Divide to Defend: Collusive Security Games

Shahrzad Gholami, Bryan Wilder, Matthew Brown, Dana Thomas,
Nicole Sintov, and Milind Tambe

Computer Science Department,
University of Southern California
{sgholami,bwilder,matthew.a.brown,danathom,
sintov,tambe}@usc.edu

Abstract. *Research on security games has focused on settings where the defender must protect against either a single adversary or multiple, independent adversaries. However, there are a variety of real-world security domains where adversaries may benefit from colluding in their actions against the defender, e.g., wildlife poaching, urban crime and drug trafficking. Given such adversary collusion may be more detrimental for the defender, she has an incentive to break up collusion by playing off the self-interest of individual adversaries. As we show in this paper, breaking up such collusion is difficult given bounded rationality of human adversaries; we therefore investigate algorithms for the defender assuming both rational and boundedly rational adversaries. The contributions of this paper include (i) collusive security games (COSGs), a model for security games involving potential collusion among adversaries, (ii) SPECTRE-R, an algorithm to solve COSGs and break collusion assuming rational adversaries, (iii) observations and analyses of adversary behavior and the underlying factors including bounded rationality, imbalanced- resource-allocation effect, coverage perception, and individualism / collectivism attitudes within COSGs with data from 700 human subjects, (iv) a learned human behavioral model that incorporates these factors to predict when collusion will occur, (v) SPECTRE-BR, an enhanced algorithm which optimizes against the learned behavior model to provide demonstrably better performing defender strategies against human subjects compared to SPECTRE-R.*

Keywords: Stackelberg Security Game, Collusion, Human Behavior Model, Amazon Mechanical Turk

1 Introduction

Models and algorithms based on Stackelberg security games have been deployed by many security agencies including the US Coast Guard, the Federal Air Marshal Service, and Los Angeles International Airport [23] in order to protect against attacks by strategic adversaries in counter-terrorism settings. Recently, security games research has explored new domains such as wildlife protection, where effective strategies are needed to tackle sustainability problems such as illegal poaching and fishing [4].

Crucially, though, most previous work on security games assumes that different adversaries can be modeled independently [10, 18, 11]. However, there are many real-world security domains in which adversaries may collude in order to more effectively

evade the defender. One example domain is wildlife protection. Trade in illicit wildlife products is growing rapidly, and poachers often collude both with fellow poachers and with middlemen who help move the product to customers [26]. These groups may coordinate to gain better access to information, reduce transportation costs, or reach new markets. This coordination can result in higher levels of poaching and damage to the environment. Additionally, connections have been observed between illicit wildlife trade and organized crime as well as terrorist organizations, and thus activities such as poaching can serve to indirectly threaten national security [27].

Another example domain is the illegal drug trade where international crime syndicates have increased collusive actions in order to facilitate drug trafficking, expand to distant markets, and evade local law enforcement [1]. In some cases, drug traders must collude with terrorist organizations to send drugs through particular areas. More broadly, expansion of global transportation networks and free trade has motivated collusion between criminal organizations across different countries [20]. A third example of a domain with collusive actions is the "rent-a-tribe" model in the payday lending industry. Authorities in the US attempt to regulate payday lenders which offer extremely high interest rates to low-income borrowers who cannot obtain loans from traditional banks. Recently, payday lenders have begun to operate in partnership with Native American tribes, which are exempt from state regulations. Thus, regulators seek policies which prevent collusion between payday lenders and Native American tribes [8].

Despite mounting evidence of the destructive influence of collusive behavior, strategies for preventing collusion have not been explored in the security games literature (there are some recent exceptions, which we discuss in Section 2). Furthermore, analysis of collusive adversary behaviors is complicated by the bounded rationality of human adversaries; such analysis with data from human players is also missing in the security games literature. To address these limitations and improve defender performance by combating collusion between adversaries, this paper (i) introduces the COllusive Security Game (COSG) model with three players: one defender and two adversaries with the potential to collude against the defender, (ii) provides a baseline algorithm, SPECTRE-R, which optimizes against collusive adversaries assuming them to be perfectly rational, (iii) analyzes data from an experiment involving 700 human subjects, (iv) proposes a data driven human behavioral model based on these factors to predict the level of collusion between human adversaries, and (v) develops a novel algorithm, SPECTRE-BR, which optimizes against the learned behavior model to better prevent collusion between adversaries (and as a result, outperforms SPECTRE-R). Indeed, we find that human adversaries are far from perfectly rational when deciding whether or not to collude. Our experiments show that defenders can improve their utility by modeling the subjective perceptions and attitudes which shape this decision and crafting strategies tuned to prevent collusion.

2 Background and Related Work

The Stackelberg Security Game model, introduced almost a decade ago, has led to a large number of applications and has been discussed widely in the literature [12, 23, 17]. All of these works consider adversaries as independent entities and the goal is for

a defender (leader) to protect a set of targets with a limited set of resources from a set of adversaries (followers)[1]. The defender commits to a strategy and the adversaries observe this strategy and each select a target to attack. The defender's pure strategy is an assignment of her limited resources to a subset of targets and her mixed strategy refers to a probability distribution over all possible pure strategies. This mixed strategy is equivalently expressed as a set of coverage probabilities, $0 \leq c_t \leq 1$, that defender will protect each target, t [12]. Defender's utility is denoted by $U^u_\Theta(t)$ when target t is uncovered and attacked by the adversary and by $U^c_\Theta(t)$ if t is covered and attacked by the adversary. The payoffs for the attacker are analogously written by $U^u_\Psi(t)$ and $U^c_\Psi(t)$. The expected utilities of the defender, $U_\Theta(t, C)$, and attacker, $U_\Theta(t, C)$ for the defender coverage vector C, are then computed as follows:

$$U_\Theta(t, C) = \quad c_t \cdot U^c_\Theta(t) + (1 - c_t)U^u_\Theta(t) \tag{1}$$

$$U_\Psi(t, C) = \quad c_t \cdot U^c_\Psi(t) + (1 - c_t)U^u_\Psi(t) \tag{2}$$

The solution concept for security games involves computing a strong Stackelberg equilibrium (SSE) which assumes that the adversaries maximize their own expected utility and break ties in favor of the defender [11, 23].

Given this basic information about SSG, we next start a discussion of related work. Security game models where an adversary is capable of attacking multiple targets simultaneously have been explored in [29, 13]. To address cooperation between adversaries, [7] introduced a communication network based approach for adversaries to share their skills and form coalitions in order to execute more attacks. However, no previous work on security games has conducted behavioral analysis or considered the bounded rationality of human adversaries in deciding whether to collude in the first place.

Another area of related work, as well as one that provides concepts that we will use in this paper for modeling and analyzing adversary behaviors in COSGs is that of behavioral models in game theory [3]. This area is particularly relevant given our focus on modeling human adversaries in this paper. In real-world settings, it is useful to model human adversaries as not strictly maximizing their expected utility, but rather, as their choosing strategies stochastically [14]. Quantal response equilibrium (QRE) is a solution concept based on the assumption of bounded rationality [15]. The intuition behind the QR model is that the higher the expected utility for an action, the higher the probability of the adversary selecting that action. SUQR [19] has been proposed as an extension of QR and seen to outperform QR in modeling human adversaries [28]. This model is used in this paper to predict the probability of attack at each target. The logit function shown in Equation 3 is the most common specification for QR and SUQR functional form where q_t is the probability of choosing strategy t among all possible strategies in set of T.

$$q_t = \frac{e^{\hat{U}_\Psi(t,C)}}{\sum_{t \in T} e^{\hat{U}_\Psi(t,C)}} \tag{3}$$

[1] We use the convention in the security game literature where the defender is referred as "she" and an adversary is referred to as "he".

