Playing with enemies – a game theoretic analysis on intrusion detection in heterogenous networks

Jouer avec l'ennemi – une analyse de la détection d'intrusion dans les réseaux hétérogènes basée sur la théorie des jeux

Lin Chen
Jean Leneutre

2007D014

2007

Département Informatique et Réseaux
Groupe RMS : Réseaux, Mobilité et Sécurité

Jouer avec l’ennemi – une analyse de la détection d’intrusion dans les réseaux hétérogènes basée sur la théorie des jeux

Résumé

Dans ce rapport, nous modélisons les interactions entre les attaquants et les systèmes de détection d’intrusion (IDSs) dans un réseau hétérogène comme un jeu non-coopératif à « somme non nulle ». Nous déduisons les équilibres de Nash dans différents contextes, ce qui permet de déduire le comportement attendu de la part d’attaquants rationnels. Nous caractérisons ensuite le nombre minimum d’IDSs nécessaire pour protéger un système et la stratégie optimale pour qu’un IDS contre efficacement les attaquants. La modélisation est ensuite validée par des résultats de simulation.

Playing with Enemies – A Game Theoretic Analysis on Intrusion Detection in Heterogenous Networks

Lin Chen, Jean Leneutre
Department of Computer Science and Networking
École Nationale Supérieure des Télécommunications
{Lin.Chen, Jean.Leneutre}@enst.fr

***Abstract*—Due to the dynamic, distributed and heterogenous nature of today's networks, intrusion detection systems (IDSs) have become a necessary addition to the security infrastructure and are widely deployed as a complementary line of defense to the classical security approaches. In this paper, we address the intrusion detection problem in heterogenous networks consisting of nodes with different security assets. In our study, two crucial questions are: What are the expected behaviors of rational attackers? What is the optimal strategy of the defenders (IDSs)?**

We answer the questions by formulating the network intrusion detection as a non-cooperative game and performing an in-depth analysis on the Nash equilibrium and the engineering implications behind. Based on our game theoretical analysis, we derive the expected behaviors of rational attackers, the minimum monitor resource requirement and the optimal strategy of the defenders. We then provide the guidelines for IDS design and deployment. Finally, we illustrate the application of our results to design efficient defense system in two typical scenarios. The numerical results show both the correctness of the analytical results and the effectiveness of the proposed guidelines.

I. Introduction

Today's computer and communication networks are becoming more and more dynamic, distributed and heterogenous, which, combined with the complexity of underlying computing and communication environments, increases significantly the security risk by making the network control and management much more challenging than ever. As a consequence, nowadays networks are much more vulnerable to various attacks such as TCP SYN flooding, SSPing and DoS attack, just to name a few. The last few years have witnessed significant increase of attacks and their damages. In such context, the intrusion detection system (IDS) is widely deployed as a complementary line of defense to the classical security approaches aiming at removing the vulnerabilities which may not be very effective or even fail to function in some cases.

In almost all contemporary networks, network nodes (targets from the attackers's point of view) usually have different sensibility levels or they possess different security assets depending on their roles and the data or information they hold. In other words, the networks are usually heterogenous in terms of security. More specifically, some targets are more "attractive" to attackers than others. Examples of such targets includes the servers containing much sensible secret information, high hierarchy nodes in military networks, etc. These targets are usually also better protected and are thus more difficult or costly to attack. In such heterogenous environments, two natural but crucial questions are: What are the expected behaviors of rational attackers? What is the optimal strategy of the defenders (IDSs)?

In this paper, we answer the posed questions by developing a non-cooperative game model of the network intrusion detection problem, analyzing the equilibrium point of the game and investigating the engineering implications behind the analytical results. We then derive optimal strategy for the defender side and the guidelines for IDS design and deployment.

Intrusion detection has been an active research field in recent years. Most research efforts address the problem of how to improve the performance of the IDS: e.g., increase coverage of attack types, boost detection rate and keep false alarm rate low, etc [1], [2], [3]. On the other hand, Subhadrabandhu et al. [8] developed a statistical framework for intrusion detection in ad hoc networks using theories of hypothesis testing and approximation algorithms. Several game theoretical approaches have been proposed to model the interaction between the attackers and IDSs. Kodialam et al. [4] proposed a game theoretic framework to model the intrusion detection game between the service provider and the intruder. The objective of intruder is to minimize the probability of being detected by choosing a set of paths to inject malicious packets, and the objective of the service provider is to sample a set of links to maximize the detection probability. The equilibrium strategy of both players is to play the minmax strategy of the game. Alpcan et al. [5] model the intrusion detection as a noncooperative non-zero-sum game with both finite and continuous-kernel versions. In their model a fictitious player is added to the game to represent the output of the IDS sensor network. The authors showed the existence and uniqueness of the Nash equilibrium and studied the dynamics of the game. [9] studied the problem using Bayesian game theory in the context of ad hoc networks where both players update their strategies based on their observation of previous results. Agah et al. [6] and Alpcan et al. [7] reconsidered the problem in sensor networks where each player's optimal strategy depends only on the payoff function of the opponent.

Our work differs with the existing work in that: 1). We address the network intrusion detection problem in heterogenous environments consisting of targets with different security assets; 2). We conduct quantitative analysis on the equilibrium points of the game and the engineering implications behind to further derive the minimum monitor resource requirement and the optimal strategy of the defenders in such environments.

Our main contributions can be summarized as follows:

- We model the network intrusion detection as a non-cooperative game and perform an in-depth analysis on the equilibrium and the engineering implications behind.
- Based on our game theoretical analysis, we derive the expected behaviors of rational attackers, the minimum monitor resource requirement of the defenders and the optimal strategy of the defenders. We then provide the guidelines for IDS design and deployment.
- We illustrate the application of our results to design efficient defense system in two typical scenarios. The numerical results show both the correctness of the analytical results and the effectiveness of the proposed guidelines.

II. Network Intrusion Detection Game Model

We consider a network $\mathcal{N} = (\mathcal{S}_\mathcal{D}, \mathcal{S}_\mathcal{A}, \mathcal{T})$ where $\mathcal{S}_\mathcal{D}$ is the set of agents equipped with the intrusion detection system (IDS) module which we refer to as *defenders* throughout the paper, $\mathcal{S}_\mathcal{A}$ is the set of *attackers* and $\mathcal{T} = \{1, 2, \cdots, N\}$ is the set of network nodes which may be attacked by the attackers, referred to as *targets*. We start with the simplest case where there are only one attacker and one defender in the system. We model the interactions between them as a non-cooperative game. The objective of the attacker is to attack the targets without being detected. To this end, it chooses the strategy $\mathbf{p} = \{p_1, p_2, \cdots, p_N\}$ which is the attack probability distribution over the target set $\mathcal{T}$ where p_i is the probability of attacking the target i. $\sum_{i\in\mathcal{T}} p_i \leq P \leq 1$ represents the attack resource constraint of the attacker. The constraint $P \leq 1$ can be relaxed if the attacker can attack multiple targets simultaneously, e.g., broadcasting malicious packets to attack many network nodes at the same time. This case will be addressed in later sections. For the defender, in order to detect the attacks, it monitors the targets with the probability distribution $\mathbf{q} = \{q_1, q_2, \cdots, q_N\}$, where q_i is the probability of monitoring the target i. Here monitor means that the defender collects audit data and examines them for of signs of security problems. Similarly, we have $\sum_{i\in\mathcal{T}} q_i \leq Q \leq 1$ that represents the monitor resource constraint of the defender.

We assume that each target $i \in \mathcal{T}$ processes an amount of security asset denoted as W_i, which represents the loss of security when the attacks on i are successful, e.g., loss of reputation, loss of data integrity, cost of damage control, etc. The security assets of the targets depend on their roles in the network and the data or information they hold. We also assume that the gain for the defender is also W_i in case where the attacks on i are detected.

Table 1 illustrates the payoff matrix of the attacker-defender interaction on the target i in the strategic form. In the payoff matrix, a denotes the detection rate (i.e., true positive rate) of the IDS of the defender, b denotes the false alarm rate (i.e., false positive rate), and $a, b \in [0, 1]$. The cost of attacking and monitoring (e.g., energy cost) the target $i \in \mathcal{T}$ are also taken into account in our model and are assumed proportional to the security asset of i, denoted by C_aW_i and C_mW_i respectively. C_fW_i represents the loss of a false alarm. In our study, we implicitly assume that $C_a < 1$, otherwise the attacker has no incentive to attack, similarly $C_m < 1$.

	Monitor	Not monitor
Attack	$(1-2a)W_i - C_aW_i$, $-(1-2a)W_i - C_mW_i$	$W_i - C_aW_i, -W_i$
Not attack	$0, -bC_fW_i - C_mW_i$	$0, 0$

TABLE I
Strategy form of the game for target i

The overall payoff of the attack and the defender is defined by the utility functions U_A and U_I as follows:

$$\begin{aligned} U_A(\mathbf{p}, \mathbf{q}) &= \sum_{i\in\mathcal{T}} p_i q_i \left[(1-2a)W_i - C_aW_i\right] + p_i(1-q_i)(W_i \\ &\quad -C_aW_i) = \sum_{i\in\mathcal{T}} p_i W_i (1 - 2aq_i - C_a) \\ U_I(\mathbf{p}, \mathbf{q}) &= \sum_{i\in\mathcal{T}} p_i q_i(-(1-2a)W_i - C_mW_i) - p_i(1-q_i)W_i \\ &\quad -(1-p_i)q_i(bC_fW_i + C_mW_i) \\ &= \sum_{i\in\mathcal{T}} [q_iW_i\left[p_i(2a + bC_f) - (bC_f + C_m)\right] - p_iW_i] \end{aligned}$$

We are now ready to define the network intrusion detection game with one attacker and one defender.

