IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 3 February 2024, accepted 10 March 2024, date of publication 18 March 2024, date of current version 22 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3377102

RESEARCH ARTICLE

P²SPA: Privacy Preservation Strategy With Pseudo-Addresses for Edge Computing Networks

JIAYUAN DU, GUOWEI ZHANG, XIAOWEI YUAN, AND XIAODONG ZANG
School of Cyber Science and Engineering, Qufu Normal University, Qufu 273165, China

Corresponding author: Guowei Zhang (zhanggw@qfnu.edu.cn)

This work was supported by the Natural Science Foundation of Shandong Province under Grant ZR2021QF090.

ABSTRACT In recent years, edge computing networks have been widely adopted to achieve low latency, save bandwidth, and improve flexibility. However, most of the current Edge Nodes (ENs) are in semi-trusted or untrusted environments, where interactions among users are unsafe. Therefore, providing cost-effective protection strategies for ENs under resource limitations remains a great challenge. To cope with this, we propose an edge computing model with "End-Edge-Cloud" collaborative services, and a Privacy Preservation Strategy with Pseudo-Addresses (P²SPA) is constructed to maximize the cost-effectiveness while protecting the location privacy of the ENs. We quantify the privacy protection preference of user information using the Analytic Hierarchy Process (AHP) to select the optimal EN. Considering the dynamic change in the attack frequency, a pseudo-address selection and updating strategy is constructed based on the Stackelberg game theory; thus, the optimal pseudo-address update frequency is achieved. Numerical estimations are performed to verify the effectiveness of the proposed P²SPA strategy. Compared with the existing methods, P²SPA achieves a compromise service strategy with satisfactory performance on both the defense effect and defense cost.

INDEX TERMS Edge computing, privacy protection, mobile target defense, pseudo-address, Stackelberg game.

I. INTRODUCTION

In recent years, the rapid expansion of mobile internet technology has led to a rapid increase in the number of mobile devices worldwide. As a consequence, users expect higher standards for network performance [1]. Despite the significant computational capabilities of cloud computing, it often fails to meet user demands for data transmission rates, latency, and overall service quality [2]. Consequently, Mobile Edge Computing (MEC) has emerged as a solution [3]. MEC repositions computing and storage resources from centralized clouds to the edges of networks. This shift enables more efficient handling of tasks that demand high computing power and minimal latency [4], [5], especially in applications such as the Internet of Vehicles (IoV) [6] and the smart cities [7]. Unlike cloud computing, MEC places strong emphasis on collaborative resource usage among edge devices [8]. However, this relocation of resources also exposes Edge Nodes (ENs) to increased risks, particularly in environments that are only partially trusted or potentially malicious [9]. For instance, adversaries might impersonate genuine users in an attempt to gain unauthorized access, a strategy recognized as identity spoofing attacks. They may also endeavor to infiltrate ENs for the purpose of acquiring sensitive information, disrupting system operations, or assuming control of devices—an attack category known as malware injection. Moreover, there could be endeavors to overload ENs, resulting in service unavailability and impacting overall system availability; this is commonly labeled as a DDoS attack. Nevertheless, numerous ENs currently rely on static

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed M. Elmisery.

and passive security measures [10], such as firewalls [11], intrusion detection systems [12], and DDoS attack detection [13].

The widespread adoption of 5G technology has significantly enhanced ENs by offering greater bandwidth, lower latency, and reduced energy consumption [14], [15]. To transition from passive to active defense strategies, Moving Target Defense (MTD) has emerged as a primary focus of research [16]. MTD involves continuous random alterations to the system configurations, deliberately creating an environment of uncertainty for potential network adversaries [17]. This proactive approach aims to thwart attacks by constantly changing their surface. The rapid evolution of network communication technology has expanded the potential applications of MTD [18]. Research on MTD has primarily focused on two categories: Software-Defined Networks (SDN) and virtual IP address technology [19]. This approach involves frequent alterations to the network attack surface, offering improved defense effectiveness but increased costs. Hence, identifying the optimal transition frequency, while ensuring robust protection for ENs, is crucial. To maximize benefits within resource limitations, studies have sought equilibrium points using game models. For example, Li et al. [20] introduced a Stackelberg game model involving multiple leaders and followers. This model aim to identify an equilibrium solution for resource allocation within the network slicing. Such models play a vital role in determining the optimal resource allocation strategies while considering various stakeholders in the network environment.

In the face of dynamically changing attack frequencies, to achieve economically efficient protection, we introduce a lightweight Privacy Preservation Strategy with Pseudo-Addresses (P^2SPA). This strategy aims to identify the most cost-effective protection solution while ensuring the security of ENs. The primary contributions of our study can be summarized as follows:

1) To maximize the utilization of limited protection resources for ENs, we have designed an algorithm based on the Analytic Hierarchy Process (AHP). This algorithm enables the optimal offloading of tasks by considering protection preferences, effectively reducing overhead during the task offloading process while ensuring the desired protection outcome.

2) Considering the need to minimize interactions with non-trusted entities for ENs, we introduce continuously updated pseudo-addresses as relay nodes. Based on the Stackelberg game model, we have designed a pseudo-address updating algorithm to determine the optimal update frequency. This significantly reduces the additional overhead generated by pseudo-address updates, while ensuring an effective protection outcome. It represents a cost-effective strategy for safeguarding edge nodes.

3) To demonstrate the performance of the proposed P^2SPA scheme, we conducted a comprehensive theoretical analysis and performance evaluation encompassing privacy protection efficacy, security overhead, and other pertinent characteristics. The evaluative findings indicate that the P^2SPA scheme surpasses the existing solutions in terms of both cost-effectiveness and robustness.

The remainder of this paper is organized as follows. Section II introduces the related researches and their limitations, and Section III provides the problem statement. Section IV describes the solution and implementation of the proposed system model. Section V presents numerical simulation results and analyses. Finally, Section VI concludes the paper and presents the potential research directions.

II. RELATED WORK

To address the limitations associated with passive defense dependency, latency, and high overhead, several schemes [21], [22], [23], [24], [25], [26] have shifted their focus towards active defense research. For instance, Seo et al. [21] have presented an active moving target defense strategy for Unmanned Aerial Vehicles (UAVs) utilizing a Partially Observable Markov Decision Process (POMDP) threat model. This model considers the sequence of operations both inside and outside the UAV, raising attack costs and latency. However, this approach exhibits limited generalizability. In a different approach, Xu et al. [22] ensure the reliability of transmission channels by introducing a key. They employ a cooperative jamming scheme, imposing superimposed channel measurements on repeaters and potential eavesdroppers, effectively safeguarding transmitted data. Nevertheless, this method does not extend protection to the privacy of the edge nodes themselves. Furthermore, to safeguard node privacy, Tan et al. [23] proposed a topology spoofing scheme. This approach reduces the risk of critical UAVs being identified by deploying spoofing nodes to extend scanning time and increase the attacker's cost. Although effective in protecting critical nodes, it introduces substantial overhead. Xing et al. [24] introduced a double k-anonymity based location privacy protection method. This approach conceals user location and request information, offering extensive protection for user location privacy. However, it comes with significant overhead. The widespread application of deep learning algorithms has also propelled advancements in active defense. Specifically, Liu et al. [25] achieved diverse distributed task migration through a counterfactual multi-agent (COMA) reinforcement learning approach. While enhancing the Quality of Service (QoS), this method prioritizes minimizing latency but does not explicitly address the protection of privacy information. Wu et al. [26] proposed a method to enhance privacy in video streaming through secure reversible transformation based on GAN networks (PECAM). This approach removes some visual details without compromising user feature accuracy, thereby enhancing the security of user feature privacy. However, it is associated with high overhead and may not be applicable in resource-constrained contexts.

