

Human Adversaries in Opportunistic Crime Security Games: How Past success (or failure) affects future behavior

Yasaman Dehghani Abbasi Arunesh Sinha
Nicole Sintov Chao Zhang Milind Tambe

Univeristy of Sothern California
Los Angeles, CA, USA

{ydehghan , aruneshs, sintov, zhan661, tambe }@usc.edu

Martin Short

Georgia Institute of Technology
Atlanta, GA

mbshort@math.gatech.edu

Abstract

There are a growing number of automated decision aids based on game-theoretic algorithms in daily use by security agencies to assist in allocating or scheduling their limited security resources. These applications of game theory, based on the “security games” paradigm, are leading to fundamental research challenges: one major challenge is modeling human bounded rationality. More specifically, the security agency, assisted with an automated decision aid, is assumed to act with perfect rationality against a human adversary; it is important to investigate the bounded rationality of these human adversaries to improve effectiveness of security resource allocation. In (Abbasi *et al*, 2015), the authors provide an empirical investigation of adversary bounded rationality in *opportunistic crime settings*. In this paper, we propose two additional factors in the “subjective utility quantal response” model.

1. Introduction

In recent years, the Stackelberg Security Games (SSG) model has received significant attention for its success in modeling physical security problems and application to real world settings, such as scheduling patrols conducted by the US Coast Guards at multiple major US ports (Shieh *et al*. 2012), allocating federal air marshals on flights of US Air Carriers, and several other applications (Tambe 2011). SSG provides a game theory-based representation of the interaction between an attacker and defender, and provides computational tools to optimize the defender’s action based on possible attacker moves (Tambe 2011, Korzyk, Conitzer and Parr 2010, Gatti 08).

In SSG, the defender (leader) moves first by choosing to play a particular defense strategy. The adversary (follower) observes this strategy and then chooses a best response strategy. In order to prevent the adversary from predicting the defenders actions, the defender must play a distribution over strategies, known as a mixed strategy, rather than a single fixed one. The Stackelberg equilibrium computation involves finding the utility maximizing mixed strategy, taking into consideration the adversary’s response.

Traditionally, SSG assumes a model of a perfectly rational adversary, but in domains such as urban crime, this assumption appears weak. It is known that adversaries in these domains are boundedly rational (Zhang *et al*. 2014) and moreover, human subjects do not generally demonstrate perfect rationality in their decisions (Camerer and Chongn 2004; Costa-Gomes *et al*. 2011). Failure to account for this bounded rationality can lead to non-optimal defender strategies in SSG and hence significant losses for the defender. Therefore, constructing a reliable model of the adversary behavior is vital for security against urban crime.

Models of bounded rationality have received significant attention recently (Gal, Pfeffer 2007; Ficici, Pfeffer 2008; Nguyen *et al*. 2013). A commonly used model is Quantal Response (McKelvey and Palfrey 1995), which models bounded rationality of human subjects by introducing uncertainty into their decision making process.

In SSG literature, variations of Quantal Response (QR) models have been investigated (Yang *et al*. 2013; Nguyen *et al*. 2013; Cui *et al*. 2014). However, only recently a different category of adversaries have been investigated: opportunistic adversaries (Zhang *et al*. 2014). A significant portion of urban crime is opportunistic in nature (Zhang *et al*. 2014); these adversaries, in addition to not being completely rational, are flexible in execution of crime and in seeking opportunities for crime.

In (Abbasi *et al*, 2015), the authors investigate human adversary models in an opportunistic crime setting. This paper focuses on expanding one of the presented models -- Subjective Utility Quantal Response (SUQR) -- and compares it with other proposed models. We show that the new SUQR model outperforms the already presented SUQR in the context of opportunistic crime.

