Evolving Risk Management Against Advanced Persistent Threats in Fog Computing

Shaohan Feng[1], Zehui Xiong[1], Dusit Niyato[1], Ping Wang[2], and Amir Leshem[3]
[1] School of Computer Science and Engineering, Nanyang Technological University, Singapore
[2] Department of Electrical Engineering and Computer Science, York University, Canada
[3] Faculty of Engineering, Bar-Ilan University, Israel

***Abstract*—With the capability of support mobile computing demand with small delay, fog computing has gained tremendous popularity. Nevertheless, its highly virtualized environment is vulnerable to cyber attacks such as emerging Advanced Persistent Threats attack. In this paper, we propose a novel approach of cyber risk management for the fog computing platform. Particularly, we adopt the cyber-insurance as a tool for neutralizing cyber risks from fog computing platform. We consider a fog computing platform containing a group of fog nodes. The platform is composed of three main entities, i.e., the fog computing provider, attacker, and cyber-insurer. The fog computing provider dynamically optimizes the allocation of its defense computing resources to improve the security of the fog computing platform. Meanwhile, the attacker dynamically adjusts the allocation of its attack resources to improve the probability of successful attack. Additionally, to prevent from the potential loss due to attacks, the provider also makes a dynamic decision on the purchases ratio of cyber-insurance from the cyber-insurer for each fog node. Thereafter, the cyber-insurer accordingly determines the premium of cyber-insurance for each fog node. To model this dynamic interactive decision making, we formulate a dynamic Stackelberg game, where the attacker and provider act as the followers, and the cyber-insurer acts as the leader. In the lower level, we formulate an evolutionary subgame to analyze the provider's defense and cyber-insurance subscription strategies as well as the attacker's attack strategy. In the upper level, the cyber-insurer optimizes its premium determination strategy, taking into account the evolutionary equilibrium at the lower-level evolutionary subgame. We analytically prove that the evolutionary equilibrium is unique and stable. Moreover, we provide a series of insightful analytical and numerical results on the equilibrium of the dynamic Stackelberg game.**

***Keywords*—Risk management, fog computing, Advanced Persistent Threats attacks, cyber-insurace, game theory.**

I. Introduction

With the decentralized computing infrastructure, fog computing essentially extends cloud computing services to the edge of the network. As such, fog computing gains advantages from getting cloud resources closer to the position where the data is created and used upon. For example, fog computing based Internet of Things (IoT) system is applicable to meet strict quality of service (QoS) requirements, e.g., high-speed data processing. Due to the decentralized computing infrastructure, fog computing has been applied in extensive domains, e.g., smart home and health data management [1]. However, as everything else of value operating online, fog computing is vulnerable to cyber attacks, e.g., Advance Persistent Threats (APT) [2]. As one of the most popular cyber attacks, APT are created and launched by advanced and well-resourced attackers through multiple sophisticated methods to continuously and stealthily steal data from the targeted networking system. APT attacks have caused serious privacy leakage and millions of dollars' loss [3]. For example, in August 2014, a healthcare provider community announced that its computer system had fallen victim to an APT attack, and the sensitive information of 4.5 million of its patients may be compromised [4].

Recently, a few approaches such as deception [5] have been introduced in defending against APT attacks. However, due to the immense progress in the sophisticated APT attack, completely securing fog computing networks through security techniques may be impossible. As such, an extensive application prospect of fog computing has been critically hindered, especially in business services in which the high-level service security tops the list of evaluation criterion. To deal with APT attacks, the fog computing provider does not only focus on the improvement of security techniques, but also considers alternative means of cyber risk management. Recently, by transferring the cyber risks to the insurers, cyber-insurance has been recognized as a promising approach for efficient management of the cyber risks [6]. Similar to the traditional insurance, the customer of a cyber-insurance product, i.e., a policyholder, is insured once it settles the contract with the insurer by paying a premium. After being insured, the customer will receive the claim paid by the cyber-insurer once attacks happen and damage is incurred.

In this paper, we consider a fog computing platform targeted by APT attacks as shown in Fig. 1. There are mainly three entities under consideration, namely, a fog computing provider, an APT attacker, and a cyber-insurer. The fog computing platform is composed of a group of fog nodes which perform different types of networking functions, e.g., storage and cache. APT attackers launch an APT attack to the fog computing platform continuously and stealthily, e.g., through malwares [7]. Meanwhile, the fog computing provider can apply countermeasure to protect the fog computing platform from the APT attack. For example, the fog computing provider can use available computing resources to monitor the usage of the memory to detect activities of any malwares. Therefore, it is necessary for both the APT attacker and fog computing provider to optimize

This work was supported in part by WASP/NTU M4082187 (4080), Singapore MOE Tier 1 under Grant 2017-T1-002-007 RG122/17, MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15, NRF2015-NRF-ISF001-2277, and EMA Energy Resilience under Grant NRF2017EWT-EP003-041.

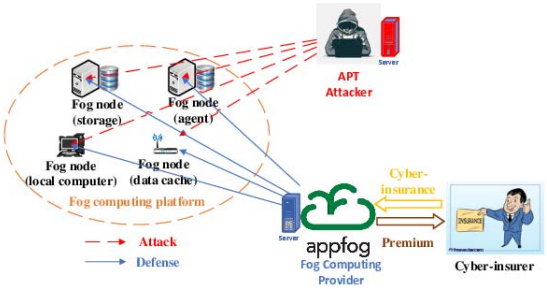

Figure 1: System model.

their attack/defense strategies by optimally allocating their attack/defense computing resources. Meanwhile, due to the imperfect security techniques and the incentive to neutralize the economic/financial loss incurred by APT attacks, the fog computing provider can purchase the cyber-insurance from the cyber-insurer.

To model and analyze the interaction dynamics for the considered fog computing platform, we propose a hierarchical dynamic Stackelberg game framework. In the lower level, the fog computing provider's defense and cyber-insurance subscription strategies as well as the APT attacker's attack strategy are formulated as an evolutionary subgame. We model the learning and adaptation of these strategies by using replicator dynamics. The evolutionary equilibrium is the solution of this subgame. In the upper level, the cyber-insurer optimizes its premium determination for payoff maximization, taking into account the solution of the lower-level evolutionary subgame. Unlike traditional Stackelberg games in which the strategies of the players are static, we formulate a dynamic Stackelberg game based on optimal control theory to enable the dynamic control of these strategies.