With the rapid evolution of information technology, the landscape of network attacks is progressively diversifying.

Owing to the temporal and cost-related asymmetry between attackers and defenders, cyberspace finds itself in a security predicament characterized as ''easy to attack but difficult to defend''. Consequently, the emerging Moving Target Defense (MTD) technology has garnered significant attention from both domestic and international researchers, serving as a revolutionary approach to address the current disadvantageous position of defenders. Various schemes [27], [28], [29], [30], [31] leverage sophisticated technologies, such as Software-Defined Networks (SDN) and network address transformation, to implement MTD strategies. Specifically, Meneses et al. [27]employs SDN to manage end-to-end traffic, significantly elevating the cost for potential attackers. However, its applicability is primarily confined to specific scenarios with ample resources, such as cloud computing. Other methodologies involve the randomization of IP addresses across nodes, as demonstrated by Chang [28] and collaborators, who randomized IP addresses for MTD. They also synchronized IP addresses between nodes in a networked path using hash-chain-based synchronization signatures. However, these methods have proven insufficiently effective in defending against a broad spectrum of attack scenarios. Yungaicela-Naula et al. [29] proposed an SDN-based security framework that autonomously monitors, detects, and mitigates slow DDoS attacks. Simulation results demonstrate the framework's effectiveness in mitigating malicious connections and defending against multiple slow DDoS attacks with varying numbers of attackers and victims. Nevertheless, it exhibits limitations when confronted with other forms of attacks. Yoon et al. [30] developed an attack graph-based MTD technique that updates a host's network configuration (e.g., MAC/IP/port address) based on the host's criticality. This approach aims to minimize the probability of attack success with minimal MTD cost, yet it prioritizes critical hosts that are more susceptible to attack, falling slightly short in terms of dynamism. Jafarian et al. [31] enhance defense levels by determining a range of virtual IP addresses through low-frequency hops and selecting IP addresses through high-frequency hops. However, this approach introduces a significant overhead.

Through the aforementioned studies, it is evident that achieving a balance between protection effectiveness and cost in MEC privacy protection poses a significant challenge. In response to this challenge, some methodologies [32], [33], [34], [35], [36], [37] employ game-theoretic approaches to identify equilibrium solutions. In the domain of car charging scheduling, Zhang et al. [32] introduce a fully distributed multi-intelligence deep reinforcement learning method based on Stackelberg game. This approach not only addresses privacy and communication concerns but also significantly enhances computational efficiency and scalability. For pricing and allocation decisions, Xie et al. [33] model the interactions between providers and customers, analyzing Nash equilibria involving uniform and differential pricing strategies using a game. This enables dynamic price adjustments for individual customers and resolves transmission congestion issues. In market competition scenarios, De Silva et al. [34] utilize the Stackelberg duopoly model to maximize market share. Their study of two competing firms aims to determine conditions for ''winner-take-all'' competition by characterizing strong/weak Nash equilibria in the game. Games have also found widespread application in task offloading. Liu et al. [35] devised an offloading method to minimize expenditures in MEC while maximizing cloud revenue and minimizing user costs. Meanwhile, Gao et al. [36] constructed an online framework to balance access latency, communication latency, and service exchange costs through a game and service switching costs to enhance QoS cost-effectively. Wu et al. [37] propose a management operation framework, HiTDL, to make globally throughput-optimal resource allocation decisions by solving a fairness-aware multi-choice knapsack problem. In summary, games have demonstrated efficacy in addressing trade-off problems when node resources are limited. Consequently, in this paper, we integrate the game model with MTD to determine the optimal pseudo-address updating frequency. This integration allows us to strike a balance between protection effectiveness and cost when the attack frequency dynamically changes.

III. PROBLEM STATEMENT

In this section, we formally define the system model, design goals and initialization settings.

A. SYSTEM MODEL

The system model is shown in Fig. 1, and consists of request users, a cloud server, edge servers, a pseudo-address generator, and edge computing nodes. Important variable symbols and their meanings in the system model are listed in Table 1.

Cloud Server (CS): A CS is a trusted entity with powerful computing and storage capabilities. It can receive, allocate, and compute task information from requesting users.

Edge Servers (ES): ES has the capability to locally process task information received from the CS or offload it to edge computing nodes. It is noteworthy that ES can perform task scheduling and select the optimal edge computing node for task offloading.

Pseudo Address Generator (PAG): The PAG can generate pseudo-address PA_h. It can also calculate the optimal update frequency of pseudo-addresses with the goal of maximizing defense gain.

Request User (RU_i): The request user RU_i uploads task information TI_i to the CS, which may be malicious.

Edge Computing Node (EN_j): The edge computing node EN_j responds to the cooperation signal from the ES and cooperates with the CS to perform task information TI_i processing.

B. DESIGN GOALS

Each TI_i possesses unique conservation preferences, with some prioritizing energy consumption, whereas others

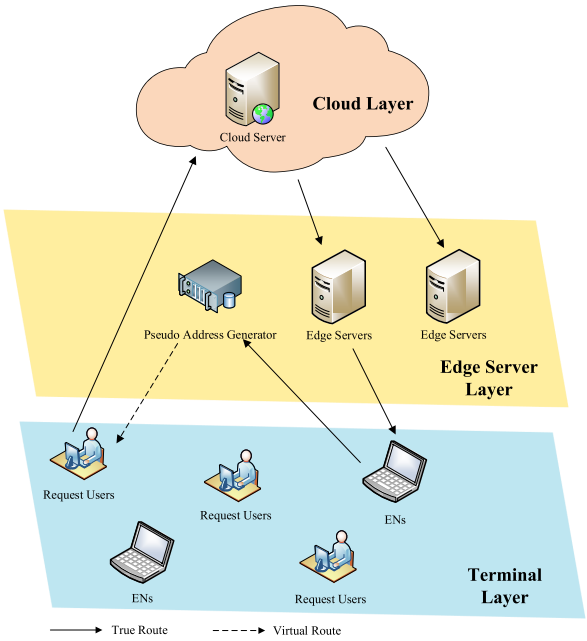


FIGURE 1. Edge computing model.

TABLE 1. Significant variable symbols and their meanings.

Notation	Definition
u_1, u_2, u_3	Weight of information
n	Order of judgment matrix
Q_E^{ij}, Q_{mean}^{ij}, Q_t^{ij}	Degree of unloading loss
PA_h	Pseudo address
TI_i, $TI_i^{'}$	Uploaded and returned task
Q_{loss}^i, T_{max}^i, E_{max}^i	Minimum of loss degree, maximum delay and energy consumption of TI_i
$f_a(t), f_d(t)$	Frequency of interactions and updates
$pf_a(t)$	Attack frequency
r	Time loss rate
$\varepsilon_0 f_a(t)$, $\varepsilon_1 f_d(t)$	Attack and defense costs
$H(t)$, $D(t)$	Interactive costs
$R_a(t)$, $R_d(t)$	Earnings function
$x(t)$	Privacy leakage

emphasize semantic privacy or specific task completion times. Consequently, P²SPA offers more precise protection for individual TI_i instances, enabling the achievement of the same protection effect with fewer resources. To prevent malicious users from deducing the privacy information of EN_j, P²SPA introduces the pseudo-address PA_h as an intermediary node positioned between EN_j and RU_i. This arrangement effectively prevents the direct exposure of EN_j to RU_i, ensuring the relative independence of EN_j. Additionally, to mitigate the potential risks arising from prolonged interactions, P²SPA dynamically updates the PA_h. This measure prevents the nodes from risking over extended periods.

