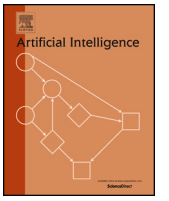
Artificial Intelligence 334 (2024) 104162

Contents lists available at ScienceDirect

Artificial Intelligence

journal homepage: www.elsevier.com/locate/artint



An extensive study of security games with strategic informants

Weiran Shen [a,*], Minbiao Han [d], Weizhe Chen [b], Taoan Huang [b], Rohit Singh [c], Haifeng Xu [d], Fei Fang [e]

[a] *Renmin University of China, China*
[b] *University of Southern California, United States of America*
[c] *World Wide Fund for Nature, Singapore*
[d] *University of Chicago, United States of America*
[e] *Carnegie Mellon University, United States of America*

ARTICLE INFO

Keywords:
Security game
Informant
Community engagement
Stackelberg game

ABSTRACT

Over the past years, game-theoretic modeling for security and public safety issues (also known as *security games*) have attracted intensive research attention and have been successfully deployed in many real-world applications for fighting, e.g., illegal poaching, fishing and urban crimes. However, few existing works consider how information from local communities would affect the structure of these games. In this paper, we systematically investigate how a new type of players – *strategic informants* who are from local communities and may observe and report upcoming attacks – affects the classic defender-attacker security interactions. Characterized by a private type, each informant has a utility structure that drives their strategic behaviors.

For situations with a single informant, we capture the problem as a 3-player extensive-form game and develop a novel solution concept, Strong Stackelberg-perfect Bayesian equilibrium, for the game. To find an optimal defender strategy, we establish that though the informant can have infinitely many types in general, there always exists an optimal defense plan using only a linear number of patrol strategies; this succinct characterization then enables us to efficiently solve the game via linear programming. For situations with multiple informants, we show that there is also an optimal defense plan with only a linear number of patrol strategies that admits a simple structure based on plurality voting among multiple informants.

Finally, we conduct extensive experiments to study the effect of the strategic informants and demonstrate the efficiency of our algorithm. Our experiments show that the existence of such informants significantly increases the defender's utility. Even though the informants exhibit strategic behaviors, the information they supply holds great value as defensive resources. Compared to existing works, our study leads to a deeper understanding on the role of informants in such defender-attacker interactions.

* Corresponding author.
E-mail addresses: shenweiran@ruc.edu.cn (W. Shen), minbiaohan@uchicago.edu (M. Han), weizhech@usc.edu (W. Chen), taoanhua@usc.edu (T. Huang), rsingh@wwf.sg (R. Singh), haifengxu@uchicago.edu (H. Xu), feif@cs.cmu.edu (F. Fang).

https://doi.org/10.1016/j.artint.2024.104162
Received 24 March 2023; Received in revised form 3 June 2024; Accepted 5 June 2024

Available online 12 June 2024

1. Introduction[1]

Protecting wildlife and other natural resources against illegal activities, such as poaching, remains one of the world's most common pressing challenges [2,3]. However, due to insufficient funding and other supportive resources, the current low number of defensive resources (compared with the number of targets that need protection) makes protection even harder [4]. The significant disparity between protection needs and available defensive resources has led to intensive research efforts in the allocation of resources to fight these illegal activities.

Existing work on security games models the interaction between the defensive units (such as rangers) and their opponents (such as poachers and illegal loggers) as a defender-attacker security game [2,5,6], and develops algorithms to compute an optimal strategy to protect those natural resources for the defender. The classic defender-attacker security game is a game played by two players, who are referred to as the defender and the attacker. The defender moves first by committing to a defense plan. Under conventional security game terminology, the term "patrol strategy" is referred to as how the defender allocates their defensive units to the targets. However, in this paper, the strategic behaviors of the defender are notably more intricate (e.g., additional design of informant message set). In order to avoid potential ambiguities, we employ the term "defense plan" to describe this complicated defender strategy with an informant message set. However, we still utilize the term "patrol strategy" to specifically allude to the distribution of defensive units after receiving messages from the informants. After observing the defense plan, the attacker responds by attacking some target. Perhaps surprisingly, an important factor, community engagement, has thus far largely been ignored in the literature despite the wide real-world practice of employing local communities for the assistance of surveillance. This paper aims to bridge this gap by developing richer security game models to incorporate information from local communities, and designing better defense tactics.

An example motivating domain is the green security game for preventing illegal poaching in national parks. When there are no detectable traces of poaching activity in the landscape, encouraging local communities to engage and serve as a surveillance role has been listed as one of the six pillars towards zero-poaching [7], and also plays an important role in other domains, such as fighting urban crime [8]. However, the local communities may have their own utility structures and can be unwilling to cooperate. For example, if some poaching activities are observed around a farm, the farmer may not give out such information, or even provide false information, if the farm is suffering loss from the human-wildlife conflict, where there is a direct or indirect negative interaction between wild animals and human activities [9]. Such strategic behavior poses additional challenges in designing better strategies for the defender.

To capture these strategic behaviors, we introduce a new kind of player – strategic informants – to the standard security game and aim to understand how this new player would affect the original game between the defender and the attacker. The informants may have different types that correspond to different utility structures. We first consider the single informant case. We model the game as an extensive-form game as it involves sequential movements of the players and view the informant as an extra layer between the defender and the attacker: after the attacker sets a target but before the attack is successfully completed, the informant strategically chooses whether to report and what message to report to the defender. When making a defense plan, the defender needs to take the strategic reasoning of both the attacker and the informants into consideration.

Given the structure of the 3-player game, we propose a new solution concept called *strong Stackelberg-perfect Bayesian equilibrium (SS-PBE)*. Essentially, such a solution concept is motivated by viewing the game from two different levels. At a lower level, we choose the perfect Bayesian equilibrium as the solution to the subgame between the attacker and the informant. At a higher level, we view the game as a Stackelberg game between the defender and the other two players. We show that the defender can actually enforce the best perfect Bayesian equilibrium of the subgame by introducing a slight perturbation to the defense plan.

The defender's defense plan contains 3 components: the set of messages that an informant can report, the routine patrol strategy, and the informed patrol strategy. The routine patrol strategy is used when the informant reports nothing, and the informed patrol strategy is a function that maps the reported messages to an actual coverage probability of the targets.

An informant may report different messages under different situations. At first glance, the number of possible messages the defender needs to design seems to depend on the number of different informant types. This makes the problem intractable as there can be infinitely many different informant types. We borrow tools from the mechanism design literature and show that a variant of the revelation principle holds in our setting. Based on that, in the case with a single informant, we reduce the number of messages to $n+1$ (n is the number of targets) in the case with a single informant, which does not depend on the number of informant types. Following the convention of solving Stackelberg games, we formulate the problem of finding the optimal defense plan in this case as solving multiple linear programs.

In the case of multiple informants, the information provided by the informants may not coincide as they may have conflicting interests. If the number of informants is constant, the optimal defense plan can still be found efficiently by solving a set of linear

[1] A preliminary version of the work [1] appeared in Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence. In the preliminary version, we focused on analyzing security games with a single strategic informant. This article substantially extends the preliminary version by adding a series of results on *multiple* strategic informants (Section 4 & 5; pages 9 to 17, 18 to 20). First of all, we show the properties of the single strategic informant case such as the revelation principle can carry over to the case with multiple strategic informants. Based on this, we develop a linear program to solve for the optimal defense plan with multiple informants by taking into account all possible message profiles (Program (11)). However, it turns out this problem becomes much more complicated with multiple informants because the size of all message profiles grows *exponentially* with the number of informants. In order to overcome the computational hardness, we propose a novel plurality voting defense plan (Program (17)). Then we show how the optimal plurality voting plan can be computed efficiently by linear programming while still providing the optimal defender utility (Theorem 7). Finally, we conduct additional experiments on the security game with multiple strategic informants (Section 5.4 & 5.5) to demonstrate the influence of multiple informants.

programs. However, if the number of informants is not constant, we cannot afford to enumerate possible message combinations reported by the informants. To handle this case, we propose a voting-based defense plan. Our defense plan scales well with respect to the number of informants and is optimal.

To show the effect of strategic informants, we conduct experiments to evaluate both the defender's and the attacker's utility and the number of defensive resources needed, by changing the informant type distribution. Our experiments also show that the defender can suffer a huge utility loss if they fail to take into account the informants' strategic behaviors, which implies that the informants and their strategic behaviors play an important role in the game. Our results provide a useful guideline for law enforcement agencies when facing strategic informants.

1.1. Related works

The most relevant topic is the Stackelberg games [10,11]. Stackelberg Security Game [2] has been applied to a variety of security problems [12,5,13,6]. Previous work on green security games with community engagement [14] has considered the presence of non-strategic informants, whereas we consider informants with their own utility structures. Security games with the presence of alarm systems, drones, and cameras that can provide real-time information have also been studied [15–17]. These works differ from ours in that the informants in our setting can have strategic behaviors. Gan et al. [18] studies security games with deceptive attackers. Xu et al. [19], Bondi et al. [20] study a variant of the security game that considers sensors with detection and signaling capability. All these papers involve additional information processing of the defender. However, none of them considers information from a third party.

Our work also makes use of the revelation principle [21] in mechanism design and is closely related to finding equilibria in extensive form games [22].

In criminology, Smith and Humphreys [23], Moreto [24], Duffy et al. [25] investigate the role of community engagement in wildlife conservation. Based on the network of reliable informants, Linkie et al. [26], Gill et al. [27] show the positive effects of community-oriented strategies. However, none of these works consider the effects of strategic informants and how to design the defender's strategies in the presence of such informants.

In evolutionary game theory, Short et al. [28] shows the effect of the presence of informants and Short et al. [29] solves for the optimal informant recruitment strategy.

2. Preliminaries

We consider a game with 3 different parties: the defender, the attacker, and the informants. Let $T = \{1, 2, \dots, n\}$ be the set of targets and assume that the defender has r defensive resources. We say a target is *covered*, if the defender sends a defensive resource to protect it. When a covered target t is attacked, the attacker gets penalty P_t^a and the defender gets reward R_t^d; Otherwise, if an uncovered target is attacked, the attacker gets reward R_t^a and the defender gets penalty P_t^d. We assume $R_t^d > P_t^d$ and $R_t^a > P_t^a$, which means both agents strictly prefer the reward over penalty for all t.

Suppose that when the attacker plans to attack, the attacked target t may be observed by an informant with probability p_w. The attacker's strategy is defined as $y \in \Delta(T) = \{y : \sum_{t \in T} y_t = 1\}$.[2] Each informant has a private type θ, which is randomly drawn from a finite set Θ of all possible informant types according to a publicly known probability distribution $p(\theta)$.[3] An informant with type θ gets utility $U_t^c(\theta)$ ($U_t^u(\theta)$) if the attacked target t is covered (uncovered), and we assume, throughout the paper, that each informant is not indifferent to the attack for any target, i.e., $U_t^c(\theta) \neq U_t^u(\theta), \forall t, \theta$. This is because in cases where an informant remains indifferent, the defender has the opportunity to acquire helpful information at a minimal cost by offering auxiliary rewards to the informant.

Assume there are k informants. The defender's defense plan is a tuple $d = (M, x, x^0)$ containing a routine patrol strategy x^0 (when no messages are reported), a set of possible messages M, and a patrol strategy $x : M^k \mapsto [0, 1]^n$ that maps the reported messages to a patrol strategy, which is an n-dimensional vector, with each element being the coverage probability of the corresponding target. A patrol strategy x is feasible if the sum of all elements is less than the number of defensive resources, i.e., $\sum_i x_i(m) \leq 1$, where m is any reported message profile. The set M is defined by the defender, this is because allowing the informant to report arbitrary messages can lead to inconsistent or conflicting defense strategies. For simplicity and model tractability, it is typically assumed that M is a finite set. This allows for the formulation of linear programming (LP) problems to determine optimal defense strategies, where the dimension of the LP scales with the size of M. It is also common to assume that the defender makes their defense plan public. Making the defense plan public is a widely adopted assumption in Stackelberg (security) games [3,30,31], which can enhance transparency and communication, allowing potential informants and attackers to understand the defender's intentions and security measures.

After observing the attack target t, each informant i can choose to send a message $m_i \in M$ to the defender. The defender then uses the tip-guided patrol strategy $x(m)$ against the attacker, where m is the reported message profile. We summarize all notations in Table 1.

[2] We start from this general definition and will later show the optimal attacker strategy can be achieved by a pure strategy, which is also consistent with the literature.