Definition 1: The intrusion detection game with one attacker and one defender G is defined as follows:

Players: Attacker, Defender

Strategy set: Attacker: $A_A = \{\mathbf{p} : \mathbf{p} \in [0, P]^N, \sum_{i\in\mathcal{N}} p_i \leq P\}$

Defender: $A_D = \{\mathbf{q} : \mathbf{q} \in [0, Q]^N, \sum_{i\in\mathcal{N}} q_i \leq Q\}$

Payoff: U_A for attacker, U_D for defender

Game rule: The attacker/defender selects its strategy $\mathbf{p}/\mathbf{q} \in A_A/A_D$ to maximize U_A/U_D

III. Solving the Game

For non-cooperative games as G, the most important solution concept is the Nash equilibrium (NE), where no player has incentive to deviate from its current strategy [10]. The NE can be seen as optimal "agreements" between the players. In the case of the G, we have the following definition of NE.

Definition 2: A strategy vector $(\mathbf{p}^*, \mathbf{q}^*)$ is said to be a NE of G if neither the attacker nor the defender can improve its utility by unilaterally deviating its strategy from the NE.

$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) \geq U_A(\mathbf{p}', \mathbf{q}^*) & \forall \mathbf{p}' \in A_A \\ U_D(\mathbf{p}^*, \mathbf{q}^*) \geq U_D(\mathbf{p}^*, \mathbf{q}') & \forall \mathbf{q}' \in A_D \end{cases}$$

A. Sensible Target Set

In G, since the attack has limited attack resource, a natural question is that whether a rational attacker will focus on some targets or allocate its attack resource to all targets to reduce the probability of being detected. Next we study this question before delving into the analysis of the NE. To facilitate the analysis, we sort the targets based on their security asset W_i

as: $W_1 \geq W_2 \geq \cdots \geq W_N$. We then define the sensible target set and the quasi-sensible target set as follows:

Definition 3: The sensible target set $\mathcal{T}_\mathcal{S}$ and the quasi-sensible target set $\mathcal{T}_\mathcal{Q}$ are defined such that:

$$\begin{cases} W_i > \dfrac{|\mathcal{T}_\mathcal{S}|\cdot(1-C_a)-2aQ}{(1-C_a)(\sum_{j\in\mathcal{T}_\mathcal{S}}\frac{1}{W_j})} & \forall i \in \mathcal{T}_\mathcal{S} \\ W_i = \dfrac{|\mathcal{T}_\mathcal{S}|\cdot(1-C_a)-2aQ}{(1-C_a)(\sum_{j\in\mathcal{T}_\mathcal{S}}\frac{1}{W_j})} & \forall i \in \mathcal{T}_\mathcal{Q} \\ W_i < \dfrac{|\mathcal{T}_\mathcal{S}|\cdot(1-C_a)-2aQ}{(1-C_a)(\sum_{j\in\mathcal{T}_\mathcal{S}}\frac{1}{W_j})} & \forall i \in \mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q} \end{cases} \tag{1}$$

where $|\mathcal{T}_\mathcal{S}|$ is the cardinality of $\mathcal{T}_\mathcal{S}$, $\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}$ denotes the set of targets in the target set $\mathcal{T}$ but neither in $\mathcal{T}_\mathcal{S}$ nor in $\mathcal{T}_\mathcal{Q}$.

The following lemma further characterizes $\mathcal{T}_\mathcal{S}$ and $\mathcal{T}_\mathcal{Q}$:

Lemma 1: Given a network $\mathcal{N}$, both $\mathcal{T}_\mathcal{S}$ and $\mathcal{T}_\mathcal{Q}$ are uniquely determined. $\mathcal{T}_\mathcal{S}$ consists of N_A targets with the largest security assets such that:

- If $W_N > \dfrac{N(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{N}\frac{1}{W_j}}$, then $N_A = N$, $\mathcal{T}_\mathcal{Q} = \Phi$
- If $W_N \leq \dfrac{N(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{N}\frac{1}{W_j}}$, N_A is determined by the following equations:

$$\begin{cases} W_{N_A} > \dfrac{N_A\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{N_A}\frac{1}{W_j}} \\ W_{N_A+1} \leq \dfrac{N_A\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{N_A}\frac{1}{W_j}} \end{cases} \tag{2}$$

$\mathcal{T}_\mathcal{Q}$ consists of the target(s) i such that

$$W_i = \frac{N_A\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{N_A}\frac{1}{W_j}}$$

Proof: The proof consists of showing that $\mathcal{T}_\mathcal{S}$ is composed of n targets with largest security assets and then proving $n = N_A$ by showing neither $n < N_A$ nor $n > N_A$ is possible. It follows obviously that $\mathcal{T}_\mathcal{Q}$ is also uniquely determined.

Here we prove case 2 of the lemma, case 1 can be proven similarly. It is obvious that N_A targets with the largest security assets satisfying (2) consists of a sensible target set $\mathcal{T}_\mathcal{S}$ in that (1) holds in such case. We then need to prove that $\mathcal{T}_\mathcal{S}$ is unique.

We first show that if $i \in \mathcal{T}_\mathcal{S}$, then $j \in \mathcal{T}_\mathcal{S}, \forall j < i (W_j \geq W_i)$, if not, there exists $j_0 < i (W_{j_0} \geq W_i)$ such that $j_0 \in \mathcal{T}-\mathcal{T}_\mathcal{S}$. It follows that $W_{j_0} \leq \dfrac{|\mathcal{T}_\mathcal{S}|\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{k\in\mathcal{T}_\mathcal{S}}\frac{1}{W_k}}$. On the other hand, it holds that $W_i > \dfrac{|\mathcal{T}_\mathcal{S}|\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{k\in\mathcal{T}_\mathcal{S}}\frac{1}{W_k}}$. Thus we have $W_i > W_{j_0}$ which contradicts with $W_{j_0} \geq W_i$. Hence $\mathcal{T}_\mathcal{S}$ is composed of n targets with largest security assets.

We then prove $n = N_A$ by showing that it is impossible that $n < N_A$ or $n > N_A$. If $n < N_A$, on one hand, we have $W_{n+1} \leq \dfrac{n\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{n}\frac{1}{W_j}}$; On the other hand, from (2), we have

$$W_{N_A} > \frac{N_A\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{N_A}\frac{1}{W_j}}$$

$$\Rightarrow W_{N_A}(\sum_{j=1}^{N_A}\frac{1}{W_j}) > \frac{N_A\cdot(1-C_a)-2aQ}{1-C_a} = N_A - \frac{2aQ}{1-C_a}$$

$$\Rightarrow W_{N_A}(\sum_{j=1}^{N_A}\frac{1}{W_j}) - (N_A-n-1) > n+1-\frac{2aQ}{1-C_a}$$

Noticing $W_{N_A} \leq W_i, \forall i \leq N_A$, we have

$$\begin{aligned} W_{n+1}(\sum_{j=1}^{n}\frac{1}{W_j}) &\geq W_{N_A}(\sum_{j=1}^{n}\frac{1}{W_j}) \\ &= W_{N_A}(\sum_{j=1}^{N_A}\frac{1}{W_j}) - W_{N_A}(\sum_{j=n+1}^{N_A}\frac{1}{W_j}) \\ &\geq W_{N_A}(\sum_{j=1}^{N_A}\frac{1}{W_j}) - (N_A-n-1) \\ &> n+1-\frac{2aQ}{1-C_a} \\ &\Rightarrow W_{n+1} > \frac{n\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{n}\frac{1}{W_j}} \end{aligned}$$

which contradicts with $W_{n+1} \leq \dfrac{n\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{n}\frac{1}{W_j}}$, thus it is impossible that $n < N_A$. Similarly we can show that it is impossible that $n > N_A$. Hence, $n = N_A$ is uniquely determined, so is $\mathcal{T}_\mathcal{S}$. It follows obviously that $\mathcal{T}_\mathcal{Q}$ is also uniquely determined. This concludes our proof of the lemma. ■

Remark: It follows straightforwardly from Lemma 1 that $N_A \geq 1$. Given the performance parameter of IDS and the attack cost, $\mathcal{T}_\mathcal{S}$ depends on the security assets of targets and the monitor resource of the defender. $|\mathcal{T}_\mathcal{S}|$ is non-decreasing w.r.t. Q. If $2aQ \geq N(1-C_a)$, $|\mathcal{T}_\mathcal{S}| = N$ or $\mathcal{T}_\mathcal{S} = \mathcal{T}$. We explore the following three typical scenarios to gain a more in-depth insight on $\mathcal{T}_\mathcal{S}$: 1). In the degenerated case where $N = 1$, $N_A = 1$; 2). In the homogeneous case where $W_i = W_j, \forall i, j \in \mathcal{T}$, $N_A = N$; 3). In an extremely heterogeneous case where $W_1 \simeq \cdots \simeq W_k \gg W_{k+1} \geq \cdots \geq W_N$, $N_A = k$. On the other hand, $\mathcal{T}_\mathcal{Q}$ may be empty. In fact $\mathcal{T}_\mathcal{Q}$ can be regarded as the border set between $\mathcal{T}_\mathcal{S}$ and $\mathcal{T}-\mathcal{T}_\mathcal{S}$.