2. Background

2.1. Stackelberg Security Game

A Stackelberg Security Game (SSG) is a game model that captures the interaction between a single defender (leader) and one adversary (follower) (Tambe 2011). The defender

protects a set of targets T with limited number of resources from attack by the adversary. A pure strategy of the defender is an assignment of the security resources to the targets. A mixed strategy is a probability distribution over the set of all possible pure strategies, which is succinctly represented as a vector x of size $|T|$ in which each element of the vector represents the probability of covering a target (Korzhyk, Conitzer, and Parr 2010). SSG assumes strategic adversaries who learn the defender’s strategy by conducting long-term surveillance; the adversary’s pure strategy best response is then to choose a target to attack that maximizes the adversary’s expected utility. The utility of the adversary is given by $U_a^c(t)$ and $U_a^u(t)$ when the adversary attacks the target t and it is covered or uncovered, respectively (the utility of the defender is given by $U_d^c(t)$ and $U_d^u(t)$, respectively). Given the defender mixed strategy x , the adversary’s expected utility in attacking target t is given by the following equation

$$U_a(t, x) = x_t U_a^c(t) + (1 - x_t) U_a^u(t). \quad (1)$$

The equilibrium in this game corresponds to the optimal strategy x that maximizes the defender’s utility assuming the adversary provides his best response. However, Equation 1 assumes a perfectly rational adversary, which may be appropriate in domains such as counter-terrorism. However, in domains such as opportunistic crime settings discussed next, the adversary’s behavior may be governed by models of bounded rationality (Nguyen *et al.* 2013). We review human behavior models accounting for adversary bounded rationality in SSG in Section 2.3.

2.2. Opportunistic Security Game (OSG)

SSG assumes strategic adversaries who learn the defender’s strategy and then decide an attack plan that will not change. However, in domains such as urban crime and theft on trains, the attackers (adversary) are opportunistic, i.e., they are flexible about their plan and seek opportunities for crime rather than strategically planning attacks. For example, a thief may decide not to steal if he observes a police officer, and may move to another area to seek opportunities for committing a crime. Recent work (Zhang *et al.* 2014) explores a model (Quantal Biased Random Movement) of opportunistic attackers within a game interaction between the defender and attackers. Specifically, the authors describe three characteristics of an opportunistic attacker: (i) opportunistically and repeatedly seeks to commit crimes, using a boundedly rational process to select the next crime location; (ii) reacts to real-time information at execution time

rather than planning attacks in advance; and (iii) has limited observation of defender strategy. Section 0 of this paper evaluates the QBRM model along with other models for bounded rationality in the OSG domain.

2.3. Human Behavior Models

In this section, we describe details of some human behavior models that have been explored in the literature, including SUQR and QBRM.

2.3.1. Subjective Utility Quantal Response (SUQR) (Conditional Logit)

In a recent work on SSG (Nguyen *et al.* 2013), the authors combined two key notions of decision making -- Subjective Expected Utility (SEU) (Fischhoff, Goitein, and Shapira 1981) and Quantal Response (McKelvey and Palfrey 1995) -- and proposed the SUQR model. The SUQR model is mathematically equivalent to the conditional logit model in discrete choice theory.

QR models the uncertainty in the decisions made by an agent. Traditionally, the utility maximizing rational agent chooses the action a_i that provides highest utility u_i . In the logit QR model, the rationality assumption is relaxed by positing that the decision making agent chooses an action a_i with probability proportional to e^{u_i} . In the context of SSG, given the defender’s mixed strategy x , the probability of the adversary choosing to attack target t is given by

$$q_t(x) = \frac{e^{\lambda U_a(t, x)}}{\sum_{t' \in T} e^{\lambda U_a(t', x)}} \quad (2)$$

Other models of QR have assumed a power function for formulation of q_t , which is given by

$$q_t(x) = \frac{U_a(t, x)^\lambda}{\sum_{t' \in T} U_a(t', x)^\lambda} \quad (3)$$