[3] We note that while there can be an infinite number of types for the informant in general, the relevant informant type is solely determined by whether the informant is aligned with the defender or attacker for each target, regardless of their precise utility parameters. Consequently, it is reasonable to simplify the analysis by considering a finite set of informant types without sacrificing generality.

Table 1
Notations used in this paper.

$T = \{1, 2, \cdots, n\}$	The set of targets
r	The number of defensive resources
P_t^d / R_t^d	Defender penalty/reward for target t
P_t^a / R_t^a	Attacker penalty/reward for target t
$m \in M$	Messages reported by the informants
$x^0 \in [0,1]^n$	Routine patrol strategy
$x : M^k \mapsto [0,1]^n$	Tip-guided patrol strategy
$d = (M, x, x^0)$	Defender's defense plan
$y \in \Delta(T)$	Attacker strategy
$\theta \in \Theta$	Informant type
$p(\theta)$	Publicly known prior distribution over informant type
p_w	The probability each informant observes the attack
$U_t^c(\theta)/U_t^u(\theta)$	Informant utility when target t is covered/uncovered
$\Theta^+(t)$, $\Theta^-(t)$	The sets $\{\theta : U_t^c(\theta) > U_t^u(\theta)\}$ and $\{\theta : U_t^c(\theta) < U_t^u(\theta)\}$
$p_+(t)$, $p_-(t)$	$p_+(t) = \sum_{\theta \in \Theta^+(t)} p(\theta)$, $p_-(t) = \sum_{\theta \in \Theta^-(t)} p(\theta)$

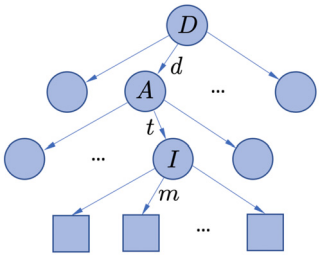


Fig. 1. Game tree of the security game with strategic informants, where we omit the step of Nature choosing the informant types.

We assume that the attacker is rational (utility-maximizing) and aware of the existence of strategic informants when deciding the attack strategy y. The type of each informant is private information, i.e., only known to the informant themselves. The goal of the defender is to design a defense plan (M, x, x^0) to maximize their expected utility.

Formally, we consider the security game with strategic community engagement defined below:

Definition 1. The security game with strategic community engagement (Fig. 1) proceeds as follows:

1. The defender announces a defense plan $d = (M, x, x^0)$;
2. Observing the defense plan, the attacker decides on an attack strategy y, and chooses a target t according to y;
3. If an informant i observes t, they can remain silent or send a message m_i to the defender (e.g., "Target t will be attacked" or "The attacker will go south");
4. According to the reported messages m, the defender adopts the patrol strategy defined by the announced defense plan.
5. The security resources are allocated according to the chosen patrolling strategy; target t is attacked, and the game reaches an outcome.

3. The single informant case

In this section, we consider the case with only a single informant. This case is much easier to analyze since we do not need to consider the game among the informants. For simplicity, we denote that an informant reports a dummy message $\perp$ if the informant observes the target but chooses to report nothing. In this case, we assign the value x^0 to the dummy message, meaning $x(\perp) = x^0$.

3.1. Solution concept

To establish our solution concept for the above game, we first focus on the subgame between the attacker and the informant while the defender's defense plan (M, x, x^0) is considered as given and fixed. We call the subgame the "attacker-informant" game. In this game, the attacker moves first, and then with probability p_w, the informant observes the attack and chooses a message according to their type. We consider *perfect Bayesian equilibrium* as the solution concept for the subgame.

Definition 2 *(Perfect Bayesian equilibrium (PBE))*. A perfect Bayesian equilibrium is a solution to an extensive form game if the following two conditions are satisfied:

1. Sequential rationality: each player's strategy is optimal given the player's belief;
2. Belief consistency: each player's belief is updated according to Bayes' rule.

For any target $t \in T$, any informant type $\theta \in \Theta$, and any reported message $m \in M$, the expected utilities of the attacker, the defender, and the informant can be written as:

$$\begin{aligned} U_a(t,m) =& (1-p_w)[x_t^0 P_t^a + (1-x_t^0)R_t^a] + \\ & p_w[x_t(m)P_t^a + (1-x_t(m))R_t^a], \end{aligned} \tag{1}$$

$$\begin{aligned} U_d(t,m) =& (1-p_w)[x_t^0 R_t^d + (1-x_t^0)P_t^d] + \\ & p_w[x_t(m)R_t^d + (1-x_t(m))P_t^d], \end{aligned} \tag{2}$$

$$\begin{aligned} U(t,m;\theta) =& (1-p_w)[x_t^0 U_t^c(\theta) + (1-x_t^0)U_t^u(\theta)] + \\ & p_w[x_t(m)U_t^c(\theta) + (1-x_t(m))U_t^u(\theta)], \end{aligned} \tag{3}$$

where the first part of the utility terms denotes the players' expected utilities if the informant does not observe the attack, and the second part denotes their utilities if the attack is observed.

Lemma 1. *Given a defender defense plan (M, x, x^0), let $m = m(t;\theta)$ be any strategy of the informant. There exists an attacker strategy y, such that (y,m) is a perfect Bayesian equilibrium of the attacker-informant game, if and only if m satisfies*[4]*:*

$$U_i(t,m;\theta) = \max_{m' \in M} \{U(t,m';\theta)\}, \forall t, \theta. \tag{4}$$

Moreover, for any perfect Bayesian equilibrium (y,m), the utilities for all three players in the original game only depend on the attacker strategy y.

Proof. (y,m) **is a PBE** $\Rightarrow$ m **satisfies Equation** (4)**.** The informant knows their own type and only the attacker has a belief about the informant's type. And since the attacker moves first and only moves once in the game, their belief will remain as the prior type distribution $p(\theta)$ during the two-step game. The informant has access to the attacker's actual action. As (y,m) is a perfect Bayesian equilibrium, by definition, we have $\forall t, \theta$:

$$m(t;\theta) \in \arg\max_m \{U(t,m;\theta)\} = \begin{cases} \arg\max_m x_t(m) & \text{if } U_t^c(\theta) > U_t^u(\theta) \\ \arg\min_m x_t(m) & \text{if } U_t^c(\theta) < U_t^u(\theta) \end{cases}. \tag{5}$$

m **satisfies Equation** (4) $\Rightarrow$ (y,m) **is a PBE.** Since the above equation does not involve the attacker's strategy y, any informant strategy satisfying Equation (4) is actually a weakly dominant strategy. The above equation also implies that given any type θ, any such strategy $m(t;\theta)$ results in the same coverage probability $x_t(m)$ for target t. On the other hand, when the attacker moves, their strategy should optimize the expected utility:

$$\begin{aligned} \mathop{\mathbf{E}}_{\theta,t}[U_a(t,m)] &= \sum_{\theta\in\Theta} p(\theta) \sum_{t\in T} y(t) \left\{ (1-p_w)[x_t^0 P_t^a + (1-x_t^0)R_t^a] + \right. \\ &\qquad \left. p_w[x_t(m)P_t^a + (1-x_t(m))R_t^a] \right\} \\ &= \sum_t y(t) \left\{ (1-p_w)[x_t^0 P_t^a + (1-x_t^0)R_t^a] + \right. \\ &\qquad \left. p_w \left[P_t^a \sum_\theta p(\theta) x_t(m) + R_t^a \sum_\theta p(\theta)(1-x_t(m)) \right] \right\}. \end{aligned}$$

Thus the attacker's expected utility only depends on the coverage probability $x_t(m)$ for each t and θ. To best respond, the attacker only needs to choose any distribution y over the set $\arg\max_t \mathbf{E}_{\theta,t}[U_a(t,m)]$.

The above analysis shows that switching to any other strategy satisfying Equation (4) does not change the utilities for both the attacker and the informant. Thus in any PBE (y,m) the expected utilities for both of them only depend on y. To show that the expected utility for the defender also only depends on y, simply notice that the defender's expected utility also only depends on the actual coverage probability of each target (Equation (2)). □

Corollary 1. *It is without loss of generality to only consider a pure strategy for the informant, i.e., the informant reports one message deterministically.*

Proof. Immediate from Lemma 1. □

[4] Throughout the paper, we assume $\max_{m'} \{U_i(t,m';\theta)\}$ always exists even if $|M| = \infty$. Otherwise, there can be no equilibrium.

According to Lemma 1, in the original game, the defender's expected utility may depend on how the attacker breaks ties. In the same spirit of the strong Stackelberg equilibrium, we consider the following solution concept:

Definition 3 *(Strong Stackelberg-perfect Bayesian equilibrium (SS-PBE)).* A strategy profile (d, y, m) is a Strong Stackelberg-perfect Bayesian equilibrium if:

1. (y, m) is a perfect Bayesian equilibrium:

$$y = \arg\max_{y'} \sum_{\theta\in\Theta} p(\theta) \sum_{t\in T} y(t)\big\{(1-p_w)[x_t^0 P_t^a + (1-x_t^0)R_t^a] + p_w[x_t(m)P_t^a + (1-x_t(m))R_t^a]\big\}$$

$$m(t;\theta) = \arg\max_{m'} U_i(t, m'; \theta), \quad \forall t, \theta;$$

2. the attacker breaks ties in favor of the defender;
3. based on the above two conditions, x maximizes the defender's expected utility:

$$x = \arg\max_{x'} \sum_{\theta\in\Theta} p(\theta) \sum_{t\in T} y(t)\left\{(1-p_w)[x_t^0 R_t^d + (1-x_t^0)P_t^d] + p_w[x_t(m)R_t^d + (1-x_t(m))P_t^d]\right\}.$$

Lemma 2. *It is without loss of generality to assume that the informant always reports a message in M after observing any attack target. In addition, there always exists an SS-PBE where the following property holds:*

$$\min_{m\in M} x_t(m) = x_t^0 = x_t(\perp) \le \max_{m\in M} x_t(m), \forall t.$$

Proof. Let (d, y, m) be any SS-PBE. By definition, we have $x_t^0 = x_t(\perp)$. Thus, $\min_{m\in M} x_t(m) \le x_t^0 \le \max_{m\in M} x_t(m)$. So it remains to show $\min_{m\in M} x_t(m) = x_t^0$. Assume, on the contrary, that $x_t^0 < \min_{m\in M} x_t(m)$ for some t. Then we can modify x by adding a new message m' to M with

$$x_t(m') = x_t^0,$$

$$\min_{m\in M} x_{t'}(m) \le x_{t'}(m') \le \max_{m\in M} x_{t'}(m), \forall t' \ne t.$$

Clearly, (d, y, m) is still an SS-PBE. And according to Equation (5) and Lemma 1, it would still be an SS-PBE if we slightly modify m so that the informant always breaks ties to favor reporting a message in M. For example, we can set $m_t(\theta) = m'$ for all θ with $U_t^c(\theta) < U_t^u(\theta)$. We can repeat the above process until the condition in the lemma is satisfied. During the process, all three players' utilities remain the same, and in the final SS-PBE, the informant always reports a message in M after observing any attack target. □

3.2. The optimal defense plan

Once the attacker has chosen a target t to attack according to the distribution $y \in \Delta(T)$, the expected utilities for both the attacker and the defender only depend on the defender's actual coverage probability x_t of target t, which, in turn, depends on the informant's reported message m. In general, the concrete meaning of the message is irrelevant as long as both the informant and the defender interpret it as the same patrol strategy $x(m)$. However, to help later analysis, we start with the case where $\bar{M} = T \times \Theta$ and consider the following direct defense plan, analogous to the direct or revelation mechanism in the mechanism design literature.

Definition 4 *(Direct defense plan).* A direct defense plan is a tuple $(\bar{M}, \bar{x}, \bar{x}^0)$ where $\bar{M} = T \times \Theta$.

Definition 5 *(Incentive compatibility).* A direct defense plan is incentive compatible, or truthful, if the informant's best strategy is to report the actual target of the attacker and their true type, i.e., $(t, \theta) = m(t; \theta) \in \bar{M}, \forall t \in T, \forall \theta \in \Theta$.

Now we consider a variant of the well-known revelation principle [21] that fits in our setting. We provide a brief proof for completeness.

Theorem 1 *(Revelation principle [21]). For any defense plan (M, x, x^0), there exists a truthful direct defense plan $(\bar{M}, \bar{x}, \bar{x}^0)$, such that for any target t chosen by the attacker, and any informant type θ, all the 3 players obtain the same expected utilities as in the original defense plan.*

The intuition behind the revelation principle is to let the mechanism "lie" for the informant (See Fig. 2).

