A Game-Theoretical Approach for Finding Optimal Strategies in an Intruder Classification Game

Lemonia Dritsoula, Patrick Loiseau, and John Musacchio

Abstract— **We consider a game in which a strategic defender classifies an intruder as spy or spammer. The classification is based on the number of file server and mail server attacks observed during a fixed window. The spammer naively attacks (with a known distribution) his main target: the mail server. The spy strategically selects the number of attacks on his main target: the file server. The defender strategically selects his classification policy: a threshold on the number of file server attacks. We model the interaction of the two players (spy and defender) as a nonzero-sum game: The defender needs to balance missed detections and false alarms in his objective function, while the spy has a tradeoff between attacking the file server more aggressively and increasing the chances of getting caught. We give a characterization of the Nash equilibria in mixed strategies, and demonstrate how the Nash equilibria can be computed in polynomial time. Our characterization gives interesting and non-intuitive insights on the players' strategies at equilibrium: The defender uniformly randomizes between a set of thresholds that includes very large values. The strategy of the spy is a truncated version of the spammer's distribution. We present numerical simulations that validate and illustrate our theoretical results.**

I. Introduction

Cybersecurity is important to businesses and individuals. According to a recent study conducted by Symantec [1], the number of cyber attacks and threats has increased during 2011, resulting in lost productivity, reduced revenue, and bad reputation for the associated businesses. Different kinds of attacks (e.g., internal unintentional actions and external malicious ones) should be treated differently and organizations need the security intelligence to respond to all threats rapidly. Since only less than half of organizations are currently pursuing security issues, there is still room for improvement. Our work contributes to the understanding of the interaction between network operators and potential attackers.

In almost every network security situation, the administrator of a network (defender) has limited resources. The defender needs to distinguish between different types of attackers (spy or spammer) and decide whether to take actions or not. For example, an attack on a mail server by a spammer (causing at most network congestion) should be treated differently than an attack on a file server (possibly involving identity theft) by a spy. Therefore, the defender should employ various statistical tests, based on the observed number of file and mail server attacks and decide upon the type of the attacker. Knowing that a defender is trying to classify attackers, the strategic spy is likely to change the way he attacks in order to make it more difficult to be classified as a spy. In this work, we analyze a simple model of such a classification game and extract key insights.

There exists a growing body of works on the topic of intrusion detection. In [2], Alpcan and Başar present a security game between an attacker and an intrusion detection system and address some of the basic security tradeoffs, e.g., false alarms versus undetected attackers. They also provide insightful overview on how different network parameters affect the performance of the intruder detection system. Our game-theoretic framework investigates a more complex game and provides analytic expressions for the defender's NE strategies. In the presence of a non-strategic player who is represented with a fixed and known probability distribution, the defender's task of distinguishing the type of the attacker becomes more challenging. It is also interesting to see how the non-strategic spammer influences the spy's strategy.

In [3], Patcha and Park model the interaction between a node that might be regular or dangerous and a defender who has some prior probability for the existence of each type in an ad hoc network. They consider a signaling and dynamic game with multiple stages and the players update their beliefs and distributions based on Bayes' rule. On the contrary, our work considers a one-stage game with a fixed duration and we compute the Nash equilibria in mixed strategies.

Chen and Leneutre [4] address the intrusion detection problem in heterogeneous networks consisting of nodes with different non-correlated security assets, in the same way that the file and mail servers are of different importance in our work. They consider a static game with full information and limited attack and monitoring resources. We do not consider such limitations and we assume asymmetric information, since the defender is not aware of the attacker's type.

Bao, Kreidl, and Musacchio [5] also consider an intruder classification game, in which the sequence of attacks is taken into account. While their model has many similarities with ours, we focus on less complex (but still realistic) payoff functions that allow us to go one step further than simulations and analyze the structure of the Nash equilibria.

Gueye, Walrand, and Anantharam [6], [7] have investigated the structure of the Nash equilibria in a network topology game, in which attacker and defender select which links to attack and use for communication respectively. They consider a special case of nonzero-sum games, in which the different term in the players' payoffs is controlled only by one player. Such games are easier to analyze than general

This work was supported by AFOSR grant FA9550-09-1-0049.

Lemonia Dritsoula and John Musacchio are with University of California, Santa Cruz, CA, USA. {lenia, johnm}@soe.ucsc.edu

Patrick Loiseau is with EURECOM, Sophia-Antipolis, France. Part of this work was done while he was at UC Santa Cruz, CA, USA. patrick.loiseau@eurecom.fr

nonzero-sum games, and they give interesting insights on the strategies of the two players. Our work is using a similar payoff formulation in a different setting: the defender selects a threshold on file server attacks (not a set of links to use) and there are two different types of attackers. We use a different proof technique that does not require the computation of the blocker and we obtain a stronger result on the Nash equilibrium structure.

To the best of our knowledge, [8] is the most relevant work to ours. Dalvi et al. address the problem of classifying a malicious intruder in the presence of an innocent user. The malicious intruder can perturb his behavior to confuse the classifier and evade detection. However, their work focuses only on one iteration of the game and how each player can once adjust his strategy to optimize his expected payoff, given a strategy of the other player rather than finding a pair of simultaneous best responses. In contrast, we focus on the Nash equilibria of the game.

In recent works [9], [10], Brückner and Scheffer go further than [8] by studying the strategic interaction between a spam filter (learner) and a spammer (the strategic attacker in their work). They also show empirical results on real data. However, their payoff formulation is different from ours, and they restrict their analysis to pure-strategy equilibria. Consequently, their results are very different from ours in spirit.

In summary, our contributions are the following. We propose a game-theoretic model to analyze the interactions between two adversaries: a classifier (defender) and a malicious attacker when a non-strategic spammer is present. We characterize all Nash equilibria in mixed strategies and demonstrate how the Nash equilibria can be computed in polynomial time. We perform numerical experiments that validate the theoretical computation and give non-intuitive insights on the players' strategies.

The rest of the paper is organized as follows. Section II describes the game model and underlying assumptions. Section III explains how to reduce the complexity of the game and compute the Nash equilibria in polynomial time. Section IV presents the performance evaluation through numerical experiments and Section V concludes the paper.

II. Game Model

The game model is as follows. A network consists of a defender and two servers that are monitored for potential attacks: a File Server (FS) with sensitive data and a Mail Server (MS) with contents of inferior importance. We assume a constant classification window of N time slots (discrete time), during which the defender observes the number of hits on the FS / MS coming from a single attacker. Nature decides the type of the attacker in the network: spy or spammer with probabilities p and $1-p$ respectively.

The defender is a strategic player and seeks to correctly classify the intruder. He selects a threshold T. If he observes T or more hits on the FS, he classifies the attacker as spy; otherwise as spammer. The spy is also a strategic player that selects the number of FS attacks H he will perform. He seeks to attack the FS as frequently as possible, while evading detection.

The spammer is a non-strategic player that mostly attacks the MS and adds noise to the network. He also attacks the FS Z times (Z follows a known distribution). For instance, he can be modeled to follow the Bernoulli distribution at each time slot with a small per-period probability θ_0 of a FS hit.

Our results are based on a relatively simple model where there are only two possible targets and two possible types of attackers. However, our solution captures a more general setting than the one presented above. We only require that the attacker has some cost function if he gets detected or missed. We describe the model around the example scenario in which there are two servers, one of which is of primary interest to the strategic attacker (the file server) in order to be more concrete. However, the model we develop is quite general and applicable to many settings in which there is a target of special interest to a strategic attacker but who is incentivized to mix his attack across other targets to make classification more difficult.

