Green Security Game with Community Engagement

Taoan Huang
Tsinghua University
hta15@mails.tsinghua.edu.cn

Tianyu Gu
Carnegie Mellon University
tianyug@andrew.cmu.edu

Rohit Singh
World Wildlife Fund, Cambodia
rsingh@wwf.panda.org

Fei Fang
Carnegie Mellon University
feifang@cmu.edu

ABSTRACT

Green security problems such as protecting wildlife from poaching and protecting fisheries from illegal overfishing are particularly challenging due to the frequent illegal activities and a very low average density of defensive resources such as rangers or patrol boats (referred to as patrollers). To assist patrols, community members recruited by law enforcement agencies (referred to as informants) sometimes provide informative tips that can lead patrollers to areas that have ongoing illegal activities or will have illegal activities in a particular period of time.

While game theoretic models and algorithms have been developed to combat illegal activities, none of the existing work considers this crucial aspect of community engagement. We fill this gap and (i) introduce a novel two-stage security game model built specifically with consideration of community engagement; (ii) provide a polynomial time algorithm for computing optimal strategy to allocate patrollers given the tips and the recruited informants; (iii) show the problem of selecting the optimal set of informants is NP-Hard and develop exact, approximate and heuristic algorithms for solving the problem; (iv) evaluate the algorithms through extensive experiments and analyze the trade-off between recruiting more patrollers and recruiting more informants given a limited total budget. The algorithms and analysis can provide useful insights and guidance to law enforcement agencies in allocating the budget and recruiting informants.

KEYWORDS

Noncooperative Game; Security Games; Community Engagement

1 INTRODUCTION

Security problems exist all around the world in various domains. The major challenge in these domains is that sufficient coverage is hard to reach due to lack of defensive resources. Security game models have been proposed to study the defender-attacker interactions [30] and algorithms have been developed to compute efficient allocation of defensive resources [4, 12]. They have been applied to reduce traffic [25], combat oil-siphoning [33], and deceive cyber adversaries [24] in addition to handling challenges in infrastructure security domains such as protecting airports [23] and green security domains such as designing ranger patrols [6].

In green security domains, a common lack of funding leads to an extremely low density of defensive resources, e.g., 1 patroller 167 square kilometers in wildlife conservation area [9]. What makes it more challenging is that there are often multiple attackers and frequent attacks. The attackers, even got caught, can often continue to launch attacks, due to the insufficient level of sanction which often in the format of fine or short imprisonment [14, 15]. To combat criminal activities more effectively, law enforcement agencies (referred to as defenders) often recruit informants from local communities and plan defensive resources based on tips provided by them [16]. 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*, parallel to ranger patrols [36, 37]. Community engagement has been studied in criminology, specifically in anti-poaching [20] and reducing crime [7, 18, 32], without principled mathematical models. On the other hand, existing models of security games completely ignored this essential element of community engagement.

In this paper, we provide the first study to fill the gap. Our first contribution is a novel two-stage security game model that takes community engagement into account by representing the social network between potential informants and attackers using a bipartite graph. While more informants are desirable, reaching out to informants and training them is costly and time-consuming [28]. Therefore, defenders should recruit informants strategically. We address this aspect by having the defender decide which subset of informants to recruit in the first stage of the game with a budget constraint. In the second stage, the defender then chooses a set of targets to protect based on the tips provided by the recruited informants.

Our second contribution is an optimal linear time computable strategy to allocate defensive resources given the set of recruited informants and their tips. If defenders have already obtained tips from recruited informants, then they are able to find the optimal set of targets to protect by computing the expected gain for each target if it is protected and allocate defensive resources to the targets with the highest gains. This optimal set is not necessarily a subset or superset of the set of targets on which we get tips as it depends on the total number of attackers that conduct frequent attacks, the importance of the targets, the set of informants recruited, and how the informants are connected to those attackers.

Proc. of the 18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019), N. Agmon, M. E. Taylor, E. Elkind, M. Veloso (eds.), May 2019, Montreal, Canada

https://doi.org/doi

The third contribution of this paper is that we show the problem of selecting the optimal set of informants is NP-Hard and develop algorithms to find the optimal or close-to-optimal set of informants to recruit. We develop an exact exponential time algorithm EDPA to find the optimal set of informants based on enumeration and dynamic programming. We develop an efficient approximation algorithm C-Truncated by assuming that many attacks are unlikely to happen at the same time and provide an error bound. We develop another approximation algorithm T-Sampling by using sampling to estimate defender's expected utility and a greedy search algorithm GSA to find a set of informants to recruit.

We finally evaluate the scalability and solution quality of each algorithm through extensive experiments in different settings and conduct a case study to analyze the trade-off between recruiting more patrollers and recruiting more informants given a limited total budget. The algorithms and analysis can help defenders such as conservation agencies make better decisions when allocating their budgets.

While we use anti-poaching as an example application domain, the importance of community engagement goes beyond merely protecting wildlife. Community engagement could significantly help defenders planning allocation of defensive resources in different domains, including fighting opportunistic crime, protecting infrastructure, and combating illegal fishery. Therefore, our model has a wide range of application.

2 RELATED WORK AND BACKGROUND

In criminology, there is a line of work on community engagement. [5, 20, 28] investigates the relationship between rangers and community members and explores the role that community engagement plays in wildlife conservation. [16] demonstrates the significance of cultivating and utilizing a network of reliable informants by showing that patrols conducted with the help of community engagement were significantly more likely to detect snares than routine patrols in Kerinci Seblat National Park in Sumatra. For fighting urban crime, [32] shows that a program that focuses on improving the relationship between the police and residents help reducing crime in two urban areas. [18] studies the role of an intelligence model that incorporates the perspectives of partner agencies and local communities with parameters for both reactive and proactive responses to crime. [7] shows that community-oriented policing strategies help improve perceptions of the police and has positive effects on police legitimacy. As for fighting terrorism, [2] outlines a case for a community-based approach in the UK including key developments since 2005 and [29] suggests a more socially inclusive approach should be applied so that working with a boarder range of communities would be encouraged. However, those pieces of work do not study community engagement from the lens of computational game theory.

Recruitment of informants has also been proposed to study societal attitudes in relation to committing and reporting crime using evolutionary game theory models. [26] shows that the presence of informants can lead to decreases in crime and [27] formulates the problem of solving recruitment strategies as an optimal control problem to account for limited resources and budget. In contrast to their work which focuses on crime reporting only, we emphasize on the synergy of community engagement and allocation of defensive resources and aim to find the best strategy of recruiting informants and allocating defensive resources.

