A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks

Lin Chen, *Member, IEEE*, and Jean Leneutre

***Abstract*—Due to the dynamic, distributed, and heterogeneous 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 classical security approaches. In this paper, we address the intrusion detection problem in heterogeneous networks consisting of nodes with different noncorrelated 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 noncooperative 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 guidelines for IDS design and deployment. We also show how our game theoretical framework can be applied to configure the intrusion detection strategies in realistic scenarios via a case study. Finally, we evaluate the proposed game theoretical framework via simulations. The simulation results show both the correctness of the analytical results and the effectiveness of the proposed guidelines.**

***Index Terms*—Game theory, intrusion detection system (IDS), Nash equilibrium (NE).**

I. Introduction

TODAY'S computer and communication networks are becoming more and more dynamic, distributed, and heterogeneous, 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. Consequently, today's networks are much more vulnerable to various attacks such as TCP SYN flooding, SSPing, and DoS attack, etc. 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.

Manuscript received January 07, 2008; revised February 02, 2009. First published April 17, 2009; current version published May 15, 2009. This work was supported French ANR project grant, ANR-05-SSIA-0018 (CLADIS). The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Roy A. Maxion.

The authors are with the Department of Computer Science and Networks, Telecom ParisTech, CNRS LTCI-UMR 5141 Laboratory, 75013 Paris, France (e-mail: lchen@enst.fr; leneutre@enst.fr).

Digital Object Identifier 10.1109/TIFS.2009.2019154

In almost all contemporary networks, network nodes (targets from the attackers's point of view) usually have different sensibility levels or possess different security assets depending on their roles and the data or information they hold. In other words, the networks are usually heterogeneous in terms of security. More specifically, some targets are more "attractive" to attackers than others. Examples of such targets include the servers containing 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 heterogeneous 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 noncooperative game model of the network intrusion detection problem, analyzing the resulting equilibria, 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.

Our main contributions can be summarized as follows:

1) We provide a game theoretical framework of intrusion detection in heterogeneous networks where targets have different security assets.
2) Under the framework, we derive the expected behaviors of rational attackers, the minimum monitor resource requirement of the defenders, and the optimal strategy of the defenders.

The paper proceeds as follows. In Section II, we formulate the noncooperative intrusion detection game. In Sections III and IV, we study the Nash equilibrium (NE) of the game in the case of single and multiple attacker(s)/defender(s), respectively. Based on our analysis, we derive optimal defender strategy and guidelines for IDS design and deployment. In Section V, we show how our game theoretical framework can be applied to configure the intrusion detection strategies via a case study. Section VI discusses some variants and extensions of the game. Section VII provides numerical results of the game theoretical framework. Section VIII discusses related work, and Section IX concludes the paper.

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 IDS module which we refer to as *defenders* throughout the paper, $\mathcal{S}_\mathcal{A}$ is the set of *attackers* and $\mathcal{T} = \{1, 2, \ldots, N\}$ is the set of network nodes which may be attacked by the attackers, referred to as *targets*. We start with

TABLE I
STRATEGIC FORM OF THE GAME FOR TARGET i

	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	$0, -bC_fW_i - C_mW_i$	$0, 0$

the simplest case where there are only one attacker and one defender. We model the interactions between them as a noncooperative game. The objective of the attacker is to attack the targets without being detected. To this end, it chooses the strategy $\mathbf{p} = \{p_1, p_2, \ldots, p_N\}$ which is the attack probability distribution over the target set $\mathcal{T}$, where p_i is the probability of attacking target i. $\sum_{i\in\mathcal{T}} p_i \leq P \leq 1$ represents the attacker's resource constraint. This constraint 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 $\mathbf{q} = \{q_1, q_2, \ldots, q_N\}$, where q_i is the probability of monitoring target i. Here, monitor means that the defender collects audit data and examines them for signs of security problems. Similarly, we have $\sum_{i\in\mathcal{T}} q_i \leq Q \leq 1$ that represents the defender's monitor resource constraint.

We assume that each target $i \in \mathcal{T}$ processes an amount of security asset denoted as W_i, representing the loss of security when the attacks on i are successful, e.g., loss of reputation or 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. In practice, the security assets are evaluated in the risk analysis/assessment phase using formal analysis or specific tools before the IDS deployment. If the attack on target i is not detected, then the attacker gets payoff W_i while the defender gets payoff $-W_i$. Otherwise, the payoffs for the attacker and defender are $-W_i$ and W_i, respectively. Other payoff formulations are also possible. In those cases, our analysis in this paper can be extended by modifying the utility function of the attacker and defender.

Throughout this paper, we assume that the security assets of different targets are independent. We argue that this assumption holds in many scenarios such as ad hoc networks where no hierarchy or infrastructure is available and each node operates independently of others. A natural extension is to study the scenarios where the security assets of the targets are correlated. This extension is not addressed in this paper, but it is on our research plan. Another limitation of our work in this study is the static full information game formulation. However, despite this simplification and limitation, the results and their implications are far from trivial. In fact, our model presented here can serve as a theoretical basis for further more sophisticated game models on the intrusion detection problem tailored to specific scenarios.

Table I illustrates the payoff matrix of the attacker/defender interaction on target i in the strategic form. In the matrix, a denotes the detection 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) 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 denotes 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 $C_m < 1$.

The overall payoffs of the attacker and defender, defined by the utility functions U_A and U_D, are as follows:

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

We end this section with the definition of the network intrusion detection game with one attacker/defender.

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

$$\begin{aligned} &\text{Players:} && \text{Attacker, Defender} \\ &\text{Strategy set:} && \text{Attacker:} \\ &&& A_A = \left\{\mathbf{p}: \mathbf{p}\in[0,P]^N, \sum_{i\in\mathcal{N}} p_i \leq P\right\} \\ &&& \text{Defender:} \\ &&& A_D = \left\{\mathbf{q}: \mathbf{q}\in[0,Q]^N, \sum_{i\in\mathcal{N}} q_i \leq Q\right\} \\ &\text{Payoff:} && U_A \text{ for attacker, } U_D \text{ for defender} \\ &\text{Game rule:} && \text{The attacker/defender selects its strategy} \\ &&& \mathbf{p}/\mathbf{q} \in A_A/A_D \text{ to maximize } U_A/U_D. \end{aligned}$$

III. SOLVING THE GAME

For noncooperative games as G, the most important solution concept is the NE, where no player has incentive to deviate from its current strategy [14]. The NE can be seen as optimal "agreements" between the players. In the case of G, we have the following definition of NE.

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

A. Sensible Target Set

In G, since the attacker has limited attack resources, a natural question is 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

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

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:

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

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

$\mathcal{T}_\mathcal{Q}$ consists of the target(s) i such that $W_i = (N_A\cdot(1-C_a)-2aQ)/((1-C_a)\sum_{j=1}^{N_A}(1/W_j))$.

