Multi-dimensional Network Security Game: How do attacker and defender battle on parallel targets?

Yuedong Xu*, John C.S. Lui†
*Department of Electronic Engineering, Fudan University, China
† Department of Computer Science & Engineering, The Chinese University of Hong Kong, China
Email: {ydxu@fudan.edu.cn, cslui@cse.cuhk.edu.hk}

***Abstract*—In this paper, we consider a new network security game wherein an attacker and a defender are battling over "*multiple*" targets. This type of game is appropriate to model many current network security conflicts such as Internet phishing, mobile malware or network intrusions. In such attacks, the attacker and the defender need to decide how to allocate resources on each target so as to maximize their utilities within their resource limits. We model such a multi-dimensional network security game as a constrained non-zero sum game. Two security breaching models, the product-form and the proportion-form, are considered. For each breaching model, we prove the existence of a unique Nash equilibrium (NE) based on Rosen's theorem and propose efficient algorithms to find the NE when the games are strictly concave. Furthermore, we show the existence of multiple NEs in the product-form breaching model when the strict concavity does not hold. Our study sheds light on the strategic behaviors of the attacker and the defender, in particular, on how they allocate resources to the targets which have different weights, and how their utilities as well as strategies are influenced by the resource constraints.**

I. Introduction

The economics of network security has become a thriving concern in fixed line and mobile Internet. Due to the popularity of e-commerce and other online services, malicious attacks have evolved into profit driven online crimes in the forms of Internet phishing, network intrusion, mobile malware etc. Although security defence is essential, the networking community is still witnessing an increased number of global attacks. Part of reasons are the economic benefits on performing attacks by hackers as well as the inadequate protection against the persistent attacks. Therefore, economic studies beyond the technological solutions are vitally important to reveal the behaviors of the defenders and the malicious attackers, and game theory serves as a well suited mathematical tool to bring about this fundamental understanding. A prominent application of game theory in security is intrusion detection where an attacker exploits system vulnerabilities and a defender monitors the events occurring in a network strategically [1][3]. Recent advances of network security games have two features. One is called *uncertainty* that incorporates incomplete information of players [3] and stochastic properties of players or environments [4]. The other is called *interdependency* in which the actions of players may affect other players. This type of interactions are sometimes regarded as network effects with positive or negative externality [6], [7], [12].

In this work, we explore a new type of network security game which is characterized by *multi-dimensional* attacks. We are motivated by three facts. Firstly, the effectiveness of attack or defence depends on the amount of resources that are used. The resource is an abstract representation of manpower, machines, technologies, etc. For instance, many resources are needed to create malicious websites in phishing attacks, or to camouflage malicious apps in mobiles, or to recruit zombie machines in DDoS attacks, or to probe server vulnerabilities in intrusion attacks. However, one needs to note that resource is *not free* for the attacker and the defender. Secondly, the attacker and the defender usually possess limited resources. For instance, the number of active bots that a botmaster can manipulate is usually constrained to a few thousands [19]. Thirdly, the attacker can assaults *multiple* targets for better economic returns. These targets may represent different banks in the Internet phishing attack [8], or different Android apps in mobile malware, or different servers in network intrusion attacks. These targets vary in values or importances. Attacking (resp. protecting) more targets requires a larger amount of resources, which may exceed the resource budget of the attacker (resp. defender). As a consequence, the conflicts on multiple targets are conjoined whenever the attacker or the defender has limited amount of resources. This transforms the decision making in network security issues into myopic constrained optimization problems.

We propose a non-zero sum game to characterize the constrained resource allocation between an attacker and a defender. The utility of the attacker is modeled as the profit, which is equivalent to the loss of victims minus the costs of attack resources. The utility of the defender is modeled as the loss of victims plus the costs of defence resources. Both players aim to optimize their individual utilities. We express the loss of victims on a target as a product of its weight and the security breaching probability. Two breaching models are considered; one is the product-form of attack and defence efficiencies, the other is the proportion-form of attack and defence efficiencies. In our work, we focus on the following questions: *1) How does a player select targets to attack/defend and how does he* *allocate resources to heterogenous targets at the NE? 2) How do the resource limits of the players influence the NE and their performance at the NE?*

This work provides important insights into the multi-dimensional network security issues. In the *product-form* breaching model, both players allocate positive resources to the subsets of more valuable targets at the NE. For any two targets protected by the defender, he always allocates more resources to one with a higher value. While the attacker may allocate more resources to the more important targets, or evade the well-protected valuable targets, depending on the defender's *relative ineffectiveness of defence (RID)*. We also show the existence of multiple NEs that yield different utilities to the players when the attack and defence efficiencies are linear. In the *proportion-form* breaching model, the attacker and the defender allocate resources on all the targets. Each player allocates more resources to more valuable targets. In both models, a player may place positive amount of resources to more targets when he possesses a larger resource budget. A resource insufficient player can reduce the utility of his opponent by acquiring more resources, while not necessarily improving his own utility at the NE.

Our major contributions are summarized as below:

- We propose a novel network security game that captures the competition on multiple targets simultaneously.

- We present efficient algorithms to find the unique NE when the games are strictly concave.

- We also show the existence of multiple NEs when the objective functions are not strictly concave in the product-form game.

- We provide important insights on how the attacker(s) and the defender allocate resources to heterogeneous targets under resource limits, and how the NE(s) is (are) influenced by the resource limits.

The remainder of this paper is as follows. Section II describes the game model. Section III carries out the analysis of the NE as well as the impact of resource limits on the NE. Section IV presents a linear intrusion detection game analysis. We analyse the NE of the proportion-form breaching model in Section V. Section VI surveys the related works and Section VII concludes.

II. Game Model and Basic Properties

In this section, we present a game-theoretic model for network security that contains two players; one being an attacker and the other being a defender. They simultaneously compete on multiple targets.

A. Motivation

We are motivated by new features of network attacks and defences that are not well captured by existing works (e.g. [3] and references therein). Most of state-of-the-art researches focus on the one dimensional strategies (i.e., monitoring probability of intrusion, channel access probability or insurance adoption of a node). Such game models are insufficient to characterize the modern days security attacks such as phishing and mobile malware, etc. Here, we present some salient features of network security issues that lead to our game formulation.

Firstly, the attackers and the defenders are resource constrained. Resources are defined in a variety of forms. For instance, in the fast-flux phishing attack, the hijacked IP address is one type of resources of the attackers. In a mobile malware attack, the attacker's resources can be the technology and the manpowers used to spoof the security check mechanism of the third-party apps markets. In DDoS attacks, a botmaster is usually able to control only a few thousands active bots [19]. Similarly, the defender needs to allocate resources such as technologies and manpowers to detect and remove these attacks. In general, both the attacker and the defender only possess limited resources.

Secondly, the efficiencies of attacks and defences depend on how many resources are allocated. While existing works (e.g. references in [3]) assume that the payoffs of the attacker and the defender are determined by whether the target is attacked or defended. We take phishing attack as an example. By creating more malicious websites, the phishing attacker is able to seduce more users and to perform more persistent attacks. If the defender allocates more resources to perform proactive detection, more malicious sites will be ferreted out in zero-day, and the attack time window will be reduced. Similarly, if more efforts are spent to create malicious Android apps, the attacker can carry out more effective camouflage, thus gaining more profits through stealing private information or sending premium SMS imperceptibly. As a countermeasure, the defender installs these apps on his cloud and examines their suspicious events for a certain amount of time.