Another related problem is the influence maximization problem [11] where one wants to choose a set of seed nodes in a social network to spread influence according to some diffusion model optimally. Recently, new applications of influence maximization, including preventing HIV [34, 38–40] and helping homeless youth [35, 40], have emerged. There are also work on game theoretic models for strategic interaction in social networks, e.g., competing for influence [3, 31]. These work differ from ours in that we consider the case where the defender recruits informants from a local community given the interaction network so as to get tips for guiding the patrols to combat illegal activities.

In security domians, Stackelberg Security Game (SSG) has been applied to a variety of security problems [10, 13, 41]. In a SSG, the defender plays the role of the leader and the attacker plays the role of the follower. Several variants of SSG that are related to ours have been studied. [1] studies a variant of security game with the presence of an alarm system that is able to detect attacks in real time. [17] applies SSG to the problem of placing security surveillance cameras. [8] explores a game where the defender is able to disguise resources. The key aspect of community engagement to security game in our work is that we are able to know the activities of attackers reported by informants and the defender can decide which informants to recruit. While assuming fully rationality on the adversary has been widely adopted in the study of SSG, quantal response (QR)-adversary model [19] has also been explored [42]. Our paper mainly focuses on how the defender recruits informants and reacts to tips, assuming the attacker responds to a regular patrol strategy with any known behavioral pattern, including best response and quantal response models.

3 MODEL

In this section, we introduce our novel two-stage green security game model with community engagement. The key new element in this game model is the consideration of informants, who are members of the community. They are recruited and trained by the defender to provide tips about ongoing or upcoming attacks to the defender. This new element results in the two-stage model where in the first stage of the game, the defender recruits informants, and in the second stage, the defender receives tips from hired informants and allocates resources to protect targets.

Following the prevalent security game model [10, 13], the game we consider in this paper features a set of n targets $T = [n]$. The defender has r units of defensive resources to protect the targets. The outcomes of the game depend only on whether each attack is successful or not. If target i is under attack, the defender receives reward $R_i^d > 0$ if it is covered, otherwise receives penalty $P_i^d < 0$. Similarly, $P_i^a < 0$ and $R_i^a > 0$ are the attacker's payoff.

While everyone in the community can potentially be recruited as informants, how often they can get the tips and how valuable their tips are may vary. The main impacting factor is how they interact with the potential attackers. We model the potential interactions and connections between the groups of potential informants and the groups of potential attackers using a bipartite graph. When an attacker decides to launch an attack, some potential informants who had interacted with the attacker may be able to perceive his or her targeted location. However, we do not assume that such information could be shared among informants. Since in the real world, informants do not know the existence of each other and may have different means of information collection.

Formally, the potential informants and attackers are represented by two disjoint sets of people X and Y ($X \cap Y = \emptyset$) respectively. X consists of people who will not attack targets and are potential informants, and Y consists of potential attackers who will attack a target with some probability. 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 of them takes action independently. The social connection between these two groups of people is represented by a bipartite graph $G_S = (X, Y, E)$, where an edge $(u, v) \in E$ is associated with an information sharing intensity w_{uv} representing the probability of the targeted location of $v \in Y$ being reported by $u \in X$, given v go attacking and u is recruited as an informant.

In the first stage of the game, 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 recruit a set of k informants in the first stage in order to maximize the expected utility in the second stage. The utility is defined as the summation of the utilities of outcomes on all attacks.

Let U denote the set of recruited informants in the first stage where $|U| \leq k$, and $V = \{v : (u, v) \in E \wedge u \in U\}$ denote the set of attackers that are connected with at least one informant in U. We define tips as all pieces of information provided by the recruited informants U, which could be represented by 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 $i, j \in T$. We say an attacker v is *reported* if there exists $i \in T$ such that $v \in V_i$, otherwise he is *unreported.*

We also denote by $V_0 = \bigcup_{i \in T} V_i$ the set of reported attackers. Note that we could possibly have $V_0 = \emptyset$ and we say the defender is *informed* if $V_0 \neq \emptyset$.

Getting tips is infrequent in general in practice, and the attackers are generally not aware of the existence of informants. Therefore in the second stage, we assume that when the defender is not informed, he or she will adopt the regular defending strategy $\mathbf{x} = (x_1, \ldots, x_n)$, which is the equilibrium strategy the defender will commit in the SSG based on the adversary's quantal response [42] and can be observed by the attackers. We assume the attackers are bounded rational and follow the quantal response(QR)-adversary model [19]. Each attacker, if committing an attack on a target, will quantally respond to $\mathbf{x}$ with $\lambda \geq 0$ being the precision parameter [19]. The probability q_i of an attacker attacking location i, can be computed as

$$q_i = \frac{e^{\lambda(x_i P_i^a + (1-x_i) R_i^a)}}{\sum_{j \in T} e^{\lambda(x_j P_j^a + (1-x_j) R_j^a)}}.$$

In fact, our algorithms and results do not rely on this specific QR-adversary model and can be applied various behavior models of the adversary, as will be discussed in Section 7. We also discuss the relaxation of the assumptions of getting tips is infrequent in Section 7.

If informed, the defender will optimally allocate defensive resources according to the provided tips and the attackers' behaviour in order to achieve the maximum expected utility.

We denote the defender's utility with a set U of recruited informants by $\mathsf{DefEU}(U)$. Our goal is to recruit a set U of no more than k informants that maximizes $\mathsf{DefEU}(U)$.

4 COMPLEXITY RESULTS

In this section, we provide complexity results of the problem. We first show when the defender is informed by the recruited informants, we can determine in linear time the optimal strategy to allocate defensive resources based on the tips. We then show the problem of selecting an optimal set of informants is NP-Hard.

First, we show in Theorem 4.1 that, when the defender is informed by the set of informants U, the optimal allocation of defensive resources can be determined in linear time based on the given tips $\mathbf{V}$. The allocation is determined in a greedy fashion. Given the tips, the defender could infer the posterior probability of each unreported attacker launching an attack, and calculate each target i's expected increment in utility if i is covered, and allocate the resources to targets that lead to the highest utility.

Before proving the theorem, we define some useful notations. Given 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 $V_0 = \bigcup_{i \in T} V_i$. Note $\tilde{p}_v(V_0)$ could be calculated as

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

where $\tilde{w}_v = 1 - \prod_{(u,v) \in E, u \in U}(1 - w_{uv})$ is the probability of v being reported given he or she attacks. Given V_0 and $t_i = |V_i|$ reported attacks on each target i, the expected utility on i could be calculated as

$$\mathsf{EU}_i^c(t_i, V_0) := \left(t_i + q_i \sum_{v \in Y \setminus V_0} \tilde{p}_v(V_0)\right) R_i^d$$

if i is covered and

$$\mathsf{EU}_i^u(t_i, V_0) := \left(t_i + q_i \sum_{v \in Y \setminus V_0} \tilde{p}_v(V_0)\right) P_i^d$$

if not, and the expected gain of the target if covered 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 4.1. *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 $\mathbf{V} = (V_1, \ldots, V_n)$.*

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 of the targets with the highest EG_i.