Proof: The proof consists of first showing that $\mathcal{T}_\mathcal{S}$ is composed of n targets with the largest security assets and then proving $n = N_A$ by showing that 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 straightforwardly. It is obvious that N_A targets with the largest security assets satisfying (2) consist of a sensible target set $\mathcal{T}_\mathcal{S}$ in that (1) holds in such a 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 $\forall j < i (W_j \ge W_i)$; it holds that $j \in \mathcal{T}_\mathcal{S}$, if not, there exists $j_0 < i (W_{j_0} \ge W_i)$ such that $j_0 \in \mathcal{T}-\mathcal{T}_\mathcal{S}$. It follows that $W_{j_0} \le (|\mathcal{T}_\mathcal{S}|\cdot(1-C_a)-2aQ)/((1-C_a)\sum_{k\in\mathcal{T}_\mathcal{S}}(1/W_k))$. On the other hand, from Definition 3, we have $W_i > (|\mathcal{T}_\mathcal{S}|\cdot(1-C_a)-2aQ)/((1-C_a)\sum_{k\in\mathcal{T}_\mathcal{S}}(1/W_k))$. It follows that $W_i > W_{j_0}$, which contradicts with $W_{j_0} \ge W_i$. 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 $n < N_A$, from (2), we have

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

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

$$\Longrightarrow W_{N_A}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right) - (N_A-n) > n - \frac{2aQ}{1-C_a}.$$

Noticing $W_{N_A} \le W_i, \forall i \le N_A$ and $n < N_A$ (i.e. $W_{n+1} \ge W_{N_A}$), we have

$$\begin{aligned} W_{n+1}\left(\sum_{j=1}^{n}\frac{1}{W_j}\right) &\ge W_{N_A}\left(\sum_{j=1}^{n}\frac{1}{W_j}\right) \\ &= W_{N_A}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right) - W_{N_A}\left(\sum_{j=n+1}^{N_A}\frac{1}{W_j}\right) \\ &\ge W_{N_A}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right) - (N_A-n) \\ &> n - \frac{2aQ}{1-C_a}. \end{aligned}$$

Hence, $W_{n+1} > (n\cdot(1-C_a)-2aQ)/((1-C_a)\sum_{j=1}^{n}(1/W_j))$. On the other hand, from Definition 3, we have $W_{n+1} \le (n\cdot(1-C_a)-2aQ)/((1-C_a)\sum_{j=1}^{n}(1/W_j))$. This contradiction shows that 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, and 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 $N_A \ge 1$. 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 nondecreasing in Q. If $2aQ \ge N(1-C_a)$, $|\mathcal{T}_\mathcal{S}| = N$ or $\mathcal{T}_\mathcal{S} = \mathcal{T}$. We investigate the following three typical scenarios to gain a more in-depth insight on $\mathcal{T}_\mathcal{S}$.

1) In the degenerate 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 $W_1 \simeq \cdots \simeq W_k \gg W_{k+1} \ge \cdots \ge W_N$, $N_A = k$.

$\mathcal{T}_\mathcal{Q}$ can be regarded as the border set between $\mathcal{T}_\mathcal{S}$ and $\mathcal{T}-\mathcal{T}_\mathcal{S}$ and may be empty.

We now study the security implications of $\mathcal{T}_\mathcal{S}$ in the following theorem.

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 of 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 $W_N \ge (N_A\cdot(1-C_a)-2aQ)/((1-C_a)\sum_{j=1}^{N_A}(1/W_j))$, $\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q} = \emptyset$, the theorem holds evidently. We now prove the case where $W_N < (N_A\cdot(1-C_a)-2aQ)/((1-C_a)\sum_{j=1}^{N_A}(1/W_j))$, in other words, $\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q} \ne \emptyset$.

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

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

It holds that $q_i^0 \ge 0$ and $\sum_{i=1}^{N_A} q_i^0 = Q$. Let $\mathbf{q} = (q_1, q_2, \ldots, q_N)$ denote the monitor probability distribution of the defender, by the Pigeon Hole Principle, it holds that $\sum_{i=1}^{N_A} q_i \le Q$, thus $\exists m \in \mathcal{T}_\mathcal{S}$ such that $q_m \le q_m^0$.

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

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

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

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

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 if 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: A rational defender only needs to monitor the targets in $\mathcal{T}_\mathcal{S} + \mathcal{T}_\mathcal{Q}$.

B. NE Analysis

In this subsection, we derive the NE of the intrusion detection game G. We can easily check that G is a two-person game defined in [13] and thus admits at least one NE following Theorem 1 in [13]. Moreover, let $(\mathbf{p}^*, \mathbf{q}^*)$ denote the NE of G, it holds that

$$\begin{aligned} 0 &\leq (1-2aq_i^*-C_a)W_i = (1-2aq_j^*-C_a)W_j \\ &\geq (1-2aq_k^*-C_a)W_k \ \ \forall i,j,k \in \mathcal{T}, p_i^*, p_j^* > 0, p_k^* = 0. \end{aligned} \quad (3)$$

Equation (3) can be shown by noticing the attacker's utility function U_A: if $(1-2aq_i^*-C_a)W_i < 0$, then the attacker has incentive to change p_i^* to 0; if $(1-2aq_i^*-C_a)W_i < (1-2aq_j^*-C_a)W_j$, then the attacker has incentive to decrease p_i^* and increase p_j^*; if $(1-2aq_i^*-C_a)W_i < (1-2aq_k^*-C_a)W_k$, then the attacker gets more payoff by adding p_i^* to p_k^* and setting $p_i^* = 0$. In the same way, noticing the defender's utility function U_D, it holds that

$$\begin{aligned} 0 &\leq W_i\left[p_i^*(2a+bC_f) - (bC_f+C_m)\right] \\ &= W_j\left[p_j^*(2a+bC_f) - (bC_f+C_m)\right] \\ &\geq W_k\left[p_k^*(2a+bC_f) - (bC_f+C_m)\right] \\ &\quad \forall i,j,k \in \mathcal{T}, q_i^*, q_j^* > 0, q_k^* = 0. \end{aligned} \quad (4)$$

Noting the resource constraint of the players, we consider the following cases.

Case 1: $\sum_{i\in\mathcal{T}} q_i^* = Q$ and $\sum_{i\in\mathcal{T}} p_i^* = P$: In this case, combining (3) and (4) leads to

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

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

where $P_A > (N_A - W_{N_A}\sum_{j=1}^{N_A}(1/W_j))((bC_f+C_m)/(2a+bC_f))$, and $\sum_{i\in\mathcal{T}} p_i^* = P$. The necessary condition for the solution to be an NE is

$$\begin{cases} W_i\left[p_i^*(2a+bC_f) - (bC_f+C_m)\right] \geq 0, P_A \leq P \\ (1-2aq_i^*-C_a)W_i \geq 0, & i \in \mathcal{T}_\mathcal{S} \end{cases} \Longrightarrow \begin{cases} N_D \geq N_A \\ N_A(1-C_a) \geq 2aQ \end{cases}$$

where $N_D = \lfloor (2a+bC_f)P/(bC_f+C_m) \rfloor$, where $\lfloor n \rfloor$ denotes the largest integer not more than n.