In SUQR model, $\hat{U}_{\Psi}(t, C)$ refers to subjective utility, and it replaces expected utility. Subjective utility in SUQR is defined as a linear combination of key domain features including the defender's coverage probability and the adversary's reward and penalty at each target which are respectively weighted by ω_1, ω_2 and ω_3.These are assumed to be the most salient features in the adversary's decision-making process.

$$\hat{U}_{\Psi}(t, C) = \omega_1 \cdot c_t + \omega_2 \cdot U^u_{\Psi}(t) + \omega_3 \cdot U^c_{\Psi}(t) \tag{4}$$

Another relevant aspect of bounded rationality is how humans weight probabilities. Prospect Theory (PT) proposes that individuals overweight low probabilities and underweight high probabilities; essentially, probabilities are transformed by an inverse S-shaped function[9, 25]. Various functional forms have been proposed to capture this relationship [9, 25]. Later work, specific to security games, has found the opposite of what Prospect Theory suggests: human players underweight low probabilities and overweight high probabilities[10]. This corresponds to an S-shaped weighting function. In either case, incorporating a model of probability perception allows the defender to exploit inaccuracies in the adversary's reasoning. Human subject experiments have been conducted for security games to test both bounded rationality and probability weighting [10], but have never included the collusive actions investigated in this paper.

Additionally, humans' decisions in strategic settings can be influenced by the relative advantage of participants. According to Inequity Aversion (IA) theory humans are sensitive to inequity of outcome regardless of whether they are in the advantaged or disadvantaged situation and they make decisions in a way that minimizes inequity [5]. Inequity aversion has been widely studied in economics and psychology and is consistent with observations of human behavior in standard economic experiments such as the dictator game and ultimatum game in which the most common choice is to split the reward 50-50 [2]. Along these lines and contrary to the theoretical predictions, IA theory also supports our analyses in the security game domain.

Finally, the personal attitudes and attributes of participants can also influence their interactions in strategic settings. A key characteristic is the well-established individualism-collectivism paradigm, which describes cultural differences in the likelihood of people to prioritize themselves versus their in-group [22]. This paper is the first to provide analysis of human adversary behavior in security games using individualism-collectivism paradigm. Specifically, those who identify as part of collectivistic cultures, compared to people in individualistic cultures, tend to identify as part of their in-groups, prioritize group-level goals, define most relationships with in-group members as communal, and are more self-effacing. Individualism-collectivism can be reliably measured using psychometrically-validated survey instruments [24].

3 Illustrative Motivating Domain: Wildlife Poaching Game

As an illustrative motivating domain for the work reported in this paper, we focus on the challenge of wildlife poaching. Wildlife poaching poses a serious threat to the environment as well as national security in numerous countries around the world and is now estimated to be worth $5 billion annually. The most common types of illicitly poached and traded wildlife products include elephant ivory, rhino horn, tiger parts, and caviar

[16]. Biodiversity loss, invasive species introduction, and disease transmission resulting from illicit wildlife trade can all have disastrous impacts on the environment. Evidence [26] confirms that collusive actions (e.g., cost sharing for storage, handling, and transportation of goods) among adversaries can increase the rate of poaching and cause further damage to the environment. Modeling this as a security game, the defender is a ranger whose goal is to allocate patrolling resources optimally over the targets. The adversaries are poachers or illegal traders who execute attacks, possibly in collusion with one another. To better understand collusion in the wildlife poaching domain, we designed a game for human subjects to play on Amazon Mechanical Turk (AMT). Participants were asked to play our game in different settings and answer survey questions. Afterwards, their actions were analyzed using the theories explained above, allowing us to test assumptions about the rationality of human adversaries.

3.1 Game Overview

In our game, human subjects are asked to play the role of a poacher in a national park in Africa. The entire park area (see Figure 1) is divided into two sections (right and left) and each human subject can only attack in one section (either right or left); however, they can explore the whole park to obtain information about the other player's situation. To ensure repeatability of the experiments, the other side is played by a computer, not a real player. Since our goal is to study human adversaries, we do not reveal the identity of the other player to the human subjects. This creates a more realistic environment since the subjects believe that they are playing against another human. Each section of the park is divided into a 3×3 grid, giving each player nine potential targets to attack.

There are different numbers of hippopotamus distributed over the area which indicate the animal density at each target. The adversary's reward at each target is equal to the animal density at that target; hereafter, reward and animal density are used interchangeably. Players are able to view the probability of success and failure, as well as the reward and penalty, at any target on either section of the park as shown on the sides of the Figure 1. To help the human subjects better visualize the success/failure percentages (i.e., defender coverage) for each sub-regions, we overlaid a heat-map of the success probability on Google Maps imagery of the park. Also, to help the players understand the collusion mechanism, we provided a table that summarizes all possible payoffs for both colluding and not colluding. The human subjects may decide to attack "individually and independently" or "in collusion" with the other player. In both situations, they will attack different sections separately but if both agree to attack in collusion, they will share all of their payoffs with each other equally.

3.2 Experimental Procedure

To enhance understanding of the game, participants were provided with a background story and detailed instructions about the game and then asked to play one trial game to become familiar with the game interface and procedures. After the trial game, participants played a validation game to ensure that had they read the instructions and were fully aware of the rules and options of the game. For our analysis, we included only players whose performance in the validation game passed a set of baseline criteria.

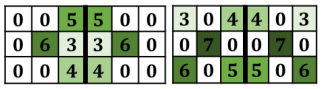
Fig. 1. Poachers vs. Rangers game: Right side of the park is assigned to the player and the left side is assigned to Bob who is the other fellow poacher. Payoffs for each marked target are shown.

Lastly, subjects played the main game for the analysis. After finishing all of the games, participants answered a set of survey questions.

In each individual game, the human player is given a set amount of time to explore the park and make decisions about: (i) whether to collude with the other player or not and (ii) which region of the park to place their snare. While the other player is a computer, it is suggested that they are actually another human. To make the first decision, a question appears on the screen which asks whether the human player is inclined to collude or not. After answering this question, a message appears on the screen that indicates whether collusion was preferred by both players or not. Collusion occurs only if it is preferred by both players. It is worth noting that the human participant has no opportunity to communicate with or learn about the other player. Next, players are asked to choose a target in their own region to attack. As before, players cannot communicate about which target to attack.

We analyze two situations: one where the human attacker is placed in an advantaged situation, with fewer defender resources protecting his side of the park than the other; and a disadvantaged situation, which is the reverse. In each situation, as we mentioned, we first check if the player is inclined to collude. Next, we designed a computer agent with rational behavior to play as the second adversary; thus there is an algorithm generating defender strategies, and two adversaries (one a human and one a computer agent). This computer agent seeks collusion when it is placed on the disadvantaged side and refuses collusion when it is in advantaged situation (Choosing a computer agent as a second player let us to avoid requiring coordination between two human players in the experiments). To simplify the analysis, we assume that the second stage of decision making (where each adversary chooses a target to attack) depends on his own inclination for collusion and does not depend on the attitude of the other adversary.

Consequently, there are four possible types of human adversaries in this game: (i) a disadvantaged attacker who decides to collude, DA-C, (ii) a disadvantaged attacker



(a) RS1 (b) RS2

Fig. 2. Reward (animal density) structures deployed on AMT. Darker green shows higher reward.

who decides not to collude, DA-NC, (iii) an advantaged attacker who decides to collude, A-C, and (iv) an advantaged attacker who decides not to collude, A-NC.

