Game-Theoretic Intrusion Prevention System Deployment for Mobile Edge Computing

Zhan-Lun Chang*, Chun-Yen Lee†, Chia-Hung Lin†, Chih-Yu Wang*, Hung-Yu Wei†
*Research Center for Information Technology Innovation, Academia Sinica
†Department of Electrical Engineering, National Taiwan University

***Abstract*—The network attack such as Distributed Denial-of-Service (DDoS) attack could be critical to latency-critical systems such as Mobile Edge Computing (MEC) as such attacks significantly increase the response delay of the victim service. Intrusion prevention system (IPS) is a promising solution to defend against such attacks, but there will be a trade-off between IPS deployment and application resource reservation as the deployment of IPS will reduce the number of computation resources for MEC applications. In this paper, we proposed a game-theoretic framework to study the joint computation resource allocation and IPS deployment in the MEC architecture. We study the pricing strategy of the MEC platform operator and purchase strategy of the application service provider, given the expected attack strength and end user demands. The best responses of both MPO and ASPs are derived theoretically to identify the Stackelberg equilibrium. The simulation results confirm that the proposed solutions significantly increase the social welfare of the system.**

I. Introduction

Mobile edge computing (MEC) is a promising technique to provide low-latency computing services. MEC platform providers (MPOs) deploy MEC servers at the network edge to provide computation resources for latency-critical tasks. Application service providers (ASPs) purchase those resources to deploy their applications for the end users. This architecture serves as the foundation of 5G/B5G killer applications such as Vehicle Automation, AR/VR, Smart City, etc.

Nevertheless, the network attack has been considered a serious threat to most network services. One of the most common attacks is the Distributed Denial-of-Service (DDoS) attack, which is performed by a significant number of infected devices to send fake requests to the victim service. The service requests of normal end users will be denied afterward due to that the victim service is out of resources. We observe that DDoS would be critical in the MEC architecture, as the available resource at the MEC servers are usually limited and cannot be expanded, while the deployed applications are mostly latency-critical and cannot tolerate service denial. A defensive measurement is necessary to guarantee the MEC service quality under the foreseen DDoS attacks.

Intrusion prevention system (IPS) is an effective measurement to identify and respond to the malicious behaviors performed by the attackers. In DDoS attack, for instance, an effective IPS instance can identify those malicious requests and isolate them from the service requests from the normal end users. Nevertheless, due to the deployment limitation of network edge environment, the candidate IPS for MEC is likely to be software-based, which means there will be a trade-off between IPS deployment and application resource reservation: the deployment of IPS will reduce the amount of computation resource for applications as some are occupied by the IPS instances, and thus the service latency may increase accordingly. On the other hand, lacking sufficient IPS will make the application vulnerable to DDoS attacks. Such a trade-off should be considered by the ASP when deploying its application at the MEC system.

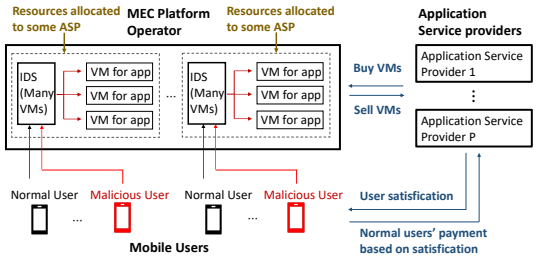

Fig. 1: System Architecture

In this paper, we proposed a game-theoretic framework to study the joint computation resource allocation and IPS deployment in the MEC architecture, from the economic perspective. Specifically, the MPO provides the MEC computation resource in the form of virtual machines with a price. The ASPs buy the VM from the MPO to deploy their applications, and the IPS can be optionally deployed if the DDoS attack is expected. In the proposed framework, we form the problem as a Stackelberg game to study the pricing strategy of the MPO and the optimal amount of VMs for application and IPS deployment of the ASPs. The best responses of both MPO and ASPs are derived theoretically to identify the Stackelberg equilibrium. The simulation results confirm that the proposed solutions significantly increase the social welfare of the system, that is, the total benefit of the whole MEC system.

The main contributions of this work are as follows:

1) To the best of our knowledge, we are the first group to study the DDoS attack and defense measurements in the MEC environment in a game-theoretic approach. This approach will help both MPO and ASPs to optimize their configurations in terms of their economic benefits.
2) We propose a flexible IPS deployment strategy to defend DDoS attack at MEC system by allowing ASPs to determine the resource allocation for IPS and main service

according to the expected attack strength.

3) The optimal strategies of both MPO and ASPs are analyzed through the proposed Stackelberg game model, which can be used to identify the equilibrium in polynomial time. The simulation results verify the effectiveness of the proposed solution in maintaining social welfare.