In Subjective Expected Utility (SEU) - as proposed in behavioral decision-making (Savage 1972; Fischhoff *et al.* 1981) - the key idea is that individuals have their own evaluations of different factors during decision making process. In a SSG, the factors considered by an adversary in choosing the target to attack include the marginal coverage on target t (x_t) and the reward and penalty for the attacker (R_t^a, P_t^a). Inspired by the idea of SEU, a subjective utility function for the adversary in an SSG setting is as follows: $w_1 x_t + w_2 R_t^a + w_3 P_t^a$, where the weights, w_i , denote the relative importance given to these factors by the adversary. While unconventional at first glance, this model leads to higher prediction accuracy than the classic expected

value function (Nguyen *et al.* 2013). This might be due to the fact that human decision making process may be based on simple heuristics.

The SUQR model replaces the expected value function in logit QR model with the SEU function. In the SUQR model, the probability that the adversary chooses target t is given by:

$$q_t(x) = \frac{e^{w_1 x_t + w_2 R_t^a + w_3 P_t^a}}{\sum_{t' \in T} e^{w_1 x_{t'} + w_2 R_{t'}^a + w_3 P_{t'}^a}} \quad (4)$$

2.3.2. Quantal Biased Random Movement

Quantal Biased Random Movement (QBRM) is a model proposed to describe an opportunistic attacker’s behavior in a defender-attacker interaction on graphs (Zhang *et al.* 2014). The defender moves from node to node on the graph according to some strategic transition matrix, in the hope of dissuading the attacker from committing crimes (not in an effort to catch the attacker). The adversary likewise moves from node to node seeking opportunities for crime at each node. The adversary may commit a crime if no defender is present at a node, but does not commit a crime if a defender is present, which models the flexibility of his plans. The adversary also has a belief about the defender’s position, which is based on the defender’s coverage probability over different stations and trains. The belief of the attacker, c_b , about the defender’s position at any given time is a probability distribution over possible defender positions, and it also depends on real-time observations. That is, if a defender is currently observed, then the attacker’s belief about the position of the observed defender matches the actual position, otherwise it is a probability distribution based on the stationary distribution. Given belief c_b^t at time t and current position i of the adversary, the adversary has an expected utility $U(j|i, c_b^t)$ of moving to position j .

The adversary is also assumed to have bounded rationality, hence the QR model is used to model his choice of actions. More specifically, the probability of the adversary moving from position i to position j is given by the following equation:

$$q_j(i, c_b^t) = \frac{U(j|i, c_b^t)^\lambda}{\sum_k U(k|i, c_b^t)^\lambda} \quad (5)$$

The authors provide algorithms to compute the optimal strategy of the defender, given parameters of the adversary model.

In this paper we use a setting similar to OSG, but explore a variety of different models of the adversary. And to the best

of our knowledge, our work is the first to perform human subject experiments in the context of OSG.

3. Experiments

3.1. Experimental Procedure

We used the data from (Abbasi *et al.*, 2015) to evaluate the performance of various models of human behavior in OSG settings. To simulate urban crimes, an online treasure hunting game was developed, which was set in a metro transportation system. Human subjects, recruited from Amazon Mechanical Turk (AMT), played the role of a treasure hunter. These players attempt to maximize the rewards they receive by accumulating stars from metro stations in a limited time. Each participant played eight games in total: two practice games, two validation games, and four main games. After each practice round, players were provided with feedback on their choices. Then they played two simple validation games, but they were not informed that these were validation games. The results of players who did not score a set threshold in the validation rounds were discarded, in order to eliminate invalid data

Before playing the game, players were provided with detailed instructions explaining the game mechanics (which were also available for review at any time during the game). After the game, a brief survey was used to gather data about the players’ perception of the game, demographics, and risk seeking tendencies.

