The Title of Your Book

Your Name
Department of Computer Science
Brown University

December 3, 2022

Contents

Preface

Which labor market institutions worked better in containing job losses during the Great Recession of 2008–2009? Is it good for employment to increase the progressiveness of taxation? Does it make sense to contrast "active" and "passive" labor market policies? Who actually gains and who loses from employment protection legislation? Why are minimum wages generally diversified by age? Is it better to have decentralized or centralized bargaining systems in monetary unions? Should migrants have access to welfare benefits? Should governments regulate working hours? And can equal opportunity legislation reduce discrimination against women or minority groups in the labor market?

Current labor economics textbooks neglect these relevant policy issues. In spite of significant progress in analyzing the costs and benefits of labor market institutions, these textbooks have a setup that relegates institutions to the last paragraph of chapters or to a final institutional chapter. Typically a book begins by characterizing labor supply (including human capital theory), labor demand, and the competitive equilibrium at the intersection of the two curves; it subsequently addresses such topics as wage formation and unions, compensating wage differentials, and unemployment without a proper institutional framework. There is little information concerning labor market institutions and labor market policies. Usually labor market policies are mentioned only every now and then, and labor market institutions are often not treated in a systematic way. When attention is given to these institutions, reference is generally made to the U.S. institutional landscape and to competitive labor markets in which, by definition, any type of policy measure is distortionary.

Acknowledgments

Your acknowledgments are included in the Preface as the final section.

Your Name
March 2014

1 Green Security Game and Community Engagement[1]

Weiran Shen, Fei Fang

While game-theoretic models and algorithms have been developed to fight against illegal activities, such as poaching and over-fishing, in green security domains, none of the existing work considers the crucial aspect of community engagement: community members are recruited by law enforcement as informants and can provide valuable tips, e.g., the location of ongoing illegal activities, to assist patrols. In this chapter, we fill this gap and introduce a novel two-stage security game model for community engagement, with a bipartite graph representing the informant-attacker social network and a level-l response model for attackers inspired by cognitive hierarchy. We provide complexity results and exact, approximate, and heuristic algorithms for selecting informants and allocating patrollers against level-l ($l < \infty$) attackers; We also provide a novel algorithm to find the optimal defender strategy against level-∞ attackers. Our algorithm converts the problem of optimizing a parameterized fixed-point to a bi-level optimization problem, where the inner level is just a linear program, and the outer level has only a linear number of variables and a single linear constraint. We also evaluate the algorithms through extensive experiments.

1.1 Background

Despite the significance of protecting natural resources to environmental sustainability, a common lack of funding leads to an extremely low density of law enforcement units (referred to as defenders) to combat illegal activit ies such as wildlife poaching and overfishing (referred to as attacks).

Due to insufficient sanctions, attackers are able to launch frequent attacks [Le Gallic and Cox 2006, Leader-Williams and Milner-Gulland 1993], making it even more challenging to effectively detect and deter criminal activities through patrolling. To improve patrol efficiency, law enforcement agencies often recruit informants from local communities and plan defensive resources based on tips provided by them [Linkie et al. 2015].

[1] This chapter is adapted from the paper "Green Security Game with Community Engagement", which was originally published In Proceedings of the 18th International Conference on Autonomous Agents and Multiagent Systems.

Since attackers are often from the same local community and their activities can be observed by informants through social interactions, such tips contain detailed information about ongoing or upcoming criminal activities and, if known by defenders, can directly be used to guide allocating defensive resources. In fact, community engagement is listed by World Wild Fund for Nature as one of the *six pillars towards zero poaching* [WWF 2015]. The importance of community engagement goes beyond these green security domains about environment conservation and extends to domains such as fighting urban crimes [Gill et al. 2014, Tublitz and Lawrence 2014].

Previous research in computational game theory have led to models and algorithms that can help the defenders allocate limited resources in the presence of attackers, with applications to enforce traffic [Rosenfeld and Kraus 2017], combat oil-siphoning [Wang et al. 2018], and deceive cyber adversaries [Schlenker et al. 2018] in addition to protecting critical infrastructure [Pita et al. 2008] and combating wildlife crime [Fang et al. 2017]. However, none of the work has considered this essential element of community engagement.

Community engagement leads to fundamentally new challenges that do not exist in previous literature. First, the defender not only needs to determine how to patrol but also needs to decide whom to recruit as informants. Second, there can be multiple attackers, and the existence of informants makes the success or failure of their attacks interdependent since any tip about other attackers' actions can change the defender's patrol. Third, because of the combinatorial nature of the tips, representing the defender's strategy requires exponential space, making the problem of finding the optimal defender strategy extremely challenging. Fourth, attackers may notice the patrol pattern over time and adapt their strategies accordingly.

In this chapter, we provide the first study to fill the gap and provide a novel two-stage security game model for community engagement which represents the social network between potential informants and attackers with a bipartite graph. In the first stage of the game, the defender recruits a set of informants under a budget constraint, and in the second stage, the defender chooses a set of targets to protect based on tips from recruited informants. Inspired by the quantal cognitive hierarchy model [Wright and Leyton-Brown 2014], we use a level-l response model for attackers, taking into account the fact that the attacker can make iterative reasoning and the attacker's strategy will impact the actual marginal strategy of the defender.

Our second contribution includes complexity results and algorithms for finding an optimal defender strategy against level-l ($l < \infty$) attackers. We show that the problem of selecting the optimal set of informants is NP-Hard.

Further, based on sampling techniques, we develop an approximation algorithm to compute the optimal patrol strategy and a heuristic algorithm to find the optimal set of informants to recruit. For an expository purpose, we mainly describe the algorithms for level-0 attackers and provide a brief extension to level-l ($0 < l < \infty$) attackers in the last section of the chapter.

The third contribution is a novel algorithm to find the optimal defender strategy against level-∞ attackers, which is an extremely challenging task: an attacker's strategy may affect

the defender's marginal strategy, which in turn affects the attackers' strategies and level-∞ attackers is defined through a fixed-point argument; as a result, the defender's utility relies crucially on solving a parameterized fixed-point problem.

A naïve mathematical programming-based formulation is prohibitively large to solve. We instead reduce the program to a bi-level optimization problem, where both levels become more tractable. In particular, the inner level optimization is a linear program, and the outer level optimization is one with a linear number of variables and a single linear constraint.

Finally, we conduct extensive experiments. We compare the running time and solution quality of different algorithms. We show that our bi-level optimization algorithm achieves better performance than the algorithm adapted from previous works. We also compare level-0 attackers and the case with insider threat (i.e., the attacker is aware of the informants), where we formulate the problem as a mathematical program and solve it by adapting an algorithm from previous works. We show that the defender suffers from utility loss if the insider threat is not taken into consideration and the defender still assumes a naïve attacker model (level-0).

1.2 Literature Review

Community engagement is studied in criminology. Duffy et al. [2015], Moreto [2015], Smith and Humphreys [2015] investigate the role of community engagement in wildlife conservation. Gill et al. [2014], Linkie et al. [2015] show the positive effects of community-oriented strategies. However, they lack a mathematical model for strategic defender-attacker interactions.

Recruitment of informants has also been proposed to study societal attitudes in relation to crimes using evolutionary game theory models. Short et al. [2013] formulate the problem of solving recruitment strategies as an optimal control problem to account for limited resources and budget. In contrast to their work, we emphasize the synergy of community engagement and allocation of defensive resources and aim to find the best strategy of recruiting informants and allocating defensive resources.

In security domains, Stackelberg Security Game (SSG) has been applied to a variety of security problems [Tambe 2011], with variants accounting for alarm systems, surveillance cameras, and drones that can provide information in real time [Basilico et al. 2017, Guo et al. 2017, Ma et al. 2018]. Unlike the sensors that provide location-based information as studied in previous works, the kind of tips the informants can provide depends on their social connections, an essential feature about community engagement.

Other than the full rationality model, boundedly rational behavioral models such as quantal response (QR) [McKelvey and Palfrey 1995, Yang et al. 2012] and subjective utility quantal response [Nguyen et al. 2013] have been explored in the study of SSG. Our model and solution approach are compatible with most existing behavioral models in the SSG literature, but for an expository purpose, we only focus on the QR model.

1.3 Model

This section describes the two-stage green security game with community engagement. Compared to existing models, the key addition is the consideration of informants from local communities. They can be recruited and trained by the defender to provide tips about ongoing or upcoming attacks.

Following existing works on SSG [Jain et al. 2010, Korzhyk et al. 2011], we consider a game with a set of targets $T = [n] = \{1, \ldots, n\}$. The defender has r units of defensive resources and each can protect or cover one target with no scheduling constraint. An attacker can choose a target to attack. If target i is attacked, the defender (attacker) receives $R_i^d > 0$ ($P_i^a < 0$) if it is covered, otherwise receives $P_i^d < 0$ ($R_i^a > 0$).

Informants recruited by the defender can provide tips regarding the exact targets in ongoing or upcoming attacks but tip frequency and usefulness may vary due to heterogeneity in the informants' social connections. We model the interactions and connections between potential informants X (i.e., members of the community that are known to be non-attacker and can be recruited by the defender) and potential attackers Y using a bipartite graph $G_S = (X, Y, E)$ with $X \cap Y = \emptyset$. Here we assume the defender has access to a list of potential attackers which could be provided by the conservation site manager, since the deployment of our work relies on the manager's domain knowledge, experience, and understanding of the social connections among community members.

When an attacker decides to launch an attack, an informant who interacted with the attacker previously may know his target location. Formally, for each $v \in Y$, we assume that v will attack a target with probability p_v but the target is unknown without informants and each attacker takes actions independently. An edge $(u, v) \in E$ is associated with an information sharing intensity w_{uv}, representing the probability of attack activities of attacker v being reported by u, given v attacks and u is recruited as an informant.

In the first stage, the defender recruits k informants, and in the second stage, the defender receives tips from the informants and allocates r units of defensive resources. The defender's goal is to maximize the expected utility defined as the summation of the utilities for each attack.

Let U denote the set of recruited informants in the first stage where $|U| \leq k$, and $V = \{v \mid \exists u \in V, (u, v) \in E\}$ denote the set of attackers that are connected with at least one informant in U. We represent tips as a vector of disjoint subsets of attackers $\mathbf{V} = (V_1, \ldots, V_n)$, where V_i is the set of attackers who are reported to attack target $i \in T$ such that $V_i \subseteq V, V_i \cap V_j = \emptyset$ for any $i, j \in T$ with $i \neq j$. An attacker v is *reported* if there exists $i \in T$ such that $v \in V_i$, otherwise he is *unreported.*

Denote by $V_0 = \bigcup_{i \in T} V_i$ the set of reported attackers. It is possible that $V_0 = \emptyset$ and we say the defender is *informed* if $V_0 \neq \emptyset$. Note that $\mathbf{V}$ is a compact representation of the tips

received by the defender as it neglects the identity of the informants, which is not crucial in the defender's decision making given that all the tips are assumed to be correct.

In practice, tips are infrequent and the defender is often very protective of the informants. Thus, the attackers are often not aware of the existence of informants unless there is a significant insider threat. In addition, patrols can be divided into two categories – routine patrols and ambush patrols, where the latter are in response to tips from informants. Ambush patrols are costly, often requiring rangers to lie in wait for many hours for the possibility of catching a poacher. If not informed, the defender follows their routine patrol strategy $\mathbf{x}_0 = (x_1, \ldots, x_n)$ with x_i denoting the probability that target i is covered. Naturally, under this assumption the defender should use a strategy $\mathbf{x}_0$ that is optimal against the QR model, which can be computed by adapting the method proposed by Yang et al. [2012]. If informed, they use different strategies $\mathbf{x}(\mathbf{V})$ based on the tip $\mathbf{V}$. Assume that each attacker, if deciding to attack a target, will respond to the defender's strategy following a known behavioral model – the QR model.