Notational Conventions:
We use "$\min[\boldsymbol{v}]$" to denote the minimum element of a vector $\boldsymbol{v}$, and "minimize" when we minimize a specific expression over some constraints. We use the *prime* sign ($'$) for transpose of matrices and vectors. All vectors are assumed to be column vectors and are denoted by bold lowercase letters (e.g., $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$). For matrix notation we use capital greek letters (e.g., Λ). The indicator function is denoted by $\mathbb{1}_{\text{cond}}$; it is equal to 1 if "cond" holds and is equal to 0 otherwise. The column vector of ones of length N is denoted by $\mathbf{1}_N$ and the matrix of ones of dimensions $N \times M$ is denoted by $1_{N\times M}$. The norm of a vector $\boldsymbol{x}$ of length N, denoted by $\|\boldsymbol{x}\|$, always refers to the 1-norm, i.e, $\|\boldsymbol{x}\| = |x_1| + |x_2| + \ldots + |x_N|$. An overview of our notation is shown in Table I.

A. *Spy's cost function*

The spy is detected when $T \leq H$, which incurs a cost of c_{d} to the spy. Each of the H FS hits gives the spy a benefit of c_{a}. We assume that the spy gains nothing from attacking the MS. We will work with a cost function for the attacker rather than a payoff function, thus, his overall cost function can be expressed as follows

$$J_A(T,H) = c_{\text{d}} \cdot \mathbb{1}_{T\leq H} - c_{\text{a}} \cdot H.$$

B. *Defender's reward function*

The defender's expected reward function depends on the type of the attacker.

- With probability p the defender faces a spy and classifies him correctly when $T \leq H$. The defender gains c_{d} for the correct classification of the spy, but loses c_{a} per FS hit.
- With probability $1-p$ the defender faces a spammer, who is incorrectly classified as spy with probability $\phi(T) = \Pr\{Z \geq T\}$. The expected false alarm penalty in this case is $c_{\text{fa}} \cdot \phi(T)$.

Combining the above two scenarios, the defender's expected payoff is

$$\tilde{U}_D(T,H) = p \cdot (c_{\text{d}} \cdot \mathbb{1}_{T \le H} - c_{\text{a}} \cdot H) - (1-p) \cdot c_{\text{fa}} \cdot \phi(T).$$

By scaling the above function, we get

$$U_D(T,H) = c_{\text{d}} \cdot \mathbb{1}_{T \le H} - c_{\text{a}} \cdot H - \mu(T),$$

where $\mu(T) = \dfrac{1-p}{p} \cdot c_{\text{fa}} \cdot \phi(T)$. Function $\phi(T)$ is non-increasing and we also assume that it is strictly decreasing: $\Pr\{Z \ge T\} > \Pr\{Z \ge T+1\}$.

C. Players' interactions

For a fixed observation window N the spy has $N+1$ available actions (attack the file server $H \in \{0,\dots,N\}$ times), whereas the defender has $N+2$ available actions (select $T \in \{0,\dots,N+1\}$ as the classification threshold). A threshold of 0 always results in spy classification (any intruder will attack the FS at least 0 times); a threshold of $N+1$ always results in spammer classification (a spy cannot attack $N+1$ times during N).

We model our problem as a nonzero-sum game, where the term in the defender's payoff that is different from the spy's cost depends only on the defender's strategy ($U_D(T,H) = J_A(T,H) - \mu(T)$). These games are known as almost zero-sum games or quasi zero-sum games.

We are interested in Nash equilibria in mixed strategies for the following reason. In most cases the spy's best response to a threshold T is to attack the file server a number of times H just below T (unless the cost of being detected is so low that the spy prefers to attack as often as possible even while being detected). Likewise, in most cases, the defender's best response to an H is to choose the threshold T to be just equal to H in order to have the lowest false alarm penalty possible while still detecting the spy. Since each player wants to pick "lower" than the other, there is no pure strategy Nash equilibrium in most cases of interest, so we consider mixed strategies. The spy chooses a distribution vector $\boldsymbol{\alpha}$ on the allowed number of FS hits; $\boldsymbol{\alpha}$ is a vector of size $N+1$ (with non-negative elements that sum to 1). Similarly, the defender chooses a distribution vector $\boldsymbol{\beta}$ on the collection of possible thresholds T; $\boldsymbol{\beta}$ is a vector of size $N+2$ (with non-negative elements that sum to 1).

Let $\tilde{\Lambda}$ be a $(N+1) \times (N+2)$ matrix representing the spy's strategies' cost. Since the number of strategies available to each player is not the same, the cost matrix $\tilde{\Lambda}$ is not square. We express the cost matrix of the attacker as

$$\tilde{\Lambda} = c_{\text{d}} \cdot \underbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 & 0 \\ \vdots & 1 & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \ddots & \vdots & \vdots \\ \vdots & & & \ddots & 0 & \vdots \\ 1 & \cdots & \cdots & \dots & 1 & 0 \end{pmatrix}}_{\tilde{\Lambda}_1} - c_{\text{a}} \cdot \underbrace{\begin{pmatrix} 0 \\ 1 \\ 2 \\ \vdots \\ N-1 \\ N \end{pmatrix} \cdot \mathbf{1}'_{N+2}}_{\tilde{\Lambda}_2}$$

with $\tilde{\Lambda}_1(i,j) = \mathbb{1}_{j \le i}$, where $i \in \{0,\dots,N\}$ designates the row and $j \in \{0,\dots,N+1\}$ the column.

TABLE I

Main Notations

p	probability for spy	$\boldsymbol{\alpha}$	spy's mixed strategy
c_{d}	detection cost	$\boldsymbol{\beta}$	def. mixed strategy
c_{a}	FS attack cost	$\boldsymbol{\mu}$	false alarm cost vector
c_{fa}	false alarm penalty	$\theta(\boldsymbol{\beta})$	defendability of $\boldsymbol{\beta}$
H	spy's strategy (# FS hits)	Λ	cost matrix of spy
T	def. strategy (threshold)	s	first tight inequality
Z	# of FS hits by spammer	f	last tight inequality

Each row i of $\tilde{\Lambda}$ corresponds to one of the $N+1$ possible spy strategies. For instance, row "0" corresponds to spy attacking the FS 0 times (or $H = 0$). Each column of $\tilde{\Lambda}$ corresponds to one of the $N+2$ possible defender strategies. For instance, column "0" corresponds to defender selecting $T = 0$ (or always classify as spy). In $\tilde{\Lambda}_2$, every column j (defender strategy) incurs the same benefit to the spy. No matter what the decision threshold is, the impact of the spy's attacks is the same.

Let $\boldsymbol{\alpha}, \boldsymbol{\beta}$ be the spy and defender distributions respectively. The spy cost can be written as $\boldsymbol{\alpha}'\tilde{\Lambda}\boldsymbol{\beta}$ and the defender payoff can be written as $\boldsymbol{\alpha}'\tilde{\Lambda}\boldsymbol{\beta} - \boldsymbol{\mu}'\boldsymbol{\beta}$, where $\boldsymbol{\mu}$ is a strictly decreasing vector (component-wise) with μ_i being the i^{th} component of vector $\boldsymbol{\mu}$. Certain computations are simplified by using a matrix with only positive entries. We define

$$\Lambda = \tilde{\Lambda} + K \cdot 1_{(N+1)\times(N+2)},$$

where K is such that every element of matrix Λ is positive. Since $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ must each sum to 1, the expressions $\boldsymbol{\alpha}'\Lambda\boldsymbol{\beta}$ and $\boldsymbol{\alpha}'\Lambda\boldsymbol{\beta} - \boldsymbol{\mu}'\boldsymbol{\beta}$ are respectively the attacker cost and defender payoff shifted by a constant. Adding a constant to the players' payoff does not affect their best responses, thus from here on we will consider these expressions to be the payoff functions of each player.

