A Game Theoretical Model for Optimal Distribution of Network Security Resources

Ziad Ismail[1](✉), Christophe Kiennert[2], Jean Leneutre[1], and Lin Chen[3]

[1] Télécom ParisTech, Université Paris-Saclay, 46 Rue Barrault, 75013 Paris, France
ismail.ziad@telecom-paristech.fr
[2] Télécom SudParis, 9 Rue Charles Fourier, 91011 Evry, France
[3] University of Paris-Sud 11, 15 Rue Georges Clemenceau, 91400 Orsay, France

Abstract. Enforcing security in a network always comes with a trade-off regarding budget constraints, entailing unavoidable choices for the deployment of security equipment over the network. Therefore, finding the optimal distribution of security resources to protect the network is necessary. In this paper, we focus on Intrusion Detection Systems (IDSs), which are among the main components used to secure networks. However, configuring and deploying IDSs efficiently to optimize attack detection and mitigation remain a challenging task. In particular, in networks providing critical services, optimal IDS deployment depends on the type of interdependencies that exists between vulnerable network equipment. In this paper, we present a game theoretical analysis for optimizing intrusion detection in such networks. First, we present a set of theoretical preliminary results for resource constrained network security games. Then, we formulate the problem of intrusion detection as a resource constrained network security game where interdependencies between equipment vulnerabilities are taken into account. Finally, we validate our model numerically via a real world case study.

Keywords: Intrusion detection · Optimization · Non-cooperative game theory

1 Introduction

As the amount of network communications keeps growing and the complexity of architectures keeps increasing, designing secure networks has become more challenging. One critical aspect of network security is optimizing the distribution of security resources given a constrained defense budget. In addition to firewalls,

This research was initially supported by the MSSTB project, in collaboration with Airbus Defence & Space CyberSecurity and Cogisys, through the Program *Investissement d'Avenir* funded by the French public financial organization *Caisse des Dépôts et des Consignations*, and later by the Cyber CNI Chair of Institut Mines-Télécom held by Télécom Bretagne and supported by Airbus Defence and Space, Amossys, BNP Paribas, EDF, Orange, La Poste, Nokia, Société Générale, and the Regional Council of Brittany, and acknowledged by the Center of Excellence in Cybersecurity.

S. Rass et al. (Eds.): GameSec 2017, LNCS 10575, pp. 234–255, 2017.
DOI: 10.1007/978-3-319-68711-7_13

reverse proxies, or application level countermeasures, Intrusion Detection Systems (IDSs) allow network administrators to substantially refine security management by analyzing data flows dynamically. However, analyzing all the traffic in the network can be complex and costly. Therefore, an optimal IDS deployment strategy to maximize the overall probability of detecting attacks is needed.

In general, based on the data they store, some equipment in a network will be more attractive to attack than others. The interdependencies of equipment vulnerabilities need also to be taken into account. For example, accessing a user workstation is generally not very useful for an attacker unless if it allows him to get access to sensitive equipment more easily. Therefore, it is important to take into account such sequence of attacks in realistic approaches, as the actions of an attacker are not limited to independent atomic attacks.

In addition to classic security approaches, approaches based on game theory were recently used to study and analyze network security problems [1], and more specifically intrusion detection [2]. One of the first game theoretical approaches for intrusion detection was proposed by Alpcan and Basar in [3]. The authors describe and solve a static nonzero-sum imperfect information game where the attacker targets subsystems in the network and the defender tries to optimize the sensitivity of the IDS in each subsystem. This work was later extended in [4] with a zero-sum stochastic game formulation that aims to take into account the uncertainty of attack detection. The authors analyze the equilibria in the case of perfect and imperfect information, and compare the performances of various Q-learning schemes in the case of imperfect information.

Chen and Leneutre [2] consider the intrusion detection problem under budget constraints in a network comprised of independent nodes with different security assets. Nguyen et al. [5] address the same problem, but take into account node interdependencies, both in terms of vulnerabilities and security assets, modeled using linear influence networks [6]. Following the formalism introduced in [7], Nguyen et al. formulate the problem as a two-player zero-sum stochastic game where the states of the game are characterized by the state of each node, either compromised or healthy. Though we also take node interdependencies into account in this paper, formulating the problem as a static game allows us to manipulate more complex utility functions in order to remain as realistic as possible while keeping the solution tractable.

Another approach for the resource allocation problem consists in finding the optimal sampling rate of the IDS on each link in the network under budget constraints. Kodialam and Lakshman in [8] describe the problem as an attacker injecting malicious packets from a fixed entry node and trying to reach a target node without being detected. They formulate the problem as a zero-sum static game, where the attacker aims at choosing the path that minimizes the detection probability over all possible paths from the entry node to the target node. This work was later extended in [9, 10] where the sampling rate problem under budget constraints and in the case of fragmented malicious packets are addressed respectively.

The paper proceeds as follows. In Sect. 2, we present a class of security games which we refer to as Resource Constrained Network Security (RCNS) games. The aim of this section is to present a generic framework that will serve as a basis for the analysis of different types of security games. In Sect. 3, we define our game theoretic model, which is as a subclass of RCNS games, for optimizing the allocation of defense resources in a network, focusing on intrusion detection in which the equipment interdependent vulnerabilities are taken into account. We pay a particular attention to the evaluation of the model parameters, as they are chosen in order to be naturally derived from information security risk assessment methods and correspond to what a chief information security officer would expect to find. We analyze the behavior of the attacker and the defender at the Nash Equilibrium (NE). In Sect. 4, we validate our model numerically via a case study. Finally, we conclude the paper in Sect. 5.

2 Resource Constrained Network Security Games

In this section, we introduce a new class of security games which we will refer to as Resource Constrained Network Security (RCNS) games. Before giving the definition of a RCNS game, we will introduce a number of simple intermediary games. In the remaining of this section, we will refer to a network as a set of interconnected nodes that could also be security-wise interdependent. The nodes can refer to the set of equipment in the network or the set of services running on equipment. Therefore, allocating a set of defense resources on a node refers to the set of defense resources used to monitor the node for any sign of security intrusion. This abstraction of the notion of a network node will allow us to cover a wide spectrum of use cases for applying our formal model.

2.1 Attack/Defense Game

Let $\mathcal{N}$ be a network consisting of $\mathcal{T}$ nodes.

Definition 1 (AD game). *A simple Attack/Defense (AD) game is a static game played on a node i in the network $\mathcal{N}$ between two players: an attacker and a defender. The attacker's actions are restricted to $\{$Attack/Not attack$\}$ while the defender's actions are restricted to $\{$Defend/Not defend$\}$.*

An AD game is a simple game played between the attacker and the defender. It is *restricted* in the sense that the actions of each player are restricted to a single node in the network. The strategic form of a general AD game is given in Table 1.

Assumption 1. In an AD game, we can have $u_i \leq t_i$, $s'_i \leq u'_i$, $r_i - s_i \leq t_i - u_i$, and $r'_i - t'_i \geq s'_i - u'_i$.

Definition 2 (Realistic AD game). *A* realistic *AD game is an AD game satisfying Assumption 1.*

Table 1. Strategic form of the AD game for node i

	Defend	Not defend
Attack	r_i, r'_i	t_i, t'_i
Not attack	s_i, s'_i	u_i, u'_i

We suppose that a realistic AD game satisfies $u_i \leq t_i$ since the attacker will get a higher payoff when attacking a node that is not defended. Similarly, we have $s'_i \leq u'_i$ since the defender is better off defending a node when that node is under attack. Moreover, the difference in payoff for the attacker between the Attack/Not attack actions is higher when the defender chooses not to defend, which translates to $r_i - s_i \leq t_i - u_i$. Similarly, on the defender's side, we have $r'_i - t'_i \geq s'_i - u'_i$. We also note that in general, the attacker's payoffs r_i, s_i, t_i, and u_i are nonnegative real numbers and the defender's payoffs r'_i, s'_i, t'_i, and u'_i are nonpositive real numbers.

Let $(p_i, 1-p_i)$ and $(q_i, 1-q_i)$ be the mixed strategy Nash equilibrium of the attacker and the defender for choosing the actions {Attack/Not attack} and {Defend/Not defend} respectively. Given the strategic form of the game shown in Table 1, the utility function $u^i_A(p_i, q_i)$ of the attacker can be written as $u^i_A(p_i, q_i) = \alpha_i p_i + \sigma_i q_i + \gamma_i p_i q_i + \delta_i$, where $\alpha_i = t_i - u_i$, $\sigma_i = s_i - u_i$, $\gamma_i = r_i - s_i - t_i + u_i$, and $\delta_i = u_i$. Similarly, the utility function $u^i_D(p_i, q_i)$ of the defender can be written as $u^i_D(p_i, q_i) = \alpha'_i p_i + \sigma'_i q_i + \gamma'_i p_i q_i + \delta'_i$, where $\alpha'_i = t'_i - u'_i$, $\sigma'_i = s'_i - u'_i$, $\gamma'_i = r'_i - s'_i - t'_i + u'_i$, and $\delta'_i = u'_i$. We have the following lemma, which follows directly from Assumption 1:

Lemma 1. *In a realistic AD game, we have $\alpha_i \geq 0$, $\gamma_i \leq 0$, $\sigma'_i \leq 0$, and $\gamma'_i \geq 0$.*

2.2 Network Security Game

Let $n = |\mathcal{T}|$ be the number of nodes in the network $\mathcal{N}$. We define a network security game as follows:

Definition 3 (NS game). *A Network Security (NS) game is a game in which the attacker and the defender play n independent AD games on each node of the network $\mathcal{N}$.*

We also refer to a NS game where Assumption 1 holds in each of the n AD games as a *realistic NS game*. The NS game can be as well viewed as a game played between n attackers and n defenders where the attackers and the defenders do not cooperate with each other.