Last but not least, the attacker and the defender battle not on a single, but rather, multiple targets. Attackers are profit-driven. They are inclined to attack many targets in parallel. The targets are specified as different E-banks in phishing, different apps in mobile malware attacks and different servers in network intrusions. Note that the targets vary in their valuations, so the attacker and the defender may allocate different amount of resources to them. To attack (resp. protect) multiple targets, more resources are required. How to perform parallel attacks becomes a challenging problem when players have certain resource limits. All these motivate our study on the strategic allocation of limited resources by the players on multiple targets simultaneously.

B. Models

Let us start with the basic security game which consists of two players, an attacker $\mathcal{A}$ and a defender $\mathcal{D}$. The attacker launches attacks on N targets (or "battlefields" interchangeably) which we denote as $\mathcal{B}=\{B_1,\cdots,B_N\}$. The target B_i is associated with a weight w_i $(i=1,\cdots,N)$. When $w_i{>}w_j$, B_i is more valuable than B_j. Without loss of generality, we rank all targets from 1 to N in the descending order of their weights (i.e. $w_i>w_j$ if $i<j$).

Attacking a target may consume some resources such as manpower to design malware, social engineering techniques to camouflage them, or dedicate many compromised machines for attacks. Defending a target needs manpower, investment in technology, and computing facilities etc. Here, we monetarize different types of resources. Let c be the price of per-unit of $\mathcal{A}$'s resources, and let $\hat{c}$ be that of $\mathcal{D}$'s resources. We next define two important terms that form the utilities of the attacker and the defender.

- *Attack efficiency.* Let x_i be the amount of resources spent by $\mathcal{A}$ on B_i, and let $f(x_i)$ be the corresponding attack efficiency on target B_i. Here, $f(\cdot)$ reflects the ability of the attacker to intrude a system, or to camouflage the malware, etc. We assume that $f(x_i)$ is a differentiable, strictly increasing and concave function with respect to (w.r.t.) x_i. The concavity means that the increment of attack efficiency decreases when $\mathcal{A}$ further increases x_i. Without loss of generality, we let $f(0)=0$ and $0\leq f(x_i)\leq 1$.
- *Defence efficiency.* Denote y_i as the resources that $\mathcal{D}$ uses to detect and remove the attacks on target B_i. Let $g(y_i)$ be the defence efficiency when $\mathcal{D}$ allocates y_i to B_i. We assume that $g(y_i)$ is a differentiable, strictly increasing and concave function of y_i with $g(0)=0$ and $0\leq g(y_i)\leq 1$. For the sake of convenience, we define a complementary function $\tilde{g}(y_i)$, the defence inefficiency, which has $\tilde{g}(y_i)=1-g(y_i)$. Then, $g(\cdot)$ is a decreasing and convex function.

It is very difficult to capture the loss of victims (also the revenue of the attacker) due to the obscure interaction between the attack efficiency of $\mathcal{A}$ and the defence efficiency of $\mathcal{D}$. Here, we formulate two simplified *breaching* models, one is named a "product-form" model and the other is named a "proportion-form" model. Denote by p_i the breaching probability of target B_i. Then, there exist

- *Product-form model:* $p_i=f(x_i)\tilde{g}(y_i)$;
- *Proportion-form model:* $p_i=\frac{f(x_i)}{f(x_i)+g(y_i)}$.

In the product-form model, the change of attack (resp. defence) efficiency causes a linear change of breaching probability. For mobile phishing attacks, the defence efficiency can be regarded as the probability of detecting malware, and the attack efficiency represents the ratio of victims defrauded by the attacker. Then, the breaching probability can be taken as a product of attack efficiency and defence inefficiency. A classic example of the product-form model is the matrix-form intrusion detection game where $f(x_i)$ and $g(y_i)$ are linear functions [3]. The attack efficiency denotes the probability of performing an attack and the defence efficiency denotes the probability of performing a detection action. In reality, the resources of the attacker and the defender have a coupled effect on the security of a target. The increase of attack efficiency might not yield a linearly augmented breaching probability. However, it is very difficult to quantify their coupling. Here, we present a proportion-form breaching model that generalizes the cyber-security competition in [18] and the DDoS attacks on a single target in [9]. The breaching probability increases with the attack efficiency, while at a shrinking speed.

In practice, both $\mathcal{A}$ and $\mathcal{D}$ have limited resource budgets which we denote by $X_{\mathcal{A}}$ and $Y_{\mathcal{D}}$ respectively, with $0<X_{\mathcal{A}},Y_{\mathcal{D}}<\infty$. Our focus is to unravel the allocation strategies of the players on multiple targets with the consideration of resource limits. To achieve this goal, we make the following assumption on the attack and defence efficiencies.

Assumption: $\lim_{x_i\to\infty}f(x_i)=1$ and $\lim_{y_i\to\infty}g(y_i)=1$ in the product-form model if not mentioned explicitly.

Late on, we consider the linear $f(x_i)$ and $g(y_i)$ that generalize intrusion detection game to multiple targets. As a consequence of attacking B_i, $\mathcal{A}$ receives an expected revenue of w_ip_i. Let $U_{\mathcal{A}}$ be the aggregate profit of $\mathcal{A}$ on all the N targets. We have $U_{\mathcal{A}}=\sum_{i=1}^{N}w_ip_i-c\sum_{i=1}^{N}x_i$. The attacker $\mathcal{A}$ is usually profit driven and is assumed to be risk-neutral. His purpose is to maximize $U_{\mathcal{A}}$ under the resource cap $X_{\mathcal{A}}$. Then, the constrained resource allocation problem is expressed as

$$\begin{aligned}\max_{\{x_i\}_{i=1}^{N}} &\quad U_{\mathcal{A}}\\ \text{subject to} &\quad \sum\nolimits_{i=1}^{N}x_i\leq X_{\mathcal{A}}.\end{aligned}\tag{1}$$

The defender $\mathcal{D}$'s objective is to minimize the revenue of the attacker $\mathcal{A}$ with the consideration of his resource budget. Let $U_{\mathcal{D}}$ be the *disutility* of $\mathcal{D}$ given by $U_{\mathcal{D}}=-\sum_{i=1}^{N}w_ip_i-\hat{c}\sum_{i=1}^{N}y_i$. When $\hat{c}$ (resp. c) is 0, $\mathcal{D}$ (resp. $\mathcal{A}$) has a use-it-or-lose-it cost structure such that he will utilize *all* his resources. The resource allocation problem of $\mathcal{D}$ can be formulated as:

$$\begin{aligned}\max_{\{y_i\}_{i=1}^{N}} &\quad U_{\mathcal{D}}\\ \text{subject to} &\quad \sum\nolimits_{i=1}^{N}y_i\leq Y_{\mathcal{D}}.\end{aligned}\tag{2}$$

Noticing that $\mathcal{A}$ and $\mathcal{D}$ have conflicting objectives, we model the resource allocation problem as a two-player non-cooperative game and we denote it as $\mathbf{G}$. Let $\mathcal{H}$ be a convex hull expressed as $\{(x_i,y_i)|x_i\geq 0,y_i\geq 0,\sum_{i=1}^{N}x_i\leq X_{\mathcal{A}},\sum_{i=1}^{N}y_i\leq Y_{\mathcal{D}}\}$. In what follows, we define a set of concepts for the game.