The above strategy is indeed optimal since the expected utility is given by $\sum_{i \in T} \mathsf{EU}_i^u(|V_i|, V_0)$ with no resource, 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 $\mathrm{EG}_i(|V_i|, V_0)$ for each $i \in T$ can be done in $O(n + |Y|)$ time, and finding the r largest $\mathrm{EG}_i(|V_i|, V_0)$ can be done in $O(n)$ time, leading to the overall complexity of $O(|Y| + n)$. □

Next, we prove that the problem is NP-Hard even for a relatively simple case by constructing a reduction from maximum coverage problem (MCP).

Theorem 4.2. *Computing the optimal set of informants to recruit is NP-Hard.*

Proof. We prove that the problem is NP-Hard even for a simple case of the problem. Consider a case of the problem where $r = 1$, $p_v = w_{uv} = 1$ 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. Let $\lambda = 0$.

To start with, we investigate how $\mathrm{DefEU}(U)$ 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 an 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 he goes attacking. Then the defender's expected utility $\mathrm{DefEU}(U)$ could be written as

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

Now we check that to maximize DefEU is to maximize the term $\left(\mathbb{E}\left[\max_{i\in T} X_i\right] - \frac{|V|}{n}\right)$, which depends only on the size of V.

We can prove by induction on $|V|$ that $\left(\mathbb{E}\left[\max_{i\in T} X_i\right] - \frac{|V|}{n}\right)$ 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 $|V| = 2$, it holds for $|V| = 1$.
2. Consider $|V| \geq 1$ 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 he targeting the location with the largest X_i. Thus the expected maximum increase by p. Since $p \geq \frac{1}{n}$ and by a simple coupling argument, we have that $\mathbb{E}\left[\max_{i\in T} X_i\right]$ increases by at least $\frac{1}{n}$.

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 use a reduction from MCP to show that the optimization problem is NP-Hard. Consider an instance of MCP with 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. □

5 FINDING THE OPTIMAL SET OF INFORMANTS

In this section, we develop exact and heuristic informant selection algorithms to recruit the optimal set of informants. Since our goal is to find U that maximizes $\mathrm{DefEU}(U)$, we need to compute $\mathrm{DefEU}(U)$. As we can see in the special case given in the proof of Theorem 4.2, $\mathrm{DefEU}(U)$ could be written in closed form since we know the sets of reported attackers. However in the general case, the attackers are heterogeneous, and we do not know which set of attackers will be reported on a particular day, which makes it hard to compute $\mathrm{DefEU}(U)$. Thus, we first develop exact and approximate algorithms for calculating $\mathrm{DefEU}(U)$, on which the informant selection algorithms heavily rely.

5.1 Calculating $\mathrm{DefEU}(U)$

In this subsection, we treat the set of recruited informants U as given, and focus on calculating $\mathrm{DefEU}(U)$. By following the optimal allocation strategy, we develop an enumeration and dynamic programming-based algorithm (EDPA) that runs in exponential time to calculate the exact value of $\mathrm{DefEU}(U)$ for the general case with the aid of a dynamic programming-based calculation. For the case with strong information sharing intensity (SISI) where $\forall (u, v) \in E$ $w_{uv} = 1$, we show that $\mathrm{DefEU}(U)$ can be computed in polynomial time. We also introduce approximation methods, C-Truncated and T-Sampling, to efficiently estimate $\mathrm{DefEU}(U)$ and show that under certain assumptions C-Truncated provides estimations with bounded error.

By following the optimal allocation strategy Theorem 4.1 provides, we develop EDPA to compute the exact $\mathrm{DefEU}(U)$ as shown in Algorithm 1.

First, we compute the utility on the case when the defender is not informed (line 4-6), where DefEU_0 is the expected utility when using the regular defending strategy against a single attack. DefEU_0 can be obtained by the algorithms introduced in [42]. Then we focus on calculating the total utility $\mathrm{DefEU}'(U)$ on the case when the defender is informed. $\mathrm{DefEU}'(U)$ can be computed as the summation of the expected utility on all targets by linearity of expectation. 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 (line 2,7). We denote the type a 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 having the tips of type (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

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

is the probability of having V_0 being the set of reported attackers given U (line 3). Then we have the expected utility on target i that all instances of tips with type (t_i, V_0) can contribute to $\mathrm{DefEU}(U)$

as

$$\Pr(t_i, V_0|U) \cdot \mathsf{EU}_i(t_i, V_0) + P_{V_0}\tbinom{|V_0|}{t_i} q_i^{t_i} \cdot P_{i,r} \cdot \mathsf{EG}_i(t_i, V_0)$$
$$= P_{V_0}\tbinom{|V_0|}{t_i} q_i^{t_i} \left((1-q_i)^{|V_0|-t_i}\mathsf{EU}_i(t_i, V_0) + P_{i,r}\mathsf{EG}_i(t_i, V_0)\right),$$

where $P_{i,r}$ is the probability of i being among r of the targets with the highest expected gain given (t_i, V_0) and U (line 12-13). As a result,

$$\mathsf{DefEU}'(U)$$
$$= \sum_{V_0 \neq \emptyset, i, t_i} P_{V_0}\binom{|V_0|}{t_i} q_i^{t_i} \left((1-q_i)^{|V_0|-t_i}\mathsf{EU}_i(t_i, V_0) + P_{i,r}\mathsf{EG}_i(t_i, V_0)\right)$$

The calculation of $P_{i,r}$ is all that remains. At first sight, $P_{i,r}$ can be calculated by enumerating all possible tips of type (t_i, V_0), so that we can easily know, for each instance, whether i is among the r targets with the highest EG_i. To get $P_{i,r}$, we simply add up the probabilities of having those corresponding tips. However, this can be done very efficiently via Algorithm 2, a dynamic programming-based calculation. Let $\{i_1, \ldots, i_{n-1}\}$ denote the set of targets apart from i, i.e., $T \setminus \{i\}$ (line 1) and $y! \cdot f(s, x, y)$ be 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

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

which can be calculated via a dynamic programming (line 5-13). The dynamic programming for computing $f(s, x, y)$ is done in a similar way of counting the number of s-partitions on integer y, where we also considers the constraint brought in by the limitation on the number of resources. To calculate $f(s, x, y)$, we enumerate a_s as $\tilde{y}$ (line 8) and compare $\mathsf{EG}_{i_s}(a_s, V_0)$ with $\mathsf{EG}_i(t_i, V_0)$ (line 10). If $EG_{i_s}(a_s, V_0) > EG_i(t_i, V_0)$, we check the value of $f(s-1, x-1, y-\tilde{y})$ (line 11), otherwise check $f(s-1, x, y-\tilde{y})$ (line 13). Thus, we have $P_{i,r} = (|V_0| - t_i)! \left(\sum_{x=0}^{r-1} f(s, x, |V_0| - t_i)\right)$.