We define $\mathsf{QR}(\mathbf{x}') := (q'_1, \ldots, q'_n)$, where q'_i is the probability of attacking target i defined by

$$q'_i = \frac{\exp\left(\lambda\left[x'_i P_i^a + (1 - x'_i) R_i^a\right]\right)}{\sum_{j \in T} \exp\left(\lambda\left[x'_j P_j^a + (1 - x'_j) R_j^a\right]\right)}, \tag{1.1}$$

and $\mathbf{x}'$ is the attacker's *subjective belief* of the coverage probabilities. In the above equation, $\lambda \geq 0$ is the precision parameter [McKelvey and Palfrey 1995], which is assumed known throughout the chapter. We discuss the relaxation of the some of the assumptions mentioned above in Section 1.9.

1.3.1 Level-l Response Model

Motivated by the costly ambush patrols and inspired by the cognitive hierarchy theory, we propose the level-l response model as the attackers' behavior model.

When the informants' report intensities are negligible, the attackers are almost always faced with the routine patrol $\mathbf{x}_0$. But when the informants' report intensities are not negligible, the attackers' behavior will change the marginal probability that a target is covered. Thus we assume that level-0 attackers just play the quantal response against the routine patrol $\mathbf{x}_0$: $\mathbf{q}^0 = \mathsf{QR}(\mathbf{x}_0)$. Then the defender will likely get informed with different tips $\mathbf{V}$, and respond with $\mathbf{x}(\mathbf{V})$ accordingly. Over time, the attackers will learn about the change in the frequency that a target is covered. We denote the induced defender's marginal strategy at level 0 by $\hat{\mathbf{x}}^0 = \mathsf{MS}(\mathbf{x}_0, \mathbf{x}, \mathbf{q}^0)$. After observing $\hat{\mathbf{x}}^0$ at level 0, level-1 attackers will update their strategies from $\mathbf{q}^0$ to $\mathbf{q}^1 = \mathsf{QR}(\hat{\mathbf{x}}^0)$. Similarly, attackers at level l ($0 < l < \infty$) will use quantal response against the defender's marginal strategy at level $l-1$, i.e., $\mathbf{q}^l = \mathsf{QR}(\hat{\mathbf{x}}^{l-1})$, where $\hat{\mathbf{x}}^{l-1} = \mathsf{MS}(\mathbf{x}_0, \mathbf{x}, \mathbf{q}^{l-1})$. In Section 1.6, we also define level-∞ attackers.

Denote by $\mathsf{DefEU}(U)$ the defender's optimal utility when they recruit a set of informants U and use the optimal defending strategy. The key questions raised given this model are (i) how to recruit a set U of at most k informants and (ii) how to respond to the provided tips to maximize the expected $\mathsf{DefEU}(U)$?

1.4 Defending against Level-0 Attackers

In this section, we first tackle the case where all attackers are level-0 by providing complexity results and algorithms to find the optimal set of informants. Designing efficient algorithms to solve this computationally hard problem is particularly challenging due to the combinatorial nature of the tips and exponentially many possibilities of informant selections. Furthermore, in the general case, attackers are heterogeneous and we do not know which attackers will be reported, making it hard to compute $\mathsf{DefEU}(U)$.

1.4.1 Complexity Results

Let $\mathbf{q}^0 = (q_1, \ldots, q_n)$. Before presenting our complexity results, we first define some useful notations. Given the set of informants U and the tips $\mathbf{V} = (V_1, \ldots, V_n)$, we denote by $\tilde{p}_v(V_0)$ the probability of $v \in Y$ attacking a target given V_0 such that $V_0 = \bigcup_{i \in T} V_i$. We can compute $\tilde{p}_v(V_0)$ with

$$\tilde{p}_v(V_0) = \begin{cases} 1 & v \in V_0 \\ \frac{(1-\tilde{w}_v)p_v}{(1-\tilde{w}_v)p_v + 1 - p_v} & v \in V \setminus V_0 \\ p_v & v \in Y \setminus V \end{cases},$$

where $\tilde{w}_v = 1 - \prod_{(u,v) \in E, u \in U}(1 - w_{uv})$ is the probability of v being reported conditioned on that v attacks. Given V_0 and $t_i = |V_i|$ reported attacks on each target i, we compute the expected utility of covering i by $\mathsf{EU}_i^c(t_i, V_0) := \left(t_i + q_i \sum_{v \in Y \setminus V_0} \tilde{p}_v(V_0)\right) R_i^d$. The expected utility $\mathsf{EU}_i^u(t_i, V_0)$ of not covering i can also be computed similarly. Then, the expected gain of covering the target can be written as $\mathsf{EG}_i(t_i, V_0) := \mathsf{EU}_i^c(t_i, V_0) - \mathsf{EU}_i^u(t_i, V_0)$.

Theorem 1.1. *When the defender is informed by informants U, the optimal allocation of defensive resources can be determined in $O(|Y| + n)$ time given the tips $\mathbf{V} = (V_1, \ldots, V_n)$.*

Given tips from recruited informants, the defender can find the optimal resource allocation by greedily protecting the targets with the highest expected gains.

Proof. Given the tips $\mathbf{V}$, the defender should calculate $\mathsf{EG}_i(|V_i|, V_0)$ for each target $i \in T$, and then allocate the resources to r targets with the highest expected utility gains.

The above strategy is indeed optimal since the expected utility with no resources is given by $\sum_{i \in T} \mathsf{EU}_i^u(|V_i|, V_0)$, and once an additional unit of resource is given, it should always be allocated to the uncovered target that could lead to the largest increment in expected utility, i.e., the target with the largest $\mathsf{EG}_i(|V_i|, V_0)$.

The calculation of $\mathsf{EG}_i(|V_i|, V_0)$ for each $i \in T$ can be done in $O(n+|Y|)$ time, and finding the r largest $\mathsf{EG}_i(|V_i|, V_0)$ can be done in $O(n)$ time, leading to the overall complexity of $O(|Y|+n)$. □

However, the problem of computing the optimal set of informants is still hard.

Theorem 1.2. *Computing the optimal set of informants to recruit is NP-Hard.*

Proof. Consider the case where $r = 1$, $\lambda = 0$, and $p_v = w_{uv} = 1$ for all u, v, and the targets are uniform i.e., R_i^d's (R_i^a, P_i^d, P_i^a) are the same for all $i \in T$. We use the notation R^d (P^d) instead of R_i^d (P_i^d) for simplicity.

To start with, we investigate how $\mathsf{DefEU}(U)$ depends on a given U. Since $p_v = 1$ and $w_{uv} = 1$ for all $u \in X, v \in Y$, all attackers in V will be reported to attack a location. Let random variable $X_i = |V_i|$ be the number of attackers who are reported to attack location i. Since the targets are uniform, an attacker will attack each location with probability $q_i = \frac{1}{n}$ if they decide to attack. Then the defender's expected utility $\mathsf{DefEU}(U)$ could be written as

$$\begin{aligned}\mathsf{DefEU}(U) &= \left(\mathbb{E}\left[\max_{i\in T} X_i\right] + \frac{|Y|-|V|}{n}\right) R^d + \left(|V| - \mathbb{E}\left[\max_{i\in T} X_i\right] + \frac{n-1}{n}(|Y|-|V|)\right) P^d \\ &= \left(\mathbb{E}\left[\max_{i\in T} X_i\right] - \frac{|V|}{n}\right)\left(R^d - P^d\right) + \frac{|Y|}{n}R^d + \frac{(n-1)|Y|}{n}P^d.\end{aligned}$$

The latter two terms are independent of the choice of informants. Therefore, to maximize DefEU, it suffices the maximize $\mathbb{E}\left[\max_{i\in T} X_i\right] - \frac{|V|}{n}$.

We can prove by induction on $|V|$ that $\mathbb{E}\left[\max_{i\in T} X_i\right] - \frac{|V|}{n}$ increases as $|V|$ increases, or $\mathbb{E}\left[\max_{i\in T} X_i\right]$ increases by at least $\frac{1}{n}$ if $|V|$ is increased by 1:

1. Since $\mathbb{E}\left[\max_{i\in T} X_i\right] = 1$ when $|V| = 1$, and $\mathbb{E}\left[\max_{i\in T} X_i\right] = 1 + \frac{1}{n}$ when $|V| = 2$, the above statement holds for $|V| = 1$.
2. Consider the case with $|V| \geq 1$ and the corresponding sequence $\{X_i\}_{i=1}^n$. Let $X_m = \max_{1\leq i\leq n}\{X_i\}$. We add an attacker to V and denote by p the probability of the attacker targeting the location with the largest X_i. Thus $\mathbb{E}\left[\max_{i\in T} X_i\right]$ increases by p, where we know $p \geq \frac{1}{n}$.

Thus, in this case, solving for the optimal solution of the original problem is equivalent to solving for U that maximizes the size of V in the first stage.

We show that the optimization problem is NP-Hard using a reduction from the maximum coverage problem (MCP): we are given a number k and a collection of sets S. The objective is to find a subset $S' \subseteq S$ of sets such that $|S'| \leq k$ and the number of covered elements $\left|\bigcup_{S_i\in S'} S_i\right|$ is maximized. Let $X = \{x_1, \ldots, x_{|S|}\}$, $Y = \bigcup_{S_i\in S} S_i$, $E = \{(x_i, y) : i \in [|S|] \wedge y \in S_i\}$, $p_v = 1$ for all $v \in Y$ and $W_e = 1$ for all $e \in E$. Thus to find a $U \subseteq X$ with $|U| \leq k$ that maximizes the size of V is equivalent to finding a subset of sets with size no larger than k that maximizes the number of covered elements in the instance of MCP. □

1.4.2 Finding the Optimal Set of Informants

We now develop exact and heuristic informant selection algorithms to compute the optimal set of informants. To find the U that maximizes $\mathsf{DefEU}(U)$, we first focus on computing $\mathsf{DefEU}(U)$. We provide a dynamic programming-based algorithm, as well as approximate algorithms.

1.4.2.1 Calculating $\mathsf{DefEU}(U)$

Let DefEU_0 be the defender's expected utility when using the optimal patrol strategy against a single attacker in the case with no informants, which can be obtained by using the algorithms introduced by Yang et al. [2012]. Then $\mathsf{DefEU}(U)$ can be explicitly written as

$$\mathsf{DefEU}(U) = \Pr[V_0 = \emptyset]\mathsf{DefEU}_0 + \Pr[V_0 \neq \emptyset]\mathsf{E}\left[\sum_{i\in[n]} \mathbf{x}_i(V)\mathsf{EG}_i(t_i, V_0) + \mathsf{EU}_i(t_i, V_0)\middle| V_0 \neq \emptyset\right].$$

Directly computing $\mathsf{DefEU}(U)$ with the above equation is formidable due to exponentially many tip combinations. However, it is possible to reduce the amount of enumerations by handling the calculation carefully. We first develop an Enumeration and Dynamic Programming-based Algorithm (EDPA) to compute the exact $\mathsf{DefEU}(U)$ as shown in Algorithm 1.