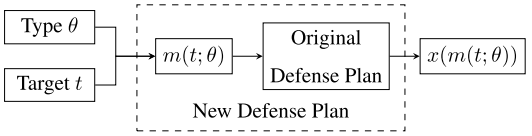


Fig. 2. Framework of the revelation principle.

Proof. Let $m = m(t;\theta)$ be the informant's strategy in the original defense plan. Then the defender uses the patrol strategy $x(m(t;\theta))$. Let $\bar{x}^0 = x^0$ and define $\bar{x}(t,\theta) = x(m(t;\theta)), \forall t, \forall\theta$. It is easy to see that the direct plan $(\bar{M}, \bar{x}, \bar{x}^0)$ is truthful. Otherwise, assume that reporting a different (t',θ') leads to a strictly higher informant's utility, i.e.,

$$\begin{aligned}&(1-p_w)[x_t^0 U_t^c + (1-x_t^0)U_t^u] + p_w[\bar{x}_t(t',\theta')U_t^c(\theta) + (1-\bar{x}_t(t',\theta'))U_t^u(\theta)]\\ >&(1-p_w)[x_t^0 U_t^c + (1-x_t^0)U_t^u] + p_w[\bar{x}_t(t,\theta)U_t^c(\theta) + (1-\bar{x}_t(t,\theta))U_t^u(\theta)].\end{aligned}$$

This means that in the original defense plan, we have:

$$\begin{aligned}&(1-p_w)[x_t^0 U_t^c + (1-x_t^0)U_t^u] + p_w\{x_t(m(t';\theta'))U_t^c(\theta) + [1-x_t(m(t';\theta'))]U_t^u(\theta)\}\\ >&(1-p_w)[x_t^0 U_t^c + (1-x_t^0)U_t^u] + p_w\{x_t(m(t;\theta))U_t^c(\theta) + [1-x_t(m(t;\theta))]U_t^u(\theta)\},\end{aligned}$$

which implies that $m(t',\theta')$ is a better strategy for the informant, contradicting Equation (4).

Now we show that all three players have the same expected utility under the new direct defense plan. According to Equation (1), (2) and (3), for any target t and informant type θ, all three players' utilities in the game only depend on the actual coverage probability $x_t(m)$ for the target. For any t and θ, the informant will report $m(t;\theta)$ and (t,θ) in both the two plan, resulting in coverage probabilities $x_t(m(t;\theta))$ and $\bar{x}_t(t,\theta)$. And we have $\bar{x}(t,\theta) = x(m(t;\theta))$ by definition. □

According to Theorem 1, it is without loss of generality to focus on truthful direct plans. We remark that this is only for ease of analysis, while in actual deployment, it may be more appropriate to still use the original format of defense plans, which does not consider the truthful direct defense plans but considers a simplified message set.

Although focusing on truthful direct defense plans simplifies our analysis, it is still challenging to compute the optimal plan for the defender. For each message m, we need to specify a patrol strategy, which contains $n = |T|$ variables. And we have $n|\Theta|$ possible messages, which means we need to determine $n^2|\Theta|$ different variables. This could lead to a heavy computational burden if $|\Theta|$ is very large.

However, we claim that it is possible to achieve the optimal defender's utility with only $n+1$ messages (no longer a direct defense plan of course), even though the number of different informant types cannot be controlled by the defender.

We view the game from the defender's perspective and define the *partial outcome* of the game to be the parameterized mapping $z : T \times \Theta \mapsto [0,1]$, that maps a target to its coverage probability, parameterized by the informant's type θ, or equivalently $z(t,\theta) = x_t(m(t;\theta))$.

The following lemma is useful for proving the above claim.

Lemma 3. *Given any message set M and any defender strategy $x(m)$, there are at most 2^n different outcomes, or equivalently, we only need to consider at most 2^n different informant types, since the outcome is parameterized by it.*

Proof. For each t and each θ, the partial outcome $z(t,\theta) = x_t(m)$ depends on the message $m(t;\theta)$, which in turn only depends on whether $U_t^c(\theta)$ is greater than $U_t^u(\theta)$ or not. The reason is that any two types θ and θ' that have the same property (e.g., $U_t^c(\theta) \geq U_t^u(\theta)$ and $U_t^c(\theta') \geq U_t^u(\theta')$) would favor the same outcome and report the same message. So for each target t, there are at most 2 different x_t's. And there can be at most 2^n different partial outcomes. □

Now we are ready to show that $|M| = n+1$ is sufficient to achieve the optimal defender's utility.

Theorem 2. *There exists a defender strategy $d = (M, x, x^0)$, with $|M| = n+1$, that achieves the optimal defender's utility.*

Proof. Let $\hat{d} = (\hat{M}, \hat{x}, \hat{x}^0)$ be an optimal truthful direct defense plan. We will construct a new defense plan based on $\hat{d}$. To ensure truthfulness, $\hat{x}$ must satisfy:

$$\hat{x}_t(t,\theta) \geq \hat{x}_t(t,\theta'), \forall\theta', \forall\theta \text{ with } U_t^c(\theta) > U_t^u(\theta),$$

$$\hat{x}_t(t,\theta) \leq \hat{x}_t(t,\theta'), \forall\theta', \forall\theta \text{ with } U_t^c(\theta) < U_t^u(\theta).$$

Therefore, if two different types θ and θ' both satisfy $U_t^c(\theta) > U_t^u(\theta)$ and $U_t^c(\theta') > U_t^u(\theta')$, then we must have $\hat{x}_t(t,\theta) = \hat{x}_t(t,\theta')$. The coverage probabilities of other targets are irrelevant as long as they guarantee truthfulness.

We construct the new defense plan $d = (M, x, x^0)$ as follows: first set $x^0 = \hat{x}^0$. Then for each t, let $\theta^+(t)$ be any informant type with $U_t^c(\theta^+(t)) > U_t^u(\theta^+(t))$. We add a message $m(t) = (t, \theta^+(t))$ for each t to M, and set $x(m(t)) = \hat{x}(t, \theta^+(t))$. In the end, we add $\perp$ to M and set $x_t(\perp) = x_t^0, \forall t$. Note that for any t, $x_t^0 = \hat{x}_t^0 = \hat{x}_t(\perp) = \min_{m \in \hat{M}} \{\hat{x}_t(m)\}$, we have that $x_t(\perp) = \min_{m \in \hat{M}} \{\hat{x}_t(m)\}, \forall t$.

With the above construction, we have $|M| = n + 1$. It is easy to check that $\sum_t x_t(m) \le r, \forall m \in M$. Now we show that this new defense plan has the same expected utility for the defender as in $\hat{d}$. For any target t, and any informant type θ, the informant will either choose to report $m(t)$ or $\perp$. For example, if θ satisfies $U_t^c(\theta) > U_t^u(\theta)$, then $x_t(m(t)) = \hat{x}_t(t, \theta^+(t)) = \max_{\theta'} \{\hat{x}_t(t, \theta')\} \ge \max_{m'} \{x_t(m')\}$. We also have $\hat{x}_t(t, \theta^+(t)) \ge x_t^0$ as $\hat{d}$ is truthful. This implies $x_t(m(t)) \ge x_t^0$, i.e., under the new defense plan d, this informant will report $m(t)$ instead of staying silent. If $U_t^c(\theta) < U_t^u(\theta)$, it is clear that $x_t(\perp) = \min_{m \in \hat{M}} \hat{x}_t(m) = \min_{m \in M} x_t(m)$. Similar to our argument above for the case of $U_t^c(\theta) > U_t^u(\theta)$, the informant with $U_t^c(\theta) < U_t^u(\theta)$ will report $\perp$ rather than nothing. This means that in defense plan d, no matter which target t the attacker chooses to attack, the informant will always choose a message that gives exactly the same expected defender (and also attacker and informant) utility as in $\hat{d}$. Taking expectation over t completes the proof. □

The intuition behind Theorem 2 is that the informant utility's dependence on the type ultimately represents the preference for a higher or lower coverage probability. Therefore, it suffices to let the informant ask to either increase or decrease the coverage probability. Note that decreasing the coverage probability on any target always leads to a feasible patrol strategy as it never uses more defensive resources.

Definition 6 *(Defender-aligned and attacker-aligned informant types).* An informant type θ is said to be defender-aligned if $U_t^c(\theta) > U_t^u(\theta), \forall t$, and attacker-aligned if $U_t^c(\theta) < U_t^u(\theta), \forall t$.

Lemma 4. *If all informant types are attacker-aligned, there exists an optimal defense plan where the defender always uses the routine patrol strategy x^0, i.e., sets $M = \emptyset$.*

Proof. For any defense plan $d = (M, x, x^0)$, the expected defender's utility is:

$$U_d = \sum_\theta p(\theta) \sum_t y(t) \Big\{ (1 - p_w) \left[x_t^0 R_t^d + (1 - x_t^0) P_t^d \right] + p_w \left[x_t(m(t;\theta)) R_t^d + (1 - x_t(m(t;\theta))) P_t^d \right] \Big\}.$$

Since all informant types are attacker-aligned, we have $U_t^c(\theta) < U_t^u(\theta), \forall t, \theta$, which means:

$$x_t(m(t;\theta)) = \min_{m'} x_t(m') \le x_t^0, \forall t, \theta,$$

where the inequality is by Lemma 2. Thus,

$$\begin{aligned} U_d &= \sum_\theta p(\theta) \sum_t y(t) \Big\{ (1 - p_w) \left[x_t^0 R_t^d + (1 - x_t^0) P_t^d \right] + \\ &\qquad p_w \left[x_t(m(t;\theta))(R_t^d - P_t^d) + P_t^d \right] \Big\} \\ &\le \sum_\theta p(\theta) \sum_t y(t) \Big\{ (1 - p_w) \left[x_t^0 (R_t^d - P_t^d) + P_t^d \right] + \\ &\qquad p_w \left[x_t^0 (R_t^d - P_t^d) + P_t^d \right] \Big\} \\ &= \sum_t y(t) [x_t^0 U_t^c + (1 - x_t^0) U_t^u], \end{aligned}$$

where the inequality is because $R_t^d > P_t^d$, and the last term is the defender's expected utility of always using x_t^0. Since the above analysis is true for any defense plan, it also holds for any optimal defense plan $\hat{d} = (\hat{M}, \hat{x}, \hat{x}^0)$. Thus always using $\hat{x}^0$ gives a weakly better utility, which implies that $\hat{x}^0$ alone is also optimal. □

Example 1 *(Effect of different informants).* Suppose there are two targets and the defender has $r = 1$ resource. Consider the following symmetric, zero-sum instance:

	1	2
1	$l, -l$	$-l, l$
2	$-l, l$	$l, -l$

The defender and the attacker are the row player and the column player, respectively. Clearly, when there is no informant, the defender will just use a strategy $(0.5, 0.5)$, which gives both the defender and the attacker a utility of 0. If there is a defender-aligned informant with $p_w = 1$, then in the optimal defense plan, the defender will always listen to the informant and allocate the 1 unit of defensive resource accordingly, which gives a utility of l. And if there is an attacker-aligned informant, according to Lemma 4, the optimal defense strategy is still to use $(0.5, 0.5)$, leading to a 0 utility. However, if the defender does not know that the informant is attacker-aligned but still listens to him, then the defender will end up with $-l$ utility.

Table 2
Additional notations for the security game with multiple informants.

$o \in \{0,1\}^k$	Each element indicates whether the corresponding informant observes the attacker or not
$p_+(s;k,t)$	Probability that s out of k informants reported a message t

We now consider how to compute an optimal defense plan. When deciding the attack strategy to optimize Equation (1), the attacker cannot observe the informant's type. Thus similar to the standard Stackelberg setting, the optimal attacker strategy can be achieved with a pure strategy, i.e., attacking a certain target with probability 1. We break ties in favor of the defender when attacking multiple targets gives the attacker the same expected utility.

With Theorem 2, we can index the $n+1$ messages such that $m_t = m(t)$, and $m_{n+1} = \perp$. To ensure that the informant always chooses m_t or m_{n+1} when t is the target, we need to guarantee that $x_t(m_t) \geq x_t(m') \geq x_t(m_{n+1}), \forall m' \in \boldsymbol{M}$.