II. Related Work

Intrusion detection has been proposed with different approaches, including entropy-based method [1], reinforcement learning [2], and Deep Convolution Neural Network Q-learning model [3]. Several studies have been conducted to defend against DDoS attacks in the MEC environment. Alharbi *et al.* introduced NFV and edge computing architecture to design a two-stage DDoS mitigation network [4]. Mert *et al.* provided a similar paradigm that security function on edge computing defend the DDoS attack [5]. A multi-level DDoS mitigation framework [6] was proposed by Yan *et al.* to mitigate the DDoS attack to IoT. Shen *et al.* [7] implemented a Two-Phase DDoS detection system and showed that it can detect attacks with smaller overhead. Furthermore. Yang *et al.* devised a collaborative task offloading scheme to balance the task load between overloaded and underloaded cloudlets [8]. Li *et al.* explored the cooperative defense strategy and provided an online cooperative defense framework [9]. Introduced by Mtibaa *et al.* , detecting and isolating malicious nodes for D2D communication was proposed [10].

Distinguished from previous works, we focus on the resource allocation problems when defending DDoS attacks from the economic perspective of both MPO and ASPs. We use the Stackelberg game to formulate the relationships between MPO and ASPs and solve the optimization problems to maximize the utility of both sides under the DDoS attacks.

III. System Model

We consider a system with a MEC platform operator (MPO), a set of application service providers (ASPs) $\mathcal{I} = \{1, \cdots, I\}$, and end-users (EUs) (Fig 1). The MPO manages the computation resources in terms of virtual machines (VMs). The ASPs request for the MPO's VMs to deploy their applications. The goal of the MPO is to maximize its profit by finding the optimal unit selling price Ψ_m^v per VM. The ASPs determine the number of VMs to buy (denoted by z_i^v) from MPO to maximize their profit. Then, we denote the set of EUs associated with ASP $i \in \mathcal{I}$ as U_i and further categorize it into two kinds: normal users (NUs) U_i^n and malicious users (MUs) U_i^m. NUs seek the service from the ASPs with latency requirements, while the MUs aim to interrupt the service by sending fake tasks. Each EU $j \in \mathrm{U}_i$ has the Poisson task arrival rate λ_{ij}, latency requirement d_{ij}, and task size s_{ij}. We assume the EUs cannot handle these tasks locally because they rely on the computation resources and backbone model/database offered by the ASPs.

The ASPs utilize these purchased VMs to either run the application service for NUs or mitigate the DDoS security attacks from MUs. If ASPs devote most of their VMs to running the application service, they are prone to DDoS security attacks from MUs. The security threat would damage the quality of experience (QoE) of NUs and thus the revenue of ASPs. On the other hand, if the ASPs devote most of their VMs to mitigating the DDoS attack, the latency requirements of NUs may still not be satisfied if the available resource is not enough. Therefore, it is crucial to find an optimal resource allocation between running the application service and mitigating the DDoS attacks.

Specifically, the ASPs can intercept malicious requests by employing a software-based intrusion prevention system (IPS) [11]. The IPS of all ASPs monitors and filters all task requests, and all VMs devoted to running the application service process the filtered task requests. We assume the IPS can perfectly identify the normal task requests, but it may classify some malicious task requests as normal. The number of malicious requests the IPS filter can filter depends on the number of VMs the ASPs dedicate to the IPS. We use $H(\cdot)$ to represent the relationship between the quantity of intercepted malicious requests and the number of devoted VMs. $H(\cdot)$ is assumed to be non-decreasing and concave. Also, $H(0) = 0$. In this paper, we consider a linear function form of $H(x) = \eta x$, where η denotes the IPS efficiency.

We consider orthogonal frequency-division multiple access (OFDMA) system and thus the bandwidth of the edge servers whose computation resources are allocated to ASP i denoted by B_i can be divided into $|\mathrm{U}_i|$ sub-bands of size $W_i = B_i/|\mathrm{U}_i|$. Each EU $j \in \mathrm{U}_i$ transmits the data at a dedicated sub-band to avoid interference. The maximum achievable uplink data transmission rate R_{ij} between ASP i and EU $j \in \mathrm{U}_i$ is

$$R_{ij} = W_i \cdot log_2\Big(1 + \frac{p_{ij} g_{ij}}{N_0}\Big), \tag{1}$$

where p_{ij} is the maximum transmission power of EU j in U_i, and g_{ij} denotes the uplink channel gain between ASP i and EU j. N_0 is the background noise power. The mean transmission time of workload consisting of tasks with size s_{ij} from EU $j \in \mathrm{U}_i$ to ASP i is

$$T_{ij}^t = \frac{\lambda_{ij} \cdot s_{ij}}{R_{ij}}. \tag{2}$$

The task arrival process at ASP i also follows the Poisson process according to the Poisson process's stationary property. Specifically, the mean arriving rate of the Poisson process at ASP i can be expressed as $\lambda_i = \sum_{j \in \mathrm{U}_i} \lambda_{ij}$ based on the superposition property of the Poisson process. Since the ASPs buy VMs from the MPO whose overall computation resources are still limited compared to the cloud platform, we model the meaning processing delay of all VMs purchased by ASPs using the $M/M/1$ queue. Each VM of MPO is homogeneous and can process f_m^v CPU cycles per second. As the average required CPU cyles for a task of ASP i may be different, the mean service rate of the queue at ASP i denoted by μ_i^v (in

task per second) is different for every ASP i. We denote the required CPU cycles of user $j \in \mathrm{U}_i$ as χ_{ij}. Thus, we have

$$\mu_i^v = f_m^v / (\frac{\sum_{j \in \mathrm{U}_i} \chi_{ij}}{|\mathrm{U}_i|}) \tag{3}$$