We now study the security implications of $\mathcal{T}_\mathcal{S}$:

Theorem 1: A rational attacker has no incentive to attack any target $i \in \mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}$.

Proof: The proof consists of showing that regardless the defender's strategy $\mathbf{q}$, for any $\mathbf{p} \in A_A$ such that $\exists i \in \mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}, p_i > 0$, we can construct another strategy $\mathbf{p}'$ such that $p'_i = 0, \forall i \in \mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}$ and $U_A(\mathbf{p},\mathbf{q}) < U_A(\mathbf{p}',\mathbf{q})$.

If $W_N \geq \dfrac{N_A\cdot(1-C_a)-2aQ}{(1-C_a)\sum_{j=1}^{N_A}\frac{1}{W_j}}$, $\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q} = \varnothing$, the theorem holds evidently. We now prove the case where $W_N <$

$\dfrac{N_A \cdot (1-C_a) - 2aQ}{(1-C_a)\sum_{j=1}^{N_A} \frac{1}{W_j}}$, in other words, $\mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}} \neq \varnothing$.

Consider a vector $\mathbf{q^0} = (q_1^0, q_2^0, \cdots, q_N^0)$ where

$$q_i^0 = \begin{cases} \dfrac{1}{2a}\left(1 - C_a - \dfrac{N_A \cdot (1-C_a) - 2aQ}{\sum_{j=1}^{N_A} \frac{1}{W_j}}\right) & i \in \mathcal{T}_{\mathcal{S}} \\ 0 & i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} \end{cases}$$

It holds that $q_i^0 \geq 0$ and $\sum_{i=1}^{N_A} q_i^0 = Q$. Let $\mathbf{q} = (q_1, q_2, \cdots, q_N)$ be the monitor probability distribution of the defender, it holds that $\sum_{i=1}^{N_A} q_i \leq Q$, thus $\exists m \in \mathcal{T}_{\mathcal{S}}$ such that $q_m \leq q_m^0$.

We now consider any attacker strategy profile $\mathbf{p} = (p_1, p_2, \cdots, p_N) \in A_A$ satisfying $\sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i > 0$, i.e., the attacker attack at least one target outside the sensible target set with non-zero probability. We construct another attacker strategy profile $\mathbf{p}'$ based on $\mathbf{p}$ such that

$$p_i' = \begin{cases} p_i & i \in \mathcal{T}_{\mathcal{S}} \text{ and } i \neq m \\ p_m + \sum_{j \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_j & i = m \\ p_i & i \in \mathcal{T}_{\mathcal{Q}} \\ 0 & i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}} \end{cases}$$

By comparing the attacker's payoff operating at $\mathbf{p}$ and $\mathbf{p}'$, noticing the fact that $W_i < \dfrac{N_A \cdot (1-C_a) - 2aQ}{(1-C_a)\sum_{j=1}^{N_A} \frac{1}{W_j}}, \forall i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}$, we obtain:

$$\begin{aligned} & U_A(\mathbf{p}) - U_A(\mathbf{p}') \\ = \; & \sum_{i \in \mathcal{T}} p_i W_i (1 - 2aq_i - C_a) - \sum_{i \in \mathcal{T}} p_i' W_i (1 - 2aq_i - C_a) \\ = \; & \sum_{i \in \mathcal{T}} p_i W_i (1 - 2aq_i - C_a) - \Big(\sum_{i \in \mathcal{T}_{\mathcal{S}} + \mathcal{T}_{\mathcal{Q}}, i \neq m} p_i W_i (1 - \\ & 2aq_i - C_a) + (p_m + \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i) W_m (1 - 2aq_m - C_a) \Big) \\ = & \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i W_i (1 - 2aq_i - C_a) - \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i W_m (1 - 2aq_m - C_a) \\ \leq & \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i W_i (1 - 2aq_i - C_a) - \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i W_m (1 - 2aq_m^0 - C_a) \\ = & \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i W_i (1 - 2aq_i - C_a) - \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i \frac{N_A \cdot (1-C_a) - 2aQ}{\sum_{j=1}^{N_A} (1-C_a) \frac{1}{W_j}} \\ = & \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i W_i - \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i \frac{N_A \cdot (1-C_a) - 2aQ}{\sum_{j=1}^{N_A} (1-C_a) \frac{1}{W_j}} \\ = & \sum_{i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} - \mathcal{T}_{\mathcal{Q}}} p_i \left(W_i - \frac{N_A \cdot (1-C_a) - 2aQ}{\sum_{j=1}^{N_A} (1-C_a) \frac{1}{W_j}} \right) < 0 \end{aligned}$$

Hence, operating at $\mathbf{p}'$ gives the attacker more payoff than operating at $\mathbf{p}$. As a result, a rational attacker has no incentive to choose $\mathbf{p}$ compared with $\mathbf{p}'$. ■

Remark: Theorem 1 is a powerful result in that it shows that focusing only on the targets in $\mathcal{T}_{\mathcal{S}}$ and $\mathcal{T}_{\mathcal{Q}}$ is enough to maximize the attacker's payoff. Other targets are "self-secured" such that they are not "attractive" enough to draw the attacker's attention due to their security assets and the monitor resource constraint of the defender, even these targets are not monitored by the defender.

Noticing the utility function of the defender, if the attacker does not attack the target i, then the defender has no incentive to monitor i, either. The following guideline for the defender is thus immediate:

Guideline 1: The defender should not monitor any target outside $\mathcal{T}_{\mathcal{S}}$ and $\mathcal{T}_{\mathcal{Q}}$.

B. Nash Equilibrium Analysis

The game G is a finite strategic game, thus admits at least one NE (pure or mixed strategy) [10]. We cite the following well known lemma [10] to conduct further analysis on the NE:

Lemma 2: Every action in the support of any player's equilibrium mixed strategy yields that player the same payoff. Any other action yields that player less payoff.

Apply Lemma 2, we obtain the following results on the NE:

Theorem 2: The strategy profile $(\mathbf{p}^*, \mathbf{q}^*)$ is a NE of G if and only if it holds that

1) If $P \leq \dfrac{bC_f + C_m}{2a + bC_f}$, then $q_i^* = 0, \forall i \in \mathcal{T}$,

$$p_i^* \begin{cases} \in [0, P] & W_i = W_1 \\ = 0 & W_i < W_1 \end{cases}$$

where $\sum_{W_i = W_1} p_i^* = P$.

2) If $P > \dfrac{bC_f + C_m}{2a + bC_f}$, then let

$$P = (N_D + \delta)\frac{bC_f + C_m}{2a + bC_f}, N_D \in \mathbb{Z}^+, 0 \leq \delta < 1$$

a) If $N_D < N_A$, then

$$p_i^* = \begin{cases} \dfrac{bC_f + C_m}{2a + bC_f} & i \leq N_D \ (W_i > W_{N_D+1}) \\ \in \left[0, \dfrac{bC_f + C_m}{2a + bC_f}\delta\right] & W_i = W_{N_D+1} \\ 0 & W_i < W_{N_D+1} \end{cases}$$

where $\displaystyle\sum_{W_i = W_{N_D+1}} p_i^* = \frac{bC_f + C_m}{2a + bC_f}\delta$

$$q_i^* = \begin{cases} \dfrac{1}{2a}\left(1 - C_a - \dfrac{N_D(1-C_a) - 2aQ^0}{W_i \sum_{j=1}^{N_D} \frac{1}{W_j}}\right) & i \leq N_D \\ 0 & i > N_D \end{cases}$$

where $Q^0 = \dfrac{1-C_a}{2a}\left(N_D - W_{N_D+1}\displaystyle\sum_{j=1}^{N_D} \frac{1}{W_j}\right)$

b) If $N_D \geq N_A$ and $N(1-C_a) > 2aQ$, then

$$q_i^* = \begin{cases} \dfrac{1}{2a}\left(1 - C_a - \dfrac{N_A(1-C_a) - 2aQ}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}}\right) & i \in \mathcal{T}_{\mathcal{S}} \\ 0 & i \in \mathcal{T} - \mathcal{T}_{\mathcal{S}} \end{cases}$$

$$p_i^* = \begin{cases} \dfrac{P_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - \left(\dfrac{N_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - 1 \right) \cdot \\ \dfrac{bC_f + C_m}{2a + bC_f} \quad i \in \mathcal{T_S} \\ \in \Big[0, \dfrac{P_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - \left(\dfrac{N_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - 1 \right) \cdot \\ \dfrac{bC_f + C_m}{2a + bC_f} \Big] \quad i \in \mathcal{T_Q} \\ 0 \quad i \in \mathcal{T} - \mathcal{T_S} - \mathcal{T_Q} \end{cases}$$

where $P_A > \left(N_A - W_{N_A} \sum_{j=1}^{N_A} \dfrac{1}{W_j} \right) \dfrac{bC_f + C_m}{2a + bC_f}$, and $\sum_{i \in \mathcal{T}} p_i^* = P$

c) If $N_D \geq N_A$ and $N(1 - C_a) \leq 2aQ$, in this case $N_D = N_A = N$, then

$$\begin{cases} p_i^* = \dfrac{bC_f + C_m}{2a + bC_f} \\ q_i^* = \dfrac{1 - C_a}{2a} \end{cases}$$

Proof: The proof consists of showing that: 1). $\forall \mathbf{p} \in A_A, \forall \mathbf{q} \in A_D$, it holds that $U_A(\mathbf{p}^*, \mathbf{q}^*) \geq U_A(\mathbf{p}, \mathbf{q}^*)$ and $U_I(\mathbf{p}^*, \mathbf{q}^*) \geq U_I(\mathbf{p}^*, \mathbf{q})$; 2). $\forall \mathbf{p} \in A_A$ and $\mathbf{p} \neq \mathbf{p}^*$, $\forall \mathbf{q} \in A_D$ and $\mathbf{q} \neq \mathbf{q}^*$, it holds that $U_A(\mathbf{p}^*, \mathbf{q}^*) > U_A(\mathbf{p}, \mathbf{q}^*)$ and $U_I(\mathbf{p}^*, \mathbf{q}^*) > U_I(\mathbf{p}^*, \mathbf{q})$.