P²SPA is designed as a lightweight edge computing node protection strategy to achieve optimal cost-effectiveness. It specifically tailors precise protection for TI_i based on the protection preferences of RU_i, effectively economizing the protection resources for EN_j. The ES dynamically adjusts the update frequency $f_d(t)$ of the pseudo-addresses in response to the interaction frequency of RU_i. Ultimately, through the pursuit of a Nash equilibrium, we ensure the continual adoption of the locally optimal solution $f_d(t)$ which maintains optimal cost-effectiveness.

C. INITIALIZATION SETTINGS

Definition 1: Information Weights. Each information weight is denoted by U_i=<u_1, u_2, u_3>, where u_1, u_2,and u_3 are constants in [0, 1], whose definitions correspond to the TI_i on the importance of energy consumption, semantic privacy, and completion time, respectively.

Definition 2: Total Loss Degree. TI_i's total loss degree for offloading to EN_j can be written as Q_{ij} ={ Q_E^{ij}, Q_{mean}^{ij}, Q_t^{ij} }. where Q_E^{ij}, Q_{mean}^{ij}, and Q_t^{ij} represent the degree of energy consumption loss, semantic loss degree, and task completion time, respectively. When the CS performs task offloading, redundant data are added to the message before offloading, which defines the degree of semantic loss [38]:

$$Q_{mean}^{ij} = \frac{Q_r^{ij}}{L_i + Q_r^{ij}}, \tag{1}$$

where Q_r^{ij} represents the size of the redundant data, and L_i represents the size of the original data. The completion time of TI_i including the computing time and transmission time, can be expressed as:

$$Q_t^{ij} = \frac{C_i}{f_m^j} + \frac{D_i}{B}. \tag{2}$$

Parameter C_i represents the required computing resources, and f_m^j denotes the computational speed of EN_j, and D_i denotes the size of TI_i, and B denotes the network bandwidth of ES. Furthermore, by considering the power consumption denoted as p_j^c for EN_j and p^E for ES, we can derive the overall computational energy consumption of EN_j as follows:

$$Q_E^{ij} = p_j^c \frac{C_i}{f_m^j} + p^E \frac{D_i}{B}. \tag{3}$$

Meanwhile, we can obtain the total loss degree function of TI_i for offloading to EN_j is:

$$Q_{loss}^{ij} = u_1 Q_E^{ij} + u_2 Q_{mean}^{ij} + u_3 Q_t^{ij}. \tag{4}$$

In particular, we used the *Analytic Hierarchy Process* (AHP) [39] to scientifically quantify the weights. Furthermore, we assume that the pseudo-address PA_h can satisfy the transmission bandwidth requirements of TI_i'. When using the PA_h, no new semantic loss degree is generated; however, the task completion time can be expressed as

$$T_F^i = Q_t^{ij} + \frac{D_i}{d}, \tag{5}$$

where d denotes the size of PA_h network bandwidth. Parameter p_i^t, representing the power of PA_h, is introduced to address the new total energy consumption, and its further derivation is presented as follows:

$$E^i = Q_E^{ij} + p_i^t \frac{D_i}{d}. \tag{6}$$

It is worth noting that malicious nodes have the initiative to act as leaders and always have a first mover advantage. The PAG acts as a follower, which in turn creates a Stackelberg game. The prerequisites are as follows.

1) Because the frequency of attacks is not easily observable, the interaction frequency $f_a(t)$ can be with the risk factor p is considered as the attack frequency. The risk factor p is a constant in (0, 1], and is inversely proportional to the RU_i's degree of trust [10].

2) The malicious node cannot know the task offloading path and thus cannot launch a targeted attack on EN_j. Because TI_i is time-sensitive, we can regard the constant T as timeliness. If the timeliness is exceeded, the attack loses significance [10].

3) The interaction frequency $f_a(t)$ and update frequency $f_d(t)$ are all observable, which is consistent with the scenario of a complete information game.

4) As the risk encountered by EN_j correlates with the duration of interaction, the communication overhead (referred to as the interaction cost) will correspondingly escalate over time to safeguard the security of the information transmission phase. Consequently, the total interaction cost can be succinctly articulated as a second-order differentiable concave function $D(t) = \theta_1 t^2 + \theta_2 t$. In the Stackelberg game model, the cost incurred by EN_j is typically considered as the malicious node's benefit, resulting in the malicious node's interaction cost being denoted as $H(t) = \theta_0 t - D(t)$ (where θ_0, θ_1, and θ_2 all signify constants representing the cost per unit of time discounting factors).

5) Due to the first-mover advantage held by the malicious node, EN_j generates a specific degree of privacy leakage when $f_a(t) > f_d(t)$, and the magnitude of privacy leakage is directly proportional to the disparity between $f_a(t)$ and $f_d(t)$. Conversely, even in the absence of an attack, EN_j will still contribute to the leakage amount of $x'(t)$ due to its intrinsic factors. A portion of this leakage will be acquired by the malicious node. To quantify the privacy leakage, we introduce the discount factor ε_2, ε_3, and express the privacy leakage amount $x(t)$ as:

$$x(t) = \varepsilon_2[f_a(t) - f_d(t)] + \varepsilon_3 x'(t). \tag{7}$$

Meanwhile, the malicious node gain function is obtained for the time [0, T] as:

$$R_a(t) = max \int_0^T \{\lambda_1 f_a(t)[pf_a(t) - f_d(t)] - H(t) - \varepsilon_0 f_a(t) + \varepsilon_1 f_d(t) - x(t)\} e^{-rt} dt, \tag{8}$$

where λ_1 and λ_2 represent the discount factors for malicious nodes and EN_j respectively, and r represents the discount rate, which is proportional to the timeliness of the information. Similarly, the gain function of EN_j is obtained as

$$R_d(t) = max \int_0^T \{\lambda_2 f_d(t)[f_d(t) - pf_a(t)] + H(t) + \varepsilon_0 f_a(t) - \varepsilon_1 f_d(t) + x(t)\} e^{-rt} dt. \tag{9}$$

IV. PROPOSED STRATEGY

This section delineates our devised protection strategy for ENs against dynamic attacks, aiming to maximize cost-effectiveness by integrating the AHP and Stackelberg game models. Herein, we present the problem definition, formula derivation, and the strategy process.

