applied sciences

MDPI

Article

Mean-Field Stackelberg Game-Based Security Defense and Resource Optimization in Edge Computing

Li Miao [1,2,*], Shuai Li [1,2], Xiangjuan Wu [1,2] and Bingjie Liu [3]

[1] School of Information Engineering, Ningxia University, Yinchuan 750021, China; lis@nxu.edu.cn (S.L.); xjwu@nxu.edu.cn (X.W.)
[2] Ningxia Key Laboratory of Artificial Intelligence and Information Security for Channeling Computing Resources from the East to the West, Yinchuan 750021, China
[3] College of Information and Management Science, Henan Agricultural University, Zhengzhou 450002, China; liubingjie@henau.edu.cn
* Correspondence: limiao_smile@nxu.edu.cn

Abstract: Edge computing brings computation and storage resources to the edge of the mobile network to solve the problems of low latency and high real-time demand. However, edge computing is more vulnerable to malicious attacks due to its open and dynamic environments. In this article, we investigate security defense strategies in edge computing systems, focusing on scenarios with one attacker and multiple defenders to determine optimal defense strategies with minimal resource allocation. Firstly, we formulate the interactions between the defenders and the attackers as the mean-field Stackelberg game model, where the state and the objective functions of the defenders are coupled through the mean-field term, and are strongly influenced by the strategy of the attacker. Then, we analyze the local optimal strategies of the defenders given an arbitrary strategy of the attackers. We demonstrate the Nash equilibrium and the mean-field equilibrium for both the defenders and the attackers. Finally, simulation analysis will illustrate the dynamic evolution of the defense strategy of the defenders and the trajectory of the attackers based on the proposed Stackelberg game model.

Keywords: edge computing; mean-field Stackelberg game; optimal control

check for updates

Citation: Miao, L.; Li, S.; Wu, X.; Liu, B. Mean-Field Stackelberg Game-Based Security Defense and Resource Optimization in Edge Computing. *Appl. Sci.* **2024**, *14*, 3538. https://doi.org/10.3390/app14093538

Academic Editor: Mirosław Klinkowski

Received: 14 February 2024
Revised: 1 April 2024
Accepted: 5 April 2024
Published: 23 April 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the rapid development of Internet of Things (IoT) technology, intelligent algorithms, and 5G communication technology, the number of mobile terminals and IoT devices is growing exponentially, generating a series of applications with latency-sensitive, compute-intensive, and continuous service characteristics such as smart healthcare, intelligent transportation, and virtual reality [1]. Cloud computing remains the finest approach for processing huge amounts of data. Nevertheless, the cloud is limited by the high load and high latency of the backbone network, making it difficult to provide low latency for the above intelligent applications [2,3].

Edge computing architecture eliminates the bottleneck of cloud computing as it processes and storages the resources at the network edge [4]. As a new distributed computing paradigm, edge computing has brought some new research topics such as computation offloading, edge caching, etc. [5,6]. Due to the highly open and dynamic environment, resource-limited terminal devices, and multi-source heterogeneous data, edge computing is susceptible to targeted attacks [7]. For example, a malware called "Mirai" took control of up to four hundred thousand damaged smart devices and launched DDoS attacks on edge servers [8]. Moreover, secure communication for edge devices usually relies heavily on traditional cloud-based security mechanisms such as detection, identity authentication, etc., which need more computation resources and energy [9]. Therefore, how to achieve efficient defense strategies while considering the consumption of the limited resources of mobile devices is a challenge.

This study concentrates on addressing security defense challenges in edge computing environments to identify and implement optimal defense strategies. We examine the interaction behavior between defenders and attackers by using the mean-field Stackelberg game theory [10–12], which can solve complex and dynamic problems with large players. In the mean-field game model, the interaction behavior of individuals can be coupled through the mean-field term, and then the global problem can be converted into individual subproblems that greatly reduce the computing complexity of large-scale networks. The mean-field game (MFG) model has been applied to the security defense problem in [13,14]. For large-scale edge devices, the authors in [13] designed an anti-attack model based on the mean-field game and obtained the equilibrium through a self-organizing neural network. In [14], the authors proposed a finite-horizon indefinite mean-field stochastic cooperative linear–quadratic difference game and analyzed the balance between the minimization of investments and the security level. In this paper, we consider the number of attackers as one player, which is modeled as the leader, while the defenders are the followers. In this case, the leader first chooses and then announces the optimal strategy to the defenders. Each defender will choose its optimal defense strategy to minimize the loss based on the leader's observed strategy. We aim to obtain the optimal defense strategies based on the minimization of resource consumption and the strategy of the attacker. Meanwhile, the objective is to balance the profits and the resource consumption for both the defenders and the attackers. The contributions of this article can be summarized as follows.

(1) Firstly, we analyze an edge computing system environment where the attacker is the leader, while the defenders are the followers. We propose an optimization problem that jointly optimizes resource consumption and player decisions by including state and decision variables.
(2) Secondly, we formulate a mean-field Stackelberg game model to analyze the optimization problem, in which the dynamic evolutions of the states of the defenders are coupled with each other through the mean-field term and strongly influenced by the attack intensity. Moreover, we analyze the impact of the defense strategy on the evolution of the state of the attacker. The objectives for the defenders are to minimize the cost of defending against attackers and reduce the losses caused by attacks. The objective for the attackers is to minimize their attack cost.
(3) Finally, we solve a local optimal control problem of the defenders given an arbitrary strategy of the attackers and discuss how the defenders' optimal decentralized strategies lead to an ε-Nash equilibrium for each fixed strategy of the leader, where ε converges to zero as $N \to \infty$. We then consider the leader's local optimal control problem and obtain the leader's decentralized optimal controller.

The remainder of this article is organized as follows. The related works are introduced in Section 2. The system model and problem formulation are provided in Section 3, and the local mean-field equilibrium and the Nash equilibrium are discussed in Section 4. Numerical simulations are given in Section 5. Finally, we conclude the work in Section 6.

2. Related Works

Edge computing has received much attention in recent years. Several studies have focused on the security issues in edge computing and provided some defense mechanisms. For instance, Alwarafy et al. [15] summarized the challenge of the security issues of Internet of Things (IoT) edge devices. The focus of this work was mainly on the classifications of attacks and threats for the devices with limited resources and a discussion of the defense strategies at different edge network layers for different security threats. In [16], a study was conducted to focus on the deployment of defense mechanisms to address security issues in edge computing. In this work [16], the security issues in edge computing systems were categorized into the perception layer, network layer, and application layer, and then the defense problem was analyzed from the perspective of artificial intelligence.