When ASP i buys z_i^v VMs from the MPO and devotes z_i^h to IPS, the mean processing delay is

$$T_i^p(z_i^v, z_i^h) = \frac{1}{(z_i^v - z_i^h)\mu_i^v - \big(\lambda_i - H(z_i^h)\big)} \tag{4}$$

The payment from NU $j \in \mathrm{U}_i^n$ to the ASP i depends on whether the latency requirements $d_{ij}\, \forall j \in \mathrm{U}_i^n$ are satisfied. NU $j \in \mathrm{U}_i^n$ pays a price Ψ_{ij} to ASP i only if latency requirements d_{ij} are met. The heterogeneity of the payment reflects the different characteristics of NUs. The MUs $j \in \mathrm{U}_i^m$, on the other hand, will not pay any money to the ASP i in any case. We represent the payment of EU $j \in \mathrm{U}_i$:

$$\mathcal{K}_{ij}(z_i^v, z_i^h) = \begin{cases} \Psi_{ij} & \text{if } T_{ij}^t + T_i^p(z_i^v, z_i^h) \le d_{ij},\ j \in \mathrm{U}_i^n \quad (5a) \\ 0 & \text{if } T_{ij}^t + T_i^p(z_i^v, z_i^h) > d_{ij},\ j \in \mathrm{U}_i^n \quad (5b) \\ 0 & j \in \mathrm{U}_i^m \quad (5c) \end{cases}$$

IV. Game Formulation

We model the interaction between MPO and ASPs as a two-stage single-leader-multi-followers Stackelberg game to capture the intrinsic hierarchy between MPO and ASPs and the influence between ASPs in the competition for the VMs.

In the proposed Stackelberg game, the MPO first decides the price per VM Ψ_m^v, and then the ASPs determine how many VMs to buy from MPO $z_i^v\, \forall i$. The MPO's selection of price per VM affects how many VMs those ASPs would buy, which in turn has an impact on the profit of the MPO. Due to the finite number of available VMs, the number of VMs one ASP can buy is influenced by the decisions of other ASPs. We illustrate the actions and utilities of MPO and ASPs and then formulate the optimization problems.

A. The Action and The Utility of ASPs

Given the MPO's price per VM Ψ_m^v, each ASP i decides the number of VMs to buy from the MPO z_i^v to maximize its profit, which is the revenue accrued from the NU $j \in \mathrm{U}_i^n$ minus the payment to the MPO for purchasing z_i^v VMs. We define the utility of ASP i when it purchases z_i^v VMs from MPO as the maximum expected profit across the different number of VMs dedicates to the IPS z_i^h with respect to the distribution of latency requirement d_{ij}. We assume that the latency requirements $d_{ij}\, \forall j \in \mathrm{U}_i$ of NUs served by ASP i follow the uniform distribution over the interval $[a_i, b_i]$ denoted by $\mathcal{U}(a_i, b_i)$. The utility of ASP i given Ψ_m^v is

$$Y_i(z_i^v|\Psi_m^v) \triangleq \max_{z_i^h} \mathsf{E}_{d_{ij}} \Big[\sum_{j \in \mathrm{U}_i^n} \mathcal{K}_{ij}(z_i^v, z_i^h) - \Psi_m^v z_i^v \Big] \tag{6}$$

$$= \max_{z_i^h} [\sum_{j \in \mathrm{U}_i^n} \Psi_{ij} (1 - \frac{T_{ij}^t + T_i^p(z_i^v, z_i^h) - a_i}{b_i - a_i}) - \Psi_m^v z_i^v] \tag{7}$$

$$\triangleq \max_{z_i^h} X_i(z_i^h|z_i^v, \Psi_m^v) \tag{8}$$

$\mathsf{E}_{d_{ij}}$ means taking expectation with respect to the distribution of d_{ij}. Given z_i^v, we have two constraints on z_i^h. First, the number of VMs dedicated to IPS z_i^h must be no larger than the number of purchased VMs z_i^v. Second, the mean service rate by the VMs dedicated to running the service must be higher than the mean arrival rate for EUs $j \in \mathrm{U}_i$ for a stable processing queue. To define the utility of ASP i when the purchased VMs from the MPO is z_i^v, we have to solve the following optimization problem.