III. Game-Theoretic Analysis

It is known that every finite game (finite number of players with finite number of actions for each player) has a mixed-strategy Nash equilibrium [13]. Our game is finite, thus it admits a NE in mixed strategies. In a two-player game, the players' strategies $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are a NE if each player's strategy is a best response to the other player's mixed strategy.

A. Best response analysis

We will first prove a series of lemmata that will help us state and prove our two theorems.

Lemma 1. *A spy who plays a best response to a defender strategy $\boldsymbol{\beta}$ has a cost $\delta = \min[\Lambda\boldsymbol{\beta}]$.*

Proof. Since Λ is positive, for a given defender strategy $\boldsymbol{\beta}$, the minimum spy cost is achieved by putting positive probability only on strategies corresponding to the minimum entries of the vector $\Lambda\boldsymbol{\beta}$. Thus the spy's optimal cost is $\delta = \min[\Lambda\boldsymbol{\beta}]$. □

Definition 1 (Defendability)**.** *The defendability of a mixed strategy $\boldsymbol{\beta}$ is defined as*

$$\theta(\boldsymbol{\beta}) = \min[\Lambda\boldsymbol{\beta}] - \boldsymbol{\mu}'\boldsymbol{\beta}. \tag{1}$$

It corresponds to the defender's payoff when the attacker plays a best response to $\boldsymbol{\beta}$*.*

The defendability is similar to the notion of vulnerability in [7], which is a measure of how vulnerable a set of links is. An interesting property of the defendability is that it depends only on the defender's strategy and not on the spy's selection of $\boldsymbol{\alpha}$. This is due to the aforementioned "almost" zero-sum game. We will exploit this property in the subsequent analysis.

In Nash equilibrium, each player in the game selects a best response to the other player's strategies. We show below (Theorem 1) that the defender's best response to any spy's best response maximizes the defendability.

We proved in Lemma 1 that the best response of the spy against any defender strategy $\boldsymbol{\beta}$, gives a spy cost $\delta = \min[\Lambda\boldsymbol{\beta}]$. The attacker's optimization problem, subject to the constraint that he limits the defender to the defendability $\theta(\boldsymbol{\beta})$ takes the following form

Primal with constraints:

$$\begin{aligned} \underset{\boldsymbol{\alpha}}{\text{minimize}} \quad & \boldsymbol{\alpha}'\Lambda\boldsymbol{\beta} \\ \text{subject to} \quad & \boldsymbol{\alpha} \geq \mathbf{0}, \mathbf{1}'_{N+1} \cdot \boldsymbol{\alpha} \geq 1, \\ & \boldsymbol{\alpha}'\Lambda - \boldsymbol{\mu}' \leq \theta(\boldsymbol{\beta}) \cdot \mathbf{1}'_{N+2}. \end{aligned} \tag{2}$$

The last constraint in the above linear program (LP) comes from the fact that in NE, the defender is indifferent among the strategies in his support. If $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is a NE, then $\boldsymbol{\alpha}$ is the solution of the above LP (2). The dual constrained LP is

Dual with constraints:

$$\begin{aligned} \underset{\boldsymbol{y},z}{\text{maximize}} \quad & (-\mathbf{1}'_{N+2} \cdot \theta(\boldsymbol{\beta}) - \boldsymbol{\mu}')\boldsymbol{y} + z \\ \text{subject to} \quad & \boldsymbol{y} \geq \mathbf{0},\ z \geq 0 \\ & z \cdot \mathbf{1}_{N+1} - \Lambda\boldsymbol{y} \leq \Lambda\boldsymbol{\beta}. \end{aligned} \tag{3}$$

As we show below, the optimal value of the dual LP given by (3) is equal to δ if and only if $\boldsymbol{\beta}$ is a maximizer of the function $\theta(\boldsymbol{\beta})$. If the optimal value was greater than δ, then the attacker would not play a best response against a strategy $\boldsymbol{\beta}$, namely we would not be in NE.

Working on (3), the last constraint gives $\Lambda(\boldsymbol{\beta} + \boldsymbol{y}) \geq z \cdot \mathbf{1}_{N+1}$, and since we seek to maximize a non-negative z with an upper limit, $z = \min[\Lambda(\boldsymbol{\beta} + \boldsymbol{y})]$. We note here that since Λ and $(\boldsymbol{\beta} + \boldsymbol{y})$ are non-negative matrix and vector respectively, their multiplication is also a non-negative vector and the above optimal value for z is valid. With the above substitution for z, we get the following LP

$$\begin{aligned} \underset{\boldsymbol{y}}{\text{maximize}} \quad & -\|\boldsymbol{y}\|\theta(\boldsymbol{\beta}) - \boldsymbol{\mu}'\boldsymbol{y} + \min[\Lambda(\boldsymbol{\beta} + \boldsymbol{y})] \\ \text{subject to} \quad & \boldsymbol{y} \geq \mathbf{0}. \end{aligned} \tag{4}$$

Theorem 1. *A defender strategy* $\boldsymbol{\beta}$ *is part of a Nash equilibrium strategy profile* $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ *for some* $\boldsymbol{\alpha}$ *if and only if the defendability* $\theta(\boldsymbol{\beta})$ *is maximal.*

Proof. Part I: Suppose that the defender's strategy is $\boldsymbol{\beta}$ such that $\theta(\boldsymbol{\beta}) < \theta(\boldsymbol{\xi})$, where $\boldsymbol{\xi} = \arg\max\theta$. Let $\boldsymbol{y} = k\boldsymbol{\xi}$, with $k \gg 1$. Then (4) gives

$$\begin{aligned} \underset{k}{\text{maximize}} \quad & -\|k\boldsymbol{\xi}\|\theta(\boldsymbol{\beta}) - \boldsymbol{\mu}'k\boldsymbol{\xi} + \min[\Lambda(\boldsymbol{\beta} + k\boldsymbol{\xi})] \\ \text{subject to} \quad & k \gg 1. \end{aligned} \tag{5}$$

Since $\Lambda k\boldsymbol{\xi} \gg \Lambda\boldsymbol{\beta}$ (Λ is positive), $\|\boldsymbol{\xi}\| = 1$ and $\theta(\boldsymbol{\xi}) = \min[\Lambda\boldsymbol{\xi}] - \boldsymbol{\mu}'\boldsymbol{\xi}$, the argument that needs to be maximized in (5) becomes $-k\theta(\boldsymbol{\beta}) + k\theta(\boldsymbol{\xi})$ or $k\left(\theta(\boldsymbol{\xi}) - \theta(\boldsymbol{\beta})\right)$. Since $\theta(\boldsymbol{\xi}) > \theta(\boldsymbol{\beta})$, this expression can be made arbitrarily large. Therefore, the optimal value of (4) is infinity. Since the optimal value of the dual problem is unbounded, the initial primal problem is infeasible [11]. Hence, if the defendability $\theta(\boldsymbol{\beta})$ is not maximal, then $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is not a NE for any $\boldsymbol{\alpha}$.