We tested different defender mixed strategies based on both the assumption of rationality and bounded rationality given by a behavioral model introduced in Section 6. For each strategy deployed on AMT, we recruited a new set of participants (50 people per setup) to remove any learning bias and to test against a wider population. Using the rational model for adversaries, four different defender strategies were deployed for each reward structure. The data sets collected from rational model deployments were used to learn the parameters of the bounded rationality model. This learning mimics the fact that in the real world, often data about past poaching incidents is available to build models of poacher behavior [18]. Players were given a base compensation of $\$0.50$ for participating in the experiment. In order to incentivize the players to perform well, we paid each player a performance bonus based on the utility that they obtained in each game. This bonus had a maximum total value of $\$1.32$ and a minimum of $\$0.04$.

3.3 Game Payoff Design

This "Poachers vs Rangers" game is a three-player security game with 9 targets available to each adversary. There is one defender with m resources to cover all the 18 targets (sub-regions in the park) and there are two adversaries that can attack a side of the park. An adversary's reward at each cell for an uncovered attack is equal to the animal density at that cell and the penalty at each cell for a covered attack is equal to -1. We deployed two different reward structures, $RS1$ and $RS2$, shown in Figures 2(a) and 2(b). In both of these symmetric structures, both players have an identical 3×3 reward distribution. In $RS1$ animal density is concentrated along the central axis of the park and is covered by 3 defender resources and in $RS2$ animal density is concentrated toward the center of each half of the park and is covered by 4 defender resources. We assumed a bonus of 1 for collusion in both set-ups; this bonus is added to the payoff for each successful attack if both attackers decide to collude. Section 4 gives further mathematical description and motivates the introduction of this bonus. This game is zero-sum, i.e., at each target the uncovered payoffs for the attacker and defender sum to zero.

4 Collusive security game model

In the collusive security game which we study in this paper, there is one defender, Θ, and multiple adversaries, Ψ_1,...,Ψ_N, where N is the total number of attackers. Similarly to standard Stackelberg Security Games [23], the defender is the leader and the attackers

are the followers. In this subsection, we focus on the games with one defender and two adversaries, such that adversaries can attack separate targets, but they have two options: i) attack their own targets individually and earn payoffs independently or ii) attack their own targets individually but collude with each other and share all of the payoffs equally. If the attackers decide to collude, the utility for a successful attack increases by ϵ. This reward models many of the example domains where adversaries operate in different geographic areas or portions of a supply chain, and so do not directly compete over the same targets. Instead, they choose to combine their operations or share information in some way which produces extra utility exogenous to the targets themselves.

To precisely define the model, let $T = \{t_1, ..., t_n\}$ be a set of targets. T is partitioned into disjoint sets T_1 and T_2 which give the targets accessible to the first (resp. second) attacker. The defender has m resources, each of which can be assigned to cover one target. Since we consider games with no scheduling constraints [29], the set of defender pure strategies is all mappings from each of the m resources to a target. A mixed strategy is a probability distribution over such schedules, and can be compactly represented by a coverage vector C which gives the probability that each target is covered. Each attacker pure strategy is the combination of a choice of target to attack and the decision of whether or not to collude. Since the attackers choose their strategies after the defender, there is always an equilibrium in which they play only pure strategies [11]. Hence, we encapsulate the targets which are attacked in a set of binary variables a_t, $t \in T$, where the variables corresponding to the targets which are attacked are set to 1.

We denote the utility that the defender receives when target t is attacked by $U^u_\Theta(t)$ if t is uncovered, and $U^c_\Theta(t)$ if t is covered. The payoffs for the ith attacker are analogously written $U^u_{\Psi_i}(t)$ and $U^c_{\Psi_i}(t)$. Suppose that the attackers select target $t_1 \in T_1$ and $t_2 \in T_2$. Since each may be covered or uncovered, four different outcomes are possible. Table 1 summarizes the players' payoffs in all possible cases when the attackers do not collude (the first two columns) and collude (the last two columns). In this table the first row indicates the payoffs when both targets are uncovered and both adversaries are successful. The second and third rows show the payoffs when only one attacker succeeds and the last row indicates the case of failure for both attackers.

Table 1. Payoffs table for individual and collusive attacks

Payoffs for individual attacks		Payoffs for collusive attacks	
Attackers: Ψ_1, Ψ_2	Defender: Θ	Each attacker: Ψ_1 or Ψ_2	Defender: Θ
$U^u_{\Psi_1}(t_1), U^u_{\Psi_2}(t_2)$	$U^u_\Theta(t_1)$+$U^u_\Theta(t_2)$	$(U^u_{\Psi_1}(t_1) + U^u_{\Psi_2}(t_2) + 2\epsilon)/2$	$U^u_\Theta(t_1)$+$U^u_\Theta(t_2) - 2\epsilon$
$U^u_{\Psi_1}(t_1), U^c_{\Psi_2}(t_2)$	$U^u_\Theta(t_1)$+$U^c_\Theta(t_2)$	$(U^u_{\Psi_1}(t_1) + U^c_{\Psi_2}(t_2) + \epsilon)/2$	$U^u_\Theta(t_1)$+$U^c_\Theta(t_2) - \epsilon$
$U^c_{\Psi_1}(t_1), U^u_{\Psi_2}(t_2)$	$U^c_\Theta(t_1)$+ $U^u_\Theta(t_2)$	$(U^c_{\Psi_1}(t_1) + U^u_{\Psi_2}(t_2) + \epsilon)/2$	$U^c_\Theta(t_1)$+ $U^u_\Theta(t_2) - \epsilon$
$U^c_{\Psi_1}(t_1), U^c_{\Psi_2}(t_2)$	$U^c_\Theta(t_1)$+$U^c_\Theta(t_2)$	$(U^c_{\Psi_1}(t_1) + U^c_{\Psi_2}(t_2))/2$	$U^c_\Theta(t_1)$+$U^c_\Theta(t_2)$

If the attackers collude with each other, they share all of their utility equally. Additionally, they receive a bonus reward, ϵ, for any successful attack. As we focus on zero-sum games for the experiments, this bonus value is deducted from the defender's payoff. Further, while we assume that adversaries who choose to collude split their

combined payoff equally, it is important to note that the algorithms we present are easily generalized to accommodate arbitrary payoff splits. There are two principal reasons as to why we specify a 50-50 split in this work. First, this division is motivated by inequity aversion theory, as outlined earlier. Second, our focus here is on the factors which lead individuals to collude in the first place, not on the bargaining process which decides their allocation of the rewards (a topic which is itself the subject of a great deal of work in game theory and psychology). Since the reward structures we consider are symmetric between the players, an equal distribution of rewards is a natural assumption. Thus, we can isolate the factors which lead subjects to enter into collusion instead of confounding the decision to collude with an additional bargaining process.

For a given coverage vector C defender's utility at each target t_i attacked individually by attacker i is defined by Equation 5. By replacing Θ with Ψ, the same notation applies for the expected utility of the attacker.

$$U_{\Theta}(t_i, C) = \quad c_{t_i} \cdot U^c_{\Theta}(t_i) + (1 - c_{t_i}) U^u_{\Theta}(t_i) \tag{5}$$

Now we introduce our solution concept for COSGs, the Collusive Security Equilibrium (CSE), which generalizes the SSE to the case of multiple attackers. Let the defender's strategy be a coverage vector C, and the attackers' strategies g_1 and g_2 be functions from coverage vectors to $T \times \{collude, not\ collude\}$. Recall that a strategy profile forms an SSE if (1) the attacker and defender play mutual best responses and (2) the attacker breaks ties in favor of the defender. In COSGs, each attacker's best response depends on the other, since the decision of whether or not to collude depends on the utility the other attacker will obtain. Essentially, any fixed C induces a game between the attackers; the defender sets the attackers' payoff at each target via their resource allocation. The following conditions define a CSE:

1. C is a best response to g_1 and g_2.
2. $g_1(C)$ and $g_2(C)$ form a Nash equilibrium in the game where each target's utility is $U_{\Psi}(t, C)$.
3. Both attackers play *collude* if they obtain strictly greater utility in a (*collude, collude*) equilibrium than (*not collude, not collude*) equilibrium.
4. The attackers break ties between equilibria which satisfy (1)-(3) in favor of the defender.