The rest of the paper is organized as follows. Section II describes the system model and the dynamic Stackelberg game formulation. Section III analyze the equilibrium in the proposed dynamic Stackelberg game. Section IV presents the performance evaluation. Section V concludes the paper.

II. System Description

In this section, we investigate the attack/defense strategies in the fog computing platform as well as the pricing problem of the cyber-insurance. Both the APT attacker and fog computing provider optimize their attack and defense strategies, respectively. Similar to [8], we assume that the APT attacker and fog computing provider need to allocate CPUs on each fog node to attack and defend the fog nodes, respectively. Furthermore, the fog computing provider also decides on subscribing to a cyber-insurance or not for each fog node. Accordingly, the cyber-insurer determines the price of the cyber-insurance, i.e., premium, for each fog node.

A. Followers' Payoffs and Leader's Profit

As shown in Fig. 1, there exists a set of fog nodes in the fog computing platform, denoted by $\mathcal{N}$. The number of all the CPUs owned by the APT attacker and fog computing provider are denoted by M^{A} and M^{P}, respectively. To attack fog node $i \in \mathcal{N}$, the APT attacker decides on the number of CPUs allocated on this node, i.e., $v_i M^{\mathrm{A}}$, where v_i is the ratio between the number of CPUs attacking fog node i and the number of all CPUs owned by the APT attacker. v_i is called the attack CPU ratio of fog node i. To protect the fog node i, the fog computing provider decides on the number of CPUs allocated on this node, i.e., $u_i M^{\mathrm{P}}$, where u_i is the ratio between the number of CPUs defending fog node i and the number of all CPUs owned by the fog computing provider. u_i is called the defense CPU ratio of fog node i. According to [9], the probability of successful APT attack is $\frac{v_i M^{\mathrm{A}}}{u_i M^{\mathrm{P}}+v_i M^{\mathrm{A}}+\sigma}$, and the corresponding probability of successful defense is $1-\frac{v_i M^{\mathrm{A}}}{u_i M^{\mathrm{P}}+v_i M^{\mathrm{A}}+\sigma}=\frac{u_i M^{\mathrm{P}}+\sigma}{u_i M^{\mathrm{P}}+v_i M^{\mathrm{A}}+\sigma}$, where σ is the basic security effort of the fog computing provider on the fog computing platform. Let λ_i denote the data size, i.e., information asset, stored at each fog node $i \in \mathcal{N}$. The expected payoffs of the fog computing provider and APT attacker on fog node i obtained from the attack/defense strategies are $\lambda_i \frac{u_i M^{\mathrm{P}}+\sigma}{u_i M^{\mathrm{P}}+v_i M^{\mathrm{A}}+\sigma}$ and $\lambda_i \frac{v_i M^{\mathrm{A}}}{u_i M^{\mathrm{P}}+v_i M^{\mathrm{A}}+\sigma}$, respectively. Launching the APT attack on fog node i as well as protecting the fog node i incur certain costs. The costs are proportional to the number of CPUs allocated on fog node i, i.e., $a_i v_i M^{\mathrm{A}}$ and $d_i u_i M^{\mathrm{P}}$, respectively. a_i is the APT attacker's attack unit cost and d_i is the fog computing provider's defense unit cost of allocating one unit of CPU on fog node i.

To rationally manage the cyber risk, the fog computing provider considers purchasing the cyber-insurance offered by the cyber-insurer. The cyber-insurer determines the premium, i.e., p_i for fog node i. The fog computing provider decides on the purchasing ratio of cyber-insurance for each fog node, i.e., x_i. The ratio is proportional to the risk on fog node i that the fog computing provider wants to transfer to the cyber-insurer. In return, the fog computing provider receives the claim of $x_i \lambda_i$ paid by the cyber-insurer if the APT attack happens and costs damage and loss. The fog computing provider will gain internal benefits of $s_i x_i - r_i {x_i}^2$ from subscribing to the cyber-insurance. The linear-quadratic function is used to capture the decreasing marginal returns. r_i is the intrinsic demand elasticity factor and s_i is the maximum intrinsic demand rate [10]. Note that the internal benefits come from the fact that the cyber-insurer not only provides the loss covering service to the fog computing provider but also attaches some other additional services to the cyber-insurance. For example, the cyber-insurance also offers the remedy plan for the business's and individual's reputation damage as an additional service attached to its cyber-insurance product [11]. By receiving the additional services, the fog computing provider will gain the internal benefits from the subscription to the cyber-insurance [12].

The expected payoff of the fog computing provider on fog node i is

$$\begin{aligned} {U^{\mathrm{P}}}_i(u_i, v_i, x_i, p_i) = \lambda_i \frac{u_i M^{\mathrm{P}}+\sigma}{u_i M^{\mathrm{P}}+v_i M^{\mathrm{A}}+\sigma} - d_i u_i M^{\mathrm{P}} \\ -p_i x_i + s_i x_i - r_i {x_i}^2 + \lambda_i x_i \frac{v_i M^{\mathrm{A}}}{u_i M^{\mathrm{P}}+v_i M^{\mathrm{A}}+\sigma}, \end{aligned} \tag{1}$$

and that of the APT attacker is

$$U^{\mathrm{A}}{}_i\left(u_i, v_i\right) = \lambda_i \frac{v_i M^{\mathrm{A}}}{u_i M^{\mathrm{P}} + v_i M^{\mathrm{A}} + \sigma} - a_i v_i M^{\mathrm{P}}, \tag{2}$$

where $\sum\limits_{i\in\mathcal{N}} u_i = 1$, $\sum\limits_{i\in\mathcal{N}} x_i = 1$, and $\sum\limits_{i\in\mathcal{N}} v_i = 1$.