To prove Theorem 3, we show that only the strategy profile(s) $(\mathbf{p}^*, \mathbf{q}^*)$ satisfying the conditions in the theorem satisfies the following property of NE

$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) \geq U_A(\mathbf{p}', \mathbf{q}^*) & \forall \mathbf{p}' \in A_A \\ U_D(\mathbf{p}^*, \mathbf{q}^*) \geq U_D(\mathbf{p}^*, \mathbf{q}') & \forall \mathbf{q}' \in A_D \end{cases}$$

We show the above relation holds for case 2.(a) of Theorem 3, other cases can be shown in the same way and are omitted here. For case 2.(a), $P > \dfrac{bC_f + C_m}{2a + bC_f}$ and $N_D \geq N_A$, $\forall \mathbf{p}' \in A_A$, it follows $W_i = \dfrac{N_A(1 - C_a) - 2aQ}{\sum_{j=1}^{N_A} \frac{1}{W_j}}, \forall i \in \mathcal{T}_Q$:

$$\begin{aligned} U_A(\mathbf{p}^*, \mathbf{q}^*) &= \sum_{i \in \mathcal{T}} p_i^* W_i (1 - 2aq_i^* - C_a) \\ &= \sum_{i \in \mathcal{T_S}} p_i^* \frac{N_A(1 - C_a) - 2aQ}{\sum_{j=1}^{N_A} \frac{1}{W_j}} + \sum_{i \in \mathcal{T_Q}} p_i^* W_i \\ &= \sum_{i \in \mathcal{T_S} + \mathcal{T_Q}} p_i^* \frac{N_A(1 - C_a) - 2aQ}{\sum_{j=1}^{N_A} \frac{1}{W_j}} \\ &= P \cdot \frac{N_A(1 - C_a) - 2aQ}{\sum_{j=1}^{N_A} \frac{1}{W_j}} \end{aligned}$$

Following Theorem 1 that the attacker has no incentive to attack any targets outside $\mathcal{T_S}$ and $\mathcal{T}_Q$, we have:

$$\begin{aligned} U_A(\mathbf{p}', \mathbf{q}^*) &= \sum_{i \in \mathcal{T}} p_i' W_i (1 - 2aq_i^* - C_a) \\ &= \sum_{i \in \mathcal{T_S}} p_i' \frac{N_A(1 - C_a) - 2aQ}{\sum_{j=1}^{N_A} \frac{1}{W_j}} + \sum_{i \in \mathcal{T_Q}} p_i' W_i \\ &= \sum_{i \in \mathcal{T_S} + \mathcal{T_Q}} p_i' \frac{N_A(1 - C_a) - 2aQ}{\sum_{j=1}^{N_A} \frac{1}{W_j}} \\ &\leq P \cdot \frac{N_A(1 - C_a) - 2aQ}{\sum_{j=1}^{N_A} \frac{1}{W_j}} = U_A(\mathbf{p}^*, \mathbf{q}^*) \end{aligned}$$

Note that the above relation holds in both cases where $\mathbf{T_Q} = \varnothing$ and $\mathbf{T_Q} \neq \varnothing$. In the same way, we can show that $U_A(\mathbf{p}^*, \mathbf{q}^*) \geq U_A(\mathbf{p}^*, \mathbf{q}'), \forall \mathbf{q}' \in A_D$.

It leaves for us to prove that any other strategy profile $(\mathbf{p^N}, \mathbf{q^N}) \neq (\mathbf{p}^*, \mathbf{q}^*)$ cannot be the NE. Otherwise, if the IDS's strategy profile at the NE $\mathbf{q^N} \neq \mathbf{q}^*$, noticing $U_A(\mathbf{p^N}, \mathbf{q^N}) = \sum_{i \in \mathcal{T}} p_i^N W_i (1 - 2aq_i^N - C_a)$, we can solve p^N as

$$p_i^N \begin{cases} \in [0, P] & i \in \mathcal{T_M} \\ = 0 & i \in \mathcal{T} - \mathcal{T_M} \end{cases}$$

where $\mathcal{T_M}$ consists of target i such that $(1 - 2aq_i^N - C_a)W_i$ is maximized, $\sum_{i \in \mathcal{T_M}} p_i^N = P$.

It follows that $q_i^N < q_i^*, \forall i \in \mathcal{T_M}$, otherwise if $\exists m$ such that $q_m^N \geq q_m^*$, then $\forall i \in \mathcal{T_M}, i \in \mathcal{T_S}$, it follows $(1 - 2aq_i^N - C_a)W_i = (1 - 2aq_m^N - C_a)W_m$ that $q_i^N \geq q_i^*$; $\forall i \in \mathcal{T} - \mathcal{T_M}, i \in \mathcal{T_S}$, it follows $(1 - 2aq_i^N - C_a)W_i < (1 - 2aq_m^N - C_a)W_m$ that $q_i^N > q_i^*$; It follows that $\sum_{i \in \mathcal{T}} q_i^N > \sum_{i \in \mathcal{T_S}} q_i^* = Q$, which leads to the contradiction.

On the other hand, we have $\mathcal{T_M} \subseteq \mathcal{T_S}$, otherwise if $\exists i$ such that $i \in \mathcal{T_M}$ and $i \in \mathcal{T} - \mathcal{T_S}$, it follows $\exists j \in \mathcal{T_S}$ such that $q_j^N < q_j^*$ that $(1 - 2aq_i^N - C_a)W_i = (1 - 2aq_j^N - C_a)W_j$. It follows that $q_j^N \geq q_j^*$, which contradicts with $q_i^N < q_i^*$.

Moreover, we can show that $\mathcal{T} \neq \mathcal{T_S}$, if not, by solving the equations $(1 - 2aq_i^N - C_a)W_i = (1 - 2aq_j^N - C_a)W_j, \forall i, j \in \mathcal{T_S}$, we obtain $q_i^N = q_i^*, \forall i \in \mathcal{T_S}$, which leads to contradiction. Hence, $|\mathcal{T_M}| < N_A \leq N_D$.

It follows $q_i^N < q_i^*, \forall i \in \mathcal{T_M}$ that $\sum_{i \in \mathcal{T_M}} q_i^N < Q$. It follows $P > \dfrac{bC_f + C_m}{2a + bC_f}$ that $\exists k \in \mathcal{T_M}$ such that $p_k^N > \dfrac{bC_f + C_m}{2a + bC_f}$. We then construct another strategy profile $\mathbf{q}''$ such that

$$q_i'' = \begin{cases} q_i^N & i \in \mathcal{T_M}, i \neq k \\ q_i^N + Q - \sum_{j \in \mathcal{T_M}} q_j^N & i = k \end{cases}$$

We have $U_D(\mathbf{p^N}, \mathbf{q^N}) - U_D(\mathbf{p^N}, \mathbf{q}'') = -\left(p_k - \dfrac{bC_f + C_m}{2a + bC_f} \right) W_k < 0$, which indicates that $(\mathbf{p^N}, \mathbf{q^N})$ with $\mathbf{q^N} \neq \mathbf{q}^*$ cannot be a NE. In the same way, we can show that any strategy profile $\mathbf{p^N} \neq \mathbf{p}^*$ cannot be a NE, neither. This concludes our proof. ■

Remark 1: The case 1 and 2.(a) are the cases where the attacker disposes limited attack resource such that the defender does not use up all its monitor resource or even does not monitor at all. This may also be due to the fact that the monitor cost is too high or the detection rate a is too low. The valuable information can be drawn is that in some cases where the attack intensity is low, it is a waste of resource for the defender to monitor all the time. On the contrary, if the monitor cost outweighs the gain, the defender is better off to keep silent.