Part II: Suppose that the defender's strategy $\boldsymbol{\beta} \in \arg\max\theta(\boldsymbol{\lambda})$. We show that the optimal values of the attacker's constrained and unconstrained LP problems are the same, i.e., $\delta_{const} = \delta$, where δ_{const} is the optimal value of (2). This implies that $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is a NE, where $\boldsymbol{\alpha}$ is a solution of (2).

Since (2) is a minimization problem over a smaller set (extra constraints),

$$\delta_{const} \geq \delta. \tag{6}$$

With the change of variable $\boldsymbol{q} = \boldsymbol{\beta} + \boldsymbol{y}$, we transform (4) to the following problem

$$\begin{aligned} \underset{\boldsymbol{q}}{\text{maximize}} \quad & -(\|\boldsymbol{q}\| - \|\boldsymbol{\beta}\|)\theta(\boldsymbol{\beta}) - \boldsymbol{\mu}'(\boldsymbol{q} - \boldsymbol{\beta}) + \min[\Lambda\boldsymbol{q}] \\ \text{subject to} \quad & \boldsymbol{q} \geq \boldsymbol{\beta}. \end{aligned} \tag{7}$$

We take now a relaxed version of the above problem, where the constraint is $\boldsymbol{q} \geq \mathbf{0}$ instead of $\boldsymbol{q} \geq \boldsymbol{\beta}$

$$\underset{\boldsymbol{q} \geq \mathbf{0}}{\text{maximize}}\{-(\|\boldsymbol{q}\| - \|\boldsymbol{\beta}\|)\theta(\boldsymbol{\beta}) - \boldsymbol{\mu}'(\boldsymbol{q} - \boldsymbol{\beta}) + \min[\Lambda\boldsymbol{q}]\}.$$

Clearly the optimal value $\delta_{relax-const}$ in the above relaxed maximization problem is greater than or equal to the optimal value δ_{const} of the original problem (7), since we maximize the same objective function over a larger set. Thus

$$\delta_{relax-const} \geq \delta_{const}. \tag{8}$$

Since $\|\boldsymbol{\beta}\| = 1$ and $\delta = \theta(\boldsymbol{\beta}) + \boldsymbol{\mu}'\boldsymbol{\beta}$, from the above relaxed problem we get

$$\underset{\boldsymbol{q} \geq \mathbf{0}}{\text{maximize}}\{\delta - \|\boldsymbol{q}\|\theta(\boldsymbol{\beta}) + \min[\Lambda\boldsymbol{q}] - \boldsymbol{\mu}'\boldsymbol{q}\}. \tag{9}$$

But $\min[\Lambda\boldsymbol{q}] - \boldsymbol{\mu}'\boldsymbol{q} = \|\boldsymbol{q}\| \cdot \theta(\boldsymbol{q}) \leq \|\boldsymbol{q}\| \cdot \theta(\boldsymbol{\beta})$, since $\boldsymbol{\beta} \in \arg\max\theta(\boldsymbol{\lambda})$. Thus, the maximization in (9) always gives an optimal value

$$\delta_{relax-const} \leq \delta. \tag{10}$$

From (6), (8) and (10) we get $\delta \leq \delta_{const} \leq \delta_{relax-const} \leq \delta$, which yields $\delta_{const} = \delta$. □

Theorem 1 gives an intuitive characterization of the defender's strategy in NE. To further develop the computation of the NE strategies, we introduce the following definitions.

Definition 2. *A* **polyhedron** *is the solution set of a finite number of linear equalities and inequalities. An inequality constraint is* **tight** *if it holds as an equality; otherwise, it is loose. A point $\boldsymbol{x} = (x_0, \dots, x_{N+1})$ of a polyhedron is said to be* **extreme** *if there is no $\boldsymbol{x}'$ whose set of tight constraints is a strict superset of the set of tight constraints of $\boldsymbol{x}$. We say that a point $\boldsymbol{x}$ of the polyhedron* **corresponds** *to strategy $\boldsymbol{\beta}$, if $\boldsymbol{\beta} = \boldsymbol{x}/\|\boldsymbol{x}\|$.*

Lemma 2. *The defendability is maximized amongst the defender strategies $\boldsymbol{\beta}$ that correspond to the extreme points of the polyhedron defined by $\Lambda\boldsymbol{x} \geq \mathbf{1}_{N+1}$, $\boldsymbol{x} \geq \mathbf{0}$.*

Proof. As we proved in Theorem 1, in NE, the defender maximizes the defendability, that is, he solves the following "defendability LP"

$$\begin{aligned} \underset{\boldsymbol{\beta}, z}{\text{maximize}} \quad & -\boldsymbol{\mu}'\boldsymbol{\beta} + z \\ \text{subject to} \quad & z \cdot \mathbf{1}_{N+1} \leq \Lambda\boldsymbol{\beta} \\ & \mathbf{1}'_{N+2} \cdot \boldsymbol{\beta} = 1, \; \boldsymbol{\beta} \geq \mathbf{0}. \end{aligned} \tag{11}$$

Let $[\boldsymbol{\beta}, z]$ be a solution of (11) that is an extreme point of the polyhedron defined by the constraints of (11). This point must exist by the fundamental theorem of Linear Programming, and $z = \min[\Lambda\boldsymbol{\beta}]$. Let $\boldsymbol{x} := \boldsymbol{\beta}/z$. Then $\boldsymbol{x}$ satisfies the constraints $\Lambda\boldsymbol{x} \geq \mathbf{1}_{N+1}$ and $\boldsymbol{x} \geq 0$. We show that $\boldsymbol{x}$ is an extreme point of the polyhedron defined by these constraints[1].

Let S be the set of indices of tight inequalities of $\Lambda\boldsymbol{\beta} \geq z \cdot \mathbf{1}_{N+1}$, and P be the set of indices of tight inequalities in $\boldsymbol{\beta} \geq \mathbf{0}$. Substituting for $\boldsymbol{x}$, the above constraints become $\Lambda\boldsymbol{x} \geq \mathbf{1}_{N+1}$, $\boldsymbol{x} \geq \mathbf{0}$, and $\boldsymbol{x}$ satisfies this set of constraints. The same sets S and P specify the tight inequalities and $\boldsymbol{x}$ is an extreme point for the above constraints. If it is not extreme, then there exists a point $\hat{\boldsymbol{x}}$ with corresponding sets of tight inequalities $\hat{S} \supseteq S$ and $\hat{P} \supseteq P$, one of which is a strict superset.