First, we compute the utility of the defender when they are not informed (lines 4-6). Then, we focus on calculating the total utility $\mathsf{DefEU}'(U)$ in the case when the defender is informed. By the linearity of expectation, $\mathsf{DefEU}'(U)$ is just the summation of the expected utility obtained from all targets. Therefore, we focus on the calculation of the expected utility of a single target i. For each target i, Algorithm 1 enumerates all possible types of tips (lines 2-7). We denote each type of tip by a tuple (t_i, V_0), which encodes the set of reported attackers $V_0 \neq \emptyset$ and the number of reported attackers t_i targeting location i. The probability of receiving (t_i, V_0) can be written as

$$\Pr(t_i, V_0|U) = P_{V_0}\binom{|V_0|}{t_i} q_i^{t_i}(1-q_i)^{|V_0|-t_i},$$

where

$$P_{V_0} = \prod_{v\in V_0}(\tilde{w}_v p_v) \prod_{v\in V\setminus V_0}(1-\tilde{w}_v p_v) \tag{1.2}$$

is the probability of having V_0 as the set of reported attackers given U (line 3). Let $P_{i,r}$ be the probability of i being among the r targets with the highest expected gain given (t_i, V_0) and U (lines 12-13). For any tip tuple (t_i, V_0), the expected contribution to $\mathsf{DefEU}'(U)$ of target i is

$$\begin{aligned}&\Pr(t_i, V_0|U)\cdot\mathsf{EU}_i(t_i, V_0) + P_{V_0}\binom{|V_0|}{t_i} q_i^{t_i}\cdot P_{i,r}\mathsf{EG}_i(t_i, V_0)\\ =&P_{V_0}\binom{|V_0|}{t_i} q_i^{t_i}\left[(1-q_i)^{|V_0|-t_i}\mathsf{EU}_i(t_i, V_0) + P_{i,r}\mathsf{EG}_i(t_i, V_0)\right].\end{aligned}$$

Algorithm 1: Calculate $\mathsf{DefEU}(U)$.

1 $\mathsf{EU} \leftarrow 0$;
2 **forall** *possible sets of reported attackers* $V_0 \subseteq V$ **do**
3 $\quad P_{V_0} \leftarrow \prod_{v\in V_0}(\tilde{w}_v p_v)\prod_{v\in V\setminus V_0}(1-\tilde{w}_v p_v)$;
4 $\quad$ **if** $V_0 = \emptyset$ **then**
5 $\quad\quad \mathsf{EU} \leftarrow \mathsf{EU} + P_{V_0}\sum_{v\in Y}\tilde{p}_v(V_0)\mathsf{DefEU}_0$;
6 $\quad\quad$ Continue to line 2;
7 $\quad$ **end**
8 $\quad$ **for** *target* $i \in T$ *and* $0 \le t_i \le |V_0|$ **do**
9 $\quad\quad$ Calculate $f(\cdot)$ given $|V_0|, i, t_i$;
10 $\quad\quad \mathsf{EG}_i \leftarrow (t_i + q_i\sum_{v\in Y\setminus V_0}\tilde{p}_v(V_0))(R_i^d - P_i^d)$;
11 $\quad\quad \mathsf{EU}_i^u \leftarrow (t_i + q_i\sum_{v\in Y\setminus V_0}\tilde{p}_v(V_0))P_i^d$;
12 $\quad\quad P_{i,r} \leftarrow (|V_0|-t_i)!\left(\sum_{x=0}^{r-1} f(s,x,|V_0|-t_i)\right)$;
13 $\quad\quad \mathsf{EU} \leftarrow \mathsf{EU} + P_{V_0}\binom{|V_0|}{t_i} q_i^{t_i}\cdot P_{i,r}\cdot \mathsf{EG}_i$;
14 $\quad\quad \mathsf{EU} \leftarrow \mathsf{EU} + P_{V_0}\binom{|V_0|}{t_i} q_i^{t_i}(1-q_i^{t_i})\mathsf{EU}_i^u$;
15 $\quad$ **end**
16 **end**
17 $\mathsf{DefEU}(U) \leftarrow \mathsf{EU}$;

We can then compute $\mathsf{DefEU}'(U)$ by summing over all possible $t_i, V_0 \neq \emptyset$.

The calculation of $P_{i,r}$ is all that remains. This can be done very efficiently via Algorithm 2, a dynamic programming-based calculation. Let $f(s,x,y)$ be such that $y!\cdot f(s,x,y)$ is the probability of having y reported attacks among the first s targets with x of the targets having expected gain higher than EG_i given the tips of type (t_i, V_0). Therefore, $f(s,x,y)$ can be neatly written as

$$f(s,x,y) \quad = \sum_{\substack{a_1+\cdots+a_s=y,\\ \sum_{j=1}^{s}\mathbf{1}_{[\mathsf{EG}_{i_j}(a_j,V_0)>\mathsf{EG}_i(t_i,V_0)]}=x}} \frac{q_{i_1}^{a_1}q_{i_2}^{a_2}\cdots q_{i_s}^{a_s}}{a_1!a_2!\cdots a_s!},$$

which can be calculated using dynamic programming (line 5-11). We can compute $f(s,x,y)$ accordingly by counting the number of s-partitions on integer y, where we also consider the constraint brought in by the limited number of resources. To calculate $f(s,x,y)$, we enumerate a_s as $\tilde{y}$ (line 6) and compare $\mathsf{EG}_{i_s}(a_s,V_0)$ with $\mathsf{EG}_i(t_i,V_0)$ (line 8). If $\mathsf{EG}_{i_s}(a_s,V_0) > \mathsf{EG}_i(t_i,V_0)$, we check the value of $f(s-1,x-1,y-\tilde{y})$ (line 9). Otherwise, we check $f(s-1,x,y-\tilde{y})$ (line 11). Thus, we have $P_{i,r} = (|V_0|-t_i)!\left(\sum_{x=0}^{r-1} f(s,x,|V_0|-t_i)\right)$. Therefore, the time complexity for Algorithm 1 and 2 is $O(2^{|Y|}n^2r|Y|^3)$ and $O(nr|Y|^2)$, respectively.

Algorithm 2: Calculate $f(\cdot)$ given $|V_0|, i, t_i$.

$\mathsf{EG}_i \leftarrow (t_i + q_i \sum_{v \in Y \setminus V_0} \tilde{p}_v(V_0))(R_i^d - P_i^d)$;
Initialize $f(s,x,y) \leftarrow 0$ for all s,x,y;
$f(0,0,0) \leftarrow 1$;
for *s in* $[1, n-1]$, *x in* $[0, \min(s,r)]$, *y in* $[0, |V_0| - t_i]$ **do**
  for $\tilde{y}$ *in* $[0,y]$ **do**
    $\mathsf{EG}_{i_s} \leftarrow (\tilde{y} + q_{i_s} \sum_{v \in Y \setminus V_0} \tilde{p}_v(V_0))(R_{i_s}^d - P_{i_s}^d)$;
    if $\mathsf{EG}_{i_s} > \mathsf{EG}_i$ **then**
      $f(s,x,y) \leftarrow f(s,x,y) + \frac{q_{i_s}^{\tilde{y}}}{\tilde{y}!} f(s-1, x-1, y-\tilde{y})$;
    else
      $f(s,x,y) \leftarrow f(s,x,y) + \frac{q_{i_s}^{\tilde{y}}}{\tilde{y}!} f(s-1, x, y-\tilde{y})$;
    end
  end
end

Since EDPA runs in exponential time, we introduce approximation methods to estimate $\mathsf{DefEU}(U)$. Let $\mathsf{DefEU}(U,C)$ be the estimated defender's utility returned by only enumerating subsets V_0 with $|V_0| < C$ in Algorithm 1. We denote by C-TRUNCATED this approach of estimating $\mathsf{DefEU}(U)$. Next, we show that $\mathsf{DefEU}(U,C)$ is close to the exact $\mathsf{DefEU}(U)$ when it is unlikely to have many attacks happening at the same time. Formally, assume that the expected number of attacks is bounded by a constant C', that is $\sum_{v \in Y} p_v \leq C'$, $\mathsf{DefEU}(U,C)$ for $C > C'$ is an estimation of $\mathsf{DefEU}(U)$ with bounded error.

Lemma 1.1. *Assume that* $\sum_{v \in Y} p_v \leq C'$ *and* $|P_i^d|, |R_i^d| \leq Q$, *the error of estimation* $|\mathsf{DefEU}(U,C) - \mathsf{DefEU}(U)|$ *for* $C > C'$ *is at most:*

$$Q \cdot \exp\left(\frac{-2(C-C')^2}{|Y|}\right)\left(C + \frac{1}{1 - \exp\left(-4(C-C')/|Y|\right)}\right).$$

Proof. Let the random variable W be the number of attacks. Let $\mathcal{A}_1$ be the set of events of having no less than C reported attackers and $\mathcal{A}_2$ be the set of events of having no less than C attacks. Let E_A be the expected defender's utility taken over all possible tips given an event A. By noticing that $\mathcal{A}_1 \subseteq \mathcal{A}_2$, we have

$$|\mathsf{DefEU}(U) - \mathsf{DefEU}(U,C)| \leq \sum_{A \in \mathcal{A}_1} \Pr[A]|E_A| \leq \sum_{A \in \mathcal{A}_2} \Pr[A]|E_A| \leq Q \sum_{i=C}^{|Y|} \Pr[W=i] \cdot i \quad (1.3)$$

Note that

$$\begin{aligned}\sum_{i=C}^{|Y|}\Pr[W=i]\cdot i =& C\cdot\Pr[W\geq i]+\sum_{i=C+1}^{|Y|}\Pr[W=i]\cdot(i-C)\\ =& C\cdot\Pr[W\geq i]+\sum_{i=C+1}^{|Y|}\Pr[W=i]\cdot\sum_{j=C+1}^{i}1.\end{aligned}$$

By switching the order of summation in the last term, we have

$$\sum_{i=C}^{|Y|}\Pr[W=i]\cdot i = C\cdot\Pr[W\geq i]+\sum_{j=C+1}^{|Y|}\sum_{i=j}^{|Y|}\Pr[W=i] = C\cdot\Pr[W\geq i]+\sum_{j=C+1}^{|Y|}\Pr[W\geq j]$$

Plugging back into Equation (1.3), we get

$$\begin{aligned}|\mathsf{DefEU}(U)-\mathsf{DefEU}(U,C)| \leq& Q\left(C\cdot\Pr[W\geq i]+\sum_{i=C+1}^{|Y|}\Pr[W\geq i]\right)\\ \leq& Q\left[C\cdot\exp\left(\frac{-2(C-C')^2}{|Y|}\right)+\sum_{i=C+1}^{|Y|}\exp\left(\frac{-2(i-C')^2}{|Y|}\right)\right]\\ <& Q\cdot\exp\left(\frac{-2(C-C')^2}{|Y|}\right)\left(C+\frac{1}{1-\exp\left(-4(C-C')/|Y|\right)}\right),\end{aligned}$$

where the second inequality follows from the Chernoff Bound, and the last inequality holds since

$$\begin{aligned}\sum_{i=C+1}^{|Y|}\exp\left(\frac{-2(i-C')^2}{|Y|}\right) \leq& \exp\left(\frac{-2(C+1-C')^2}{|Y|}\right)\sum_{i\geq 0}\exp\left(\frac{-4i(C+1-C')}{|Y|}\right)\\ <& \exp\left(\frac{-2(C-C')^2}{|Y|}\right)\cdot\frac{1}{1-\exp\left(-4(C-C')/|Y|\right)}.\end{aligned}$$

□

Following analyses similar to that of Algorithm 1 and 2, it is not difficult to see that the time complexity of C-TRUNCATED is $O(n^2r|Y|^{C+3})$. However, for the case where $\sum_{v\in Y}p_v$ is large, we have to set C to be larger than $\sum_{v\in Y}p_v$ for C-TRUNCATED in order to obtain a high-quality solution; otherwise the error will become unbounded. To mitigate this limitation, we also propose an alternative sampling approach, M-SAMPLING, to estimate $\mathsf{DefEU}(U)$ for general cases without restrictions on $\sum_{v\in Y}p_v$. Instead of enumerating all possible V_0 as EDPA does, in M-SAMPLING, we draw M i.i.d. samples of the set of reported attackers where each sample V_0 is drawn with probability P_{V_0}. M-SAMPLING averages over all the samples to estimate $\mathsf{DefEU}(U)$. We can sample V_0 as follows:

1. Let $V_0=\emptyset$ initially;
2. For each $v\in V$, add v to V_0 with probability $\tilde{w}_v p_v$;

3. Return V_0 as a sample of the set of reported attackers.

From Equation (1.2), the above sampling process is consistent with the distribution of V_0. M-SAMPLING returns an estimation of $\mathsf{DefEU}(U)$ in $O(Mn^2r|Y|^3)$ time.