Li et al. [17] introduced a cooperative defense framework for defending against DDoS attacks in mobile edge computing, which could adapt to traffic changes by automatically

coordinating container-carrying defense resources among the edge nodes. Myneni et al. [18] proposed a distributed deep defense framework by using edge computing approaches, which could detect and mitigate DDoS attacks near the data source; this defense framework could significantly reduce unnecessary bandwidth consumed by DDoS traffic going from edge network to edge network. Uddin et al. [19] proposed a layered approach to research the different categories of denial of service (DoS) and distributed denial of service (DDoS) attacks in edge computing systems. They analyzed the inherent vulnerabilities and weaknesses of attacks and proposed an architecture with detection and defense mechanisms based on federated learning. Zhou et al. [20] proposed a new defense framework in edge computing scenarios for the prediction and detection of DDoS attacks.

Wang et al. [21] introduced an eavesdropping-based attack-aware cache defense algorithm that could mitigate the effects of the attacker on the caching performance. Qiu et al. [22] proposed a defensive quantization method to mitigate the perturbations from the malicious samples in edge computing. Since improving the defense level means occupying more additional computation resources, the authors of [23] discussed the tradeoff between limited resource optimization and defense level improvement in edge computing offloading. Moreover, game theory has been used to solve the problem of resource-constrained resources and the security defense level. The survey in [24,25] summarized the methods that have been adopted to solve attacker-defender games and found that the current attacker-defender games that focus on technology adoption assume that the defender will deploy a single new technology at all target sites. The work discussed the future trends and research directions for applying game theory models in edge services and considering usage scenarios. For edge DDoS attacks, [26] proposed a novel game-theoretical approach named EDM Game and obtained the Nash equilibrium by using a decentralized algorithm. Wang et al. [27] analyzed the gains of defense mechanisms based on the stochastic differential game theory. Miao et al. [28] modeled the interaction behavior between defenders and attackers as a stochastic game model for resource-constrained devices and determined the optimal defense strategy. Qian et al. [29] proposed a mean-field game model to solve the data security issues in edge computing.

Although several works have considered the balance between limited resource consumption and security, some schemes achieve this goal by designing specific detection and defense technology, while others achieve this through game models. Few works consider the coupling relationship between the objective of attackers and the strategy of each defender and the dynamic changes in defense decisions under constrained resource consumption.

3. System Model and Problem Statement

In this section, we consider an edge computing system with N defender nodes, and the attackers modeled as one player. As shown in Figure 1, the structure of the edge computing architecture comprises three layers, which are named the terminal device layer, the edge layer, and the cloud layer. Edge computing architecture enables practical applications by providing resources and services through collaborative computing between the terminal and the edge cloud. Edge servers are connected to the cloud, which collects and centrally analyzes data from terminal devices and provides feedback to the bottom two layers. The terminal devices with limited resources process the calculation and storage of local real-tasks.

In this paper, the dynamic interactions between attackers and defenders are studied by using mean-field Stackelberg differential games, in which the attacker can be considered as the leader and the defenders as the followers. The attacker chooses the strategy before the start of the games and announces it to the defenders. The defenders choose their optimal strategies noncooperatively and simultaneously based on the attack level. Moreover, the information structures for both the attacker and the defenders are given by each agent's initial condition in the proposed game model.

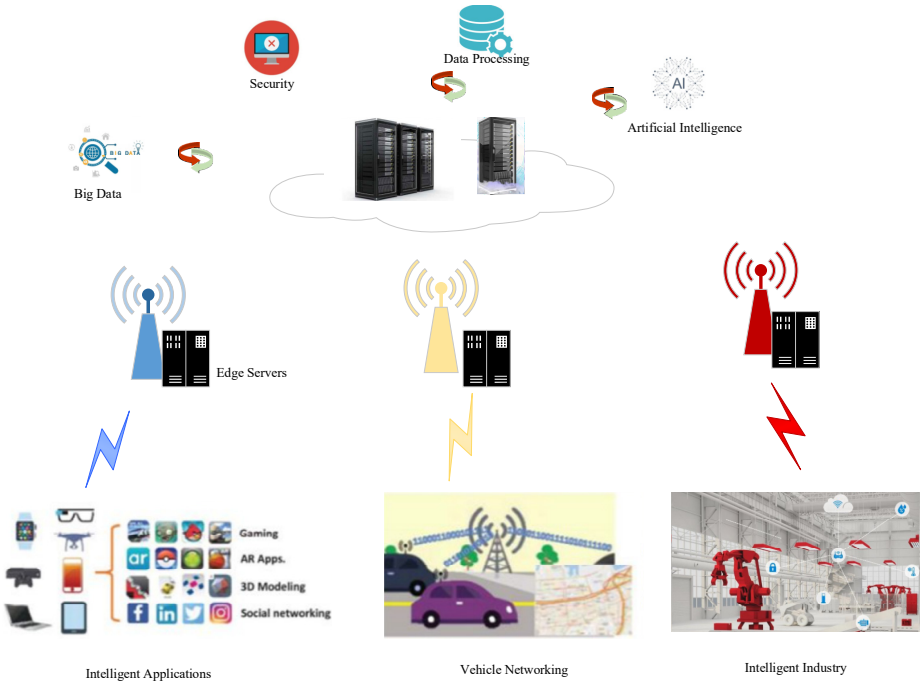

Figure 1. The architecture of edge computing.

We consider $\{x_i(t), 1 \leq i \leq N\}$ as the resource consumption level of the edge device i, $x_0(t)$ as the number of attackers, $u_i(t)$ as the defense level of the defender $i(1 \leq i \leq N)$, and $u_0(t)$ as the attack level of the attacker. The evolution of the system states is influenced by the strategic decisions made by both the defenders and attackers in the context of edge computing security. The evolution of the state $x_i(t)$ is also related to the mass behavior of the defenders. $\|x\|^2 =< x, x >$ denotes the induced 2-norm. Hence, the dynamic evolution states of the defenders and attackers can be given by

$$\frac{dx_i(t)}{dt} = a_i x_i(t) + b_i u_i(t) + c_i \|x_i(t) - Ax^N(t)\|^2 + c_0 u_0(t) \tag{1}$$

$$\frac{dx_0(t)}{dt} = a_0 x_0(t) + b_0 u_0(t) + \sum_{i=1}^{N} \kappa_i u_i(t) \tag{2}$$

where a_i, b_i, a_0, b_0, c_i, c_0, and λ_i are the real parameters. Specifically, a_i is a random coefficient of resource consumption to process the local tasks for the device i, b_i is the probability of the device responding to the defense mechanism. $x^N(t) = \frac{1}{N} \sum_{i=1}^{N} x_i(t)$ is the mean-field term that captures the mass behavior of all the edge devices. $c_i \|x_i(t) - Ax^N(t)\|^2$ means the available resource to detect the behavior of the attackers. b_0 is the probability of successful attacks, and κ_i is the probability that the number of attackers is detected and filtered by the defense mechanisms.