Since a NS game is just a set of AD games played in parallel between the attacker and the defender, the utility of the attacker can be expressed as $U_A(\mathbf{p}, \mathbf{q}) = \sum_{i \in \mathcal{T}} u^i_A(p_i, q_i)$, where $u^i_A(p_i, q_i)$ is the utility the attacker gets from playing the AD game on node i, $\mathbf{p} = (p_1, ..., p_n) \in [0,1]^n$, and

$\mathbf{q} = (q_1, ..., q_n) \in [0,1]^n$. Similarly, the utility of the defender can be expressed as $U_D(\mathbf{p}, \mathbf{q}) = \sum_{i \in \mathcal{T}} u_D^i(p_i, q_i)$.

2.3 Resource Constrained Network Security Game

In a NS game, the choices of actions in the AD game played on node i is independent of any other AD game played on node $j \neq i$. However, in realistic interactions between a defender and an attacker targeting the network, the choice of an action on a node depends on the choices of actions on other nodes as well. For example, given two target nodes, the attacker may assess the success likelihood of his attack and its potential payoff and decide to attack only one of these nodes. In practice, one of the main factors that play a role in the attacker's decision process is the set of attack resources at his disposal. Similarly, a constrained defense budget will influence the defender's allocation of security resources on network nodes. This observation leads us to define the class of resource constrained network security games.

Definition 4 (RCNS game). *A* Resource Constrained Network Security (RCNS) *game is a non-cooperative two player, static, complete information game between an attacker and a defender. The game features a set $\mathcal{T}$ of n targets. Let $\mathbf{p} = (p_1, ..., p_n) \in [0,1]^n$ and $\mathbf{q} = (q_1, ..., q_n) \in [0,1]^n$ be the strategies of the attacker and the defender, where p_i and q_i refer to the attack and defense resources allocated on node i respectively. The game features the resource constraints $\sum_{i \in \mathcal{T}} p_i \leq P \leq 1$ and $\sum_{i \in \mathcal{T}} q_i \leq Q \leq 1$.*

A RCNS game can be seen as a NS game where the allocation of attack and defense resources p_i and q_i on node i refer to the mixed strategy NE of an AD game played on node i. In fact, for the NS game, we have $U_A(\mathbf{p}, \mathbf{q}) = \sum_{i \in \mathcal{T}} u_A^i(p_i, q_i) = \sum_{i \in \mathcal{T}} \alpha_i p_i + \sigma_i q_i + \gamma_i p_i q_i + \delta_i$. Similarly, for the defender, we have $U_D(\mathbf{p}, \mathbf{q}) = \sum_{i \in \mathcal{T}} \alpha'_i p_i + \sigma'_i q_i + \gamma'_i p_i q_i + \delta'_i$. By just looking at the shape of $U_A(\mathbf{p}, \mathbf{q})$ and $U_D(\mathbf{p}, \mathbf{q})$, it is as if we have a game in which the attacker and the defender are trying to find strategies $\mathbf{p} = (p_1, ..., p_n) \in [0,1]^n$ and $\mathbf{q} = (q_1, ..., q_n) \in [0,1]^n$ respectively. This is similar to what we have defined in the RCNS game in Definition 4. However, while p_i and q_i for each node i in the NS game are defined as probabilities, these variables refer to the attack and defense resources allocated on node i in the RCNS game respectively. Therefore, p_i and q_i differ only semantically in these two types of games. In addition, in a RCNS game, we have constraints related to the set of resources available to each player.

Definition 5 (Realistic RCNS game). *A* realistic *RCNS game is a RCNS game where $u_i \leq t_i$, $s'_i \leq u'_i$, $r_i - s_i \leq t_i - u_i$, and $r'_i - t'_i \geq s'_i - u'_i$, $\forall i \in \mathcal{T}$, and there exists at least one $j \in \mathcal{T}$ s.t. $\alpha_j + \gamma_j q_j > 0$, $q_j \in [0,1]$.*

We can notice that the first set of conditions in Definition 5 are similar to the set of conditions in the definition of realistic AD games. In a realistic RCNS game, we assume that there exists at least one target node $j \in \mathcal{T}$ s.t. $\alpha_j + \gamma_j q_j > 0$. Otherwise, by analyzing the utility of the attacker, we can notice that he will not have any incentive to attack any target. Therefore, the conditions defined in a realistic RCNS game ensure that the attacker will *play along* by giving him an incentive to allocate a set of his attack resources to target nodes in the network. We note that in a realistic RCNS game, we have $\alpha_i \geq 0$ and $\gamma_i \leq 0$, $\forall i$.

2.3.1 Nash Equilibrium Analysis

Many network security games, such as [2,11,12], can be formulated as RCNS games. The resource constraints $\sum\limits_{i \in \mathcal{T}} p_i \leq P$ and $\sum\limits_{i \in \mathcal{T}} q_i \leq Q$ represent constraints on players' budgets. In the rest of this section, we present a necessary condition for the existence of a NE in this type of games. In particular, we show that when $\gamma_i < 0$ and $\gamma_i' > 0$, at least the attacker has to use all his resources for a NE to exist.

Theorem 1. *A necessary condition for* $(\mathbf{p}^*, \mathbf{q}^*)$ *to be a Nash equilibrium in a realistic RCNS game where* $\gamma_i < 0$ *and* $\gamma_i' > 0$ *is* $\sum\limits_{i \in \mathcal{T}} p_i^* = P$.

Proof. We consider a realistic RCNS game. We have $\gamma_i \leq 0$ and $\gamma_i' \geq 0$. First, we analyze the case where $\gamma_i = 0$. If $\gamma_i = 0$, then the hypothesis $t_i \geq u_i$ implies $r_i \geq s_i$. In this case, the attacker will always decide to attack node i since the payoff is higher independently from the behavior of the defender. This case being of no interest, we will suppose for the rest of this section that $\gamma_i < 0$. Similarly, we can show that when $\gamma_i' = 0$, the defender always gets a higher payoff by choosing not to defend. In the rest of this section, we suppose $\gamma_i' > 0$.

Let $\mathcal{T}_{S_d}$ be the set of targets on which the defender will allocate defense resources. For example, in a network, the defender monitors a subset of the network nodes to detect intrusions. Similarly, let $\mathcal{T}_{S_a}$ denote the target set that will be attacked by the attacker. In general, we note that $\mathcal{T}_{S_d} \cap \mathcal{T}_{S_a} \neq \varnothing$.

The conditions for the existence of a NE vary according to the hypothesis made on $\sum\limits_{i \in \mathcal{T}} p_i$ and $\sum\limits_{i \in \mathcal{T}} q_i$. In the general case where $\sum\limits_{i \in \mathcal{T}} p_i \leq P$ and $\sum\limits_{i \in \mathcal{T}} q_i \leq Q$, if a NE ($\mathbf{p}^*$, $\mathbf{q}^*$) exists, $\mathbf{p}^*$ is a best response strategy to the defender strategy and $\mathbf{q}^*$ is a best response strategy to the attacker strategy. Since the utility of the attacker is linear with respect to the attacker's strategy $\mathbf{p}$, if a solution to the attacker's optimization problem exists, then an optimal solution at an extreme point of the feasible set defined by $\sum\limits_{i \in \mathcal{T}} p_i \leq P$ exists (when $\sum\limits_{i \in \mathcal{T}} p_i = P$). A similar analysis can be conducted for the case of the defender.

Case 1: $\sum\limits_{i \in \mathcal{T}} p_i = P$ and $\sum\limits_{i \in \mathcal{T}} q_i = Q$

From the definitions of $\mathcal{T}_{S_a}$ and $\mathcal{T}_{S_d}$, the constraints on the attack and defense resources become $\sum\limits_{i \in \mathcal{T}_{S_a}} p_i = P$ and $\sum\limits_{i \in \mathcal{T}_{S_d}} q_i = Q$. From the Karush-Kuhn-Tucker (KKT) conditions, there exists $\lambda > 0$ s.t. $\dfrac{\partial U_A}{\partial p_i} = \lambda$ and $\lambda' > 0$ s.t.