Definition *1:* Nash Equilibrium: Let $\boldsymbol{x}=(x_1,\cdots,x_N)$ and $\boldsymbol{y}=(y_1,\cdots,y_N)$ be the feasible resource allocations by $\mathcal{A}$ and $\mathcal{D}$ in the convex hull $\mathcal{H}$ respectively. An allocation profile $S=\{\boldsymbol{x}^*,\boldsymbol{y}^*\}$ is a Nash equilibrium (NE) if $U_{\mathcal{A}}(\boldsymbol{x}^*,\boldsymbol{y}^*)\geq U_{\mathcal{A}}(\boldsymbol{x},\boldsymbol{y}^*)$ and $U_{\mathcal{D}}(\boldsymbol{x}^*,\boldsymbol{y}^*)\geq U_{\mathcal{D}}(\boldsymbol{x}^*,\boldsymbol{y})$ for any $\boldsymbol{x}\neq\boldsymbol{x}^*$ and $\boldsymbol{y}\neq\boldsymbol{y}^*$.

Definition *2:* [5] *(Concave game)* A game is called ***concave*** if each player i chooses a real quantity in a convex set to maximize his utility $u_i(x_i,\boldsymbol{x}_{-i})$ where $u_i(x_i,\boldsymbol{x}_{-i})$ is concave in x_i.

Theorem *1:* [5] *(Existence and Uniqueness)* A concave game has a NE. Let M be a $n\times n$ matrix function in which

$M_{ij}{=}\varphi_i \frac{\partial^2 u_i}{\partial x_i \partial x_j}$, for some constant choices of $\varphi_i{>}0$. If $M{+}M^T$ is strictly negative definite, then the NE is unique.

Theorem *2:* The multi-dimensional security game **G** has a unique NE for the product-form breaching model if the attack and defence efficiencies are strictly concave, and for the proportion-form breaching model.

All the proofs in this work can be found in the technical report [20].

III. Nash Equilibrium and Influence of Resource Limits for Product-form Model

In this section, we propose an algorithm to find the NE and present its properties. Furthermore, we analyze how the resource limits $X_{\mathcal{D}}$ and $Y_{\mathcal{D}}$ influence the allocation strategies of the attacker and the defender.

A. Solving NE for the Generalized Game

In the previous section, we have shown the existence of a unique NE in the multi-dimensional security game **G1**. However, we have not stated how to derive the NE, which is nontrivial in fact. Define $(\boldsymbol{x}^*, \boldsymbol{y}^*)$ as the NE of **G1**. We show that $(\boldsymbol{x}^*, \boldsymbol{y}^*)$ has the following property.

Theorem *3:* There exist non-negative variables λ and ρ such that

$$-w_i f(x_i^*)\tilde{g}'(y_i^*) - \hat{c} \begin{cases} = \rho & \text{if} \quad y_i^* > 0 \\ \leq \rho & \text{if} \quad y_i^* = 0 \end{cases}, \tag{3}$$

$$w_i f'(x_i^*)\tilde{g}(y_i^*) - c \begin{cases} = \lambda & \text{if} \quad x_i^* > 0 \\ \leq \lambda & \text{if} \quad x_i^* = 0 \end{cases}, \tag{4}$$

where

$$\begin{cases} \lambda \geq 0 & \text{if} \quad \sum_{i=1}^N x_i^* = X_{\mathcal{A}} \\ \lambda = 0 & \text{if} \quad \sum_{i=1}^N x_i^* < X_{\mathcal{A}} \end{cases} \quad \text{and} \tag{5}$$

$$\begin{cases} \rho \geq 0 & \text{if} \quad \sum_{i=1}^N y_i^* = Y_{\mathcal{D}} \\ \rho = 0 & \text{if} \quad \sum_{i=1}^N y_i^* < Y_{\mathcal{D}} \end{cases}. \tag{6}$$

Herein, λ and ρ are viewed as shadow prices of violating the resource limits. From Theorem 3, one can see that x_i^* and y_i^* may take on 0, which occurs when $\mathcal{A}$ or $\mathcal{D}$ decides not to attack or defend target B_i. Our main question here is that given $X_{\mathcal{A}}$ and $Y_{\mathcal{D}}$, how λ and ρ are solved at the NE? Before answering this question, we state the sets of targets with positive resources of $\mathcal{A}$ and $\mathcal{D}$ at the NE.

Lemma *1:* Let $K_{\mathcal{A}}$ be the number of targets with positive resources of $\mathcal{A}$, and $K_{\mathcal{D}}$ be that with positive resources of $\mathcal{D}$ at the NE. We have i) the set of targets being attacked is $\{B_1, \cdots, B_{K_{\mathcal{A}}}\}$ and the set of targets being defended is $\{B_1, \cdots, B_{K_{\mathcal{D}}}\}$; ii) $K_{\mathcal{A}} \geq K_{\mathcal{D}}$.

Remark: The utility of Lemma 1 is that it *greatly reduces* the space of searching $K_{\mathcal{D}}$ and $K_{\mathcal{A}}$, which is essential for us to compute the values of λ, ρ, x_i^* and y_i^* at the NE. In fact, we only need to test at most $(N{+}1)(N{+}2)/2$ possible sets of targets. Define two inverse functions $h_{\mathcal{D}}(\cdot) := \{\tilde{g}'\}^{-1}(\cdot)$ and $h_{\mathcal{A}}(\cdot) := \{f'\}^{-1}(\cdot)$. At the NE, the resources used by $\mathcal{A}$ and $\mathcal{D}$ on a target are given by

$$x_i^* = \begin{cases} h_{\mathcal{A}}(\frac{c+\lambda}{w_i\tilde{g}(y_i^*(\lambda,\rho))}) & \forall \ i \leq K_{\mathcal{D}} \\ h_{\mathcal{A}}(\frac{c+\lambda}{w_i\tilde{g}(0)}) & \forall \ K_{\mathcal{D}}{<}i{\leq}K_{\mathcal{A}} \\ 0 & \forall \ i > K_{\mathcal{A}} \end{cases}, \tag{7}$$

$$y_i^* = \begin{cases} h_{\mathcal{D}}(\frac{-(\rho+\hat{c})}{w_i f(x_i^*(\lambda,\rho))}) & \forall \ i \leq K_{\mathcal{D}} \\ 0 & \forall \ i > K_{\mathcal{D}} \end{cases}. \tag{8}$$

In what follows, we define a set of notations w.r.t. the total resources (denoted as Tot_Res) used by both players at the NE in Table I. The pair $(X_{\mathcal{A}}^{suf}, Y_{\mathcal{D}}^{suf})$ denote the *sufficient* amount of resources needed by $\mathcal{A}$ and $\mathcal{D}$ when λ and ρ are both 0. If both $X_{\mathcal{A}}{>}X_{\mathcal{A}}^{suf}$ and $Y_{\mathcal{D}}{>}Y_{\mathcal{D}}^{suf}$ hold, $\mathcal{A}$ and $\mathcal{D}$ have some unused resources at the NE. Then, the strategies of $\mathcal{A}$ and $\mathcal{D}$ on one target are independent of the other targets. We can partition the plane of $(X_{\mathcal{A}}, Y_{\mathcal{D}})$ into four domains: $\mathbf{D_1}$) $X_{\mathcal{A}}{\geq}X_{\mathcal{A}}^{suf}$ and $Y_{\mathcal{D}}{\geq}Y_{\mathcal{D}}^{suf}$; $\mathbf{D_2}$) $X_{\mathcal{A}}{<}X_{\mathcal{A}}^{suf}$ and $Y_{\mathcal{D}}{\geq}\hat{Y}_{\mathcal{D}}^{suf}$; $\mathbf{D_3}$) $X_{\mathcal{A}}{\geq}\hat{X}_{\mathcal{A}}^{suf}$ and $Y_{\mathcal{D}}{<}Y_{\mathcal{D}}^{suf}$; $\mathbf{D_4}$) none of the above. If $(X_{\mathcal{A}}, Y_{\mathcal{D}}) \in D_1$, the consumed resources of $\mathcal{A}$ and $\mathcal{D}$ at the NE are $X_{\mathcal{A}}^{suf}$ and $Y_{\mathcal{D}}^{suf}$ respectively. If $(X_{\mathcal{A}}, Y_{\mathcal{D}}) \in D_2$, the resources of $\mathcal{A}$ are insufficient. Then, $\mathcal{A}$ uses $X_{\mathcal{A}}$ resources and $\mathcal{D}$ uses $\hat{Y}_{\mathcal{D}}^{suf}$ at the NE. If $(X_{\mathcal{A}}, Y_{\mathcal{D}}) \in D_3$, the resources of $\mathcal{D}$ are insufficient. Then, $\mathcal{A}$ uses $\hat{X}_{\mathcal{A}}^{suf}$ resources and $\mathcal{D}$ uses $Y_{\mathcal{D}}$ at the NE. If $(X_{\mathcal{A}}, Y_{\mathcal{D}}) \in D_4$, $\mathcal{A}$ uses $X_{\mathcal{A}}$ and $\mathcal{D}$ uses $Y_{\mathcal{D}}$ resources at the NE. The partition of $(X_{\mathcal{A}}, Y_{\mathcal{D}})$ enables us to understand when the attacker (resp. the defender) possesses sufficient amount of resources for the attack (resp. defence).