$$\underset{z_i^h \in \mathbb{R}}{\text{maximize}} \quad X_i(z_i^h|z_i^v, \Psi_m^v) \tag{9a}$$

$$\text{subject to} \quad 0 \le z_i^h \le \xi_i z_i^v, \tag{9b}$$

$$0 < (z_i^v - z_i^h)\mu_i^v - \lambda_i + H(z_i^h) \tag{9c}$$

In (9b), we introduce $\xi_i \in [0, 1]$ as the upper bound of z_i^h to reserve computation resource for basic service. Similarly, in (9c), the service rate must exceed the arrival rate to make the queue stable. Showing the utility of the ASP i, $Y_i(z_i^v)$, is well-defined is equivalent to proving the optimization problem (9) has at least one solution, which can be proved by showing it is a convex optimization problem. The proof is omitted due to the page limitation. We then formulate the optimization problem of ASP i given the MPO's price per VM Ψ_m^v.

$$\underset{z_i^v \in \mathbb{R}}{\text{maximize}} \quad Y_i(z_i^v|\Psi_m^v) \tag{10a}$$

$$\text{subject to} \quad \lambda_i + \gamma_i \le z_i^v \mu_i^v, \tag{10b}$$

$$0 \le Y_i(z_i^v|\Psi_m^v) \tag{10c}$$

The constraint (10b) regulates that when the ASP i dedicates all purchased VMs to running the application service, the mean service rate must be larger than the mean arrival rate by at least γ_i, where $\gamma_i \ge 0$, as reserve computation resources for IPS.The constraint (10c) represents the individual rationality for every ASP. That is, when making the processing queue stable gives a negative utility, the ASPs would rather choose to end its service and receive zero utility. We denote the solution to (10) as $(z_i^v(\Psi_m^v))^*$ to emphasize the dependence on the MPO's price per VM Ψ_m^v.

B. The Action and The Utility of The MPO

The MPO chooses the price per VM Ψ_m^v to maximize its utility which is defined as the MPO's profit, which is its revenue minus the operating cost of the deployed VMs. The revenue of the MPO is the sum of payments from all ASPs. The cost for operating $\sum_{i \in \mathcal{I}} (z_i^v(\Psi_m^v))^*$ VMs is denoted as $C_m^v\big(\sum_{i \in \mathcal{I}} (z_i^v(\Psi_m^v))^*\big)$. The function $C_m^v(\cdot)$ is assumed to be convex and non-decreasing.We then denote the MPO's utility as $Y_m(\Psi_m^v)$ and formulate the MPO's optimization problem.

$$\underset{\Psi_m^v \in 0 \cup \mathbb{R}^+}{\text{maximize}} \quad \Psi_m^v \cdot \sum_{i \in \mathcal{I}} (z_i^v(\Psi_m^v))^* - C_m^v\big(\sum_{i \in \mathcal{I}} (z_i^v(\Psi_m^v))^*\big) \tag{11a}$$

$$\text{subject to} \quad \sum_{i \in \mathcal{I}} (z_i^v(\Psi_m^v))^* \le \mathcal{Q}_v \tag{11b}$$

The constraint (11b) mandates the maximum number of available VMs. The constraint (11b) imposes a lower bound for MPO's price per VM.

V. Stackelberg Equilibrium

We would leverage the backward induction principle to solve the formulated Stackelberg game to find the Stackelberg equilibrium. In this principle, we solve the followers' (ASPs') optimization problems first and then the leader's (MPO's) optimization problem based on responses of ASPs to the MPO's price per VM, i.e., $(z_i^v(\Psi_m^v))^* \, \forall i \in \mathcal{I}$.

A. ASP Optimization Problem

We analyze the solution process of the formulated Stackelberg game according to whether the solution to (9) is at the extreme point or boundary point of the constraint.

Case 1: The optimal point of (9) is the extreme point whose first derivative with respect to z_i^h equals zero.

However, this case doesn't happen with $H(x) = \eta x$. We explain the property in the following lemma.

Lemma 1. *$X_i(z_i^h|z_i^v, \Psi_m^v)$ doesn't have extreme point in feasible z_i^h if $H(x) = \eta x$.*

Proof. The derivative of $X_i(z_i^h|z_i^v, \Psi_m^v)$ with respect to z_i^h is

$$[(z_i^v - z_i^h) - \lambda_i + \eta z_i^h]^{-2} \cdot (-\mu_i^v + \eta) \tag{12}$$

Obviously, no matter what the value of z_i^h is, (12) equaling zero will never be satisfied. Therefore, the extreme point of (9a) does not exist in feasible z_i^h, so the maximum value of $X_1(z_i^h|z_i^v, \Psi_m^v)$ only happens at the boundary points. □

Case 2: The optimal point of (9) happens at the right boundary of (9b). That is, the ASP i's optimal number of VMs devoted to the IPS is

$$(z_i^h)^* = \xi_i z_i^v \tag{13}$$

When we substitute (13) into (4), the mean processing delay in this case denoted as $T_{i,2}^p(z_i^v) = [(1-\xi_i)z_i^v\mu_i^v - \big(\lambda_i - H(\xi_i z_i^v)\big)]^{-1}$ According to (7) and (8), the objective function (10a) becomes

$$Y_i^2(z_i^v|\Psi_m^v) \triangleq \sum_{j \in \mathrm{U}_i^n} \Psi_{ij}(1 - \frac{T_{ij}^t + T_{i,2}^p(z_i^v) - a_i}{b_i - a_i}) - \Psi_m^v z_i^v \tag{14}$$

We can characterize the solution to the optimization problem (10) when the objective function (10a) equals $Y_i^2(z_i^v|\Psi_m^v)$ in the following theorem with a specific form of $H(\cdot)$. Before stating the result, we define the feasible region of (10b) as Υ_i for ASP i while the feasible region of (10c) as Υ_i^2 when the $Y_i(z_i^v|\Psi_m^v)$ equals $Y_i^2(z_i^v|\Psi_m^v)$.