A. PROBLEM DEFINITION

From the formula, it can be observed that for a certain time interval, the gain functions of the attacking and defending parties $R_a(t)$ and $R_d(t)$ both depend directly on $pf_a(t)$ and $f_d(t)$. Under the premise of selecting the optimal EN_j, a convex optimization problem was defined. This problem can be formulated as follows:

$$\min_{f_a(t), f_d(t)} -R_d(t). \tag{10}$$

Satisfaction:

$$Q_{loss}^{ij} \le Q_{loss}^{i} \tag{11}$$

$$T_F^i \le T_{max} \tag{12}$$

$$E^i \le E_{max} \tag{13}$$

Among them, Q_{loss}^i is the minimum of the total loss degree for TI_i. T_{max}, and E_{max} represent the maximum completion time and energy consumption of TI_i allowed, respectively. (10) is to maximize the gain function of the PAG. (11) ensures that the EN_j with the minimum total loss degree is put into service. (12) and (13) are used to select the T_F^i and E^i that meet the requirements PA_h to transmit TI_i'.

B. ALGORITHM DEFINITION

We define the algorithms used in this study. The main algorithms were the Edge computing Node Selection (ENSel) and the Stackelberg game to find Optimal Frequency (SOF) algorithms.

To satisfy the requirement of (11), that is, to find the optimal EN for task offloading, an ENSel algorithm was designed, as shown in Algorithm 1. It is noteworthy that the procedure for generating pseudo-addresses is not the primary focus of this research paper and is detailed in [31]. This information will not be reiterated herein.

We need to select the pseudo-address within the ES service area that meets the requirements of (12) and (13) as the relay nodes for EN_j to interact with RU_i. Pseudo-addresses were updated at a certain frequency. We used the SOF algorithm to meet the goal of problem (10), as shown in Algorithm 2, and the detailed derivation is described as follows.

Algorithm 1 ENSel

Initialization:
Input a judgment matrix P based on the TI_i (Refer to Table. 2).
Step 1: Normalize P by columns and compute $u_i = \frac{\sum_{j=1}^{n} P_{ij}}{n}$. Calculate its maximum eigenvalue λ_{max} and the largest eigenvector.
Step 2: Calculate $CI = \frac{\lambda_{max}-n}{n-1}$, $CR = \frac{CI}{RI}$.(Refer to Table. 3)
Step 3: Consistency check.
IF $CR \leq 0.1$
Output u_1, u_2, u_3.
ELSE
Retain weights that do not pass the consistency test. The weights $C_i = \frac{(\prod_{j=1}^{n} p_{ij})^{\frac{1}{n}}}{\sum_{k=1}^{n}(\prod_{j=1}^{n} p_{kj})^{\frac{1}{n}}}$. Solve the equation $PW = \lambda_{max} W$ to obtain the eigenvectors W and obtain the weights after normalization. Final calculation of the average and Output u_1, u_2, u_3.
END IF
Step 4:
If there are m ENs, generating the total loss degree of TI_i is:
FOR $j = 1, 2 \ldots m$;
$Q_{loss}^{ij} = u_1 Q_E^{ij} + u_2 Q_{mean}^{ij} + u_3 Q_t^{ij}$.
END FOR
Finally we should select the EN_j which have smallest Q_{loss}^{ij} for task offloading.

C. FORMULA DERIVATION

For malicious nodes, taking $pf_a(t)$-$f_d(t)$ multiplied by the discount factor λ_1 as the payoff function, there exists a continuously differentiable function $\psi(t,x)$ satisfying the Bellman equation, that is.

$$\begin{aligned} -\psi_t'(t,x) = \max_{f_a(t)} \{ & [\lambda_1 f_a(t)(pf_a(t) - f_d(t)) - H(t) \\ & - \varepsilon_0 f_a(t) + \varepsilon_1 f_d(t) - x(t)] e^{-rt} \\ & + \psi_x'(t,x)[\varepsilon_2 f_a(t) + \varepsilon_3 x(t) - \varepsilon_2 f_d(t)] dt \}. \end{aligned} \tag{14}$$

By taking a partial derivation of (14) with respect to $f_a(t)$ can obtain the optimal attack frequency $f_a^*(t)$ for malicious nodes:

$$f_a^*(t) = \frac{-\varepsilon_2 \psi_x'(t,x) e^{rt} + \lambda_1 f_d(t) + \varepsilon_0}{2\lambda_1 p}. \tag{15}$$

The differential equation for PAG can be obtained in the same way:

$$\begin{aligned} -\phi_t'(t,x) = \max_{f_d(t)} \{ & [\lambda_2 f_d(t)(f_d(t) - pf_a(t)) + H(t) \\ & + \varepsilon_0 f_a(t) - \varepsilon_1 f_d(t) + x(t)] e^{-rt} \\ & + \phi_x'(t,x)[\varepsilon_2 f_a(t) + \varepsilon_3 x(t) - \varepsilon_2 f_d(t)] dt \}. \end{aligned} \tag{16}$$

By taking the partial derivation of (16) with respect to $f_d(t)$, we obtain the optimal update frequency $f_d^*(t)$ at this time:

$$f_d^*(t) = \frac{\varepsilon_2 \phi_x'(t,x) e^{rt} + \lambda_2 pf_a(t) + \varepsilon_1}{2\lambda_2}. \tag{17}$$

(14) is solved by constructing an analytical solution such that

$$\psi(t,x) = [A(t)x + B(t)] e^{-rt}. \tag{18}$$

First-order differentiation of equation (18) with respect to t and x respectively.

$$\psi_t'(t,x) = \left\{ \left[-rA(t) + A'(t) \right] x + \left[-rB(t) + B'(t) \right] \right\} e^{-rt}. \tag{19}$$

$$\psi_x'(t,x) = A(t) e^{-rt}. \tag{20}$$

Substituting (19) and (20) into (14), we obtain:

$$\begin{aligned} & [rA(t)x - A'(t)x + rB(t) - B'(t)] e^{-rt} \\ & = [\lambda_1 f_a(t)(pf_a(t) - f_d(t)) - H(t) - \varepsilon_0 f_a(t) + \varepsilon_1 f_d(t) \\ & \quad - x(t)] e^{-rt} + A(t) e^{-rt} [\varepsilon_2 f_a(t) + \varepsilon_3 x(t) - \varepsilon_2 f_d(t)]. \end{aligned} \tag{21}$$

(21) is simplified to give: $A'(t) = (r - \varepsilon_3) A(t) + 1$.

Algorithm 2 SOF

Initialization:
Input: The interaction frequency $f_a(t)$ of RU_i.
Step 1: The malicious node attacks with frequency of $pf_a(t)$ and based on the TI_i's timeliness to determine the maximum attack time T.
Step 2: The defender uses the frequency $f_d(t)$ for updating the psseudo-address, and both sides form their own gain functions as follow.
Malicious node (**Leader**):
Take the partial derivative of the gain function with respect to $f_a(t)$, and obtain $f_a^*(t) = \frac{-\varepsilon_2 \psi_x'(t,x) e^{rt} + \lambda_1 f_d(t) + \varepsilon_0}{2\lambda_1 p}$.
PAG (**Followers**):
The same reasoning leads to $f_d^*(t) = \frac{\varepsilon_2 \phi_x'(t,x) e^{rt} + \lambda_2 pf_a(t) + \varepsilon_1}{2\lambda_2}$.
Step 3: Use $f_a^*(t)$ and $f_d^*(t)$ to play the game and back substitute with each other to obtain the solution in the equilibrium case.
Step 4: Find the analytic solution of the implicit function $\psi(t,x)$ and $\phi(t,x)$.
$\psi_x'(t,x) = \frac{-1}{(r-\varepsilon_3)}[1 - e^{(r-\varepsilon_3)(t-T)}] e^{-rt}$.
$\phi_x'(t,x) = \frac{1}{(r-\varepsilon_3)}[1 - e^{(r-\varepsilon_3)(t-T)}] e^{-rt}$.
Step 5: The results of **Step 4** are back substituted to obtain the optimal pseudo-address update frequency $f_d^*(t)$.