The first two conditions are analogous to the best response conditions for SSE. In particular, when the followers play a Nash equilibrium (Condition 2), each is playing a best response to the fixed strategies of the other two players. Condition 3 removes the trivial equilibrium where neither attacker chooses to collude because they cannot gain unless the other attacker also decides to collude. Condition 4 enforces the normal SSE condition that remaining ties are broken in favor of the defender.

5 SPECTRE-R: Optimal defender strategy for rational adversaries

SPECTRE-R (Strategic Patrolling to Extinguish Collaborative ThREats from Rational adversaries) takes a COSG as input and solves for an optimal defender coverage vector

corresponding to a CSE strategy through a mixed integer linear program (MILP). This MILP is based on the ERASER formulation introduced by Kiekintveld et al. [11]. The original formulation was developed for SSGs with one defender and one adversary. We extend these ideas to handle collusion between two adversaries via the MILP in Equations 6-20. It is important to note that while the rewards structures we consider in the experiments are zero sum, the MILP we give applies to general sum games. Additionally, our methods are not restricted to the case of two adversaries. In the online appendix[2], we provide a generalization of this MILP to COSGs with N adversaries. Since a naive extension would entail a number of constraints which is exponential in N, we conduct more detailed analysis of the structure of the game, which allows us to formulate a MILP with only $O(N^3)$ constraints. However, this analysis is also deferred to the appendix as our experimental focus is on COSGs with two adversaries.

$$\max d \quad \text{s.t.} \tag{6}$$

$$a_t^{nc}, a_t^c, \alpha_1, \alpha_2, \beta \in \{0, 1\} \tag{7}$$

$$c_t \in [0, 1] \tag{8}$$

$$\sum_{t \in T} c_t \leq m \quad \sum_{t_i \in T_i} a_{t_i}^{nc} = 1 \quad \sum_{t_i \in T_i} a_{t_i}^{c} = 1 \tag{9}$$

$$U_{\Theta}^c(t_1, t_2, C) = U_{\Theta}(t_1, C) + U_{\Theta}(t_2, C) - (1 - c_{t_1})\epsilon - (1 - c_{t_2})\epsilon \tag{10}$$

$$U_{\Theta}^{nc}(t_1, t_2, C) = U_{\Theta}(t_1, C) + U_{\Theta}(t_2, C) \tag{11}$$

$$d - U_{\Theta}^c(t_1, t_2, C) \leq (1 - a_{t_1}^c)Z + (1 - a_{t_2}^c)Z + (1 - \beta)Z \tag{12}$$

$$d - U_{\Theta}^{nc}(t_1, t_2, C) \leq (1 - a_{t_1}^{nc})Z + (1 - a_{t_2}^{nc})Z + \beta Z \tag{13}$$

$$U_{\Psi_i}^c(t_i, C) = U_{\Psi_i}(t_i, C) + (1 - c_{t_i})\epsilon \tag{14}$$

$$U_{\Psi_i}^{nc}(t_i, C) = U_{\Psi_i}(t_i, C) \tag{15}$$

$$0 \leq k_i^c - U_{\Psi_i}^c(t_i, C) \leq (1 - a_{t_i}^c)Z \tag{16}$$

$$0 \leq k_i^{nc} - U_{\Psi_i}^{nc}(t_i, C) \leq (1 - a_{t_i}^{nc})Z \tag{17}$$

$$-\alpha_i Z \leq k_i^{nc} - \frac{1}{2}(k_1^c + k_2^c) \leq (1 - \alpha_i)Z \tag{18}$$

$$\beta \leq \alpha_i \tag{19}$$

$$(\alpha_1 + \alpha_2) \leq \beta + 1 \tag{20}$$

We now proceed to an explanation of the above MILP which is named as SPECTRE-R algorithm in this paper and optimizes defender utility, d, against collusive adversaries. In all equations, nc stands for not colluding cases and c stands for colluding cases, and Z is a large constant. Additionally, constraints with free indices are repeated across all possible values, e.g. $i = 1, 2$ or $t \in T$. Equation 7 defines the binary decision variables. a_t^c and a_t^{nc} whether each target would be attacked if the corresponding adversary chooses to collude or not collude, respectively. α_1 and α_2 indicate each adversary's decision of whether to collude. β is indicates whether collusion actually occurs; it is one if and only if both α_1 and α_2 are one. c_t, introduced in Equation 8 is the defender cover-

[2] https://www.dropbox.com/s/kou5w6b8nbvm25o/nPlayerAppendix.pdf?dl=0

age probability at target t. Equation 9 enforces the defender resource constraint, and that the attackers each select exactly one target. Equations 10 and 11 calculate the defender expected utilities at each target in the case of collusion and no collusion. Equations 12 and 13 define the defender's final expected payoff based on which target is attacked in each case.

Equations 14 and 15 define the expected utility of the attackers in colluding and non-colluding situations. Equations 16 and 17 constrain the attackers to select a strategy in attack set of C in each situation. Equation 18 requires each attacker to collude whenever they obtain higher utility from doing so. Lastly, Equations 19 and 20 set $\beta = \alpha_1 \wedge \alpha_2$.

Proposition 1. *Any solution to the above MILP is a CSE.*

Proof. We start by showing that the followers play a Nash equilibrium as required by condition (2). Let $(a^*_{t_i}, \alpha^*_i)$ be the action of one of the followers produced by the MILP where t_i is the target to attack and α_i is the decision of whether to collude. Let (a_{t_i}, α_i) be an alternative action. We need to show that the follower cannot obtain strictly higher utility by switching from $(a^*_{t_i}, \alpha^*_i)$ to (a_{t_i}, α_i). If $\alpha^*_i = \alpha_i$, then Equations 16 and 17 imply that a_{t_i} already maximizes the follower's utility. If $\alpha^*_i \neq \alpha_i$ then Equation 18 implies that $(a^*_{t_i}, \alpha^*_i)$ yields at least as much utility as $(a_{t_i}, 1 - \alpha^*_i)$, for the a_{t_i} which maximizes the follower's utility given that they make the opposite decision about collusion. So, $(a^*_{t_i}, \alpha^*_i)$ yields at least as much utility as (a_{t_i}, α_i), and condition (2) is satisfied. For condition (3), note that in Equation 18, both followers compute the utility for collusion assuming that the other will also collude. So, if follower i would be best off with $\beta = 1$, the MILP requires that $\alpha_i = 1$. Thus, if both followers receive strictly highest utility in an equilibrium with $\beta = 1$, both will set $\alpha = 1$. In all other cases, the objective is simply maximizing d, which satisfies conditions (1) and (4) by construction.

The following observations and propositions hold for the games with symmetric reward distribution between the two adversaries.