The time complexity for Algorithm 2 is $O(nr|Y|^2)$, resulting in a time complexity of $O(2^{|Y|}n^2r|Y|^3)$ for Algorithm 1. Though EDPA runs in exponential time, the calculation of $\mathsf{DefEU}(U)$ can be done in polynomial time for the special case of SISI, i.e., the information sharing intensity is strong ($w_{uv} = 1\,\forall(u, v) \in E$). This is the case where the informants have strong connections with a particular group of attackers, and they can get full access to their attack plans while not to the others'.

Lemma 5.1. *Given the set of recruited informants U, the defender's expected utility* $\mathsf{DefEU}(U)$ *can be computed in polynomial time if* $w_{uv} = 1\,\forall(u, v) \in E$.

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 $O(n^2r|Y|^4)$ time. □

Denote by ASISI (Algorithm for SISI) the polynomial time algorithm Lemma 5.1 indicates. See the Appendix [1] for the pseudocode of ASISI.

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

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

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

```
1: $\{i_1, \ldots, i_{n-1}\} \leftarrow T \setminus \{i\}$
2: $\mathsf{EG}_i \leftarrow (t_i + q_i \sum_{v \in Y \setminus V_0} \tilde{p}_v(V_0))(R_i^d - P_i^d)$
3: Initialize $f(s, x, y) \leftarrow 0$ for all $s, x, y$
4: $f(0, 0, 0) \leftarrow 1$
5: for $s \leftarrow 1$ to $n - 1$ do
6:     for $x \leftarrow 0$ to $\min(s, r)$ do
7:         for $y \leftarrow 0$ to $|V_0| - t_i$ do
8:             for $\tilde{y} \leftarrow 0$ to $y$ do
9:                 $\mathsf{EG}_{i_s} \leftarrow (\tilde{y} + q_{i_s} \sum_{v \in Y \setminus V_0} \tilde{p}_v(V_0))(R_{i_s}^d - P_{i_s}^d)$
10:                if $\mathsf{EG}_{i_s} > \mathsf{EG}_i$ then
11:                    $f(s, x, y) \leftarrow f(s, x, y) + \frac{q_{i_s}^{\tilde{y}}}{\tilde{y}!} f(s-1, x-1, y-\tilde{y})$
12:                else
13:                    $f(s, x, y) \leftarrow f(s, x, y) + \frac{q_{i_s}^{\tilde{y}}}{\tilde{y}!} f(s-1, x, y-\tilde{y})$
```

Next, we introduce approximation methods to estimate $\mathsf{DefEU}(U)$. Let $\mathsf{DefEU}(U, C)$ be the estimated defender's utility returned by Algorithm 1 if only subsets of reported attackers V_0 with $|V_0| < C$ are enumerated in line 2. 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

[1] An anonymous link to the Appendix: https://www.dropbox.com/s/ql4fp2r4i1wrw2v/AppendixCE.pdf?dl=0.

happen at the same time. Formally, assume that the expected number of attacks is bounded by a constant C', that is $\sum_{v\in Y} p_v \le C'$, $\mathrm{DefEU}(U,C)$ for $C > C'$ is an estimation of $\mathrm{DefEU}(U)$ with bounded error.

Lemma 5.2. *Assume that $\sum_{v\in Y} p_v \le C'$ and $|P_i^d|, |R_i^d| \le Q$, the estimation $\mathrm{DefEU}(U,C)$ of $\mathrm{DefEU}(U)$ for $C > C'$ satisfies*

$$\begin{aligned} & |\mathrm{DefEU}(U) - \mathrm{DefEU}(U,C)| \\ < \quad & Q \cdot e^{-2(C-C')^2/|Y|}\left(C + \frac{1}{1-e^{-4(C-C')/|Y|}}\right). \end{aligned}$$

Proof. Let random variables 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

$$\begin{aligned} & |\mathrm{DefEU}(U) - \mathrm{DefEU}(U,C)| \\ \le \quad & \sum_{A\in\mathcal{A}_1} \Pr[A]|E_A| \le \sum_{A\in\mathcal{A}_2} \Pr[A]|E_A| \\ \le \quad & Q\sum_{i=C}^{|Y|} \Pr[W=i]\cdot i = Q\left(C\Pr[W\ge C] + \sum_{i=C+1}^{|Y|} \Pr[W\ge i]\right) \\ \le \quad & Q\left(Ce^{-2(C-C')^2/|Y|} + \sum_{i=C+1}^{|Y|} e^{-2(i-C')^2/|Y|}\right) \qquad (2) \\ < \quad & Q\cdot e^{-2(C-C')^2/|Y|}\left(C + \frac{1}{1-e^{-4(C-C')/|Y|}}\right). \qquad (3) \end{aligned}$$

(2) follows by the Chernoff Bound, (3) follows since

$$\begin{aligned} \sum_{i=C+1}^{|Y|} e^{-2(i-C')^2/|Y|} \quad & \le \quad e^{-2(C+1-C')^2/|Y|}\sum_{i\ge 0} e^{-4i(C+1-C')/|Y|} \\ & < \quad e^{-2(C-C')^2/|Y|}\cdot\frac{1}{1-e^{-4(C-C')/|Y|}}. \end{aligned}$$

□

The time complexity of C-Truncated is given by $O(n^2r|Y|^{C+3})$

However, for the case where $\sum p_v$ is large, we have to set C to be larger than $\sum p_v$ for C-Truncated in order to obtain a high-quality solution; otherwise the error will become unbounded. To mitigate this limitation, in the following part we propose an alternative sampling approach, T-Sampling, to estimate $\mathrm{DefEU}(U)$ for general cases without restrictions on $\sum p_v$. Instead of enumerating all possible V_0 as EDPA does, in T-Sampling, we draw T i.i.d. samples of the set of reported attackers where each sample V_0 is drawn with probability P_{V_0}. T-Sampling takes the average of the expected defender's utility when having V_0 as the reported attackers over all samples as the estimation of $\mathrm{DefEU}(U)$. A sample of V_0 can be drawn as follow: (i) Let $V_0 = \emptyset$ initially; (ii) For each $v \in V$, add v to V_0 with probability $\tilde{w}_v p_v$; (iii) Return V_0 as a sample of the set of reported attackers. From Equation (1), the above sampling process is consistent with the distribution of V_0.