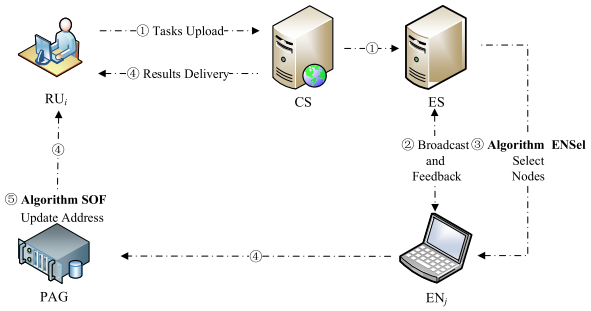


FIGURE 2. Flow of P²SPA strategy.

Solving the above equation, we get

$$A(t) = \frac{-1}{(r-\varepsilon_3)}\left[1 - e^{(r-\varepsilon_3)(t-T)}\right]. \tag{22}$$

Bringing (22) into (20),

$$\psi_x'(t,x) = \frac{-1}{(r-\varepsilon_3)}[1 - e^{(r-\varepsilon_3)(t-T)}]e^{-rt}. \tag{23}$$

Similarly, constructing an analytical solution to (16) and organizing it yields:

$$\phi_x'(t,x) = \frac{1}{(r-\varepsilon_3)}[1 - e^{(r-\varepsilon_3)(t-T)}]e^{-rt}. \tag{24}$$

The dynamic game process is to substitute (15) and (17) back into each other and organize to obtain a the formula containing the implicit function.

$$f_a^*(t) = \frac{-2\varepsilon_2\psi_x'(t,x)\,e^{rt} + 2\varepsilon_0}{3\lambda_1 p} + \frac{\varepsilon_2\phi_x'(t,x)e^{rt} + \varepsilon_1}{3\lambda_2 p}. \tag{25}$$

$$f_d^*(t) = \frac{2\varepsilon_2\phi_x'(t,x)\,e^{rt} + 2\varepsilon_1}{3\lambda_2} + \frac{-\varepsilon_2\psi_x'(t,x)e^{rt} + \varepsilon_0}{3\lambda_1}. \tag{26}$$

Substituting Equations (23) and (24) into (25) and (26) yields the optimal pseudo address update frequency as:

$$f_a^*(t) = \frac{2\varepsilon_2(1 - e^{(r-\varepsilon_3)(t-T)})}{3\lambda_1 p(r-\varepsilon_3)} + \frac{2\varepsilon_0}{3\lambda_1 p} + \frac{\varepsilon_2(1 - e^{(r-\varepsilon_3)(t-T)})}{3\lambda_2 p(r-\varepsilon_3)} + \frac{\varepsilon_1}{3\lambda_2 p}. \tag{27}$$

$$f_d^*(t) = \frac{2\varepsilon_2(1 - e^{(r-\varepsilon_3)(t-T)})}{3\lambda_2(r-\varepsilon_3)} + \frac{2\varepsilon_1}{3\lambda_2} + \frac{\varepsilon_2(1 - e^{(r-\varepsilon_3)(t-T)})}{3\lambda_1(r-\varepsilon_3)} + \frac{\varepsilon_0}{3\lambda_1}. \tag{28}$$

D. STRATEGY PROCESS OF P²SPA

This study did not address the CS to ES selection process. Instead, it assumes that the CS conducts task offloading to the ES. The P²SPA strategy is illustrated in Fig. 2. Below, we present the implementation details of the key processes within P²SPA.

TABLE 2. Scale of proportions (Horizontal factors).

Scale	Meaning
1	Equally important
3	Slightly important
5	Clearly important
7	Critically important
9	Extremely important
2, 4, 6, 8	Medium value

TABLE 3. Reference table for RI in the AHP methodology.

Order	*RI*
1	0
2	0
3	0.52
4	0.89
5	1.12

① Tasks Upload. RU$_i$ sends TI_i to the CS, which chooses to process locally or offload to the ES, considering the utilization of its own computing resources.

② Broadcast and Feedback. The ES receives TI_i and broadcasts the computational requirements to all EN$_j$, EN$_j$ that want to participate in the task send node feedback $\{Q_E^{ij}, Q_{mean}^{ij}, Q_t^{ij}\}$ to ES.

③ Nodes Selection. After the ES receives all node feedback $\{Q_E^{ij}, Q_{mean}^{ij}, Q_t^{ij} | \ j = 1, 2, \ldots m\}$, where m represents the number of ENs. It first normalizes the three attributes [40]

$$D_{ji} = \frac{d_{ji}}{\sum_{j=1}^{N} d_{ji}}, \tag{29}$$

where d_{ji} represents the value of the i attribute of EN$_j$, N represents the total number of EN$_j$, and D_{ij} represents the result of the normalization. Subsequently, judgment matrix P is constructed with factors denoted as p_{ji} which represents the importance of j compared to indicator i. This can be expressed using Table.2 and its reciprocal. Finally, the optimal EN$_j$ is selected to offload the task using the ENSel algorithm.

④ Results Delivery. CS and EN$_j$ for the TI_i are processed separately. The locally processed results are directly sent back from the CS to RU$_i$, and the results processed at EN$_j$ send TI_i to RU$_i$ by PA_h, which is generated by PAG.

⑤ Address Update. PA_h frequent interaction with RU$_i$ poses a risk; it is necessary to use Algorithm SOF to obtain the optimal pseudo-address update frequency $f_d^*(t)$ according to $f_a(t)$.

V. SIMULATION RESULTS

To ascertain the effectiveness of this strategy, we undertake simulation verification within a virtual network model comprising servers, a Pseudo Address Generator(PAG), ENs, and request users.

A. SIMULATION SETTINGS

Assuming the cloud server as the origin and attributing a communication range of 10 km to it, a coordinate system with pointers was established. In a circular area with a radius of 10 km, a star topology was adopted to deploy four ENs and PAG. The network speed of the ENs fell within the range of [50Mbps, 100Mbps]. For simulation purposes, a malicious node initiates a task message directed towards the cloud server, which subsequently offloads this task to an EN for computation. The simulation involves assessing the frequency of attacks targeting this task and monitoring the pseudo-address updating frequency over a 10-minute period.

The relevant parameters in the simulation are as follows: u_1, u_2, and u_3 represent the preference degrees for energy consumption, semantic accuracy, and time delay of task information, respectively. These values vary for each task and fall within the range of (0, 1). The parameter r indicates the time discount degree, ranging from (0, 1], and is associated with the task information's timeliness. The gain factors λ_1 and λ_2, with values in the range [1, 2], are related to the value of the task information. The parameters θ_1, θ_2, and θ_3, each ranging from (0, 5], represent the cost factor per unit time associated with the communication overhead caused by task information. Additionally, ε_0, and ε_1, with values ranging from (0, 5], represent the cost factors of attack and defense. The factors ε_2 and ε_3, acting as privacy leakage factors, are associated with the task's intrinsic characteristics, with values in the range (0, 1] and $[r, 1]$, respectively. Task processing is simulated in various scenarios by adjusting these parameters.

B. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

We conduct a comparative analysis against the low-frequency IP hopping strategy [31] and high-frequency IP hopping strategy [41] in terms of cost and protection effectiveness. P²SPA employs pairwise attribute comparison during task offloading and constructs a judgment matrix through $\frac{n(n-1)}{2}$ assessments. This method allows for more precise protection with reduced resource utilization. Our simulation involves 1000 tasks with varying protection preferences, demonstrating loss degree pairs, as shown in Fig. 3.

As shown in Fig. 3, P²SPA consistently exhibits superior resource utilization (as indicated by smaller loss degrees) across diverse information types with varied protection preferences, emphasizing its cost-effective superiority over other strategies. Following the selection of the optimal EN for offloading, we delve into an analysis of the frequency variations in pseudo-address updating concerning attacks of differing frequencies.

The variance in p signifies distinct levels of trustworthiness of malicious nodes. As illustrated in Fig. 4, a reduction in p implies an increase in the PAG's trust in a user, prompting the malicious node to elevate its attack frequency in the pursuit of greater gains. Consequently, PAG becomes more proactive

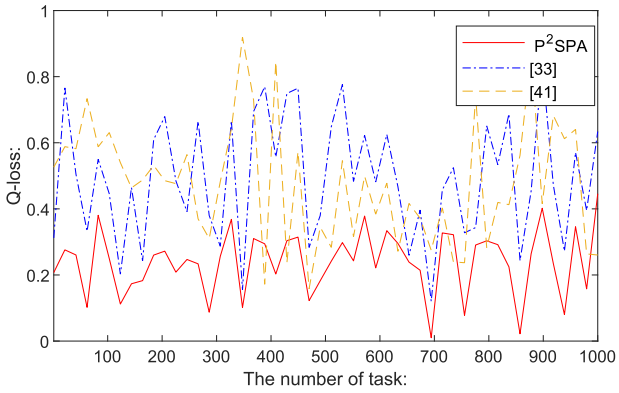


FIGURE 3. The comparison of Q_{loss}.

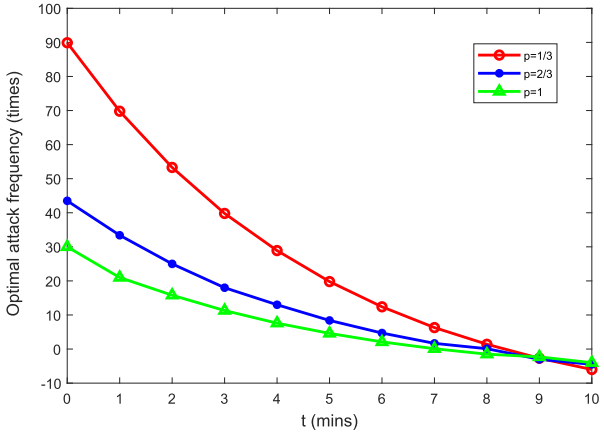


FIGURE 4. Variation process of optimal attack frequency with p.

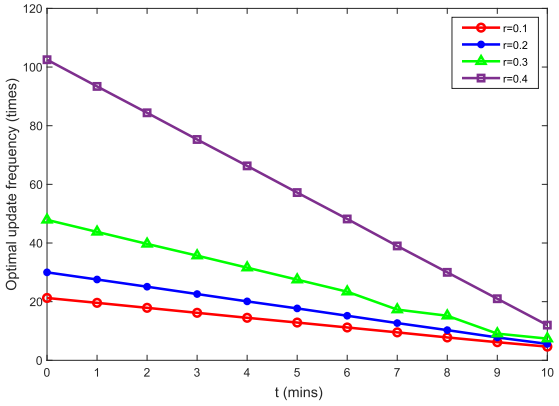


FIGURE 5. Variation process of update frequency with r.

in adjusting its privacy protection measures, resulting in a progressively rapid convergence of attack frequencies. Over time, the immediacy of information diminishes, leading to a gradual decline in attack frequencies. Negative attack frequency values denote instances in which the active response of the PAG results in a negative gain function for the attacker, signifying successful resistance against the attack.

Considering the varying timeliness of different task information, we introduce the time discount rate r, which is

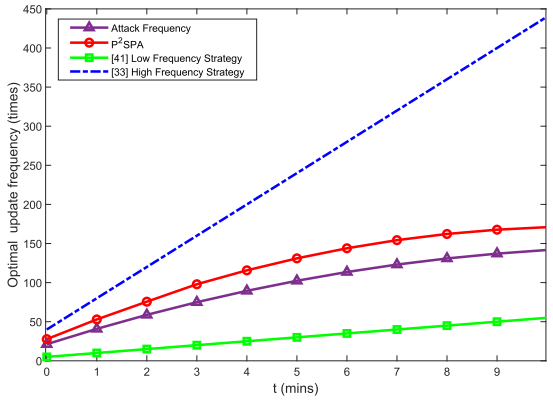


FIGURE 6. Degree of fit between update and attack frequency.

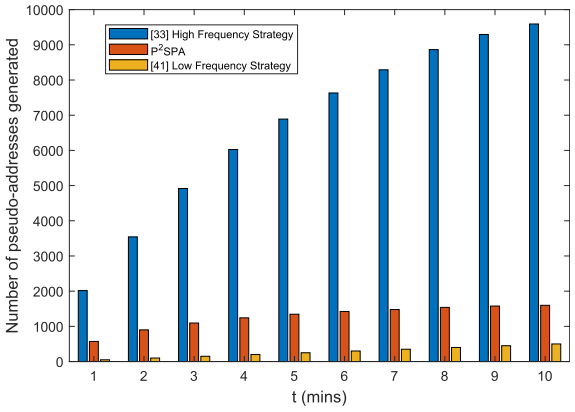


FIGURE 7. Comparison of the number of addresses.

directly proportional to the urgency of the task information. Fig. 5 demonstrates an increasing trend in the optimal pseudo-address update frequency with a higher r, indicating a relatively rapid convergence speed. This trend stems from r serving as a pivotal parameter in EN's defense gain function, significantly influencing the determination of pseudo-address updating frequency during the dynamic game process. A greater task urgency, denoted by a higher r correlates with an increased need for frequent pseudo-address updates. Conversely, as information becomes less time-sensitive over time, its significance gradually diminishes, leading to convergence in the number of pseudo-address updates.

To further substantiate the superiority of P²SPA, we conducted a comparative analysis against the strategies from [33] and [41]. The differentiation between low and high attack frequencies is established relative to the attack frequency $pf_a(t)$, where low frequency refers to instances where $f_d(t)<f_a(t)$ and high frequency denotes scenarios where $f_d(t)$ significantly surpasses $f_a(t)$ (i.e., $f_d(t)>2f_a(t)$) [10]. We quantified the cost of protection based on the alignment of $f_d(t)$ with $pf_a(t)$, using $r = 0.2$. By employing the original parameters, we calculated the mean values of $f_a(t)$ and $f_d(t)$ for each strategy across multiple simulations. The reason are shown in Fig. 6.