To compute an optimal defense plan, we follow the approach of Conitzer and Sandholm [11] and solve a linear program (Program (6)) for each target t. After obtaining all the solutions to the programs, we choose the one that gives the defender the highest utility.

maximize:

$$\sum_{\theta} p(\theta)\Big\{(1-p_w)\left[x_t^0 R_t^d + (1-x_t^0)P_t^d\right] + p_w\left[x_t(m(t;\theta))R_t^d + (1-x_t(m(t;\theta)))P_t^d\right]\Big\}$$

subject to:

$$\begin{aligned}
&\sum_{\theta} p(\theta)\Big\{(1-p_w)\left[x_t^0 P_t^a + (1-x_t^0)R_t^a\right] + p_w\left[x_t(m(t;\theta))P_t^a + (1-x_t(m(t;\theta)))R_t^a\right]\Big\} \\
\geq\ &\sum_{\theta} p(\theta)\Big\{(1-p_w)\left[x_{t'}^0 P_{t'}^a + (1-x_{t'}^0)R_{t'}^a\right] + p_w\left[x_{t'}(m(t';\theta))P_{t'}^a + (1-x_{t'}(m(t';\theta)))R_{t'}^a\right]\Big\} && \forall t' \in T \\
& x_{t'}(m_{n+1}) \leq x_{t'}(m') && \forall m' \in \boldsymbol{M}, t' \in T \\
& x_{t'}(m_{n+1}) \leq x_{t'}^0 && \forall t' \in T \\
& x_{t'}(m_{t'}) \geq x_{t'}(m') && \forall m' \in \boldsymbol{M}, t' \in T \\
& x_{t'}(m_{t'}) \geq x_{t'}^0 && \forall t' \in T \\
& \sum_{t'} x_{t'}^0 \leq r \\
& 0 \leq x_{t'}^0 \leq 1 && \forall t' \in T \\
& \sum_{t'} x_{t'}(m) \leq r && \forall m \in \boldsymbol{M} \\
& 0 \leq x_{t'}(m) \leq 1 && \forall m \in \boldsymbol{M}, t' \in T
\end{aligned} \tag{6}$$

Theorem 3. *The optimal defense plan can be computed by solving LP (6) for all t and then choosing the best solution among them with the highest defender utility.*

Proof. The first constraint of Program (6) ensures that choosing target t is the best strategy for the attacker. The second to the fifth constraint ensures that the informant always reports m_t or m_{n+1}, i.e., $m(t;\theta)$ is either m_t or m_{n+1}. Also, the informant's strategy $m(t;\theta)$ only depends on the informant type θ given any target t and thus can be pre-computed based on $U_t^c(\theta)$ and $U_t^u(\theta)$. The remaining constraints are feasibility constraints that ensure x_t is always a probability, and that the total number of used resources does not exceed the total number of available resources. □

4. The multiple informants case

Now we consider the more challenging case with multiple informants, i.e., $k > 1$. In reality, it is possible that more than one informant report messages to the defender. And to make matters worse, these messages may even disagree with one another. Therefore, in this case, we need to consider the game among multiple informants. We first introduce additional notations to denote a security game with multiple strategic informants, listed in Table 2.

The game procedure is similar to the single informant case. The only difference is that after the attacker chooses a target to attack, all the informants are playing a Bayesian game among themselves. In this case, we need to slightly modify the definition of incentive compatibility.

Definition 7 *(Incentive compatibility).* A direct defense plan is incentive compatible if, in the game among the informants, it constitutes a Bayesian Nash equilibrium when all informants observing the attacker's target report truthfully.

Similar to Theorem 1, we can prove that the revelation principle still holds in this case. The following lemma shows that to achieve the optimal utility, the defender needs only $2n$ messages.

Lemma 5. *There exists an optimal defense plan with* $|M| = 2n + 1$.

Let θ_i be the type of informant i. We abuse notation and denote the type profile of all informants by $\theta = (\theta_1, \theta_2, \dots, \theta_k)$. Following game theoretic conventions, we use θ_{-i} to denote the type profile of all informants except i. We still use $d = (M, x, x^0)$ to denote a defense plan, where x^0 is still the routine patrol strategy when no message is reported to the defender, and x maps the reported messages to an informed strategy. Note that the routine patrol strategy $x^0 = x(\perp, \perp, \dots, \perp)$. For ease of presentation, we only consider x and ignore x^0 from now on. Let $o \in \{0,1\}^k$ be a binary vector with each element indicating whether an informant observes the attacker. Let $\Theta^+(t)$ and $\Theta^-(t)$ be the sets of informant types θ with $U_t^c(\theta) > U_t^u(\theta)$ and $U_t^c(\theta) < U_t^u(\theta)$, respectively.

Proof. According to the revelation principle, we can without loss of generality consider only truthful direct defense plans. Therefore, we have:

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, m_i)\right] \geq \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, m_i')\right], \forall m_i \in t \times \Theta^+(t), m_i' \in T \times \Theta, \tag{7}$$

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, m_i)\right] \geq \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, \perp)\right], \forall m_i \in t \times \Theta^+(t), \tag{8}$$

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, m_i)\right] \leq \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, m_i')\right], \forall m_i \in t \times \Theta^-(t), m_i' \in T \times \Theta, \tag{9}$$

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, m_i)\right] \leq \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, \perp)\right], \forall m_i \in t \times \Theta^-(t). \tag{10}$$

Specifically,

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, (\theta_i, t))\right] \geq \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, (\theta_i', t))\right], \forall \theta_i, \theta_i' \in \Theta^+(t),$$

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, (\theta_i, t))\right] \leq \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, (\theta_i', t))\right], \forall \theta_i, \theta_i' \in \Theta^-(t).$$

These imply:

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, (\theta_i, t))\right] = \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, (\theta_i', t))\right], \forall \theta_i, \theta_i' \in \Theta^+(t),$$

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, (\theta_i, t))\right] = \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}, (\theta_i', t))\right], \forall \theta_i, \theta_i' \in \Theta^-(t).$$

The above equations do not necessarily mean that $x_t(m_{-i}, (\theta_i, t)) = x_t(m_{-i}, (\theta_i', t))$ for any m_{-i}, if θ_i and θ_i' both belong to $\Theta^+(t)$ or $\Theta^-(t)$. However, we show that there exists an optimal defense plan where these equations hold.

Define

$$\bar{x}_t^+(m_{-i}) = \mathop{\mathbf{E}}_{o_i,\theta_i \in \Theta^+(t)}\left[x_t(m_{-i}, m_i)\right],$$

$$\bar{x}_t^-(m_{-i}) = \mathop{\mathbf{E}}_{o_i,\theta_i \in \Theta^-(t)}\left[x_t(m_{-i}, m_i)\right],$$

$$p_+(t) = \sum_{\theta \in \Theta^+(t)} p(\theta),$$

$$p_-(t) = \sum_{\theta \in \Theta^-(t)} p(\theta).$$

Consider the following strategy:

$$x_t'(m_{-i}, (\theta_i, t)) = \begin{cases} \bar{x}_t^+(m_{-i}) & \text{if } \theta_i \in \Theta^+(t) \\ \bar{x}_t^-(m_{-i}) & \text{if } \theta_i \in \Theta^-(t) \end{cases}.$$

Clearly, switching from x_t to x_t' does not affect informant i's behavior, as Equations (7) to (10) still hold. As for the resource constraint, we have:

$$\sum_t x_t(m) \le r, \forall m.$$

Taking expectation over o_i, θ_i conditioned on $\theta_i \in \Theta^+(t)$ yields:

$$\sum_t \mathop{\mathbf{E}}_{o_i, \theta_i \in \Theta^+(t)} [x_t(m_{-i}, m_i)] \le r, \forall m_{-i},$$

which indicates:

$$\sum_t x'_t(m_{-i}, (\theta_i, t)) \le r, \forall m_{-i}, \forall \theta_i \in \Theta^+(t).$$

Similarly, we also have:

$$\sum_t x'_t(m_{-i}, (\theta_i, t)) \le r, \forall m_{-i}, \forall \theta_i \in \Theta^-(t).$$

As for other agents, the expected utilities of the defender, the attacker, and other informants all depend on the expected coverage probability x_t, which, in turn, depends on m_i. And since the type θ_i and the observation indicator o_i are both independent of those of other informants, when computing an agent's utility, we can first fix m_i, take expectation over o_i, and then take expectation again over θ_i. This implies that all the terms involving m_i in the utility function of any agent except informant i can be expressed using $\bar{x}_t^+(m_{-i})$ and $\bar{x}_t^-(m_{-i})$. Therefore, changing from x_t to x'_t will also not affect other agents' utilities, hence their behaviors.

The above discussion implies that when designing patrol strategy x, we only need to care about whether an informant's type falls in $\Theta^+(t)$ or $\Theta^-(t)$. Therefore, along with possible targets T, $2n$ messages plus the dummy message $\perp$ suffice to achieve the optimal defender utility. □

Lemma 5 indicates that there are at most $(2n+1)^k$ different message profiles. The $2n+1$ messages used are $M = T \times \{+, -\} \cup \{\perp\}$, where the signs "+" and "−" indicate whether the informant wants the defender to increase the coverage probability for the corresponding target t reported by him. The extra one message $\perp$ compared to Lemma 5 is used when the informant does not report anything.

Given any target t, the message profile from k informants is determined by the informants' types θ and their observations o, denoted as $m(t, \theta, o)$. Similarly, we denote the message profile from all informants except for informant i as $m_{-i}(t, \theta_{-i}, o_{-i})$. Thus, when the number of total informants k is small, we can afford to enumerate strategies for all possible message profiles. To obtain the optimal solution, we can still solve a linear program for each target t and choose the best defense plan from the solutions.

maximize:

$$\mathop{\mathbf{E}}_{o,\theta} \left[x_t\big(m(t,\theta,o)\big) R_t^d + (1 - x_t\big(m(t,\theta,o)\big)) P_t^d \right]$$

subject to:

$$\begin{aligned}
&\mathop{\mathbf{E}}_{o,\theta} \left[x_t\big(m(t,\theta,o)\big) P_t^a + \big(1 - x_t\big(m(t,\theta,o)\big)\big) R_t^a \right] \\
\ge\ &\mathop{\mathbf{E}}_{o,\theta} \left[x_{t'}\big(m(t',\theta,o)\big) P_{t'}^a + (1 - x_{t'}\big(m(t',\theta,o)\big)) R_{t'}^d \right], && \forall t' \\
\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}} &\left[x_t(m_{-i}(t,\theta_{-i},o_{-i}), t^+) \right] \ge \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}} \left[x_t(m_{-i}(t,\theta_{-i},o_{-i}), m'_i) \right], && \forall m'_i \\
\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}} &\left[x_t(m_{-i}(t,\theta_{-i},o_{-i}), t^-) \right] \le \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}} \left[x_t(m_{-i}(t,\theta_{-i},o_{-i}), m'_i) \right], && \forall m'_i \\
\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}} &\left[x_t(m_{-i}(t,\theta_{-i},o_{-i}), \perp) \right] \le \mathop{\mathbf{E}}_{o_{-i},\theta_{-i}} \left[x_t(m_{-i}(t,\theta_{-i},o_{-i}), m'_i) \right], && \forall m'_i \\
&\sum_{t'} x_{t'}\big(m(t,\theta,o)\big) \le r, && \forall m, \theta, o \\
&0 \le x_{t'}\big(m(t,\theta,o)\big) \le 1, && \forall m, t', \theta, o
\end{aligned} \tag{11}$$

where $m_{-i}(t, \theta_{-i}, o_{-i})$ represents the other informants' truthful reports. Specifically, $m_{-i}(t, \theta_{-i}, o_{-i}) \in \left\{t^+, t^-\right\}^{k-1}$, and every informant among the $k-1$ informants reports t^+ if their type falls in $\Theta^+(t)$, and t^- otherwise.