Case 2: $\sum_{i\in\mathcal{T}} q_i^* < Q$ *and* $\sum_{i\in\mathcal{T}} p_i^* = P$*:* In this case, noticing U_D, we have

$$\begin{aligned} &W_i\left[p_i^*(2a+bC_f)-(bC_f+C_m)\right]=0 \\ &\geq W_j\left[p_j^*(2a+bC_f)-(bC_f+C_m)\right] \quad \forall i,j\in\mathcal{T}, q_i^*>0, q_j^*=0. \end{aligned}$$

Otherwise the defender will increase q_i^* to get more payoff. Combining the above equation with (3) and (4), we can solve $\mathbf{p}^*, \mathbf{q}^*$ as

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

$$q_i^* = \begin{cases} \frac{1-C_a}{2a}\left(1-\frac{W_{N_D+1}}{W_i}\right), & W_i > W_{N_D+1} \\ 0, & W_i \leq W_{N_D+1} \end{cases}$$

where $\sum_{i\in\mathcal{T}} p_i^* = P$. The necessary condition for the derived solution to be an NE is

$$\begin{aligned} \sum_{W_i>W_{N_D+1}} q_i^* < 1 &\Longrightarrow N_D < W_{N_D+1} \sum_{W_i>W_{N_D+1}} \frac{1}{W_i} + \frac{2aQ}{1-C_a} \\ &\Longrightarrow N_D < N_A \quad \text{(From (2) in Lemma 1).} \end{aligned}$$

Particularly, if $N_D = 0$, then $q_i^* = 0, \forall i \in \mathcal{T}$ and

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

where $\sum_{i\in\mathcal{T}, W_i=W_1} p_i^* = P$.

Case 3: $\sum_{i\in\mathcal{T}} q_i^* < Q$ *and* $\sum_{i\in\mathcal{T}} p_i^* < P$*:* In this case, we have

$$\begin{cases} (1-2aq_i^*-C_a)W_i = 0 \\ W_i\left[p_i^*(2a+bC_f)-(bC_f+C_m)\right]=0 \end{cases} \quad i\in\mathcal{T}$$

$$\Longrightarrow \begin{cases} p_i^* = \frac{bC_f+C_m}{2a+bC_f} \\ q_i^* = \frac{1-C_a}{2a} \end{cases} \quad i\in\mathcal{T}.$$

The necessary condition of $\sum_{i\in\mathcal{T}} q_i^* < Q$ and $\sum_{i\in\mathcal{T}} p_i^* < P$ is $N_D \geq N$ and $N(1-C_a) \geq 2aQ$. Moreover, from Lemma 1, in this case, it holds that $N_A = N$.

The following theorem summarizes the above analysis results on the NE of G.

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

1) If $N_D < N_A$, then

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

$$q_i^* = \begin{cases} \frac{1-C_a}{2a}\left(1-\frac{W_{N_D+1}}{W_i}\right), & W_i > W_{N_D+1} \\ 0, & W_i \leq W_{N_D+1} \end{cases}$$

where $\sum_{i\in\mathcal{T}} p_i^* = P$.

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

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

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

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

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

$$p_i^* = \frac{bC_f+C_m}{2a+bC_f}, \quad q_i^* = \frac{1-C_a}{2a}, \quad i\in\mathcal{T}.$$

Remark 1: In Case 1 of Theorem 2, the attacker disposes limited attack resources such that the defender does not use up all of 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 that can be drawn is that in some cases where the attack intensity is low, it is a waste of resources for the defender to monitor all the time. If the monitor cost outweighs the gain, the defender is better off keeping silent.

Remark 2: In Case 2, both the attacker and defender use up all their resources 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_D is monotonously increasing in P/Q; i.e., given more resources, both players can increase their payoff, as shown in the following:

$$\begin{cases} U_A(\mathbf{p}^*,\mathbf{q}^*) = P\frac{N_A\cdot(1-C_a)-2aQ}{\sum_{j=1}^{N_A}\frac{1}{W_j}} \\ U_D(\mathbf{p}^*,\mathbf{q}^*) = Q\left[\frac{P(2a+bC_f)}{\sum_{j=1}^{N_A}\frac{1}{W_j}} - \frac{N_A(bC_f+C_m)}{\sum_{j=1}^{N_A}\frac{1}{W_j}}\right] \\ \quad -\frac{PN_A}{\sum_{j=1}^{N_A}\frac{1}{W_j}} + \frac{N_A^2}{\sum_{j=1}^{N_A}\frac{1}{W_j}}\frac{bC_f+C_m}{2a+bC_f} - \frac{bC_f+C_m}{2a+bC_f}\sum_{j=1}^{N_A} W_j. \end{cases} \tag{5}$$

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 in this case.

Corollary 1: In Case 2 of Theorem 2, for $\forall \mathbf{p}' \neq \mathbf{p}^*$, $\forall \mathbf{q}' \neq \mathbf{q}^*$, let $\widehat{\mathbf{p}} = \arg\max_{\mathbf{p}\in A_A} U_A(\mathbf{p},\mathbf{q}')$, $\widehat{\mathbf{q}} = \arg\max_{\mathbf{q}\in A_I} U_D(\mathbf{p}',\mathbf{q})$ it holds that $U_D(\mathbf{p}^*,\mathbf{q}^*) > U_D(\widehat{\mathbf{p}},\mathbf{q}')$ and $U_A(\mathbf{p}^*,\mathbf{q}^*) > U_A(\mathbf{p}',\widehat{\mathbf{q}})$.

Proof: The proof is similar to that of Theorem 1. ■

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. From the defender's point of view, operating on $\mathbf{q}$ is the optimal strategy in the worst-case scenario where the attack has sufficient attack resources.

Remark 3: In Case 3, 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 is $\mathcal{T}_{\mathcal{S}} = \mathcal{T}$, 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 targets. Moreover, at the NE, we have

$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) = 0 \\ U_D(\mathbf{p}^*, \mathbf{q}^*) = -\frac{bC_f + C_m}{2a + bC_f} \sum_{j=1}^{N} W_j. \end{cases} \tag{6}$$

The implications behind (6) are as follows.

1) Disposing more attack or monitor resources 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.

C. Further Security Implications Behind NE

Theorem 2 quantifies the behavior of a rational attacker and defender at the NE from which no player has 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. From Theorem 2, we can see that a rational attacker will never choose the extreme strategies such as attacking the target with the largest security asset, or 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 focuses its attack on $\mathcal{T}_{\mathcal{S}}$ and $\mathcal{T}_{\mathcal{Q}}$ 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 nonmonitored targets.

In fact, to equalize the attacker's payoff of attacking any monitored targets turns out 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 defender's payoff 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 Case 2 where the monitor resource is constrained and Case 3 where defender disposes sufficient resource.

From (5) and (6), we can see that the resource constraint has a significant negative impact on the system when P is large: For the attacker, it cannot get any profit if the defender has enough resources 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

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

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

Following the above analysis, the necessary conditions to limit the damage caused by the attacker are disposing sufficient monitor resources and operating on $\mathbf{q}^*$ of Case 3 of Theorem 2 in that the attacker's payoff drops to 0 at the NE regardless of the attack resource P.