By pricing the cyber-insurance, the cyber-insurer receives the revenue, i.e., $p_i x_i$ from fog node i. The cyber-insurer needs to pay the claim, i.e., $\lambda_i x_i$, once the APT attack happens. Recall that the probability of successful APT attack is denoted by $\frac{v_i M^{\mathrm{A}}}{u_i M^{\mathrm{P}} + v_i M^{\mathrm{A}} + \sigma}$. Let $\mathbf{u} = \left[u_1, u_2, \dots u_N\right]^\top \in \mathcal{D}_{\mathbf{u}} = \underset{i\in\mathcal{N}}{\times} \mathcal{D}_{u_i}$, $\mathbf{v} = \left[v_1, v_2, \dots v_N\right]^\top \in \mathcal{D}_{\mathbf{v}} = \underset{i\in\mathcal{N}}{\times} \mathcal{D}_{v_i}$, $\mathbf{x} = \left[x_1, x_2, \dots x_N\right]^\top \in \mathcal{D}_{\mathbf{x}} = \underset{i\in\mathcal{N}}{\times} \mathcal{D}_{x_i}$, and $\mathbf{p} = \left[p_1, p_2, \dots p_N\right]^\top \in \mathcal{D}_{\mathbf{p}} = \underset{i\in\mathcal{N}}{\times} \mathcal{D}_{p_i}$, the overall profit function of the cyber-insurer is therefore expressed as follows:

$$\Pi_{\mathrm{I}}\left(\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{p}\right) = \sum_{i\in\mathcal{N}} \left[p_i x_i - \lambda_i x_i \frac{v_i M^{\mathrm{A}}}{u_i M^{\mathrm{P}} + v_i M^{\mathrm{A}} + \sigma} \right], \tag{3}$$

where N is the cardinality of the set $\mathcal{N}$, $\mathcal{D}_{u_i} = [0, 1]$, $\mathcal{D}_{v_i} = [0, 1]$, $\mathcal{D}_{x_i} = [0, 1]$, and $\mathcal{D}_{p_i} = [0, p^{\mathrm{u}}]$, $\forall\, i \in \mathcal{N}$ are the domains of definition of u_i, v_i, x_i, and p_i, $\forall\, i \in \mathcal{N}$, respectively.

B. Lower-Level Evolutionary Subgame Formulation

The proposed evolutionary game framework is composed of two entities with three strategies, i.e., the cyber-insurance subscription strategy and defense strategy of the fog computing provider as well as the attack strategy of the APT attacker.

With the expected payoff defined in (1), the average payoff of the fog computing provider on the fog computing platform from the defense strategy is given by

$${}^{\mathrm{D}}\bar{U}^{\mathrm{P}}\left(\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{p}\right) = \sum_{i\in\mathcal{N}} u_i U^{\mathrm{P}}{}_i\left(u_i, v_i, x_i, p_i\right) \tag{4}$$

and that from cyber-insurance subscription is given by

$${}^{\mathrm{I}}\bar{U}^{\mathrm{P}}\left(\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{p}\right) = \sum_{i\in\mathcal{N}} x_i U^{\mathrm{P}}{}_i\left(u_i, v_i, x_i, p_i\right). \tag{5}$$

Similarly, the average payoff of the APT attacker on the fog computing platform is as follows:

$$\overline{U}^{\mathrm{A}}\left(\mathbf{u}, \mathbf{v}\right) = \sum_{i\in\mathcal{N}} v_i U^{\mathrm{A}}{}_i\left(u_i, v_i\right). \tag{6}$$

Then, by the pairwise proportional imitation protocol [13] and given the cyber-insurer's premium determination strategy, i.e., $\mathbf{p}\left(t\right) \in \mathcal{D}_{\mathbf{p}}$, the replicator dynamic yields the lower-level evolutionary subgame as shown in (7). This is from a system of Ordinary Differential Equations (ODEs), with initial strategies, i.e., Dirichlet boundary condition, $\left[\mathbf{u}\left(0\right); \mathbf{v}\left(0\right); \mathbf{x}\left(0\right)\right] = \left[\mathbf{u}^0; \mathbf{v}^0; \mathbf{x}^0\right]$, and $\mathcal{D}_{\mathbf{u}}$, $\mathcal{D}_{\mathbf{v}}$, $\mathcal{D}_{\mathbf{x}}$, and $\mathcal{D}_{\mathbf{p}}$ that have been transferred into Banach spaces with $\mathcal{L}^q$ norm, e.g., $\forall \mathbf{p} \in \mathcal{D}_{\mathbf{p}}$, $\left\|\mathbf{p}\right\| = \left(\int\limits_{\mathcal{T}} \left|\mathbf{p}\left(t\right)\right|^q \mathrm{d}t \right)^{\frac{1}{q}}$, $q \in (1, +\infty)$. Therein, ∇_t is the differential operator, i.e., $\frac{\mathrm{d}}{\mathrm{d}t}$, with respect to t, and the usage of the differential operator is defined similarly in the rest of this paper. For the convenience of equilibrium analysis in Section III, we introduce the expression in (8). As a result, the left-hand-side of the equation in (7) can be simplified as shown in (9).

Therefore, the lower-level evolutionary subgame defined in (7) is simplified as follows:

$$\begin{aligned} &\nabla_t \begin{pmatrix} \mathbf{u}\left(t\right) \\ \mathbf{v}\left(t\right) \\ \mathbf{x}\left(t\right) \end{pmatrix} = \begin{pmatrix} \mathbf{f}\left(\mathbf{u}\left(t\right), \mathbf{v}\left(t\right), \mathbf{x}\left(t\right), \mathbf{p}\left(t\right)\right) \\ \mathbf{g}\left(\mathbf{u}\left(t\right), \mathbf{v}\left(t\right)\right) \\ \mathbf{h}\left(\mathbf{u}\left(t\right), \mathbf{v}\left(t\right), \mathbf{x}\left(t\right), \mathbf{p}\left(t\right)\right) \end{pmatrix}, \\ &\left[\mathbf{u}\left(0\right); \mathbf{v}\left(0\right); \mathbf{x}\left(0\right)\right] = \left[\mathbf{u}^0; \mathbf{v}^0; \mathbf{x}^0\right]. \end{aligned} \tag{10}$$

C. A Stackelbery Game Formulation

The profit of the cyber-insurer at time t is given by

$$\begin{aligned} &\Pi_{\mathrm{I}}\left(\mathbf{u}\left(t\right), \mathbf{v}\left(t\right), \mathbf{x}\left(t\right), \mathbf{p}\left(t\right)\right) \\ &= \sum_{i\in\mathcal{N}} \left[p_i\left(t\right) x_i\left(t\right) - \lambda_i x_i\left(t\right) \frac{v_i\left(t\right) M^{\mathrm{A}}}{u_i\left(t\right) M^{\mathrm{P}} + v_i\left(t\right) M^{\mathrm{A}} + \sigma} \right]. \end{aligned} \tag{11}$$