Let $\hat{\boldsymbol{\beta}} = \dfrac{\hat{\boldsymbol{x}}}{\mathbf{1}'_{N+2} \cdot \hat{\boldsymbol{x}}}$, and $\hat{z} = \min[\Lambda\hat{\boldsymbol{\beta}}]$. It can be easily shown that $\hat{\boldsymbol{\beta}}$ satisfies the inequalities $\Lambda\boldsymbol{\beta} \geq z \cdot \mathbf{1}_{N+1}$, and $\boldsymbol{\beta} \geq \mathbf{0}$. Indeed, $\Lambda\hat{\boldsymbol{\beta}} \geq \min[\Lambda\hat{\boldsymbol{\beta}}] = \hat{z} \cdot \mathbf{1}_{N+1}$, and since $\hat{\boldsymbol{x}} \geq \mathbf{0}$, $\hat{\boldsymbol{\beta}} \geq \mathbf{0}$. It can also be shown that $\hat{\boldsymbol{\beta}}$ has tight inequalities in $\hat{S}$ and $\hat{P}$. Indeed $\forall j \in \hat{P}, \hat{\beta}_j = 0$ (thus $\hat{\boldsymbol{\beta}}$ has tight inequalities in $\hat{P}$). $\forall i \in \hat{S}$, $\hat{\boldsymbol{x}}$ has tight inequalities in $\hat{S}$, thus $[\Lambda\hat{\boldsymbol{x}}]_i = \min[\Lambda\hat{\boldsymbol{x}}] = 1$. We divide the last equation with $\mathbf{1}'_{N+2} \cdot \hat{\boldsymbol{x}}$ (constant, can get inside the min) and get $\left[\Lambda\left(\dfrac{\hat{\boldsymbol{x}}}{\mathbf{1}'_{N+2} \cdot \hat{\boldsymbol{x}}}\right)\right]_i = \min\left[\Lambda\dfrac{\hat{\boldsymbol{x}}}{\mathbf{1}'_{N+2} \cdot \hat{\boldsymbol{x}}}\right]$. But $\dfrac{\hat{\boldsymbol{x}}}{\mathbf{1}'_{N+2} \cdot \hat{\boldsymbol{x}}} = \hat{\boldsymbol{\beta}}$, thus $[\Lambda\hat{\boldsymbol{\beta}}]_i = \min[\Lambda\hat{\boldsymbol{\beta}}]$, so $\hat{\boldsymbol{\beta}}$ has tight inequalities in $\hat{S}$. Thus $[\hat{\boldsymbol{\beta}}, \hat{z}]$ has a strict superset of tight inequalities to $[\boldsymbol{\beta}; z]$; this is a contradiction with our hypothesis that $[\boldsymbol{\beta}; z]$ was an extreme point. Thus, the defendability is maximized amongst the defender strategies $\boldsymbol{\beta}$ that correspond to the extreme points of the polyhedron defined by $\Lambda\boldsymbol{x} \geq \mathbf{1}_{N+1}$, $\boldsymbol{x} \geq \mathbf{0}$. □

Adding the constant parameter $Nc_\text{a} + \epsilon$ to every element of Λ does not change the structure of the Nash equilibria but renders Λ strictly positive. We thus avoid the problems that arise when the minimum element of the vector is zero (infinite solution). As we have shown, computing the defender's NE strategy is the same as solving the linear program (11).

Since there exist well-known algorithms to solve a linear program in polynomial time, this directly guarantees that we can compute the NE in polynomial time for any almost-zero-sum game. In the next section, we derive a simpler algorithm taking into account the particular structure of our game.

B. Form of players' strategies in NE

1) Defender's NE strategy: As we saw in Lemma 2, the best response strategy of the defender is found by looking at the extreme points of the polyhedron $\Lambda\boldsymbol{x} \geq \mathbf{1}_{N+1}$, $\boldsymbol{x} \geq \mathbf{0}$. We call the first type "inequality" constraints and the second type "positivity" constraints. We have $N + 1$ "inequalities" and $N + 2$ "positivity" constraints. Writing down the "inequality" constraints, we get

$$\begin{aligned} c_\text{d} \cdot x_0 + (Nc_\text{a} + \epsilon)\|\boldsymbol{x}\| \quad &\geq \quad 1 \\ c_\text{d} \cdot (x_0 + x_1) + [(N-1)c_\text{a} + \epsilon]\|\boldsymbol{x}\| \quad &\geq \quad 1 \\ &\vdots \\ c_\text{d} \cdot (x_0 + x_1 + \ldots + x_N) + \epsilon\|\boldsymbol{x}\| \quad &\geq \quad 1. \end{aligned}$$

Our goal is to eliminate non-extreme points that are not selected by a defender in NE, so that we reduce the number of points we have to check.

Lemma 3. *An extreme point $\boldsymbol{x}$ satisfies at least one tight inequality.*

Proof. If none of the inequalities are tight, we scale the vector $\boldsymbol{x}$ down until one inequality becomes tight. The new vector's set of tight inequalities is a strict superset of those of the original vector, thus the point with no tight inequalities is not extreme. □

Lemma 4. *Two points $\boldsymbol{x_1}$ and $\boldsymbol{x_2}$ of the polyhedron, with $\|\boldsymbol{x_1}\| = \|\boldsymbol{x_2}\|$, correspond to defender strategies $\boldsymbol{\beta_1}$ and $\boldsymbol{\beta_2}$ respectively with $\min[\Lambda\boldsymbol{\beta_1}] = \min[\Lambda\boldsymbol{\beta_2}]$.*

Proof. If $\boldsymbol{x_1}$ and $\boldsymbol{x_2}$ have at least one tight inequality, then $\min[\Lambda\boldsymbol{x_1}] = \min[\Lambda\boldsymbol{x_2}] = 1$. Since $\min[\Lambda\boldsymbol{\beta}] = 1/\|\boldsymbol{x}\|$, $\|\boldsymbol{x}_1\| = \|\boldsymbol{x}_2\|$ immediately implies $\min[\Lambda\boldsymbol{\beta_1}] = \min[\Lambda\boldsymbol{\beta_2}]$. □

Lemma 5. *If $\|\boldsymbol{x_1}\| = \|\boldsymbol{x_2}\|$ and $\boldsymbol{\mu}'\boldsymbol{x_1} < \boldsymbol{\mu}'\boldsymbol{x_2}$, then $\boldsymbol{x_1}$ corresponds to a defender strategy $\boldsymbol{\beta_1}$ with a better defendability, i.e., $\theta(\boldsymbol{\beta_1}) > \theta(\boldsymbol{\beta_2})$.*

Proof. Since $\|\boldsymbol{x_1}\| = \|\boldsymbol{x_2}\|$, by Lemma 4 $\min[\Lambda\boldsymbol{\beta_1}] = \min[\Lambda\boldsymbol{\beta_2}]$. The definition of the defendability yields

$$\begin{aligned} \theta(\boldsymbol{\beta_1}) - \theta(\boldsymbol{\beta_2}) &= \min[\Lambda\boldsymbol{\beta_1}] - \boldsymbol{\mu}'\boldsymbol{\beta_1} - (\min[\Lambda\boldsymbol{\beta_2}] - \boldsymbol{\mu}'\boldsymbol{\beta_2}) \\ &= \boldsymbol{\mu}'\boldsymbol{\beta_2} - \boldsymbol{\mu}'\boldsymbol{\beta_1}. \end{aligned}$$

[1] If multiple extreme points of the polyhedron achieve the optimal solution, then there is an infinity of maximizers of the defendability that correspond to linear combinations of optimal extreme points.