For the defenders, the purpose is to reduce the limited resource consumption, minimize the loss caused by the attackers, and obtain the optimal strategies to maximize against the attacks. The objective function of the defenders is given by

$$J_i(x_i, u_i, u_0) = \min_{u_i(t)} \int_0^T \left[\alpha_i \|x_i(t) - Ax^N(t)\|^2 + \beta_i \|u_i(t)\|^2 + \lambda_i u_i(t) u_0(t) \right] dt \tag{3}$$

where $\alpha_i, \beta_i (i = 1, 2, \cdots, N)$ are positive numbers satisfying $\sum_{i=1}^{N} \alpha_i = 1$, $\alpha_i \|x_i(t) - Ax^N(t)\|^2$ is the cost of deviation from the whole average resource level of the node, $\beta_i \|u_i(t)\|^2$ is the cost of the defense mechanisms, and $\lambda_i u_i^T(t) u_0(t)$ is the payment for defenders, which

depends on both the defense mechanisms and the attack level. Meanwhile, the attacker aims to choose the optimal attack strategy to damage the edge devices and try to increase its attack intensity by maximizing its attack frequency. The objective function of the attacker is given by

$$J_0(x_0, u_i, u_0) = \min_{u_0} E \int_0^T \left(\alpha_0 \|x_0(t) - Ax^N(t)\|^2 + \beta_0 \|u_0(t)\|^2 + \gamma_i u_i(t) \right) dt \tag{4}$$

where α_0, β_0, and γ_i are positive parameters. $\beta_0 \|u_0(t)\|^2$ is the cost of the attacker caused by the attack intensity. The second component $\alpha_0 \|x_0(t) - Ax^N(t)\|^2$ is the cost of successful attacks, and $\gamma_i u_i(t)$ is the cost caused by the defense mechanism.

According to the above analysis, the attacker in the proposed model chooses and then announces their strategies to the defenders. The defenders choose their optimal strategies noncooperatively and simultaneously based on the leader's observed strategy. Each individual defender will choose its optimal defense strategy to minimize the loss caused by the attacks. Next, we will solve a local optimal control problem of the defenders given an arbitrary strategy of the attackers. We will then discuss the local optimal control problem of the attackers.

4. Mean-Field Games Equilibrium and Optimal Strategies

In this section, we consider the mean-field Stackelberg game for the system model, in which the attacker can be considered as the leader because it first chooses the strategy. The defenders are considered as the followers, and they can detect the behavior of attackers. In this framework, each player knows its parameters while the attacker also knows the parameters of the defenders. Since the defenders are coupled through the mean-field term, the optimal control problem of each defender can be considered as an independent mean-field equilibrium problem, which we discuss below.

4.1. Local Optimal Control Problem for the Defenders

Due to the heterogeneity of the edge devices, we replace $x^N(t)$ with $z(t)$, which can be viewed as the mass behavior of the defenders when $N \to \infty$, in which the individual influence of each defender will be negligible. We will obtain the optimal strategies of the defenders under this consideration.

Proposition 1. *Corresponding to system models* (1) *and* (3), *we consider the local optimal strategy problem for each defender. There exists a unique optimal defense strategy $u_i^*(t)$ if and only if*

$$u_i^*(t) = \beta_i^{-1} p_i(t) b_i - \beta_i^{-1} \lambda_i u_0(t) \tag{5}$$

where the adjoint process and the optimal trajectory satisfy the following equations:

$$dx_i^*(t) = \left(a_i x_i^*(t) + c_i \|x_i^*(t) - Ax^N(t)\|^2 - b_i^{-1} \alpha_i^{-1} b_i p_i(t) + \left(c - \beta_i b_i \alpha_i^{-1} \right) u_0(t) \right) dt \tag{6}$$

$$dp_i(t) = \left[-p_i(t) \left(a_i + c_i \left(x_i(t) - Ax^N(t) \right) \right) + \alpha_i \left(x_i(t) - Ax^N(t) \right) \right] dt \tag{7}$$

where $x_i^*(0) = x_{i0}$, $p_i(T) = 0$.

Proof. Consider the variation of defense strategy $\delta u_i(t)$ for each i, which is the control process, such as $u_i(t) = \delta \cdot \delta u_i(t) + u_i^*(t)$. The variational equation is as follows:

$$\begin{cases} d\delta x_i(t) = \left(a_i \delta x_i(t) + b_i \delta u_i(t) + c_i \|\delta x_i(t) - Ax^N(t)\|^2 + c \delta u_0(t) \right) dt \\ \delta x_i(0) = 0 \end{cases} \tag{8}$$

where $\delta x_i(0) = 0$. □

Since the cost function is convex, Equation (5) is the optimal defense strategy if and only if the first-order cost function case

$$\begin{aligned} 0 &= \delta J_i^*\left(u_i^*(t)\right) := \tfrac{d}{d\delta} J_i^*\left(\delta \cdot \delta u_i(t) + u_i^*(t)\right)\Big|_{\delta=0} \\ &= E\int_0^T \left[\alpha_i \delta x_i(t)\left(x_i(t) - Ax^N(t)\right) + \delta u_i^*(t)\beta_i u_i(t) + \lambda_i \delta u_i(t) u_0(t)\right] dt \end{aligned} \tag{9}$$

Next, we use the Itô formula:

$$d\delta x_i(t) p_i(t) = \delta b_i u_i(t) p_i(t) dt + \delta x_i(t)\Big(x_i(t) - Ax^N(t)\Big) dt \tag{10}$$

Since $\delta x_i(0) = 0$, and $p_i(T) = 0$, we obtain the optimal control.