OBSERVATION 1. *The defender optimizes against rational adversaries by enforcing an imbalance in resource allocation between the sides and preventing collusion.*

In SPECTRE-R, the key idea for preventing collusion between two adversaries is to impose a resource imbalance between their situations. This places one adversary in an advantaged condition and the other in a disadvantaged condition. Assuming perfectly rational adversaries, we expect that the disadvantaged adversary will always seek to collude, and the advantaged attacker will always refuse (provided the imbalance outweighs the bonus ϵ). In other words, the optimal solution provided by SPECTRE-R satisfies $\theta \neq 0$ where $\theta = |x_1 - x_2|$, $x_i = \sum_{t_i \in T_i} c_{t_i}$ is difference in total resource allocation to the two sides. This approach incentivizes one attacker to refuse to collude by putting them in a better position than the other.

To analyze the effect of the imbalance in resource allocation on defender expected payoff, we added another constraint to the MILP formulation shown in Equation 21 forces a resource imbalance at an arbitrary level, δ. For the case of symmetric reward distribution, WLOG, we can fix the first attacker to be the one who receives higher payoff and simply linearize the following equation; however generally, we can divide the equation into two separate linear constraints.

$$|k^{nc}_1 - k^{nc}_2| = \delta \tag{21}$$

OBSERVATION 2. *By varying δ, the following cases can occur:*

1. *For $\delta < \delta^*$, $k_i^{nc} - \frac{1}{2}(k_1^c + k_2^c) < 0$ for both attackers and consequently $\alpha_i = 1$ for $i = 1, 2$. In other words, the defender is not able to prevent collusion between the attackers and $\beta = 1$.*
2. *For $\delta = \delta^*$, $k_1^{nc} - \frac{1}{2}(k_1^c + k_2^c) = 0$ for one of the attackers and $k_2^{nc} - \frac{1}{2}(k_1^c + k_2^c) < 0$ for the other one, so consequently α_1 can be either 0 or 1 and $\alpha_2 = 1$. In this case, the followers break ties in favor of the leader, so $\alpha_1 = 0$ and $\beta = 0$.*
3. *For $\delta > \delta^*$, $k_1^{nc} - \frac{1}{2}(k_1^c + k_2^c) > 0$ for one of the attackers and consequently $\alpha_1 = 0$. For the other attacker $k_2^{nc} - \frac{1}{2}(k_1^c + k_2^c) < 0$ and $\alpha_2 = 1$. In other words, the defender is able to prevent collusion between the attackers and $\beta = 0$.*

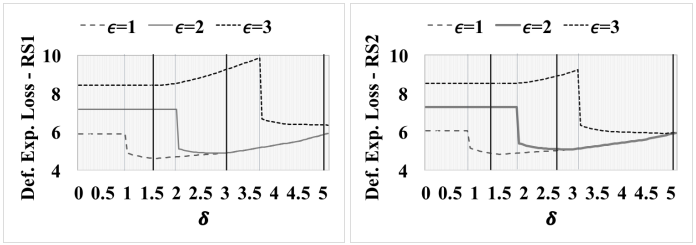
Proposition 2. *The switch-over point, δ^*, introduced in the observation 2 is lower bounded by 0 and upper bounded by 2ϵ.*

Proof. Using Equation 17, we know that at any target t_i, $k_i^{nc} \geq U_{\Psi_i}^{nc}(t_i, C)$. If we assume that the attacker attacks target t_i^c with coverage $c_{t_i}^c$ by adding and subtracting a term as $\epsilon(1 - c_{t_i}^c)$, we can conclude that $k_i^{nc} \geq k_i^c - \epsilon(1 - c_{t_i}^c)$. Consequently, $k_1^c + k_2^c \leq k_1^{nc} + k_2^{nc} + \epsilon(1 - c_{t_1}^c) + \epsilon(1 - c_{t_2}^c)$. On the other hand, according to observation 2.2, at $\delta = \delta^*$, we have $k_1^{nc} - \frac{1}{2}(k_1^c + k_2^c) = 0$. Combining these last two equations, we will get $(k_1^{nc} - k_2^{nc}) \leq \epsilon(1 - c_{t_1}^c) + \epsilon(1 - c_{t_2}^c)$. The LHS is equal to δ^* and the RHS can be rearranged as $2\epsilon - \epsilon(c_{t_1}^c + c_{t_2}^c)$, so we will have $\delta^* \leq 2\epsilon - \epsilon(c_{t_1}^c + c_{t_2}^c)$. Given the fact that coverage at each target is in range $[0, 1]$, the upper bound for $-(c_{t_1}^c + c_{t_2}^c)$ will be zero. Finally, by aggregating these results, we can conclude that $\delta^* \leq 2\epsilon$. Following the same analysis, the lower bound for δ^* can be found starting from $k_1^c + k_2^c \geq k_1^{nc} + k_2^{nc} + \epsilon(1 - c_{t_1}^{nc}) + \epsilon(1 - c_{t_2}^{nc})$ and as a result, $0 \leq \delta^*$.

Given the facts presented in Proposition 2, by enforcing an imbalance of maximum 2ϵ, the defender will be able to prevent collusion. These bounds can be tighter, if we have more information about the distribution of reward at targets. For instance, if reward distribution over targets is close enough to uniform distribution, then the average coverage on each side will be $\bar{c}_{t_1} = \frac{2x_1}{n}$ and $\bar{c}_{t_2} = \frac{2x_2}{n}$, where x_1 and x_2 are fraction of resources assigned to each side and there are $\frac{n}{2}$ targets on each side. As a result, $-(c_{t_1}^c + c_{t_2}^c) \approx -(\bar{c}_{t_1} + \bar{c}_{t_2})$. So we will be able to find an approximate upper bound of $2\epsilon(1 - \frac{m}{n})$, where $m = x_1 + x_2$. This implies that when the ratio of $\frac{m}{n}$ is large, less imbalance in resource allocation is needed to prevent collusion. In the human subject experiments that will be discussed in the next section, we also observed that with a wider range of rewards ($RS2$ compared to $RS1$ in Figure 5(a) in OBSERVATION A) over targets, it becomes harder to prevent collusion between attackers.

SIMULATION 1. Simulation results of SPECTRE-R algorithm for the two games introduced in Section 3 are shown in Figure 3(a) and 3(b) for different values of the bonus ϵ. We vary δ along the x axis, and show the defender loss on the y axis. In all of the plots, *for each epsilon value*, there is a δ value (indicated with gray vertical lines) at which collusion breaks and also a δ^* value (which corresponds to an optimal resource

imbalance θ^*) at which collusion is broken and defender loss is minimized (indicated with solid black vertical lines). The higher the benefit of collusion, the larger the loss of the defender. Note that before collusion is broken, imposing a resource imbalance sometimes increases the defender's loss (see plots for $\epsilon = 3$) because the defender deviates from the optimal coverage probabilities for a traditional SSG without reaping the benefit of reduced cooperation. Similarly, note that defender loss increases for $\delta > \delta^*$ since cooperation is already broken, so the defender only suffers by further reducing coverage on the advantaged player. This emphasizes the importance of precision in modeling and recognizing the optimal δ for allocating resources in real-world settings.



(a) RS1: Def. Exp. Loss vs. δ vs. ϵ (b) RS2: Def. Exp. Loss vs. δ vs. ϵ

Fig. 3. Simulation results of SPECTRE-R: Defender Expected Loss vs. resource imbalance

6 Human Behavioral Approach

6.1 COSG model for bounded rational adversaries

While for perfectly rational adversaries the calculations shown in Figure 3 would hold, our observations from human subject experiments did not match this expectation; the probability of collusion varied continuously with the level of asymmetry in the adversary's' situations. To address this problem, we propose a two layered model which is able to predict (i) the probability of collusion between the adversaries and (ii) the probability of attack over each target for each type of adversary. These layers account for ways in which human behavior experimentally differed from perfect rationality. We then use this model to generate the corresponding optimal patrol schedule.