Until now, our analysis was based on the condition that there is one defender, i.e., $Q \leq 1$. In cases where $N(1 - C_a) > 2a$, one defender is not enough to maintain the favorable NE. Obviously, more than one defender is needed. 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? How can they be configured to maximize U_D?

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 themselves 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 simultaneously with success, the attack gain is $U_A^m = (1 - C_a)W_m$, not $2(1 - C_a)W_m$.

Assumption 3 is a simplified scenario. In fact, the attack gain may range from $(1 - C_a)W_m$ to $\min\{2(1 - C_a)W_m, 2W_m\}$ depending on the specific scenarios; noticing that target m cannot lose more than the security asset W_m, it holds even in the worst case. Here in order to perform a closed-form analysis, we focus on the simplified scenario where the gain of multiple attacks on the same target is not cumulative. We consider it a reasonable assumption when the attackers can communicate among them and multiplying attacks does not increase the chance of success or decrease the attack cost. In other scenarios, the assumption does not hold. However, our analysis in the simplified case can

be adapted to investigate these cases by modifying the attackers' utility function to take into account the cumulative effect of the attacks on the attacker's gain and cost.

At the defender side, having multiple defenders monitor the same target influences the detection and the false alarm rate; thereby it may change the final payoff. We thus 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. 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 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. Applying Theorem 2, the NE $(\mathbf{p}^*, \mathbf{q}^*)$ can be derived as follows.

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 attacks. The payoffs of the players at the NE are
$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) = (1 - C_a - 2a) \sum_{i \in \mathcal{T}} W_i \\ U_D(\mathbf{p}^*, \mathbf{q}^*) = -(1 - 2a + C_m) \sum_{i \in \mathcal{T}} W_i. \end{cases}$$
2) If $2a > 1 - C_a$, then $p_i^* = (bC_f + C_m)/(2a + bC_f)$, $q_i^* = (1 - C_a)/2a$, $i \in \mathcal{T}$. The correspondent payoffs are: $U_A(\mathbf{p}^*, \mathbf{q}^*) = 0$ and $U_D(\mathbf{p}^*, \mathbf{q}^*) = -\sum_{i \in \mathcal{T}}((bC_f + C_m)/(2a + bC_f))W_i$.

Here we implicitly assume that $C_m \leq 2a$ in that $C_m > 2a$ leads to $q_i^* = 0$, which is the trivial case that we do not address 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, $\sum_{i \in \mathcal{T}} q_i = N(1 - C_a)/2a$. Noticing that each defender disposes at most $q_i = 1$ as a monitor resource, we need at least $N_{\min} = \lceil N(1 - C_a)/2a \rceil$ 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 $C_a \ll 1$, $N_{\min} \sim (N(1 - C_a)/2a) \sim (N/2a) > (N/2)$.

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 resources are required because in such a 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. As to price, the monitor cost is higher.

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
$$\begin{cases} a_x^y = \sum_{i=y}^{x} \binom{x}{i} a^i (1 - a)^{x-i} \\ b_x^y = \sum_{i=y}^{x} \binom{x}{i} b^i (1 - b)^{x-i} \end{cases}$$
where a and b are the detection and false alarm rates of the individual defender. The following lemma studies a_x^y and b_x^y. The proof is straightforward and thus is omitted here.

Lemma 2: $\forall x, y \in \mathbb{Z}^+, y \leq x$ and $0 < a, b < 1$, it holds that
- 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 $p_i^* = 1$, $q_i^* = 1, \forall i \in \mathcal{T}$
$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) = \left(1 - C_a - 2a_{x_i}^{y_i}\right) \sum_{i \in \mathcal{T}} W_i \\ U_D(\mathbf{p}^*, \mathbf{q}^*) = -\left(1 - 2a_{x_i}^{y_i} + x_i C_m\right) \sum_{i \in \mathcal{T}} W_i. \end{cases}$$
2) If $2a_{x_i}^{y_i} > 1 - C_a$, then $p_i^* = (b_{x_i}^{y_i} C_f + x_i C_m)/(2a_{x_i}^{y_i} + b_{x_i}^{y_i} C_f)$, $q_i^* = (1 - C_a)/2a_{x_i}^{y_i}$, $i \in \mathcal{T}$. The correspondent payoff is $U_A(\mathbf{p}^*, \mathbf{q}^*) = 0$ and $U_D(\mathbf{p}^*, \mathbf{q}^*) = -\sum_{i \in \mathcal{T}}(b_{x_i}^{y_i} C_f + x_i C_m)/(2a_{x_i}^{y_i} + b_{x_i}^{y_i} C_f)W_i$

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 degenerate case $x_i = y_i = 1$. For Case 1, we have $N_{\min} = N$ at $x_i = y_i = 1$. For Case 2, if $x_i = 1$, $N_{\min} = N$; if $x_i > 1$, it follows from Lemma 2 that $N_{\min} = \lceil \sum_{i \in \mathcal{T}} x_i((1 - C_a)/2a_{x_i}^{y_i}) \rceil \geq \lceil N(1 - C_a)/2a \rceil$.

Compare the above analysis with the results in Section IV-A, where each target is monitored by one defender; 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 a 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 $\max_{1\le y_i\le x_i} U_D(\mathbf{p}^*,\mathbf{q}^*)$, as summarized in the following theorem.

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^*

$$(x^*,y^*)=\begin{cases}\arg\min\limits_{1\le y\le x,2a_x^y\le 1-C_a} 1-2a_x^y+C_m, & C_1<C_2\\ \arg\min\limits_{1\le y\le x,2a_x^y>1-C_a} \frac{b_x^yC_f+xC_m}{2a_x^y+b_x^yC_f}, & C_1\ge C_2\end{cases}$$

where

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

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 suboptimality at the defender side even if it disposes sufficient monitor resource. We will show this point via numerical study in Section VII.

At the optimal configuration, at least $N_{\min}=\lceil(Nx^*(1-C_a)/2\sum_{i=y^*}^{x^*}C_{x^*}^i a^i(1-a)^{x^*-i})\rceil$ 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: At least $\lceil N(1-C_a)/2a\rceil$ defenders are needed in order to effectively monitor the targets.

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

V. Model Application: Case Study

In this section, we show how our game theoretical framework can be applied in IDS configuration and deployment via a case study. In [11], Subhadrabandhu *et al.* postulate that the wireless ad hoc networks in near future will consist of two classes of nodes: 1) inside nodes communicate using the network and at the same time perform system tasks like relaying packets, discovering routes, securing communication, etc.; 2) outside nodes only communicate using the network. Examples of inside nodes include predeployed terminals, access points, and trusted users. Outside nodes are usually common users and visitors. In such architecture, to ensure the security of the network, a subset of inside nodes are equipped with IDS modules. Such inside nodes are called IDS capable inside nodes. Operating in promiscuous mode, the IDS capable inside nodes monitor the outside nodes in their neighborhood in order to isolate any malicious attackers. Due to the coverage redundancy, each outside node is monitored by multiple IDS capable inside nodes, which may decide differently based on their own observations. These different decisions are further combined to make the final decision. In such context, the task for the IDS designer is to determine how many IDS capable inside nodes are needed to monitor efficiently the outside nodes and how to configure them.