$\frac{\partial U_D}{\partial q_i} = \lambda'$. We have $\frac{\partial U_A}{\partial p_i} = \alpha_i + \gamma_i q_i$. Therefore, $\alpha_i + \gamma_i q_i > 0 \Rightarrow q_i < -\frac{\alpha_i}{\gamma_i} \Rightarrow Q < \sum\limits_{i\,\in\,\mathcal{T}_{S_d}} \frac{-\alpha_i}{\gamma_i}$. Since $\alpha_i \geq 0$ and $\gamma_i < 0$, we have $\sum\limits_{i\,\in\,\mathcal{T}_{S_d}} \frac{-\alpha_i}{\gamma_i} \geq 0$. Similarly, considering $\frac{\partial U_D}{\partial q_i} = \sigma_i' + \gamma_i' p_i$, we have $P > \sum\limits_{i\,\in\,\mathcal{T}_{S_a}} \frac{-\sigma_i'}{\gamma_i'}$. Since $\sigma_i' \leq 0$ and $\gamma_i' > 0$, we have $\sum\limits_{i\,\in\,\mathcal{T}_{S_a}} \frac{-\sigma_i'}{\gamma_i'} \geq 0$. We have already established that if a NE solution exists, it must exist at least when $\sum\limits_{i\,\in\,\mathcal{T}} p_i = P$ and $\sum\limits_{i\,\in\,\mathcal{T}} q_i = Q$. Therefore, from the results above, the necessary conditions for the existence of a NE are $Q < \sum\limits_{i\,\in\,\mathcal{T}_{S_d}} \frac{-\alpha_i}{\gamma_i}$ and $P > \sum\limits_{i\,\in\,\mathcal{T}_{S_a}} \frac{-\sigma_i'}{\gamma_i'}$.

Case 2: $\sum\limits_{i\,\in\,\mathcal{T}} p_i = P$ and $\sum\limits_{i\,\in\,\mathcal{T}} q_i < Q$

Similarly to Case 1, we can verify that the conditions for the existence of a NE are $Q < \sum\limits_{i\,\in\,\mathcal{T}_{S_d}} \frac{-\alpha_i}{\gamma_i}$ and $P = \sum\limits_{i\,\in\,\mathcal{T}, \mathcal{T} \neq \mathcal{T}_{S_a}} \frac{-\sigma_i'}{\gamma_i'}$.

Case 3: $\sum\limits_{i\,\in\,\mathcal{T}} p_i < P$ and $\sum\limits_{i\,\in\,\mathcal{T}} q_i \leq Q$

We have $\frac{\partial U_A}{\partial p_i} = 0$. Therefore, $q_i = -\frac{\alpha_i}{\gamma_i} \Rightarrow \sum\limits_{i\,\in\,\mathcal{T}} q_i = -\sum\limits_{i\,\in\,\mathcal{T}} \frac{\alpha_i}{\gamma_i}$. However, from the first case, we have $Q < \sum\limits_{i\,\in\,\mathcal{T}_{S_d}} \frac{-\alpha_i}{\gamma_i} \leq \sum\limits_{i\,\in\,\mathcal{T}} \frac{-\alpha_i}{\gamma_i} = \sum\limits_{i\,\in\,\mathcal{T}} q_i$. Therefore, $Q < \sum\limits_{i\,\in\,\mathcal{T}} q_i$ which contradicts the fact that $\sum\limits_{i\,\in\,\mathcal{T}} q_i \leq Q$. As a result, the scenario in which $\sum\limits_{i\,\in\,\mathcal{T}} q_i \leq Q$ and $\sum\limits_{i\,\in\,\mathcal{T}} p_i < P$ does not admit a NE. □

Table 2 exhibits the possible scenarios for the existence of a NE with respect to the assumptions about the resources of the attacker and the defender. In particular, given the conditions that P and Q must satisfy, a NE cannot be found when $\sum\limits_{i\,\in\,\mathcal{T}} q_i < Q$ and $\sum\limits_{i\,\in\,\mathcal{T}} p_i < P$.

Table 2. Conditions for the existence of the NE in a realistic RCNS game

	Conditions
$\sum\limits_{i\,\in\,\mathcal{T}} q_i = Q$, $\sum\limits_{i\,\in\,\mathcal{T}} p_i = P$	$Q < \sum\limits_{i\,\in\,\mathcal{T}_{S_d}} \frac{-\alpha_i}{\gamma_i}$, $P > \sum\limits_{i\,\in\,\mathcal{T}_{S_a}} \frac{-\sigma_i'}{\gamma_i'}$
$\sum\limits_{i\,\in\,\mathcal{T}} q_i < Q$, $\sum\limits_{i\,\in\,\mathcal{T}} p_i = P$	$Q < \sum\limits_{i\,\in\,\mathcal{T}_{S_d}} \frac{-\alpha_i}{\gamma_i}$, $P = \sum\limits_{i\,\in\,\mathcal{T}, \mathcal{T} \neq \mathcal{T}_{S_a}} \frac{-\sigma_i'}{\gamma_i'}$
$\sum\limits_{i\,\in\,\mathcal{T}} q_i \leq Q$, $\sum\limits_{i\,\in\,\mathcal{T}} p_i < P$	Impossible

2.3.2 Stackelberg Equilibrium Analysis

In a Stackelberg game, a leader chooses his strategy first. Then, the follower, informed by the leader's choice, chooses his strategy. In this section, we analyze the scenario where the defender is the leader and the follower is the attacker. In this case, the defender tries to anticipate the attacker's strategy and chooses a strategy that minimizes the potential impact of attacks on the system.

Stackelberg games are generally solved by backward induction and the solution is known as Stackelberg Equilibrium (SE). We start by computing the best response strategy of the follower as a function of the leader's strategy. Then, according to the follower's best response, we compute the best strategy of the leader.

The attacker solves the following optimization problem:

$$\mathbf{p}(\mathbf{q}) = \underset{\mathbf{p}\,\in\,[0,1]^n}{\text{argmax}}\, U_A(\mathbf{p},\mathbf{q})\; s.t. \sum_{i\,\in\,\mathcal{T}} p_i \leq P$$

On the other hand, the defender solves the following optimization problem:

$$\mathbf{q}(\mathbf{p}) = \underset{\mathbf{q}\,\in\,[0,1]^n}{\text{argmax}}\, U_D(\mathbf{p}(\mathbf{q}),\mathbf{q})\; s.t. \sum_{i\,\in\,\mathcal{T}} q_i \leq Q$$

Assumption 2. The attacker's resource allocation strategy on a node i depends only on the defender's strategy on that node.

As a result of Assumption 2, we have $p_i(\mathbf{q}) = p_i(q_i)\ \forall i \in \mathcal{T}$. In the rest of this section, we suppose that Assumption 2 holds. In what follows, we present necessary conditions for the existence of a Stackelberg equilibrium in a realistic RCNS game. In particular, we have the following theorem:

Theorem 2. *In a realistic RCNS game, the necessary conditions for the existence of a Stackelberg equilibrium are as follows,* $\forall i \in \mathcal{T}$*:*
If $\alpha'_i = \gamma'_i = 0$*,* $\forall j \in \mathcal{T}$ *s.t.* $\gamma'_j = \alpha'_j = 0$*, we have* $\sigma'_i = \sigma'_j$*. Otherwise, if* $\alpha'_i \neq 0$ *or* $\gamma'_i \neq 0$*,* $\exists \tau' \geq 0$ *s.t. the strategy of the attacker* p_i *have the following form:*

$$p_i = p_i^0 \left| \frac{\alpha'_i}{\alpha'_i + \gamma'_i q_i} \right| + \frac{\tau' - \sigma'_i}{\alpha'_i + \gamma'_i q_i}\Big(q_i + D_i\Big)$$

$$\textit{where } p_i^0 = p_i(0) \textit{ and } D_i = \begin{cases} 0 & \textit{if } \gamma'_i = 0, \alpha'_i \neq 0 \\ 0 & \textit{if } \gamma'_i > 0, \alpha'_i \geq 0, q_i \neq \dfrac{-\alpha'_i}{\gamma'_i} \\ 0 & \textit{if } \gamma'_i > 0, \alpha'_i \leq 0, q_i \in \Big[0, \min\Big(\dfrac{-\alpha'_i}{\gamma'_i}, Q\Big)\Big[\\ \dfrac{2\alpha'_i}{\gamma'_i} & \textit{if}\gamma'_i > 0, \alpha'_i \leq 0, q_i \in \Big]\min\Big(\dfrac{-\alpha'_i}{\gamma'_i}, Q\Big), Q\Big] \end{cases}$$

Proof. Let $\mathbf{p}(\mathbf{q})$ be the strategy of the attacker. Next, we establish the conditions that $\mathbf{p}(\mathbf{q})$ must satisfy for a Stackelberg equilibrium for the RCNS game to exist in the presence of constraints on the attack and defense budgets.

From Assumption 2, we have $p_i(\mathbf{q}) = p_i(q_i)\ \forall i \in \mathcal{T}$. The utility of the defender is therefore given by:

$$U_D(\mathbf{p}(\mathbf{q}), \mathbf{q}) = \sum_{i \in \mathcal{T}} \alpha'_i p_i(q_i) + \sigma'_i q_i + \gamma'_i p_i(q_i) q_i + \delta'_i$$

We have the following constraint $\sum\limits_{i \in \mathcal{T}} q_i \leq Q$. From the KKT conditions, there exists $\tau' \geq 0$ s.t. $\frac{\partial U_D}{\partial q_i} = \tau'$. Therefore, we have $\frac{\partial p_i}{\partial q_i}(\alpha'_i + \gamma'_i q_i) + \gamma'_i p_i + \sigma'_i = \tau'$.

Let $p_i(0) = p_i^0$.