Remark 2: The case 2.(b) is the case where both the attacker and defender use up all their resource to attack and monitor. In other words, the attacker's resource P and the defender's resource Q are constrained in the sense that at the NE, the payoff U_A/U_I is the monotonously increasing w.r.t. P/Q, i.e., given more resource, both players can increase their payoff, as shown in the following:

$$\begin{cases} U_A(\mathbf{p}^*,\mathbf{q}^*) = P\dfrac{N_A \cdot (1-C_a) - 2aQ}{\sum_{j=1}^{N_A}\frac{1}{W_j}} \\ U_D(\mathbf{p}^*,\mathbf{q}^*) = Q\left[\dfrac{P(2a+bC_f)}{\sum_{j=1}^{N_A}\frac{1}{W_j}} - \dfrac{N_A(bC_f+C_m)}{\sum_{j=1}^{N_A}\frac{1}{W_j}}\right] \\ -\dfrac{PN_A}{\sum_{j=1}^{N_A}\frac{1}{W_j}} + \dfrac{N_A^2}{\sum_{j=1}^{N_A}\frac{1}{W_j}}\dfrac{bC_f+C_m}{2a+bC_f} - \dfrac{bC_f+C_m}{2a+bC_f}\displaystyle\sum_{j=1}^{N_A} W_j \end{cases} \tag{3}$$

In this case, the game G can be regarded as a resource allocation problem that each player tries to choose the most profitable strategy under the resource constraint. The following corollary further highlights the NE:

Corollary 1: In the case 2.(b) of Theorem 2, for $\forall \mathbf{p}' \neq \mathbf{p}^*$, $\forall \mathbf{q}' \neq \mathbf{q}^*$, let $\widehat{\mathbf{p}} = \text{argmax}_{\mathbf{p}\in A_A} U_A(\mathbf{p},\mathbf{q}')$, $\widehat{\mathbf{q}} = \text{argmax}_{\mathbf{q}\in A_I} U_I(\mathbf{p}',\mathbf{q})$ it holds that $U_I(\mathbf{p}^*,\mathbf{q}^*) > U_I(\widehat{\mathbf{p}},\mathbf{q}')$ and $U_A(\mathbf{p}^*,\mathbf{q}^*) > U_A(\mathbf{p}',\widehat{\mathbf{q}})$.

Proof: The proof is similar as that of Theorem 1 and is omitted here. ■

Corollary 1 implicates that if the defender does not operate on the NE $\mathbf{q}^*$, since the attacker chooses its strategy $\widehat{\mathbf{p}}$ that maximizes its payoff U_A, as a result, the defender gets less payoff than operating at $\mathbf{q}^*$. This also holds for the attacker. Hence, the NE not only corresponds to an equilibrium which is acceptable for both players such that they have no incentive to deviate, but consists of the optimal choice for both players.

Remark 3: The case 2.(c) corresponds to the case where both the attacker's resource P and the defender's resource Q are sufficient to attack and defend. In this case, the sensible target set $\mathcal{T}_S = \mathcal{T}$, i.e., all targets are attacked/monitored. However, both the attacker and the defender do not use up the total resource to attack/defend, but rather reach an intermediate compromise at the NE which is unique. In such context, the situation can be regarded such that the attack and the defender are playing N atomic intrusion detection games G ($N = 1$) on each of the N target. Moreover, at the NE, we have

$$\begin{cases} U_A(\mathbf{p}^*,\mathbf{q}^*) = 0 \\ U_D(\mathbf{p}^*,\mathbf{q}^*) = -\dfrac{bC_f+C_m}{2a+bC_f}\displaystyle\sum_{j=1}^{N} W_j \end{cases} \tag{4}$$

which implicates that: 1). Disposing more attack or monitor resource does not influence the NE and the payoff of both players at the NE; 2). For the attacker, decreasing the attack cost will not increase its utility at the NE since the defender will increase its monitor probability which will further drag U_A^* to 0; 3). For the defender, protecting more valuable targets represents more risk; Given the security assets of the targets, improving the performance of the IDS module (increasing a and/or decreasing b) or/and decreasing the monitor cost/false alarm cost can increase its utility and alleviate the attack intensity at the NE.

One interesting feature is that the strategy of the attacker $\mathbf{p}^*$ only depends on the performance parameters of the IDS of the defender. In other words, the defender can actually "control" the behavior of the attacker at the NE in this case.

C. Further Security Implications Behind the Nash Equilibrium

Theorem 2 quantifies the behavior of a rational attacker and defender at the NE from which no players have incentive to deviate. In some cases, the attacker's strategy at the NE $\mathbf{p}^*$ is not unique, but all $\mathbf{p}^*$ yields the attacker the same payoff. In contrast, the defender's strategy at the NE $\mathbf{q}^*$ is unique in all cases. Moreover, a rational attacker will never choose the extreme strategies such as 1) attacking the target with the largest security asset, or 2) evenly distributing its attack resource. Such strategies can be easily defended by the defender and thus cannot bring the most payoff to the attacker. Hence the attacker actually focuses its attack on $\mathcal{T}_S$ and $\mathcal{T}_Q$ with the probability distribution $\mathbf{p}^*$. With this information in mind, we provide the following guidelines for the defender:

Guideline 2: The defender should choose the monitor probability distribution $\mathbf{q}^*$ according to Theorem 2. Under such context, the attacker gets the same payoff by attacking any monitored targets and gets less payoff by attacking any non-monitored targets.

In fact, to equalize the attacker's payoff of attacking any monitored targets turns to be the best choice since otherwise, the attacker will attack the least protected target i where $(1 - C_a - 2aq_i)W_i$ is maximized to gain extra payoff and the payoff of the defender decreases accordingly.

We then study the impact of the monitor resource constraint on the system to gain a more in-depth insight on the NE. To this end, we compare the defender's payoff at the NE of the case 2.(b) where the monitor resource is constrained and 2.(c) where defender disposes sufficient resource.

From (3) and (4), we can see that the resource constraint have a significant negative impact on the system when P is large: for the attacker, it cannot get any profit if the defender has enough resource to monitor ($U_A = 0$), on the contrary if the monitor resource is not sufficient, the attacker's payoff reaches $O(W_i)$; at the defender side, we can quantify the payoff loss due to the lack of monitor resource as:

$$\begin{aligned} L = & -Q\left[\frac{P(2a+bC_f)}{\sum_{j=1}^{N_A}\frac{1}{W_j}} - \frac{N_A(bC_f+C_m)}{\sum_{j=1}^{N_A}\frac{1}{W_j}}\right] + \frac{PN_A}{\sum_{j=1}^{N_A}\frac{1}{W_j}} \\ & - \frac{N_A^2}{\sum_{j=1}^{N_A}\frac{1}{W_j}}\frac{bC_f+C_m}{2a+bC_f} - \frac{bC_f+C_m}{2a+bC_f}\sum_{j=N_A+1}^{N} W_j \end{aligned}$$

We can see that with the increase of P, the loss due to the resource constraint turns positive and may raise to $O(W_i)$.

Following this analysis, the necessary conditions to limit the damage caused by the attacker is to dispose sufficient monitor resource and to operate on the NE of the case 2.(c) of Theorem 2 in the sense that: 1) The defender can actually "control" the behavior of the attacker at the NE; 2). The attacker's payoff drops to 0 at the NE regardless of the attack resource P;

Until now, our analysis is based on the condition that there is one defender, i.e., $Q \leq 1$. In case where $N(1-C_a) > 2a$, one defender is not enough to maintain the favorable NE. Obviously more than one defenders are required. Hence, a natural question we pose is that under such context, how much monitor resource Q or, moreover, how many defenders are needed to achieve system optimality in terms of security? Furthermore, how to configure them to maximize U_I?

IV. Intrusion Detection Game with Multiple Attackers/Defenders

In this section, we extend our efforts to the intrusion detection game with multiple attackers/defenders to study the posed questions. To this end, we relax the resource constraint $P \leq 1$ and $Q \leq 1$. We base our study on the following assumptions: 1). the attacker side disposes sufficient attack resource P; 2). the attackers can communicate and cooperate among them to launch attacks and so do the defenders to arrange their monitoring; 3). the attack gain on the same target is not cumulative, i.e., if attackers A_i and A_j attack the same target m with probability p_m at the same time with success, the attack gain for these attacks is $U_A^m = (1-C_a)W_m$, not $2(1-C_a)W_m$. This assumption is reasonable when the attackers can communicate and cooperate among them. However, it is not the case at the defender side in that having multiple defenders monitor the same target influences the detection and the false alarm rate, and thus may change the final payoff.

We conduct our analysis for the following two cases. In the first case, each target is monitored by at most one defender at any time. In the second case, we allow one target to be monitored by several defenders simultaneously and their results are combined to further detect possible attacks.

A. Case 1

Since the attack gain is not cumulative, the attackers will never attack the same target simultaneously, i.e., $p_i \leq 1, \forall i \in \mathcal{T}$. In this subsection, we address the case where any target is monitored by at most one defender at any time. The intuition of adopting this strategy at the defender side is to use the monitor resource in an economic way, i.e., to cover the most targets possible with the monitor resource Q. In such context, our previous analysis can be applied with slight modification on the notation p_i and q_i: now p_i denotes the total attack resource from the attackers spent to attack the target i; similarly, q_i denotes the total monitor resource from the defenders spent to monitor the target i. Apply Theorem 2, at the NE $(\mathbf{p}^*, \mathbf{q}^*)$, we have:

1) If $2a \leq 1-C_a$, then $p_i^* = 1$ and $q_i^* = 1, \forall i \in \mathcal{T}$. In this case, the IDS modules of the defenders are not efficient enough to thwart the attacks. The payoff of the attacker and the defender side at the NE is
$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) = (1-C_a-2a)\sum_{i\in\mathcal{T}} W_i \\ U_D(\mathbf{p}^*, \mathbf{q}^*) = -(1-2a+C_m)\sum_{i\in\mathcal{T}} W_i \end{cases}$$
2) If $2a > 1-C_a$, then $p_i^* = \dfrac{bC_f + C_m}{2a+bC_f}$, $q_i^* = \dfrac{1-C_a}{2a}$, $i \in \mathcal{T}$. The correspondent payoff is: $U_A(\mathbf{p}^*, \mathbf{q}^*) = 0$, $U_D(\mathbf{p}^*, \mathbf{q}^*) = -\sum_{i\in\mathcal{T}} \dfrac{bC_f + C_m}{2a+bC_f} W_i$.