Proposition 1.1. *Let* $\mathsf{DefEU}^{(M)}(U)$ *be the estimation of* $\mathsf{DefEU}(U)$ *given by* M-SAMPLING *using M samples. We have:* $\lim_{M\to\infty}\mathsf{DefEU}^{(M)}(U)=\mathsf{DefEU}(U)$

1.4.2.2 Selecting Informants U

Given the algorithms for computing $\mathsf{DefEU}(U)$, a straightforward way of selecting informants is through enumeration (denoted by SELECT).

When using C-TRUNCATED as a subroutine to compute $\mathsf{DefEU}(U)$, the solution quality of the selected set of informants is guaranteed by the following theorem.

Theorem 1.3. *Assume that* $\sum_{v\in Y}p_v\le C'$ *and* $|P_i^d|,|R_i^d|\le Q$. *Let* U_{OPT} *and* U' *be the optimal set of informants and the one chosen by* C-TRUNCATED. *Then for* $C>C'$, *the error* $|\mathsf{DefEU}(U_{\mathsf{OPT}})-\mathsf{DefEU}(U')|$ *can be bounded by:*

$$2Q\cdot\exp\left(\frac{-2(C-C')^2}{|Y|}\right)\left(C+\frac{1}{1-\exp(-4(C-C')/|Y|)}\right).$$

Proposition 1.2. *Using* M-SAMPLING *to estimate* DefEU, *the optimal set of informants can be found when* $M\to\infty$.

Algorithm 3: $\mathsf{Search}(U')$.

```
if |U'| = k then
    Update OPT with (U', DefEU(U'));
    return;
end
u_1 ← arg max_{u∈X} DefEU(U' ∪ {u});
u_2 ← arg max_{u∈X\{u_1}} DefEU(U' ∪ {u});
Search(U' ∪ {u_1}), Search(U' ∪ {u_2});
```

Based on existing results in submodular optimization [Nemhauser et al. 1978], one may expect a greedy algorithm that step by step adds an informant that leads to the largest utility to work well. However, the set function $\mathsf{DefEU}(U)$ in our problem violates submodularity and such greedy algorithm will not guarantee an approximation ratio of $1-1/e$. Consider the following example:

Example 1.1. *Consider a network* $G_S=(X,Y,E)$ *where* $X=\{u_1,u_2\}$, $Y=\{v_1,v_2,v_3\}$, $E=\{(u_1,v_2),(u_2,v_3)\}$, $p_v=1\,\forall v\in Y$ *and* $w_{uv}=1\,\forall(u,v)\in E$. *There are 2 targets* $T=\{1,2\}$, *where* $R_i^d=i$, $P_i^d=-10^{-8}\approx 0$ *for any* $i\in T$. *Letting* $\lambda=0$ *yields* $q_i=0.5$. *The*

defender has only 1 resource. We can see that $\mathsf{DefEU}(\emptyset) = \mathsf{DefEU}(\{1\}) = \mathsf{DefEU}(\{2\}) = 3$, $\mathsf{DefEU}(\{1,2\}) = \frac{1}{4}(2+0.5) + \frac{1}{4}(4+1) + \frac{1}{2}(2+1) = 3.375$. *As a result,* $\mathsf{DefEU}(\{1,2\}) + \mathsf{DefEU}(\emptyset) > \mathsf{DefEU}(\{1\}) + \mathsf{DefEU}(\{2\})$.

Therefore, we propose GSA (Greedy-based Search Algorithm) for the selection of informants as shown in Algorithm 3. GSA starts by calling $\mathsf{Search}(\emptyset)$. While $|U'| < k$, $\mathsf{Search}(U')$ expands the current set of informants U' by adding u_1, u_2 to U' and recursing, where u_1 and u_2 are the two informants that give the largest marginal gain in DefEU (line 4-5); Otherwise, it updates the optimal solution with U' (line 1-3).

We identify a tractable case to conclude the section.

Lemma 1.2. *Given the set of recruited informants U, the defender's expected utility* $\mathsf{DefEU}(U)$ *can be computed in polynomial time if $w_{uv} = 1 \forall (u,v) \in E$. When k is a constant, the optimal set of informants can be computed in polynomial time.*

Proof. Since $w_{uv} = 1$ for all u, v, we have $\tilde{p}_v(V_0) = 0$ for each $v \in V \setminus V_0$ given V_0. Therefore, the expected gain of target j with $\tilde{y}$ reported attacks can be written as $\mathsf{EG}_j = (\tilde{y} + q_j \sum_{v \in Y \setminus V} p_v)(R_j^d - P_j^d)$ and the calculation of $f(\cdot)$ depends only on the size of $|V_0|$. Thus, instead of enumerating V_0, we enumerate $0 \le t_0 \le |V|$ as the size of V_0 in line 2 of Algorithm 1, and replace P_{V_0} in Algorithm 1 with P_{t_0}, where $P_{t_0} = \Pr[|V_0| = t_0 | U]$ can be obtained by expanding the following polynomial $\prod_{v \in V}(1 - p_v + p_v x) = \sum_{i=0}^{|V|} P_i x^i$. Therefore, $\mathsf{DefEU}(U)$ can be calculated in $O(n^2 r |Y|^4)$ time.

Since all possible U can be enumerated in $O(|X|^k)$, the optimal set of informants can be computed in $O(|X|^k n^2 r |Y|^4)$. □

This represents the case where the informants have strong connections with a particular group of attackers and can get full access to their attack plans. We refer to the property of $w_{uv} = 1$ for all u, v as SISI (Strong Information Sharing Intensity). Denote by ASISI (Algorithm for SISI) the polynomial-time algorithm described in Lemma 1.2. We provide detailed descriptions of ASISI in Algorithm 4 and Algorithm 5.

We summarize the time complexity of all algorithms for computing the optimal U in the following table:

1.5 Defending Against Level-l Attackers

In the section 1.4, we consider the case with only level-0 attackers and provide algorithms to find the optimal set of informants to recruit. In this section, we show how those approaches can be easily extended to the case with level-l attackers.

Once given $\hat{\mathbf{x}}^{l-1}$, $\mathbf{q}^l$ can be easily obtained. So as DefEU_l, the defender's expected utility using $\mathbf{x}_0$ against a single attack of a level-l attacker. To get the solution, we simply replace $\mathsf{DefEU}_0, \mathbf{q}^0$ with $\mathsf{DefEU}_l, \mathbf{q}^l$ and apply algorithm SELECT or GSA. In order to calculate $\hat{\mathbf{x}}^{l-1}$,

Algorithm 4: Calculate $\mathsf{DefEU}(U)$.

1 Expand polynomial $\prod_{v\in V}(1-p_v+p_v x)=\sum_{j=0}^{|V|}P_j x^j$;
2 $\mathsf{EU}\leftarrow 0$;
3 **forall** *possible number of reported attackers* $0\le t_0\le |V|$ **do**
4 **if** $t_0=0$ **then**
5 $\mathsf{EU}\leftarrow \mathsf{EU}+P_{t_0}\sum_{v\in Y}p_v\mathsf{DefEU}_0$;
6 Continue to line 3;
7 **end**
8 **for** *target* $i\in T$ *and* $0\le t_i\le t_0$ **do**
9 Calculate $f(\cdot)$ given t_0,i,t_i;
10 $\mathsf{EG}_i\leftarrow (t_i+q_i\sum_{v\in Y\setminus V}p_v)(R_i^d-P_i^d)$;
11 $\mathsf{EU}_i^u\leftarrow (t_i+q_i\sum_{v\in Y\setminus V}p_v)P_i^d$;
12 $P_{i,r}\leftarrow (t_0-t_i)!\left(\sum_{x=0}^{r-1}f(s,x,t_0-t_i)\right)$;
13 $\mathsf{EU}\leftarrow \mathsf{EU}+P_{t_0}\binom{t_0}{t_i}q_i^{t_i}\cdot P_{i,r}\cdot EG_i$;
14 $\mathsf{EU}\leftarrow \mathsf{EU}+P_{t_0}\binom{t_0}{t_i}q_i^{t_i}(1-q_i^{t_i})\mathsf{EU}_i^u$;
15 **end**
16 **end**
17 $\mathsf{DefEU}(U)\leftarrow \mathsf{EU}$;

all that remains is to calculate $\mathsf{MS}(\mathbf{x}_0,\mathbf{x},\mathbf{q}^i)$ for $i<l$. The marginal probability of each target being covered can be calculated in a way similar to EDPA.

1.6 Defending Against Level-∞ Attackers

As discussed in Section 1.3.1, a level-l attacker may keep adapting to the new marginal strategy formed by his current level of behavior. In this section, we first show in Theorem 1.4 that there exists a fixed-point strategy for the attacker in our level-l response model, and then use that to define the level-∞ attackers.

We formulate the problem of finding the optimal defender's strategy for this case as a mathematical program. However, such a program can be too large to solve. We propose a novel technique that reduces the program to a bi-level optimization problem, with both levels much more tractable.

Theorem 1.4. *Let* $\Delta_n=\{\mathbf{q}\mid \mathbf{q}\in[0,1]^n,\mathbf{1}^M\mathbf{q}\le 1\}$. *Given defender's strategies* $\mathbf{x}_0$ *and* $\mathbf{x}(\mathbf{V})$, *there exists* $\mathbf{q}^*\in\Delta_n$ *such that* $\mathbf{q}^*=\mathsf{QR}(\mathsf{MS}(\mathbf{x}_0,\mathbf{x},\mathbf{q}^*))$.

Proof. Since Δ_n is a compact convex set and $\mathsf{QR}(\mathsf{MS}(\mathbf{x}_0,\mathbf{x},\mathbf{q}^*))$ is a continuous function of $\mathbf{q}$, by Brouwer fixed-point theorem, there exists $\mathbf{q}^*\in\Delta_n$ such that $\mathbf{q}^*=\mathsf{QR}(\mathsf{MS}(\mathbf{x}_0,\mathbf{x},\mathbf{q}^*))$. □

Algorithm 5: Calculate $f(\cdot)$ given t_0,i,t_i.

