located is unsafe, so the calculation workload of uploading should be reduced and the risk of being eavesdropped should be lowered. Therefore, the optimal uploading workload is decreasing, which leads to the increase of the delay of the intelligent terminal.

Through qualitative analysis, this paper proposes a joint intelligent terminal computing task splitting, wireless resource allocation (including time delay and energy consumption), and security overflow probability to minimize the overall time delay of the system. The main goal of this paper is to minimize the overall time delay (including transmission time delay and calculation time delay) under the limited energy consumption budget while completing the computing task of the intelligent terminal and meeting the security requirements of the intelligent terminal. Based on the consideration of eavesdropping, this paper also puts forward the concept of overflow probability, that is, the transmission rate of the intelligent terminal when actually distributing data is less than the probability that the intelligent terminal allocates the data transmission rate to the edge server. Finally, by comparing various situations of each layer, we can find the global optimal solution and finally solve the initial optimization problem. Finally, the accuracy of this algorithm is verified by comparing with other heuristic algorithms.

5. Conclusions

Traditional intrusion detection systems have some problems in the detection algorithm and decision-making control mechanism. In the field of game theory, there are already a set of mature theories and methods to solve the problem of competition and mutual influence among people with different goals in the same system. These methods have been successfully applied in many fields such as political economy, decision theory, and control theory.

In order to improve the accuracy of the intrusion detection system, it is necessary to analyze the attacks on network layer routing, data link layer, transport layer, and application layer and the layers need to cooperate with each other. Based on the mobile edge computing technology, this paper puts forward the security computing diversion strategy in two scenarios and obtains a series of research results. A multireceiver cryptosystem can send the same ciphertext to multiple receivers, which is more efficient than encrypting the same message and then sending the ciphertext to the corresponding receivers. Firstly, this paper combines the advantages of a multireceiver cryptosystem and signcryption cryptosystem and constructs a certificateless multireceiver signcryption scheme, which realizes that each independent receiver in the designated multireceiver can recover the message.

This paper still has some limitations. Because of the complexity of network information, it is difficult to determine the parameters in the revenue function. How to combine the fuzzy game theory with fuzzy control and multiobjective evaluation methods to improve the accuracy of the intrusion detection decision control model is also the next task to improve the intrusion detection system based on the game theory.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by the Science and Technology Project of Henan Province: innovative application of big data in the field of industrial digital upgrading (no. 222102210338).

References

[1] G. Thumbur, N. B. Gayathri, P. V. Reddy, M. Z. U. Rahman, and A.'. Lay-Ekuakille, “Efficient pairing-free identity-based ADS-B authentication scheme with batch verification,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 5, pp. 2473–2486, 2019.

[2] S. Shamshad, M. Rana, K. Mahmood, M. K. Khan, and M. S. Obaidat, “On the security of a secure anonymous identity-based scheme in new authentication architecture for mobile edge computing,” *Wireless Personal Communications*, vol. 124, no. 1, pp. 283–292, 2022.

[3] W. Liu, J. Song, H. Wu et al., “Non-crypto authentication for smart grid based on edge computing,” *Journal of Physics: Conference Series*, vol. 1646, no. 1, article 012060, 2020.

[4] F. J. Mora-Gimeno, H. Mora-Mora, D. Marcos-Jorquera, and B. Volckaert, “A secure multi-tier mobile edge computing model for data processing offloading based on degree of trust,” *Sensors (Basel, Switzerland)*, vol. 1, no. 4, pp. 58–66, 2018.

[5] C. C. Lee, “ES-HAS: ECC-based secure handover authentication scheme for roaming mobile user in global mobility networks,” *Cryptography*, vol. 5, no. 4, p. 35, 2021.

[6] H. Huang, Y. Wu, F. Xiao, and R. Malekian, “An efficient signature scheme based on mobile edge computing in the NDN-IoT environment,” *IEEE Transactions on Computational Social Systems*, vol. 8, no. 1, pp. 1108–1120, 2021.

[7] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, “Information security model of block chain based on intrusion sensing in the IoT environment,” *Cluster Computing*, vol. 22, no. 1, pp. 451–468, 2019.

[8] J. Zhao, “Research on intrusion detection system based on joint mobile agent technology in cloud computing environment,” *Automation & Instrumentation*, vol. 8, no. 2, pp. 46–55, 2017.

[9] X. Zhu, H. Xu, Z. Zhao et al., “An environmental intrusion detection technology based on WiFi,” *Wireless Personal Communications*, vol. 119, no. 2, pp. 1425–1436, 2021.

[10] M. Zhong, Y. Zhou, and G. Chen, “Sequential model based intrusion detection system for IoT servers using deep learning methods,” *Sensors*, vol. 21, no. 4, article 1113, 2021.

[11] X. Chu and Z. Leng, “Multiuser computing offload algorithm based on mobile edge computing in the Internet of things environment,” *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 6107893, 9 pages, 2022.

[12] X. Wang, X. Wang, and Y. Li, “NDN-based IoT with edge computing,” *Future Generation Computer Systems*, vol. 115, no. 2, pp. 397–405, 2021.

[13] Y. C. Yang, F. Ali, and S. Nazir, “Selection of devices based on multicriteria for mobile data in Internet of things environment,” *Mobile Information Systems*, vol. 2021, Article ID 2117915, 7 pages, 2021.

[14] J. Li, X. Li, G. Li, and R. Zhang, “Non-cooperative game forwarding leveraging user trustworthiness in mobile edge networks,” *Sustainability*, vol. 14, no. 8, p. 4473, 2022.

[15] A. Alferaidi, K. Yadav, Y. Alharbi et al., “Distributed deep CNN-LSTM model for intrusion detection method in IoT-based vehicles,” *Mathematical Problems in Engineering*, vol. 2022, 8 pages, 2022.

[16] S. Koo and Y. Lim, “A multi-objective computation offloading algorithm for dependent tasks based on a mobile edge

computing environment," *KIISE Transactions on Computing Practices*, vol. 27, no. 2, pp. 122–127, 2021.

[17] C. Song, M. Y. Zhang, W. P. Peng, Z. Jia, Z. Liu, and X. Yan, "Research on pairing-free certificateless batch anonymous authentication scheme for VANET," *Journal on Communications*, vol. 3, no. 2, pp. 49–55, 2017.

[18] L. Wang and Z. Xu, "An English learning system based on mobile edge computing constructs a wireless distance teaching environment," *Mobile Information Systems*, vol. 2021, Article ID 2718859, 9 pages, 2021.

[19] I. A. Kamil and S. O. Ogundoyin, "A lightweight certificateless authentication scheme and group key agreement with dynamic updating mechanism for LTE-V-based Internet of vehicles in smart cities," *Journal of Information Security and Applications*, vol. 63, article 102994, 2021.

[20] C. Jiang, C. Huang, Q. Huang, and J. Shi, "A multi-source big data security system of power monitoring network based on adaptive combined public key algorithm," *Symmetry*, vol. 13, no. 9, article 1718, 2021.

[21] S. W. Park and I. Y. Lee, "Mutual authentication scheme based on lattice for NFC-PCM payment service environment," *International Journal of Distributed Sensor Networks*, vol. 12, no. 7, Article ID 9471539, 2016.

[22] K.-H. Yeh, "A secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments," *IEEE Systems Journal*, vol. 12, no. 2, pp. 2027–2038, 2018.