We now obtain the local optimal strategy for the defender and the corresponding state trajectory. The purpose of this analysis is to determine the mean-field approximation and the ε-Stackelberg equilibrium problem. It can be seen from Proposition 1 that the optimal defense strategy is determined by the threat level of the attackers and the adjoint operator, whereas the defense strategy also depends on the state because of the limited resources of edge devices. Hence, we can refine the adjoint operator $p_i(t)$.

To obtain the feedback representation of the defenders in (5) and (6), let $p_i(t) = -V_i(t)x_i^*(t) + \varphi_i(t)$, where $V_i(t)$ is the value function, and $\varphi_i(t)$ is the continuously differentiable function satisfying $\varphi_i(T) = 0$ and

$$-\frac{dV_i(t)}{dt} = -\beta_i^{-1} b_i^2 V_i^2(t) + 2a_i V_i(t) + \phi_i \tag{11}$$

$$V_i(T) = 0 \tag{12}$$

By using the above transformation, the corresponding optimal state equation and the optimal defense strategy can be re-written as follows:

$$dx_i^*(t) = \left[\Big(a_i - \beta_i^{-1} b_i^2 V_i(t)\Big) x_i^*(t) + \beta_i^{-1} b_i^2 \varphi_i(t) + c_i \|x_i^*(t) - Ax^N(t)\|^2 + \Big(c - \beta_i^{-1}\lambda_i\Big) V_i(t)\right] dt \tag{13}$$

$$d\varphi_i(t) = \left[\Big(a_i - \beta_i^{-1} b_i^2 V_i(t)\Big)\varphi_i(t) - \phi_i A z(t) - V_i(t)\Big(\beta_i^{-1}\lambda - c\Big) u_0(t)\right] dt \tag{14}$$

where $z(t) = \lim_{N\to\infty} x^N(t)$, $x_i^*(0) = x_i(0)$, $\varphi_i(T) = 0$. The corresponding optimal defense strategy with state feedback representation is given by

$$u_i^*(t) = -\beta_i^{-1} V_i(t) b_i x_i^*(t) + \beta_i^{-1} b_i \phi_i - \beta_i^{-1}\lambda_i u_0(t) \tag{15}$$

Hence, for each defender, Equations (5) and (11) are both the optimal defense strategy for defenders and the latter is with the optimal state feedback representation. Meanwhile, $\varphi_i(t)$ is decoupled from $x_i^*(t)$, and Equation (10) has a unique solution with $V_i(t) \geq 0$ and $V_i(T) = 0$.

4.2. Optimality for the N Defenders: ε-Nash Equilibrium

In edge computing with large nodes, each defender node has the same system and it influences the choice of the strategy of another defender through the mean-field term. We can discuss the mean-field equilibrium in this case. We apply the optimal strategy (5) and the associated optimal state trajectory (6) to the N defenders. Let $z(t) = \lim_{N\to\infty} x^N(t)$, and $p(t) = \lim_{N\to\infty} p^N(t)$; hence, we have the following differential equations:

$$dz(t) = \left[\alpha_i z(t) + b_i\Big(\beta_i^{-1} p(t) b_i - \beta_i^{-1}\lambda_i u_0(t)\Big) + c_i\|\bar{z}(t) - Az(t)\|^2 + c u_0(t)\right] dt \tag{16}$$

$$dp(t) = [a_i p(t) + \alpha_i(\bar{z}(t) - Az(t))] dt \tag{17}$$

where $\bar{z}(t) = \lim_{N\to\infty} x_i^{*N}(t)$, $p(T) = 0$, and $E[x_0(0)] = x_0$. With the equations given in (13) and (14), the above equivalent representation can be re-written as

$$dz(t) = \Big[\Big(a_i - \beta_i^{-1}b_i^2V_i(t)\Big)z(t) + \beta_i^{-1}b_i^2\varphi(t) + c_i\|z(t) - Az(t)\|^2 + \Big(c - \beta_i^{-1}\lambda_i\Big)V_i(t)\Big]dt \tag{18}$$

$$d\varphi(t) = \Big[\Big(a_i - \beta_i^{-1}b_i^2V_i(t)\Big)\varphi(t) - \phi_iAz(t) - V_i(t)\Big(\beta_i^{-1}\lambda - c\Big)u_0(t)\Big]dt \tag{19}$$

where $\varphi(t) = \lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N}\varphi_i(t)$ and $\varphi(T) = 0$. While the pair (x_i^*, u_i^*) is the optimal solution of the game, (z, p) has a unique solution. Moreover, if the number of defenders N is large enough, we will obtain the mean-field approximate equilibrium solution, which is dependent on the strategy of the attacker.

Definition 1. *For any strategy $u_0(t)$, the strategy set $U = \{u_1(t), u_2(t), \cdots, u_N(t)\}$ is called to satisfy an ε-Nash equilibrium with respect to the cost J_i for any i, if there exists$\varepsilon_1 \geq 0$ such that for each defender i, we have*

$$J_i\big(u_i^*, u_{-i}^*, u_0\big) \leq \inf_{u_i\in U_i(u_0)} J_i\big(u_i, u_{-i}^*, u_0\big) + \varepsilon_1 \tag{20}$$

Theorem 1. *For any strategy of the attacker, we have*

$$\sup_{0\leq t\leq T} E|x^*(t) - z(t)|^2 = O\Big(\frac{1}{N}\Big) \tag{21}$$

$$\big|J_i\big(u_i^*, u_{-i}^*, u_0\big) - J_i\big(u_i, u_{-i}^*, u_0\big)\big| = O\Big(\frac{1}{\sqrt{N}} + \frac{1}{N}\Big) \tag{22}$$

Moreover, we have

$$E\int_0^T \|x^*(t) - z(t)\|^2 = O\Big(\frac{1}{N}\Big) \tag{23}$$

Proof. We prove the first statement (22) because the second representation (23) can be proved similarly. By the state trajectory (16) and Gronwall's inequality, we have

$$E|x^*(t) - z(t)|^2 \sim E\left|\int_0^T (a_i - \alpha_i)(x^*(t) - z(t))dt\right| = O\Big(\frac{1}{N}\Big) \tag{24}$$

Thus, (21) is obtained.