Proposition 5.3. $\lim_{\mathsf{T}\to\infty} \mathrm{DefEU}^{(\mathsf{T})}(U) = \mathrm{DefEU}(U)$, *where* $\mathrm{DefEU}^{(\mathsf{T})}(U)$ *is the estimation of* $\mathrm{DefEU}(U)$ *given by* T-Sampling *using* T *samples.*

T-Sampling returns an estimation of $\mathrm{DefEU}(U)$ in $O(\mathsf{T}n^2r|Y|^3)$ time.

Algorithm	Time Complexity
EDPA	$O(\lvert X\rvert^k 2^{\lvert Y\rvert} n^2 r \lvert Y\rvert^3)$
C-Truncated	$O(\lvert X\rvert^k n^2 r \lvert Y\rvert^{C+3})$
T-Sampling	$O(\lvert X\rvert^k \mathsf{T} n^2 r \lvert Y\rvert^3)$
ASISI	$O(\lvert X\rvert^k n^2 r \lvert Y\rvert^4)$
GSA	$O(2^k \lvert X\rvert n^2 r \lvert Y\rvert^3)$

Figure 1: Complexity Table

5.2 Selecting Informants U

In this section, we design and analyze informant selection algorithms to recruit the optimal set of informants. We first introduce the main algorithm, which is a standard routine that integrates the algorithms for computing the defender's utility we have introduced previously. Then we provide an efficient heuristic search algorithm.

We formally introduce the main algorithm in Algorithm 3. Algorithm 3 takes an instance of the game as input (line 1), compute DefEU_0 and q_i for all targets i (line 2), and enumerate all possible sets U with no more than k informants (line 4). For each U, we deploy the algorithms for computing the defender's utility (EDPA, C-Truncated, ASISI, T-Sampling) as a subroutine to obtain (an estimation of) $\mathrm{DefEU}(U)$ (line 5) and then update the optimal U (line 6).

Algorithm 3 Main Algorithm

```
1: Input an instance of the game
2: Compute $q_i$ for all $i \in T$ and $\mathrm{DefEU}_0$
3: OPT ← $\emptyset$
4: for $U \subseteq X$, $|U| \le k$ do
5:     $S$ ← Calculate $\mathrm{DefEU}(U)$
6:     Update OPT with $(U, S)$
7: return OPT
```

In the rest of the context, we let the variants of the main algorithm inherit the name of the subroutine it uses to calculate (or estimate) $\mathrm{DefEU}(U)$. For example, T-Sampling is the one that we obtain estimations of $\mathrm{DefEU}(U)$ via the sampling method in the main algorithm.

For C-Truncated, the solution quality of the selected set of informants is guaranteed by the following theorem.

Theorem 5.4. *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 *respectively, for $C > C'$ it holds that*

$$\begin{aligned} & \mathrm{DefEU}(U_{\mathrm{OPT}}) - \mathrm{DefEU}(U') \\ < \quad & 2Q\cdot e^{-2(C-C')^2/|Y|}\left(C + \frac{1}{1-e^{-4(C-C')/|Y|}}\right). \end{aligned}$$

Proof. By definition of C-Truncated, we have $\mathrm{DefEU}(U',C) \ge \mathrm{DefEU}(U_{\mathrm{OPT}},C)$. Let $B = 2Q\cdot e^{-2(C-C')^2/|Y|}\left(C + \frac{1}{1-e^{-4(C-C')/|Y|}}\right)$. Suppose $\mathrm{DefEU}(U_{\mathrm{OPT}}) - \mathrm{DefEU}(U') \ge 2B$, by Lemma 5.2, we have

$$\mathrm{DefEU}(U',C) < \mathrm{DefEU}(U')+B \le \mathrm{DefEU}(U_{\mathrm{OPT}})-B < \mathrm{DefEU}(U_{\mathrm{OPT}},C),$$

which leads to a contradiction. □

For ASISI and T-Sampling, we have the following propositions.

Proposition 5.5. *Given that k is a constant, the optimal set of informants and the optimal defender's utility can be computed in polynomial time by* ASISI *if $w_{uv} = 1$ for all u, v.*

Proof. It follows by Lemma 5.1, since all possible U can be enumerated in $O(|X|^k)$. □

Proposition 5.6. T-Sampling *returns the optimal set of informants and the optimal defender's utility when* $\mathsf{T} \to \infty$.

Algorithm 4 Search(U')

```
1: if $|U'| = k$ then
2:     $S \leftarrow$ Calculate DefEU($U'$)
3:     Update OPT with $(U', S)$
4:     return
5: for $u \in X$ do
6:     Calculate DefEU($U' \cup \{u\}$)
7: $u_1 \leftarrow \arg\max_{u \in X}$ DefEU($U' \cup \{u\}$)
8: $u_2 \leftarrow \arg\max_{u \in X \setminus \{u_1\}}$ DefEU($U' \cup \{u\}$)
9: Search($U' \cup \{u_1\}$), Search($U' \cup \{u_2\}$)
```

Next, we propose GSA (greedy-based search algorithm) for the selection of informants as shown in Algorithm 4. GSA starts by calling Search($\emptyset$). If $|U'| < k$, Search(U') expands the current set of informants U' by adding u_1, u_2 to U' respectively and then recursively calls Search($U' \cup \{u_1\}$) and Search($U' \cup \{u_2\}$) , where u_1 and u_2 chosen as the informants that lead to the first and second largest increments in the defender's utility (line 7-9); Otherwise, it updates the optimal solution with U' (line 1-4).

Notice that if we only consider u_1 instead of both u_1 and u_2, GSA would be exactly the same as a greedy algorithm that step by step adds an informant the leads to the largest utility. However, this is not a submodular maximization problem [21], since DefEU(U) is not a submodular set function in general. Such greedy algorithm will not simply guarantee an approximation ratio of $1 - 1/e$. We provide a counterexample that disproves the submodularity of DefEU(U).

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 DefEU($\emptyset$) = DefEU($\{1\}$) = DefEU($\{2\}$) = 3, DefEU($\{1, 2\}$) = $\frac{1}{4}(2 + 0.5) + \frac{1}{4}(4 + 1) + \frac{1}{2}(2 + 1) = 3.375$. As a result, DefEU($\{1, 2\}$) + DefEU($\emptyset$) > DefEU($\{1\}$) + DefEU($\{2\}$).

We provide a table in Figure 1 that summarizes the time complexity of all algorithms for computing the optimal U.

6 EXPERIMENT

In this section, we demonstrate the effectiveness of our proposed algorithms through extensive experiments. We first introduce the experiment setup and then present the experimental results.