Theorem 3 can be applied to answer the above question. More specifically, by solving the optimization problem $\max_{1\le x\le y} U_D(\mathbf{p}^*,\mathbf{q}^*)$, we obtain x^* and y^*. The resulting optimal strategy is thus to let x^* IDS capable insides nodes monitor one outside node simultaneously with the detection threshold y^*. 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. Moreover, let N_o be the number of outside nodes to be monitored in the network, $\lceil(N_ox^*(1-C_a)/2\sum_{i=y^*}^{x^*}\binom{x^*}{i}a^i(1-a)^{x^*-i})\rceil$ IDS capable inside nodes are needed to efficiently monitor the outside nodes in the network. In other words, each outside node should be monitored by at least $\lceil(x^*(1-C_a)/2\sum_{i=y^*}^{x^*}\binom{x^*}{i}a^i(1-a)^{x^*-i})\rceil$ IDS capable inside nodes.

After dimensioning the IDS capable inside nodes, the next step is to select the IDS capable inside nodes among all inside nodes. The goal of this step is to minimize the number of IDS capable nodes under the constraint that each outside node is monitored by at least $\lceil(N_ox^*(1-C_a)/2\sum_{i=y^*}^{x^*}\binom{x^*}{i}a^i(1-a)^{x^*-i})\rceil$ IDS capable inside nodes. The heuristic algorithm MUNEN proposed in [11] can be applied here to select IDS inside nodes.

It is interesting to compare our work with that in [11] where the authors propose a statistical framework for intrusion detection for ad hoc networks. They focus on minimizing the monitor resource consumption subject to limiting the security risk under given threshold. Our work, on the other hand, focuses on finding the optimal strategy for the defenders to achieve system optimality in terms of security. These two solutions actually address the intrusion detection problem from two different angles, in [11] from an optimization angle while in ours from a game theoretical angle.

VI. Extensions and Variants

In this section, we investigate some variants and extensions of our model.

A. Stackelberg Network Intrusion Detection Game

In the previous sections, we focused on the intrusion detection game where both the attacker and the defender side take the decision locally at the same time. However, in many cases, the attackers may launch attacks based on the strategy of the defenders or conversely, the defenders decide the strategy based on the attackers' strategy. In this subsection, we address these cases by modeling the interaction between the attackers and the defenders as a Stackelberg game [14], in which a "leader" chooses a strategy and then a "follower," informed of the leader's choice, chooses its strategy accordingly such that both sides try to maximize their payoff. We thus formulate a noncooperative Stackelberg game for the intrusion detection G^S as follows. In the

following formulation, the attacker side plays the role of leader; the counterpart case where the defender side plays the role of leader can be formulated in the same way

Players :	Leader : attacker side; Follower : defender side
Strategy :	$\mathbf{p} \in A_A$ and $\mathbf{q} \in A_D$
Payoff :	U_A for leader and U_D for follower
Game rule :	the leader decides $\mathbf{p}$ first, the follower decides $\mathbf{q}$ after knowing $\mathbf{p}$.

Follower's Problem:
The follower is given the leader's chosen strategy. It then chooses its strategy to maximize its payoff. Formally, for any given $\mathbf{p} \in A_A$, the follower solves the following optimization problem:

$$\mathbf{q}(\mathbf{p}) = \arg\max_{\mathbf{q} \in A_D} U_D(\mathbf{p}, \mathbf{q}).$$

Leader's Problem:
The leader knows that the follower will choose its strategy to greedily maximize its payoff. Therefore, the leader chooses its strategy which will maximize its payoff, given the follower will subsequently choose its strategy to maximize its payoff. Formally, the leader solves the following optimization problem:

$$\mathbf{p}(\mathbf{q}) = \arg\max_{\mathbf{p} \in A_A} U_A\left(\mathbf{p}, \mathbf{q}(\mathbf{p})\right).$$

The above analysis implicitly assumes that the solution of the follower's problem $\mathbf{q}(\mathbf{p})$ is a point-to-point mapping. In the case where $\mathbf{q}(\mathbf{p})$ is not unique, i.e., $\mathbf{q}(\mathbf{p})$ is a point-to-set mapping, it is natural to perform a worst-case analysis at the leader side. More specifically, the leader chooses its strategy that yields the best payoff in the worst case, as will be shown in later analysis.

The Stackelberg game is often solved by backwards induction: First solve the follower's problem for every possible strategy taken by the leader. The solution consists of the best response strategy of the follower as a function of the leader's strategy. Then the leader decides its optimal strategy according to the follower's best response strategy. The obtained solution is often referred to as a Stackelberg equilibrium (SE) or Stackelberg–Nash equilibrium (SNE).

Next we study the SNE of G^S for the case where the attacker side is the leader and the follower, respectively. In the following study, we focus on the scenario where $2a > 1 - C_a$, $C_m, C_a \ll 1$, both the attacker and the defender side process sufficient attack and monitor resource P and Q respectively, and each target is monitored by at most one defender at any time. However, our study is also applicable in other cases although the result may be different.

1) Leader: Attacker Side; Follower: Defender Side: In this case, the attacker side is the leader. By performing backwards induction, we can solve the best response of the follower as

$$q_i(\mathbf{p}) \begin{cases} = 0, & p_i < \frac{bC_f + C_m}{2a + bC_f} \\ \in [0,1], & p_i = \frac{bC_f + C_m}{2a + bC_f} \\ = 1, & p_i > \frac{bC_f + C_m}{2a + bC_f}. \end{cases}$$

Noticing the payoff of the leader is $\sum_{i \in \mathcal{T}} p_i W_i (1 - C_a - 2aq_i(\mathbf{p}))$, we obtain the SNE $(\mathbf{p^S}, \mathbf{q^S})$ as follows:

$$\begin{cases} p_i^S = \frac{bC_f + C_m}{2a + bC_f}, & i \in \mathcal{T} \\ q_i^S = 0, & i \in \mathcal{T}. \end{cases}$$

The corresponding payoff of the leader and follower is as follows:

$$\begin{cases} U_A(\mathbf{p^S}, \mathbf{q^S}) = \frac{bC_f + C_m}{2a + bC_f}(1 - C_a) \sum\limits_{i \in \mathcal{T}} W_i \\ U_D(\mathbf{p^S}, \mathbf{q^S}) = -\frac{bC_f + C_m}{2a + bC_f} \sum\limits_{i \in \mathcal{T}} W_i. \end{cases}$$

However, the above obtained SNE is a weak equilibrium in that $U_D(\mathbf{p^S}, \mathbf{q^S}) = U_D(\mathbf{p^S}, \mathbf{q}'), \forall \mathbf{q}' \in \mathbf{A_D}$; hence, the leader is not sure whether the follower will operate on $\mathbf{q^S}$ or not. This may have detrimental effect on the payoff of the leader: e.g., if the follower sets $q_i = 1$ for all target i instead of $q_i = 0$, then $U_A = ((bC_f + C_m)/(2a + bC_f)(1 - C_a - 2a)) \sum_{i \in \mathcal{T}} W_i < 0$, as a consequence, the leader get negative payoff. This is clearly not desirable for the leader (attacker) in that its payoff is 0 when doing nothing.