Case 1: $\gamma'_i = 0$ and $\alpha'_i = 0$

In this case, $\tau' = \sigma'_i$. However, if there are two nodes i and j in which $\gamma'_i = \alpha'_i = 0$, $\gamma'_j = \alpha'_j = 0$ and $\sigma'_i \neq \sigma'_j$, then a Stackelberg equilibrium does not exist.

Case 2: $\gamma'_i = 0$ and $\alpha'_i \neq 0$

In this case, we have $\frac{\partial p_i}{\partial q_i} = \frac{\tau' - \sigma'_i}{\alpha'_i} \Rightarrow p_i = \frac{\tau' - \sigma'_i}{\alpha'_i} q_i + p_i^0$

Case 3: $\gamma'_i > 0$ and $q_i \neq \frac{-\alpha'_i}{\gamma'_i}$

In this case, we have $\frac{\partial p_i}{\partial q_i} + \frac{\gamma'_i}{\alpha'_i + \gamma'_i q_i} p_i = \frac{\tau' - \sigma'_i}{\alpha'_i + \gamma'_i q_i}$. This first order differential equation has a unique solution s.t. $p_i(0) = p_i^0$ and is given by:

$$p_i = p_i^0 e^{F(0) - F(q_i)} + \int_0^{q_i} \frac{\tau' - \sigma'_i}{\alpha'_i + \gamma'_i x} e^{F(x) - F(q_i)} dx$$

where $F(x) = \int \frac{\gamma'_i}{\alpha'_i + \gamma'_i t} dt = \log(|\alpha'_i + \gamma'_i x|)$.

Therefore, $p_i^0 e^{F(0) - F(q_i)} = p_i^0 \left| \frac{\alpha'_i}{\alpha'_i + \gamma'_i q_i} \right|$ and $\int_0^{q_i} \frac{\tau' - \sigma'_i}{\alpha'_i + \gamma'_i x} e^{F(x) - F(q_i)} dx = \int_0^{q_i} \frac{\tau' - \sigma'_i}{\alpha'_i + \gamma'_i x} \left| \frac{\alpha'_i + \gamma'_i x}{\alpha'_i + \gamma'_i q_i} \right| dx$

Case 3.1: $\alpha'_i \geq 0$

In this case, we have $\int_0^{q_i} \frac{\tau' - \sigma'_i}{\alpha'_i + \gamma'_i x} \left(\frac{\alpha'_i + \gamma'_i x}{\alpha'_i + \gamma'_i q_i} \right) dx = \frac{\tau - \sigma'_i}{\alpha'_i + \gamma'_i q_i} q_i$

Case 3.2: $q_i \in \left[0, \min\left(\frac{-\alpha'_i}{\gamma'_i}, Q\right)\right[$ and $\alpha'_i \leq 0$

Similar to Case 3.1.

Case 3.3: $q_i \in \left] \min\left(\frac{-\alpha'_i}{\gamma'_i}, Q\right), Q\right]$ and $\alpha'_i \leq 0$

In this case, we have:

$$\int_0^{q_i} \frac{\tau'-\sigma'_i}{\alpha'_i+\gamma'_i x}.\frac{|\alpha'_i+\gamma'_i x|}{\alpha'_i+\gamma'_i q_i}dx = \int_0^{\frac{-\alpha'_i}{\gamma'_i}} \frac{\tau'-\sigma'_i}{\alpha'_i+\gamma'_i x}.\frac{(-\alpha'_i-\gamma'_i x)}{\alpha'_i+\gamma'_i q_i}dx + \int_{\frac{-\alpha'_i}{\gamma'_i}}^{q_i} \frac{\tau'-\sigma'_i}{\alpha'_i+\gamma'_i x}.\frac{(\alpha'_i+\gamma'_i x)}{\alpha'_i+\gamma'_i q_i}dx = \frac{\tau-\sigma'_i}{\alpha'_i+\gamma'_i q_i}\left(q_i+2\frac{\alpha'_i}{\gamma'_i}\right)$$

Combining the 3 cases completes the proof. □

Theorem 3. *$\forall i \in \mathcal{T}$ s.t. $\alpha'_i \neq 0$ and $\gamma'_i = 0$. If the conditions in Theorem 2 are satisfied, a necessary condition for the uniqueness of the players' strategies on node i at the Stackelberg equilibrium is that $\exists \tau \geq 0$ s.t.:*

$$\begin{cases} \Gamma(\alpha'_i)\big((\alpha_i-\tau)(\tau'-\sigma'_i)-\alpha'_i(\gamma_i p_i^0-\sigma_i)\big) \leq 0 \\ \Gamma(\alpha'_i)\alpha'_i\gamma_i(\tau'-\sigma'_i) > 0 \end{cases}$$

where $\Gamma : \mathbb{R} \to \{1,-1\}$ s.t. $\Gamma(x) = 1$ if $x > 0$ and -1 otherwise.

Proof. The utility function of the attacker is given by: $U_A(\mathbf{p},\mathbf{q}) = \sum_{i \in \mathcal{T}} \alpha_i p_i + \sigma_i q_i + \gamma_i p_i q_i + \delta_i$. To find the Stackelberg equilibrium, the attacker solves the following maximization problem:

$$\mathbf{p}(\mathbf{q}) = \underset{\mathbf{p} \in [0,1]^{N_c}}{\operatorname{argmax}} U_A(\mathbf{p},\mathbf{q})\, s.t. \sum_{i \in \mathcal{T}} p_i \leq P$$

Let $\Gamma : \mathbb{R} \to \{1,-1\}$ s.t. $\Gamma(x) = 1$ if $x > 0$ and -1 otherwise.

Case 1: $\gamma'_i = 0, \alpha'_i \neq 0$

From Theorem 2, we know that a necessary condition for the existence of a Stackelberg equilibrium is that $\exists \tau' \geq 0$ s.t. $p_i = p_i^0 + \frac{\tau'-\sigma'_i}{\alpha'_i}q_i$.

Case 1.1: $\tau' = \sigma'_i$

In this case, the attacker's strategy p_i on node i is independent from the defender strategy q_i. Therefore, the strategy of the defender on node i has no influence on the attacker's strategy on that node. In this case, we may have an unlimited number of Stackelberg equilibriums. We note that if $\forall i \in \mathcal{T}$, $\tau' = \sigma'_i$, the study of this type of games is not interesting.

Case 1.2: $\tau' \neq \sigma'_i$

In this case, we have $q_i = \frac{\alpha'_i(p_i-p_i^0)}{\tau'-\sigma'_i}$. From the KKT conditions, there exists $\tau \geq 0$ s.t. $\frac{\partial U_A}{\partial p_i} = \tau$. Therefore, we have $2p_i\alpha'_i\gamma_i(\tau'-\sigma'_i)+(\tau'-\sigma'_i)\big((\alpha_i-\tau)(\tau'-\sigma'_i)-\alpha'_i\gamma_i p_i^0+\alpha'_i\sigma_i\big) = 0$. We have $p_i \in [0,1]$ $\forall i \in \mathcal{T}$. Therefore, a necessary condition for the existence of a unique strategy on node i at the Stackelberg equilibrium in this case is that $\Gamma(\alpha'_i)\big((\alpha_i-\tau)(\tau'-\sigma'_i)-\alpha'_i(\gamma_i p_i^0-\sigma_i)\big) \leq 0$ and $\Gamma(\alpha'_i)\alpha'_i\gamma_i(\tau'-\sigma'_i) > 0$. □

Theorem 4. *$\forall i \in \mathcal{T}$ s.t. $\gamma'_i > 0$ and $\alpha'_i \neq 0$, there exists at most two possible couple of strategies $(\mathbf{p_i^*}, \mathbf{q_i^*})$ and $(\mathbf{p_i^\dagger}, \mathbf{q_i^\dagger})$ at the Stackelberg equilibrium on each node i.*

Proof. There are 3 possible cases to analyze.

Case 1: $\gamma'_i > 0$, $\alpha'_i \geq 0$, $q_i \neq \dfrac{-\alpha'_i}{\gamma'_i}$, and $p_i \neq \dfrac{\tau' - \sigma'_i}{\gamma'_i}$

In this case, we have $p_i = \dfrac{\alpha'_i p_i^0}{\alpha'_i + \gamma'_i q_i} + \dfrac{(\tau' - \sigma'_i) q_i}{\alpha'_i + \gamma'_i q_i}$. We have a constraint on the attack budget $\sum\limits_{i \in \mathcal{T}} p_i \leq P$. Therefore, from the KKT conditions, $\exists \tau \geq 0$ s.t. $\dfrac{\partial U_A}{\partial p_i} = \tau$. Therefore, we have:

$$\alpha_i + \alpha'_i \gamma_i \left(\frac{p_i^0 - p_i}{\gamma'_i p_i - (\tau' - \sigma'_i)} \right) + (\sigma_i + \gamma_i p_i) \left(\frac{\alpha'_i(\tau' - \sigma'_i) - \alpha'_i \gamma'_i p_i^0}{\left(\gamma'_i p_i - (\tau' - \sigma'_i)\right)^2} \right) = \tau$$

which can be written as $A_i p_i^2 + B_i p_i + C_i = 0$ where $A_i = \gamma_i^{2'}(\alpha_i - \tau) - \alpha'_i \gamma'_i \gamma_i$, $B_i = 2(\tau' - \sigma'_i)(\alpha'_i \gamma_i - \gamma'_i(\alpha_i - \tau))$, and $C_i = (\tau' - \sigma'_i)\big((\alpha_i - \tau)(\tau' - \sigma'_i) - \alpha'_i \gamma_i p_i^0 + \alpha'_i \sigma_i\big) - \alpha'_i \gamma'_i \sigma_i p_i^0$. This quadratic equation has at most 2 solutions, which concludes the proof for this case.