$\{i_1,\ldots,i_{n-1}\} \leftarrow T \setminus \{i\}$;
$\mathsf{EG}_i = (t_i + q_i \sum_{v\in Y\setminus V} p_v)(R_i^d - P_i^d)$;
Initialize $f(s,x,y) \leftarrow 0$ for all s,x,y;
$f(0,0,0) \leftarrow 1$;
for $s \leftarrow 1$ *to* $n-1$ **do**
  for $x \leftarrow 0$ *to* $\min(s,r)$ **do**
    for $y \leftarrow 0$ *to* $t_0 - t_i$ **do**
      for $\tilde{y} \leftarrow 0$ *to* y **do**
        $\mathsf{EG}_{i_s} = (\tilde{y} + q_{i_s} \sum_{v\in Y\setminus V} p_v)(R_i^d - P_i^d)$;
        if $\mathsf{EG}_{i_s} > \mathsf{EG}_i$ **then**
          $f(s,x,y) \leftarrow f(s,x,y) + \frac{q_{i_s}^{\tilde{y}}}{\tilde{y}!} f(s-1,x-1,y-\tilde{y})$;
        else
          $f(s,x,y) \leftarrow f(s,x,y) + \frac{q_{i_s}^{\tilde{y}}}{\tilde{y}!} f(s-1,x,y-\tilde{y})$;
        end
      end
    end
  end
end

Algorithm	Time Complexity
EDPA	$O(\lvert X\rvert^k 2^{\lvert Y\rvert} n^2 r \lvert Y\rvert^3)$
C-TRUNCATED	$O(\lvert X\rvert^k n^2 r \lvert Y\rvert^{C+3})$
M-SAMPLING	$O(\lvert X\rvert^k M n^2 r \lvert Y\rvert^3)$
ASISI	$O(\lvert X\rvert^k n^2 r \lvert Y\rvert^4)$
GSA	$O(2^k \lvert X\rvert n^2 r \lvert Y\rvert^3)$

Table 1.1: Complexity of Different Algorithms

According to the definition of level-l attackers, we have $\mathbf{q}^{l+1} = \mathsf{QR}(\mathsf{MS}(\mathbf{x}_0,\mathbf{x},\mathbf{q}^l))$. Slightly generalizing the definition, we define a level-∞ attacker as:

Definition 1.1 (level-∞ attacker)**.** *Given the defender's strategies* $\mathbf{x}_0$ *and* $\mathbf{x}(\mathbf{V})$*, the strategy* $\mathbf{q}$ *of a level-*∞ *attacker satisfies* $\mathbf{q} = \mathsf{QR}(\mathsf{MS}(\mathbf{x}_0,\mathbf{x},\mathbf{q}))$.

Remark 1.1. *Note that Definition 1.1 is not obtained by taking the limit of the level-l definition, since such a limit may not even exist. Consider an example where there is a single attacker and two targets with the following payoffs:*

$$R_1^a = 0.6, R_2^a = 0.8,$$
$$P_1^a = -0.8, P_2^a = -0.6.$$

In this case, there are only two possible tips: the attacker attacks target 1 ($\mathbf{V}_1$), and the attacker attacks 2 ($\mathbf{V}_2$). Assume that only 1 informant is recruited with report probability $w = 0.5$. The defender has only 1 defensive resource and uses the following strategy:

$$\mathbf{x}_0 = (0.5, 0.5), \mathbf{x}(\mathbf{V}_1) = (1.0, 0.0), \mathbf{x}(\mathbf{V}_2) = (0.0, 1.0).$$

When the attacker has $\lambda = 2.9$, the level-l response will converge to $\mathbf{q} = (0.4283, 0.5717)$. However, if $\lambda = 3.0$, then the process will eventually oscillate between $\mathbf{q} = (0.2924, 0.7076)$ and $\mathbf{q}' = (0.5676, 0.4324)$ iteratively.

Remark 1.2. *Although the level-∞ attacker is defined through a fixed point argument, we still stick to the Stackelberg assumption: the defender leads and the attacker follows. Notice that in the equation $\mathbf{q} = \mathsf{QR}(\mathsf{MS}(\mathbf{x}_0, \mathbf{x}, \mathbf{q}))$, $\mathbf{q}$ will only be defined after the defender commits to strategies $\mathbf{x}_0$ and $\mathbf{x}$. However, it is different from the standard Strong Stackelberg Equilibrium [Korzhyk et al. 2011] in that the attacker is following a level-∞ response model, as defined by the fixed point equation.*

Also, as we will discuss in Section 1.8.1.3 on our experiments, when $r = n$, the defender's optimal strategy is not to use up all the available resources. This is clearly different from a Nash equilibrium, as the defender still has incentives to use more resources.

1.6.1 Convergence Condition for the Level-l Response Model

We focus on the single-attacker case, where there are only n different types of tips. We use $\mathbf{V}_i$ to denote the tips where the attacker is reported to attack target i. When the attacker is using strategy q, the probability of receiving $\mathbf{V}_i$ is $\Pr\{\mathbf{V}_i\} = wq_i$.

Theorem 1.5. *Let $\bar{x}_i = \max_j\{x_i(\mathbf{V}_j)\}$. In the single attacker case, if there exists constant $L \in [0,1)$, such that $\bar{x}_i \leq \frac{L}{n\lambda(R_i^a - P_i^a)}, \forall i$, then level-l agents converge to level-∞ agents as l approaches infinity.*

The proof of Theorem 1.5 is omitted since it is immediate from the following lemma:

Lemma 1.3. *In the single attacker case, if there exists constant $L \in [0,1)$, such that $\bar{x}_i \leq \frac{L}{n\lambda(R_i^a - P_i^a)}$ for all i, then $g(\mathbf{q})$ is L-Lipschitz with respect to the L^1-norm, i.e., $g(\mathbf{q})$ is a contraction.*

Proof. Given defender's strategy $\mathbf{x}_0$ and $\mathbf{x}(\mathbf{V})$, define:

$$g(\mathbf{q}) = \mathsf{QR}(\mathsf{MS}(\mathbf{x}_0, \mathbf{x}, \mathbf{q})).$$

Then a level-(l+1) attacker's strategy can be computed by

$$\mathbf{q}^{l+1} = g(\mathbf{q}^l) = g(g(\mathbf{q}^{l-1})) = \cdots = g^l(\mathbf{q}).$$

The convergence of level-l is equivalent to the convergence of $g^l(\mathbf{q})$.

The marginal strategy $\hat{\mathbf{x}}$ can be written as:

$$\hat{\mathbf{x}}(\mathbf{q}) = \sum_{\mathbf{V}} \Pr\{\mathbf{V}\}\mathbf{x}(\mathbf{V}) = (1-w)\mathbf{x}_0 + \sum_i wq_i\mathbf{x}(\mathbf{V}_i).$$

Notice that the function $g(\mathbf{q})$ is just the quantal response against $\hat{\mathbf{x}}$:

$$g_i(\mathbf{q}) = \frac{\exp\left(\lambda u_i^a(\hat{x}_i)\right)}{\sum_j \exp\left(\lambda u_j^a(\hat{x}_j)\right)},$$

where $u_i^a(\hat{x}_i)$ is the attacker's expected utility of attacking target i when the defender's marginal strategy is $\hat{\mathbf{x}}$: $u_i^a(\hat{x}_i) = R_i^a - \hat{x}_i(R_i^a - P_i^a)$. Therefore,

$$\begin{aligned}
\frac{\partial g_i}{\partial q_j} =& \frac{\partial g_i}{\partial u_i^a}\frac{\partial u_i^a}{\partial q_j} + \sum_{i' \neq i} \frac{\partial g_i}{\partial u_{i'}^a}\frac{\partial u_{i'}^a}{\partial q_j} \\
=& \lambda w g_i(1-g_i)(P_i^a - R_i^a)x_i(\mathbf{V}_j) + \sum_{i' \neq i} \lambda w g_i g_{i'}(R_{i'}^a - P_{i'}^a)x_k(\mathbf{V}_j) \\
=& \lambda w g_i \left[(P_i^a - R_i^a)x_i(\mathbf{V}_j) + \sum_{i'=1}^{n} g_{i'}(R_{i'}^a - P_{i'}^a)x_{i'}(\mathbf{V}_j) \right].
\end{aligned}$$

Note that in the above equation, $0 \leq w, g_i, g_{i'}, x_i(\mathbf{V}_j), x_{i'}(\mathbf{V}_j) \leq 1$, $P_i^a - R_i^a < 0$ and $R_{i'}^a - P_{i'}^a > 0$. Thus we have:

$$\lambda(P_i^a - R_i^a)x_i(\mathbf{V}_i) < \frac{\partial g_i}{\partial q_j} < \lambda \sum_{i'=1}^{n} g_{i'}(R_{i'}^a - P_{i'}^a)x_{i'}(\mathbf{V}_j). \tag{1.4}$$

Our assumption $\bar{x}_i \leq \frac{L}{n\lambda(R_i^a - P_i^a)}$ for all i implies that $x_i(\mathbf{V}_j) \leq \frac{L}{n\lambda(R_i^a - P_i^a)}, \forall j, \forall i$. Plugging into Equation (1.4), we get:

$$-\frac{L}{n} < \frac{\partial g_i}{\partial q_j} < \frac{L}{n}\sum_{i'=1}^{n} g_{i'} = \frac{L}{n}.$$

For any $\mathbf{q}' \neq \mathbf{q}$, let $\mathbf{q}^{(i)} = (q_1, \ldots, q_i, q'_i, \ldots, q'_n)$. So $\mathbf{q}^{(0)} = \mathbf{q}'$ and $\mathbf{q}^{(n)} = \mathbf{q}$. Therefore,

$$\begin{aligned}
\left\|g(\mathbf{q}) - g(\mathbf{q}')\right\|_1 &= \sum_{i=1}^{n} \left|g_i(\mathbf{q}) - g_i(\mathbf{q}')\right| \\
&= \sum_{i=1}^{n} \left| \sum_{j=1}^{n} \left[g_i(\mathbf{q}^{(j)}) - g_i(\mathbf{q}^{(j-1)}) \right] \right| \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} \left| g_i(\mathbf{q}^{(j)}) - g_i(\mathbf{q}^{(j-1)}) \right| \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} \left| \int_{q'_j}^{q_j} \frac{\partial g_i(\mathbf{q})}{\partial q_j} \Big|_{\mathbf{q}=(q_1,\ldots,q_{i-1},s,q'_{i+1},\ldots,q'_n)} \mathrm{d}s \right| \\
&< \sum_{i=1}^{n} \sum_{j=1}^{n} \int_{q'_j}^{q_j} \frac{L}{n} \mathrm{d}s \\
&\leq \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{L}{n} |q_j - q'_j| \\
&= \sum_{i=1}^{n} \frac{L}{n} \|\mathbf{q} - \mathbf{q}'\|_1 \\
&= L \|\mathbf{q} - \mathbf{q}'\|_1.
\end{aligned}$$

□

Corollaryrk 1.1. *In the single attacker case, if there exists a constant $L \in [0,1)$, such that $\frac{L}{n\hat{\lambda}(R_i^a - P_i^a)} > 1, \forall i$, then level-$l$ agents converge to level-∞ agents as l goes to infinity.*

1.6.2 A Bi-Level Optimization for Solving the Optimal Defender's Strategy

In this section, we still consider the single attacker case and assume the defender has $r \geq 1$ resources. Clearly, the optimal set of informants should contain the ones with the highest information sharing intensities. It remains to compute the optimal strategies $\mathbf{x}_0$ and $\mathbf{x}(\mathbf{V})$. Given the optimal set of informants U^*, the probability of receiving a tip is $w = 1 - \prod_{u \in U^*}(1 - w_{u1})$. Let $\Pr\{\mathbf{V}\}$ be the probability of receiving tips $\mathbf{V}$, which depends $\mathbf{q}$. Let $\mathbf{x}(\mathbf{V}) = (x_1(\mathbf{V}), \ldots, x_n(\mathbf{V}))$ be the defender strategy when receiving tips $\mathbf{V}$.