$X_{\mathcal{A}}^*$	$:= \sum_{i=1}^N x_i^*$ (Tot_Res used by $\mathcal{A}$ at the NE)
$Y_{\mathcal{D}}^*$	$:= \sum_{i=1}^N y_i^*$ (Tot_Res used by $\mathcal{D}$ at the NE)
$X_{\mathcal{A}}^{suf}$	Tot_Res used by $\mathcal{A}$ at the NE with $\lambda{=}\rho{=}0$
$Y_{\mathcal{D}}^{suf}$	Tot_Res used by $\mathcal{D}$ at the NE with $\lambda{=}\rho{=}0$
$\hat{X}_{\mathcal{A}}^{suf}$	Tot_Res needed by $\mathcal{A}$ at the NE to let $\lambda{=}0$, given $Y_{\mathcal{D}} < Y_{\mathcal{D}}^{suf}$ (i.e. $\rho{>}0$)
$\hat{Y}_{\mathcal{A}}^{suf}$	Tot_Res needed by $\mathcal{D}$ at the NE to let $\rho{=}0$, given $X_{\mathcal{A}} < X_{\mathcal{A}}^{suf}$ (i.e. $\lambda{>}0$)

TABLE I
NOTATIONS OF TOTAL AMOUNT OF RESOURCES

The remaining challenge on deriving the NE is how λ and ρ are found for the given $K_{\mathcal{A}}$ and $K_{\mathcal{D}}$. Intuitively, we can solve λ and ρ based on Eqs. (5)(6)(7)(8). However, there does not exist an explcit expression in general. We propose a bisection algorithm in Fig. 1 to search λ and ρ. The basic idea is to express ρ as two functions of λ, $\rho_1(\lambda)$ obtained from Eqs. (5)(7)(8) and $\rho_2(\lambda)$ obtained from Eqs. (6)(7)(8), and then compute their intersection. To guarantee that the bisection algorithm can find feasible λ and ρ if they exist, we show the monotonicity of $\rho_1(\lambda)$ and $\rho_2(\lambda)$ in the following lemma.

Lemma *2:* Suppose that feasible λ and ρ (i.e. $\lambda, \rho{\geq}0$) exist for the fixed $K_{\mathcal{A}}$ and $K_{\mathcal{D}}$ at the NE. The following properties hold i) if λ is 0, there has a unique $\rho \geq 0$; ii) if ρ is 0, there has a unique λ; iii) $\rho_1(\lambda)$ is a strictly increasing function and $\rho_2(\lambda)$ is a strictly decreasing function.

The monotonicity property enables us to use bisection algorithm to check the existence of the pair (λ, ρ) and solve them if they exist. When $X_{\mathcal{A}}$ and $Y_{\mathcal{D}}$ are sufficient, the NE can be directly computed via eqs.(7) and (8). When the resources of either $\mathcal{A}$ or $\mathcal{D}$ are insufficient, the NE is found by the lines 5$\sim$17 in Fig.1. When both players have insufficient resources, the NE is obtained by the lines 18$\sim$26. The complexity order of finding the sets with positive resource allocation is merely $O(N^2)$.

```
Input: $N$, $X_{\mathcal{A}}$, $Y_{\mathcal{D}}$, $w_i$, $c$, $\hat{c}$, $f(\cdot)$ and $g(\cdot)$;
Output: $K_{\mathcal{A}}$, $K_{\mathcal{D}}$, $\lambda$, $\rho$, $x_i^*$ and $y_i^*$
1: Initialize $K_{\mathcal{A}} = K_{\mathcal{D}} = N$
2: Let $\lambda$=$\rho$=0, compute $y_i^*$, $x_i^*$ using eqs. (7),(8) for all $i$;
3: Compute $X_{\mathcal{A}}^{suf} := \sum_{i=1}^{N} x_i^*$ and $Y_{\mathcal{D}}^{suf} = \sum_{i=1}^{N} y_i^*$;
4. If both $X_{\mathcal{A}} \geq X_{\mathcal{A}}^{suf}$ and $Y_{\mathcal{D}} \geq Y_{\mathcal{D}}^{suf}$, exit;
5: For $K_{\mathcal{A}} \geq 1$
6:   $K_{\mathcal{D}} = K_{\mathcal{A}}$
7:   For $K_{\mathcal{D}} \geq 1$
8:     If $X_{\mathcal{A}} \leq X_{\mathcal{A}}^{suf}$
9:       Find $\lambda$ by letting $\rho = 0$ and $X_{\mathcal{A}}^* = X_{\mathcal{A}}$ via (7)(8);
10:    Elseif $Y_{\mathcal{D}} \leq Y_{\mathcal{D}}^{suf}$
11:      Find $\rho$ by letting $\lambda = 0$ and $Y_{\mathcal{D}}^* = Y_{\mathcal{D}}$ via (7)(8);
12:    End;
13:    If $x_i^* \geq 0$, $y_i^* \geq 0$, exit;
14:    $K_{\mathcal{D}} = K_{\mathcal{D}} - 1$
15:  End
16:  $K_{\mathcal{A}} = K_{\mathcal{A}} - 1$
17: End
18: For $K_{\mathcal{A}} \geq 1$
19:  $K_{\mathcal{D}} = K_{\mathcal{A}} = N$
20:  For $K_{\mathcal{D}} \geq 1$
21:    Compute the fixed point $(\rho, \lambda)$ which solves (7)
       and (8) by setting $Y_{\mathcal{D}}^*$=$Y_{\mathcal{D}}$ and $X_{\mathcal{A}}^*$=$X_{\mathcal{A}}$; Given
       new pair $(\lambda, \rho)$, compute $y_i^*$ and $x_i^*$ via (7) and (8);
22:  If $x_i^* \geq 0$, $y_i^* \geq 0$, exit;
23:  $K_{\mathcal{D}} = K_{\mathcal{D}} - 1$
24:  End
25:  $K_{\mathcal{A}} = K_{\mathcal{A}} - 1$
26: End
```

Fig. 1. Algorithm to find $K_{\mathcal{A}}$, $K_{\mathcal{D}}$, λ, ρ, x_i^* and y_i^* at the NE

B. Properties of NE

Given the resource limits $X_{\mathcal{A}}$, $Y_{\mathcal{D}}$ and other system parameters, we now know the way to compute the unique NE. Our subsequent question is how a player disposes resources on heterogeneous targets at the NE.