Case 2: $\gamma'_i > 0, \alpha'_i \leq 0, q_i \in \left[0, \min\left(\dfrac{-\alpha'_i}{\gamma'_i}, Q\right)\right[$, and $p_i \neq \dfrac{\tau' - \sigma'_i}{\gamma'_i}$

Similar to Case 2.

Case 3: $\gamma'_i > 0, \alpha'_i \leq 0, q_i \in \left]\min\left(\dfrac{-\alpha'_i}{\gamma'_i}, Q\right), Q\right]$, and $p_i \neq \dfrac{\tau' - \sigma'_i}{\gamma'_i}$

Similary to Case 1, from the partial derivative of U_A w.r.t. p_i, we can find that the strategy of the attacker is the solution of the quadratic equation $A_i p_i^2 + B_i p_i + C'_i = 0$ where $C'_i = (\tau' - \sigma'_i)\big((\alpha_i - \tau)(\tau' - \sigma'_i) - \alpha'_i \gamma_i p_i^0 - \gamma_i(\tau' - \sigma'_i)\dfrac{2\alpha'_i}{\gamma'_i} - \alpha'_i \sigma_i\big) - \alpha'_i \gamma'_i \sigma_i p_i^0$. □

Lemma 2. *A realistic RCNS game can have an infinite number of Stackelberg equilibriums if $\exists i \in \mathcal{T}$ s.t. $\gamma'_i = 0, \alpha'_i \neq 0$, and $\tau' = \sigma'_i$. Otherwise, a realistic RCNS game can have at most 2^n Stackelberg equilibriums.*

Lemma 2 follows directly from Theorems 3 and 4.

2.3.3 Maximin Strategy

In this section, we will be interested in analyzing the *maximin* strategy of the attacker. For space limitations, we will omit the analysis of the *maximin* strategy of the defender, which can be analyzed similarly.

A player's *maximin* strategy is a strategy in which he tries to maximize the worst payoff he can get for any strategy played by the other player. The attacker's *maximin* strategy is therefore given by $\mathbf{p} = \operatorname*{argmax}_{\mathbf{p'}} \min_{\mathbf{q}} U_A(\mathbf{p'}, \mathbf{q})$.

We will study the attacker's *maximin* strategy under different constraints on the attacker's and defender's budgets $\sum_{i\in\mathcal{T}} p_i$ and $\sum_{i\in\mathcal{T}} q_i$ respectively.

Theorem 5. *For each strategy of the attacker, there exists a sensible target set $\mathcal{R}_D$ that will be of interest to the defender.*

Proof. For a given attacker strategy $\mathbf{p}$, the defender tries to compute $\min_{\mathbf{q}} U_A(\mathbf{p},\mathbf{q}) = \min_{\mathbf{q}} \big(\sum_{i\in\mathcal{T}} \alpha_i p_i + \delta_i + q_i(\sigma_i + \gamma_i p_i)\big)$. In the case of unconstrained defense budget, there exists a sensible target set $\mathcal{R}_D$ where $\forall i \in \mathcal{R}_D$, we have $q_i = 1$ and $\sigma_i + \gamma_i p_i < 0$, and $\forall j \in \mathcal{T}\backslash\mathcal{R}_D$, we have $q_j = 0$ and $\sigma_j + \gamma_j p_j \geq 0$. In case of constrained defense budget $\sum_{i\in\mathcal{T}} q_i = Q$, the sensible target set $\mathcal{R}_D$ is defined s.t. $\forall\{i,k\} \in \mathcal{R}_D$, $\sigma_i + \gamma_i p_i = \sigma_k + \gamma_k p_k$ and $i = \underset{j\in\mathcal{T}}{\operatorname{argmin}}(\sigma_j + \gamma_j p_j)$. □

Theorem 6. *In the case of unconstrained defense budget, for a given sensible target set $\mathcal{R}_D$, there exists either 1 or an infinite* maximin *strategies for the attacker.*

Proof. Let ζ be the set of targets i s.t. $\alpha_i + \gamma_i = 0$. Let $\mathbb{1}_{expr} = 1$ if *expr* is true and 0 otherwise. In the case of unconstrained attacker budget, if $\zeta = \varnothing$, there exists a unique attacker *maximin* strategy where the attack resource on node i is determined by analyzing $r_i - t_i$ and σ_i. This can be found easily by analyzing the attacker's payoff $\alpha_i p_i + \delta_i + (\sigma_i + \gamma_i p_i) q_i$ on each target i. Otherwise, if $\zeta \neq \varnothing$, there exists an infinite number of attacker *maximin* strategies yielding at least a payoff of $\sum_{j\in\zeta} \delta_j + \sigma_j \mathbb{1}_{\sigma_j<0}$ for targets in ζ. □

In the rest of this section, we will analyze the attacker's *maximin* strategy in the presence of constraints on the defender's budget.

Let S be a large positive number. By analyzing the attacker's utility function $U_A(\mathbf{p},\mathbf{q})$, we have the following lemma:

Lemma 3. *If $\sum_{i\in\mathcal{T}} q_i = Q$ and in the absence of constraints on the attacker's budget, finding a* maximin *strategy for the attacker is equivalent to solving the following Mixed Integer Quadratic Program (MIQP):*

$$\begin{aligned}
\max_{\mathbf{p},\mathbf{q},\mathbf{y},b}\ & U_A(\mathbf{p},\mathbf{q}) \\
s.t.\quad & (y_i - 1)S \leq b - \sigma_i - \gamma_i p_i \leq 0 \\
& q_i \leq y_i S \\
& \sum_{i\in\mathcal{T}} q_i = Q \\
& y_i \in \{0,1\},\ p_i \in [0,1],\ q_i \in [0,Q],\ b \in \mathbb{R}
\end{aligned}$$

Lemma 4. *In the presence of constraints on the defender budget $\sum_{i\in\mathcal{T}} q_i = Q$, for any sensible target set $\mathcal{R}_D$, assuming that the defender will focus on defending only one target in $\mathcal{R}_D$ will not change the impact of the defender's strategy on the* maximin *strategy of the attacker.*

Proof. If $\sum_{i \in \mathcal{T}} q_i = Q$, the defender will allocate his resources on the set of target i with the lowest $\sigma_i + \gamma_i p_i$. In addition, we have $\sigma_j + \gamma_j p_j = \sigma_m + \gamma_m p_m$, $\forall \{j, m\} \in \mathcal{R}_D$. By analyzing the attacker's utility function, we can notice that instead of setting $q_j \neq 0 \; \forall j \in \mathcal{R}_D$, the attacker can pick $m \in \mathcal{R}_D$ and set $q_m = Q$ without that changing the attacker's payoff. □

Lemma 5. *In the presence of constraints on the attacker and defender budgets (resp.* $\sum_{i \in \mathcal{T}} p_i = P$ *and* $\sum_{i \in \mathcal{T}} q_i = Q$*), finding a* maximin *strategy for the attacker is equivalent to solving the following Mixed Integer Linear Program (MILP):*

$$\begin{aligned}
\max_{\mathbf{y},\mathbf{x},b} \; & \sum_{i \in \mathcal{T}} \Big(\alpha_i \sum_{j \in \mathcal{T}} x_{ji} + \delta_i + (\sigma_i y_i + \gamma_i x_{ii})Q\Big) \\
s.t. \;\; & (y_i - 1)S \leq b - \sigma_i - \gamma_i \sum_{j \in \mathcal{T}} x_{ji} \leq 0 \\
& \sum_{i \in \mathcal{T}} y_i = 1 \\
& y_i P \leq \sum_{j \in \mathcal{T}} x_{ij} \leq P \\
& \sum_{i \in \mathcal{T}} x_{ij} \leq P \\
& \sum_{i \in \mathcal{T}} \sum_{j \in \mathcal{T}} x_{ij} = P \\
& y_i \in \{0, 1\}, \; x_{ij} \in [0, P], \; b \in \mathbb{R}
\end{aligned}$$

Proof. From Lemma 4, we can assume that the defender will defend 1 target with a resource Q. Let $y_i \in \{0, 1\} \; \forall i \in \mathcal{T}$. The *maximin* strategy of the attacker can then be found by maximizing $\sum_{i \in \mathcal{T}} \alpha_i p_i + \delta_i + (\sigma_i + \gamma_i p_i) y_i Q$ w.r.t. $\mathbf{p}$, $\mathbf{y}$, and b s.t. $(y_i - 1)S \leq b - \sigma_i - \gamma_i p_i \leq 0$, $\sum_{i \in \mathcal{T}} y_i = 1$, $\sum_{i \in \mathcal{T}} p_i = P$, and $b \in \mathbb{R}$. We can linearize this Mixed Integer Quadratic Program through the change of variables $x_{ij} = y_i p_j \; \forall \{i, j\} \in \mathcal{T}$. □

3 Intrusion Detection Game

3.1 Game Model and Parameters

In this section, we introduce an intrusion detection game, which is a specific case of a RCNS game. We consider a heterogeneous network comprised of n interdependent equipment referred to as nodes in the remaining of this paper. The network can be represented as a weighted directed graph $\mathcal{G} = (\mathcal{T}, \mathcal{E}, \Theta)$, where $\mathcal{T} = \{1, ..., n\}$ is the set of network nodes, and $\mathcal{E}$ is a particular subset of $\mathcal{T}^2$ and referred to as the edges of $\mathcal{G}$. In particular, an edge (i, j) exists between node i and node j if compromising node i makes it easier for the attacker to compromise node j. Finally, a weight $\theta_i^j \in \Theta$, $\theta_i^j \in]0, 1]$, is associated to each edge $(i, j) \in \mathcal{E}$, quantifying the vulnerability dependency from node i to node j.