Let $\mathbf{q} = (q_1, \ldots, q_n)$ be the strategy of the level-∞ attacker. Given $\mathbf{V}$ and the corresponding t_i's, the expected number of attackers that are going to attack target i is $d_i = t_i + (1 - \sum_j t_j)\tilde{p}_v(\emptyset)q_i$. Therefore, given $\hat{\mathbf{x}}$ we have the defender's expected utility $\mathsf{DefEU}(\mathbf{x}_0, \mathbf{x})$ as

$$\mathsf{DefEU}(\mathbf{x}_0, \mathbf{x}) = \sum_{\mathbf{V},i} \Pr\{\mathbf{V}\} d_i \left[P_i^d + x_i(\mathbf{V}) \left(R_i^d - P_i^d \right) \right].$$

Then the problem of finding the optimal defender strategy can be formulated as the following mathematical program:

$$\begin{aligned} \underset{\mathbf{x}_0, \mathbf{x}}{\text{maximize}} \quad & \mathsf{DefEU}(\mathbf{x}_0, \mathbf{x}) \\ \text{subject to} \quad & \mathbf{q} = \mathsf{QR}(\mathsf{MS}(\mathbf{x}_0, \mathbf{x}, \mathbf{q})) \end{aligned}$$

In the single-attacker case, we need n and n^2 variables to represent $\mathbf{x}_0$ and $\mathbf{x}$. We can use the `QRI-MILP` algorithm to find the solution. However, this approach needs to solve a mixed integer program and does not scale well.

To tackle the problem, we focus on the defender's marginal strategy instead of the full strategy representation, and decompose the above program into a bi-level optimization problem.

Let $\hat{\mathbf{x}} = \mathsf{MS}(\mathbf{x}_0, \mathbf{x}, \mathbf{q}) = \sum_{\mathbf{V}} \Pr\{\mathbf{V}\}\mathbf{x}(\mathbf{V})$, where we slightly abuse notation and use $\mathbf{V} = \emptyset$ to denote the case of receiving no tip, $\mathbf{x}(\emptyset)$ to denote $\mathbf{x}_0$. The bi-level optimization method works as follows. At the inner level, we fix an arbitrary feasible $\hat{\mathbf{x}}$, and solve the following mathematical program:

$$\begin{aligned} \underset{\mathbf{x}(\mathbf{V})}{\text{maximize}} \quad & \mathsf{DefEU}(\hat{\mathbf{x}}) \\ \text{subject to} \quad & \sum_{\mathbf{V}} \Pr\{\mathbf{V}\}\mathbf{x}(\mathbf{V}) = \hat{\mathbf{x}}, \\ & \mathsf{QR}(\hat{\mathbf{x}}) = \mathbf{q}, \\ & \mathbf{1}^\top \mathbf{x}(\mathbf{V}) \le r, \qquad \forall \mathbf{V}, \\ & x_i(\mathbf{V}) \in [0,1], \qquad \forall i \end{aligned}$$

Since $\hat{\mathbf{x}}$ is fixed, $\mathbf{q}$ and $\Pr\{\mathbf{V}\}$ are also fixed. Thus, the program above becomes a linear program, with $\mathbf{x}(\mathbf{V})$ as variables. We can always find a feasible solution to it by simply setting $\mathbf{x}(\mathbf{V}) = \hat{\mathbf{x}}, \forall \mathbf{V}$. Solving this linear program gives us the optimal defender's utility $\mathsf{DefEU}(\hat{\mathbf{x}})$ for any possible $\hat{\mathbf{x}}$. To find the optimal defender strategy, we solve the outer-level optimization problem below:

$$\begin{aligned} \underset{\hat{\mathbf{x}}}{\text{maximize}} \quad & \mathsf{DefEU}(\hat{\mathbf{x}}) \\ \text{subject to} \quad & \mathbf{1}^\top \hat{\mathbf{x}} \le r, \\ & \hat{\mathbf{x}}_i \in [0,1], \quad \forall i \end{aligned}$$

Since the feasible region of $\hat{\mathbf{x}}$ is continuous, we can use any known algorithm (e.g., gradient descent) to solve the outer-level program.

The inner-level linear program still suffers from the scalability problem. However, when there are multiple attackers, the optimal objective value can be well-approximated by simply

sampling a subset of possible $\mathbf{V}$'s, or focusing only on the $\mathbf{V}$'s with the highest probabilities. For those $\mathbf{V}$'s that are not considered, we can always use $\mathbf{x}_0$ as the default strategy for $\mathbf{x}(\mathbf{V})$.

1.7 Defending Against Informant-Aware Attackers

We now consider a variant of our model where attackers take into account the impact of informants when determining the target they attack. Specifically, we assume the attackers follow the QR behavior model but incorporate the probability of being discovered when determining their expected utility for attacking a target.[2] In this setting, the attackers' subjective belief $\mathbf{x}'$ of the target coverage probability does not necessarily satisfy $\sum_i x'_i \leq r$. Consider the example of a single attacker and a single informant with report intensity 1. Assume that the defender has $r = 1$ and always protects the target being reported with probability 1. Then no matter which target the attacker chooses to attack, it will always be covered.

We focus on the single attacker case with $r \geq 1$. We first consider the problem of computing the optimal defender strategy when given the set of informants U and associated probability of receiving a tip $w = 1 - \prod_{u \in U}(1 - w_{u1})$. In the general case with multiple attackers, we will need to specify the defender strategy for each combination of tips received. However, when there is only one attacker, we can succinctly describe the defender strategy by their default strategy without tips, $\mathbf{x}$, and their probability of defending a location after receiving a tip for that location, $\mathbf{z}$. Then, under the QR adversary model, the probability q_i of the attacker targeting location i will be:

$$q_i = \frac{\exp\left(\lambda\left\{[(1-w)x_i + wz_i]\,P_i^a + [1-(1-w)x_i - wz_i]\,R_i^a\right\}\right)}{\sum_{j\in\mathcal{T}} \exp\left(\lambda\left\{[(1-w)x_j + wz_j]\,P_j^a + [1-(1-w)x_j - wz_j]\,R_j^a\right\}\right)}.$$

This leads to the following optimization problem, `QRI`, to compute the optimal defender strategy:

$$\begin{aligned}
\underset{\mathbf{x},\mathbf{y},\mathbf{z}}{\text{maximize}} \quad & \frac{\sum_{i\in\mathcal{T}} \exp\left(\lambda R_i^a\right) \exp\left(-\lambda(R_i^a - P_i^a)y_i\right)\left[(R_i^d - P_i^d)y_i + P_i^d\right]}{\sum_{i\in\mathcal{T}} \exp\left(\lambda R_i^a\right) \exp\left(-\lambda(R_i^a - P_i^A)y_i\right)} \\
\text{subject to} \quad & y_i = (1-w)x_i + wz_i, \quad \forall i \in \mathcal{T}, && \text{(1.5a)} \\
& \sum_{i\in\mathcal{T}} x_i \leq r, && \text{(1.5b)} \\
& x_i, z_i \in [0,1], \qquad \forall i \in \mathcal{T} && \text{(1.5c)}
\end{aligned}$$

We can compute the optimal defender strategy by adapting the approach used in the PASAQ algorithm [Yang et al. 2012]. Proposition 1.3 and 1.4 shows that the conditions for algorithm PASAQ hold in our setting.

[2] Consider attackers that have had experience playing against the defender. Over time, the attacker might start to consider their expected utility in practice, which is affected by informants.

Proposition 1.3. *The optimal objective of* `QRI` *is non-decreasing in w.*

Proof. Consider the two optimization problems induced by different values for w: w_1, w_2 where $w_2 > w_1$. Let $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ be a solution for when $w = w_1$. Then, $(\mathbf{x}, \mathbf{y}, \frac{w_1}{w_2}\mathbf{z} + (1 - \frac{w_1}{w_2})\mathbf{x})$ is a feasible solution for when $w = w_2$ that achieves the same objective value. To see why it is feasible, observe that constraint (1.5a) is satisfied by construction and constraint (1.5c) is satisfied since the new value for each z_i is a convex combination of the previous x_i, z_i, which were both in $[0,1]$. □

Proposition 1.3 implies that when selecting informants, it is optimal to simply maximize w. Since $w = 1 - \prod_{u \in U}(1 - w_{u1})$, we can select informants greedily and choose the k informants with the largest information sharing intensity w_{u1}. We can then solve the optimization problem to find the optimal allocation of resources. Finally, we discuss how to find an approximate solution to `QRI` using a MILP approach.

We can compute the optimal defender strategy by adapting the approach used in the PASAQ algorithm [Yang et al. 2012]. Let $N(y), D(y)$ be the numerator and denominator of the objective in `QRI`. As with PASAQ, we binary search on the optimal value δ^*. We can check for feasibility of a given δ by rewriting the objective to $\min_{x,y,z} \delta D(y) - N(y)$ and checking if the optimal value is less than 0. To solve the new optimization problem, which still has a non-linear objective function, we adapt their approach of approximating the objective function with linear constraints and write a MILP.

First, let $\theta_i = \exp(\lambda R_i^a)$, $\beta_i = \lambda(R_i^a - P_i^a)$, and $\alpha_i = R_i^d - P_i^d$. We rewrite the objective as

$$\sum_{i \in \mathcal{T}} \theta_i(\delta - P_i^d)\exp(-\beta_i(y_i)) + \sum_{i \in \mathcal{T}} \theta_i \alpha_i y_i \exp(-\beta_i(y_i))$$

We have two non-linear functions that need approximation $f_i^1(y) = \exp(-\beta_i y)$ and $f_i^2(y) = y \cdot \exp(-\beta_i y)$. Let γ_{ij} be the slope for the linear approximation of $f_i^1(y)$ from $(\frac{j}{K}, f_i^1(\frac{j}{K}))$ to $(\frac{j+1}{K}, f_i^1(\frac{j+1}{K}))$ and similarly with μ_{ij} for $f_i^2(y)$.