However, it turns out that for this program, the defender can still benefit from strategic informants' reports even if they are fully attacker-aligned. For example, consider an extreme case where *all* strategic informants are *attacker-aligned* and observe the attacker's attack with probability 1. By the incentive compatibility constraint, all the informants will report t^- when they observe that the attacker is attacking some target t. However, these reports still help the defender to learn the actual target since all informants give the same report. Therefore, a rational defender would increase the coverage probability for target t. Naturally, an attacker-aligned informant would choose to report a dummy message $\perp$ instead of providing any helpful information. Thus, we consider the following strategy for the informants:

$$m_i(\theta_i, t, o_i) = \begin{cases} t^+ & \text{if } \theta_i \in \Theta^+(t) \text{ and } o_i = 1 \\ \perp & \text{otherwise} \end{cases}.$$

Clearly, the messages t^- are never used in this strategy. We can safely discard the superscript and simplify the message set to $M = T \cup \{\perp\}$. Therefore, we propose another defense plan with $M = T \cup \{\perp\}$ under which using the above strategy forms an equilibrium among the informants. In this case, there are at most $(n+1)^k$ different message profiles in total. Similarly, the linear program that maximizes the defender's utility with respect to target t can be written as follows.

$$
\begin{aligned}
&\text{maximize:} \\
&\qquad \mathbf{E}_{o,\theta}\left[x_t\big(m(t,\theta,o)\big)R_t^d + \big(1 - x_t(m(t,\theta,o))\big)P_t^d\right] \\
&\text{subject to:} \\
&\qquad \mathbf{E}_{o,\theta}\left[x_t\big(m(t,\theta,o)\big)P_t^a + \big(1 - x_t(m(t,\theta,o))\big)R_t^a\right] \\
&\geq \mathbf{E}_{o,\theta}\left[x_{t'}\big(m(t',\theta,o)\big)P_{t'}^a + \big(1 - x_{t'}(m(t',\theta,o))\big)R_{t'}^d\right], \qquad \forall t' \\
&\mathbf{E}_{o_{-i},\theta_{-i}}\left[x_t\big(m_{-i}(t,\theta_{-i},o_{-i}),t^+\big)\right] \geq \mathbf{E}_{o_{-i},\theta_{-i}}\left[x_t\big(m_{-i}(t,\theta_{-i},o_{-i}),m_i'\big)\right], \quad \forall m_i' \\
&\mathbf{E}_{o_{-i},\theta_{-i}}\left[x_t(m_{-i}(t,\theta_{-i},o_{-i}),\perp)\right] \leq \mathbf{E}_{o_{-i},\theta_{-i}}\left[x_t\big(m_{-i}(t,\theta_{-i},o_{-i}),m_i'\big)\right], \quad \forall m_i' \\
&\qquad \textstyle\sum_{t'} x_{t'}\big(m(t,\theta,o)\big) \leq r, \qquad \forall m,\theta,o \\
&\qquad 0 \leq x_{t'}\big(m(t,\theta,o)\big) \leq 1, \qquad \forall m,t',\theta,o
\end{aligned}
\tag{12}
$$

Theorem 4. *The optimal defense plan with multiple informants can be computed by solving LP* (12) *for all* $t = 1, \cdots, n$ *and then choosing the best solution among them with the highest defender utility.*

Proof. The first constraint of Program (12) ensures that choosing target t is the best strategy for the attacker. The second to the fifth constraint ensures that the informant always reports t^+ or $\perp$, i.e., $m(t;\theta)$ is either t^+ or $\perp$. The remaining constraints are feasibility constraints that ensure x_t is always a probability, and that the total number of used resources does not exceed the total number of available resources. The objective is the defender's expected utility given the attacker attacking target t. □

However, the above program does not scale well due to the exponential number of message profiles (i.e., $(n+1)^k$). To solve this problem, we propose a defense plan based on plurality voting. Let x^* be the optimal defense plan obtained by solving Program (12) for each target $t \in T$. Denote by s the number of informants who report a message t.

Definition 8 *(Naïve plurality voting defense plan).* A naïve plurality voting defense plan x is defined as follows. If $s > 2$, we apply plurality voting to these s messages to determine a target t (the target reported by most informants), and allocate an entire unit of resource to t. If $s \leq 2$, the defender uses patrol strategy x^*.

However, the above defense plan still involves x^* which can only be obtained by solving Program (12). What is more, the plurality voting defense plan only cares about the number of informants who report t instead of which informants report t. As a result, we can ignore the informants' identity and denote by $m^{s,t}$ the message profile representing that exactly s informants report message t and all the others report messages $\perp$, and $m_{-i}^{s,t}$ the same message profile excluding the message reported by informant i.

Let

$$
p_+(s;k,t) = \binom{k}{s}\left[p_+(t)p_w\right]^s\left[1 - p_+(t)p_w\right]^{k-s}
$$

be the probability that s out of k informants report message t. Thus, the expected utility of the defender is:

$$
\sum_{s=0}^{2} p_+(s;k,t)\left[x_t(m^{s,t})R_t^d + (1 - x_t(m^{s,t}))P_t^d\right] + R_t^d\sum_{s=3}^{k} p_+(s;k,t).
$$

Recall that $m_i(t;\theta)$ represents the strategy of an informant with type θ when observing target t. To ensure that the informants report message t (i.e., $m_i(t;\theta) = t$) when $\theta \in \Theta^+(t)$, and message $\perp$ ($m_i(t;\theta) = \perp$) when $\theta \in \Theta^-(t)$, we need to design the patrol strategy x such that reporting other messages leads to a weakly lower expected utility. When $\theta \in \Theta^+(t)$, the informant benefits from increasing the expected coverage probability of target t. So we need to ensure that for all possible $m_i' \neq t$:

$$
\begin{aligned}
&\sum_{s=0}^{1} p_+(s;k-1,t)x_t(m_{-i}^{s,t},t) + \sum_{s=2}^{k-1} p_+(s;k-1,t) \\
&\geq \sum_{s=0}^{2} p_+(s;k-1,t)x_t(m_{-i}^{s,t},m_i') + \sum_{s=3}^{k-1} p_+(s;k-1,t),
\end{aligned}
$$

which is equivalent to:

$$
\sum_{s=0}^{1} p_+(s;k-1,t)x_t(m_{-i}^{s,t},t) + p_+(2;k-1,t) \geq \sum_{s=0}^{2} p_+(s;k-1,t)x_t(m_{-i}^{s,t},m_i'). \tag{13}
$$

Note that $(m_{-i}^{s,t}, t) = m^{s+1,t}$ and that when $m_i' = \perp$, m_i' will be ignored by the defender and $(m_{-i}^{s,t}, m_i') = m^{s,t}$. Similarly, when $\theta \in \Theta^-(t)$, we need to ensure:

$$\sum_{s=0}^{2} p_+(s;k-1,t)x_t(m^{s,t}) \le \sum_{s=0}^{2} p_+(s;k-1,t)x_t(m_{-i}^{s,t}, m_i'). \tag{14}$$

When $m_i' = t$, we have $(m_{-i}^{s,t}, m_i') = m^{s+1,t}$ and $x_t(m^{3,t}) = 1$ by Definition 8.

Therefore, we can obtain the defense plan for $s \le 2$ by solving Program (15) for each target t. The second to the fourth constraints in Program (15) come from combining Equation (13) and (14).

Definition 9 *(Plurality voting defense plan).* A plurality voting defense plan x is defined to be the solution obtained by solving Program (15) for each target t and choosing the best one.

$$\begin{aligned}
&\text{maximize:} \\
&\quad \sum_{s=0}^{2} p_+(s;k,t)\left[x_t(m^{s,t})R_t^d + (1-x_t(m^{s,t}))P_t^d\right] + R_t^d \sum_{s=3}^{k} p_+(s;k,t) \\
&\text{subject to:} \\
&\quad \sum_{s=0}^{2} p_+(s;k,t)\left[x_t(m^{s,t})P_t^a + (1-x_t(m^{s,t}))R_t^a\right] + P_t^a \sum_{s=3}^{k} p_+(s;k,t) \\
&\ge \sum_{s=0}^{2} p_+(s;k,t')\left[x_{t'}(m^{s,t'})P_{t'}^a + (1-x_{t'}(m^{s,t'}))R_{t'}^a\right] + P_{t'}^a \sum_{s=3}^{k} p_+(s;k,t'), && \forall t' \\
&\quad \sum_{s=0}^{1} p_+(s;k-1,t)x_t(m^{s+1,t}) + p_+(2;k-1,t) \\
&\ge \sum_{s=0}^{2} p_+(s;k-1,t)x_t(m_{-i}^{s,t}, m_i'), && \forall t, m_i' \\
&\sum_{s=0}^{1} p_+(s;k-1,t)x_t(m^{s+1,t}) + p_+(2;k-1,t) \ge \sum_{s=0}^{2} p_+(s;k-1,t)x_t(m^{s,t}), && \forall t \\
&\sum_{s=0}^{2} p_+(s;k-1,t)x_t(m^{s,t}) \le \sum_{s=0}^{2} p_+(s;k-1,t)x_t(m_{-i}^{s,t}, m_i'), && \forall t, m_i' \\
&\sum_{t'} x_{t'}(m) \le r, && \forall m \\
&0 \le x_t(m) \le 1, && \forall t, m
\end{aligned} \tag{15}$$

Program (15) guarantees that under such a defense plan, using strategy $t = m_i(t;\theta)$ when $\theta \in \Theta^+(t)$ and $\perp = m_i(t;\theta)$ when $\theta \in \Theta^-(t)$ forms a Bayesian Nash equilibrium. Notice that we can no longer use the term "incentive compatibility" here, as the plurality voting defense plan is not a direct defense plan. But this property is similar to the incentive compatibility property in the sense that truthfully revealing the information required by the defender constitutes a Bayesian Nash equilibrium. Nevertheless, we will abuse notation and still use the term "incentive compatibility" to describe such a property.

Theorem 5. *The plurality voting defense plan is incentive compatible.*

Proof. Immediate from the constraints of Program (15). □

Since the plurality voting defense plan is incentive compatible, one can easily check that when $s > 2$, the defender can always correctly identify the target chosen by the attacker. It follows that in this case, the defender always catches the attacker with probability 1. However, this may not benefit the defender in the end. The reason is that the attacker may not choose the target that gives the defender the highest utility if he knows that he will always be caught with a high probability. In fact, the defender's utility may be arbitrarily worse compared with the optimal one. Consider the following extreme example:

Example 2. Suppose there are 3 informants with observation probability $p_w = 1$. All informants are defender-aligned, i.e., $U_t^c(\theta) > U_t^u(\theta), \forall t$ and $|\Theta| = 1$. The defender has 1 unit of defense resource. The utilities of the defender and the attacker are listed in Table 3.

In this example, if the defender adopts the plurality voting defense plan, all the 3 informants will always report the true target. And according to the plurality voting defense plan, the attacker will be caught with probability 1. In this case, the attacker will choose to attack target 2 since it gives the attacker a higher utility. As a result, the defender gets utility ε.

However, the defender can change the defense plan, and only covers target 1 with a probability of 0.5 when all the 3 informants report target 1 to the defender. In this case, the attacker's expected utility of attacking target 1 is 0.5ε, which is now slightly higher than that of attacking target 2. Thus the attacker will choose to attack target 1 and the defender's utility becomes 0.5. The ratio of the defender's utility in the two cases is $\frac{0.5}{\varepsilon}$, which approaches infinity as ε approaches 0.

Table 3
The defender and the attacker's payoff matrix. The first (second) number in each cell is the defender's (attacker's) utility.

	Target 1	Target 2
cover	$1,-1$	$\epsilon,0$
uncover	$0,1+\epsilon$	$-1,1$

Example 2 not only shows how the plurality voting defense plan can be arbitrarily worse than the optimal one, but also gives us insights on how to improve the plurality voting defense plan: by not being so greedy and lowering the coverage probabilities of certain targets. Let us first consider the following strategy.

Let x^∞ be an optimal patrol strategy when there is no informant but the defender has an unlimited number of resources, i.e., x^∞ is obtained by solving the following linear program for each target t and then choosing the best solution among them:

$$\begin{aligned} \text{maximize:} \quad & x_t R_t^d + (1-x_t)P_t^d \\ \text{subject to:} \quad & x_t P_t^a + (1-x_t)R_t^a \geq x_{t'} P_{t'}^a + (1-x_{t'})R_{t'}^d, \ \forall t' \in T \\ & 0 \leq x_{t'} \leq 1, \qquad \forall t' \end{aligned} \tag{16}$$

Denote by t^∞ the target chosen by the attacker when the defender uses x^∞. Define $\hat{x}^\infty$ as follows:

$$\hat{x}_t^\infty = \begin{cases} x_t^\infty & \text{if } t = t^\infty \\ 1 & \text{otherwise} \end{cases}.$$

Compared to x^∞, $\hat{x}^\infty$ increases the coverage probabilities for all targets except t^∞. It is clear that $\hat{x}^\infty$ achieves the same defender utility as x^∞, hence also optimal. In this case, the defender's utility is $\hat{x}_{t^\infty}^\infty R_{t^\infty}^d + (1-\hat{x}_{t^\infty}^\infty)P_{t^\infty}^d$.