Theorem 1. *The solution to the optimization problem (10) when the objective function (10a) equals $Y_i^2(z_i^v|\Psi_m^v)$ and $H(x) = \eta x$ is $(z_{i,2}^v(\Psi_m^v))^*$, if $\Upsilon_i \cap \Upsilon_i^2 \neq \emptyset$*

$$= \begin{cases} \dfrac{\lambda_i + \gamma_i}{\mu_i^v} & (z_{i,2}^{v,e}(\Psi_m^v))^* < \frac{\lambda_i+\gamma_i}{\mu_i^v} \quad (15a) \\ (z_{i,2}^{v,e}(\Psi_m^v))^* & (z_{i,2}^{v,e}(\Psi_m^v))^* \geq \frac{\lambda_i+\gamma_i}{\mu_i^v} \quad (15b) \end{cases}$$

where

$$(z_{i,2}^{v,e}(\Psi_m^v))^* = \sqrt{\frac{\sum_{j \in \mathrm{U}_i^n} \Psi_{ij}}{(b_i - a_i)\Psi_m^v[(1-\xi_i)\mu_i^v + \xi_i\eta]}} + \frac{\lambda_i}{(1-\xi_i)\mu_i^v + \xi_i\eta} \tag{16}$$

and if $\Upsilon_i \cap \Upsilon_i^2 = \emptyset$

$$(z_{i,2}^v(\Psi_m^v))^* = 0 \tag{17}$$

The proof is omitted due to page limitation. A sketch of the proof is that we can first show that $Y_i^2(z_i^v|\Psi_m^v)$ is concave in feasible z_i^v. Then, we show the feasible region is a convex set. Finally, we provide case-by-case discussions to show the optimal solution in each sub-region.

From Theorem 1, we can obtain the MPO's price per VM Ψ_m^i which makes the ASP i's optimal response switch among (17), (15a) and (15b)by solving the Ψ_m^v that satisfies $Y_i^2(\frac{\lambda_i+\gamma_i}{\mu_i^v}|\Psi_m^v) = 0$ and $(z_{i,2}^{v,e}(\Psi_m^v))^* = \frac{\lambda_i+\gamma_i}{\mu_i^v}$.

$$\Psi_{m,2}^{i,z} = \sum_{j \in \mathrm{U}_i^n} \Psi_{ij}(1 - \frac{T_{ij}^t + T_{i,2}^p(\frac{\lambda_i+\gamma_i}{\mu_i^v}) - a_i}{b_i - a_i}) \times (\frac{\mu_i^v}{\lambda_i + \gamma_i}) \tag{18}$$

.

$$\Psi_{m,2}^{i,l} = \frac{\sum_{j \in \mathrm{U}_i^n} \Psi_{ij}}{(b_i - a_i)[(1-\xi_i)\mu_i^v + \xi_i\eta]} \times \big[\frac{\lambda_i + \gamma_i}{\mu_i^v} - \frac{\lambda_i}{(1-\xi_i)\mu_i^v + \xi_i\eta}\big]^{-2} \tag{19}$$

Case 3: The optimal point of (9) happens at the left boundary of (9b). That is, when the purchased number of VM is z_i^v, the ASP i's optimal number of VMs devoted to the IPS $(z_i^h)^*$ is

$$(z_i^h)^* = 0 \tag{20}$$

When we substitute (20) into (4), the mean processing delay denoted as $T_{i,3}^p(z_i^v) = [z_i^v\mu_i^v - \lambda_i]^{-1}$

According to (7) and (8), the objective function (10a) becomes

$$Y_i^3(z_i^v|\Psi_m^v) \triangleq \sum_{j \in \mathrm{U}_i^n} \Psi_{ij}(1 - \frac{T_{ij}^t + T_{i,3}^p(z_i^v) - a_i}{b_i - a_i}) - \Psi_m^v z_i^v \tag{21}$$

Similarly, We can characterize the solution to the optimization problem (10) when the objective function (10a) equals $Y_i^3(z_i^v|\Psi_m^v)$ in the following theorem with a specific form of $H(\cdot)$. Similarly in Case 2, we define the feasible region of (10c) as Υ_i^3 when the $Y_i(z_i^v|\Psi_m^v)$ equals $Y_i^3(z_i^v|\Psi_m^v)$.