The corresponding total profit of the cyber-insurer over the time horizon $\mathcal{T} = [0, T]$ is expressed as follows:

$$\int\limits_{\mathcal{T}} \Pi_{\mathrm{I}}\left(\mathbf{u}\left(t\right), \mathbf{v}\left(t\right), \mathbf{x}\left(t\right), \mathbf{p}\left(t\right)\right) \mathrm{d}t. \tag{12}$$

With the lower-level evolutionary subgame defined in (10), the Stackelberg game can be formulated as follows:

$$\begin{aligned} \max_{\mathbf{p}\in\mathcal{D}_{\mathbf{p}}} \quad & \int\limits_{\mathcal{T}} \Pi_{\mathrm{I}}\left(\mathbf{u}\left(t\right), \mathbf{v}\left(t\right), \mathbf{x}\left(t\right), \mathbf{p}\left(t\right)\right) \mathrm{d}t \\ \text{s.t.} \quad & \nabla_t \begin{pmatrix} \mathbf{u}\left(t\right) \\ \mathbf{v}\left(t\right) \\ \mathbf{x}\left(t\right) \end{pmatrix} = \begin{pmatrix} \mathbf{f}\left(\mathbf{u}\left(t\right), \mathbf{v}\left(t\right), \mathbf{x}\left(t\right), \mathbf{p}\left(t\right)\right) \\ \mathbf{g}\left(\mathbf{u}\left(t\right), \mathbf{v}\left(t\right)\right) \\ \mathbf{h}\left(\mathbf{u}\left(t\right), \mathbf{v}\left(t\right), \mathbf{x}\left(t\right), \mathbf{p}\left(t\right)\right) \end{pmatrix} \\ & \left[\mathbf{u}\left(0\right); \mathbf{v}\left(0\right); \mathbf{x}\left(0\right)\right] = \left[\mathbf{u}^0; \mathbf{v}^0; \mathbf{x}^0\right], \end{aligned} \tag{13}$$

which is an optimal control problem.

III. Equilibrium Analysis

With the formulation of the Stackelberg game in Section II-C and lower-level evolutionary subgame in Section II-B, we analyze their equilibriums. We first prove that the solution to the lower-level evolutionary subgame is unique and stable with a given strategy of the cyber-insurer by using Cauchy-Lipschitz theorem and Lyapunov's second method for stability, respectively. Then, we prove that the objective of the formulated optimal control problem, i.e., the objective of the upper-level subgame of the Stackelberg game defined in (13), approaches its supremum in a bounded set and admits a solution.

A. Solution to Lower-Level Evolutionary Subgame

We investigate the uniqueness of the solution to the lower-level evolutionary subgame defined in (10), i.e., the uniqueness of the evolutionary equilibrium, by using the following lemma.

Lemma 1. Cauchy-Lipschitz theorem *[14]: Consider a system of ODEs*

$$\begin{aligned} \nabla_t \mathbf{y}\left(t\right) &= \mathbf{F}\left(\mathbf{y}\left(t\right), t\right), \forall\, t \in \mathcal{T} \\ \mathbf{y}\left(0\right) &= \mathbf{y}^0, \end{aligned} \tag{14}$$

where $\mathbf{y}\left(t\right) \in \mathcal{D} \subseteq \mathbb{R}^n$ denotes the system state vector, $\mathcal{D}$ is the domain of definition of $\mathbf{y}\left(t\right)$ containing the origin point,

$$\nabla_t\left[\mathbf{u}\left(t\right);\mathbf{v}\left(t\right);\mathbf{x}\left(t\right)\right]=\left(\begin{array}{c} u_1\left(t\right)\left[{U^{\mathrm{P}}}_1\left(u_1\left(t\right),v_1\left(t\right),x_1\left(t\right),p_1\left(t\right)\right)-{}^{\mathrm{D}}\bar{U}^{\mathrm{P}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)\right] \\ \vdots \\ u_N\left(t\right)\left[{U^{\mathrm{P}}}_N\left(u_N\left(t\right),v_N\left(t\right),x_N\left(t\right),p_N\left(t\right)\right)-{}^{\mathrm{D}}\bar{U}^{\mathrm{P}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)\right] \\ v_1\left(t\right)\left[{U^{\mathrm{A}}}_1\left(u_1\left(t\right),v_1\left(t\right)\right)-\bar{U}^{\mathrm{A}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right)\right)\right] \\ \vdots \\ v_N\left(t\right)\left[{U^{\mathrm{A}}}_N\left(u_N\left(t\right),v_N\left(t\right)\right)-\bar{U}^{\mathrm{A}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right)\right)\right] \\ x_1\left(t\right)\left[{U^{\mathrm{P}}}_1\left(u_1\left(t\right),v_1\left(t\right),x_1\left(t\right),p_1\left(t\right)\right)-{}^{\mathrm{I}}\bar{U}^{\mathrm{P}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)\right] \\ \vdots \\ x_N\left(t\right)\left[{U^{\mathrm{P}}}_N\left(u_N\left(t\right),v_N\left(t\right),x_N\left(t\right),p_N\left(t\right)\right)-{}^{\mathrm{I}}\bar{U}^{\mathrm{P}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)\right] \end{array}\right) \tag{7}$$

$$\begin{aligned} f_i\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)&=u_i\left(t\right)\left[{U^{\mathrm{P}}}_i\left(u_i\left(t\right),v_i\left(t\right),x_i\left(t\right),p_i\left(t\right)\right)-{}^{\mathrm{D}}\bar{U}^{\mathrm{P}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)\right], \\ g_i\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right)\right)&=v_i\left(t\right)\left[{U^{\mathrm{A}}}_i\left(u_i\left(t\right),v_i\left(t\right)\right)-\bar{U}^{\mathrm{A}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right)\right)\right], \qquad \forall i\in\mathcal{N} \\ h_i\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)&=x_i\left(t\right)\left[{U^{\mathrm{P}}}_i\left(u_1\left(t\right),v_i\left(t\right),x_i\left(t\right),p_i\left(t\right)\right)-{}^{\mathrm{I}}\bar{U}^{\mathrm{P}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)\right], \end{aligned} \tag{8}$$