Now we are ready to define the *modified plurality voting defense plan* based on $\hat{x}^\infty$. The main modification is that the coverage probability of the target from plurality voting is not fixed to be 1, but the probability we computed from $\hat{x}^\infty$.

Definition 10 *(Modified plurality voting defense plan).* In a modified plurality voting defense plan, if $s > 2$, we use plurality voting to determine a target t, and allocate $\hat{x}_t^\infty$ units of resources to t. If $s \leq 2$, we use patrol strategy x obtained by solving Program (17) (which is modified from Program (11) for target t^∞).

$$\begin{aligned} &\text{maximize}: \\ &\quad \sum_{s=0}^{2} p_+(s;k,t)\left[x_t(m^{s,t})R_t^d + \left(1-x_t(m^{s,t})\right)P_t^d\right] + \\ &\qquad \sum_{s=3}^{k} p_+(s;k,t)\left[\hat{x}_t^\infty R_t^d + \left(1-\hat{x}_t^\infty\right)P_t^d\right] \\ &\text{subject to}: \\ &\quad \sum_{s=0}^{2} p_+(s;k,t)\left[x_t(m^{s,t})P_t^a + (1-x_t(m^{s,t}))R_t^a\right] + \\ &\qquad \sum_{s=3}^{k} p_+(s;k,t)\left[\hat{x}_t^\infty P_t^a + \left(1-\hat{x}_t^\infty\right)R_t^a\right] \\ &\geq \sum_{s=0}^{2} p_+(s;k,t')\left[x_{t'}(m^{s,t'})P_{t'}^a + \left(1-x_{t'}(m^{s,t'})\right)R_{t'}^a\right] + \\ &\qquad \sum_{s=3}^{k} p_+(s;k,t')\left[\hat{x}_{t'}^\infty P_{t'}^a + \left(1-\hat{x}_{t'}^\infty\right)R_{t'}^a\right], \qquad \forall t' \\ &\quad \sum_{s=0}^{1} p_+(s;k-1,t)x_t(m^{s+1,t}) + p_+(2;k-1,t)\hat{x}_t^\infty \\ &\geq \sum_{s=0}^{2} p_+(s;k-1,t)x_t(m_{-i}^{s,t}, m_i'), \qquad \forall t, m_i' \\ &\quad \sum_{s=0}^{1} p_+(s;k-1,t)x_t(m^{s+1,t}) + p_+(2;k-1,t)\hat{x}_t^\infty \\ &\geq \sum_{s=0}^{2} p_+(s;k-1,t)x_t(m^{s,t}), \qquad \forall t \\ &\sum_{s=0}^{2} p_+(s;k-1,t)x_t(m^{s,t}) \leq \sum_{s=0}^{2} p_+(s;k-1,t)x_t(m_{-i}^{s,t}, m_i'), \ \forall t, m_i' \\ &\qquad \sum_{t'} x_{t'}^m \leq r, \qquad \forall m \\ &\qquad 0 \leq x_{t'}(m) \leq \hat{x}_{t'}^\infty, \qquad \forall t, m \end{aligned} \tag{17}$$

Remark 1. Compared to the plurality voting defense plan, the modified version is almost identical except that the number of resources allocated to target t^∞ is capped by $\hat{x}_t^\infty$.

The modified version is still incentive compatible, and the proof is similar to that of Theorem 5. Thus, we omit the proof but only state the result here.

Theorem 6. *The modified plurality voting defense plan is incentive compatible.*

Since both Program (16) and (17) can be solved in polynomial time, it follows that the modified plurality voting defense plan can also be found in polynomial time. Furthermore, we can show that such a defense plan is actually optimal.

Theorem 7. *Programs (12) and (17) have the same optimal objective value and, moreover, any feasible solution of one program can be efficiently converted into a feasible solution of the other program with the same objective value.*

Proof. We begin by introducing some additional notations. Define

$$\langle \Theta, O\rangle_t^{s,k} = \left\{ \langle \theta, o\rangle : \sum_{i=1}^{k} \mathbb{1}\left(\theta_i \in \Theta^+(t) \text{ and } o_i = 1\right) = s \right\}. \tag{18}$$

Note that for all t, we have $\bigcup_{s=0,\cdots,k} \langle \Theta, O\rangle_t^{s,k} = \Theta \times O$ since given any $\theta \in \Theta$ and $o \in O$, there always exists s such that $\langle \theta, o\rangle \in \langle \Theta, O\rangle_t^{s,k}$. Similarly, we denote by $\langle \Theta, O\rangle_t^{s,k-1}$ the set of type and observation pairs from $k-1$ informants.

By definition, we have

$$\sum_{\langle \theta, o\rangle \in \langle \Theta, O\rangle_t^{s,k}} p(\theta)p(o) = \binom{k}{s} \left[p_+(t)p_w\right]^s \left[1 - p_+(t)p_w\right]^{k-s}.$$

The rest of the proof consists of two steps.

Step 1. Denote by $x(\hat{m}^{s,t})$ the optimal solution to Program (17). For any message profile $\hat{m}(\theta, o, t)$, we can easily obtain the corresponding message profile $\hat{m}^{s,t}$ by ignoring the informants' identity. Now we construct another defense plan $\hat{m}(\theta, o, t)$ by setting $\hat{x}(\hat{m}(\theta, o, t)) = x(\hat{m}^{s,t})$ whenever $\sum_{i=0}^{k} \mathbb{1}\left(\theta_i \in \Theta^+(t) \text{ and } o_i = 1\right) = s$. Next, we show it is a feasible solution to Program (12) with the same objective value.

For the first constraint of Program (12), we have:

$$\begin{aligned}
&\mathop{\mathbf{E}}_{o,\theta}\left[\hat{x}_t(m(t,\theta,o))P_t^a + (1 - \hat{x}_t(m(t,\theta,o)))R_t^a\right] \\
&= \sum_{\theta}\sum_{o} p(\theta)p(o)\left[\hat{x}_t(m(t,\theta,o))P_t^a + (1 - \hat{x}_t(m(t,\theta,o)))R_t^a\right] \\
&= \sum_{s=0}^{k} \sum_{\langle \theta, o\rangle \in \langle \Theta, O\rangle_t^{s,k}} p(\theta)p(o)\left[\hat{x}_t(m(t,\theta,o))P_t^a + (1 - \hat{x}_t(m(t,\theta,o)))R_t^a\right] \\
&= \sum_{s=0}^{k} p_+(s;k,t)\left[x_t(m^{s,t})P_t^a + (1 - x_t(m^{s,t}))R_t^a\right].
\end{aligned}$$

Since x is an optimal solution to Program (17), x must satisfy the first constraint of it. Combining with the above equation shows that $\hat{x}$ satisfies the first constraint of Program (12).

As for the second and the third constraints of Program (12), we consider 3 cases for each informant i. When $m_i(t, \theta_i, o_i) = t$, we have:

$$\begin{aligned}
&\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[\hat{x}_t(m_{-i}(t,\theta_{-i},o_{-i}),t)\right] \\
&= \sum_{\theta_{-i}}\sum_{o_{-i}} p(\theta_{-i})p(o_{-i})\hat{x}_t(m_{-i}(t,\theta_{-i},o_{-i}),t) \\
&= \sum_{s=0}^{k-1} \sum_{\langle \theta_{-i}, o_{-i}\rangle \in \langle \Theta, O\rangle_t^{s,k-1}} p(\theta_{-i})p(o_{-i})\hat{x}_t(m_{-i}(t,\theta_{-i},o_{-i}),t) \\
&= \sum_{s=0}^{k-1} p_+(s;k-1,t)x_t(m^{s+1,t}).
\end{aligned}$$

When $m_i(t, \theta_i, o_i) = \perp$, we have

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[\hat{x}_t(m_{-i}(t,\theta_{-i},o_{-i}),\perp)\right]=\sum_{s=0}^{k-1}p_+(s;k-1,t)x_t(m^{s,t}).$$

And when $m_i(t,\theta_i,o_i)=t'\neq t$, we have

$$\mathop{\mathbf{E}}_{o_{-i},\theta_{-i}}\left[\hat{x}_t(m_{-i}(t,\theta_{-i},o_{-i}),t')\right]=\sum_{s=0}^{k-1}p_+(s;k-1,t)x_t(m^{s,t},t').$$

As a result, we can conclude that $\hat{x}$ satisfies the second and the third constraints of Program (12) since x satisfies the corresponding constraints in Program (17).

Finally, we can also write the defender's expected utility as

$$\begin{aligned}&\mathop{\mathbf{E}}_{o,\theta}\left[\hat{x}_t(m(t,\theta,o))R_t^d+(1-\hat{x}_t(m(t,\theta,o)))P_t^d\right]\\&=\sum_{s=0}^{k}p_+(s;k,t)\left[x_t(m^{s,t})R_t^d+(1-x_t(m^{s,t}))P_t^d\right],\end{aligned}$$

proving that the new defense plan has the same objective value as in (12).

Step 2. Consider any optimal solution $x(m(\theta,o,t))$ to Program (12), we construct a feasible $\hat{x}(m^{s,t})$ for Program (17) and show it achieves the same objective value. For any s, let

$$\hat{x}(m^{s,t})=\frac{1}{\left|\langle\Theta,O\rangle_t^{s,k}\right|}\sum_{\langle\theta,o\rangle\in\langle\Theta,O\rangle_t^{s,k}}x(m(\theta,o,t)),$$

$$\hat{x}(m_{-i}^{s,t},m_i)=\frac{1}{\left|\langle\Theta,O\rangle_t^{s,k-1}\right|}\sum_{\langle\theta,o\rangle\in\langle\Theta,O\rangle_t^{s,k-1}}x(m_{-i}(\theta_{-i},o_{-i},t),m_i).$$

For the attacker, the utility of attacking target t is

$$\begin{aligned}&\sum_{s=0}^{k}p_+(s;k,t)\left[\hat{x}_t(m^{s,t})P_t^a+(1-\hat{x}_t(m^{s,t}))R_t^a\right]\\&=\sum_{s=0}^{k}p_+(s;k,t)\left[(P_t^a-R_t^a)\hat{x}_t(m^{s,t})+R_t^a\right]\\&=\sum_{s=0}^{k}\sum_{\langle\theta,o\rangle\in\langle\Theta,O\rangle_t^{s,k}}p(\theta)p(o)\left[(P_t^a-R_t^a)\frac{\sum_{\theta,o\in\langle\Theta,O\rangle_t^{s,k}}x(m(\theta,o,t))}{\left|\langle\Theta,O\rangle_t^{s,k}\right|}+R_t^a\right]\\&=\sum_{s=0}^{k}\sum_{\langle\theta,o\rangle\in\langle\Theta,O\rangle_t^{s,k}}p(\theta)p(o)[(P_t^a-R_t^a)x(m(\theta,o,t))+R_t^a]\\&=\mathop{\mathbf{E}}_{o,\theta}\left[x_t\big(m(t,\theta,o)\big)P_t^a+\big(1-x_t(m(t,\theta,o))\big)R_t^a\right].\end{aligned}\tag{19}$$

With arguments similar to Step 1, we know that the constructed defense plan $\hat{x}$ satisfies the first constraint of Program (17).