Fig. 6 clearly demonstrates that the update frequency $f_d(t)$ proposed by our strategy dynamically adjusts in response to fluctuations in the attack frequency $pf_a(t)$. Not only does $f_d(t)$ consistently surpass $pf_a(t)$, but it also exhibits a superior closeness effect. This indicates that the efficiency of the edge server cost-saving defense strategy without compromising defense efficacy. In contrast, the strategies presented in [31] and [41] maintain relatively fixed update frequencies, lacking adaptive adjustments corresponding to changes in the attack frequency. Consequently, these strategies struggle to effectively fend off attacks or lead to wastage of resources. Moreover, we conducted a comparative analysis between P²SPA, [31] and [41], evaluating the defense cost based on the generated number of pseudo-addresses. The simulation results are shown in Fig. 7.

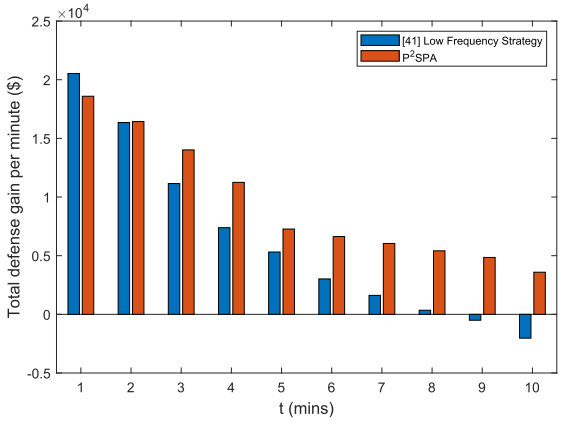


FIGURE 8. Comparison of the defense returns over a 10 minutes period.

Fig. 7 illustrates that [31] consistently updates pseudo-addresses at a high frequency, achieving a commendable defense effect but incurring significant wastage of the ENs' limited protection resources. Conversely, while [41] exhibits a lower cost, it faces vulnerability when the attack frequency surpasses its IP address set because of infrequent updates. This situation provides malicious nodes with ample time for packet analysis and potential intrusions. P²SPA presented a balanced approach, offering effective protection at a lower cost, making it more suitable for ENs operating within constrained resources. It is worth noting that [31], although not directly tailored for edge networks, demonstrates superior defense effectiveness for ENs. Therefore, we conducted a comparative analysis between P²SPA and [41] in terms of defense effectiveness.

As shown in Fig. 8, [41] initially demonstrated a high defense benefit owing to its low defense cost. However, over time, an attacker progressively deciphers its defense characteristics, leading to a gradual decline in its defense gain. This deterioration culminates in EN breach, resulting in a negative defense effect. Conversely, in P²SPA, the attacker fails to achieve the anticipated gain, prompting the attack to stabilize. Consequently, the corresponding defense gain exhibited a similar trend.

VI. CONCLUSION

In the context of future MEC facilitating secure task offloading to ENs for reduced latency, this study delves into ENs location privacy protection. Addressing the constraints of the ENs' limited resources, P²SPA is devised. This strategy optimally selects EN based on the varying protection preferences of the task information. Employing pseudo-addresses for user interactions, P²SPA determines optimal update frequencies through Stackelberg game dynamics to safeguard the ENs. Comparative evaluations against existing methods highlight P²SPA's favorable balance between defense effects and cost-effectiveness. The numerical estimations affirm P²SPA's proficiency in achieving a compromise service strategy with a satisfactory cost-effective performance. Overall, it is a lightweight and robust protection strategy for ENs, and future research will explore information transmission across non-secure channels.

REFERENCES

[1] X. Hu, L. Wang, K.-K. Wong, M. Tao, Y. Zhang, and Z. Zheng, "Edge and central cloud computing: A perfect pairing for high energy efficiency and low-latency," *IEEE Trans. Wireless Commun.*, vol. 19, no. 2, pp. 1070–1083, Feb. 2020.

[2] P. Dong, J. Ge, X. Wang, and S. Guo, "Collaborative edge computing for social Internet of Things: Applications, solutions, and challenges," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 1, pp. 291–301, Feb. 2022.

[3] Y. Zhang, X. Lan, J. Ren, and L. Cai, "Efficient computing resource sharing for mobile edge-cloud computing networks," *IEEE/ACM Trans. Netw.*, vol. 28, no. 3, pp. 1227–1240, Jun. 2020.

[4] H. Wang, T. Liu, B. Kim, C.-W. Lin, S. Shiraishi, J. Xie, and Z. Han, "Architectural design alternatives based on cloud/edge/fog computing for connected vehicles," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2349–2377, 4th Quart., 2020.

[5] S. Chen, L. Wang, and F. Liu, "Optimal admission control mechanism design for time-sensitive services in edge computing," in *Proc. INFOCOM IEEE Conf. Comput. Commun.*, London, U.K., May 2022, pp. 1169–1178.

[6] Z. Ning, K. Zhang, X. Wang, M. S. Obaidat, L. Guo, X. Hu, B. Hu, Y. Guo, B. Sadoun, and R. Y. K. Kwok, "Joint computing and caching in 5G-envisioned Internet of Vehicles: A deep reinforcement learning-based traffic control system," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5201–5212, Aug. 2021.

[7] X. Xu, X. Liu, Z. Xu, F. Dai, X. Zhang, and L. Qi, "Trust-oriented IoT service placement for smart cities in edge computing," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4084–4091, May 2020.

[8] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.

[9] B. Gu, L. Gao, X. Wang, Y. Qu, J. Jin, and S. Yu, "Privacy on the edge: Customizable privacy-preserving context sharing in hierarchical edge computing," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2298–2309, Oct. 2020.

[10] Y. He, M. Zhang, X. Yang, Q. T. Sun, J. Luo, and Y. Yu, "The intelligent offense and defense mechanism of Internet of Vehicles based on the differential game-IP hopping," *IEEE Access*, vol. 8, pp. 115217–115227, 2020.

[11] A. X. Liu and M. G. Gouda, "Firewall policy queries," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 6, pp. 766–777, Jun. 2009.

[12] Z. Yang and K. L. Yeung, "SDN candidate selection in hybrid IP/SDN networks for single link failure protection," *IEEE/ACM Trans. Netw.*, vol. 28, no. 1, pp. 312–321, Feb. 2020.

[13] X. Chen, L. Xiao, W. Feng, N. Ge, and X. Wang, "DDoS defense for IoT: A Stackelberg game model-enabled collaborative framework," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9659–9674, Jun. 2022.

[14] J. Rischke, P. Sossalla, S. Itting, F. H. P. Fitzek, and M. Reisslein, "5G campus networks: A first measurement study," *IEEE Access*, vol. 9, pp. 121786–121803, 2021.

[15] Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, "Toward edge intelligence: Multiaccess edge computing for 5G and Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6722–6747, Aug. 2020.

[16] R. E. Navas, F. Cuppens, N. Boulahia Cuppens, L. Toutain, and G. Z. Papadopoulos, "MTD, where art thou? A systematic review of moving target defense techniques for IoT," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7818–7832, May 2021.

[17] Z. Chen, X. Chang, Z. Han, and Y. Yang, "Numerical evaluation of job finish time under MTD environment," *IEEE Access*, vol. 8, pp. 11437–11446, 2020.

[18] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and B. Yang, "SCEMA: An SDN-oriented cost-effective edge-based MTD approach," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 667–682, 2023.