Since $\boldsymbol{\mu}'\boldsymbol{x_1} < \boldsymbol{\mu}'\boldsymbol{x_2}$, the point $\boldsymbol{x_1}$ corresponds to a defender strategy $\boldsymbol{\beta_1}$ with a smaller false alarm cost, $\boldsymbol{\mu}'\boldsymbol{\beta_1} < \boldsymbol{\mu}'\boldsymbol{\beta_2}$. Hence $\theta(\boldsymbol{\beta_1}) > \theta(\boldsymbol{\beta_2})$. □

Lemma 6. *An extreme point $\boldsymbol{x}$ corresponding to a defender NE strategy $\boldsymbol{\beta}$ satisfies exactly one contiguous set (of indices) of tight inequalities.*

Proof. An extreme point satisfies at least one tight inequality (Lemma 3). Let s and f be the index of the first and last tight inequalities respectively and suppose that there is a loose inequality with index k between s and f (this is possible only if $f > s+1$). Since k is loose, it should be that $x_k > \frac{c_{\mathrm{a}}}{c_{\mathrm{d}}}\|\boldsymbol{x}\| > 0$ (after subtracting the loose inequality from the previous tight one). We make the following transformation

$$\hat{x}_i = \begin{cases} x_i & \text{for } i \in \{0,\dots,k-1\} \cup \{k+2,\dots,N+1\} \\ x_i - \epsilon_1 & \text{for } i = k \\ x_i + \epsilon_1 & \text{for } i = k+1, \end{cases}$$

where $\epsilon_1 > 0$ is small enough so that $\hat{x}_k \geq \frac{c_{\mathrm{a}}}{c_{\mathrm{d}}}\|\hat{\boldsymbol{x}}\|$. The transformation preserves the norm ($\|\boldsymbol{x}\| = \|\hat{\boldsymbol{x}}\|$), but $\boldsymbol{\mu}'\boldsymbol{x} > \boldsymbol{\mu}'\hat{\boldsymbol{x}}$. The latter comes from the fact that $\boldsymbol{\mu}'(\boldsymbol{x}-\hat{\boldsymbol{x}}) = \mu_k\cdot(x_k-\hat{x}_k)+\mu_{k+1}\cdot(x_{k+1}-\hat{x}_{k+1}) = \mu_k\cdot\epsilon_1+\mu_{k+1}\cdot(-\epsilon_1) = \epsilon_1\cdot(\mu_k-\mu_{k+1}) > 0$, since $\boldsymbol{\mu}$ is a strictly decreasing vector (component-wise). By Lemma 5, $\hat{\boldsymbol{x}}$ corresponds to a defender strategy with a better defendability, hence $\boldsymbol{x}$ does not correspond to a NE strategy. □

We keep the notation of the previous proof: let s and f be the indices of the first and last tight inequalities respectively.

Lemma 7. *An extreme point $\boldsymbol{x}$ that corresponds to a defender NE strategy $\boldsymbol{\beta}$ has zeros before s and after $f+1$:*

$$x_i = 0, \forall i \in \{0,\dots,s-1\} \cup \{f+2,\dots,N+1\}.$$

Proof. If $\exists i \in \{0,\dots,s-1\}$, s.t. $x_i > 0$, we reduce x_i to $\hat{x}_i$ until either $\hat{x}_i = 0$ or until the i^{th} (previously loose) inequality becomes tight, and increase x_{i+1} by the same amount. All previously tight inequalities remain tight, but we get one more tight constraint. Thus the original point was not extreme.

If $\exists i \in \{f+2,\dots,N+1\}$, s.t. $x_i > 0$, we reduce x_i until $\hat{x}_i = 0$ and increase x_{f+1} by the same amount. The previously loose $(f+1)^{\text{th}}$ inequality is made looser, all other previously loose inequalities are still loose (norm $\|\boldsymbol{x}\|$ is constant) but $\hat{\boldsymbol{x}}$ has one more tight constraint, thus $\boldsymbol{x}$ was not extreme. □

Lemma 8. *In any Nash equilibrium, $f = N$.*

Proof. Suppose that that $\boldsymbol{x}$ corresponds to a NE strategy and that $f < N$. Subtracting the tight inequality f from the loose inequality $f+1$, we get $x_{f+1} > x_m$, where $x_m = \dfrac{c_{\mathrm{a}}}{c_{\mathrm{d}}}\|\boldsymbol{x}\|$. We make the following transformation

$$\hat{x}_i = \begin{cases} x_i & \text{for } i \in \{0,\dots,f\} \cup \{f+3,\dots,N+1\} \\ x_m & \text{for } i = f+1 \\ x_{f+1} - x_m & \text{for } i = f+2. \end{cases} \tag{12}$$

With the above transformation we get

$$\begin{aligned} \boldsymbol{\mu}'(\hat{\boldsymbol{x}}-\boldsymbol{x}) &= \mu_{f+1}\cdot(\hat{x}_{f+1}-x_{f+1}) + \mu_{f+2}\cdot(\hat{x}_{f+2}-x_{f+2}) \\ &= \mu_{f+1}\cdot(x_m - x_{f+1}) + \mu_{f+2}\cdot(x_{f+1}-x_m-0) \\ &= (x_{f+1}-x_m)\cdot(\mu_{f+2}-\mu_{f+1}) \\ &< 0, \end{aligned}$$

since $x_{f+2} = 0$, $x_{f+1} > x_m$, and $\boldsymbol{\mu}$ is a strictly decreasing vector ($\mu_{f+2} < \mu_{f+1}$). Hence, for the new point $\hat{\boldsymbol{x}}$, it holds that $\|\hat{\boldsymbol{x}}\| = \|\boldsymbol{x}\|$, but $\boldsymbol{\mu}'\hat{\boldsymbol{x}} < \boldsymbol{\mu}'\boldsymbol{x}$. By Lemma 5 point $\hat{\boldsymbol{x}}$ corresponds to a defender NE strategy with a better defendability, which contradicts the assumption that $\boldsymbol{x}$ corresponds to a NE strategy. □

Lemma 9. *An extreme point $\boldsymbol{x}$ that corresponds to a defender NE strategy $\boldsymbol{\beta}$ cannot have both $x_s > 0$ and $x_{N+1} > 0$.*

Proof. By Lemmata 6–8, an extreme point $\boldsymbol{x}$ that corresponds to a defender NE strategy satisfies a contiguous block of tight inequalities with nonzero components between s through $N+1$. We make the following transformation

$$\hat{x}_i = \begin{cases} \gamma\cdot x_i & \forall i \in \{0,\dots,s-1\} \cup \{s+1,\dots,N\} \\ 0 & \text{for } i = s \\ \gamma\cdot(x_s + x_i) & \text{for } i = N+1, \end{cases} \tag{13}$$

with $\gamma = \dfrac{1}{1 - c_{\mathrm{d}}\cdot x_s} = \dfrac{1}{\|\boldsymbol{x}\|[(N-s)c_{\mathrm{a}}+\epsilon]}$. The definition of γ is such that the s^{th} inequality is still tight after the transformation: $\gamma\cdot(c_{\mathrm{d}}\cdot 0 + [(N-s)c_{\mathrm{a}}+\epsilon]\|\boldsymbol{x}\|) = 1$. The loose inequalities before s become looser with the scaling with γ ($\gamma > 1$), whereas the previously tight inequalities $s+1$ through N are still tight. Indeed, after the above transformation, any previously tight inequality with index $k \in \{s+1,\dots,N\}$ gives

$$\begin{aligned} &\gamma\,[c_{\mathrm{d}}\cdot(0 + x_{s+1} + \ldots + x_k) + [(N-s-k)c_{\mathrm{a}}+\epsilon]\|\boldsymbol{x}\|] \\ &= \gamma\,[c_{\mathrm{d}}(x_s + x_{s+1} + \ldots + x_k) + [(N-s-k)c_{\mathrm{a}}+\epsilon]\|\boldsymbol{x}\|] \\ &- \gamma\cdot c_{\mathrm{d}}\cdot x_s \text{ (after subtracting and adding } \gamma c_{\mathrm{d}} x_s) \\ &= \gamma - \gamma\cdot c_{\mathrm{d}}\cdot x_s \text{ (the } (s+1)^{\textbf{th}} \text{ inequality was tight before)} \\ &= 1 \text{ (from the definition of } \gamma). \end{aligned}$$

With the above transformation, we get an extra tight constraint ($x_s = 0$), thus the previous point was not extreme. □

Lemma 10. *For an extreme point $\boldsymbol{x}$ that corresponds to a defender NE strategy $\boldsymbol{\beta}$, we only have two possible combinations*
1. $(0,\dots,0,x_s = 0, x_{s+1} = \ldots = x_N = x_m, x_{N+1} \geq 0)$
2. $(0,\dots,0,x_s > 0, x_{s+1} = \ldots = x_N = x_m, x_{N+1} = 0)$, *where* $x_m = \dfrac{c_a}{c_d}\|\boldsymbol{x}\|$.