Probability of attack over targets: We use a separate set of SUQR parameters for each adversary introduced in Section 3.1 to reflect differences in decision making. A generalized form of subjective expected utility is defined in Equation 22 which is a linear function of the modified defender coverage, $\hat{c}_{t_i}$ at target t_i, the uncovered payoff of the attacker, $U^u_{\Psi_i}(t_i)$, the bonus for collusion ϵ and the covered payoff of the attacker $U^c_{\Psi_i}(t_i)$. β is the attackers' decision variable about collusion. A vector of $\omega^\beta_i = (\omega^\beta_{i,1}, \omega^\beta_{i,2}, \omega^\beta_{i,3})$ is assigned to each adversary. Each component of ω^β_i indicates the relative weights that the adversary gives to each feature.

$$\hat{U}_{\Psi_i}(t_i, \beta) = \omega^\beta_{i,1}.\hat{c}_{t_i} + \omega^\beta_{i,2}.(U^u_{\Psi_i}(t_i) + \beta.\epsilon) + \omega^\beta_{i,3}.U^c_{\Psi_i}(t_i) \tag{22}$$

The modified coverage probability, $\hat{c}_{t_i}$, is defined based on Prospect Theory mentioned in Section 2 and is related to the actual probability, c_{t_i}, via Equation 23, where γ and η determine the elevation and curvature of the S-shaped function [6], respectively. These functions are plotted in Section 7.3.

$$\hat{c}_{t_i} = \frac{\eta c_{t_i}^{\gamma}}{\eta c_{t_i}^{\gamma} + (1 - c_{t_i})^{\gamma}} \tag{23}$$

By the SUQR model mentioned in Section 2, the probability (conditioned on the decision about collusion) that the adversary, i, will attack target t_i is given by:

$$q_{t_i}(\hat{C} \mid \beta) = \frac{e^{\hat{U}_{\Psi_i}(t_i, \hat{C}, \beta)}}{\sum_{t_i \in T_i} e^{\hat{U}_{\Psi_i}(t_i, \hat{C}, \beta)}} \tag{24}$$

For each attacker, the SUQR weight vector ω_i^{β}, and the probability perception parameters γ_i^{β} and η_i^{β} are estimated via maximum likelihood (MLE) using data collected from the human subject experiments. This resembles obtaining past data on poaching as mentioned in Section 3.2 to learn these parameters.

Probability of offering to collude: We propose a model which is intuitively based on SUQR to predict the probability of offering collusion by each adversary from a behavioral perspective. Different from the rational behavior model (see Figure 3) where collusion is deterministic, this model assumes that the attackers make stochastic decisions concerning collusion.

The probability of collusion for each adversary is calculated using Equation 25. Here, $\bar{U}^{c}_{\Psi_i} = \sum_{i \in N} \sum_{t_i \in T_i} \hat{U}_{\Psi_i}(t_i, \beta = 1)/(N.|T_i|)$ is the average adversary utility over all targets for a collusive attack and $\bar{U}^{nc}_{\Psi_i} = \sum_{t_i \in T_i} \hat{U}_{\Psi_i}(t_i, \beta = 0)/|T_i|$ is the average adversary utility over all targets for an individual attack.

$$q_i(\beta = 1) = \frac{e^{\bar{U}^{c}_{\Psi_i}}}{e^{\bar{U}^{c}_{\Psi_i}} + e^{\bar{U}^{nc}_{\Psi_i}}} \tag{25}$$

The coefficients in ω_i^{β} are learned for advantaged and disadvantaged attackers and $\beta = 0, 1$ using MLE and data collected from human subject experiments.

6.2 SPECTRE-BR: Optimal defender strategy for bounded rational adversaries

The two above mentioned models are incorporated in SPECTRE-BR (Strategic Patrolling to Extinguish Collaborative ThREats from Boundedly Rational adversaries) to generate the defender optimal strategy by maximizing the expected utility of the defender given in Equation 26 where the defender expected utility is computed as $U_{\Theta}(t_i, C, \beta) = c_{t_i} \cdot U^{c}_{\Theta} + (1 - c_{t_i})(U^{u}_{\Theta} + \beta\epsilon)$ for target t_i, mixed strategy C and the collusion variable β. In this equation, $\mathscr{C}$ represents the set of all possible coverage vectors. We define $q(\beta = 1) = min(q_1(\beta = 1), q_2(\beta = 1))$ and $q(\beta = 0) = 1 - q(\beta = 1)$. This assumption is supported by the fact that collusive attacks happen only when both

parties are sufficiently inclined to collude, and the advantaged player will always be less inclined to offer collusion.

$$\max_{C \in \mathscr{C}} \left(\sum_{i=1}^{N} \sum_{t_i \in T_i} \sum_{\beta=0}^{1} U_{\Theta}(t_i, C, \beta) q_{t_i}(C \mid \beta) q(\beta) \right) \tag{26}$$

7 Human Subject Experiments

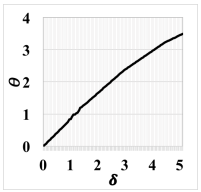
To determine how the behavior of human players differs from perfect rationality, we recruited participants from Amazon Mechanical Turk to play the game described in Section 3. Each experiment used 50 participants. Here we report on the results.

7.1 Resource imbalance effect on collusion

HYPOTHESIS A. *There exists a switch-over δ^* value, at which it is not rational for the adversaries to collude. Consequently, collusion will be broken completely.*

METHOD A. Given the intuition from the rational adversary model, the defender achieves higher expected utility by breaking collusion between the two adversaries. The main idea for preventing collusion was to place one adversary in the advantaged condition so he will avoid collusion. The corresponding optimal strategy results in an asymmetry between the maximum expected utilities on both sides which we referred to as δ. This δ is correlated with the difference between aggregated defender coverage on both sides, θ which is defined in OBSERVATION 2. Figure 4(a) illustrates this relationship by plotting δ on the x axis against the total resource imbalance on the y axis for $RS2$. As δ increases, the resource imbalance also increases. To see how deviating from balanced resource allocation affects human adversaries' decisions about collusion, we ran human subjects experiments on AMT for various δ values for two reward structures $RS1$ and $RS2$. Figures 4(b) and 4(c) illustrate two sample mixed strategy (defender coverage over targets) that we deployed on AMT for $RS2$. In Figure 4(b), resources are distributed symmetrically, while in Figure 4(c) δ was set equal to 1 and one side is covered more than the other. Next, as shown in Figure 5(a), for each reward structure, we tested 4 different coverage distribution i.e., $\delta \in \{0, 1, 2, 3\}$. For each defender strategy we recruited 50 AMT workers. It is worth noting that the models introduced in this paper are valid for both symmetric and asymmetric payoff structures; however, we show the simulation results and experiments for the symmetric case to hold the effect of other variables constant and focus mostly on the distribution of security resources.