Here we implicitly assume that $C_m \leq 2a$ ($p_i^* \leq 1$) in that $C_m > 2a$ leads to $q_i^* = 0$, which is the trivial case that we are not interested here.

For case 1, it is clear that the number of defenders required to maintain the above NE is $N_{min} = N$. For case 2, at the NE, $\sum_{i\in\mathcal{T}} q_i = \dfrac{N(1-C_a)}{2a}$. Noticing that each defender disposes at most $q_i = 1$ as monitor resource, we need at least $N_{min} = \left\lceil \dfrac{N(1-C_a)}{2a} \right\rceil$ defenders to maintain the above NE under the condition that the defenders can cooperate among them to arrange their monitoring, where $\lceil n \rceil$ denotes the smallest integer not less than n. Following the condition $2a > 1-C_a$, we have $N_{min} \leq N$ and if $C_a \ll 1$, $N_{min} \sim \dfrac{N(1-C_a)}{2a} \sim \dfrac{N}{2a} > \dfrac{N}{2}$.

The intuition behind the above results is that if the detection rate of the defenders is not high enough to thwart the attacks, then each target should be monitored as much as possible to decrease the damages caused by the attackers as much as possible. On the other hand, if the defenders are efficient enough in terms of the detection rate, then less monitor resource is required because in such context, the attacker side does not attack on the maximum intensity.

Can we improve the results by letting multiple defenders monitor the same target simultaneously and combine the monitor results to make the final decision? We answer this question by performing the following analysis.

B. Case 2

The intuition of adopting this strategy is to combine the monitor results of multiple defenders to achieve better performance. However, the price is higher monitor cost.

Consider the case where x defenders monitor the same target simultaneously and the attack is said to be detected if it is detected by at least y ($1 \leq y \leq x$, referred to as detection threshold) out of the x defenders. The aggregate detection rate a_x^y and false alarm rate b_x^y can be computed as:
$$\begin{cases} a_x^y = \sum_{i=y}^{x} C_x^i a^i (1-a)^{x-i} \\ b_x^y = \sum_{i=y}^{x} C_x^i b^i (1-b)^{x-i} \end{cases}$$
where a and b is the detection and false alarm rate of the individual defender. The following lemma studies a_x^y and b_x^y:

Lemma 3: $\forall x, y \in \mathbb{Z}^+, y \leq x$ and $0 < a, b < 1$, it holds:

- Both a_x^y and b_x^y is monotonously decreasing w.r.t. y given x and w.r.t. x given y ($y \leq x$)

- If $x > 1$, then $a_x^y < xa$, $b_x^y < xb$

Extending Theorem 2, at the NE $(\mathbf{p}^*, \mathbf{q}^*)$, we have,

1) If $2a_{x_i}^{y_i} \leq 1 - C_a$, then $p_i^* = 1, q_i^* = 1, \forall i \in \mathcal{T}$,

$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) = (1 - C_a - 2a_{x_i}^{y_i}) \sum_{i \in \mathcal{T}} W_i \\ U_D(\mathbf{p}^*, \mathbf{q}^*) = -(1 - 2a_{x_i}^{y_i} + x_i C_m) \sum_{i \in \mathcal{T}} W_i \end{cases}$$

2) If $2a_{x_i}^{y_i} > 1 - C_a$, then $p_i^* = \dfrac{b_{x_i}^{y_i} C_f + x_i C_m}{2a_{x_i}^{y_i} + b_{x_i}^{y_i} C_f}$, $q_i^* = \dfrac{1 - C_a}{2a_{x_i}^{y_i}}$, $i \in \mathcal{T}$. The correspondent payoff is: $U_D(\mathbf{p}^*, \mathbf{q}^*) = -\sum_{i \in \mathcal{T}} \dfrac{b_{x_i}^{y_i} C_f + x_i C_m}{2a_{x_i}^{y_i} + b_{x_i}^{y_i} C_f} W_i$, $U_A(\mathbf{p}^*, \mathbf{q}^*) = 0$.

where x_i denotes the number of defenders simultaneously monitoring the target i with the detection threshold y_i, p_i denotes the total attack resource from attackers spent to attack the target i, q_i denotes the monitor resource of each of the x_i defenders spent to monitor the target i.

The previous subsection where each target is monitored by at most one defender at any time can be regarded as the degenerated case with $x_i = y_i = 1$. For case 1, we have $N_{min} = N$ at $x_i = y_i = 1$. For case 2, if $x_i = 1$, then $N_{min} = N$; If $x_i > 1$, apply Lemma 3, we get $N_{min} = \left\lceil \sum_{i \in \mathcal{T}} x_i \dfrac{(1 - C_a)}{2a_{x_i}^{y_i}} \right\rceil \geq \left\lceil \dfrac{N(1 - C_a)}{2a} \right\rceil$.

Compare the above analysis with the results in Section 4.A, if each target is monitored by multiple defenders simultaneously, more defenders are usually needed to maintain the NE although the detection rate may be higher. Hence, to minimize the required number of defenders, the monitor resource should be used in an economic way such that each target is monitored by at most one defender at any time.

However, if the objective of the defender side is not to maintain the NE with minimum number of defenders, but rather to maximize its payoff at the NE, e.g., if there is sufficient monitor resource, then the answer may be different. In such context, the defender side needs to solve the optimization problem $\max_{1 \leq y_i \leq x_i} U_D(\mathbf{p}^*, \mathbf{q}^*)$. The following theorem studies the optimal strategy in such context:

Theorem 3: The optimal strategy for the defender side is to let each target be monitored by x^* defenders simultaneously with the detection threshold y^*:

$$(x^*, y^*) = \begin{cases} \underset{1 \leq y \leq x, 2a_x^y \leq 1 - C_a}{\operatorname{argmin}} & 1 - 2a_x^y + C_m \quad C_1 < C_2 \\ \underset{1 \leq y \leq x, 2a_x^y > 1 - C_a}{\operatorname{argmin}} & \dfrac{b_x^y C_f + x C_m}{2a_x^y + b_x^y C_f} \quad C_1 \geq C_2 \end{cases}$$

where

$$\begin{cases} C_1 = \min\limits_{1 \leq y \leq x} 1 - 2a_x^y + C_m & \text{s.t.} \quad 2a_x^y \leq 1 - C_a \\ C_2 = \min\limits_{1 \leq y \leq x} \dfrac{b_x^y C_f + x C_m}{2a_x^y + b_x^y C_f} & \text{s.t.} \quad 2a_x^y > 1 - C_a \end{cases}$$

Remark: The above optimization problem can be solved numerically. The choice of x^* consists of searching a tradeoff between the amount of observation based on which the final decision is made and the monitor cost. The choice of y^* consists of searching a tradeoff between the detection rate and the false alarm rate: with a larger y, the false alarm rate b_x^y decreases, but the detection rate a_x^y also decreases. A bad choice of y may lead to significant sub-optimality at the defender side even if it disposes sufficient monitor resource. We will show this point via numerical study in Section 6.

At the optimal configuration, at least $N_{min} = \left\lceil \dfrac{N x^* (1 - C_a)}{2 \sum_{i=y^*}^{x^*} C_{x^*}^i a^i (1 - a)^{x^* - i}} \right\rceil$ defenders are needed to achieve the system optimality in terms of security.

Based on the results in this section, we have the following guidelines for the defenders:

Guideline 3: In any case, at least $\left\lceil \dfrac{N(1 - C_a)}{2a} \right\rceil$ defenders are needed in order to effectively monitor the targets.

Guideline 4: In some cases, having multiple defenders monitoring each targets simultaneously and combining their results helps the defenders achieve optimal protection performance.

V. Discussion and Generalization

We generalize our model to consider the scenario where the attacker side may launch various kinds of attack with different gain and cost. Normally, more profitable attacks are more expensive to launch and usually more likely to be detected. A natural question is that what attackers's behavior can we expect and can the previous model be extended in this scenario.

To this end, we define the possible attack set $\Gamma = \{\tau_1, \tau_2, \cdots, \tau_n\}$ from which the attackers can choose a subset of attacks to launch on the target set. The expected payoff concerning $\tau_i \in \Gamma$ on the target j is $[(1 - 2a^i q_j)\theta^i - C_a^i] W_j$, where $C_a^i W_j$ is the attack cost of launching τ_i, $\theta^i W_j$ is the gain of successfully attacking the target j with τ_i without being detected, a^i is the detection rate of τ_i. Our previous modeling is based on the special case where the possible attack set has only one element, i.e., $|\Gamma| = 1$ and $\theta = 1$.

We extend the previous notations to model the interaction between the attack and the defender side in this scenario: the attacker side chooses the strategy $\mathbf{p} = \{p_1, p_2, \cdots, p_N\}$ to maximize its payoff. $p_i = \sum_{j \in \Gamma} p_i^j$ where p_i^j is the probability of launching the attack τ_j on the target i. The notation of the defender side is the same as in previous model. The utility functions are:

$$U_A = \sum_{i \in \mathcal{N}} \sum_{\tau_j \in \Gamma} p_i^j W_i (1 - 2a^j q_i - C_a^j)$$

$$U_I = \sum_{i \in \mathcal{N}} \sum_{\tau_j \in \Gamma} q_i W_i \left[p_i^j (2a^j + b^j C_f^j) - (b^j C_f^j + C_m) \right] - p_i^j W_i$$

where b^j and C_f^j denote the false alarm rate and cost of τ_j.