3.2. Main Games Description

In the main games, human subjects collect rewards by visiting any of the six stations (see an example in Figure 1), while avoiding officers on patrol. Each station has a known reward, indicated by the number of stars. These stars are guarded by two officers, and each officer patrols three stations (there is no overlap in officer patrol). If a player (human) arrives at a station when there is no officer present, his total reward increases by the number of stars of that station; if the officer is present at the station, he does not gain any reward, but does not pay any penalty either. The player’s objective is to maximize the total reward. Players must carefully choose which stations to visit, considering the available information about rewards and officers’ coverage distribution on stations. Players can travel to any station (including the current one) from their current station by train (the dotted lines in Figure 1). Sub-windows contain additional information including total reward, remaining game time, link to full instructions, and the message board.

The officers patrol (move around) stations according to a pre-determined strategy which is calculated offline using

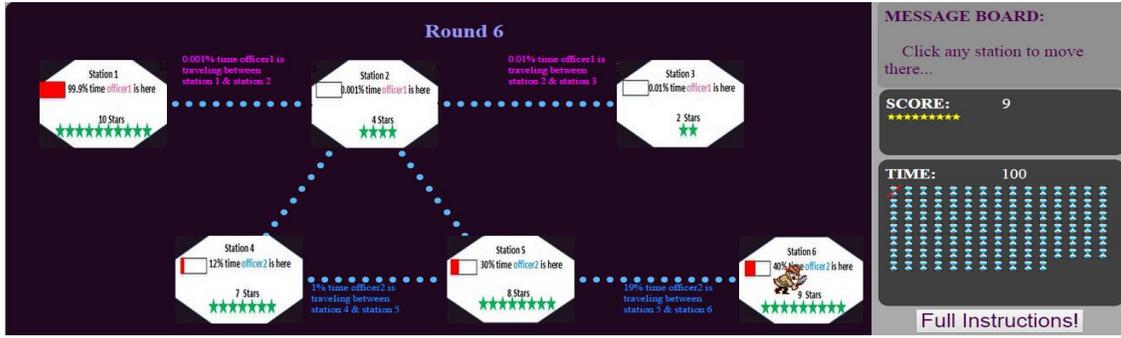


Figure 1. Game interface

an optimization algorithm similar to the one presented in (Zhang *et al.* 2014). Given the topology of the metro system and the stars at each station, a randomized patrolling strategy is generated, which can be used to determine the stationary coverage. The stationary coverage probabilities of each station and trains are revealed to the players, but the exact transition matrix is hidden. During the game, players cannot observe where officers are actually located, unless they encounter the officer at a station.

Each player starts each main game at a random station, and is given a limited amount of game time (100 units). For both the player and the officer, visiting a station takes one unit of time, and traveling to a new station takes a number of time units equal to the minimum distance between source and destination station along train routes. A connected line between two stations in the graph (called an edge) illustrates a route between the two stations with unit distance.

The game can finish in one of three ways: (1) the player exceeds the 45 minutes limit to read the instruction and play all the games or (2) uses up all 100 units of time for each game, and finally (3) each game is randomly terminated after a station visit, which happens with a 10% probability after each such visit. The random termination encourages the players to choose each action carefully, as there is a chance the game may terminate after each visit. The termination randomizer is also used to model attackers exiting the metro system (Zhang *et al.* 2014).

3.2.1. Main Games Design

Recall that our study has practice games, validation games, and four main games. In all main games, there were six stations, but each game had different layouts, different distributions of rewards at each station, and different stationary coverage probabilities. In the experiments, the four games were shown in random order.

3.2.2. Participants

To be eligible to participate, AMT participants must have played more than 500 games on AMT with at least 95% acceptance rate. The games were played in three sets of experiments. In each set, out of about 70 participants, at least 55 unique human subjects successfully completed the games; i.e. successfully passed the validation games, and played a set of four games. In total, 167 unique human subjects successfully passed the validation games and their data were used for evaluation.

4. New SUQR Model

Previous work on opportunistic crime (Abbasi *et al.*, 2015) studied how well human behavior models capture opportunistic attacker behavior and their choices. These models are based on variations of Logit Quantal Response and Subjective Utility Quantal Response. We list these models in Table 1.