We model the intrusion detection problem as a non-cooperative static game with two players, an attacker and a defender. We assume that both players are rational. The objective of the attacker is to compromise targets in the network without being detected, whereas the defender's objective is to distribute monitoring resources on network nodes in order to detect attacks. For each node $i \in \mathcal{T}$, the attacker and the defender actions are limited to *Attack/Not Attack* and *Monitor/Not Monitor* respectively. The attacker's strategy is represented by a vector $\mathbf{p} = (p_1, ..., p_n) \in [0,1]^n$, where p_i is the probability of targeting node i. Similarly, the defender's strategy is represented by a vector $\mathbf{q} = (q_1, ..., q_n) \in [0,1]^n$, where q_i is the probability of monitoring node i. The resource constraints on the attacker and the defender budgets are P and Q respectively. Therefore, we have $\sum\limits_{i=1}^{n} p_i \leq P$ and $\sum\limits_{i=1}^{n} q_i \leq Q$, where $P \leq 1$ and $Q \leq 1$.

We associate to each node $i \in \mathcal{T}$ the following parameters:

- The security asset $W_i \geq 0$ representing the importance of services provided by node i to the network. Security assets are assumed to be independent, since the existing correlations between security assets may have already been taken into account through a formal risk analysis evaluation process.
- The intrinsic vulnerability $V_i^0 \in [0,1]$ quantifying local vulnerabilities of services on node i.
- The detection probability $a_i \in [0,1]$ representing the probability of detecting an attack on node i considering the current configuration of the defense system.

We assume that the costs of attacking and monitoring a node $i \in \mathcal{T}$ are proportional to the security asset W_i. In addition, these costs are affected by the intrinsic vulnerability V_i^0 on node i. In particular, the cost of attacking node i is inversely proportional to V_i^0, while the cost of monitoring node i is proportional to V_i^0. Therefore, the costs to attack and monitor node i are given by $C_a(1-V_i^0)W_i$ and $C_m V_i^0 W_i$ respectively, where C_a and $C_m \in [0,1]$. Let $C_a^i = C_a(1-V_i^0)$ and $C_m^i = C_m V_i^0$. Finally, we introduce a dependency parameter $\beta \in [0,1]$. β is used to assess the impact of interdependencies between network nodes in the utilities of the attacker and the defender. For example, $\beta = 0$ is equivalent to the case where interdependencies between network nodes are not taken into account in the model.

3.2 Utility Functions

Let $\Gamma^-(i)$ and $\Gamma^+(i)$ refer to the set of predecessors and the set of successors of node i in the network graph $\mathcal{G}$ respectively. The effect of interdependencies on node i is defined as $\Delta_i = \beta \sum\limits_{j \in \Gamma^-(i)} \theta_j^i W_j p_j (1 - a_j q_j)$. Δ_i is the sum of the effect of interdependencies on node i from all its predecessors j that have been attacked (hence the p_j factor) without being detected (hence the $(1 - a_j q_j)$ factor) while taking into account the vulnerability dependency $\theta_j^i \in]0,1]$ from node j to i.

Table 3 presents the payoff matrix for both players in strategic form for a node $i \in \mathcal{T}$. A successful (i.e. undetected) attack on node i, which happens with probability $1 - a_i$, gives the attacker and the defender the payoffs $W_i(1 - a_i)$ and

Table 3. Payoff matrix in strategic form for node i

	Monitor	Not monitor
Attack	$W_i(1-2a_i-C_a(1-V_i^0))+\Delta_i$, $W_i(2a_i-1-C_mV_i^0)-\Delta_i$	$W_i(1-C_a(1-V_i^0)) + \Delta_i$, $-W_i-\Delta_i$
Not attack	Δ_i , $-C_mV_i^0W_i-\Delta_i$	Δ_i , $-\Delta_i$

$-W_i(1-a_i)$ respectively. However, if the attack is detected, which happens with probability a_i, the payoffs for the attacker and the defender are given by $-W_ia_i$ and W_ia_i respectively. We take into account the impact of interdependencies between vulnerable network nodes. For example, even though the attacker can choose not to attack node i directly, he can benefit from the impact of attacks on the set of nodes whose compromise can affect his state on node i (e.g. in terms of information or privileges the attacker could decide to make use of).

The utilities U_A and U_D of the attacker and the defender respectively are as follows:

$$U_A(\mathbf{p},\mathbf{q}) = \sum_{i=1}^{n} \Big(p_iq_i(W_i(1-2a_i-C_a^i) + \Delta_i) + (1-p_i)q_i\Delta_i + p_i(1-q_i)(W_i(1$$

$$-C_a^i) + \Delta_i) + (1-p_i)(1-q_i)\Delta_i\Big) = \sum_{i=1}^{n} p_iW_i(1-2a_iq_i-C_a^i) + \Delta_i$$

$$U_D(\mathbf{p},\mathbf{q}) = \sum_{i=1}^{n} q_iW_i(2a_ip_i-C_m^i) - p_iW_i - \Delta_i$$

3.3 Solving the Game

3.3.1 Node Distribution

The values of the security assets and the impact of the interdependencies between nodes can affect the strategies of the attacker and the defender. In this section, we identify the set $\mathcal{T_S}$ of sensible targets that are attractive to the attacker and needs therefore to be monitored by the defender. Let $\mathcal{T_U}$ refer to the set of unattractive nodes that will not be the target of attacks. Therefore, we have $\mathcal{T} = \mathcal{T_S} \cup \mathcal{T_U}$. Let $\lambda_i = (1 - C_a^i + \beta \sum_{j \in \Gamma^+(i)} \theta_i^j)$ and $\mu_i = a_i(2 + \beta \sum_{j \in \Gamma^+(i)} \theta_i^j)$, $\forall i \in \mathcal{T}$.

Definition 6. *The sensible target set $\mathcal{T}_S$ and the set $\mathcal{T}_U$ are defined as follows:*

$$\begin{cases} W_i\lambda_i > \xi \ \forall i \in \mathcal{T}_S \\ W_i\lambda_i < \xi \ \forall i \in \mathcal{T}_U \end{cases} \quad where\ \xi = \frac{\sum\limits_{k\in\mathcal{T}_S} \left(\frac{\lambda_k}{\mu_k}\right) - Q}{\sum\limits_{k \in \mathcal{T}_S} \left(\frac{1}{W_k\mu_k}\right)}.$$

The case where $W_i\lambda_i = \xi$ does not need to be taken into account. In fact, this case happens with very low probability. Therefore, should this case happen, and since these values rely on estimations, replacing for instance W_i with a slightly different estimation $W_i + \epsilon$ or $W_i - \epsilon$ would be enough to solve the problem.

For the rest of this paper, we suppose that network nodes are numbered according to the following rule: $i < j \Leftrightarrow W_i\lambda_i \geq W_j\lambda_j$.

Lemma 6. *Given a network comprised of n nodes, $\mathcal{T}_S$ is uniquely determined and consists of n_S nodes with the highest $W_i\lambda_i$ values. The set $\mathcal{T}_S$ can be determined using Algorithm 1.*