Applying Cauchy–Schwarz inequality, we have

$$\begin{aligned}
&\big|J_i\big(u_i^*, u_{-i}^*, u_0\big) - J_i\big(u_i, u_{-i}^*, u_0\big)\big| \\
&= \Big|E\textstyle\int_0^T\Big[\|Ax^N(t) - Az(t)\|^2 + \big(x_i^*(t) - z(t)\big)\alpha_i\big(Ax^N(t) - Az(t)\big)\Big]dt\Big| \\
&\leq \alpha_i\|A\|\Big(E\textstyle\int_0^T\|x_i^*(t) - z(t)\|^2dt\Big)^{\frac{1}{2}} + O\Big(\frac{1}{N}\Big) \\
&= O\Big(\frac{1}{\sqrt{N}} + \frac{1}{N}\Big)
\end{aligned} \tag{25}$$

Hence, we obtained the ε-Nash equilibrium for any defender i, $1 \leq i \leq N$, that is,

$$J_i\big(u_i^*(t), u_{-i}^*(t), u_0(t)\big) \leq \inf_{u_i} J_i\big(u_i(t), u_{-i}^*(t), u_0(t)\big) + \varepsilon_1 \tag{26}$$

where $\varepsilon_1 = O\Big(\frac{1}{\sqrt{N}} + \frac{1}{N}\Big)$. □

4.3. Mean-Field Equilibrium of Attacker

In this section, we discuss the equilibrium problem faced by the attacker and try to obtain the corresponding optimal strategy. The local optimal solution will be analyzed and an approximation mean-field solution will be obtained.

Due to the nature of the mean-field game under consideration, the attacker aims to minimize the following equation:

$$J_0(x_0, u_i, u_0) = E\int_0^T \Big(\alpha_0\|x_0(t) - z(t)\|^2 + \beta_0\|u_0(t)\|^2 + \gamma_i u_i(t)\Big)dt \tag{27}$$

subject to the attacker's state equation:

$$dx_0(t) = \left[a_0 x_0(t) + b_0 u_0(t) + \sum_{i=1}^{N} \kappa_i\Big(\beta_i^{-1} p_i(t) b_i - \beta_i^{-1}\lambda_i u_0(t)\Big)\right]dt \tag{28}$$

and the mean-field approximation constraint:

$$dz(t) = \Big[\alpha_i z(t) + b_i\Big(\beta_i^{-1} p(t) b_i - \beta_i^{-1}\lambda_i u_0(t)\Big) + c_i\|z(t) - Az(t)\|^2 + c u_0(t)\Big]dt \tag{29}$$

$$dp(t) = [a_i p(t) + \alpha_0(z(t) - Az(t))]dt \tag{30}$$

where $p(T) = 0$, $E[x_0(0)] = x_0$, and $E\Big[\|x_0(0)\|^2\Big] < \infty$. In (27), the mean-field term is replaced with the approximated term $z(t)$, which is dependent on the strategy of the attacker $u_0(t)$ as can be obtained from (29). Note that the mean-field game equilibrium problem for the defenders has been discussed by an approximated condition. Since the optimization problem for the attacker (27) has the initial and boundary conditions, it is much more tractable than the control problem of defenders. Based on the mean-field approximation problem in Section 4, the mean-field constraints (29) and (30) can be replaced by

$$dz(t) = \Big[\Big(a_i - \beta_i^{-1} b_i^2 V_i(t)\Big)z(t) + \beta_i^{-1} b_i^2 \varphi(t) + c_i\|\bar{z}(t) - Az(t)\|^2 + \Big(c - \beta_i^{-1}\lambda_i\Big)V_i(t)\Big]dt \tag{31}$$

$$d\varphi(t) = \Big[\Big(a_i - \beta_i^{-1} b_i^2 V_i(t)\Big)\varphi(t) - \phi_i A z(t) - V_i(t)\Big(\beta_i^{-1}\lambda - c\Big)u_0(t)\Big]dt \tag{32}$$

where $z(0) = x_0$ and $\varphi(T) = 0$.

Proposition 2. *For the optimal attack problem for $u_0(t)$, the pair (x_0^*, u_0^*) is the optimal solution for the game model* (2) *and* (4) *if and only if*

$$u_0^*(t) = -\beta_0^{-1} p(t) b_0 + \beta_0^{-1}\,\rho_0(t)\,\textstyle\sum_{i=1}^{N}\beta_i^{-1}\lambda_i^2 - \rho_1(t)\,\beta_0^{-1}\textstyle\sum_{i=1}^{N}\beta_i^{-1} b_i\,\lambda_i \tag{33}$$

where $(x_0^*, \rho_0, \rho_1)$is a solution to the equation as follows:

$$dx_0^*(t) = \Big[a_0 x_0^*(t) + b_0 u_0^*(t) + \textstyle\sum_{i=1}^{N}\lambda_i\Big(\beta_i^{-1} p(t) b_i - \beta_i^{-1}\,u_0^*(t)\Big)\Big]dt \tag{34}$$

$$d\rho_0(t) = \left[-a_0\rho_0(t) + c_0(Az(t) - x_0^*(t)) + \sum_{i=1}^{N}\lambda_i\rho_1(t)\right]dt \tag{35}$$

$$d\rho_1(t) = \Big[a_i\rho_1(t) + b_i\Big(\beta_i^{-1} p(t) b_i - \beta_i^{-1}\lambda_i u_0^*(t)\Big) + c_i\|\bar{z}(t) - Az(t)\|^2 + c u_0^*(t)\Big]dt \tag{36}$$

$$dp(t) = [-a_0 p(t) + \alpha_0(x_0^*(t) - Az(t))]dt \tag{37}$$

where $x_0(0) = x_0$, $p(T) = 0$, $\rho_0(T) = 0$, $\rho_1(0) = 0$, and $z(0) = x_0$.

4.4. Optimality for the Attacker: The ε-Nash Equilibrium

In the edge computing environment, if the defenders obtain the optimal attacker strategy, the defense strategies can obtain an approximated Stackelberg equilibrium solution. The definition is given as follows:

Definition 2. *The set of strategies* $\{u_0^*, u_i(u_0^*), \cdots, u_N(u_0^*) | i = 1, 2, \cdots, N\}$ *satisfies an* ε_2*-Nash equilibrium concerning the cost* J_0*, if there exists* $\varepsilon_2 > 0$*, such that we have*

$$J_0(u_0^*, u_i(u_0^*)) \leq \inf_{u_0} J_0(u_0, u_i) + \varepsilon_2 \tag{38}$$

Theorem 2. *For the optimal strategies* $\{u_0^*, u_i(u_0^*), \cdots, u_N(u_0^*) | i = 1, 2, \cdots, N\}$ *, we have*

$$J_0(u_0^*, u_i(u_0^*)) \leq \inf_{u_0} J_0(u_0, u_{-i}(u_0^*)) + \varepsilon_2 \tag{39}$$