Here, we propose a new SUQR (SUQR-S&F) model and compare it with other models using different metrics computed on the experimental data.

In (Abbasi *et al.*, 2015) the authors presented SUQR models with the following features: number of stars at destination station (also called the attractiveness, or *att*), stationary coverage probability (referred to as SP or *sta*) or projected coverage probability (referred to as PP or *proj*) of destination station, the distance between the current station and the destination station (*dis*), and the connectivity degree of the destination station (*con*). Thus, for example, SUQR-SP is

$$\sum_k w_k f_k(i) = w_{att} att_i + w_{sta} Proj_i + w_{dis} dis_i + w_{con} con_i \quad (6)$$

There were two variations of SUQR models in (Abbasi *et al.*, 2015). The first uses a single set of weights whether the attacker currently observes the officer or not. The second uses two sets (conditional or C) of weights, one when the officer is observed and the other when not.

Table 1- Summary of models used for human bounded rationality in OSG

Category	Model	Abbrev.	Generic Mathematical Formulation
Quantal Response	Logit Quantal Response Equilibrium	QR	$q_t(i) = \frac{e^{\lambda U(i)}}{\sum_j e^{\lambda U(j)}}$
	Quantal Biased Random Movement	QBRM	$q_t(i) = \frac{U(i)^\lambda}{\sum_j U(j)^\lambda}$
SUQR	SUQR with Projected Probability (PP)	SUQR-PP	$q_t(i) = \frac{e^{\sum_k w_k f_k(i)}}{\sum_j e^{\sum_k w_k f_k(j)}}$ See eqn.(6)
	SUQR with Stationary Probability (SP) as one factor	SUQR-SP	Same as above except using SP instead of PP
	SUQR with Projected Probability with conditional weights	SUQR-PP-C	Same as SUQR-SP, except two different set of weights
	SUQR with Stationary Probability with conditional weights for observed (o) and not observed (n) case	SUQR-SP-C	Same as above except using SP instead of PP
	SUQR with Stationary Probability with conditional weights and Successful and Failure Weights	SUQR-SP- S&F	Same as above with additional failure and Success weights

In this paper, we introduce a new version of SUQR with additional indicator features that refer to an attacker's preference to stay at (leave) the current station when he was successful (failed) there in the last round. This is to test the hypothesis that if the player successfully attacked a station, he gives additional positive weight to that station and boosts his probability of attack at the same station in the next round. On the other hand, if the player failed to attack his current station, he gives negative weight to the station which boost his probability of attacking other stations. This phenomenon, often referred to as "repeat-victimization", is well-known in criminology (Short *et al*, 2009), making it of interest in the OSG domain.

5. Model Prediction Accuracy

We used four metrics to evaluate how well different models predict human decision making:

5.1. Root-Mean-Square Error (RMSE)

RMSE represents the deviation between model's prediction of attacker's movement (\hat{p}) and the actual proportion movements of AMT players from each station to others (p). The prediction probability (\hat{p}) and proportion movements (p) both distinguish between the situations that the attacker observes and does not observe the officer. Here, n is the number of data points.

$$RMSE(\hat{p}) = \sqrt{MSE(\hat{p})} \text{ where } MSE(\hat{p}) = \frac{1}{n} \sum (\hat{p} - p)^2 \quad (7)$$

5.2. Weighted Absolute Percentage Error (WAPE)

WAPE can provide a more accurate measure of model fit in when we have outliers

$$WAPE = \sum |\hat{p} - p| / \sum P \quad (8)$$

5.3. Akaike information criterion (AIC)

AIC is a measure of relative quality of a model and of the information lost when a given model is used. The model with the smallest AIC is the best fit model among other models, but absolute AIC cannot provide any information about a particular model's goodness of fit.