Proof. We need to prove that $\mathcal{T}_S$ consists of the d highest $W_i\lambda_i$ values, where $d = n_S$ and the cases where $d < n_S$ and $d > n_S$ cannot be achieved. First, it is easy to prove that if $i \in \mathcal{T}_S$, then $\forall j < i$, $j \in \mathcal{T}_S$. We prove that $d = n_S$ with a proof by contradiction. Let us suppose that $d < n_S$, we have: $W_{n_S}\lambda_{n_S} \sum_{k=1}^{n_S} \left(\frac{1}{W_k\mu_k}\right) - \sum_{k=d+1}^{n_S} \frac{\lambda_k}{\mu_k} > \sum_{k=1}^{d} \frac{\lambda_k}{\mu_k} - Q$. Noticing that $W_{n_S}\lambda_{n_S} \leq W_i\lambda_i, \forall i \leq n_S$ and $d < n_S$, we have: $W_{d+1}\lambda_{d+1} \sum_{k=1}^{d} \left(\frac{1}{W_k\mu_k}\right) \geq W_{n_S}\lambda_{n_S} \sum_{k=1}^{d} \left(\frac{1}{W_k\mu_k}\right) = W_{n_S}\lambda_{n_S} \sum_{k=1}^{n_S} \left(\frac{1}{W_k\mu_k}\right) - W_{n_S}\lambda_{n_S} \sum_{k=d+1}^{n_S} \left(\frac{1}{W_k\lambda_k}\frac{\lambda_k}{\mu_k}\right) \geq W_{n_S}\lambda_{n_S} \sum_{k=1}^{n_S} \left(\frac{1}{W_k\mu_k}\right) - \sum_{k=d+1}^{n_S} \left(\frac{\lambda_k}{\mu_k}\right) > \sum_{k=1}^{d} \left(\frac{\lambda_k}{\mu_k}\right) - Q$. However, from Definition 6, we have $W_{d+1}\lambda_{d+1} \leq \frac{\sum_{k=1}^{d} \left(\frac{\lambda_k}{\mu_k}\right) - Q}{\sum_{k=1}^{d} \left(\frac{1}{W_k\mu_k}\right)}$. This contradiction shows that it is impossible to have $d < n_S$. Similarly, we can show that it is impossible to have $d > n_S$. Therefore, $d = n_S$ and $\mathcal{T}_S$ is uniquely determined. □

Algorithm 1. FindSensibleTargetSet

```
Data: The set of nodes $\mathcal{T}$
Result: The sensible target set $\mathcal{T}_S$
begin
    $W'_i \longleftarrow SortInDescendingOrder(W_{\sigma(i)}\lambda_{\sigma(i)})$
    $n_S \longleftarrow n$
    while $n_S \geq 1$ & $W'_{n_S} \leq \frac{\sum_{k=1}^{n_S} \frac{\lambda_k}{\mu_k} - Q}{\sum_{k=1}^{n_S} \left(\frac{1}{W'_k\mu_k}\right)}$ do
        $n_S \longleftarrow n_S - 1$
    end
    $\mathcal{T}_S = \{\sigma(i) \in \mathcal{T} : i \in [\![1, n_S]\!]\}$
end
```

Theorem 7. *A rational attacker has no incentive to attack any node $i \in \mathcal{T}_U$.*

Proof. For space limitations, we only provide a sketch of the proof. The proof consists of showing that regardless of the defender's strategy $\mathbf{q}$, for any $\mathbf{p} \in [0,1]^n$ s.t. $\exists i \in \mathcal{T}_U$, $p_i > 0$, we can construct another strategy $\mathbf{p'}$ s.t. $p'_i = 0$, $\forall i \in \mathcal{T}_U$ and $U_A(\mathbf{p}, \mathbf{q}) < U_A(\mathbf{p'}, \mathbf{q})$. If $\mathcal{T}_U = \varnothing$, the theorem holds. We focus in our proof on the case where $\mathcal{T}_U \neq \varnothing$. We consider a vector $\mathbf{q^0} = (q_1^0, q_2^0, ..., q_N^0)$ s.t.:

$$q_i^0 = \begin{cases} \dfrac{Q - \sum\limits_{k \in \mathcal{T}_S} \left(\frac{\lambda_k}{\mu_k}\right)}{W_i \mu_i \sum\limits_{k \in \mathcal{T}_S} \left(\frac{1}{\mu_k W_k}\right)} + \dfrac{\lambda_i}{\mu_i} & \forall i \in \mathcal{T}_S \\ 0 & \forall i \in \mathcal{T} - \mathcal{T}_S \end{cases}$$

It holds that $\sum\limits_{i \in \mathcal{T}_S} q_i^0 = Q$, and $q_i^0 \geq 0$, $\forall i$. Let $\mathbf{q} = (q_1, ..., q_n)$ denote a defender strategy s.t. $\sum\limits_{i \in \mathcal{T}_S} q_i \leq Q$. By the pigeonhole principle, it holds that $\exists m \in \mathcal{T}_S$ s.t. $q_m \leq q_m^0$.

We consider an attacker strategy $\mathbf{p} = (p_1, ..., p_n)$ satisfying $\sum\limits_{i \in \mathcal{T}_U} p_i > 0$, i.e. the attacker attacks at least one target outside the sensible target set $\mathcal{T}_S$ with nonzero probability. We construct another attacker strategy profile $\mathbf{p'}$ based on $\mathbf{p}$ s.t.:

$$p'_i = \begin{cases} p_i & i \in \mathcal{T}_S \textit{ and } i \neq m \\ p_m + \sum\limits_{j \in \mathcal{T}_U} p_j & i = m \\ 0 & i \in \mathcal{T}_U \end{cases}$$

After some algebraic operations, it is possible to show that $U_A(\mathbf{p}, \mathbf{q}) < U_A(\mathbf{p'}, \mathbf{q})$. Therefore, the attacker is always better off attacking nodes in the sensible target set $\mathcal{T}_S$. □

Theorem 7 shows that the attacker only needs to attack nodes that belong to $\mathcal{T}_S$ in order to maximize his utility. Therefore, the defender has no incentive to monitor nodes that do not belong to $\mathcal{T}_S$. As a consequence, valuable defense resources would be wasted by monitoring nodes in $\mathcal{T}_U$. Therefore, a rational defender only needs to monitor nodes in $\mathcal{T}_S$.

3.3.2 NE Analysis

A strategy profile $(\mathbf{p}^*, \mathbf{q}^*)$ is a Nash Equilibrium of the intrusion detection game if each player cannot improve his utility by deviating from his strategy unilaterally. Let $\sum\limits_{i \in \mathcal{T}} p_i^* = P$ and $\sum\limits_{i \in \mathcal{T}} q_i^* = Q$. In this case, the attacker/defender uses all his resources to attack/defend the network. The game can be seen as a resource allocation problem, in which each player's objective is to maximize his/her utility given the action of the other player. The strategies of the attacker and the defender at the NE are as follows:

$$\forall i \in \mathcal{T}_S,\, p_i^* = \frac{P - \sum\limits_{k \in \mathcal{T}_S} \left(\frac{C_m^k}{\mu_k}\right)}{W_i\mu_i \sum\limits_{k\in\mathcal{T}_S} \left(\frac{1}{W_k\mu_k}\right)} + \frac{C_m^i}{\mu_i} \text{ and } q_i^* = \frac{Q - \sum\limits_{k\in\mathcal{T}_S} \left(\frac{\lambda_k}{\mu_k}\right)}{W_i\mu_i \sum\limits_{k\in\mathcal{T}_S} \left(\frac{1}{W_k\mu_k}\right)} + \frac{\lambda_i}{\mu_i}$$

$$\forall i \in \mathcal{T}_U,\; p_i^* = 0 \text{ and } q_i^* = 0$$

The necessary conditions for the obtained result to be a NE are:

$$\begin{cases} W_i(2a_ip_i^* - C_m^i) + \beta W_i a_i p_i^* \sum\limits_{j\in\Gamma^+(i)} \theta_i^j \geq 0 \\ W_i(1 - 2a_iq_i^* - C_a^i) + \beta W_i(1 - a_iq_i^*) \sum\limits_{j\in\Gamma^+(i)} \theta_i^j \geq 0 \end{cases} \Rightarrow \begin{cases} P \geq \sum\limits_{i\in\mathcal{T}_\mathcal{S}} \left(\frac{C_m^i}{\mu_i}\right) \\ Q \leq \sum\limits_{i\in\mathcal{T}_\mathcal{S}} \left(\frac{\lambda_i}{\mu_i}\right) \end{cases}$$

In this case, the attacker and the defender focus on attacking and monitoring a subset $\mathcal{T}_\mathcal{S}$ of nodes in the network. These nodes yield the maximum payoff for the attacker and therefore need to be monitored.

If $\sum\limits_{i\in\mathcal{T}} p_i^* < P$ and $\sum\limits_{i\in\mathcal{T}} q_i^* < Q$, both the attacker and the defender do not use all the available resources to attack and defend the network respectively. According to Theorem 1, in a realistic instance of this game, no NE exists.

4 Numerical Analysis

We consider a network comprised of $n = 10$ nodes. The type of the nodes and the values of some of the model parameters are depicted in Tables 4 and 5. The nodes in both tables are already sorted and numbered according to decreasing $W_i\lambda_i$ values as described in Sect. 3.