For any informant i who reports t,

$$\begin{aligned}&\sum_{s=0}^{k-1}p_+(s;k-1,t)\hat{x}_t(m_{-i}^{s,t},t)\\&=\sum_{s=0}^{k-1}\sum_{\langle\theta_{-i},o_{-i}\rangle\in\langle\Theta,O\rangle_t^{s,k-1}}p(\theta_{-i})p(o_{-i})\hat{x}_t(m_{-i}^{s,t},t)\\&=\sum_{s=0}^{k-1}\sum_{\langle\theta_{-i},o_{-i}\rangle\in\langle\Theta,O\rangle_t^{s,k-1}}p(\theta_{-i})p(o_{-i})\frac{\sum_{\theta,o\in\langle\Theta,O\rangle_t^{s,k-1}}x(m_{-i}(\theta_{-i},o_{-i},t),t)}{\left|\langle\Theta,O\rangle_t^{s,k-1}\right|}.\end{aligned}\tag{20}$$

For any informant i who reports $t'\neq t$ or $\perp$, we have

$$\sum_{s=0}^{k-1}p_+(s;k-1,t)\hat{x}_t(m_{-i}^{s,t},t')$$

$$= \sum_{s=0}^{k-1} \sum_{\langle \theta_{-i}, o_{-i} \rangle \in \langle \Theta, O \rangle_t^{s,k-1}} p(\theta_{-i}) p(o_{-i}) \frac{\sum_{\theta, o \in \langle \Theta, O \rangle_t^{s,k-1}} x(m_{-i}(\theta_{-i}, o_{-i}, t), t')}{\left| \langle \Theta, O \rangle_t^{s,k-1} \right|}. \tag{21}$$

Since the defense plan x is a feasible solution to Program (12), we have

$$\sum_{s=0}^{k-1} \sum_{\langle \theta_{-i}, o_{-i} \rangle \in \langle \Theta, O \rangle_t^{s,k-1}} p(\theta_{-i}) p(o_{-i}) x(m_{-i}(t, \theta_{-i}, o_{-i}), t)$$

$$\geq \sum_{s=0}^{k-1} \sum_{\langle \theta_{-i}, o_{-i} \rangle \in \langle \Theta, O \rangle_t^{s,k-1}} p(\theta_{-i}) p(o_{-i}) x(m_{-i}(t, \theta_{-i}, o_{-i}), t'). \tag{22}$$

Plugging in Equation (20) and (21) yields:

$$\sum_{s=0}^{k-1} p_+(s; k-1, t) \hat{x}_t(m_{-i}^{s,t}, t) \geq \sum_{s=0}^{k-1} p_+(s; k-1, t) \hat{x}_t(m_{-i}^{s,t}, t'). \tag{23}$$

Similarly, we have

$$\sum_{s=0}^{k-1} p_+(s; k-1, t) \hat{x}_t(m_{-i}^{s,t}, t') \geq \sum_{s=0}^{k-1} p_+(s; k-1, t) \hat{x}_t(m_{-i}^{s,t}, \perp). \tag{24}$$

Therefore, the constructed defense plan $\hat{x}$ satisfies the second and the third constraints of Program (17), i.e., $\hat{x}$ is incentive compatible for the strategic informants.

Finally, similar to Equation (19), we have

$$\sum_{s=0}^{k} p_+(s; k, t) \left[\hat{x}_t(m^{s,t}) R_t^d + (1 - \hat{x}_t(m^{s,t})) P_t^d \right]$$

$$= \sum_{s=0}^{k} \sum_{\langle \theta, o \rangle \in \langle \Theta, O \rangle_t^{s,k}} p(\theta) p(o) \left[x_t(m(t, \theta, o)) R_t^d + (1 - x_t(m(t, \theta, o))) P_t^d \right]$$

$$= \mathbf{E}_{o,\theta} \left[x_t\big(m(t, \theta, o)\big) R_t^d + \big(1 - x_t(m(t, \theta, o))\big) P_t^d \right], \tag{25}$$

proving that the defender's utilities are the same in the two programs. □

The following corollary directly follows from Theorem 4 and Theorem 7.

Corollary 2. *The optimal defender defense plan with multiple informants can be computed efficiently in polynomial time.*

5. Experiments

All our results shown in this section are demonstrated over randomly generated game instances. The rewards and penalties for both the defender and the attacker are drawn from $U[0, 1]$ and $U[-1, 0]$, respectively. There are 3 different informant types: a defender-aligned type (θ_1), an attacker-aligned type (θ_2), and a random type (θ_3). All the informant utilities are randomly drawn from $U[0, 0.2]$. In our experiments, we change probabilities for θ_1 and θ_2 to simulate the process of changing from attacker-aligned informants to defender-aligned informants. We solve our linear program with Python using Gurobi 9.5.1 [32] as the solver.[5] The running time of our algorithm for the single informant case is depicted in Fig. 3. The results shown in this section are averaged over 100 randomly generated game instances.

Next, Section 5.1 to 5.3 report results on how the informant type changes the equilibrium of the game, while in Section 5.4 and 5.5, we show the effect of having different numbers of informants.

5.1. Utility vs. informant type

Consider an informant having one of the three types described above. We enumerate all possible type distributions satisfying $p(\theta) \in \{0.1, 0.2, \ldots, 1.0\}, \forall \theta$ and $\sum_\theta p(\theta) = 1$. We compute the corresponding utilities for both the defender and the attacker to analyze the effect of having different types of informants. As shown in Figs. 4, the defender obtains higher utilities and the attacker obtains lower utilities as the informant goes from fully attacker-aligned to fully defender-aligned under all different settings of r and p_w, which shows that the existence of the informant could significantly affect the game.

[5] The code can be found at https://github.com/AIandSocialGoodLab/securitygamewithinformants.

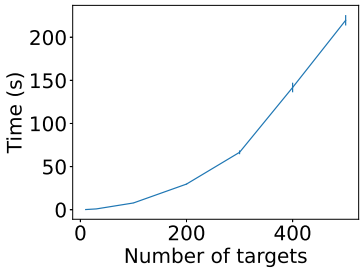


Fig. 3. The running time of our algorithm for the single informant case. The running time goes up as the number of targets increases. Even for 500 targets, our algorithm can find the optimal solution within 4 minutes.

5.2. Number of resources vs. informant type

We explore how an informant could influence the game in another dimension. We set $p(\theta_3) = 0$, and only change $p(\theta_1)$ and $p(\theta_2)$. The points on the same curve in the Fig. 5 correspond to the same defender's utility. For example, when there are 5 targets, in order to achieve the same utility of having $r = 1$ with a fully defender-aligned informant, a defender needs to have about 2 resources when faced with a fully attacker-aligned informant. And this number goes up quickly when the number of targets increases. This implies that when there is a large number of targets, a defender-aligned informant is worth many defensive resources.

5.3. Effect of misclassifying the informant

Fig. 6 shows the results when different defenders meet different informants. In the case where the defender knows the informant types (i.e., a "strategic" defender), the defender's utility goes down as the number of targets increases. But the defender can get more utility if the informant becomes more defender-aligned. However, when the informant is not fully defender-aligned (an informant with type "random" or "attacker-aligned"), the defender can suffer a huge loss by blindly following the informant's messages ("naive"). Again, this experiment shows that the strategic behaviors of the informant can have a huge impact on the defender's utility.

5.4. Utility vs. number of informants

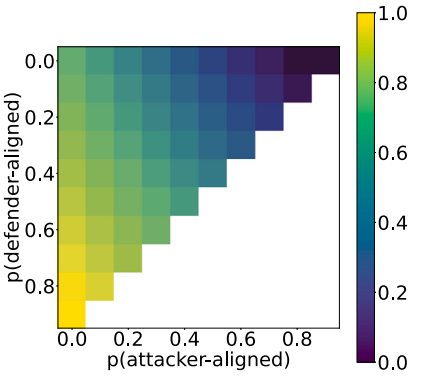
In this experiment, we explore how the number of informants influences the utilities of both the defender and the attacker, and how the influences change with respect to the informants' types. We still set $p(\theta_3) = 0$, and change $p(\theta_1)$ and $p(\theta_2)$. As shown in Fig. 7, the defender gets higher utilities and the attacker gets lower utilities as the number of informants increases. This also happens when the informants become more defender-aligned. In addition, the defender's marginal utility gain of having more defender-aligned informants increases when there are fewer informants and decreases when there are more informants. This implies that when the informants have a low probability of being defender-aligned, having more informants is crucial for the defender to obtain a high utility. In this case, a reliable informant is worth multiple unreliable ones. But with more informants, the reliability of these informants becomes less important.

5.5. Number of resources vs. number of informants

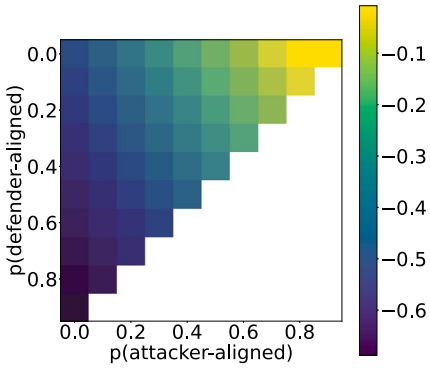
In this experiment, we compare the effect of having different numbers of informants and resources. As for the informant's type, we still set $p(\theta_3) = 0$, and let $p(\theta_1) = 0.5$ and $p(\theta_2) = 0.5$. Fig. 8 shows similar patterns to Fig. 7. The defender gets higher utilities and the attacker gets lower utilities as the number of informants gets higher or the number of resources gets higher. The effect of having more informants diminishes if the defender already has many resources to cover most targets. But in most real-world applications where defensive resources are scarce, having more informants can help the defender figure out the true target of the attacker, and thus significantly benefit the defender.

6. Conclusion

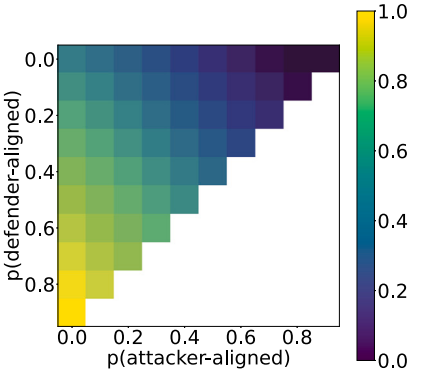
In real-world applications, there are many situations where the local community (i.e., the informants) participates in the security games between the defender and the attacker. However, the standard security model does not capture these strategic behaviors of the informants. In this paper, we provide a systematic study of security games with strategic informants to account for their behaviors. We first consider security games with a single informant case. We propose a well-defined definition of Strong Stackelberg-perfect Bayesian equilibrium and provide an efficient algorithm to solve for the optimal defender policies in polynomial time. We also consider a more complicated case with multiple strategic informants. Even though the defender's strategy space grows exponentially with the number of strategic informants, we show there also exists a polynomial time algorithm to compute the optimal defender policy by proposing a novel plurality voting defense plan. Finally, we conduct comprehensive experiments to examine the impact



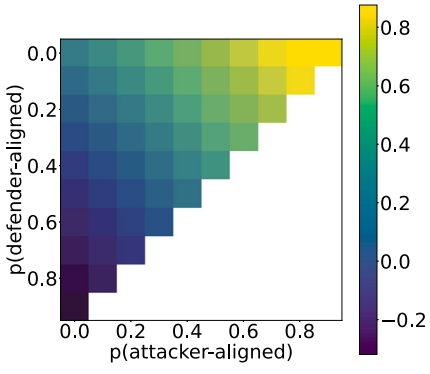
(a) Defender's utility when $r = 5$ and $p_w = 0.3$.



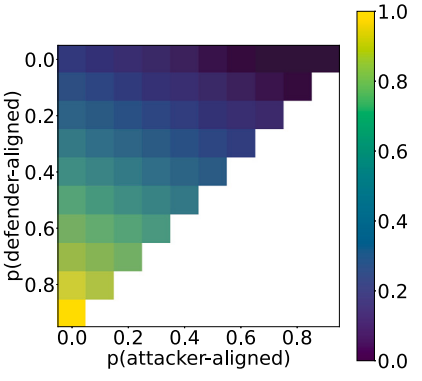
(b) Attacker's utility when $r = 5$ and $p_w = 0.3$.



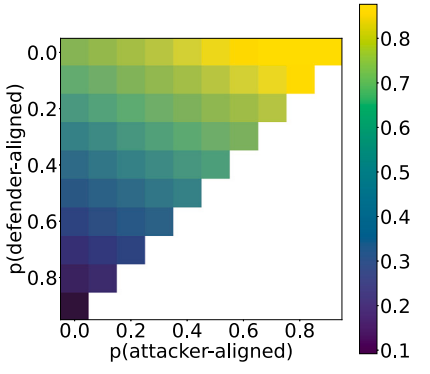
(c) Defender's utility when $r = 3$ and $p_w = 0.5$.



(d) Attacker's utility when $r = 3$ and $p_w = 0.5$.



(e) Defender's utility when $r = 3$ and $p_w = 0.3$.



(f) Attacker's utility when $r = 3$ and $p_w = 0.3$.

Fig. 4. Our study examines how variations in defender resources (r) and informant observation probability (p_w) (across different rows), and the informant type distributions (different grid points in each plot) affect the utility of both agents.

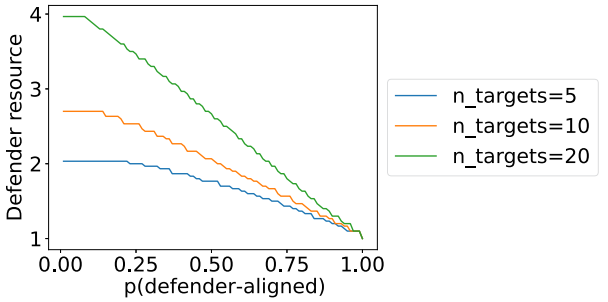


Fig. 5. Defensive resources needed with a strategic informant.