Lemma *3:* The NE $(\boldsymbol{x}^*, \boldsymbol{y}^*)$ satisfies the following properties:

- $y_i^* \geq y_j^*$ for $1 \leq i < j \leq K_{\mathcal{D}}$;
- $x_i^* \geq x_j^*$ for $K_{\mathcal{D}} < i < j \leq K_{\mathcal{A}}$;
- i) $x_i^* > x_j^*$ if $\frac{\tilde{g}'(y)}{\tilde{g}(y)}$ is strictly increasing w.r.t. y, ii) $x_i^* = x_j^*$ if $\frac{\tilde{g}'(y)}{\tilde{g}(y)}$ is a constant, and iii) $x_i^* < x_j^*$ if $\frac{\tilde{g}'(y)}{\tilde{g}(y)}$ is strictly decreasing w.r.t. y for all $1{\leq}i{<}j{\leq}K_{\mathcal{D}}$.

The first property manifests that $\mathcal{D}$ is inclined to allocate more resources to the targets with higher weights at the NE. The second property means that if two targets are not protected by $\mathcal{D}$ at the NE, $\mathcal{A}$ allocates more resources to the one of higher value. However, it is uncertain whether $\mathcal{A}$ allocates more (or less) resources to a high (or lower) value target among the top $K_{\mathcal{D}}$ targets with positive resources of $\mathcal{D}$. We next use three examples to highlight that all the possibilities can happen. These examples differ in the choice of (complementary) defence efficiency functions. We define a new term, "relative ineffectiveness of defence (RID)", as the expression $|\frac{\tilde{g}'(y)}{\tilde{g}(y)}|$. Note that the first-order derivative $\tilde{g}'(y)$ reflects how fast (i.e. the slope) $\tilde{g}(y)$ decreases with the increase of y. RID reflects the relative slope that the increase of y reduces $\tilde{g}(y)$. If $|\frac{\tilde{g}'(y)}{\tilde{g}(y)}|$ is increasing in y, further increasing y makes $\tilde{g}(y)$ decreases faster and faster. On the contrary, if $|\frac{\tilde{g}'(y)}{\tilde{g}(y)}|$ is decreasing in y, further increasing y only results in a smaller and smaller relative reduction of $\tilde{g}(y)$. For a better understanding, we investigate the competition on B_1 and B_2 that are allocated positive resources by $\mathcal{A}$ and $\mathcal{D}$.

Example 1 (InvG): $f(x)$=$1{-}(1{+}x)^{-a}$ and $\tilde{g}(y)$=$\frac{1}{1+\theta y}$. The following defence inefficiency equality holds, $|\frac{\tilde{g}'(y)}{\tilde{g}(y)}|$=$\frac{\theta}{1+\theta y}$. Then, we obtain $\frac{w_i}{w_j} = (\frac{1+x_i}{1+x_j})^{2(1+a)} \frac{1-(1+x_i)^{-a}}{1-(1+x_j)^{-a}}$. Due to $w_i > w_j$, it is easy to show $x_i > x_j$ by contradiction.

Example 2 (ExpG): $f(x)$=$1{-}(1{+}x)^{-a}$ and $g(y)$=$\exp(-\theta y)$. The expression $|\frac{\tilde{g}'(y)}{\tilde{g}(y)}|$ is equal to θ. According to the KKT conditions in Theorem 3, there has $(\frac{1+x_i}{1+x_j})^{1+a} \frac{1-(1+x_i)^{-a}}{1-(1+x_j)^{-a}} = 1$. The above equation holds only upon $x_i = x_j$.

Example 3 (QuadG): $f(x)$=$1 - (1 + x)^{-a}$ and $\tilde{g}(y) = (1 - \theta y)^2$. There exists $|\frac{\tilde{g}'(y)}{\tilde{g}(y)}|$=$\frac{2\theta}{1-\theta y}$. Theorem 3 yields $\frac{w_j}{w_i} = (\frac{1+x_i}{1+x_j})^{1+a} (\frac{1-(1+x_i)^{-a}}{1-(1+x_j)^{-a}})^2$. Then, there has $x_i^* < x_j^*$.

Remark 2: For InvG-like $\tilde{g}(y)$, RID is strictly decreasing. The attacker's best strategy is to allocate more resources to more important targets. In a word, the attacker and the defender have a "head-on confrontation". For ExpG-like $\tilde{g}(y)$, RID is a constant. The attacker sees a number of equally profitable targets. For QuadG-like $\tilde{g}(y)$, RID is an increasing function. The attacker tries to avoid the targets that are *effectively* protected by the defender.

Intuitively, when a player does not possess sufficient resources, he will gain a higher utility if his resource limit increases. First of all, we give an example to support this claim. Suppose that not all the targets are attacked by $\mathcal{A}$ and $Y_{\mathcal{D}}$ is insufficient. When $X_{\mathcal{A}}$ increases, $\mathcal{A}$ can at least gain more profits by allocating the extra resources to the targets that are not under attack. We next present a counter-intuitive example. Suppose that $\mathcal{A}$ and $\mathcal{D}$ allocate positive amount of resources to all the targets at the NE. The resources of $\mathcal{A}$ are insufficient while those of $Y_{\mathcal{D}}$ are sufficient, that is, $\lambda > 0$ and $\rho = 0$. When $X_{\mathcal{A}}$ increases, it is easy to show by contradiction that λ decreases and x_i increases. Due to the equality $-w_i f(x_i)\tilde{g}'(y_i) = \hat{c}$ in the KKT conditions, y_i also becomes larger. The utility of the attacker on target B_i at the NE is given by $w_i f(x_i)\tilde{g}(y_i) - cx_i = -\hat{c}\frac{\tilde{g}(y_i)}{\tilde{g}'(y_i)} - cx_i$. If RID of the defender, $|\frac{\tilde{g}'(y)}{\tilde{g}(y)}|$, is a constant or an increasing function of y_i, the expression $-\hat{c}\frac{\tilde{g}(y_i)}{\tilde{g}'(y_i)}$ is a constant or decreases as y_i increases. Hence, the utility of the attacker on target B_i decreases when $X_{\mathcal{A}}$ increases.

Remark 3: When the defender's resources are insufficient, the attacker gains more profits by acquiring more resources and allocating them to more important targets. When the defender's resources are sufficient, the attacker may explore new targets to attack, other than using all the resources to battle with the resource sufficient defender at the NE.

IV. A Linear Intrusion Detection Game for Product-form Model

In this section, we investigate the existence and uniqueness of NE of an intrusion detection game where the attack and defence efficiencies are linear functions.

A. A Matrix-form Game

We study a matrix-form multi-dimensional intrusion detection game. The payoff matrix on target B_i is shown in Fig.2 where A (resp. NA) denotes "attack" (resp. "not attack") strategy, and D (resp. ND) denotes "defend" (resp. "not defend") strategy. Here, w_i denotes the loss of victims for the pair-wise strategies (A, ND) and γw_i denotes that for (A, D) with $\gamma \in (0, 1)$. Let c and $\hat{c}$ be the costs of the "attack" and the "defend" strategies. Note that $\hat{c}$ refers to not only the cost of resources, but also the cost of performance such as QoS or false alarm of benign events. We consider the mixed strategies of $\mathcal{A}$ and $\mathcal{D}$ in which $\mathcal{A}$ attacks target B_i with probability x_i and $\mathcal{D}$ detects this target with probability y_i. Each player only has one action on all the targets, which yields the resource constraints: $\sum_{i=1}^N x_i \le X_{\mathcal{A}} \le 1$, $\sum_{i=1}^N y_i \le Y_{\mathcal{D}} \le 1$ and $0 \le x_i, y_i \le 1$.