[19] G. Cui, Q. He, F. Chen, H. Jin, Y. Xiang, and Y. Yang, "Location privacy protection via delocalization in 5G mobile edge computing environment," *IEEE Trans. Services Comput.*, vol. 16, no. 1, pp. 412–423, Jan. 2023.

[20] L. Li, H. Song, Y. Qian, and J. Li, "On resource allocation for network slicing with Stackelberg game," in *Proc. 2nd Int. Seminar Artif. Intell., Netw. Inf. Technol. (AINIT)*, Shanghai, China, 2021, pp. 252–256.

[21] S. Seo, H. Moon, S. Lee, D. Kim, J. Lee, B. Kim, W. Lee, and D. Kim, "D3GF: A study on optimal defense performance evaluation of drone-type moving target defense through game theory," *IEEE Access*, vol. 11, pp. 59575–59598, 2023.

[22] P. Xu, J. Yang, G. Chen, Z. Yang, Y. Li, and M. Z. Win, "Physical-layer secret and private key generation in wireless relay networks with correlated eavesdropping channels," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 985–1000, 2024.

[23] Y. Tan, J. Liu, and J. Wang, "How to protect key drones in unmanned aerial vehicle networks? An SDN-based topology deception scheme," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 13320–13331, Dec. 2022.

[24] L. Xing, X. Jia, J. Gao, and H. Wu, "A location privacy protection algorithm based on double K-anonymity in the social Internet of Vehicles," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3199–3203, Oct. 2021.

[25] C. Liu, F. Tang, Y. Hu, K. Li, Z. Tang, and K. Li, "Distributed task migration optimization in MEC by extending multi-agent deep reinforcement learning approach," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1603–1614, Jul. 2021.

[26] H. Wu, X. Tian, M. Li, Y. Liu, G. Ananthanarayanan, F. Xu, and S. Zhong, "PECAM: Privacy-enhanced video streaming and analytics via securely-reversible transformation," in *Proc. 27th Annu. Int. Conf. Mobile Comput. Netw.* New Orleans, LA, USA: ACM, Sep. 2021, pp. 229–241.

[27] F. Meneses, D. Corujo, A. Neto, and R. L. Aguiar, "SDN-based end-to-end flow control in mobile slice environments," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Verona, Italy, Nov. 2018, pp. 1–5.

[28] S.-Y. Chang, Y. Park, and B. B. Ashok Babu, "Fast IP hopping randomization to secure hop-by-hop access in SDN," *IEEE Trans. Netw. Service Manage.*, vol. 16, no. 1, pp. 308–320, Mar. 2019.

[29] N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, E. Jacob, and C. Martinez-Cagnazzo, "Physical assessment of an SDN-based security framework for DDoS attack mitigation: Introducing the SDN-SlowRate-DDoS dataset," *IEEE Access*, vol. 11, pp. 46820–46831, 2023.

[30] S. Yoon, J.-H. Cho, D. S. Kim, T. J. Moore, F. Free-Nelson, and H. Lim, "Attack graph-based moving target defense in software-defined networks," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 3, pp. 1653–1668, Sep. 2020.

[31] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "An effective address mutation approach for disrupting reconnaissance attacks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2562–2577, Dec. 2015.

[32] J. Zhang, L. Che, and M. Shahidehpour, "Distributed training and distributed execution-based Stackelberg multi-agent reinforcement learning for EV charging scheduling," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4976–4979, Nov. 2023.

[33] L. Xie, S. Meng, W. Yao, and X. Zhang, "Differential pricing strategies for bandwidth allocation with LFA resilience: A Stackelberg game approach," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 4899–4914, 2023.

[34] O. Lindamulage De Silva, V. S. Varma, M. Cao, I.-C. Morarescu, and S. Lasaulce, "A Stackelberg viral marketing design for two competing players," *IEEE Control Syst. Lett.*, vol. 7, pp. 2922–2927, 2023.

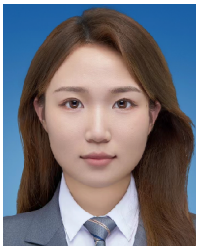
[35] M. Liu and Y. Liu, "Price-based distributed offloading for mobile-edge computing with computation capacity constraints," *IEEE Wireless Commun. Lett.*, vol. 7, no. 3, pp. 420–423, Jun. 2018.

[36] B. Gao, Z. Zhou, F. Liu, F. Xu, and B. Li, "An online framework for joint network selection and service placement in mobile edge computing," *IEEE Trans. Mobile Comput.*, vol. 21, no. 11, pp. 3836–3851, Nov. 2022.

[37] J. Wu, L. Wang, Q. Pei, X. Cui, F. Liu, and T. Yang, "HiTDL: High-throughput deep learning inference at the hybrid mobile edge," *IEEE Trans. Parallel Distrib. Syst.*, vol. 33, no. 12, pp. 4499–4514, Dec. 2022.
[38] G. Qiu, D. Guo, Y. Shen, G. Tang, and S. Chen, "Mobile semantic-aware trajectory for personalized location privacy preservation," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 16165–16180, Nov. 2021.
[39] S. Mishra, M. N. Sahoo, S. Bakshi, and J. J. P. C. Rodrigues, "Dynamic resource allocation in fog-cloud hybrid systems using multicriteria AHP techniques," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8993–9000, Sep. 2020.
[40] N. Yaraghi, P. Tabesh, P. Guan, and J. Zhuang, "Comparison of AHP and Monte Carlo AHP under different levels of uncertainty," *IEEE Trans. Eng. Manag.*, vol. 62, no. 1, pp. 122–132, Feb. 2015.
[41] A. Makanju, A. N. Zincir-Heywood, and S. Kiyomoto, "On evolutionary computation for moving target defense in software defined networks," in *Proc. Genetic Evol. Comput. Conf. Companion*. Berlin, Germany: ACM, Jul. 2017, pp. 287–288.

JIAYUAN DU received the B.S. degree in information and computing science from Qufu Normal University, Qufu, China, in 2017, where he is currently pursuing the M.S. degree in computer technology. His research interests include edge computing, privacy preservation, and game theory.

GUOWEI ZHANG received the B.S. degree in electronic information engineering from Huazhong University of Science and Technology, Wuhan, China, in 2014, and the Ph.D. degree in communication and information systems from SIMIT, Chinese Academy of Sciences, Shanghai, China, in 2019. From 2019 to 2020, he was with Huawei Technologies Company Ltd., where he was involved in the solution design of spectrum sharing. Since 2020, he has been a Lecturer with the School of Cyber Science of Engineering, Qufu Normal University. His current research interests include mobile computing, computing resource management, privacy protection, and algorithm design.



XIAOWEI YUAN received the B.S. degree in information management and information system from Qufu Normal University, Qufu, China, in 2021, where she is currently pursuing the M.S. degree with the School of Cyber Science of Engineering. Her current research interests include mobile computing, computing resource management, and privacy protection.

XIAODONG ZANG received the Ph.D. degree from the School of Cyber Science and Engineering, Southeast University, Nanjing, China, in 2020. He is a Postdoctoral Researcher with the College of Electronic Optical Engineering, Nanjing University of Posts and Telecommunications, Jinan, China. Since 2020, he has been a Lecturer with the School of Cyber Science of Engineering, Qufu Normal University. His research interests include computer networks and security, intrusion detection, network traffic, and host profiling.