To push the follower to choose the desired $\mathbf{q^S}$ from the leader's perspective, the leader has incentive to set $p_i = p_i^S - \epsilon = ((bC_f + C_m)/(2a + bC_f)) - \epsilon$, where ϵ is a small positive number. Under such context, the follower will operate on $\mathbf{q^S}$. For the leader, its payoff is $((bC_f + C_m)/(2a + bC_f))(1 - C_a) - \epsilon(1 - C_a) \sum_{i \in \mathcal{T}} W_i$, only slightly less than its desired payoff at the SNE if ϵ is sufficiently small, which we argue is acceptable for the leader.

2) Leader: Defender Side; Follower: Attacker Side: The above analysis can be applied in this symmetrical case where the leader is the defender side. The SNE $(\mathbf{p^S}, \mathbf{q^S})$ is

$$\begin{cases} p_i^S = 0, & i \in \mathcal{T} \\ q_i^S = \frac{1 - C_a}{2a}, & i \in \mathcal{T}. \end{cases}$$

To push the follower to choose the desired $\mathbf{p^S}$ from the leader's point of view, the leader sets $q_i = q_i^S - \delta = ((1 - C_a)/2a) + \delta$, where δ is a small positive number. Under such context, the follower will operate on $\mathbf{p^S}$. For the leader, its payoff is $-((1 - C_a)/2a)(C_m + bC_f) \sum_{i \in \mathcal{T}} W_i - \delta(C_m + bC_f) \sum_{i \in \mathcal{T}} W_i$, only slightly less than its desired payoff at the SNE if δ is sufficiently small.

3) Lead or Follow: We next consider an interesting scenario where the attack/defender side decides whether to be the leader (pick the leader's strategy obtained previously) or the follower (pick the follower's strategy) without the knowledge of its opponent's choice. In such context, does the strategy to be the leader dominate the strategy to be the follower in that according to our analysis, the leader may "control" the behavior of the follower to some extent, but does it hold in the scenario considered in this subsection?

We study the following "lead or follow" intrusion detection game to answer the posed question: the players are the attacker

TABLE II
PAYOFF MATRIX OF THE LEAD-OR-FOLLOW GAME

	Lead ($\mathbf{p^L}$)	Follow ($\mathbf{p^F}$)
Lead	$U_A = -\dfrac{bC_f + C_m}{2a + bC_f}\delta \sum_{i\in\mathcal{T}} W_i$	$U_A = 0$
($\mathbf{q^L}$)	$U_D = -\left[\dfrac{bC_f + C_m}{2a + bC_f} + \dfrac{1 - C_a}{2a}(2a + bC_f)\epsilon - \epsilon\right] \sum_{i\in\mathcal{T}} W_i$	$U_D = -\left(\dfrac{1 - C_a}{2a} + \delta\right)(bC_f + C_m) \sum_{i\in\mathcal{T}} W_i$
Follow	$U_A = \left(\dfrac{bC_f + C_m}{2a + bC_f} - \epsilon\right)(1 - C_a) \sum_{i\in\mathcal{T}} W_i$	$U_A = 0$
($\mathbf{q^F}$)	$U_D = -\left(\dfrac{bC_f + C_m}{2a + bC_f} - \epsilon\right)(1 - C_a) \sum_{i\in\mathcal{T}} W_i$	$U_D = 0$

and the defender side; they choose either the leader strategy (denoted by $\mathbf{p^L}$ and $\mathbf{q^L}$, respectively) or the follower strategy (denoted by $\mathbf{p^F}$ and $\mathbf{q^F}$, respectively) to maximize their payoff U_A and U_D defined previously. $\forall i \in \mathcal{T}$, we have

$$p_i^L = \frac{bC_f + C_m}{2a + bC_f} - \epsilon, \quad p_i^F = 0$$
$$q_i^L = \frac{1 - C_a}{2a} + \delta, \quad q_i^F = 0.$$

The payoff of the attacker and the defender side is depicted in Table II. Since both ϵ and δ are sufficiently small, the terms containing $\epsilon\delta$ are ignored in the table.

Recall that we consider the scenario where $2a > 1 - C_a$ and $C_m, C_a \ll 1$. From the point of view of the defender side, the first row is strictly dominated by the second row, indicating that the defender side is always better off choosing to be the follower. Moreover, there exists a unique NE for the lead-or-follow game which is $(\mathbf{p^L}, \mathbf{q^F})$, i.e., the attacker side is the leader and the defender side follows.

The obtained NE of the "lead or follow" game seems to be more favorable to the attacker side since it can control the strategy of the follower, the defender side, by being the leader and push the follower to keep silent. However, in fact the defender side also "controls" the attacker side by being the follower: this can be shown by the fact that the leader's strategy and payoff at the unique NE depend uniquely on the parameters of the defender. That is to say, the follower can exert its influence on the leader via its performance parameters, e.g., if $b, C_m \ll a$, both p_i and U_A are very small at the NE.

According to our model, an efficient defender system can not only achieve high detection rate, but also significantly limit the attack probability and consequently limit the harm that the attacker may do on the system. To let multiple defenders monitor one target simultaneously, as discussed in Section IV, is one way to increase the efficiency of the defender system, e.g., the defender side sets x, y such that $U_D = -((b_x^y C_f + C_m)/(2a_x^y + b_x^y C_f) - \epsilon)(1 - C_a) \sum_{i\in\mathcal{T}} W_i$ is maximized.

One issue we would like to mention is that the above analysis is based on the condition that both the attacker and the defender side have sufficient attack and monitor resource. The defender side being the follower ($q_i^F = 0$) does not mean that no defender is needed to maintain the NE. On the contrary, the NE can be viewed as an optimal "agreement" between the two players such that before reaching the "agreement," the players may try different strategies to choose one that maximize their payoff. If, for example, the defender side does not have enough monitor resource, the attacker will not choose the strategy $\mathbf{p^L}$, instead, it may operate on $p_i = 1$ to maximize its payoff. Thus, the sufficiency of resource is the necessary condition of the NE outcome.

B. Intrusion Detection Game With Generalized Attack Model

In this subsection, we generalize our model to consider the scenario where the attacker side may launch various kinds of attacks 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' behavior can we expect and can the previous model be extended in this scenario.