The key change in our MILP compared to PASAQ is that we replace the original defender resource constraint with constraints (1.6a) - (1.6d), which take into account the defender's ability to respond to tips. Our MILP (which we call `QRI-MILP`) is listed as follows:

$$\begin{aligned}
\underset{\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{a}}{\text{minimize}} \quad & \sum_{i \in \mathcal{T}} \theta_i(\delta - P_i^d)\left(1 + \sum_{j=1}^{K} \gamma_{ij} y_{ij}\right) - \sum_{i \in \mathcal{T}} \theta_i \alpha_i \sum_{j=1}^{K} \mu_{ij} y_{ij} \\
\text{subject to} \quad & \sum_{j=1}^{K} y_{ij} = (1-w)x_i + w z_i, \quad \forall i, && \text{(1.6a)} \\
& \sum_{i \in \mathcal{T}} x_i \leq r, && \text{(1.6b)} \\
& x_i \in [0,1], \qquad \forall i, && \text{(1.6c)}
\end{aligned}$$

$$z_i \in [0,1], \qquad \forall i, \tag{1.6d}$$

$$y_{ij} \in [0,\frac{1}{K}], \qquad \forall i,j = 1\dots K, \tag{1.6e}$$

$$a_{ij}\frac{1}{K} \leq y_{ij}, \qquad \forall i,j = 1\dots K-1, \tag{1.6f}$$

$$y_{i(j+1)} \leq a_{ij}, \qquad \forall i,j = 1\dots K-1, \tag{1.6g}$$

$$a_{ij} \in \{0,1\}, \qquad \forall i,j = 1\dots K-1 \tag{1.6h}$$

Proposition 1.4. *The feasible region for* $\mathbf{y} = \langle y_i = \sum_{j=1}^{K} y_{ij}, i \in \mathcal{T} \rangle$ *of* `QRI-MILP` *is equivalent to that of* `QRI`.

Proof. With the substitution $y_i = \sum_{j=1}^{K} y_{ij}$, constraints (1.6a) - (1.6d) are directly translated from `QRI`. The remaining constraints (1.6e) - (1.6h) can be shown to allow for any potential y_i, represented correctly with the appropriate y_{ij}. □

With the above claim shown, the proof for the approximate correctness of PASAQ applies here and we can show that we can find an ε-optimal solution for arbitrarily small ε [Yang et al. 2012].

1.8 Experiment

In this section, we demonstrate the effectiveness of our proposed algorithms through extensive experiments. In our experiments, all reported results are averaged over 30 randomly generated game instances. To generate $G_S = (X,Y,E)$, we first fix the sets X and Y. For each $u \in X$, we sample the degree of u, d_u, uniformly from $[|Y|]$ and then sample a uniformly random subset of Y of size d_u. For each $(u,v) \in E$, w_{uv} is drawn from $U[0,0.2]$. For the attack probability p_v, in the general case, each p_v is drawn from $U[0.4,1]$. When we restrict $\sum_{v\in Y} p_v \leq C'$, we draw a vector $\mathbf{t} = (t_1,\dots,t_{|Y|})$ from $U[0,1]^{|Y|}$ and set $p_v = \min\left\{1, C' \cdot \frac{t_v}{||\mathbf{t}||_1}\right\}$. For the payoff matrix, each R_i^d (R_i^a) is drawn from $U(0,Q]$ and each $P_i^d(P_i^a)$ is drawn from $U[-Q,0)$, where Q is set to 2. The precision parameter λ is set to 2. DefEU_0 and q_i's are obtained by a binary search with a convex optimization as introduced in [Yang et al. 2012]. The number of samples M used in M-SAMPLING is set to 100. In GSA, EDPA is used to calculate $\mathsf{DefEU}(U)$.

In the `QRI-MILP` algorithm, the optimal defender strategy is found with approximation parameter $K = 10$. The bi-level optimization algorithm is implemented using MATLAB R2017a. The low-level linear program is solved using the `linprog` function and the high-level optimization is solved with the `fmincon` function. Unless specified otherwise, all game instances are generated in this way.

1.8.1 Experimental Results

We compare the scalability and the solution quality of SELECT using EDPA, C-TRUNCATED, M-SAMPLING to obtain DefEU and GSA for different settings of the problems against level-0 attackers.

We first test the case with $\sum_{v\in Y} p_v < 3$. We set $|X| = 6, k = 4, n = 8, r = 3$ and enumerate $|Y|$ from 2 to 16. The results are shown in Figure 1.1. We also include GREEDY as a baseline that always chooses the informants that maximizes the probability of receiving tips. We can see that M-SAMPLING performs the best in term of runtime, but fails to provide high-quality solutions. While C-TRUNCATED is slower than M-SAMPLING, it performs the best with no error in all test cases. However, when there is no restriction on $\sum_{v\in Y} p_v$, as shown in Figure 1.2, C-TRUNCATED does not perform well, and the performance is even worse than GREEDY for large $|Y|$, while M-SAMPLING performs a lot better and GSA performs the best. We also fix $|X| = 7$, $|Y| = 10, k = 3, r = 5$ and change the number of targets n from 5 to 25 for $\sum_{v\in Y} p_v < 3$. The results are shown in Figure 1.3. GSA is the fastest but provides slightly worse solutions than C-TRUNCATED does. The runtime of GREEDY is less than 0.3s for all instances tested.

We then perform a case study to show the trade-off between the optimal number of resources to allocate and the optimal number of informants to recruit with budget constraints when defending against level-0 attackers. We set $|X| = |Y| = n = 6$ and generate an instance of the game. We set the cost of allocating one defensive resource $C_r = 3$ and the cost of hiring one informant $C_i = 1$. Given a budget B, we can recruit k informants and allocate r resources when $k \cdot C_i + r \cdot C_r \leq B$. The trade-off between the optimal k and r is shown in Figure 1.4. In the same instance, we study how the defender's utility would change by increasing the number of recruited informants with fixed r. Given a fixed number of resources, the defender should recruit as many informants as possible. We can also see that assuming the defender can acquire sufficient resources, the importance of recruiting additional informants diminishes. This result provides useful guidance to defenders such as conservation agencies in allocating their budget and recruiting informants.

1.8.1.1 Level-0 vs. Level-∞ attackers

We set $|X| = n = 6$, $|Y| = p_1 = 1$, and G_S to be fully connected. We set $r = 2, 4, 6$ and vary k from 1 to 6. We first fix the defender's strategy to the one against level-0 attackers and compare the utility achieved by the defender when defending against a level-0 attacker and a level-∞ attacker. We show how the defender utility varies with the number of informants and defensive resources in Figure 1.5a. On average, we see that the defender utility against a level-∞ attacker is lower than that against a level-0 attacker. We also show the utility of the defender using her optimal strategy against a level-∞ attacker. We can see that when facing a level-∞ attacker, the defender utility when using the optimal strategy is higher by a margin than using the one against level-0 attackers.

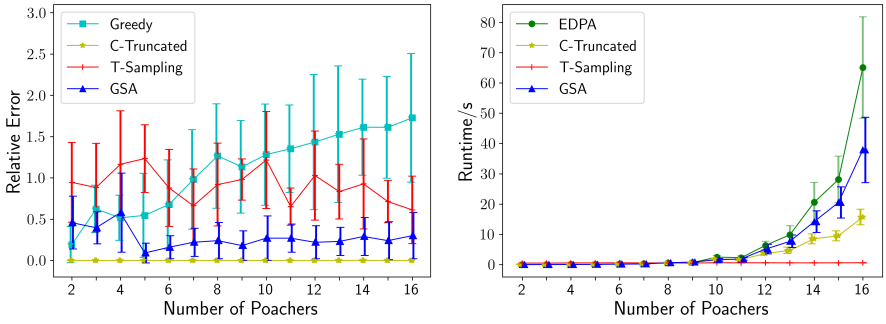


Figure 1.1: Runtime and solution quality with $\sum_{v \in Y} p_v < 3$.

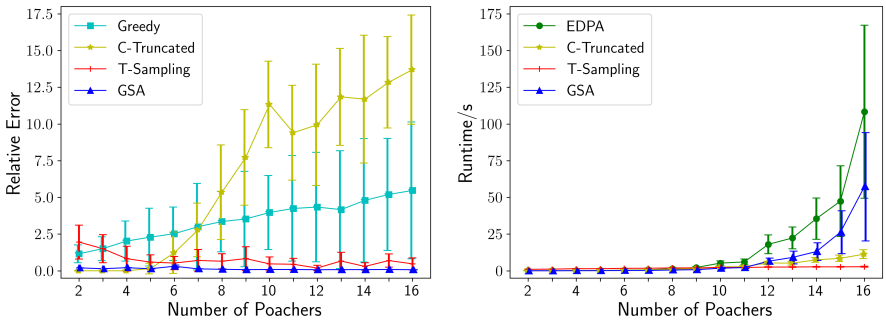


Figure 1.2: Runtime and solution quality for general cases.

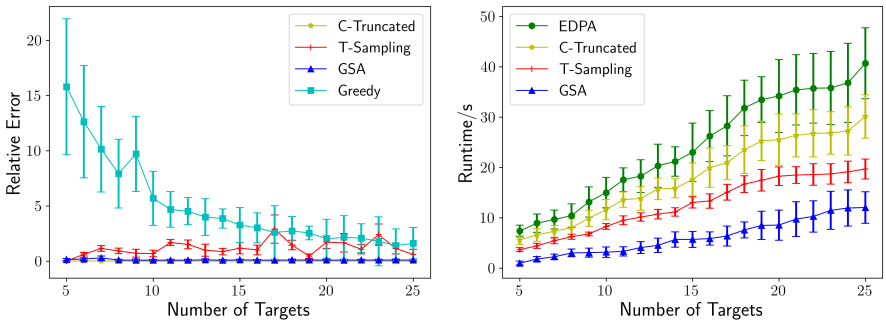


Figure 1.3: Runtime and solution quality increasing n with $\sum_{v \in Y} p_v < 3$.

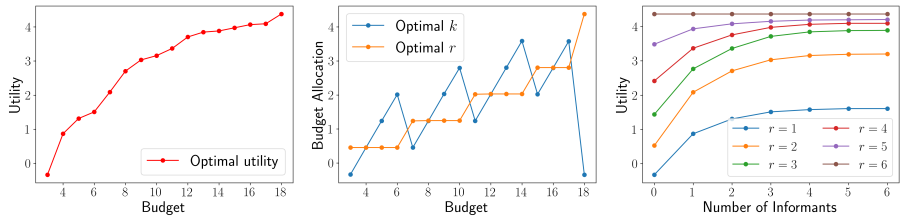
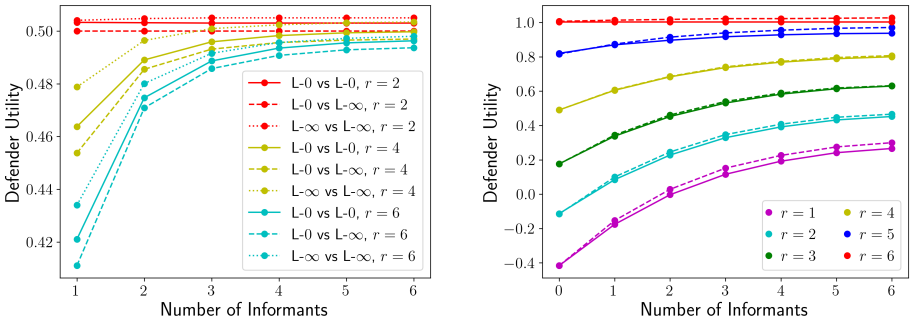


Figure 1.4: Trade-off between r and k, and increase of utility with fixed r ($|X| = 6$, $|Y| = 6$, $n = 6$).



(a) Comparison between the defender utility against attackers of different levels, where "L-0 vs L-∞" means that the defender uses the optimal strategy against a level-0 attacker, while the actual attacker is of level-∞.

(b) Comparison between defender utility against informant-aware (solid lines) and level-0 (dashed lines) attackers, where the defender uses the corresponding optimal strategy respectively.

Figure 1.5: Defender's utility when faced with different attackers.