Theorem 2. *The solution to the optimization problem (10) when the objective function (10a) equals $Y_i^3(z_i^v|\Psi_m^v)$ and $H(x) = \eta x$ is $(z_{i,3}^v(\Psi_m^v))^*$ and if $\Upsilon_i \cap \Upsilon_i^3 \neq \emptyset$*

$$= \begin{cases} \dfrac{\lambda_i + \gamma_i}{\mu_i^v} & (z_{i,3}^{v,e}(\Psi_m^v))^* < \frac{\lambda_i+\gamma_i}{\mu_i^v} \quad (22a) \\ (z_{i,3}^{v,e}(\Psi_m^v))^* & (z_{i,3}^{v,e}(\Psi_m^v))^* \geq \frac{\lambda_i+\gamma_i}{\mu_i^v} \quad (22b) \end{cases}$$

where

$$(z_{i,3}^{v,e}(\Psi_m^v))^* = \sqrt{\frac{\sum_{j\in \mathrm{U}_i^n}\Psi_{ij}}{\mu_i^v(b_i-a_i)\Psi_m^v}} + \frac{\lambda_i}{\mu_i^v} \tag{23}$$

and if $\Upsilon_i \cap \Upsilon_i^3 = \emptyset$

$$(z_{i,3}^{v}(\Psi_m^v))^* = 0 \tag{24}$$

The proof follows the same flow as of Theorem 1.

From Theorem 2, we can obtain the MPO's price per VM Ψ_m^i which makes the ASP i's optimal response switch among (24), (22a) and (22b) by solving the Ψ_m^v that satisfies $Y_i^3(\frac{\lambda_i+\gamma_i}{\mu_i^v}|\Psi_m^v) = 0$ and $(z_{i,3}^{v,e}(\Psi_m^v))^* = \frac{\lambda_i+\gamma_i}{\mu_i^v}$.

$$\Psi_{m,3}^{i,z} = \sum_{j\in \mathrm{U}_i^n}\Psi_{ij}\left(1 - \frac{T_{ij}^t + T_{i,3}^p(\frac{\lambda_i+\gamma_i}{\mu_i^v}) - a_i}{b_i - a_i}\right) \times \left(\frac{\mu_i^v}{\lambda_i+\gamma_i}\right) \tag{25}$$

.

$$\Psi_{m,3}^{i,l} = \frac{\sum_{j\in \mathrm{U}_i^n}\Psi_{ij}}{(b_i-a_i)} \times \left[\frac{\lambda_i+\gamma_i}{\mu_i^v} - \frac{\lambda_i}{\mu_i^v}\right]^{-2} \tag{26}$$

B. MPO Optimization Problem

In this section, we solve the optimization problem (11). For every ASP, the optimal solution is either Case 2 or Case 3, that is, $\mathcal{I}_{case2} \cup \mathcal{I}_{case3} = \mathcal{I}$, where $\mathcal{I}_{case2}$ indicates the ASP set which its optimal solution is in Case 2, and $\mathcal{I}_{case3}$ indicates the ASP set which its optimal solution is in Case 3. The boundary set of all ASP is $\{\Psi_{m,2}^{i,z}, \Psi_{m,2}^{i,l}, i \in \mathcal{I}_{case2}\} \cup \{\Psi_{m,3}^{j,z}, \Psi_{m,3}^{j,l}, j \in \mathcal{I}_{case3}\}$. The boundary sequence partitions the space of the MPO's price per VM Ψ_m^v into $2I+1$ intervals.

$$0 \cup \mathbb{R}^+ = \mathcal{M}^1 \cup \mathcal{M}^2 \cdots \cup \mathcal{M}^{2I+1} \tag{27}$$

Within each interval $\mathcal{M}^k, \forall k \in \{1, \cdots, 2I+1\}$, we define four sets of ASP i that has different optimal responses.

$$\begin{aligned}
\Omega^{k,z} &= \{i \in \mathcal{I} | (z_i^v(\Psi_m^v))^* = 0\} \\
\Omega^{k,l} &= \{i \in \mathcal{I} | (z_i^v(\Psi_m^v))^* = \frac{\lambda_i+\gamma_i}{\mu_i^v}\} \\
\Omega_2^{k,e} &= \{i \in \mathcal{I}_{case2} | (z_i^v(\Psi_m^v))^* = (z_{i,2}^{v,e}(\Psi_m^v))^*\} \\
\Omega_3^{k,e} &= \{i \in \mathcal{I}_{case3} | (z_i^v(\Psi_m^v))^* = (z_{i,3}^{v,e}(\Psi_m^v))^*\}
\end{aligned} \tag{28}$$

These four sets form a partition of the all ASPs. That is, $\mathcal{I} = \Omega^{k,z} \cup \Omega^{k,l} \cup \Omega_2^{k,e} \cup \Omega_3^{k,e}, \forall k \in \{1, \cdots, 2I+1\}$. The total number of VMs bought by the ASPs within each interval $\mathcal{M}^k, \forall k \in \{1, \cdots, 2I+1\}$ can be expressed

$$\begin{aligned}
\sum_{i\in\mathcal{I}}(z_i^v(\Psi_m^v))^* &= \sum_{i\in\Omega^{k,l}}\frac{\lambda_i+\gamma_i}{\mu_i^v} \\
&+ \sum_{i\in\Omega_2^{k,e}}(z_{i,2}^{v,e}(\Psi_m^v))^* + \sum_{i\in\Omega_3^{k,e}}(z_{i,3}^{v,e}(\Psi_m^v))^*
\end{aligned} \tag{29}$$