The above network intrusion detection game can be solved applying Lemma 2, as in our previous analysis, although the procedure is more tedious. In the following, instead of performing the tedious demonstration similar to our previous one, we will highlight the key results and show how our previous results can be extended here by restudying the minimum number of defenders and the optimal strategy of the defender side in this new context.

In our study, we assume that: 1). Both the attacker and defender side dispose sufficient attack and monitor resource, respectively; 2). $C_a^j < \theta^j$, $C_m < 2a^j, \forall \tau_j \in \Gamma$, otherwise the defenders have no incentive to monitor; 3). The attacker side can communicate and cooperate among them to launch attacks; 4). The attack gain on the same target is not cumulative in the sense that if the target i is attacked by τ_1, τ_2 simultaneously with success, the gain for the attacker side is $\max_{j=1,2}(\theta^j - C_a^j)W_i$. This is a simplified scenario. In fact, the gain may range from $\max_{j=1,2}(\theta^j - C_a^j)W_i$ to $\sum_{j=1,2}(\theta^j - C_a^j)W_i$ depending on the specific scenarios under the condition that $\sum_{j=1,2}(\theta^j - C_a^j)W_i \leq W_i$ because target i cannot lose more than the security asset he holds even in the worst case. Here in order to perform a closed-form analysis, we choose a simplified scenario. However, our analysis in the simplified cased can be modified to investigate other cases. Following the above assumption, the rational attackers will never attack the same target with the more than one attack simultaneously; Hence $\sum_{\tau_j \in \Gamma} p_i^j \leq 1, \forall i \in \mathcal{T}$.

In such context, for a target monitored by x defenders simultaneously with the threshold y, we define the efficient attack set $\Gamma_e^{(x,y)} \subseteq \Gamma$ such that $\Gamma_e^{(x,y)}$ consists of the attack(s) τ_j with maximum value u^j among all possible attacks, where

$$u^j = \begin{cases} \theta^j - 2(a^j)_{x_i}^{y_i} - C_a^j & \theta^j - C_a^j > 2(a^j)_{x_i}^{y_i} \\ \dfrac{\theta^j - C_a^j}{2(a^j)_{x_i}^{y_i}} & \theta^j - C_a^j \leq 2(a^j)_{x_i}^{y_i} \end{cases} \tag{5}$$

where $(a^j)_{x_i}^{y_i}$ is defined similarly as $a_{x_i}^{y_i}$.

The following theorem studies the NE of the game:

Theorem 4: Under the condition that both the attacker and defender side dispose sufficient attack and monitor resource, respectively, at the NE $(\mathbf{p}^*, \mathbf{q}^*)$, for each target i monitored by x_i defenders with the detection threshold y_i, it holds that:

- If $\theta^j - C_a^j > 2(a^j)_{x_i}^{y_i}$, then $q_i^* = 1$, $\sum_{\tau_j \in \Gamma_e^{(x_i,y_i)}} (p_i^j)^* = 1$;
- If $\theta^j - C_a^j \leq 2(a^j)_{x_i}^{y_i}$, then $q_i^* = \dfrac{\theta^j - C_a^j}{2(a^j)_{x_i}^{y_i}}$; $(p_i^j)^* = 0$ for $\tau_j \in \Gamma - \Gamma_e^{(x_i,y_i)}$ and $\sum_{\tau_j \in \Gamma_e^{(x_i,y_i)}} (p_i^j)^*(2(a^j)_{x_i}^{y_i} + (b^j)_{x_i}^{y_i} C_f^j) - ((b^j)_{x_i}^{y_i} C_f^j + C_m) = 0$;

Proof: The proof follows the same way as that of Theorem 2. ■

Theorem 3 can be extended to derive the optimal (x_i^*, y_i^*):

$$(x_i^*, y_i^*) = \begin{cases} \underset{\theta^j - C_a^j > 2(a^j)_{x_i}^{y_i}}{\operatorname{argmin}} \sum_{\tau_j \in \Gamma_e^{(x_i,y_i)}} \theta^j - 2(a^j)_{x_i}^{y_i} + C_m & C_1 < C_2 \\ \underset{\theta_j - C_a^j \leq 2(a_j)_{x_i}^{y_i}}{\operatorname{argmin}} \sum_{\tau_j \in \Gamma_e^{(x_i,y_i)}} (p_i^j)^* & C_1 \geq C_2 \end{cases}$$

where

$$\begin{cases} C_1 = \min_{1 \leq y_i \leq x_i} \sum_{\tau_j \in \Gamma_e^{(x_i,y_i)}} \theta^j - 2(a^j)_{x_i}^{y_i} - C_a^j & \text{s.t. } \theta^j - C_a^j > 2(a^j)_{x_i}^{y_i} \\ C_2 = \min_{1 \leq y_i \leq x_i} \sum_{\tau_j \in \Gamma_e^{(x_i,y_i)}} (p_i^j)^* & \text{s.t. } \theta^j - C_a^j \leq 2(a^j)_{x_i}^{y_i} \end{cases}$$

The above results implicates that among the possible of attacks, the rational attackers only choose the attack(s) in $\Gamma_e^{(x_i,y_i)}$ at the NE which is more “profitable” than others. In our context, more “profitable” does not mean that the attack(s) brings the attacker side more gain in case of success, but rather represents a better tradeoff among different factors such as the gain in case of success, the attack cost and the probability of being detected, etc, which is quantified in (5). Moreover, $\Gamma_e^{(x_i,y_i)}$ also depends on the strategy of the defender side (x_i, y_i). In other words, the defender side can “control” the behavior of the attack side to certain extent (which attack to launch and the intensity of the attack) via its own strategy. At the defender side, choosing (x_i^*, y_i^*) consists of searching the best tradeoff between the detection gain and the monitor and false alarm cost. In this context, the lower bound of the number of defenders required to maintain the NE is $\left\lceil \dfrac{\theta^j - C_a^j}{2(a^j)} \right\rceil$ (where $\tau_j \in \Gamma_e^{(1,1)}$). The lower bound is achieved if $x_i = y_i = 1$ and $\theta^j - C_a^j \leq 2(a^j)$.

We compare the analysis in this scenario with the previous analysis in Section IV. In the case where there is only one element in the efficient attack set, our previous analysis in Section IV can be applied directly in this scenario. In the case where there are more than one element in the efficient attack set, at the attacker side, it gets the same payoff as the case where it launches one attack in the efficient attack set. At the defender side, the situation is slightly different: since the NE strategy of the attacker side $\mathbf{p}^*$ is not unique in this case and different $\mathbf{p}^*$ leads to different payoff of the defender side at the NE, the optimal configuration (x_i^*, y_i^*) varies with $\mathbf{p}^*$ (In the previous model in Section IV, since $\mathbf{p}^*$ is unique, the optimal configuration of the defender side is fixed). However, this difference does not pose any additional difficulties in modeling and the previous analysis can be extended in this scenario, as shown in the above demonstration.

In our work, we focus on the interaction between the attacker and the defender side without taking into account the constraint of network topology. When applying our results in practical scenarios, the topology constraint should be considered. [8] provides an interesting investigation on how to select the IDS active nodes in multi-hop ad hoc networks in a heuristic way since the problem is proven to be NP-hard. Their results can be applied in our model to schedule and allocate the monitor resource. Adding the topology constraint in our model is out of the scope of this paper, but is on our future research plan. Other generalization of this work includes modeling the attacks which are correlated among targets and considering the scenarios where the defenders may have different IDS settings such as a, b, etc.

VI. Numerical Study

In this section, we perform numerical study on two typical scenarios to evaluate our analytical results and illustrate the application of the analytical model established in this paper to design efficient defense systems.

We first consider a network with high requirement on security, e.g., military networks usually require a high level of confidentiality and need to be resistant to various attacks. In such scenario, the security assets of targets W_i $(i \in \mathcal{T})$ are much higher than the related cost: i.e., $C_a, C_m, C_f \ll 1$. We set $C_a = C_m = 0.001$ and $C_f = 0.01$. The defenders are usually equipped with high-performance IDS modules with powerful processing capability. Hence a relatively large value $a = 0.9$ and small value $b = 0.05$ are chosen in our study.

The second scenario we consider is at the other end of the spectrum where the attack/monitor cost is important (we set $C_a = C_m = 0.1$ and $C_f = 0.3$ in this case), e.g., a WLAN in the airport where both attackers and defenders have limited battery and processing capability. The defender in such cases are usually not so efficient. We thus set $a = 0.4$ and $b = 0.2$. In both scenarios, there are 10 targets with normalized security assets: $W_i = (11 - i) * 0.1$ $(i = 1, 2, \cdots, 10)$.

A. One Attacker, One Defender

We start with the network intrusion detection game with one attacker/defender. The attack resource P and the monitor resource Q are both set to 1. Table 2 shows the NE $(\mathbf{p}^*, \mathbf{q}^*)$ calculated using our analytical model. As shown in the analytical results, both the attack and defender focus only on the targets in the sensible target set (Target 1-6 for scenario 1 and target 1-4 for scenario 2).