5.4. Average Weighted Error (AWE)

In RMSE and WAPE metrics, the prediction error is weighted equally for all stations. However, under-prediction in a station with higher rewards will result in higher penalty for the defender. Therefore, we consider weighted errors (WE) as follow:

$$WE = \sum_{l=1}^3 \sum_{k=1}^4 \sum_{j=1}^6 \sum_{i=1}^6 \max(0, p_{i,j,k,l} - \widehat{p}_{i,j,k,l}) att_{j,k,l} \quad (10)$$

where $p_{i,j,k,l}$ is the proportion movements from station i to station j in graph k in experiment l

6. Experimental Results

The following are our main observation from the experiment results, starting with significant deviation from perfectly rational play by human subjects.

- **Human decision-making does not conform to assumption of perfect rationality.** Table 3 shows perfect rationality is doing worst among all the models.
- **Adding additional weights for player success/failure results in further improvement of SUQR model.** In (Kar *et al*, 2015), the authors investigate a human behavior model in the green security domain, and reveal that the attacker adapts his future action based on past

Table 2- Model parameters and their values

Model	Parameters
1. Logit Quantal Response Equilibrium	$\lambda = 0.3645$
2. Quantal Biased Random Movement	$\lambda = 1.1955$
3. SUQR with SP as one factor	$\langle w_{att}, w_{sta}, w_{dis}, w_{con} \rangle = \langle 0.3853, -4.6033, -0.7031, 0.145 \rangle$
4. SUQR with PP as one factor	$\langle w_{att}, w_{proj}, w_{dis}, w_{con} \rangle = \langle 0.2136, -2.5495, -0.6937, 0.0327 \rangle$
5. SUQR with Stationary Probability with conditional weights	$\langle w_{att}^o, w_{sta}^o, w_{dis}^o, w_{con}^o, w_{att}^n, w_{sta}^n, w_{dis}^n, w_{con}^n \rangle = \langle 0.4206, -4.2065, -0.4281, 0.2451, 0.4106, -4.9489, -0.7634, 0.0427 \rangle$
6. SUQR with Projected Probability with conditional weights	$\langle w_{att}^o, w_{proj}^o, w_{dis}^o, w_{con}^o, w_{att}^n, w_{proj}^n, w_{dis}^n, w_{con}^n \rangle = \langle 0.1915, -1.8435, -0.7485, 0.0834, 0.2584, -3.3138, -0.6021, 0.0418 \rangle$
7. SUQR with SP with conditional weights and Successful and Failure weights	$\langle w_{att}^o, w_{proj}^o, w_{dis}^o, w_{con}^o, w_{fail}, w_{att}^n, w_{proj}^n, w_{dis}^n, w_{succ} \rangle = \langle 0.4281, -3.9527, -0.8320, 0.1491, -0.9666, 0.4068, -4.7005, -0.6816, 0.0853, 0.1452 \rangle$

successes and failures. They show that adversaries who have succeeded in attacking a target in one round tend to attack a target with ‘similar’ features in the next round.

Figure 2a, 2b, and 2c reveal similar results in our urban crime experiment. We used the data for three experiments that each include four graphs. As shown in Figure 2a, when the data for all the stations is aggregated, we get similar results as in (Kar *et al*, 2015); the players who have attacked a station successfully tend to stay at that station more than those who failed in their attack. The y-axis in the graph denotes the percentage of (i) attacks on the same station out of the total successful attacks in the previous step and (ii) attacks on the same station out of the total failed attacks in the previous step. Moreover, when the aggregated data is used, differences between the percent of successful people who stay and the percent of failed people who stay is statistically significant (using Student’ t-test with 95% CI). This motivates the addition of two further weights to SUQR-C (the winner of six previously used model) and results in SUQR-S&F: w_{fail} and $w_{succ} \cdot w_{fail}$ (w_{succ}) refers to the additional weight to staying at the same station when the player failed (succeeded). As expected, w_{fail} is negative (-0.9666) and w_{succ} is positive (0.1452). Table 3 also shows that the SUQR-S&F results in better prediction accuracy in all four categories.