To make the game non-trivial, we let $\gamma w_i \le c$ and $w_i > c \; \forall i$, i.e. the loss of victims is greater than the cost of the attacker on an unprotected target, and is less than this cost on a protected target. Given the attack probabilities $\{x_i\}_{i=1}^N$ and the detection probabilities $\{y_i\}_{i=1}^N$, the utilities of $\mathcal{A}$ and $\mathcal{D}$ can be derived easily,

$$\begin{aligned} U_{\mathcal{A}} &= w_i x_i - (1-\gamma) w_i x_i y_i - c x_i, \\ U_{\mathcal{D}} &= -w_i x_i + (1-\gamma) w_i x_i y_i - \hat{c} y_i. \end{aligned}$$

The above utility functions fall in the category of our product-form game with $f(x) := x$ and $\tilde{g}(y) := 1 - (1 - \gamma)y$. The resource constraints hold naturally because the sum of attack probabilities is no larger than 1, and the sum of detection probabilities is also no larger than 1. For the sake of simplicity, we denote a new variable as $\bar{\gamma} := 1 - \gamma$.

	D	ND
A	$(\gamma w_i - c, -\gamma_1 w_i - \hat{c})$	$(w_i - c, -w_i)$
NA	$(0, -\hat{c})$	$(0, 0)$

Fig. 2. Payoff Matrix

B. Computing NE

We take the derivatives of $U_{\mathcal{A}}$ (resp. $U_{\mathcal{D}}$) over x_i (resp. y_i) and obtain

$dU_{\mathcal{A}}/dx_i = w_i - w_i\bar{\gamma}y_i - c, \quad dU_{\mathcal{D}}/dy_i = w_i\bar{\gamma}x_i - \hat{c}.$

The existence of a NE is guaranteed by the concavity of the game. Before diving into the solution of the NE, we present a property of the sets of targets that are attacked or defended at the NE.

Lemma *4:* The sets of targets with positive resources at the NE are given by i) $\{B_1, \cdots, B_{K_{\mathcal{A}}}\}$ for the attacker and $\{B_1, \cdots, B_{K_{\mathcal{D}}}\}$ for the defender; ii) either $K_{\mathcal{A}} = K_{\mathcal{D}}$ or $K_{\mathcal{A}} = K_{\mathcal{D}} + 1$.

Lemma 4 is the sufficient condition of the existence of NE. Similar to Lemma 1, $\mathcal{A}$ and $\mathcal{D}$ allocate resources to the subsets of more important targets. The difference lies in that $\mathcal{A}$ may allocate resources to more targets than $\mathcal{D}$ when $f(\cdot)$ and $g(\cdot)$ are nonlinear functions, but to at most one more target than $\mathcal{D}$ when $f(\cdot)$ and $g(\cdot)$ are our linear functions. We proceed to find the NE by considering different regions of $X_{\mathcal{A}}$ and $Y_{\mathcal{D}}$ in the following theorem.

Theorem *4:* The multi-dimensional intrusion detection game admits a NE as below

- $P_{\mathcal{A}}(k){<}X_{\mathcal{A}}{<}P_{\mathcal{A}}(k{+}1)$ and $Y_{\mathcal{D}}{>}P_{\mathcal{D}}(k{+}1)$ for $0{\le}k{\le}N{-}1$. The NE is uniquely determined by
$$x_i^* = \begin{cases} \frac{\hat{c}}{w_i\bar{\gamma}}, & \forall\, i \le k \\ X_{\mathcal{A}} - \sum_{j=1}^k \frac{\hat{c}}{w_j}, & i{=}k{+}1 \\ 0, & \forall\, i{>}k{+}1 \end{cases} \tag{9}$$
$$y_i^* = \begin{cases} (1 - \frac{w_{k+1}}{w_i})\frac{1}{\bar{\gamma}}, & \forall\, i{\le}k \\ 0, & \forall\, i > k \end{cases}. \tag{10}$$
Here, the sum over an empty set is 0 conventionally.
- $P_{\mathcal{D}}(k){<}Y_{\mathcal{D}}{<}P_{\mathcal{D}}(k{+}1)$ and $X_{\mathcal{A}}{>}P_{\mathcal{A}}(k)$ for $1{\le}k{\le}N$. The NE is uniquely determined by
$$x_i^* = \begin{cases} (\sum_{j=1}^k \frac{w_i}{w_j})^{-1} X_{\mathcal{A}}, & \forall\, i \le k \\ 0, & \forall\, i > k \end{cases} \tag{11}$$
$$y_i^* = \begin{cases} (\sum_{j=1}^k \frac{w_i}{w_j})^{-1}\big(Y_{\mathcal{D}} - \frac{1}{\bar{\gamma}}k\big) + \frac{1}{\bar{\gamma}}, & \forall i{\le}k \\ 0, & \forall i{>}k \end{cases}. \tag{12}$$
- $X_{\mathcal{A}}{>}P_{\mathcal{A}}(N)$ and $Y_{\mathcal{D}}{>}P_{\mathcal{D}}(N{+}1)$. The NE is uniquely determined by
$$x_i^* = \frac{\hat{c}}{w_i\bar{\gamma}}, \;\; y_i^* = \frac{1}{\bar{\gamma}} - \frac{c}{w_i\bar{\gamma}}, \;\; \forall\;\, 1{\le}i{\le}N. \tag{13}$$
- $X_{\mathcal{A}}{=}P_{\mathcal{A}}(k)$ and $Y_{\mathcal{D}}{\ge}P_{\mathcal{D}}(k)$ for $1{\le}k{\le}N$. Denote by $\tilde{Y}_{\mathcal{D}}$ an arbitrary real number in the range

$[P_{\mathcal{D}}(k), \min\{Y_{\mathcal{D}}, P_{\mathcal{D}}(k{+}1)\}]$. A NE is given by

$$x_i^* = \begin{cases} \frac{\hat{c}}{w_i\bar{\gamma}}, & \forall \ i \leq k \\ 0, & \forall \ k{+}1{\leq}i{\leq}N \end{cases} \tag{14}$$

$$y_i^* = \begin{cases} \frac{1}{\bar{\gamma}}{+}(\sum_{j=1}^{k} \frac{w_i}{w_j})^{-1}(\tilde{Y}_{\mathcal{D}}{-}k\frac{1}{\bar{\gamma}}), & \forall\, i \leq k \\ 0, & \forall\, i > k \end{cases}. \tag{15}$$

- $Y_{\mathcal{D}}{=}P_{\mathcal{D}}(k)$ and $P_{\mathcal{A}}(k{-}1){\leq}X_{\mathcal{A}}{\leq}P_{\mathcal{A}}(k)$ for $2{\leq}k{\leq}N$. Denote by $\tilde{X}_{\mathcal{A}}$ an arbitrary real number in the range $[P_{\mathcal{A}}(k{-}1), X_{\mathcal{A}}]$. A NE is given by

$$x_i^* = \begin{cases} (\sum_{j=1}^{k} \frac{w_i}{w_j})^{-1}\tilde{X}_{\mathcal{A}}, & \forall\, i \leq k \\ 0, & \forall\, i{>}k{+}1 \end{cases} \tag{16}$$

$$y_i^* = \begin{cases} (1{-}\frac{w_{k+1}}{w_i})\frac{1}{\bar{\gamma}}, & \forall\, i \leq k \\ 0, & \forall\, i > k \end{cases}. \tag{17}$$

Here, $P_{\mathcal{A}}(k)$ and $P_{\mathcal{D}}(k)$ are defined as $P_{\mathcal{A}}(0){:=}0$, $P_{\mathcal{A}}(k){:=}\sum_{i=1}^{k} \frac{\hat{c}}{w_i\bar{\gamma}}$, $\forall\, 1{\leq}k{\leq}N$; $P_{\mathcal{D}}(1){=}0$, $P_{\mathcal{D}}(k){:=}$ $\sum_{i=1}^{k-1} \frac{1}{\bar{\gamma}}(1{-}\frac{w_k}{w_i})$, and $P_{\mathcal{D}}(N{+}1){:=}\frac{1}{\bar{\gamma}}N{-}\sum_{i=1}^{N} \frac{c}{w_i\bar{\gamma}}$.