Proof. Similar to the Proof of Theorem 1, and due to the fact that $E\int_0^T \|x_0(t)\|^2 dt < \infty$, we have

$$\begin{aligned} & J_0(u_0^*, u_i(u_0^*)) - J_0(u_0, u_{-i}(u_0^*)) \\ & \leq E\left|\int_0^T (x_0(t) - z(t))\alpha_0\left(Ax^N(t) - Az(t)\right)\right| dt \\ & \leq |\alpha_0||A|\left(E\int_0^T \|x_0(t) - z(t)\|^2 dt\right)^{\frac{1}{2}} \times \left(E\int_0^T \|x^N(t) - z(t)\|^2 dt\right)^{\frac{1}{2}} \\ & = O\left(\frac{1}{\sqrt{N}}\right) \end{aligned} \tag{40}$$

This completes the proof. □

4.5. Mean-Field Game Equilibrium Algorithm

This subsection shows the implementation of the mean-field game equilibrium algorithm for the proposed model, which is given in Algorithm 1. The equilibrium algorithm can be divided into the defense section and the attack section. Specifically, we calculate the optimal strategies and the corresponding state trajectories for defenders and attackers separately from the mean-field game model. Since the objective functions are quadratic, the solutions can be given based on the Stackelberg game theory, and the complexity of the mean-field equilibrium algorithm is $O(1/\sqrt{n})$. The algorithm process can be described in Algorithm 1 and Figure 2.

Algorithm 1. Mean-field game equilibrium algorithm

Input: the number of defenders N and the initial state x_0, x_{i0}.
Output: the optimal strategies u_i^* and u_0^*.
1. Set up the parameters $\alpha_i, \beta_i, \lambda_i, a_i, b_i, c_i, a_0, b_0, u_0,$ and c.
2. The defenders detect attack behavior.
3. Start the mean-field game for defenders.
4. **For** t = 1 to T
5. Calculate optimal strategies for the defenders based on Equations (11)–(15).
6. Set up the objective function J_i^* and the state trajectory x_i^*.
7. Calculate the optimal strategy for the attacker based on Equations (33)–(37).
8. Set up the objective function J_0^* and the state trajectory x_0^*.
9. **End.**
10. Return the optimal strategies u_i^* and u_0^*.

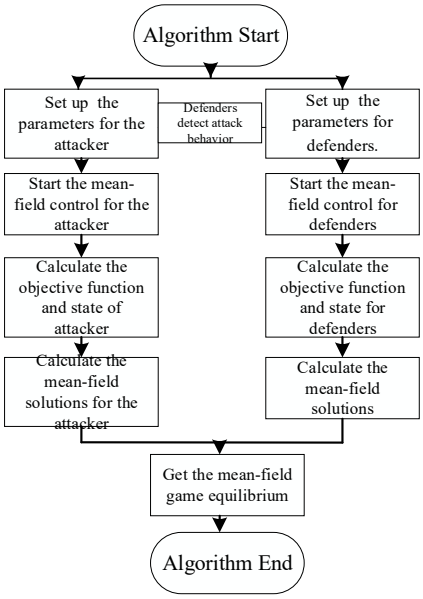

Figure 2. The procedure of the mean-field game algorithm.

5. Numerical Simulation

This section provides the simulation results to illustrate the dynamic evolution of the defense strategy of the defenders and the trajectory of the attackers based on the proposed mean-field Stackelberg game model. We first consider all the defenders as heterogeneous followers who share the same parameters and then discuss the heterogeneous case with $N = 10,000$. Each defender tries to obtain the optimal defense strategy to minimize the cost given in Equation (3). In Section 4.1, we obtained the optimal defense strategy for edge device i (5), $1 \leq i \leq N$, and in Section 4.3, we obtained the optimal attack strategy (33). We assume that the coefficients are within the range of 0 to 1. We presume that the simulation time is T = 10 min. The rest of the related simulation parameters are given in Table 1.

Table 1. Simulation parameters.

a	A	a_0	b	b_0	c	c_0	α	β	α_0	β_0	γ	λ
0.38	0.73	0.26	0.3	0.12	0.07	0.51	0.4	0.5	0.93	0.24	0.62	0.52
0.4		0.3		0.22		0.3	0.96			0.68	0.23	
0.14		0.4		0.7		0.3	0.55			0.4	0.5	

a	A	a_0	b	b_0	c	c_0	α	β	α_0	β_0	γ	λ
0.38	0.73	0.26	0.3	0.12	0.07	0.51	0.4	0.5	0.93	0.24	0.62	0.52
0.4		0.3		0.22		0.3	0.96			0.68	0.23	
0.14		0.4		0.7		0.3	0.55			0.4	0.5	

The evolution of the optimal defense strategies for any three defenders is shown in Figure 3. At the beginning of the attack, the defense level gradually increases as the defense mechanism responds and then stabilizes. The result indicates that the defenders respond to defense mechanisms to improve their defense when detecting attacks. Related to the defense strategy, the resource consumption for the defenders is given in Figure 4. It shows that the value of $x_i(t)$ gradually rises and then declines during the start of the attack, and finally, the value eventually reaches a stable range. When the defense mechanism is activated, it requires more resources for the edge devices. As a result, the node reduces the additional overhead of the computational task. When the level of offensive defense decreases, the resource consumption level starts to decrease and fluctuates within a certain range to maintain the computational requirements of the task.

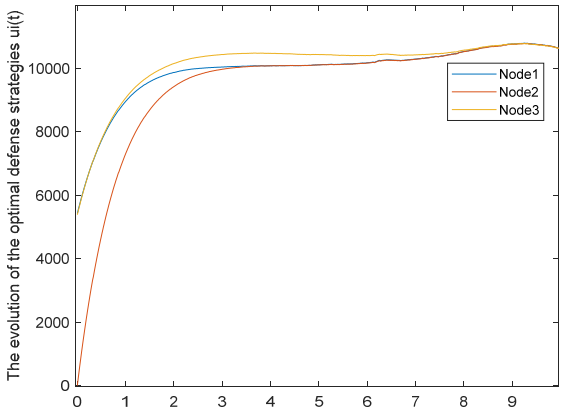

Figure 3. The evolution of the defense strategy.