Table 3- Model prediction accuracy

Model	AIC	RMSE	WAPE	WE
Perfectly Rational	-	0.1964	0.8562	50.943
QR	8801.0	0.1868	0.7944	47.268
QBRM	8748.2	0.18	0.7494	44.588
SUQR-SP	8461.0	0.1748	0.7211	42.907
SUQR-PP	8572.3	0.17669	0.7385	43.943
SUQR-SP-C	8442.6	0.17019	0.7138	42.471
SUQR-PP-C	8554.7	0.17490	0.7324	43.578
SUQR-S&F	8390.7	0.16372	0.6868	40.867

Figure 2b and 2c shows our further investigation when we group stations into two categories: stations with high reward (Figure 2b) – those with reward more than median reward in the graph - and stations with low reward. Figure 2b shows that, in all experiments and in all graphs, players who succeeded at a high reward station were more likely to remain than those who failed at a high reward station. But that is not the case for Figure 2c, indicating that the strength of this effect is related to how attractive the current station is.

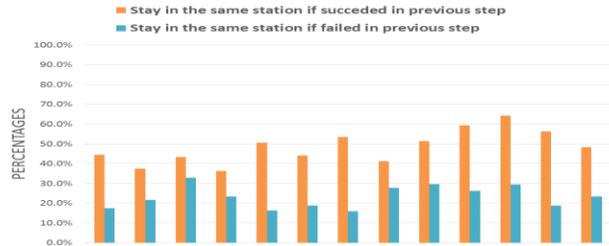


Figure 2a: Attacking the same station

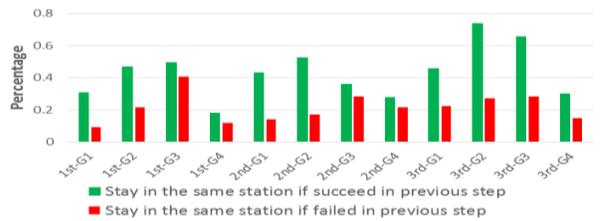


Figure 2b : Satiation with High Rewards

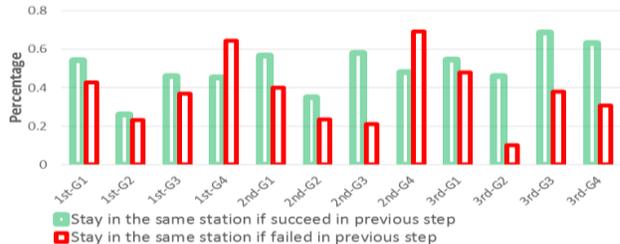


Figure 2c: Stations with Low Rewards

7. Conclusions

With the growing number of automated decision aids based on game-theoretic algorithms in daily use by security agencies, investigations of bounded rationality models of human adversary decision making are now critical, in order to ensure effective security resource allocation and scheduling. In this paper we introduced a new model and use the data from extensive human subject experiments to compare it with bounded rationality models, and illustrate that: the SUQR-S&F model significantly outperformed quantal response in predicting player behavior, thus further indicating that human decision making is not based on maximizing expected utility. These and other findings outlined in this paper provide important advice for practical implementations of decision-aids. Indeed, as police departments begin to adopt these decision aids, modeling and testing these findings in practice in the real-world provides an important next step for future work.