To this end, we define the possible attack set $\Gamma = \{\tau_1, \tau_2, \ldots, \tau_n\}$ 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 $\mathbf{p} = \{p_1, p_2, \ldots, p_N\}$ 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 the previous model. The utility functions are

$$\begin{cases} U_A = \sum_{i\in\mathcal{N}} \sum_{\tau_j\in\Gamma} p_i^j W_i \left(1 - 2a^j q_i - C_a^j\right) \\ U_D = \sum_{i\in\mathcal{N}} \sum_{\tau_j\in\Gamma} q_i W_i \left[p_i^j \left(2a^j + b^j C_f^j\right) - \left(b^j C_f^j + C_m\right)\right] \\ \qquad -p_i^j W_i \end{cases}$$

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 similarly as G in the derivation process of Theorem 2, 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.

Our study is based on the following assumptions:

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 attackers/defenders have no incentive to attack/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 $\max_{j=1,2}(\theta^j - C_a^j)W_i$.

As Assumption 3 in Section IV, Assumption 4 is a simplified scenario in which the attack gain is not cumulative. Following this 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

$$u^j = \begin{cases} \theta^j - 2(a^j)_{x_i}^{y_i} - C_a^j, & \theta^j - C_a^j > 2(a^j)_{x_i}^{y_i} \\ \frac{\theta^j - C_a^j}{2(a^j)_{x_i}^{y_i}}, & \theta^j - C_a^j \leq 2(a^j)_{x_i}^{y_i} \end{cases} \quad (7)$$

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

We can solve the NE of the game by performing similar analysis as that in Section III-B.

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

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

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

where

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

The above results imply that among the possible 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 (7). Moreover, $\Gamma_e^{(x_i,y_i)}$ also depends on the strategy of the defender side (x_i, y_i). 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 $\lceil \theta^j - C_a^j/2(a^j) \rceil$ (where $\tau_j \in \Gamma_e^{(1,1)}$). The lower bound is achieved if $x_i = y_i = 1$ and $\theta^j - C_a^j \leq 2(a^j)$.

TABLE III
NASH EQUILIBRIUM

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

TABLE IV
PAYOFF DEGRADATION DUE TO DEVIATION FROM NE

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

We compare the analysis in this scenario with previous results 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 to 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 Section IV, 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 to this scenario, as shown in the above demonstration.

VII. NUMERICAL STUDY

In this section, we perform a numerical study on two typical scenarios to validate our analytical results.

We first consider a network with a 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 a 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

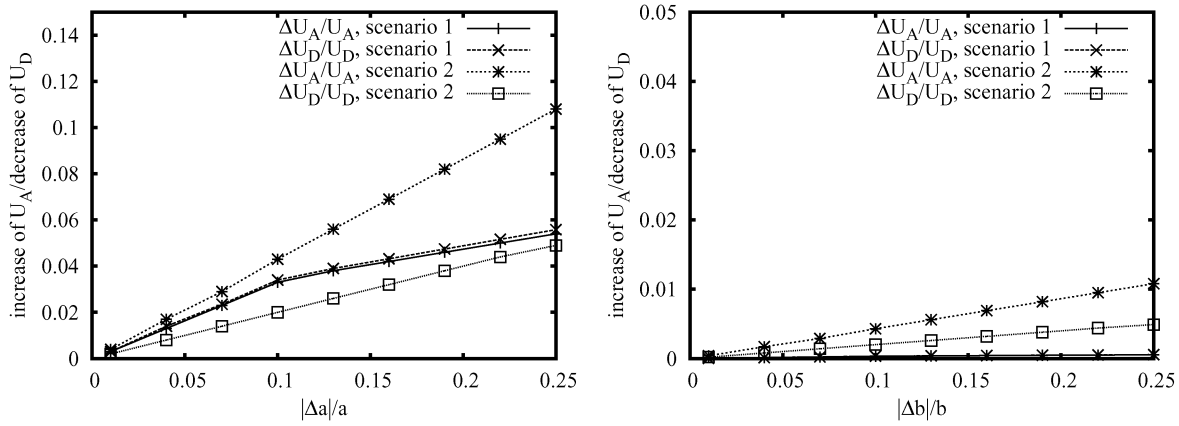

Fig. 1. Sensitivity analysis on the error of a (left) and b (right).

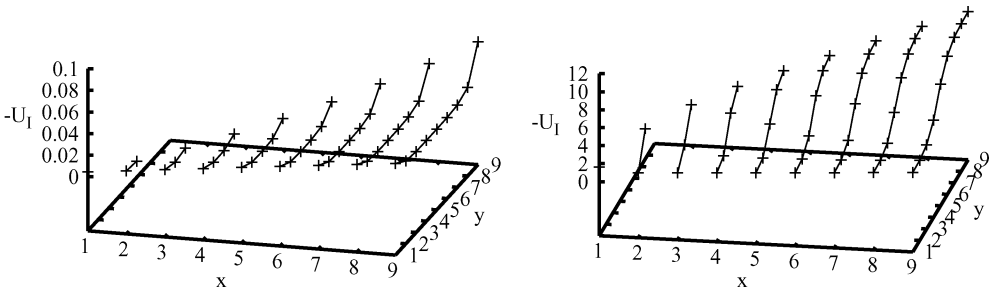

Fig. 2. $-U_D$ as function of x, y. Left: scenario 1; right: scenario 2.

at the airport where both attackers and defenders have limited battery and processing capability. The defender in such cases is usually not so efficient. We thus set $a = 0.4$ and $b = 0.2$. In both scenarios, there are ten targets with normalized security assets: $W_i = (11 - i) * 0.1$ $(i = 1, 2, \ldots, 10)$.

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 III 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 (targets 1–6 for scenario 1 and targets 1–4 for scenario 2).

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_D under the condition that the attacker chooses its strategy to maximize its payoff. Table IV shows the results: $(U_D)_{\max}$ denotes the maximum payoff of the defender with the simulated 300 random strategies, $\overline{U_D}$ denotes the average payoff of the defender, $(U_D^*)_{\min}$ 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.

In practice, the detection rate a and the false alarm rate b usually cannot be accurately measured or estimated. To evaluate the impact of the defender's estimation error of a and b on the utility of players, we conduct a sensitivity analysis. More specifically, we vary the error $|\Delta a|/a$ and $|\Delta b|/b$ and let the defender operate on the NE strategy based on the inaccurate estimation. At the attacker side, it chooses its strategy to maximize U_A. Fig. 1 plots the increase of U_A and the degradation of U_D w.r.t. U_A and U_D without estimation errors as functions of the relative estimation error $(|\Delta a|/a)$ and $(|\Delta b|/b)$ in both scenarios. The results show that the impact on the estimation error of b is negligible. In contrast, the impact of the estimation error of a on the players' payoff varies from 5%–11% when the error reaches 25%. We also observe that over estimating a always leads to more increase (decrease) of U_A (U_D) than under estimating it.

B. Multiple Attackers/Defenders

We then study the case of multiple attackers/defenders and investigate the optimal strategy for the defender side. Fig. 2 plots $-U_D$ at the NE for the studied scenarios with different x, y. Table V shows the optimal strategy for the defender side according to the analytical model.