We illustrate the relationship between NE and resource limits in Fig.3. When $f(\cdot)$ and $g(\cdot)$ are linear, the best response of a player becomes a step-like function. The feasible domain of $(X_{\mathcal{A}}, Y_{\mathcal{D}})$ is partitioned into three parts: i) D_1 - sufficient $X_{\mathcal{A}}$ and sufficient $Y_{\mathcal{D}}$; ii) D_2 - insufficient $X_{\mathcal{A}}$ and sufficient $Y_{\mathcal{D}}$; iii) D_4 - insufficient $X_{\mathcal{A}}$ and insufficient $Y_{\mathcal{D}}$. The total consumed resources at the NEs for D_1 and D_2 are located in the step-like boundary curve. When $X_{\mathcal{A}}$ or $Y_{\mathcal{D}}$ take some special values, the boundary curve illustrates the existence of multiple NEs. In the horizontal boundary, different NEs bring the same utility to the attacker, but different utilities to the defender. In the vertical boundary, the utilities of the defender are the same, while those of the attacker are different. Let us take a look at an example with $X_{\mathcal{A}}{=}\frac{\hat{c}}{w_1\bar{\gamma}}$ and $Y_{\mathcal{D}}{>}(1{-}\frac{w_2}{w_1})\frac{1}{\bar{\gamma}}$. Two NEs on target B_1 can be $(x_1^*, y_1^*)_{(1)}{=}(\frac{\hat{c}}{w_1\bar{\gamma}}, 0)$ and $(x_1^*, y_1^*)_{(2)}{=}(\frac{\hat{c}}{w_1\bar{\gamma}}, (1{-}\frac{w_2}{w_1})\frac{1}{\bar{\gamma}})$. Both $\mathcal{A}$ and $\mathcal{D}$ do not allocate resources to other targets. The utility of $\mathcal{D}$ is given by $U_{\mathcal{D}}{=}{-}\frac{1}{\bar{\gamma}}\hat{c}$ at the both NEs. The utilities of $\mathcal{A}$ are given by $U_{\mathcal{A}}^{(1)}{=}x_1^*(w_1{-}c)$ and $U_{\mathcal{A}}^{(2)}{=}x_1^*(w_2{-}c)$ at the two NEs. At the first NE, B_1 is the most profitable to $\mathcal{A}$. At the second NE, B_1 and B_2 are equally profitable. In both NEs, $\mathcal{A}$ cannot gain more profits by switching to another allocation strategy unilaterally. Besides, the total consumed resources for D_4 can be mapped to an arbitrary point in this domain, in which both players have insufficient resources.

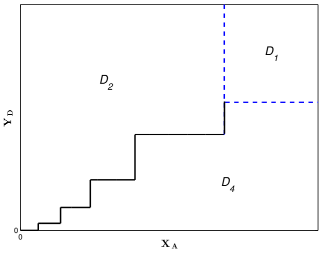

Fig. 3. Sufficiency of $X_{\mathcal{A}}$ and $Y_{\mathcal{D}}$ with linear $f(\cdot)$ and $g(\cdot)$

Remark 4: We summarize the salient properties of the NEs for linear attacking efficiency and linear uptime as below.
1) The targets with $x_i^* > 0$ are equally profitable to $\mathcal{A}$ such that $\mathcal{A}$ has no incentive to change his strategy.
2) $\mathcal{D}$ prefers to allocate more resources to the more valuable targets. As a countermeasure, $\mathcal{A}$ allocates more resources to the targets that are not effectively protected by $\mathcal{D}$.
3) The NE is not unique with some special choices for $X_{\mathcal{A}}$ and $Y_{\mathcal{D}}$. If multiple NEs exist for a given pair $(X_{\mathcal{A}}, Y_{\mathcal{D}})$, they yield the same utility for one player, but different utilities for the other player.

V. Nash Equilibrium for Proportion-form Model

In this section, we analyze the NE strategy of the players on different targets for the proportion-form breaching model.

Nash Equilibrium and its Properties:

We define $(\boldsymbol{x}^*, \boldsymbol{y}^*)$ as the NE of the game for the proportion-form model. Then, based on KKT conditions, $(\boldsymbol{x}^*, \boldsymbol{y}^*)$ is given by the following theorem.

Theorem *5:* There exist non-negative variables λ and ρ such that

$$w_i \frac{f(x_i^*)g'(y_i^*)}{(f(x_i^*) + g(y_i^*))^2} - \hat{c} \begin{cases} = \rho & \text{if} \quad y_i^* > 0 \\ \leq \rho & \text{if} \quad y_i^* = 0 \end{cases}, \tag{18}$$

$$w_i \frac{f'(x_i^*)g(y_i^*)}{(f(x_i^*) + g(y_i^*))^2} - c \begin{cases} = \lambda & \text{if} \quad x_i^* > 0 \\ \leq \lambda & \text{if} \quad x_i^* = 0 \end{cases}, \tag{19}$$

with the slackness conditions in Eq.(5) and (6).

As the first step to find the NE, we need to investigate how many targets will be attacked by $\mathcal{A}$ and defended by $\mathcal{D}$. The following lemma shows that both $\mathcal{A}$ and $\mathcal{D}$ allocate resources to all the targets in $\mathcal{B}$.

Lemma *5:* At the NE, there have $x_i^* > 0$ and $y_i^* > 0$ for all $i = 1, \cdots, K$ if $f(\cdot)$ and $g(\cdot)$ are concave and strictly increasing with $f(0) = 0$ and $g(0) = 0$.

Lemma 5 simplifies the complexity to obtain the NE strategy because we do not need to test whether a target will be attacked or defended. Then, the equalities in Eqs.(18) and (19) hold. Similarly, we partition $(X_{\mathcal{A}}, Y_{\mathcal{D}})$ into four domains to fine the NE: $\mathbf{D_1}$) $X_{\mathcal{A}}{\geq}X_{\mathcal{A}}^{suf}$ and $Y_{\mathcal{D}}{\geq}Y_{\mathcal{D}}^{suf}$; $\mathbf{D_2}$) $X_{\mathcal{A}}{<}X_{\mathcal{A}}^{suf}$ and $Y_{\mathcal{D}}{\geq}\hat{Y}_{\mathcal{D}}^{suf}$; $\mathbf{D_3}$) $X_{\mathcal{A}}{\geq}\hat{X}_{\mathcal{A}}^{suf}$ and $Y_{\mathcal{D}}{<}Y_{\mathcal{D}}^{suf}$; $\mathbf{D_4}$) none of the above. The method to find the NE contains the similar steps as those of the algorithm in Fig.1. We need to check whether $(X_{\mathcal{A}}, Y_{\mathcal{D}})$ is located in a domain from $\mathbf{D_1}$ to $\mathbf{D_4}$ one by one.