Table 4. Node types and individual parameters

Number	Node type	W_i	V_i^0	a_i
1	Business App. A	0.75	0.6	0.7
2	Intranet Portal	0.75	0.6	0.6
3	Mailing Server	0.75	0.3	0.6
4	Webmail Server	0.4	0.3	0.1
5	Business App. B	0.5	0.6	0.7
6	Intranet Common Services	1	0.6	0.1
7	Storage Area Network	1	0	0.1
8	Office Server	0.4	0.3	0.7
9	Authority Station	0.1	1	0.8
10	User Station	0.1	1	0.8

Table 5. Node interdependencies θ_i^j

i \ j	1	2	3	4	5	6	7	8	9/10
1	0	1	0	0	0	0.5	1	0	0
2	0	0	0	0	0	0.9	0.9	0	0
3	0	0	0	0	0	0.8	1	0	0
4	0	1	1	0	0	0.9	1	0	0
5	0	1	0	0	0	0.5	1	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0.5	0.9	0	0
9	0.8	0.9	0.3	0.1	0.8	0.9	0	0.3	0
10	0.5	0.5	0.2	0.1	0.5	0.9	0	0.2	0

We study the NE strategies of both players in two different scenarios. In the first scenario, we consider a typical network in which the attack and defense costs are relatively high compared with the security assets of the nodes (i.e. $C_a = C_m = 0.1$). In addition, the use of the interdependencies between nodes in the attack process is not considered of high criticality (i.e. $\beta = 0.5$). In this scenario, the attacker may not be tempted to fully exploit the node interdependencies in his attack. The resource constraints for the attacker and the defender are set to $P = 0.8$ and $Q = 0.9$ respectively, which means that the budget of the defender is slightly superior to the budget of the attacker. In the second scenario, the values of nodes security assets outweigh attack and defense costs (i.e. $C_a = C_m = 0.001$), and exploiting the interdependencies between nodes can play a significant role in the attack process (i.e. $\beta = 1$). In addition, due to the security requirements of such critical networks, the detection rate a_i on each node i is assumed to be $a_i \geq 0.5$. Finally, we consider that the attack and defense resource constraints are set to $P = 1$ and $Q = 1$ respectively.

The NE strategies of the attacker and the defender are depicted in Table 6. In both scenarios, the attacker/defender uses all his available resources to attack/defend. We note that both players focus on a sensible target set comprised of nodes 1, 2, 3, and 4 in the first scenario, and nodes 1, 2, 3, 4, and 5 in the second scenario. It is interesting to note that nodes 9 and 10 are not sensitive nodes despite having many dependencies stemming from them, as they have low security assets values to be worth attacking or defending. On the contrary, nodes 6 and 7 are not part of the sensible target set despite their relatively high security assets and the absence of dependencies stemming from them. In the second scenario, the sensible target set increased by one node (node 5). This is most probably due to the fact that the attacker has additional available resources and that node 4 had its detection probability a_i raised from 0.1 to 0.5, hence discouraging the attacker from spending too many resources to attack this node.

Table 6. Nash equilibrium for scenarios 1 and 2

Scenario 1	Scenario 2
$p_1^* = 0.0712$, $q_1^* = 0.3135$	$p_1^* = 0.1377$, $q_1^* = 0.3762$
$p_2^* = 0.0931$, $q_2^* = 0.2088$	$p_2^* = 0.1903$, $q_2^* = 0.2127$
$p_3^* = 0.0758$, $q_3^* = 0.1915$	$p_3^* = 0.1901$, $q_3^* = 0.2126$
$p_4^* = 0.5599$, $q_4^* = 0.1862$	$p_4^* = 0.2754$, $q_4^* = 0.1897$
$p_5^* = 0$, $q_5^* = 0$	$p_5^* = 0.2065$, $q_5^* = 0.0088$
$p_6^* = 0$, $q_6^* = 0$	$p_6^* = 0$, $q_6^* = 0$
$p_7^* = 0$, $q_7^* = 0$	$p_7^* = 0$, $q_7^* = 0$
$p_8^* = 0$, $q_8^* = 0$	$p_8^* = 0$, $q_8^* = 0$
$p_9^* = 0$, $q_9^* = 0$	$p_9^* = 0$, $q_9^* = 0$
$p_{10}^* = 0$, $q_{10}^* = 0$	$p_{10}^* = 0$, $q_{10}^* = 0$
$U_A = 0.898$, $U_D = -0.953$	$U_A = 1.736$, $U_D = -1.737$

The Security Information and Event Management (SIEM) software used in this industrial case study defines a metric to quantify the overall security of the network. This metric, which cannot be described in detail due to confidentiality reasons, consists in assessing, for each node, the types of attacks that can be mitigated given the current IDS configuration while taking into account the interdependencies between nodes in the evaluation process. After applying the optimal allocation of defense resources obtained at the NE, which translates in practice in configuring more efficient IDSs on critical nodes, we were able to notice a significant improvement of the overall security of the network, hence confirming the validity of our approach.

Sensitivity to $\boldsymbol{\theta_i^j}$. We analyze the impact of θ_i^j estimation errors on the identity of nodes that belong to the sensible target set $\mathcal{T}_S$. In both scenarios, nodes 8 to 10, due to their low security assets, remain in the set $\mathcal{T}_U$ even with a 20% estimation error on the values of each θ_i^j. In our model, the importance of a node is quantified by the value $W_i\lambda_i$, where λ_i mainly depends on β and the interdependencies θ_i^j. Therefore, inaccurate assessment of the interdependencies can have a significant impact on the results when the values of β and W_i are high. In our case study, when nodes 1, 2 and 3 have slightly erroneous interdependencies evaluations, we do not note any change in the sets $\mathcal{T}_S$ and $\mathcal{T}_U$. However, at the NE, we observe a small increase and decrease in the attacker and defender utilities respectively. For example, if on node 2, which has a relatively high security asset ($W_2 = 0.75$), $\sum_{j\in\Gamma^+(2)} \theta_2^j$ was overestimated by 0.4 (i.e. a 16% estimation error), U_A increases by 10% and U_D decreases by 5%. On the other hand, overestimating $\sum_{j\in\Gamma^+(5)} \theta_5^j$ by 0.1 (i.e. a 4% error) in scenario 1 is enough to include node 5 in $\mathcal{T}_S$. However, the impact of the error on U_A and U_D remains very low (<1%).

Similarly, underestimating $\sum_{j \in \Gamma^{+}(5)} \theta_5^j$ by 0.1 in scenario 2 leads to the exclusion of node 5 from $\mathcal{T}_S$. At the NE, the attacker leverages this situation and targets node 5. However, it is interesting to note that the impact on the players' utilities remains inferior to 1% in this case as well. This shows that in some cases, an approximate construction of the sensible target set $\mathcal{T}_S$ does not necessarily entail a sudden substantial utility gain (*resp.* loss) for the attacker (*resp.* defender).

These observations demonstrate that our model is robust enough to deal with slight inaccuracies in the evaluation of interdependencies parameters. However, given the number of parameters θ_i^j to evaluate in large networks, important estimation errors on these parameters could have a significant impact on the strategies of the attacker and the defender, hence justifying the need for a more formal and rigorous evaluation method of these parameters.

5 Conclusion

In this paper, we introduced a set of security games that we refer to as Resource Constrained Network Security (RCNS) games and studied the necessary conditions for the existence of NE, Stackelberg equilibrium, and *maximin* strategies for this type of games. We then presented a game theoretical model for optimizing the allocation of monitoring resources to detect attacks in a network while taking into account nodes' vulnerabilities interdependencies. Finally, we validated our model via a real world case study. Our numerical study showed that the result of the analysis is sensitive to the values of parameters quantifying the interdependencies between network nodes. Therefore, elaborating a rigorous evaluation method for these parameters will be the subject of future work. In addition, we plan to investigate the impact of imperfect information in the general framework of RCNS games on the existence and uniqueness of equilibrium solutions.

References

1. Manshaei, M.H., Zhu, Q., Alpcan, T., Basar, T., Hubaux, J.P.: Game theory meets network security and privacy. ACM Comput. Surv. **45**(3), 25–39 (2013)
2. Chen, L., Leneutre, J.: A game theoretical framework on intrusion detection in heterogeneous networks. IEEE Trans. Inf. Forensics Secur. **4**(2), 165–178 (2009)
3. Alpcan, T., Basar, T.: A game theoretic approach to decision and analysis in network intrusion detection. In: Proceedings of the 42nd IEEE Conference on Decision and Control (CDC), vol. 3 (2003)
4. Alpcan, T., Basar, T.: An intrusion detection game with limited observations. In: Proceedings of the 12th International Symposium on Dynamic Games and Applications (2006)
5. Nguyen, K., Alpcan, T., Basar, T.: Stochastic games for security in networks with interdependent nodes. In: Proceedings of the International Conference on Game Theory for Networks (GameNets) (2009)

6. Miura-Ko, R., Yolken, B., Bambos, N., Mitchell, J.: Security investment games of interdependent organizations. In: Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing (2008)
7. Sallhammar, K., Helvik, B., Knapskog, S.: Incorporating attacker behavior in stochastic models of security. In: Proceedings of the 2005 International Conference on Security and Management (2005)
8. Kodialam, M., Lakshman, T.: Detecting network intrusions via sampling: a game theoretic approach. In: IEEE INFOCOM (2003)
9. Otrok, H., Mohammed, N., Wang, L., Debbabi, M., Bhattacharya, P.: A game-theoretic intrusion detection model for mobile ad hoc networks. Comput. Commun. **31**(4), 708–721 (2008)
10. Otrok, H., Mehrandish, M., Assi, C., Debbabi, M., Bhattacharya, P.: Game theoretic models for detecting network intrusions. Comput. Commun. **31**(10), 1934–1944 (2008)
11. Zheng, D., Yu, F., Boukerche, A.: Security and quality of service (qos) co-design using game theory in cooperative wireless ad hoc networks. In: Proceedings of the Second ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (2012)
12. Djebaili, B., Kiennert, C., Leneutre, J., Chen, L.: Data integrity and availability verification game in untrusted cloud storage. In: Proceedings of the 5th International Conference on Decision and Game Theory for Security (2014)