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

TABLE V
OPTIMAL STRATEGY FOR DEFENDERS

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

TABLE VI
PAYOFF DEGRADATION DUE TO RESOURCE CONSTRAINT

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

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_D 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, respectively) 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 piece of 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. Three hundred 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 one defender at a time; for scenario 2, each target may be monitored by one or two 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 VI shows the payoff degradation due to the lack of sufficient monitor resource.

In Table VI, U_D^1 denotes the payoff of the defender side at the NE, $(U_D^2)_{\max}$ and $\overline{U_D^2}$ denote the maximum and average payoff of the defender side choosing the simulated random strategies. The results show that a 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 VI ($P = 10$) and Table IV ($P = 1$). Therefore, sufficient resource and appropriate configuration at the defender side are two necessary conditions of efficiently protecting the network from being attacked, which confirms the guidelines 3 and 4 in the analytical model.

VIII. RELATED WORK

Intrusion detection has been an active research field for a long time. Most research efforts address the problem of how to improve the performance of IDSs: e.g., increase coverage of attack types, boost detection rate, and keep false alarm rate low, etc. [1]–[3]. In [4], Zhang *et al.* proposed a distributed cooperative IDS, in which a node detecting an intrusion with low confidence can initiate a global intrusion detection procedure through a cooperative detection engine. The local detection engine is built on the rule-based classification algorithm. In a later paper [5], Yi *et al.* extended the previous work on local anomaly detection and conducted a cross-feature analysis to explore the correlations between each feature and other features using a decision-tree-based classification algorithm. An intrusion detection method based on the analysis is proposed for detecting ad hoc routing anomalies. In [11], Subhadrabandhu *et al.* took another line of research by applying theories of hypothesis testing and approximation algorithms to develop a statistical framework for intrusion detection in ad hoc networks.

Recently, several game theoretical approaches have been proposed to model the interaction between the attackers and IDSs. Kodialam *et al.* [6] proposed a game theoretic framework to model the intrusion detection game between the service provider and the intruder. The objective of the 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.* [7] model the intrusion detection as a noncooperative nonzero-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 NE and studied the dynamics of the game. Reference [12] 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. A Bayesian hybrid detection system is proposed based on the analytical results for the defender to strike a balance between its energy costs and monitoring gains. Agah *et al.* [8] and Alpcan *et al.* [9] reconsidered the problem in sensor networks where each player's optimal strategy depends only on the payoff function of the opponent. A two-player noncooperative game is thus formulated between the attacker and the defender (network), and the analysis on the resulting NE leads to a defense strategy for the network. Patcha and Park [10] modeled the interaction between an attacker and an individual node as a noncooperative signaling game where the sender is either of type Attacker or Regular. The receiver with IDS detects the attack with a probability depending on its belief which is updated according to the "message" it has received.

Despite the substantial work on the intrusion detection in the literature, none of them addresses the problem in heterogeneous environments. Motivated by this observation, our work contributes to the existing literature by providing a game theoretical framework of the network intrusion detection problem in heterogeneous environments consisting of targets with different security assets. By characterizing the resulting NE, we further derive the minimum monitor resource requirement and the optimal strategy of the defender side in such environments.

Moreover, existing game theoretical work on the intrusion detection is mainly theoretical work based on highly abstract models. In our work, besides providing the theoretical quantitative framework, we also illustrate the application of the proposed framework in real scenarios via case studies, which is absent in existing work. Our work can thus serve as a building block to guide the design and evaluation of the IDS.

IX. Conclusion

In this paper, we addressed the intrusion detection problem in heterogeneous networks consisting of nodes with different security assets. We formulated the interaction between the attackers and the defenders as a noncooperative game and performed an in-depth analysis on the NE and the engineering implications behind it. 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. We also provided a case study to show how to apply the proposed game theoretical framework to configure the intrusion detection strategies in realistic scenarios.

A natural and interesting research direction is to use the results in this paper as foundations to investigate the dynamic and limited information intrusion detection game. Moreover, the correlation among the security assets of the targets gives the problem a whole new flavor.

Acknowledgment

The authors would like to thank the anonymous reviewers who helped to significantly improve the quality of this paper.

References

[1] C. Manikopoulos and S. Papavassiliou, "Network intrusion and fault detection: A statistical anomaly approach," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 76–82, Oct. 2002.

[2] M. Meneganti, F. S. Saviello, and R. Tagliaferri, "Fuzzy neural networks for classification and detection of anomalies," *IEEE Trans. Neural Netw.*, vol. 9, no. 5, pp. 848–861, Sep. 1998.

[3] W. Lee, S. J. Stolfo, and K. W. Mok, "Adaptive intrusion detection: A data mining approach," *Artif. Intell. Rev.*, vol. 14, no. 6, pp. 533–567, Dec. 2000.

[4] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proc. MobiCom 2003*, pp. 275–283.

[5] Y. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in *Proc. 23th Int. Conf. Distributed Computing Systems (ICDCS)*, Providence, RI, May 2003.

[6] M. Kodialam and T. V. Lakshman, "Detecting network intrusions via sampling: A game theoretic approach," in *IEEE INFOCOM 2003*, San Franciso, CA.

[7] T. Alpcan and T. Basar, "A game theoretic analysis of intrusion detection in access control systems," in *Proc. 43rd IEEE Conf. Decision and Control (CDC)*, Paradise Island, Bahamas, 2004.

[8] A. Agah, S. K. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach," in *Proc. 3rd IEEE Int. Symp. Network Computing and Applications (NCA04)*, Cambridge, MA, Aug./Sep. 2004.

[9] T. Alpcan and T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection," in *Proc. 42nd IEEE Conf. Decision and Control (CDC)*, Hawaii, Dec. 2003.

[10] A. Patcha and J.-M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *Int. J. Netw. Security*, vol. 2, no. 2, pp. 146–152, Mar. 2006.

[11] D. Subhadrabandhu, S. Sarkar, and F. Anjum, "A statistical framework for intrusion detection in ad hoc networks," in *INFOCOM 2006*, Barcelona, Spain.

[12] Y. Liu, C. Comaniciu, and H. Man, "Modelling misbehaviour in ad hoc networks: A game theoretic approach for intrusion detection," *Int. J. Security Netw.*, vol. 1, pp. 243–254, 2006.

[13] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica*, vol. 33, pp. 520–534, 1965.

[14] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA: MIT Press, 1994.

Lin Chen (S'08–M'09) received the B.E. degree in radio engineering from Southeast University, China, in 2002, the Engineer Diploma from Telecom ParisTech, Paris, in 2005, and the M.S. degree in networking from Paris University.

He is currently a postdoctoral research fellow in the Department of Computer Science and Networks, Telecom ParisTech, Paris. His main research interests include security and cooperation enforcement in wireless networks, modeling and control for wireless networks, and game theory.

Jean Leneutre received the Ph.D. degree in computer science from Telecom ParisTech, Paris, in 1998.

He is an Associate Professor with the Department of Computer Science and Networks, Telecom ParisTech (French National School of Telecommunications), CNRS LTCI-UMR 5141 Laboratory. His main research interests include security models and mechanisms for mobile ad hoc networks.