Finally, the MPO's optimization problem in each interval $\mathcal{M}^k, \forall k \in \{1, \cdots, 2I+1\}$ is

$$\underset{\Psi_m^v \in \mathcal{M}^k}{\text{maximize}} \quad \Psi_m^v \cdot \sum_{i\in\mathcal{I}}(z_i^v(\Psi_m^v))^* - C_m^v\Big(\sum_{i\in\mathcal{I}}(z_i^v(\Psi_m^v))^*\Big) \tag{30a}$$

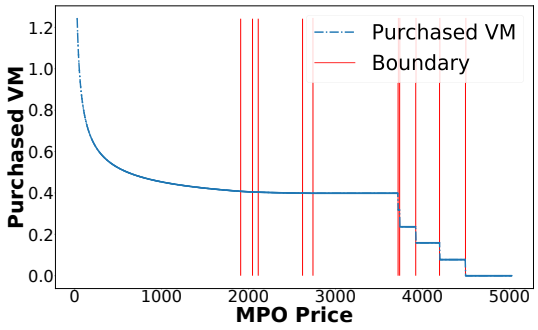

Fig. 2: Total Purchased VM v.s. MPO Price

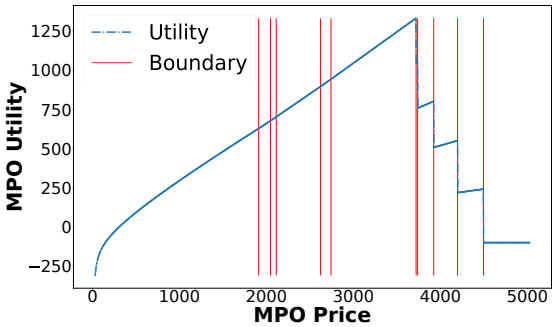

Fig. 3: MPO Utility v.s. MPO Price

$$\text{subject to} \quad \sum_{i\in\mathcal{I}}(z_i^v(\Psi_m^v))^* \le \mathcal{Q}_v \tag{30b}$$

In each interval $\mathcal{M}^k, \forall k \in \{1, \cdots, 2I+1\}$, the MPO's optimization problem (30) is a convex optimization problem. The optimal price per VM Ψ_m^v is one of the optimal prices in each $\mathcal{M}^k, \forall k \in \{1, \cdots, 2I+1\}$ that gives the highest utility.

By the above property, we can find the optimal price of VM for the MPO per interval. We then derive the optimal price Ψ_m^v in all regions for the MPO.

VI. Simulation

We evaluate the performance of the proposed Stackelberg equilibrium with simulations. We simulate a MEC system with one MPO and five ASPs. For the MPO, the CPU frequency per VM f_m^v is 0.25GHz, and the cost function is set to be $C_m^v(x) = 100e^x$. For each ASP, the bandwidth B_i is 20MHz, the transmission power p_i is 23dBm [12], the background noise power N_0 is -100dBm [13]. For path loss model, we use $g(d) = 22log_{10}(d) + 28 + 20log_{10}(f_c)$ [14], where d is the distance between EUs and ASPs, and f_c is the frequency band. As for other system parameters, ξ_i is 0.999, γ_i is 100, and the frequency band f_c is 2.1GHz.

For EUs, the distance between EU and ASP is uniformly chosen from 50m to 100m, the task size s_{ij} is uniformly chosen from 4kB to 5kB, the latency requirements of the EU are chosen uniformly between 5ms to 100ms, the required CPU cycles χ_{ij} are chosen uniform between 0.1 and 0.9 Megacycles, the arrival rate λ_{ij} is chosen uniformly between

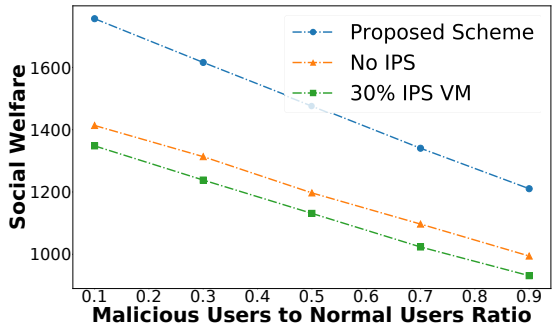

Fig. 4: Different Malicious Users to Normal Users Ratio

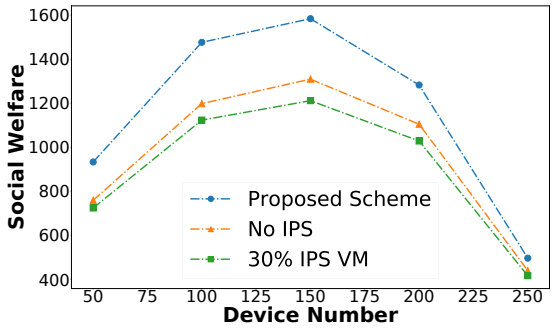

Fig. 5: Different Number of End users

1 and 3 [15], and the payments of the EUs Ψ_{ij} are chosen uniformly between 1 and 10.