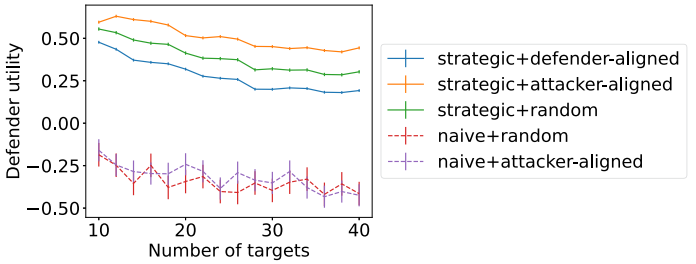


Fig. 6. The defender's utilities of different defenders meeting different informants, where "strategic+defender-aligned" means a strategic defender and a defender-aligned informant, "naive+attacker-aligned" means a defender who blindly follows the attacker-aligned informant's message.

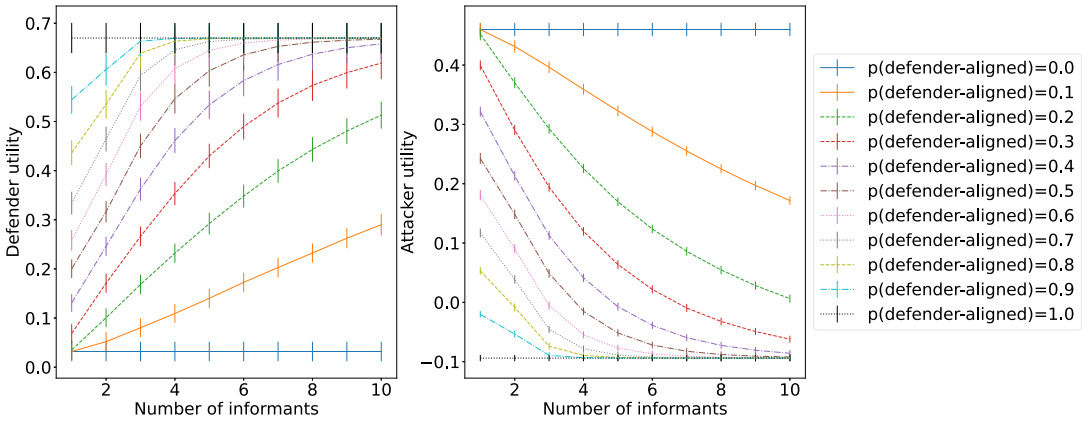


Fig. 7. The effect of having a different number of informants and different types of informants on both the defender and attacker's utilities.

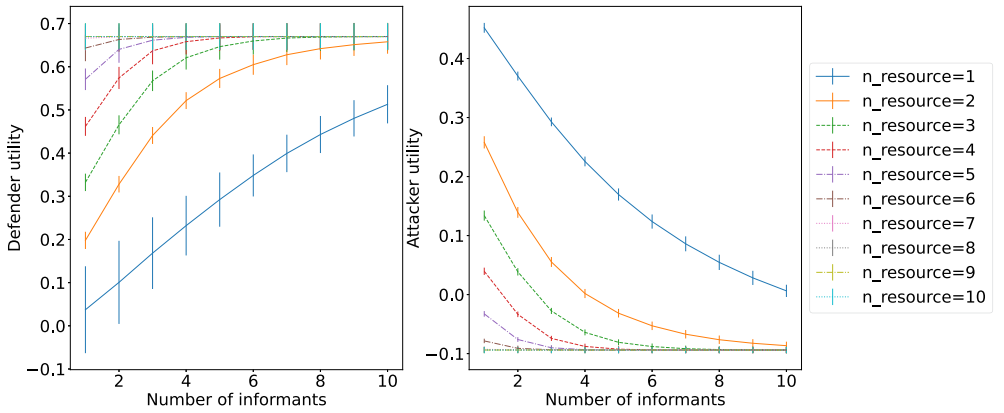


Fig. 8. The effect of having a different number of informants and different numbers of resources on both the defender and attacker's utilities.

of strategic informants and showcase the efficiency of our algorithm. Our findings reveal that the presence of such informants substantially enhances the defender's utility.

Moreover, this study opens up new avenues for many other interesting questions. For example, our strategic informant behavior model assumes perfect observations (i.e., an informant knows the exact target being attacked). However, it is also possible for the informants to have imperfect observations. It would be interesting to consider the case where each informant only has a noisy observation and study how to design the defense plan accordingly. In addition, besides the basic security game structure that we discussed in the paper, exploring the potential effect of strategic informants in other types of security games would be an intriguing avenue for future research. For example, in spatio-temporal security games that handle massive games with complex spatio-temporal settings, the attacker moves over time and thus the target changes. Even if the defender receives information about the attacker's current location, this information can only be used to infer where the attacker may possibly move next, but may not help the defender to directly capture the attacker. It would be interesting to investigate how to utilize the informants' information in such games.

CRediT authorship contribution statement

Weiran Shen: Writing – original draft, Validation, Project administration, Methodology, Funding acquisition, Formal analysis, Conceptualization. **Minbiao Han:** Writing – review & editing, Writing – original draft, Visualization, Software. **Weizhe Chen:** Visualization, Software. **Taoan Huang:** Visualization, Software. **Rohit Singh:** Supervision, Conceptualization. **Haifeng Xu:** Writing – original draft, Validation, Methodology, Conceptualization. **Fei Fang:** Writing – original draft, Project administration, Methodology, Conceptualization.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Weiran Shen reports financial support was provided by National Natural Science Foundation of China. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

Weiran Shen is supported by the National Natural Science Foundation of China (No. 62106273), the Fundamental Research Funds for the Central Universities, and the Research Funds of Renmin University of China (22XNKJ16).

References

[1] W. Shen, W. Chen, T. Huang, R. Singh, F. Fang, When to follow the tip: security games with strategic informants, in: C. Bessiere (Ed.), Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence, IJCAI-20, International Joint Conferences on Artificial Intelligence Organization, 2020, pp. 371–377, main track.
[2] M. Tambe, Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned, Cambridge University Press, 2011.
[3] B. An, M. Tambe, A. Sinha, Stackelberg security games (ssg) basics and application overview, in: Improving Homeland Security Decisions, 2017, p. 485.
[4] J.D. Margulies, L.-A. Bullough, A. Hinsley, D.J. Ingram, C. Cowell, B. Goettsch, B.B. Klitgård, A. Lavorgna, P. Sinovas, J. Phelps, Illegal wildlife trade and the persistence of "plant blindness", Plants People Planet 1 (2019) 173–182.
[5] F. Fang, T.H. Nguyen, R. Pickles, W.Y. Lam, G.R. Clements, B. An, A. Singh, B.C. Schwedock, M. Tambe, A. Lemieux, PAWS - a deployed game-theoretic application to combat poaching, AI Mag. (2017).
[6] J. Pita, M. Jain, J. Marecki, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, S. Kraus, 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, 2008, pp. 125–132.
[7] WWF, Developing an approach to community-based crime prevention, http://zeropoaching.org/pdfs/Community-based-crime%20prevention-strategies.pdf, 2015.
[8] L. Nubani, H. Fierke-Gmazel, H. Madill, A. De Biasi, Community engagement in crime reduction strategies: a tale of three cities, J. Particip. Res. Methods 4 (2023).
[9] F. Massé, A. Gardiner, R. Lubilo, M.N. Themba, Inclusive anti-poaching? Exploring the potential and challenges of community-based anti-poaching, South Afr. Crime. Q. 60 (2017) 19–27.
[10] N. Basilico, S. Coniglio, N. Gatti, Methods for finding leader-follower equilibria with multiple followers, in: AAMAS'16, 2016, pp. 1363–1364.
[11] V. Conitzer, T. Sandholm, Computing the optimal strategy to commit to, in: Proceedings of the 7th ACM Conference on Electronic Commerce, ACM, 2006, pp. 82–90.
[12] A. Rosenfeld, S. Kraus, When security games hit traffic: optimal traffic enforcement under one sided uncertainty, in: IJCAI, 2017, pp. 3814–3822.
[13] A. Schlenker, O. Thakoor, H. Xu, F. Fang, M. Tambe, L. Tran-Thanh, P. Vayanos, Y. Vorobeychik, Deceiving cyber adversaries: a game theoretic approach, in: Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems, 2018, pp. 892–900.
[14] T. Huang, W. Shen, D. Zeng, T. Gu, R. Singh, F. Fang, Green security game with community engagement, in: Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems, 2020, pp. 529–537.
[15] N. Basilico, A. Celli, G. De Nittis, N. Gatti, Coordinating multiple defensive resources in patrolling games with alarm systems, in: AAMAS'17, 2017, pp. 678–686.

[16] X. Ma, Y. He, X. Luo, J. Li, M. Zhao, B. An, X. Guan, Camera placement based on vehicle traffic for better city security surveillance, IEEE Intell. Syst. 33 (2018) 49–61.
[17] Q. Guo, B. An, B. Bošansky, C. Kiekintveld, Comparing strategic secrecy and Stackelberg commitment in security games, in: Proceedings of the 26th International Joint Conference on Artificial Intelligence, 2017, pp. 3691–3699.
[18] J. Gan, H. Xu, Q. Guo, L. Tran-Thanh, Z. Rabinovich, M. Wooldridge, Imitative follower deception in Stackelberg games, in: Proceedings of the 2019 ACM Conference on Economics and Computation, 2019, pp. 639–657.
[19] H. Xu, K. Wang, P. Vayanos, M. Tambe, Strategic coordination of human patrollers and mobile sensors with signaling for security games, in: Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence and Thirtieth Innovative Applications of Artificial Intelligence Conference and Eighth AAAI Symposium on Educational Advances in Artificial Intelligence, 2018, pp. 1290–1297.
[20] E. Bondi, H. Oh, H. Xu, F. Fang, B. Dilkina, M. Tambe, To signal or not to signal: exploiting uncertain real-time information in signaling games for security and sustainability, in: Proceedings of the AAAI Conference on Artificial Intelligence, 2020, pp. 1369–1377.
[21] R.B. Myerson, Optimal auction design, Math. Oper. Res. 6 (1981) 58–73.
[22] J. Černỳ, B. Boỳanskỳ, C. Kiekintveld, Incremental strategy generation for Stackelberg equilibria in extensive-form games, in: Proceedings of the 2018 ACM Conference on Economics and Computation, 2018, pp. 151–168.
[23] M. Smith, J. Humphreys, The Poaching Paradox: Why South Africa's 'Rhino Wars' Shine a Harsh Spotlight on Security and Conservation, Ashgate Publishing Company, 2015.
[24] W.D. Moreto, Introducing intelligence-led conservation: bridging crime and conservation science, Crime Sci. 4 (2015) 15.
[25] R. Duffy, F.A. St John, B. Büscher, D. Brockington, The militarization of anti-poaching: undermining long term goals?, Environ. Conserv. 42 (2015) 345–348.
[26] M. Linkie, D.J. Martyr, A. Harihar, D. Risdianto, R.T. Nugraha, Maryati, N. Leader-Williams, W. Wong, Editor's choice: safeguarding Sumatran tigers: evaluating effectiveness of law enforcement patrols and local informant networks, J. Appl. Ecol. (2015).
[27] C. Gill, D. Weisburd, C.W. Telep, T. Bennett, Community-oriented policing to reduce crime, disorder and fear and increase satisfaction and legitimacy among citizens: a systematic review, Journal of Experimental Criminology (2014).
[28] M.B. Short, P.J. Brantingham, M.R. D'orsogna, Cooperation and punishment in an adversarial game: how defectors pave the way to a peaceful society, Phys. Rev. E 82 (2010) 066114.
[29] M.B. Short, A.B. Pitcher, M.R. D'Orsogna, External conversions of player strategy in an evolutionary game: a cost-benefit analysis through optimal control, Eur. J. Appl. Math. 24 (2013) 131–159.
[30] H. Von Stackelberg, Market Structure and Equilibrium, Springer Science & Business Media, 2010.
[31] B. Von Stengel, S. Zamir, Leadership with commitment to mixed strategies, Technical Report, Citeseer, 2004.
[32] L. Gurobi, Optimization, Gurobi optimizer reference manual, http://www.gurobi.com, 2023.