$$\begin{aligned} \mathbf{f}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)=&\left[f_1\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right),f_2\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right),\right. \\ &\left.\ldots,f_N\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)\right]^{\top}, \\ \mathbf{g}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right)\right)=&\left[g_1\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right)\right),g_2\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right)\right),\ldots,g_N\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right)\right)\right]^{\top}, \\ \mathbf{h}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)=&\left[h_1\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)h_2\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right),\right. \\ &\left.\ldots,h_N\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)\right]^{\top}. \end{aligned} \tag{9}$$

and $\mathbf{F}:\mathcal{D}\times\mathcal{T}\mapsto\mathbb{R}^n$ *is continuous on* $\mathcal{D}\times\mathcal{T}$*. If there exists a constant* $M\in\mathbb{R}$ *such that*

$$\begin{aligned} &\left|\mathbf{F}\left(\mathbf{y}_1\left(t\right),t\right)-\mathbf{F}\left(\mathbf{y}_2\left(t\right),t\right)\right|\leq M\left|\mathbf{y}_1\left(t\right)-\mathbf{y}_2\left(t\right)\right|, \\ &\forall\left[\mathbf{y}_1\left(t\right),t\right],\left[\mathbf{y}_2\left(t\right),t\right]\in\mathcal{D}\times\mathcal{T}, \end{aligned} \tag{15}$$

then $\mathbf{F}:\mathcal{D}\times\mathcal{T}\mapsto\mathbb{R}^n$ *satisfies the Lipschitz condition, and for any* $\mathbf{y}^0\in\mathbb{R}^n$*, the system of ODEs defined in (14) is uniquely solvable.*

To prove that the lower-level evolutionary subgame defined in (10) satisfies the Lipschitz condition, i.e., Lemma 1, we first present Proposition 1.

Proposition 1. *For any given* $\mathbf{p}=\mathbf{p}^{\mathrm{given}}\in\mathcal{D}_{\mathbf{p}}$*, there exists upper bounds of*

$$\left|\frac{\mathrm{d}f_i\left(\mathbf{u}_{-j}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\right)}{\mathrm{d}z}\right|_{z=u_j\left(t\right)},\left|\frac{\mathrm{d}f_i\left(\mathbf{u}\left(t\right),\mathbf{v}_{-j}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\right)}{\mathrm{d}z}\right|_{z=v_j\left(t\right)},$$

$$\left|\frac{\mathrm{d}f_i\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}_{-j}\left(t\right),\mathbf{p}\right)}{\mathrm{d}z}\right|_{z=x_j\left(t\right)},\left|\frac{\mathrm{d}h_i\left(\mathbf{u}_{-j}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\right)}{\mathrm{d}z}\right|_{z=u_j\left(t\right)},$$

$$\left|\frac{\mathrm{d}h_i\left(\mathbf{u}\left(t\right),\mathbf{v}_{-j}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\right)}{\mathrm{d}z}\right|_{z=v_j\left(t\right)},\left|\frac{\mathrm{d}h_i\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}_{-j}\left(t\right),\mathbf{p}\right)}{\mathrm{d}z}\right|_{z=x_j\left(t\right)},$$

$$\left|\frac{\mathrm{d}g_i\left(\mathbf{u}_{-j}\left(t\right),\mathbf{v}\left(t\right)\right)}{\mathrm{d}z}\right|_{z=u_j\left(t\right)},\left|\frac{\mathrm{d}g_i\left(\mathbf{u}\left(t\right),\mathbf{v}_{-j}\left(t\right)\right)}{\mathrm{d}z}\right|_{z=v_j\left(t\right)},$$

$\forall\left[\mathbf{u}\left(t\right);\mathbf{v}\left(t\right);\mathbf{x}\left(t\right)\right]\in\mathcal{D}_{\mathbf{u}}\times\mathcal{D}_{\mathbf{v}}\times\mathcal{D}_{\mathbf{x}}$*,* $\forall i,j\in\mathcal{N}$*, denoted by* ${M^{\mathrm{dfdu}}}_{ij}$*,* ${M^{\mathrm{dfdv}}}_{ij}$*,* ${M^{\mathrm{dfdx}}}_{ij}$*,* ${M^{\mathrm{dhdu}}}_{ij}$*,* ${M^{\mathrm{dhdv}}}_{ij}$*,* ${M^{\mathrm{dhdx}}}_{ij}$*,* ${M^{\mathrm{dgdu}}}_{ij}$*, and* ${M^{\mathrm{dgdv}}}_{ij}$*, respectively, where all of them are positive finite valued real numbers,* $\mathbf{u}_{-j}\left(t\right)=\left[u_1\left(t\right);\ldots;u_{j-1}\left(t\right);z;u_{j+1}\left(t\right)\ldots;u_N\left(t\right)\right]$, $\mathbf{v}_{-j}\left(t\right)=\left[v_1\left(t\right);\ldots;v_{j-1}\left(t\right);z;v_{j+1}\left(t\right)\ldots;v_N\left(t\right)\right]$, $\mathbf{x}_{-j}\left(t\right)=\left[x_1\left(t\right);\ldots;x_{j-1}\left(t\right);z;x_{j+1}\left(t\right)\ldots;x_N\left(t\right)\right]$.

Proof. The proof is based on the fact that the first derivatives of ${U^{\mathrm{P}}}_i\left(u_i,v_i,x_i,p_i\right)$ and ${U^{\mathrm{A}}}_i\left(u_i,v_i\right)$, $\forall i\in\mathcal{N}$ are bounded. Due to the space limit, the proof is omitted. □

With Proposition 1, we are ready to prove that the lower-level evolutionary subgame is uniquely solvable as presented in Theorem 1.

THEOREM 1. *For any given* $\mathbf{p}^{\mathrm{given}}\in\mathcal{D}_{\mathbf{p}}$*, the lower-level evolutionary subgame defined in (10) is uniquely solvable and hence admits a unique evolutionary equilibrium.*

Proof. With any given $\mathbf{p}=\mathbf{p}^{\mathrm{given}}\in\mathcal{D}_{\mathbf{p}}$, the condition that

$$\left(\begin{array}{c}\mathbf{f}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\right)\\ \mathbf{g}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right)\right)\\ \mathbf{h}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\right)\end{array}\right) \tag{16}$$

satisfies Lipschitz condition with respect to $\left[\mathbf{u}\left(t\right);\mathbf{v}\left(t\right);\mathbf{x}\left(t\right)\right]\in\mathcal{D}_{\mathbf{u}}\times\mathcal{D}_{\mathbf{v}}\times\mathcal{D}_{\mathbf{x}}$, $\forall\mathbf{p}=\mathbf{p}^{\mathrm{given}}\in\mathcal{D}_{\mathbf{p}}$ can be guaranteed based on Proposition 1, and hence the lower-level evolutionary subgame defined in (10) is uniquely solvable according to Lemma 1. □

Note that due to the space limit, the proof of Theorem 1 is omitted.