6.1 Experiment Setup

All experiments are done on a 2.5GHz quad-core i7 CPU, and all algorithms are implemented in C++. All instances in experiments are generated as follows unless specified otherwise and all experiments 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 $u \in X$, the degree of u, d_u, is drawn uniformly from $[|Y|]$ and the set of d_u neighbors of u is drawn uniformly from all subsets of Y with size d_u. For each $(u, v) \in E$, w_{uv} is drawn from $U[0, 0.2]$. For the attack probability p_v's, each p_v is drawn from $U[0.4, 1]$ for the general case. For the case where we have restriction $\sum_{v \in Y} p_v \leq C'$, we draw a vector $\mathbf{t} = (t_1, \ldots, t_{|Y|})$ from $U[0, 1]^{|Y|}$ and let $p_v = \min\{1, C' \cdot \frac{t_v}{||\mathbf{t}||_1}\}$. For the payoff matrix, each R_i^d (R_i^a) is drawn from $U(0, Q]$ and each P_i^d 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 [42]. The number of samples T used in T-Sampling is set to 100.

In GSA, EDPA is used to calculate DefEU(U).

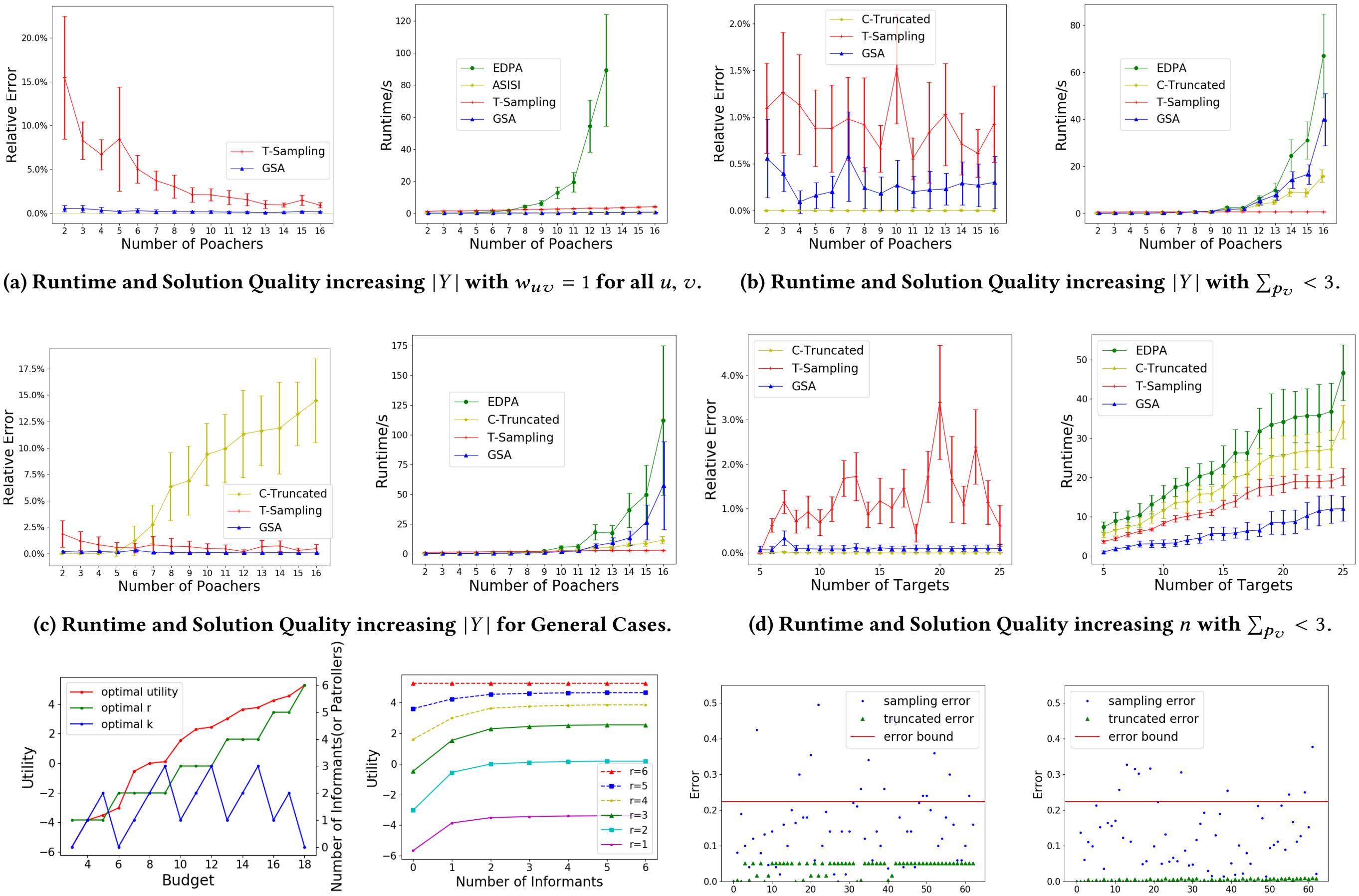
6.2 Experimental Results

We compare the scalability and the solution quality of EDPA, C-Truncated, T-Sampling, and GSA for different settings of the problems.

First, we test the case where $w_{uv} = 1\, \forall (u, v) \in E$. We set $|X| = 6, k = 4, n = 10, r = 3$ and enumerate $|Y|$ from 2 to 16. The average runtime of all algorithms including ASISI together with the relative error of GSA and T-Sampling are shown in Figure 2a. Though ASISI and GSA are the fastest among all, the average relative errors of GSA are slightly above 0%. T-Sampling is slightly slower than ASISI and GSA, and the solutions are less accurate than the other two in this case.

Next, we test the case where $\sum_{v \in Y} p_v < 3$. We set $|X| = 6, k = 4, n = 8, r = 3$ and enumerate $|Y|$ from 2 to 16. The average runtime and the solution quality of C-Truncated, T-Sampling and GSA are shown in Figure 2b. We can see that T-Sampling performs the best in term of runtime, but it fails to provide high-quality solutions. While C-Truncated is slower than T-Sampling, it performs the best with no error on all test cases. However, when there is no restriction on $\sum_{v \in Y} p_v$, as shown in Figure 2c, C-Truncated performs badly especially for large $|Y|$, while T-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 2d. GSA is the fastest among all but provides slightly worse solutions than C-Truncated does.

We then perform a case study to show the trade-off between the optimal number of defensive resources to allocate and the optimal number of informants to recruit with budget constraints. We set $|X| = 6$, $|Y| = 6$, $n = 6$ and generate an instance of the game. We also set the cost of allocating one defensive resource $C_r = 1$ and the cost of hiring one informant $C_i = 3$. Given a budget B, we could recruit k informants and allocates 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 2e. In the same instance, we study how the defender's utility would change by increasing the number of recruited informants with fixed r. The results are shown in Figure 2e. It is shown that



(a) Runtime and Solution Quality increasing $|Y|$ with $w_{uv} = 1$ for all u, v.