Proof. By Lemma 6, the inequalities s through N are tight. Subtracting any tight inequality k, $k \in \{s+1,\dots,N\}$ from the first tight inequality (s), gives $x_k = x_m$, with $x_m = \dfrac{c_{\mathrm{a}}}{c_{\mathrm{d}}}\|\boldsymbol{x}\|$. Also, by Lemma 7, $x_i = 0, \forall i \in \{0,\dots,s-1\}$.

TABLE II

DEFENDER'S STRATEGY IN NE ($\beta_m = c_{\text{A}}/c_{\text{D}}$)

#	$\dots$	β_s	β_{s+1}	$\dots$	β_N	β_{N+1}
1.	0	0	β_m	β_m	β_m	$1-(N-s)\beta_m$
2.	0	$1-(N-s)\beta_m$	β_m	β_m	β_m	0

By Lemma 9, the combination $x_s > 0$ and $x_{N+1} > 0$ is not possible, thus the only possible forms of extreme points $\boldsymbol{x}$ corresponding to defender NE strategies are the ones described above. □

Theorem 2. *A defender NE strategy $\boldsymbol{\beta}$ exists amongst the two forms in Table II for some s. If there is only one maximizing $\boldsymbol{\beta}$ amongst vectors of the form in Table II, then the Nash equilibrium is unique.*

Proof. Theorem 2 is a result of Lemmata 2 and 10. For the first type, when $x_s = 0$, the point $\boldsymbol{x}$ corresponds to a defender NE strategy $\boldsymbol{\beta}$ with $\|\boldsymbol{\beta}\| = 1$, thus $\beta_{N+1} = 1-(N-s)\cdot\beta_m$ or $\beta_{N+1} = 0$. Equivalently, for the second type, where $x_s > 0$, we have $\beta_s = 1-(N-s)\cdot\beta_m$, with $\beta_m = c_{\text{a}}/c_{\text{d}}$. Hence, the defender NE strategy $\boldsymbol{\beta}$ exists amongst the two forms of Table II. □

In the case that $(N-s)\cdot\beta_m = 1$, the two types coincide and give the same NE strategy $\boldsymbol{\beta} = (0,\dots,\beta_1 = \dots = \beta_N = \beta_m, 0)$. Then, $(N-s)\cdot c_{\text{a}} = c_{\text{d}}$ and since $s \geq 0$, the condition that needs to be satisfied is $c_{\text{d}} \leq N c_{\text{a}}$.

If the defendability LP (11) produces a unique maximizer $\boldsymbol{\beta}$, then only one of the above cases will maximize the defendability and therefore the Nash equilibrium will be unique. In the case that the solution of (11) is not unique, there is a continuum of NE, being linear combinations of the maximizing forms of extreme points. Such ties can be prevented by small perturbations to the problem (e.g., by modifying the false alarm vector $\boldsymbol{\mu}$ such that it produces a unique maximizer of the defendability).

2) Attacker's NE strategy: We have proved that in any Nash equilibrium, the defender is playing with a mix of strategies $\boldsymbol{\beta}$ that maximizes defendability. If there exists a unique maximizer $\boldsymbol{\beta}$ of the defendability and $\hat{\theta}$ is the maximum defendability, the attacker's NE strategy $\boldsymbol{\alpha}$ is uniquely derived by the following procedure. First construct a sub matrix of Λ that we call Λ_r, by keeping only the columns that correspond to the support of the defender's strategy (s through N, or $s+1$ through $N+1$, or $s+1$ through N) and rows that correspond to the support of the attacker's strategy (s through N). The defender assigns weight to $\{\beta_{\hat{s}},\dots,\beta_{N+1}\}$, according to Table II, where $\hat{s}$ optimizes the defendability. The attacker assigns positive weight to $\{\alpha_{\hat{s}},\dots,\alpha_N\}$ according to the equations

$$\boldsymbol{\alpha}' = [\mathbf{0}; \boldsymbol{\alpha}_{\boldsymbol{r}}'] \tag{14}$$

$$\boldsymbol{\alpha}_r' = (\hat{\theta}\cdot\mathbf{1}_{N-\hat{s}-1}' + \boldsymbol{\mu}_r')\cdot\Lambda_r^{-1}. \tag{15}$$

This procedure gives a unique $\boldsymbol{\alpha}$. This $\boldsymbol{\alpha}$ must be a valid probability distribution (sum to one and have non-negative elements) for if otherwise, it would contradict Nash's existence theorem.

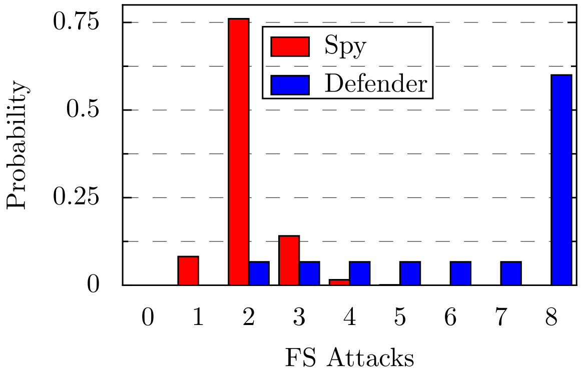

Fig. 1. (Type I) Players's best responses in NE for $N = 7,\ \theta_0 = 0.1,\ c_{\text{d}} = 15,\ c_{\text{a}} = 1,\ c_{\text{fa}} = 23,\ p = 0.2$. The bar left and right of numeral represents the spy and the defender respectively.

If there are multiple choices of $\boldsymbol{\beta}$ that maximize the defendability (and this happens either when both cases in Table II or various selections for s in the same case, give the maximal defendability), from Nash's existence theorem (and our analysis), at least one of $\boldsymbol{\beta}$ will yield an $\boldsymbol{\alpha}$ with the above procedure that corresponds to a valid probability distribution.

The complexity to find the NE is polynomial: O(N^2) to find the defendability, O(N) for each case, and O($N^2 \log N$) to invert matrix Λ_r. Since we have proved that $\boldsymbol{\beta}$ has a contiguous set of positive elements, we have reduced all the other degrees of freedom and we make only $N+1$ computations for each case to find the optimal s. For the special case that $c_{\text{d}} \leq N\cdot c_{\text{a}}$, the two forms coincide and result in the same NE.

IV. NUMERICAL RESULTS/SIMULATIONS

We conducted various experiments for different sets of parameters $N,\ c_{\text{a}},\ c_{\text{d}},\ c_{\text{fa}},$ and p, assuming that the spammer attacks with Bernoulli distribution with parameter θ_0. We followed the procedure described above to calculate the strategies of both players at equilibrium. To validate our theoretical results, we used Gambit software [12].

Figure 1 illustrates the first possible type for $N = 7$. As we can see, all the middle points are given the same weight $\beta_m = c_{\text{a}}/c_{\text{d}} = 0.0667$, $\beta_s = 0$ and $\beta_{N+1} > \beta_m$. There exists a Nash equilibrium that matches the first row of Table II with $s = 1$.