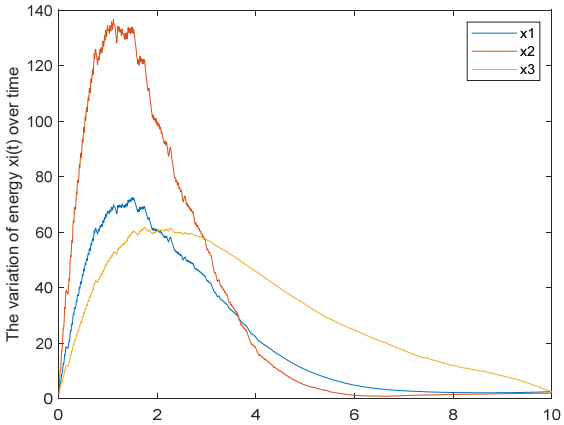

Figure 4. The optimal resource consumption state of defenders.

To ensure maximum security, each edge device will adopt its optimal defense level. In this framework, the number of attackers gradually decreases over time, which is shown in Figure 5. Figure 6 shows the evolution of the level of attack. At the beginning of the game, the intensity of the attack is high and continues to increase with time. Then, the intensity of the attack begins to decrease because the defense mechanism has been activated. The result shows that the intensity of the attack reduces rapidly when effective defense strategies are implemented. Ultimately, there is a slight variation in attack intensity within a specific range due to the underlying attack behavior in edge devices.

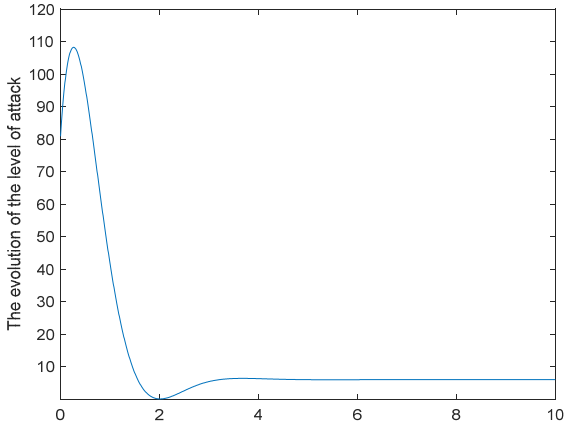

Figure 5. The evolution of the number of attackers.

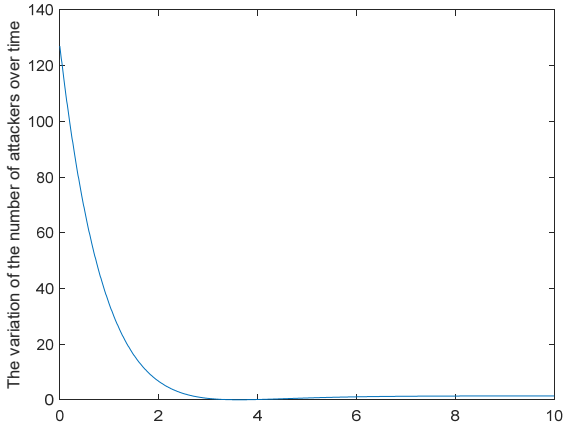

Figure 6. The evolution of the attack level.

We compare the resource consumption level of the proposed model and the energy optimization strategy [28] in Figure 7. As shown in Figure 7, the proposed scheme consumes more energy than the energy-optimized strategy at the beginning because of the level of attacks, but then the resource consumption level is gradually reduced, which indicates that the node has an optimal strategy with a minimum resource consumption at this time.

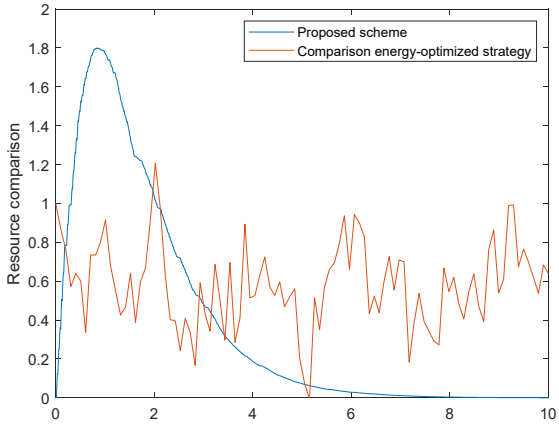

Figure 7. Resource consumption level comparison between the proposed scheme and the energy-optimized strategy.

6. Conclusions

In this article, we focused on a security strategy with limited resources in edge computing systems. We proposed a mean-field Stackelberg game-based model to optimize the defense strategies and minimize the cost of the defense mechanisms for defenders. The analysis developed in this model focused on scenarios with one attacker and multiple defenders. The attacker first chooses and then announces the optimal strategy to the defenders. Each defender will choose its optimal defense strategy to minimize the loss based on the leader's observed strategy. We achieved the optimal strategies for the defenders and attackers by solving the local optimal control problem. Using the mean-field approximation, we also determined the corresponding optimal consumption of resources of the defenders. We demonstrated that the optimal local control solutions for the defenders and attackers constitute an $(\varepsilon_1, \varepsilon_2)$-Nash equilibrium with the approximated mean-field equilibrium, where $(\varepsilon_1, \varepsilon_2)$ converges to zero as $N \to \infty$. Finally, we compared the proposed model with another scheme. The simulation results illustrated the dynamic evolution of the defense strategy given the optimal trajectory of the attackers.

In this paper, we considered the number of attackers as one player, and we evaluated the proposed model through numerical simulation. In future work, we will extend the

proposed mean-field game model to problems with multiple attackers and defenders. In these cases, the optimal control problems of the attackers will be more complex due to the multiple influences on the mean-field behavior, and we will evaluate the game model in the real edge computing environment.

Author Contributions: L.M., writing draft manuscript and game model and performance; S.L. and B.L., simulations and the objective function; X.W., project management; and all authors contributed to system analysis, simulations, and the writing of this paper. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Natural Science Foundation of Ningxia (No. 2021AAC03068 and No. 2023AAC05010), the Key R&D Program of Ningxia (No. 2021BEB04004), the National Natural Science Foundation of China (No. 62362056), and the Henan Province science and technology research project (No. 232102211087).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors would like to thank the editor and the reviewers for their valuable comments and suggestions that improved the quality of this paper.