Then, according to Lemma 2, we justify the stability of the unique evolutionary equilibrium to the lower-level evolutionary subgame defined in (10) as presented in Theorem 2.

Lemma 2. Lyapunov's second method for stability *[15]: Consider the system of ODEs defined in (14) again. Provided that there exists a function* $V\left(\mathbf{y}\left(t\right)\right):\mathbb{R}^n\mapsto\mathbb{R}$ *such that*

- $V\left(\mathbf{y}\left(t\right)\right)=0$*, if* $\mathbf{y}\left(t\right)=\mathbf{0}$*,*
- $V\left(\mathbf{y}\left(t\right)\right)>0$*, if* $\mathbf{y}\left(t\right)\neq\mathbf{0}$*,*
- $\nabla_t V\left(\mathbf{y}\left(t\right)\right)=\frac{\mathrm{d}}{\mathrm{d}\mathbf{y}\left(t\right)}V\left(\mathbf{y}\left(t\right)\right)\times\frac{\mathrm{d}}{\mathrm{d}t}\mathbf{y}\left(t\right)=\left(\nabla_{\mathbf{y}}V\right)^{\top}\times\nabla_t\mathbf{y}\left(t\right)=\left(\nabla_{\mathbf{y}}V\right)^{\top}\cdot\mathbf{F}\left(\mathbf{y}\left(t\right),t\right)\leq 0$ *for all values of* $\mathbf{y}\left(t\right)\neq\mathbf{0}$*, i.e., negative semidefinite,*

the solution to the system of ODEs defined in (14) is stable.

THEOREM 2. *For any given* $\mathbf{p}^{\text{given}} \in \mathcal{D}_{\mathbf{p}}$*, the lower-level evolutionary subgame defined in (10) admits a stable evolutionary equilibrium.*

Proof. From the Lyapunov's second method for stability introduced in Lemma 2, we design a Lyapunov function as follows:

$$V\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right)\right)=\left\{\sum_{i\in\mathcal{N}}\left[u_i\left(t\right)+v_i\left(t\right)+x_i\left(t\right)\right]\right\}^2, \quad (17)$$

where $V\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right)\right):\mathcal{D}_{\mathbf{u}}\times\mathcal{D}_{\mathbf{v}}\times\mathcal{D}_{\mathbf{x}}\mapsto\mathbb{R}$ satisfies

$$V\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right)\right)\begin{cases}=0, \text{ if } \mathbf{u}\left(t\right)=\mathbf{v}\left(t\right)=\mathbf{x}\left(t\right)=\mathbf{0},\\ >0, \text{ otherwise.}\end{cases} \quad (18)$$

By using the Lyapunov function defined in (17), the evolutionary equilibrium to the lower-level evolutionary subgame defined in (10) can be proven to be stable. Due to the space limit, the proof is omitted. □

B. Solution to Optimal Control Problem

According to Theorem 1, the lower-level evolutionary subgame defined in (10) is uniquely solvable with any given $\mathbf{p}^{\text{given}}\in\mathcal{D}_{\mathbf{p}}$. There exists a injective solution operator denoted by $\mathbf{\Gamma}:\mathcal{D}_{\mathbf{p}}\mapsto\mathcal{D}_{\mathbf{u}}\times\mathcal{D}_{\mathbf{v}}\times\mathcal{D}_{\mathbf{x}}$ such that $\left[\mathbf{u}\left(t\right);\mathbf{v}\left(t\right);\mathbf{x}\left(t\right)\right]-\mathbf{\Gamma}\left(\mathbf{p}\left(t\right),\mathbf{u}^0;\mathbf{v}^0;\mathbf{x}^0\right)=\mathbf{0}$, $\forall\, t\in\mathcal{T}$. This yields an equivalent problem of the optimal control problem (13) as follows:

$$\begin{aligned}\max_{\mathbf{p}\in\mathcal{D}_{\mathbf{p}}}\quad & \int_{\mathcal{T}}\Pi_{\text{I}}\left(\mathbf{u}\left(t\right),\mathbf{v}\left(t\right),\mathbf{x}\left(t\right),\mathbf{p}\left(t\right)\right)\mathrm{d}t\\ \text{s.t.}\quad & \left[\mathbf{u}\left(t\right);\mathbf{v}\left(t\right);\mathbf{x}\left(t\right)\right]-\mathbf{\Gamma}\left(\mathbf{p}\left(t\right),\mathbf{u}^0,\mathbf{v}^0,\mathbf{x}^0\right)=\mathbf{0},\ \forall\, t\in\mathcal{T}.\end{aligned} \quad (19)$$

We substitute the equality constraint in (19) into the objective function of (19) and have the following more simplified equivalent problem of the optimal control problem (13), i.e.,

$$\max_{\mathbf{p}\in\mathcal{D}_{\mathbf{p}}}\Psi\left(\mathbf{p}\right):=\max_{\mathbf{p}\in\mathcal{D}_{\mathbf{p}}}\int_{\mathcal{T}}\Pi_{\text{I}}\left(\mathbf{\Gamma}\left(\mathbf{p}\left(t\right),\mathbf{u}^0,\mathbf{v}^0,\mathbf{x}^0\right),\mathbf{p}\left(t\right)\right)\mathrm{d}t. \quad (20)$$