1.8.1.2 Level-0 vs. informant-aware defenders

We set $|X| = n = 6$, $|Y| = p_1 = 1$, and G_S to be fully connected. We vary both r and k from 0 to 6. We assume that the defender recruits the k informants with the highest information sharing intensity w_{u1}. The optimal defender strategy against the informant-aware attacker case is found using `QRI-MILP`. The defender strategy against the level-0 attacker case is computed using PASAQ [Yang et al. 2012]. The defender utility against the level-0 attacker is found by first computing q_i, DefEU_0 and then using the results to compute $\mathsf{DefEU}(U)$.

In Figure 1.5b, we show how the defender utility in the two cases varies with the number of informants and defensive resources. On average, we see that the defender utility is marginally

higher against the level-0 attacker than against the informant-aware attacker, particularly when the defender has either very few or very many defensive resources.

We also run experiments for the SISI case and do a case study to show the errors of the estimations for all $U \subseteq X$ on 2 instances. In Figure 1.6, we compare the performance of the level-0 defender and the informant-aware defender when playing against an informant-aware attacker. We see that despite that their strategies are computed under the level-0 attacker assumption, the utility of the level-0 defender is only slightly lower than the utility of the informant-aware defender. For a fixed r, the difference in utility grows larger as the defender recruits more informants and has a higher probability of receiving a tip.

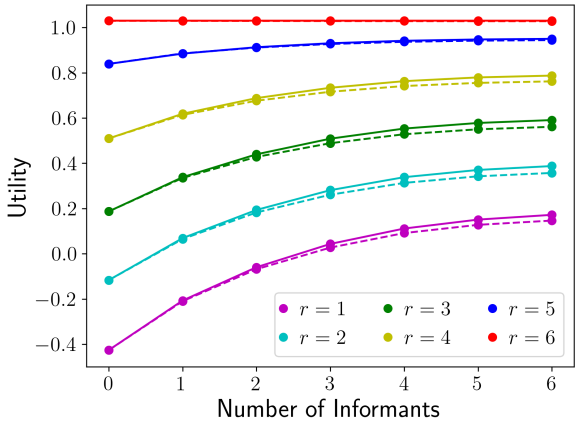


Figure 1.6: Utility comparison between the level-0 defender (dashed lines) and the informant-aware defender (solid lines) against an informant-aware attacker.

1.8.1.3 Comparison between the Bi-Level Algorithm and `QRI-MILP`

We empirically compare the bi-level optimization algorithm with `QRI-MILP`. We set $|X| = n = 6$, $|Y| = p_1 = 1$, and G_S to be fully connected. We vary r from 1 to 6 and k from 0 to 6.

In both cases, we assume that the defender recruits the k informants with the highest information sharing intensity w_{u1}. The results are shown in Figure 1.7. In general, our bi-level algorithm gives higher expected defender utilities than the `QRI-MILP` algorithm, except when $r = 1$. Our results show that both increasing the number of resources and hiring more informants increase the defender's utility. However, as the number of resources (r) increases, the utility gain from hiring more informants diminishes.

Intuitively, if the number of resources equals the number of targets, the defender should always cover all the targets, Interestingly, during our experiments, we observed that in this case, the optimal defender strategy may not always use all his resources to cover all the targets. The reason is that in a general sum game, by decreasing the probability of protecting

a certain target on purpose, the defender can lure the attacker into attacking the target more frequently, and thus increase his expected utility. Such strategies can be found in real-world wildlife protections where the patrollers may sometimes deliberately ignore the tips. This is also reflected in our bi-level algorithm. If the defender always uses all his resources, then both the defender's and the attacker's strategies are fixed, and hiring more informants does not increase the defender's expected utility. But if the defender strategy does not always use all his resources, then hiring more informants could help (see the bi-level algorithm for the $r = 6$ case in Figure 1.7).

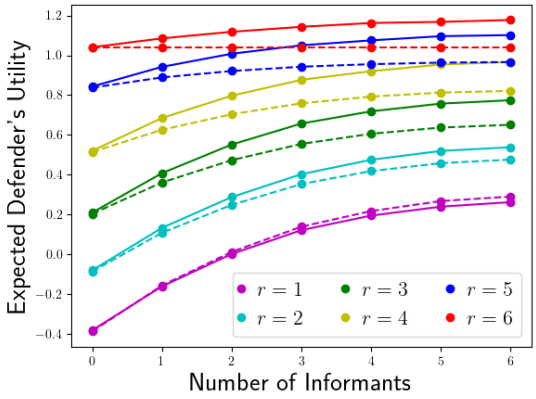


Figure 1.7: Comparison between the bi-level optimization algorithm (solid lines) and `QRI-MILP` (dashed lines).

1.9 Discussion

In this chapter, we introduced a novel two-stage security game model and a multi-level QR behavioral model that incorporated community engagement. We provided complexity results, developed algorithms to find (sub-)optimal groups of informants to recruit against level-0 attackers and evaluated the algorithms through extensive experiments. Our results also generalize to the case where informants have heterogeneous recruitment costs and to different kinds of attacker response models, such as SUQR model [Nguyen et al. 2013], which can be done by calculating the attacker's response correspondingly. In Section 1.6, we defined a more powerful type of attacker that could respond to the marginal strategy and developed a bi-level optimization algorithm to find the optimal defender's strategy in this case.

In the anti-poaching domain, some conservation site managers utilize the so-called "intelligence" operations that rely on informants in nearby villages to alert rangers when they know the poachers' plans in advance. The deployment of the work relies on the site manager to provide their understanding of the social connections among community members. The edges

and parameters of the bipartite graph in our model can be extracted from a local social media application or historical data collected by site managers. Recruiting and training reliable informants is costly and managers may only afford a limited number of them. Our model and solution can help the managers efficiently recruit informants, make the best use of tips and evaluate the trade-off between allocating budget to hiring rangers and recruiting informants in a timely fashion.

In reality, instead of using a particular behavior model, we can use historical records as training data and learn the attackers' behavior in different domains. It would also be interesting to consider the case where the informants can only provide inaccurate tips or other types of tips, e.g., some subset of targets will be attacked instead of a single location. We can also model the informants as strategic agents. In real life, it is possible that informants may also provide fake information if they have their own utility structures. We can try to reward them to elicit true information and maximize the defender's utility.

Bibliography

N. Basilico, A. Celli, G. De Nittis, and N. Gatti. 2017. Coordinating multiple defensive resources in patrolling games with alarm systems. In *AAMAS'17*, pp. 678–686.

R. Duffy, F. A. St John, B. Büscher, and D. Brockington. 2015. The militarization of anti-poaching: undermining long term goals? *Environmental Conservation*, 42(4): 345–348.

F. Fang, T. H. Nguyen, R. Pickles, W. Y. Lam, G. R. Clements, B. An, A. Singh, B. C. Schwedock, M. Tambe, and A. Lemieux. 2017. PAWS - A deployed game-theoretic application to combat poaching. *AI Magazine*. http://www.aaai.org/ojs/index.php/aimagazine/article/view/2710.

C. Gill, D. Weisburd, C. W. Telep, and T. Bennett. 2014. Community-oriented policing to reduce crime, disorder and fear and increase satisfaction and legitimacy among citizens: A systematic review. *Journal of Experimental Criminology*.

Q. Guo, B. An, B. Bosansky, and C. Kiekintveld. 2017. Comparing strategic secrecy and stackelberg commitment in security games. In *IJCAI-17*.

M. Jain, J. Tsai, J. Pita, C. Kiekintveld, S. Rathi, M. Tambe, and F. Ordónez. 2010. Software assistants for randomized patrol planning for the lax airport police and the federal air marshal service. *Interfaces*.

D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe. 2011. Stackelberg vs. nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. *Journal of Artificial Intelligence Research*, 41: 297–327.

B. Le Gallic and A. Cox. 2006. An economic analysis of illegal, unreported and unregulated (iuu) fishing: Key drivers and possible solutions. *Marine Policy*, 30(6): 689–695.

N. Leader-Williams and E. Milner-Gulland. 1993. Policies for the enforcement of wildlife laws: the balance between detection and penalties in luangwa valley, zambia. *Conservation Biology*, 7(3): 611–617.

M. Linkie, D. J. Martyr, A. Harihar, D. Risdianto, R. T. Nugraha, Maryati, N. Leader-Williams, and W. Wong. 2015. Editor's choice: Safeguarding sumatran tigers: evaluating effectiveness of law enforcement patrols and local informant networks. *Journal of Applied Ecology*.

X. Ma, Y. He, X. Luo, J. Li, M. Zhao, B. An, and X. Guan. Jul 2018. Camera placement based on vehicle traffic for better city security surveillance. *IEEE Intelligent Systems*, 33(4): 49–61. ISSN 1941-1294. http://dx.doi.org/10.1109/MIS.2018.223110904. DOI: 10.1109/mis.2018.223110904.

R. D. McKelvey and T. R. Palfrey. 1995. Quantal response equilibria for normal form games. *Games and economic behavior*.

W. D. Moreto. 2015. Introducing intelligence-led conservation: bridging crime and conservation science. *Crime Science*, 4(1): 15.

G. L. Nemhauser, L. A. Wolsey, and M. L. Fisher. 1978. An analysis of approximations for maximizing submodular set functions—i. *Mathematical programming*, 14(1): 265–294.

T. H. Nguyen, R. Yang, A. Azaria, S. Kraus, and M. Tambe. 2013. Analyzing the effectiveness of adversary modeling in security games. In *AAAI*.

J. Pita, M. Jain, J. Marecki, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus. 2008. Deployed armor protection: the application of a game theoretic model for security at the los angeles international airport. In *AAMAS: industrial track*.

A. Rosenfeld and S. Kraus. 2017. When security games hit traffic: Optimal traffic enforcement under one sided uncertainty. In *IJCAI*, pp. 3814–3822.

A. Schlenker, O. Thakoor, H. Xu, F. Fang, M. Tambe, L. Tran-Thanh, P. Vayanos, and Y. Vorobeychik. 2018. Deceiving cyber adversaries: A game theoretic approach. In *AAMAS*.

M. B. Short, A. B. Pitcher, and M. R. D'Orsogna. 2013. External conversions of player strategy in an evolutionary game: A cost-benefit analysis through optimal control. *European Journal of Applied Mathematics*, 24(1): 131–159.

M. Smith and J. Humphreys. 2015. *The Poaching Paradox: Why South Africa's 'Rhino Wars' Shine a Harsh Spotlight on Security and Conservation*. Ashgate Publishing Company.

M. Tambe. 2011. *Security and game theory: algorithms, deployed systems, lessons learned*. Cambridge University Press.

R. Tublitz and S. Lawrence. 2014. Public assessing east palo alto's fitness improvement training zone program. *The Chief Justice Earl Warren Institute on Law and Social Policy Research Brief*.

X. Wang, B. An, M. Strobel, and F. Kong. 2018. Catching captain jack: Efficient time and space dependent patrols to combat oil-siphoning in international waters. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 32.

J. R. Wright and K. Leyton-Brown. 2014. Level-0 meta-models for predicting human behavior in games. In *Proceedings of the fifteenth ACM conference on Economics and computation*, pp. 857–874. ACM.

WWF, 2015. Developing an approach to community-based crime prevention. http://zeropoaching.org/pdfs/Community-based-crime\%20prevention-strategies.pdf.

R. Yang, F. Ordonez, and M. Tambe. 2012. Computing optimal strategy against quantal response in security games. In *AAMAS*.

Author's Biography

Your Name

Your Name began life as a small child ...