Figure 2 represents the second type of Nash equilibrium strategies for $N = 7$. All the middle points are given the same weight $\beta_m = c_{\text{a}}/c_{\text{d}} = 0.1$, but here $\beta_s > \beta_m$ ($s = 0$) and $\beta_{N+1} = 0$. Note that as p increases, larger weight is given to the smallest threshold, in order to detect the most-probable-to-exist spy.

In both figures we observe that the defender gives positive weight on larger thresholds and is not focused on a range around $N\theta_0$. Every pure strategy (threshold) in the support of the defender's NE strategy must give the defender the same payoff. The attacker's NE strategy $\boldsymbol{\alpha}$ is such that he

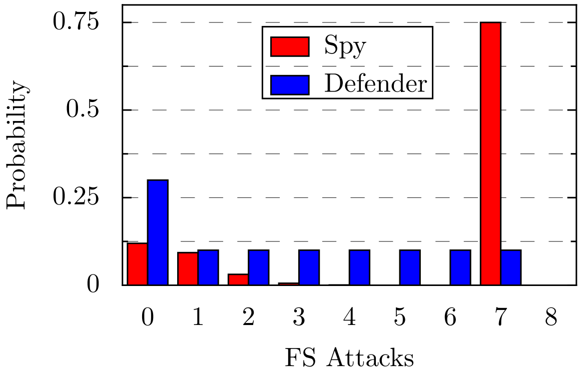

Fig. 2. (Type II) Players's best responses in NE for $N = 7,\ \theta_0 = 0.1,\ c_\text{d} = 10,\ c_\text{a} = 1,\ c_\text{fa} = 10,\ p = 0.8$. The bar left and right of numeral represents the spy and the defender respectively.

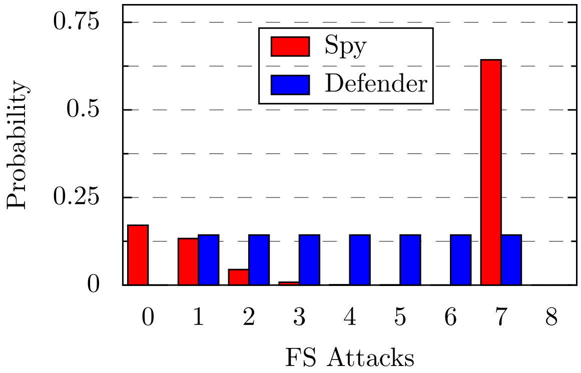

Fig. 3. Type I-II: Defender is uniform when $c_\text{d} \leq N \cdot c_\text{a}$. Other parameters are $N = 7,\ \theta_0 = 0.1,\ c_\text{a} = 1,\ c_\text{fa} = 10,\ p = 0.8,\ c_\text{d} = 7$. The bar left and right of numeral represents the spy and the defender respectively.

makes the defender's NE payoff for high thresholds the same as for lower ones. This is why the defender gives positive weight to higher thresholds, even when the probability that the spy will attack more than the threshold value is low.

Figure 3 depicts the NE in which both forms coincide, i.e., when $c_\text{d} \leq N \cdot c_\text{a}$. As we can see, the defender NE strategy is uniform and he never classifies the attacker always as spy or always as spammer.

Our simulation results indicate a match between the spy and spammer. In NE, all threshold strategies in the support of the defender give the same payoff. When the defender selects a slightly larger threshold in his support, the decrease in the false alarm cost matches the increase in the misdetection cost, i.e., $\Pr\{H = T\} = \frac{c_\text{fa}}{c_\text{d}} \frac{1-p}{p} \Pr\{Z = T\}$. Hence, the spy's NE strategy is a scaled version of the spammer's distribution. For the spammer strategies that are outside the spy's support in NE, the spy gives zero weight. The spy's NE strategy is a truncated version of the spammer's distribution, as Fig. 4 shows. When either of p or c_d or c_fa is large enough, the spy could also put some weight on the "always attack" strategy — and so that part of his strategy doesn't look like a truncated spammer distribution.

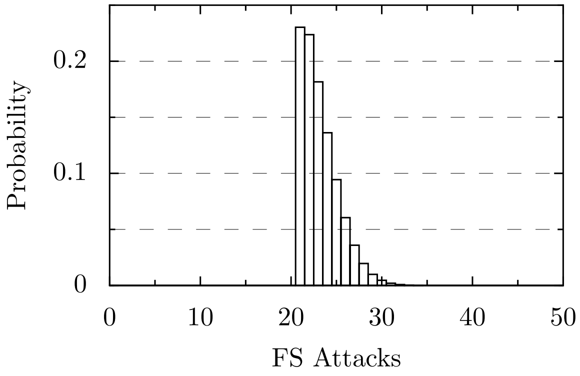

Fig. 4. Spy's NE strategy is a truncated version of spammer's distribution. Parameters: $N = 50$, $\theta_0 = 0.4$, $c_\text{d} = c_\text{fa} = 142$, $c_\text{a} = 1$, $p = 0.3$.

V. Conclusion

We investigated a classification game, where a network administrator (defender) seeks to classify an attacker as a strategic spy or a naive spammer. We showed that by taking advantage of the structure of the payoff formulation, we can characterize and anticipate the structure of the best response strategies of the two players in polynomial time. Our experimental results coincide with the theoretically expected ones: The structure of the cost matrix of the spy leads only to two forms of defender's strategies in NE. There is a relationship between the spammer's distribution and the spy's NE strategy. Furthermore, the defender NE strategy includes a contiguous set of thresholds that always include large values. If the parameters of the game satisfy a certain condition, the defender is uniformly randomizing among a set of thresholds.

References

[1] "State of Security Survey – Global Findings," Symantec, 2011.

[2] T. Alpcan, and T. Başar, "A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection," in *Proc. of the 42nd IEEE Conf. Decision and Control*, December 2003, pp. 2595–2600.

[3] A. Patcha and J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *International Journal of Network Security*, Vol. 2, No. 2, pp. 146-15, Mar. 2006.

[4] L. Chen, J. Leneutre, "A game theoretical framework on intrusion detection in heterogeneous networks," in *IEEE Transactions on Information Forensics and Security*, v.4 n.2, pp.165-178, June 2009.

[5] N. Bao, O. P. Kreidl, and J. Musacchio, "A Network Security Classification Game," in *GameNets*, April 2011.

[6] A. Gueye, J. C. Walrand, and V. Anantharam, "A Network Topology Design Game: How to Choose Communication Links in an Adversarial Environment?," in *GameNets*, April 2011.

[7] A. Gueye, "A Game Theoretical Approach to Communication Security," PhD dissertation. University of California, Berkeley, Electrical Engineering and Computer Sciences, March 2011.

[8] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, "Adverserial classification," in *International Conference on Knowledge Discovery and Data Mining (KDD)*, pp. 99–108, 2004.

[9] M. Brückner, and T. Scheffer, "Stackelberg Games for Adversarial Prediction Problems," in *KDD*, 2011.

[10] M. Brückner, and T. Scheffer, "Nash Equilibria of Static Prediction Games," in *NIPS*, 2011.

[11] D. G. Luenberger, "Linear and Nonlinear Programming." 2nd ed. Addison-Wesley, 1984.

[12] Gambit, "Gambit game theory analysis software and tools," http://www.hss.caltech.edu/gambit, 2002.

[13] J. Nash, "Non-Cooperative Games," The Annals of Mathematics 54(2):286-295, 1951.