OBSERVATION A. The experiments showed that for human adversaries, there is no switch-over point or sharp change in behavior as predicted in Figure 3 when assuming rational adversaries. Rather, the probability of offering collusion decreased smoothly as δ increased for both $RS1$ and $RS2$. This completely contradicts the results assuming a rational adversary as seen in Figure 3. These results are shown in Figure 5(a). δ varies on the x axis while the y axis shows the probability of collusion. For advantaged attackers (denoted RS1-A and RS2-A in Figure 5(a)), we observe a smooth decline in collusion as δ increases. However, for disadvantaged attackers (RS1-DA and



(a) θ vs δ

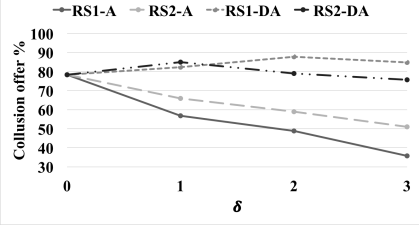
0.15	0	0.32	0.32	0	0.15
0	0.58	0	0	0.58	0
0.52	0	0.43	0.43	0	0.52

(b) $\delta = 0$, RS2

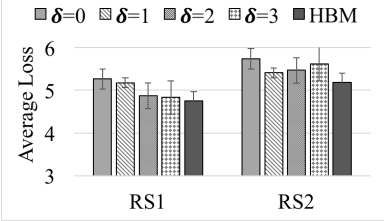
0.03	0	0.22	0.42	0	0.28
0	0.51	0	0	0.64	0
0.44	0	0.35	0.52	0	0.59

(c) $\delta = 1$, RS2

Fig. 4. Defender strategy deployed on AMT and resource imbalance



(a) Collusion level



(b) Average defender loss. SPECTRE-BR outperforms the rational model.

Fig. 5. Collusion level and average defender loss

RS2-DA), we did not observe a significant change in the level of collusion; the disadvantaged attacker always offered to collude with high probability.

ANALYSIS A. The previous observation has several implications: i) for small values of δ there were a considerable number of human players in advantaged situations who refused to collude despite the fact that collusion was rational. ii) For large values of δ, there were a considerable number of human players in advantaged situations who chose to collude despite the fact that collusion was an irrational decision in that situation. This behavior might indicate that the bounded rationality model might be a better fit than the model assuming full rationality when modeling collusive adversaries.

7.2 SPECTRE-BR outperforms model assuming perfectly rational adversaries

HYPOTHESIS B. *A lower probability of collusion decreases defender loss.*

METHOD B. See method A.

OBSERVATION B. Figure 5(b) shows the average defender loss obtained by different strategies for both reward structures, $RS1$ and $RS2$. Strategies generated based on the human behavior model (SPECTRE-BR) are labeled "HBM", while the other bars represent strategies generated by the MILP from Section 4 using the specified δ. Figure 5(b) shows the empirical utility obtained by each strategy. We calculated the average loss from human players who were in the advantaged and disadvantaged position and who decided to collude and not collude. Figure 5(b) plots the average of these losses weighted according to the frequencies with which players decided to collude, observed in the experiments. We see that the human behavior model obtains uniformly lower loss

than the perfect rationality model. In nearly all populations, the difference in utility between the strategies generated by the human behavioral model and those generated by the MILP is statistically significant ($p < 0.05$). Table 2 gives t-test results from comparing the utility obtained by the human behavioral model against each other strategy.

Table 2. Statistical Significance (t-Test p values for SPECTRE-BR and rational strategies)

RS	Rational Strategies (δ)			
	$\delta = 0$	$\delta = 1$	$\delta = 2$	$\delta = 3$
1	3.8×10^{-2}	6.6×10^{-4}	4.0×10^{-3}	4.6×10^{-3}
2	3.5×10^{-6}	1.9×10^{-3}	2.6×10^{-1}	5.1×10^{-2}

ANALYSIS B. Importantly, Figure 5(b) shows that breaking collusion does not always decrease defender loss. For example, in $RS2$, defender loss is lower at $\delta = 2$ compared to $\delta = 3$; however, the chance of collusion (as seen in Figure 5a) is higher for $\delta = 2$. Hence, simply decreasing the level of collusion (which is correlated with an increase in δ per OBSERVATION A.) may not always be optimal for the defender.

7.3 Defender coverage perception

HYPOTHESIS C. *Human adversaries' probability weightings follow S-shaped curves independent of their decision about collusion.*

METHOD C. Parameters of S-curves, γ and η in Equation 23 are learned for the data sets described in METHOD A using the techniques presented in Section 6.

OBSERVATION C. Figures 6(a) and 6(b) show the probability weighting functions learned for the disadvantaged and advantaged adversaries for both groups who are colluding and not colluding for $RS1$. In these figures the defender coverage varies along the x axis, and the attackers' perceptions of defender coverage are shown along the y axis. Figures 6(c) and 6(d) show the same for $RS2$.

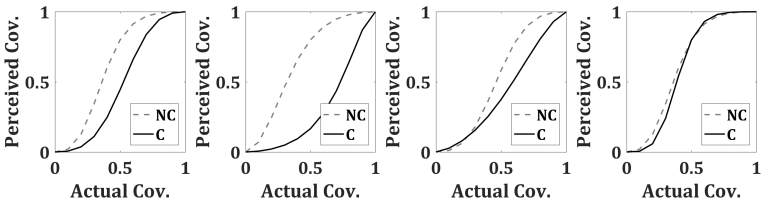
ANALYSIS C. There are two main points in these results: (i) probability weightings followed S-shaped curves, contradicting prospect theory[25, 9], i.e., low probabilities are underweighted and high probabilities are overweighted. (ii) Probability perceptions differed between those who decided to collude and not to collude. This analysis supports the use of SPECTRE-BR because humans' probability weightings are indeed nonlinear.

7.4 Individualism vs. collectivism

HYPOTHESIS D. *Human adversaries who are collectivists are more likely to collude than individualists in nearly all cases.*

METHOD D. All of the participants in our experiments were presented with a survey after playing the game. Eight questions were selected from the 16-item individualism-collectivism scale. Questions with the highest factor loading were selected because prior

research shows that these are the most accurate indicators of individualism vs collectivism [21]. Players responded on a scale from 1 (strongly disagree) to 7 (strongly agree). These responses were used to create a player's OI:OC (overall individualism to overall collectivism) ratio as follows. First, the sum of a player's collectivism responses, c, from collectivism-oriented questions, q_j and individualistic responses, i, from individualism-oriented questions, m_k were calculated as $c = \sum_{j=1}^{4} q_j, \{q_j \in \mathbb{R}^+ : 1 \leq q_j \leq 7\}$ and $i = \sum_{k=1}^{4} m_k, \{m_k \in \mathbb{R}^+ : 1 \leq m_k \leq 7\}$. A player's OI:OC ratio is simply i/c. A player is called an individualist if his OI:OC ratio falls above the median OI:OC score for all players, otherwise he is called a collectivist. We next explore how decisions differ between the two groups. Also please note that the order effect on individualism vs. collectivism analysis is discussed in the online appendix[3] due to space consideration.



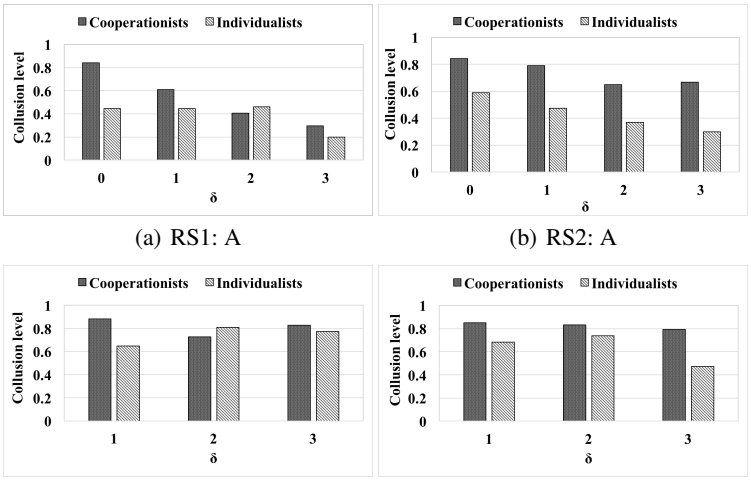
(a) RS1: DA (b) RS1: A (c) RS2: DA (d) RS2: A

Fig. 6. Probability perception curves learned based on PT

OBSERVATION D. The data confirmed that regardless of setting, collectivists are more likely to collude than individualists. This principle was applicable regardless of a player's reward structure, the game's δ value, and whether a player was predetermined to play in an advantaged or disadvantaged state. Figure 7 shows the chance of collusion on the y axis versus δ on the x axis for our two reward structures and in situations where the human is in the advantaged and then disadvantaged situations; we see that the chance of offering collusion for collectivists is always higher than individualists. There is one exception in Figure 7(c), $\delta = 2$, where the chance of collusion for collectivists and individualists is approximately the same (a difference of less than 0.1 is observed). This single case can be considered an exception to the general rule.