(b) Runtime and Solution Quality increasing $|Y|$ with $\sum p_v < 3$.

(c) Runtime and Solution Quality increasing $|Y|$ for General Cases.

(d) Runtime and Solution Quality increasing n with $\sum p_v < 3$.

(e) Trade-off between r and k, and Increase of Utility with Fixed r ($|X| = 6$, $|Y| = 6$, $n = 6$).

(f) Error of DefEU on 2 Cases with Fixed $C = 6$, $C' = 2$, $|Y| = 8$, $Q = 2$.

given a fixed number of resources, the defender should recruit as many informants as possible. We can also see that in this instance, the defender should always try to get more resources if possible, e.g., when there are 6 resources, there is no need to recruit informants. This result can provide useful guidance to defenders such as conservation agencies in allocating their budget and recruiting informants

Our last experiment is a case study on 2 instances with $\sum_{v \in Y} p_v < 2$ fixed $|X| = 6$, $|Y| = 8$, $n = 6$, $r = 3$, $Q = 2$. We run EDPA, C-Truncated ($C = 6$) and T-Sampling on each instance and show the error of the estimations for all $U \subseteq X$. The results are shown in 2f and the red lines indicate the error bound given by Inequality (2). The set of informants is represented using binary code, e.g., the set with code $19 = (010011)_2$ represents the set $\{u_1, u_2, u_4\}$. The first instance is constructed to show that the bound given by Lemma 5.2 is empirically tight, i.e., the estimation of DefEU(U) by C-Truncated could be large but still bounded. In this case, we set $p_v = 1, w_{uv} = 1\, \forall u, v$, $R_i^d = Q$ and $P_i^d = -10^{-3}$. While the other instance is randomly generated. It is shown that T-Sampling has larger errors with higher variances compared to C-Truncated.

7 DISCUSSION AND CONCLUSION

In this paper, we introduced a novel two-stage security game model that incorporates community engagement, provided a linear time computable strategy for allocating defensive resources given the tips from informants, proved the NP-Hardness of solving the optimal set of informants to recruit, developed algorithms to find (sub-)optimal groups of informants to recruit, and evaluated the algorithms through extensive experiments. Note that even in the case study the informants have homogeneous costs to recruit, our algorithms are able to support informants with heterogeneous costs. We should also notice that different kinds of attackers' response models, such as the best response model and the SUQR model [22], could be applied in our paper.

For future work, there are several directions that we can potentially pursue. First, instead of using a particular behavior model, we can use the records of history attacks as training data and learn the attackers' behavior model in specific domains. Second, different defender presence can be considered. Besides allocating defensive resources, defenders could actively identify attackers with high probabilities of carrying attacks and deter potential crimes based on tips. Third, if the defender has enough powerful informants, the defender may have a high probability of getting tips every time. In this case, even if the attackers are still not aware of the existence of informants, they may empirically observe a defence strategy that is different from the regular one. Thus the optimal defender strategy will be a random reaction strategy to each possible set of tips, which leads to an exponential space description of the defender's strategy. We defer the investigation of this situation to future work. Furthermore, we can model the informants as strategic agents. In real life, it is possible to have a more complicated situation where informants may also commit crimes and provide fake tips. We can treat the process of recruiting and rewarding informants as a mechanism design problem to elicit true information and maximize defenders' utility.

REFERENCES

[1] Nicola Basilico, Andrea Celli, Giuseppe De Nittis, and Nicola Gatti. 2017. Coordinating multiple defensive resources in patrolling games with alarm systems. In *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 678–686.

[2] Rachel Briggs. 2010. Community engagement for counterterrorism: lessons from the United Kingdom. *International affairs* 86, 4 (2010), 971–981.

[3] Andrew Clark and Radha Poovendran. 2011. Maximizing influence in competitive environments: A game-theoretic approach. In *International Conference on Decision and Game Theory for Security*. Springer, 151–162.

[4] Vincent Conitzer and Tuomas Sandholm. 2006. Computing the optimal strategy to commit to. In *Proceedings of the 7th ACM conference on Electronic commerce*. ACM, 82–90.

[5] Rosaleen Duffy, Freya AV St John, Bram Büscher, and DAN Brockington. 2015. The militarization of anti-poaching: undermining long term goals? *Environmental Conservation* 42, 4 (2015), 345–348.

[6] Fei Fang, Thanh Hong Nguyen, Rob Pickles, Wai Y. Lam, Gopalasamy R. Clements, Bo An, Amandeep Singh, Brian C. Schwedock, Milind Tambe, and Andrew Lemieux. 2017. PAWS - A Deployed Game-Theoretic Application to Combat Poaching. *AI Magazine* 38, 1 (2017), 23–36. http://www.aaai.org/ojs/index.php/aimagazine/article/view/2710

[7] Charlotte Gill, David Weisburd, Cody W Telep, Zoe Vitter, and Trevor 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* 10, 4 (2014), 399–428.

[8] Qingyu Guo, Boyuan An, Branislav Bosansky, and Christopher Kiekintveld. 2017. Comparing strategic secrecy and Stackelberg commitment in security games. In *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, IJCAI-17*.

[9] T Holmern, J Muya, and E Røskaft. 2007. Local law enforcement and illegal bushmeat hunting outside the Serengeti National Park, Tanzania. *Environmental Conservation* 34, 1 (2007), 55–63.

[10] Manish Jain, Jason Tsai, James Pita, Christopher Kiekintveld, Shyamsunder Rathi, Milind Tambe, and Fernando Ordónez. 2010. Software assistants for randomized patrol planning for the lax airport police and the federal air marshal service. *Interfaces* 40, 4 (2010), 267–290.

[11] David Kempe, Jon Kleinberg, and Éva Tardos. 2003. Maximizing the spread of influence through a social network. In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 137–146.

[12] Christopher Kiekintveld, Manish Jain, Jason Tsai, James Pita, Fernando Ordóñez, and Milind Tambe. 2009. Computing optimal randomized resource allocations for massive security games. In *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1*. International Foundation for Autonomous Agents and Multiagent Systems, 689–696.

[13] Dmytro Korzhyk, Zhengyu Yin, Christopher Kiekintveld, Vincent Conitzer, and Milind Tambe. 2011. Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. *Journal of Artificial Intelligence Research* 41 (2011), 297–327.