References

- Abbasi, Y. D., Short, M., Sinha, A., Sintov, N., Zhang, C., & Tambe, M (2015). Human Adversaries in Opportunistic Crime Security Games: Evaluating Competing Bounded Rationality Models. In *Advanced Cognitive System*
- Camerer, C.F., Ho, T., Chongn, J. (2004) A cognitive hierarchy model of games. *The Quarterly Journal of Economics*, 861-898.
- Costa-Gomes, M., Crawford, V.P., Broseta, B. (2001). Cognition and behavior in normal-form games: An experimental study, *Econometrica* 69, 1193-1235.
- Cui, J. and John, R.S. (2014). Empirical Comparisons of Descriptive Multi-objective Adversary Models in Stackelberg Security Games. *Decision and Game Theory for Security*. Springer International Publishing. 309-318.
- Ficici, S. and Pfeffer, A. (2008). Simultaneously modeling humans' preferences and their beliefs about others' preferences. In *conference on AAMAS-Volume 1* (pp. 323-330).
- Fischhoff, B., Goitein, B., and Shapira, Z. (1981). Subjective utility function: A model of decision-making. *American Society of Information Science*. 32(5), 391-399.
- Gatti, N. (2008). Game theoretical insights in strategic patrolling: Model and algorithm in normal-form, in *ECAI-08* 403-407.
- Gal, Y., Pfeffer A. (2007). Modeling reciprocal behavior in human bilateral negotiation, In *Proceedings of the National Conference on Artificial Intelligence* -Vol. 22, No. 1, p. 815.
- Kar, D., Fang, F., Delle Fave, F., Sintov, N., & Tambe, M. (2015). "A Game of Thrones": When Human Behavior Models Compete in Repeated Stackelberg Security Games." In *AAMAS*
- Kifer, D., Ben-David, Sh., Gehrke, J. (2004) Detecting change in data streams. *Proceedings of the Thirtieth international conference on Very large data bases*-Volume 30, 180-191. VLDB Endowment.
- Korzhyk, D., Conitzer, V., and Parr, R. (2010). Complexity of computing optimal stackelberg strategies in security resource allocation games. In *AAAI*.
- Nguyen, T.M., Yang R., Azaria A., Kraus S., Tambe M. (2013). Analyzing the Effectiveness of Adversary Modeling in Security Games, In *AAAI*.
- Pita, J., Jain, M., Ordóñez, F., Portway, C., Tambe, M., Western, C., and Kraus, S. (2008). ARMOR Security for Los Angeles International Airport. In *AAAI*. pp 1884-1885.
- Pita, J., John, R., Maheswaran, R., Tambe, M., Yang, R., Kraus, S. (2012): A robust approach to addressing human adversaries in security games, In *Proceedings of the 11th International Conference on AAMAS-Volume 3*, pp. 1297-1298.
- Shieh, E., Yang, R., An, B., Tambe, M., Baldwin, C., DiRenzo, J., Maule, B., Meyer, G. (2012). PROTECT: A Deployed Game Theoretic System to Protect the Ports of the United States In *Proceedings of the 11th International Conference on AAMAS-Volume 1*, pp. 13-20.
- Short, M.B., D'Orsogna, M.R., Pasour, V.B., Tita, G.E., Brantingham, P.J., Bertozzi, A.L., Chayes, L.B. (2008) A statistical model of criminal behavior. *Mathematical Models and Methods in Applied Sciences* 18, 1249-1267.
- Short, M.B., D'Orsogna, M.R., Brantingham, P.J., Tita, G.E. (2009) Measuring and modeling repeat and near-repeat burglary effects. *Journal of Quantitative Criminology* 25, 325-339.
- Tambe, M. (2011). Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned. *Cambridge University Press*.
- Yang, R., Kiekintvled, C., Ordonez, F., Tambe, M., John, R. (2013) Improving Resource Allocation Strategies Against Human Adversaries in Security Games: An Extended Study. *Artificial Intelligence Journal (AIJ)*. 195:440-469.
- Zhang, C., Jiang, A.X., Short, M.B., Brantingham, J.P. and Tambe, M. (2014). Defending Against Opportunistic Criminals: New Game-Theoretic Frameworks and Algorithms, In *Conference on Decision and Game Theory for Security* pp. 3-22 (*Gamesec*).