ANALYSIS D. Due to factors like morality, social systems, cultural patterns, personality, etc. collectivists may prefer working with a fellow player [24] regardless of reward structure and delta value. However, the fact that collusion decreases as delta value increases has valuable implications. In security games, this means that adopting more rigorous defender strategies has the effect of dissolving collusion amongst attacker groups regardless of their OI:OC ratio. However, it is important to notice that if attackers have a relatively high OI:OC ratio (meaning they are individualists), the defender strategies given here are even more effective at preventing collusion. Please see the appendix for more individualism / collectivism analysis.

[3] https://www.dropbox.com/s/uk9wqrdfq85vhk9/ICAppendix.pdf?dl=0



(a) RS1: A (b) RS2: A

(c) RS1: DA (d) RS2: DA

Fig. 7. Cooperation level for collectivists and individualists. RS1 and RS2 indicate the reward structure, while A and DA indicate that a player was on the advantaged or disadvantaged side.

8 Conclusion

This paper addresses the problem of collusion between adversaries in security domains from a game-theoretic and human behavioral perspective. Our contributions include: (i) the COSG model for security games with potential collusion among adversaries, (ii) SPECTRE-R to solve COSGs and break collusion assuming rational adversaries, (iii) observations and analyses of adversary behavior and the underlying factors including bounded rationality, imbalanced-resource-allocation effect, coverage perception, and individualism / collectivism attitudes within COSGs with data from 700 human subjects, (iv) a human behavioral model learned from the data which incorporates these underlying factors, and (v) SPECTRE-BR to optimize against the learned behavior model to provide better defender strategies against human subjects than SPECTRE-R.

9 Acknowledgement

This research is supported by MURI grant W911NF-11-1-0332.

References

1. Bartilow, H.A., Eom, K.: Free traders and drug smugglers: The effects of trade openness on states' ability to combat drug trafficking. Lat. Am. Polit. Soc. 51(2), 117–145 (2009)
2. Berg, N.: Behavioral economics. 21st century economics: A reference handbook (2010)
3. Camerer, C.: Behavioral game theory. Princeton University Press (2003)
4. Fang, F., Stone, P., Tambe, M.: When security games go green: Designing defender strategies to prevent poaching and illegal fishing. In: IJCAI (2015)

5. Fehr, E., Schmidt, K.M.: A theory of fairness, competition, and cooperation. Quarterly journal of Economics pp. 817–868 (1999)
6. Gonzalez, R., Wu, G.: On the shape of the probability weighting function. Cognitive psychology 38(1), 129–166 (1999)
7. Guo, Q., An, B., Vorobeychik, Y., Tran-Thanh, L., Gan, J., Miao, C.: Coalitional security games. In: Proceedings of AAMAS. pp. 159–167 (2016)
8. Johnson, C.: America's first consumer financial watchdog is on a leash. Cath. UL Rev. 61, 381 (2011)
9. Kahneman, D., Tversky, A.: Prospect theory: An analysis of decision under risk. Econometrica: Journal of the Econometric Society pp. 263–291 (1979)
10. Kar, D., Fang, F., Fave, F.D., Sintov, N., Tambe, M.: A game of thrones: When human behavior models compete in repeated stackelberg security games. In: AAMAS (2015)
11. Kiekintveld, C., Jain, M., Tsai, J., Pita, J., Ordóñez, F., Tambe, M.: Computing optimal randomized resource allocations for massive security games. In: AAMAS (2009)
12. Korzhyk, D., Conitzer, V., Parr, R.: Complexity of computing optimal stackelberg strategies in security resource allocation games. In: AAAI (2010)
13. Korzhyk, D., Conitzer, V., Parr, R.: Security games with multiple attacker resources. In: IJCAI Proceedings. vol. 22, p. 273 (2011)
14. McFadden, D.L.: Quantal choice analaysis: A survey. In: Annals of Economic and Social Measurement, Volume 5, number 4, pp. 363–390. NBER (1976)
15. McKelvey, R.D., Palfrey, T.R.: Quantal response equilibria for normal form games. Games and economic behavior 10(1), 6–38 (1995)
16. Narrod, C., Tiongco, M., Scott, R.: Current and predicted trends in the production, consumption and trade of live animals and their products. Rev. sci. tech. Off. int. Epiz. 30(1) (2011)
17. Nguyen, T.H., Kar, D., Brown, M., Sinha, A., Tambe, M., Jiang, A.X.: Towards a science of security games. New Frontiers of Multi-Disciplinary Research in STEAM-H (2015)
18. Nguyen, T.H., Sinha, A., Gholami, S., Plumptre, A., Joppa, L., Tambe, M., Driciru, M., Wanyama, F., Rwetsiba, A., Critchlow, R., Beale, C.: Capture: A new predictive anti-poaching tool for wildlife protection. In: AAMAS (2016)
19. Nguyen, T.H., Yang, R., Azaria, A., Kraus, S., Tambe, M.: Analyzing the effectiveness of adversary modeling in security games. In: AAAI (2013)
20. Restrepo, A.L., Guizado, Á.C.: From smugglers to warlords: twentieth century colombian drug traffickers. Can. J. Lat. Am. Caribb. Stud. 28(55-56), 249–275 (2003)
21. Singelis, T.M., Triandis, H.C., Bhawuk, D.P., Gelfand, M.J.: Horizontal and vertical dimensions of individualism and collectivism: A theoretical and measurement refinement. Cross-Cultural Research 29(3), 240–275 (1995)
22. Sivadas, E., Bruvold, N.T., Nelson, M.R.: A reduced version of the horizontal and vertical individualism and collectivism scale. Journal of Business Research 61(1), 201 (2008)
23. Tambe, M.: Security and game theory: Algorithms, deployed systems, lessons learned. Cambridge University Press (2011)
24. Triandis, H.C., Gelfand, M.J.: Converging measurement of horizontal and vertical individualism and collectivism. Journal of personality and social psychology 74(1), 118 (1998)
25. Tversky, A., Kahneman, D.: Advances in prospect theory: Cumulative representation of uncertainty. Journal of Risk and uncertainty 5(4), 297–323 (1992)
26. Warchol, G.L., Zupan, L.L., Clack, W.: Transnational criminality: An analysis of the illegal wildlife market in southern africa. International Criminal Justice Review 13(1), 1–27 (2003)
27. Wyler, L.S., Sheikh, P.A.: International illegal trade in wildlife. DTIC Document (2008)
28. Yang, R.: Human Adversaries in Security Games: Integrating Models of Bounded Rationality and Fast Algorithms. Ph.D. thesis, University of Southern California (2014)
29. Yin, Z., Korzhyk, D., Kiekintveld, C., Conitzer, V., , Tambe, M.: Stackelberg vs. nash in security games: Interchangeability, equivalence, and uniqueness. In: AAMAS (2010)