[14] Bertrand Le Gallic and Anthony Cox. 2006. An economic analysis of illegal, unreported and unregulated (IUU) fishing: Key drivers and possible solutions. *Marine Policy* 30, 6 (2006), 689–695.

[15] N Leader-Williams and EJ Milner-Gulland. 1993. Policies for the enforcement of wildlife laws: the balance between detection and penalties in Luangwa Valley, Zambia. *Conservation Biology* 7, 3 (1993), 611–617.

[16] Matthew Linkie, Deborah J. Martyr, Abishek Harihar, Dian Risdianto, Rudijanta T. Nugraha, Maryati, Nigel LeaderWilliams, and WaiMing Wong. 2015. EDITOR'S CHOICE: Safeguarding Sumatran tigers: evaluating effectiveness of law enforcement patrols and local informant networks. *Journal of Applied Ecology* 52, 4 (8 2015), 851–860. https://doi.org/10.1111/1365-2664.12461

[17] Xiaobo Ma, Yihui He, Xiapu Luo, Jianfeng Li, Mengchen Zhao, Bo An, and Xiaohong Guan. 2018. Camera Placement Based on Vehicle Traffic for Better City Security Surveillance. *IEEE Intelligent Systems* 33, 4 (Jul 2018), 4961. https://doi.org/10.1109/mis.2018.223110904

[18] Mike Maguire and Tim John. 2006. Intelligence led policing, managerialism and community engagement: Competing priorities and the role of the National Intelligence Model in the UK. *Policing & society* 16, 1 (2006), 67–85.

[19] Richard D McKelvey and Thomas R Palfrey. 1995. Quantal response equilibria for normal form games. *Games and economic behavior* 10, 1 (1995), 6–38.

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

[21] George L Nemhauser, Laurence A Wolsey, and Marshall L Fisher. 1978. An analysis of approximations for maximizing submodular set functionsI. *Mathematical programming* 14, 1 (1978), 265–294.

[22] Thanh Hong Nguyen, Rong Yang, Amos Azaria, Sarit Kraus, and Milind Tambe. 2013. Analyzing the Effectiveness of Adversary Modeling in Security Games.. In *AAAI*.

[23] James Pita, Manish Jain, Janusz Marecki, Fernando Ordóñez, Christopher Portway, Milind Tambe, Craig Western, Praveen Paruchuri, and Sarit Kraus. 2008. Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport. In *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track*. International Foundation for Autonomous Agents and Multiagent Systems, 125–132.

[24] Aaron Schlenker, Omkar Thakoor, Haifeng Xu, Fei Fang, Milind Tambe, Long Tran-Thanh, Phebe Vayanos, and Yevgeniy Vorobeychik. 2018. Deceiving Cyber Adversaries: A Game Theoretic Approach. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS '18)*. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 892–900. http://dl.acm.org/citation.cfm?id=3237383.3237833

[25] Guni Sharon, Michael Albert, Tarun Rambha, Stephen D. Boyles, and Peter Stone. 2017. Traffic Optimization For a Mixture of Self-interested and Compliant Agents. *CoRR* abs/1709.09569 (2017). arXiv:1709.09569 http://arxiv.org/abs/1709.09569

[26] MB Short, PJ Brantingham, and MR D?orsogna. 2010. Cooperation and punishment in an adversarial game: How defectors pave the way to a peaceful society. *Physical Review E* 82, 6 (2010), 066114.

[27] Martin B Short, Ashley B Pitcher, and MARIA 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 (2013), 131–159.

[28] MLR Smith and Jasper Humphreys. 2015. *The Poaching Paradox: Why South Africas Rhino Wars Shine a Harsh Spotlight on Security and Conservation*. Ashgate Publishing Company.

[29] Basia Spalek and Alia Imtoual. 2007. Muslim communities and counter-terror responses:Hard approaches to community engagement in the UK and Australia. *Journal of Muslim Minority Affairs* 27, 2 (2007), 185–202.

[30] Milind Tambe. 2011. *Security and game theory: algorithms, deployed systems, lessons learned*. Cambridge University Press.

[31] Jason Tsai, Thanh Hong Nguyen, and Milind Tambe. 2012. Security Games for Controlling Contagion.. In *AAAI*.

[32] Rebecca Tublitz and Sarah Lawrence. [n. d.]. The Fitness Improvement Training Zone Program. ([n. d.]).

[33] Xinrun Wang, Bo An, Martin Strobel, and Fookwai Kong. 2018. Catching Captain Jack: Efficient Time and Space Dependent Patrols to Combat Oil-Siphoning in International Waters. (2018). https://www.aaai.org/ocs/index.php/AAAI/AAAI18/paper/view/16312

[34] Bryan Wilder, Amulya Yadav, Nicole Immorlica, Eric Rice, and Milind Tambe. 2017. Uncharted but not uninfluenced: Influence maximization with an uncertain network. In *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 1305–1313.

[35] Bryan Wilder12, Nicole Immorlica, Eric Rice24, and Milind Tambe12. 2018. Maximizing Influence in an Unknown Social Network. (2018).

[36] WWF. 2015. Developing an approach to community-based crime prevention. http://zeropoaching.org/pdfs/Community-based-crime%20prevention-strategies.pdf. (2015).

[37] WWF. 2015. WWF and zero poaching: Vision. Mission. Strategy. http://tigers.panda.org/reports/zero-poaching/. (2015).

[38] Amulya Yadav, Hau Chan, Albert Xin Jiang, Haifeng Xu, Eric Rice, and Milind Tambe. 2016. Using social networks to aid homeless shelters: Dynamic influence maximization under uncertainty. In *Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 740–748.

[39] Amulya Yadav, Ritesh Noothigattu, Eric Rice, Laura Onasch-Vera, Leandro Soriano Marcolino, and Milind Tambe. 2018. Please be an Influencer?: Contingency-Aware Influence Maximization. (2018).

[40] Amulya Yadav, Bryan Wilder, Eric Rice, Robin Petering, Jaih Craddock, Amanda Yoshioka-Maxwell, Mary Hemler, Laura Onasch-Vera, Milind Tambe, and Darlene Woo. 2018. Bridging the Gap Between Theory and Practice in Influence Maximization: Raising Awareness about HIV among Homeless Youth.. In *IJCAI*. 5399–5403.

[41] Rong Yang, Christopher Kiekintveld, Fernando Ordonez, Milind Tambe, and Richard John. 2011. Improving resource allocation strategy against human adversaries in security games. In *IJCAI Proceedings-International Joint Conference on Artificial Intelligence*, Vol. 22. Barcelona, 458.

[42] Rong Yang, Fernando Ordonez, and Milind Tambe. 2012. Computing optimal strategy against quantal response in security games. In *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 2*. International Foundation for Autonomous Agents and Multiagent Systems, 847–854.