Lemma 3. *Let* $\mathcal{D}_{\mathbf{p}}^{\text{ad}}\subseteq\mathcal{D}_{\mathbf{p}}$ *such that* $\Psi\left(\mathbf{p}\right):\mathcal{D}_{\mathbf{p}}^{ad}\mapsto\mathbb{R}$ *is bounded, and let* $\Upsilon:=\sup\left\{\Psi\left(\mathbf{p}\right)\middle|\mathbf{p}\in\mathcal{D}_{\mathbf{p}}\right\}$*, if there exists a bounded set* $\mathcal{D}_{\mathbf{p}}^{\text{bs}}\subseteq\mathcal{D}_{\mathbf{p}}$ *and* $\epsilon\in\mathbb{R}^+$ *such that*

$$\mathbf{p}\in\mathcal{D}_{\mathbf{p}}^{\text{ad}}\backslash\mathcal{D}_{\mathbf{p}}^{\text{bs}}\ \Rightarrow\ \Psi\left(\mathbf{p}\right)\leq\Upsilon-\epsilon, \quad (21)$$

then $\Psi\left(\mathbf{p}\right)$ *approaches its supremum in a bounded set.*

Proof. As $\mathcal{D}_{\mathbf{p}}^{\text{bs}}$ is bounded, there is $\delta\in\mathbb{R}^+$ such that $\mathcal{D}_{\mathbf{p}}^{\text{bs}}\subseteq\mathscr{B}_{\delta}\left(\mathbf{0}\right)$, where $\mathscr{B}_{\delta}\left(\mathbf{0}\right)$ is a ball centered at original $\mathbf{0}\in\mathbb{R}^N$ with δ as its radius. Based on the definition of ϵ, there exists a sequence $\left\{\mathbf{p}_n\right\}_{n\in\mathbb{N}}$ in $\mathcal{D}_{\mathbf{p}}^{\text{ad}}$ such that $\lim_{n\to\infty}\Psi\left(\mathbf{p}_n\right)=\Upsilon$. Then, (21) implies that there is $n_0\in\mathbb{N}$ such that $\mathbf{p}_n$ for each $n>n_0$, i.e., $\mathbf{p}_n\in\mathcal{D}_{\mathbf{p}}^{\text{ad}}\backslash\left(\mathcal{D}_{\mathbf{p}}^{\text{ad}}\backslash\mathcal{D}_{\mathbf{p}}^{\text{bs}}\right)=\mathcal{D}_{\mathbf{p}}^{\text{ad}}\cap\mathcal{D}_{\mathbf{p}}^{\text{bs}}$, showing that $\Psi\left(\mathbf{p}_n\right)$ approaches its supremum in $\mathcal{D}_{\mathbf{p}}^{\text{ad}}$. □

THEOREM 3. *If* $\mathcal{D}_{\mathbf{p}}^{\text{ad}}\subseteq\mathcal{D}_{\mathbf{p}}$ *is nonempty, closed, and convex set, and* $\Psi\left(\mathbf{p}\right)$ *approaches its supremum and is weakly sequentially semicontinuous, then the equivalent problem of the optimal control problem defined in (13), i.e., (20), has a solution* $\overline{\mathbf{p}}\in\mathcal{D}_{\mathbf{p}}^{\text{ad}}$*. This means that the optimal control problem defined in (13) always has a solution.*

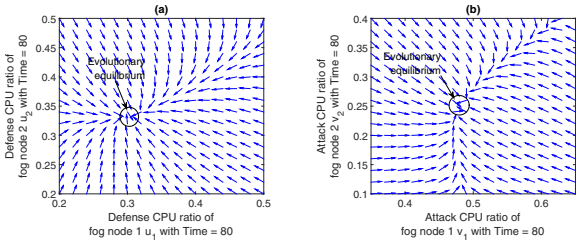

Figure 2: Direction Field of the replicator dynamics showing the stability of the evolutionary equilibrium

Proof. The proof is based on Lemma 3 and flexive Banach space theory. Due to the space limit, the proof is omitted. □

IV. PERFORMANCE EVALUATION

In this section, we conduct extensive numerical studies to evaluate the performance of the players in the dynamic Stackelberg game. For ease of illustration, we consider a fog computing platform containing 3 fog nodes, i.e, $N=3$, over the time space of $\mathcal{T}=[0,100]$. The amounts of assets in, i.e., the size and value of data stored in, fog nodes 1, 2, and 3 are 1.2 (λ_1), 1.3 (λ_2), and 1.4 (λ_3), respectively. The initial strategies of the fog computing provider's defense as well as the cyber-insurance subscription, and the APT attacker's attack are $\mathbf{u}^0=[0.35,0.25,0.4]$, $\mathbf{x}^0=[0.35,0.25,0.4]$, and $\mathbf{v}^0=[0.4,0.4,0.2]$, respectively. The numbers of total CPUs owned by the fog computing provider and the APT attacker are 50 (M^{P}) and 40 (M^{A}), respectively. The cost of employing one CPU for the APT attacker and fog computing provider to attack and defend the fog nodes are $\mathbf{a}=[0.03,0.04,0.04]$ and $\mathbf{d}=[0.03,0.04,0.04]$, respectively. The basic security effort of the fog computing provider on the fog computing platform is $\sigma=4$. Moreover, the coefficient $\gamma>0$ measuring the absolute risk-sensitivity is set to be 15, i.e., $\gamma=15$. The upper bound of the premium of the cyber-insurer is $p^{\text{u}}=2$.

A. Numerical Results

1) Demonstration of the evolutionary equilibrium stability: The stability of the evolutionary equilibrium can be verified using a direction field of the replicator dynamics. We use the evolutionary process of the fog computing provider's defense strategies as well as the APT attacker's attack strategies on fog nodes 1 and 2 as examples. The direction fields between u_1 and u_2, v_1 and v_2 are shown in Figs. 2(a) and (b), respectively. As shown in Fig. 2, any unstable strategy will follow the arrow to reach the evolutionary equilibrium, which is marked by the black circle. This demonstrates the stability of the evolutionary equilibrium and is consistent with Theorem 2.