Conflicts of Interest: The authors declare no conflicts of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Duan, S.; Wang, D.; Ren, J.; Lyu, F.; Zhang, Y.; Wu, H.; Shen, X. Distributed artificial intelligence empowered by end-edge-cloud computing: A survey. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 591–624. [CrossRef]
2. Wang, X.; Li, J.; Ning, Z.; Song, Q.; Guo, L.; Guo, S.; Obaidat, M.S. Wireless powered mobile edge computing networks: A survey. *ACM Comput. Surv.* **2023**, *55*, 1–37. [CrossRef]
3. Ahmad, S.; Shakeel, I.; Mehfuz, S.; Ahmad, J. Deep learning models for cloud, edge, fog, and IoT computing paradigms: Survey, recent advances, and future directions. *Comput. Sci. Rev.* **2023**, *49*, 100568. [CrossRef]
4. Abkenar, F.S.; Ramezani, P.; Iranmanesh, S.; Murali, S.; Chulerttiyawong, D.; Wan, X.; Jamalipour, A.; Raad, R. A Survey on Mobility of Edge Computing Networks in IoT: State-of-the-Art, Architectures, and Challenges. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 2329–2365. [CrossRef]
5. Zhao, N.; Du, W.; Ren, F.; Pei, Y.; Liang, Y.-C.; Niyato, D. Joint task offloading, resource sharing and computation incentive for edge computing networks. *IEEE Commun. Lett.* **2022**, *27*, 258–262. [CrossRef]
6. Tütüncüoğlu, F.; Dán, G. Optimal service caching and pricing in edge computing: A bayesian gaussian process bandit approach. *IEEE Trans. Mob. Comput.* **2024**, *23*, 705–718. [CrossRef]
7. Zhang, H.; Wang, J.; Zhang, H.; Bu, C. Security computing resource allocation based on deep reinforcement learning in serverless multi-cloud edge computing. *Future Gener. Comput. Syst.* **2024**, *151*, 152–161. [CrossRef]
8. He, Z.; Yin, J.; Wang, Y.; Gui, G.; Bamidele, A.; Tomoaki, O.; Haris, G.; Hikmet, S. Edge device identification based on federated learning and network traffic feature engineering. *IEEE Trans. Cogn. Commun. Netw.* **2022**, *8*, 1898–1909. [CrossRef]
9. Nencioni, G.; Garroppo, R.G.; Olimid, R.F. 5G Multi-access Edge Computing: A Survey on Security, Dependability, and Performance. *IEEE Access* **2023**, *11*, 63496–63533. [CrossRef]
10. Lasry, J.M.; Lions, P.L. Mean field games. *Jpn. J. Math.* **2007**, *2*, 229–260. [CrossRef]
11. Bensoussan, A.; Frehse, J.; Yam, P. *Mean Field Games and Mean Field Type Control Theory*; Springer: New York, NY, USA, 2013; p. 113.
12. Moon, J.; Yang, H.J. Linear-quadratic time-inconsistent mean-field type Stackelberg differential games: Time-consistent open-loop solutions. *IEEE Trans. Autom. Control* **2020**, *66*, 375–382. [CrossRef]
13. Lin, K.; Liu, J.; Han, G. AI-Based Mean Field Game against Resource-Consuming Attacks in Edge Computing. *ACM Trans. Sens. Netw.* **2022**, *18*, 52. [CrossRef]
14. Zhang, W.; Peng, C. Indefinite Mean-Field Stochastic Cooperative Linear-Quadratic Dynamic Difference Game with Its Application to the Network Security Model. *IEEE Trans. Cybern.* **2022**, *52*, 11805–11818. [CrossRef] [PubMed]
15. Alwarafy, A.; Al-Thelaya, K.A.; Abdallah, M.; Schneider, J.; Hamdi, M. A survey on security and privacy issues in edge-computing-assisted internet of things. *IEEE Internet Things J.* **2020**, *8*, 4004–4022. [CrossRef]
16. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A survey of security in cloud, edge, and fog computing. *Sensors* **2022**, *22*, 927. [CrossRef] [PubMed]

17. Wang, C.; Yuan, Z.; Zhou, P.; Xu, Z.; Li, R.; Wu, D.O. The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective. *IEEE Internet Things J.* **2023**, *10*, 22008–22032. [CrossRef]
18. Li, H.; Yang, C.; Wang, L.; Ansari, N.; Tang, D.; Hang, X.; Xu, Z.; Hu, D. A cooperative defense framework against application-level DDoS attacks on mobile edge computing services. *IEEE Trans. Mob. Comput.* **2021**, *22*, 1–18. [CrossRef]
19. Myneni, S.; Chowdhary, A.; Huang, D.; Alshamrani, A. SmartDefense: A distributed deep defense against DDoS attacks with edge computing. *Comput. Netw.* **2022**, *209*, 108874. [CrossRef]
20. Uddin, R.; Kumar SA, P.; Chamola, V. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. *Ad Hoc Netw.* **2024**, *152*, 103322. [CrossRef]
21. Zhou, H.; Zheng, Y.; Jia, X.; Shu, J. Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN. *Comput. Netw.* **2023**, *225*, 109642. [CrossRef]
22. Wang, J.; Wei, X.; Fan, J.; Duan, Q.; Liu, J.; Wang, Y. Request pattern change-based cache pollution attack detection and defense in edge computing. *Digit. Commun. Netw.* **2023**, *9*, 1212–1220. [CrossRef]
23. Qiu, H.; Zhang, T.; Zhang, T.; Li, H.; Qiu, M. DefQ: Defensive Quantization Against Inference Slow-Down Attack for Edge Computing. *IEEE Internet Things J.* **2023**, *10*, 3243. [CrossRef]
24. Hunt, K.; Zhuang, J. A review of attacker-defender games: Current state and paths forward. *Eur. J. Oper. Res.* **2024**, *313*, 301–417. [CrossRef]
25. Moura, J.; Hutchison, D. Game theory for multi-access edge computing: Survey, use cases, and future trends. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 260–288. [CrossRef]
26. He, Q.; Wang, C.; Cui, G.; Li, B.; Zhou, R.; Zhou, Q.; Yang, Y. A game-theoretical approach for mitigating edge DDoS attack. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 2333–2348. [CrossRef]
27. Wang, H.; An, J. Dynamic stochastic game-based security of edge computing based on blockchain. *J. Supercomput.* **2023**, *79*, 15894–15926. [CrossRef]
28. Miao, L.; Wang, L.; Li, S.; Xu, H.; Zhou, X. Optimal defense strategy based on the mean field game model for cyber security. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719831180. [CrossRef]
29. Qian, C.; Li, X.; Sun, N.; Tian, Y. Data security defense and algorithm for edge computing based on mean field game. *J. Cybersecur.* **2020**, *2*, 97. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.