Scenario 1	Scenario 2
$p_1^* = 0.118$, $q_1^* = 0.279$	$p_1^* = 0.239$, $q_1^* = 0.394$
$p_2^* = 0.131$, $q_2^* = 0.249$	$p_2^* = 0.245$, $q_2^* = 0.313$
$p_3^* = 0.147$, $q_3^* = 0.211$	$p_3^* = 0.253$, $q_3^* = 0.212$
$p_4^* = 0.161$, $q_4^* = 0.169$	$p_4^* = 0.262$, $q_4^* = 0.081$
$p_5^* = 0.197$, $q_5^* = 0.096$	$p_5^* = 0$, $q_5^* = 0$
$p_6^* = 0.236$, $q_6^* = 0.004$	$p_6^* = 0$, $q_6^* = 0$
$p_7^* = 0$, $q_7^* = 0$	$p_7^* = 0$, $q_7^* = 0$
$p_8^* = 0$, $q_8^* = 0$	$p_8^* = 0$, $q_8^* = 0$
$p_9^* = 0$, $q_9^* = 0$	$p_9^* = 0$, $q_9^* = 0$
$p_{10}^* = 0$, $q_{10}^* = 0$	$p_{10}^* = 0$, $q_{10}^* = 0$
$U_A^* = 0.459$, $U_I^* = -0.460$	$U_A^* = 0.585$, $U_I^* = -0.800$

TABLE II
NE

	Scenario 1	Scenario 2
$(U_I)_{max}$	-0.561	-0.965
$\overline{U_I}$	-0.823	-1.265
$(U_I^*)_{min}$	-0.461	-0.801

TABLE III
Payoff degradation due to deviation from NE

To further evaluate our analytical results and proposed design guidelines, we investigate the cases where the defender does not operate on the NE. We thus simulate 300 random strategies for the defender and we calculate the correspondent payoff U_I under the condition that the attacker chooses its strategy to maximize its payoff. Table 3 shows the results: $(U_I)_{max}$ denotes the maximum payoff of the defender with the simulated 300 random strategies, $\overline{U_I}$ denotes the average payoff of the defender, $(U_I^*)_{min}$ denotes the minimum payoff of the defender under the condition that the defender operate on $\mathbf{q}^*$ and the attacker choose its strategy to maximize its payoff. Comparing the above numerical results, we can see that in the simulated scenarios, the NE consists of the optimal choice for the defender under the condition that the attacker is intelligent to choose its strategy maximizing its payoff. The above numerical result confirms the proposed guideline 1 and 2 in the analytical model.

B. Multiple Attackers/Defenders

We then study the case of multiple attackers/defenders and investigate the optimal strategy for the defender side. Figure 1 plots $-U_I$ at the NE for the studied scenarios with different x, y. Table 4 shows the optimal strategy for the defender side according to the analytical model.

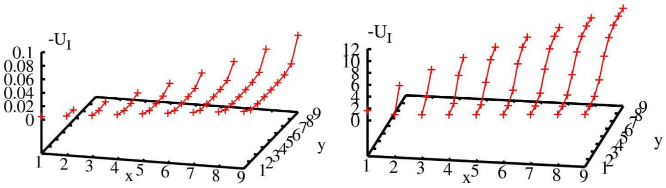

Fig. 1. $-U_I$ as function of x, y, left: scenario 1; right: scenario 2

Scenario 1	Scenario 2
$x^* = 1$, $y^* = 1$ $p_i^* = 0.00083$, $q_i^* = 0.556$ $N_{min} = 6$	$x^* = 2$, $y^* = 1$ $p_i^* = 0.237$, $q_i^* = 0.703$ $N_{min} = 15$
$U_A^* = 0$, $U_I^* = -0.0046$	$U_A^* = 0$, $U_I^* = -1.22$

TABLE IV
Optimal strategy for defenders

For scenario 1, the optimal strategy for the defender side is to let each target to be monitored by at most one defender simultaneously at the probability 0.556. The minimum number of required defenders is 6. For scenario 2, the optimal strategy for the defender side is to let each target to be monitored by 2 defenders simultaneously at the probability 0.703. In such case, we have $a(x = 2, y = 1) = 0.64$, the minimum number of required defenders is 15 according to Theorem 3.

From the above results, we can see that the optimal strategy for the defender side depends very much on the parameters such as a, b etc. The payoff U_I in scenario 1 is much less sensitive w.r.t. y especially when $y \leq x - 2$ then in scenario 2. This can be explained by the fact that a_x^y/b_x^y is less sensible w.r.t. y given x when a/b is close to 1 or 0. As a consequence, for scenario 2, deviating from the optimal strategy causes much more severe utility degradation than scenario 1. Another valuable information we can draw from the result is that appropriately configuring the defense system (e.g., setting x, y) is so important that a bad configuration not only is a waste of resource, but causes significant security damage to the system. This result confirms our remark of Theorem 3.

We then study the impact of lack of monitor resource on the network security. The following two cases are simulated: 1). There are N_{min} defenders operating at $\mathbf{q}^*$; 2). There are $N_{min} - 1$ defenders choosing random monitor strategies. 300 random strategies are simulated for this case. In case 2, we set $x = y = 1$ for scenario 1 and $x \leq 2$, $y = 1$ for scenario 2: i.e., for scenario 1, each target is monitored by at most 1 defender at a time; for scenario 2, each target may be monitored by 1 or 2 defenders simultaneously with detection threshold set to 1. This is a reasonable setting noticing the resource and the performance parameters of the scenarios. In both cases, the attacker side chooses its strategy that maximize its payoff and the attack resource P is set to 10. Table 5 shows the payoff degradation due to the lack of sufficient monitor resource.

	Scenario 1	Scenario 2
U_I^1	-0.0045	-1.24
$(U_I^2)_{max}$	-0.37	-2.98
$\overline{U_I^2}$	-1.3	-16.85

TABLE V
PAYOFF DEGRADATION DUE TO RESOURCE CONSTRAINT

In Table 5, U_I^1 is the payoff of the defender side at the NE, $(U_I^2)_{max}$ and $\overline{U_I^2}$ are the maximum and average payoff of the defender side choosing the simulated random strategies. The result shows that lack of monitor resource degrades significantly the system security. This degradation becomes more severe if the attacker side disposes more attack resource. This can be seen comparing the numerical results in Table 5 ($P = 10$) and Table 3 ($P = 1$). Therefore, sufficient resource and appropriate configuration at the defender side are two necessary conditions of efficiently protecting the network from being attacked, which confirms our guideline 3 and 4 in the analytical model.

VII. Conclusion

In this paper, we address the intrusion detection problem in heterogenous networks consisting of nodes with different security assets. We formulated the interaction between the attacks and the defenders as a non-cooperative game and performed an in-depth analysis on the NE and the engineering implications behind. Based on our game theoretical analysis, we derived expected behaviors of rational attackers. We showed that sufficient monitor resource and appropriate configuration at the defender side are two necessary conditions of efficiently protecting the network. We then derived the minimum monitor resource requirement and the optimal strategy of the defender side to achieve system optimality. Based on our results, we provided the guidelines for IDS design and configuration. Finally, two typical scenarios were studied to illustrate the application of our results to design efficient defense system.

As future work, we plan to apply the guidelines in this paper to design efficient defense system in a challenging environment: ad hoc networks.

References

[1] C. Manikopoulos and S. Papavassiliou, “Network intrusion and fault detection: a statistical anomaly approach”. IEEE Communications Magazine, 40(10):76-82, Oct. 2002.

[2] M. Meneganti, F.S. Saviello and R. Tagliaferri, “Fuzzy neural networks for classification and detection of anomalies”. IEEE Transactions on Neural Networks, 9(5):848-861, Sept. 1998.

[3] W. Lee, S.J. Stolfo and K.W. Mok, “Adaptive Intrusion Detection: A Data Mining Approach”. Artificial Intelligence Review, 14(6):533-567, Kluwer Academic Publishers, Norwell, MA, Dec. 2000.

[4] M. Kodialam and T.V. Lakshman, “Detecting Network Intrusions via Sampling: A Game Theoretic Approach”. In IEEE INFOCOM 2003, San Francisco, CA, USA.

[5] T. Alpcan and T. Basar, “A Game Theoretic Analysis of Intrusion Detection in Access Control Systems”. In Proc. 43rd IEEE Conference on Decision and Control (CDC), Paradise Island, Bahamas, 2004.

[6] A. Agah, S. K. Das, K. Basu and M. Asadi, “Intrusion Detection in Sensor Networks: A Non-cooperative Game Approach”. In Proc. 3rd IEEE International Symposium on Network Computing and Applications (NCA04), August-September 2004.

[7] T. Alpcan and T. Basar, “A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection”. In Proc. 42nd IEEE Conference on Decision and Control (CDC), Hawaii, December 2003.

[8] D. Subhadrabandhu, S. Sarkar and F. Anjum, “ A Statistical Framework for Intrusion Detection in Ad Hoc Networks”. In INFOCOM 2006, Barcelona, Spain

[9] Y. Liu, C. Comaniciu and H. Man, “Modelling misbehaviour in ad hoc networks: a game theoretic approach for intrusion detection”. International Journal of Security and Networks (IJSN) 2006, Vol. 1: 243-254

[10] M. J. Osborne and A. Rubinstein, “A course in game theory”. MIT Press

Dépôt légal : 2007 – 4ème trimestre
Imprimé à l’Ecole Nationale Supérieure des Télécommunications – Paris
ISSN 0751-1345 ENST D (Paris) (France 1983-9999)

Ecole Nationale Supérieure des Télécommunications

Groupe des Ecoles des Télécommunications - membre de ParisTech

46, rue Barrault - 75634 Paris Cedex 13 - Tél. + 33 (0)1 45 81 77 77 - www.enst.fr

Département INFRES