If not specified, the ratio of malicious users to normal users is set to 0.5, and the number of EUs is set to 100 per ASP. The IPS efficiency η is set to be 5000.

We first verify the convexity of the MPO optimization problem. The boundaries of price interval have been plot and shown in Figure 2 and Figure 3. The ASP has the same optimal response in every interval. As the MPO price increases, the optimal responses by the ASPs changes from a decreasing, convex function ((Equation (16)) and (Equation (23))) to a constant. Moreover, the MPO utility shown in Figure 3 is a concave function in every interval.

Then, we compare the different IPS allocation schemes in scenarios of different malicious to normal users ratio. Three rules are compared: No IPS, 30% IPS VM., and Proposed scheme. As seen in Figure 4, when the ratio increases, the overall social welfare decreases regardless of the applied scheme due to the increased attacks. Nevertheless, the Proposed deployment reaches the highest social welfare compared with other baselines regardless of the ratio.

We further compare different IPS allocation schemes in scenarios of various numbers of end-users. As seen in Figure 5, when the number of devices increases, the social welfare increases initially, but then decreases after the device number exceeds 150. As the device number started to exceed the available resource the MEC server can handle, ASP cannot serve excess EUs in time, thus the social welfare drops. Nevertheless, the proposed scheme still has the highest social welfare compare with other baselines.

VII. Conclusion

In the paper, we proposed a flexible IPS deployment strategy for ASPs to determine the allocation of VM resources for IPS and services to mitigate the expected DDoS attacks. The joint optimization problem of ASP and MPO is formulated as a Stackelberg game to capture the hierarchy relationship. The optimal pricing strategy of MPO and the optimal amount of purchased VM along with the ratio of IPS VM for ASPs are derived. The simulation results verify the effectiveness of the proposed solution in maintaining the service quality and social welfare compared with other baseline schemes.

VIII. Acknowledgement

This work was supported by the Ministry of Science and Technology under Grant MOST 108-2628-E-001-003-MY3, MOST 109-2221-E-002-148-MY2 and MOST 109-2218-E-002-018- and the Academia Sinica under Thematic Research Grant AS-TP-110-M07-2.

References

[1] R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed ddos detection mechanism in software-defined networking," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 310–317.

[2] H. Zhang, J. Hao, and X. Li, "A method for deploying distributed denial of service attack defense strategies on edge servers using reinforcement learning," *IEEE Access*, vol. 8, pp. 78 482–78 491, 2020.

[3] Z. Liu, X. Yin, and Y. Hu, "Cpss lr-ddos detection and defense in edge computing utilizing dcnn q-learning," *IEEE Access*, vol. 8, pp. 42 120–42 130, 2020.

[4] T. Alharbi, A. Aljuhani, and H. Liu, "Holistic ddos mitigation using nfv," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017, pp. 1–4.

[5] M. Özçelik, N. Chalabianloo, and G. Gür, "Software-defined edge defense against iot-based ddos," in *2017 IEEE International Conference on Computer and Information Technology (CIT)*, 2017, pp. 308–313.

[6] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level ddos mitigation framework for the industrial internet of things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 30–36, 2018.

[7] Y. Shen, C. Wu, D. Kong, and M. Yang, "Tpdd: A two-phase ddos detection system in software-defined networking," in *IEEE International Conference on Communications (ICC)*, 2020.

[8] N. Yang, X. Fan, D. Puthal, X. He, P. Nanda, and S. Guo, "A novel collaborative task offloading scheme for secure and sustainable mobile cloudlet networks," *IEEE Access*, vol. 6, pp. 44 175–44 189, 2018.

[9] H. Li and L. Wang, "Online orchestration of cooperative defense against ddos attacks for 5g mec," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–6.

[10] A. Mtibaa, K. Harras, and H. Alnuweiri, "Friend or foe? detecting and isolating malicious nodes in mobile edge computing platforms," in *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*, 2015, pp. 42–49.

[11] Open Information Security Foundation, "Suricata." [Online]. Available: https://github.com/OISF/suricata

[12] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception," 3GPP, Technical Specification (TS) 36.101, 4 2020, version 16.5.0.

[13] X. Chen, L. Jiao, W. Li, and X. Fu, "Efficient multi-user computation offloading for mobile-edge cloud computing," *IEEE/ACM Transactions on Networking*, vol. 24, no. 5, pp. 2795–2808, 2015.

[14] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects," 3GPP, Technical Report (TR) 36.814, 3 2017, version 9.2.0.

[15] Q. Fan and N. Ansari, "Application aware workload allocation for edge computing-based iot," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2146–2153, 2018.