We next study how $\mathcal{A}$ and $\mathcal{D}$ allocate resources to different targets, given the resource limits $X_{\mathcal{A}}$ and $Y_{\mathcal{D}}$. The NE strategy satisfies the following properties.

Lemma *6:* $\mathcal{A}$ and $\mathcal{D}$ always allocate more resources to the more important targets, i.e. $x_i^*{>}x_j^*$ and $y_i^*{>}y_j^*$ if $w_i{>}w_j$.

Remark 6: In comparison to the product-form breaching model, the players in the proportion-form breaching model always allocate more resources to the more valuable targets.

For the generalized proportion-form breaching model, it is usually difficult to analyze how the NE and the utilities at the NE are influenced by the resource limits. In the technical report [20], we consider two specific functions, $f(x) = x^a$ and $g(y) = y^a$, for the breaching probability model with $0<a\leq 1$. With this example, we show that $U_{\mathcal{D}}$ decreases accordingly when $X_{\mathcal{A}}$ increases. However, increasing $X_{\mathcal{A}}$ does not necessarily bring a higher utility to $\mathcal{A}$. Similarly, increasing $Y_{\mathcal{D}}$ yields a worse utility to $\mathcal{A}$, but not necessarily resulting a higher utility to $\mathcal{D}$.

VI. Related Work

Today's network attacks have evolved into online crimes such as phishing and mobile malware attacks. The attackers are profit-driven by stealing private information or even the money of victims. Authors in [2] measured the uptime of malicious websites in phishing attacks to quantify the loss of victims. Sheng et al. provided the interviews of experts in [15] to combat the phishing. A number of studies proposed improved algorithms to filter the spams containing links to malicious websites in [16], [17].

Game theoretic studies of network security provide the fundamental understandings of the decision making of attackers and defenders. Authors in [4] used stochastic game to study the intrusion detection of networks. More related works on the network security game with incomplete information and stochastic environment can be found in [3], [10]. Another string of works studied the security investment of nodes whose security level depended on the his security adoption and that of other nodes connected to him. Some models did not consider the network topology [6] and some others studied either fixed graph topologies [11] or the Poisson random graph [7], [12].

Among the studies of network security game, [13], [1], [14] are closely related to our work. In [13], authors used the standard Colonel Blotto game to study the resource allocation for phishing attacks. An attacker wins a malicious website if he allocates more resources than the defender, and loses otherwise. This may oversimplify the competition between an attacker and a defender. Our work differs in that the attackers perform attacks on multiple non-identical banks or e-commerce companies, and the competition is modeled as a non-zero sum game that yields a pure strategy. In [1], the authors formulated a linearized model for deciding the attack and monitoring probabilities on multiple servers in network intrusion attacks. Altman et al. in [14] studied a different type of multi-battlefield competition in wireless jamming attack that provides important insights of power allocation on OFDM channels.

VII. Conclusion

In this work, we model the conflict on multiple targets between a defender and an attacker that are resource constrained. A product-form and a proportion-form security breaching models are considered. We prove the existence of a unique NE, and propose efficient algorithms to search this NE when the game is strictly concave. Our analysis provides important insights in the practice of network attack and defence. For the *product-form* breaching model, i) the defender always allocates more resources to the more important target, while the attacker may not follow this rule; ii) when the defender has sufficient amount of resources, more resources of the attacker might not bring a better utility to him; iii) when the game is not strictly concave, there may exist multiple NEs that yield different utilities of the players. For the *proportion-form* breaching model, iv) both the attacker and the defender allocate more resources to more important targets; v) a resource insufficient player causes a reduction of his opponent's utility, while not necessarily gaining a better utility by himself when his resource limit increases.

References

[1] L. Chen, J. Leneutre, "A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks", *IEEE Trans. Information Forensics and Security*, Vol.4, No.2, 2009.

[2] T. Moore and R. Clayton, "Examining the Impact of Website Takedown on Phishing", *Proc. of eCrime Researchers Summit'07*, Pages:1-13, 2007, New York.

[3] T. Alpcan and T. Basar. *Network Security: A Decision and Game Theoretic Approach*, Cambridge, 2012.

[4] Q. Zhu, H. Tembine and T. Basar. "Network Security Configuration: A Nonzero-sum Stochastic Game Approach", *Proc. of IEEE American Control Conference'10*, 2010.

[5] J.B. Rosen, "Existence and Uniqueness of Equilibrium Points for Concave N-Person Games", *Econometrica*, Vol.33, pp:520-534, 1965.

[6] J. Grossklags, N. Christin and J. Chuang. "Secure or Insure? A Game-Theoretic Analysis of Information Security Games". *Proc. of ACM World Wide Web Conf.'08*, Beijing, 2008.

[7] Z.C. Yang, J.C.S. Lui. "Security Adoption in Heterogeneous Networks: The Influence of Cyber-insurance Market" *Proc. of IFIP Networking'12*, 2012.

[8] J Milletary. "Technical Trends in Phishing Attacks", US-CERT Technical Report. http://www.cert.org/

[9] A. Vulimiri, G.A. Agha, P.B. Godfrey and K. Lakshminarayanan. "How Well Can Congestion Pricing Neutralize Denial of Service Attacks?", *Proc. of ACM Sigmetrics'12*, London, 2012.

[10] M.H. Manshaeiy, Q.Y. Zhu, T. Alpcan, T. Basar and J.P. Hubaux. "Game Theory Meets Network Security and Privacy", *ACM Computing Surveys*, Pages:1-45, 2011.

[11] J. Omic, A. Orda and P. Van Mieghem. "Protecting against network infections: A game theoretic perspective", *Proc. of IEEE Infocom'09*.

[12] M. Lelarge and J. Bolot. "Network externalities and the deployment of security features and protocols in the internet", *Proc. of ACM Sigmetrics'08*, Pages:25-30, 2008.

[13] V. Pham, J. Chuang. "Colonel Blotto in the Phishing War", *Proc. of Decision and Game Theory for Security*, Pages:201-218, 2011.

[14] E. Altman, K. Avrachenkov, and A. Garnaev. "A Jamming Game in Wireless Networks with Transmission Cost", *Proc. of NET-COOP*, Pages:1-12, 2007.

[15] S. Sheng, P. Kumaraguru, A. Acquisti, L. Cranor and J. Hong. "Improving Phishing Countermeasures: An Analysis of Expert Interviews", *Proc. of eCrime Researchers Summit'09*, Pages:1-15, 2009.

[16] S. Marchal, J. Francois, R. State and T. Engel, "Predictive Blacklisting as an Implicit Recommendation System", *Proc. of IEEE Infocom 2010*, Pages:1640-1648, 2010.

[17] S. Marchal, J. Francois, R. State and T. Engel, "Proactive Discovery of Phishing Related Domain Names", *Proc. of RAID 2012*, Pages:190-209, 2012.

[18] V.M. Bier and K. Hausken, "Defending Against Multiple Different Attackers", *European Journal of Operational Research*, No. 211, pp:370-384, 2011.

[19] S. Yu, Y.H. Tian, S. Guo, D.P. Wu, "Can We Beat DDoS Attacks in Clouds?" *IEEE Trans. Parall. Distr.*, 2014.

[20] Y. Xu, C.S. Lui, "Multi-dimensional Network Security Game: How do attacker and defender battle on parallel targets?", *Technical report*, Available at http://homepage.fudan.edu.cn/xuyuedong/research/