2) Dynamic strategies: We next investigate the dynamic strategies of the lower-level evolutionary subgame. The dynamic strategies of the lower-level evolutionary subgame are subject to the control of the cyber-insurer's premium strategies. The dynamic change of the strategies in the lower-level evolutionary subgame indicates the adaptation of the followers' strategies. As shown in Figs. 3(b) and (c), the strategies of the

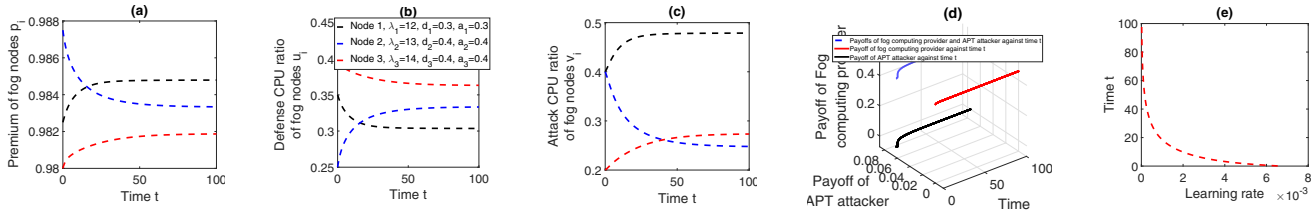

Figure 3: Evolutionary Equilibrium, Payoffs, and learning rate

lower-level evolutionary subgame converge to the evolutionary equilibrium at which neither the fog computing provider nor the APT attacker has a willingness to change their strategies unilaterally. Although the defense cost of fog node 1, i.e., $d_1 = 0.03$, is the lowest among these three fog nodes, the fog computing provider's defense CPU ratio of fog node 1, i.e., u_1, decreases from the large initial value to the smallest value at the evolutionary equilibrium. The reason is that the fog computing provider prefers the fog node with higher asset while the asset of fog node 1, i.e., $\lambda_1 = 1.2$, is the lowest among these three fog nodes. In contrast, due to the smallest initial defense effort of fog node 2, i.e., the smallest initial defense CPU ratio u_2, in Fig. 3(b) and the higher amount of asset of fog node 2 than that of fog node 1, i.e., $\lambda_2 = 1.3 > \lambda_1 = 1.2$, the fog computing provider loses its payoff and cannot optimally protect the fog computing platform. In this case, the defense CPU ratio of fog node 2 increases from the initial value to the evolutionary equilibrium. Accordingly, the APT attacker decreases the attack CPU ratio of fog node 2 and increases the attack CPU ratio of fog node 1 as shown in Fig. 3(c). This results in the largest probability of successful APT attack on fog node 1, and hence its premium is the highest at the evolutionary equilibrium.

The adaption of the strategies of the fog computing provider and the APT attacker can also be observed from Figs. 3(d) and (e). Specifically, from Fig. 3(d), we observe that the payoffs of both the fog computing provider and the APT attacker fluctuate at first due to their unstable strategies and converge to the stable payoff at the evolutionary equilibrium. Furthermore, Fig. 3(e) shows the frequency of the adaptation of the strategies, where the learning rate represents the convergence speed of the replicator dynamics. We observe that the convergence speed keeps increasing with the increasing learning rate. When all the strategies are involved in the adaption, the convergence speed is the fastest, i.e., for $t = 0$. Note that the value of the fastest learning rate depends on the gap between the initial strategies and stable strategies.

V. Conclusion

With Advanced Persistent Threats, we have presented a hierarchical dynamic game framework to analyze the attack/defense strategy in the fog computing platform as well as the pricing of the cyber-insurance. The interaction among the fog computing provider, APT attacker, and cyber-insurer has been modeled as a two-stage dynamic Stackelberg game. The dynamics of the fog computing provider's defense and the cyber-insurance subscription strategies as well as the APT attacker's attack strategy are captured by a replicator dynamics in the lower-level evolutionary subgame. The stable and unique evolutionary equilibrium has been obtained as the interior solution. Taking into account the lower-level evolutionary subgame, the pricing problem of the cyber-insurance has been formulated as an optimal control problem. Moreover, we have provided a series of insightful analytical and numerical results on the equilibrium of the dynamic Stackelberg game.

References

[1] S. Yi, Z. Hao, Z. Qin and Q. Li, "Fog computing: Platform and applications," in *Hot Topics in Web Systems and Technologies (HotWeb), 2015 Third IEEE Workshop on*. IEEE, 2015, pp. 73–78.

[2] S. Khan, S. Parkinson and Y. Qin, "Fog computing security: a review of current applications and security solutions," *Journal of Cloud Computing*, vol. 6, no. 1, pp. 19, 2017.

[3] J. Vukalović and D. Delija, "Advanced persistent threats-detection and defense," in *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*. IEEE, 2015, pp. 1324–1330.

[4] T. Micro, "Healthcare provider hit by advanced persistent threat: Protecting client information," https://blog.trendmicro.com/healthcare-provider-hit-advanced-persistent-threat-protecting-client-information/, 2014.

[5] B. M. Bowen, S. Hershkop, A. D. Keromytis and S. J. Stolfo, "Baiting inside attackers using decoy documents," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2009, pp. 51–70.

[6] S. Feng, W. Wang, Z. Xiong, D. Niyato, P. Wang and S. S. Wang, "On cyber risk management of blockchain networks: A game theoretic approach," *arXiv preprint arXiv:1804.10412*, 2018.

[7] J. Fruhlinger, "What is stuxnet, who created it and how does it work?," https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html, 2017.

[8] M. Min, L. Xiao, C. Xie, M. Hajimirsadeghi and N. B. Mandayam, "Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach," *arXiv preprint arXiv:1801.06270*, 2018.

[9] A. Garnaev, M. Baykal-Gursoy and H. V. Poor, "Security games with unknown adversarial strategies," *IEEE transactions on cybernetics*, vol. 46, no. 10, pp. 2291–2299, 2016.

[10] X. Gong, L. Duan, X. Chen and J. Zhang, "When social network effect meets congestion effect in wireless networks: Data usage equilibrium and optimal pricing," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 449–462, 2017.

[11] AIG, "Cyber insurance," https://www.aig.com.sg/business/business-products-and-services/financial-lines/cyber-insurance0, 2018.

[12] D. Zhang and G.-H. Lin, "Bilevel direct search method for leader–follower problems and application in health insurance," *Computers & Operations Research*, vol. 41, pp. 359–373, 2014.

[13] W. H. Sandholm, "Potential games with continuous player sets," *Journal of Economic theory*, vol. 97, no. 1, pp. 81–108, 2001.

[14] E. of Mathematics, "Cauchy-lipschitz theorem," https://www.encyclopediaofmath.org/index.php/Cauchy-Lipschitz_theorem.

[15] S. Sastry, "Lyapunov stability theory," in *Nonlinear Systems*, pp. 182–234. Springer, 1999.