EasyChair Preprint

№ 1922

Developing Patrol Strategies for the Cooperative Opportunistic Criminals

Yanan Zhao, Mingchu Li and Cheng Guo

November 11, 2019

Developing Patrol Strategies for the Cooperative Opportunistic Criminals *

Yanan Zhao[1,2][0000−0002−4170−3074], MingChu Li[1,2][0000−0001−7969−6415], and Cheng Guo[1,2][0000−0001−7489−7381]

[1] Dalian University of Technology School of Software, Dalian, China
yananzhao@mail.dlut.edu.cn
{mingchul, guocheng}@dlut.edu.cn
[2] Key Laboratory for Ubiquitous Network and Service Software of Liaoning Province, Dalian, China

Abstract. Stackelberg security game (SSG) has been widely used in counter-terrorism, but SSG is not suitable for modeling opportunistic crime because the criminals in opportunistic crime focus on real-time information. Hence, the opportunistic security game (OSG) model is proposed and applied in crime diffusion in recent years. However, previous OSG models do not consider that a criminal can cooperate with other criminals and this situation is very common in real life. Criminals can agree to attack the selected multiple targets simultaneously and share the utility. The police may be unable to decide which target to protect because multiple targets are attacked at the same time, so criminals can gain more utility through cooperation and interfere with police decisions. To overcome this limitation of previous OSG model, this paper makes the following contributions. Firstly, we propose a new security game framework COSG (Cooperative Opportunistic Security Game) which can capture bounded rationality of the adversaries in the cooperative opportunistic crime. Secondly, we use a compact form to solve the problem of crime diffusion in the cooperative opportunistic crime. Finally, extensive experiments to demonstrate the scalability and feasibility of our proposed approach.

Keywords: Game theory · Opportunistic crime · Cooperation mechanism · Human behavior.

1 Introduction

Stackelberg security game (SSG) is a security game framework that describes the interaction between the security agents and terrorists. There are usually two roles of leader and follower in this model, and each participant has his own set of strategies. In each round of the game, the leader always makes decisions first, and the follower makes decisions after observing the leader's strategy. The combination of their decisions affects their ultimate interests.

* Supported by National Nature Science foundation of China under grant No.s: 6157209561877007

In recent years, with the growing threat of terrorist organizations, preventing terrorist incidents has become an important and challengeable task for security agencies. Many agencies use limited resources to protect the targets and produce the strategies about how to allocate these resources [22]. However, the terrorist organizations' strategies are various and it is difficult to predict the target which will be attacked to the security agencies. Fortunately, SSG has made a huge contribution to helping the security agencies in allocating resources reasonably. Many decision systems are designed based on the security game theory. The Trusts system [24] assigns police resources in the subway network to prevent railway crimes, such as fare evasion and theft. The PROTECTION system [17] protects the coast by combating the criminal activities. The PAWS system [25] helps the rangers to find poachers' traps in Queen Elizabeth National Park (QENP) in Uganda. Most applications use the SSG theory, where defenders use limited resources to cover some targets firstly and the attackers observe the defenders' actions to make their most profitable strategies.

Many criminals do not need to take long time to observe the defenders' actions in real life. They only care about the real-time information and find the opportunity to commit crimes. We call this type of crime opportunistic crime. Opportunistic crime theory is widely used in transportation networks. Attacker seeks the target by transportation and when attacker arrives at a station, criminal can choose to commit crime if there is no police or continue to search another target if the attacker observes the police at the same station. The attacker can continue starting the next round of crime after completing a crime or stop. The SSG is not suitable for the opportunistic crimes, because the attacker needs long time observation (weeks or even months) in SSG. Therefore, a new opportunistic security game model is presented in [27]. This work has proposed the concept of OSG, and defined three characteristics of opportunistic criminals who (1) opportunistically and continually seek for targets and diffuse by transportation; (2) have real-time observation rather than long-term latency; and (3) know limited knowledge of the defender.

Traditional SSG assumes human behaviors are completely rational, and this is only fit for modeling terrorist attacks, which require long-term plans. In most cases, attackers are boundedly rational. Just like opportunistic crimes, attackers do not need long-term plan. Many human behavior models have been proposed to consider the bounded rationality of the attackers. Three well-known models are Prospect Theory (PT) and Quantal Response (QR) and Subjective Utility Quantal Response (SUQR). PT states that attackers make decisions based on the potential value of losses and gains rather than the final outcome [10]. QR indicates that the attackers are more likely to choose the targets with higher expected utility [14]. SUQR uses a linear combination of features to replace the expected utility in QR [15]. By experiments in [1], SUQR has the best performance in predicting the human behavior. In this paper, COSG uses the SUQR model to calculate the probability of a target being chosen by the player.

In the OSG criminals can cooperate with each other, for example the criminals agree to attack different targets simultaneously to increase the probability

of successful crime and the excepted utility. Recent work on security game has pointed out the application of cooperative attack in wildlife protection [23]. They have built a multi-round Stackelberg game and proposed a new human behavior model based on it.

We summarize the previous work and propose a novel model COSG (Cooperative Opportunistic Security Game). The contributions of this paper are as follows: Firstly, we combine the cooperation mechanism in SSG with the OSG and establish the COSG model, and COSG better describes the attacker's behavior who can cooperate with other attackers and continuously commit the crime. Secondly, we modify the resource allocation algorithm in traditional opportunistic crime, so that it can be quickly applied in cooperative opportunistic crime resource allocation problem. Finally, we conduct experiments to demonstrate the scalability and feasibility of our proposed approach by inviting 50 volunteers to provide us with data. Experimental results show that our model can effectively help defenders to deal with the cooperative opportunistic criminals.

2 Motivating Scenario

An example of the typical cooperative opportunistic crime is the free market in China. Free markets are trading markets that are spontaneously generated in certain places. Some small free markets generally focus on selling food, clothes, and daily supplies. In the free markets, prices are not regulated by the government. Vendors are free to set prices, and buyers can bargain with sellers. Vendors in the free market can transfer their booths according to the number of customers at different times to maximize their earnings. Although the free markets provide convenience to people, free markets generate many garbage which seriously pollutes the environment during business hours (see Fig. 1(a)). In addition, free markets affect the surrounding traffic conditions and the noise can also interfere people's daily life. Therefore, the security department has set up patrols to combat the vendors in the free markets (see Fig. 1(b)).

To facilitate the understanding, we call the vendor in the free market as attacker and the ranger as defender. The model of free market has two following features: 1)The attackers are opportunists whose behaviors are accorded with the features of opportunistic crime and they attack the targets where they can gain high expected utility. 2)An attacker can choose to cooperate or not cooperate with other attackers. If attackers agree to cooperate, they will attack different targets at the same time and their gains will be divided equally, and if not they will get the pay-offs for individual attacks. Whether to cooperate depends on the utility that an attacker can gain in cooperation and non-cooperation. As far as we know, previous models do not take into account the cooperation mechanism in opportunistic crime, but the cooperation between attackers is indeed a very common phenomenon in reality.

Fig. 1. (a): A vendor generated smoke in free market. (b): The rangers combated vendor and confiscated their tools.

3 Related Work

Crime in transportation network is a very important and challengeable to the security agencies, because the criminals can opportunistically seek targets and transfer by bus or metro train [22]. For example, an attacker arrives a station by metro train and will commit a crime if the attacker does not observe police at the same station. If the criminal finds police at the current station, the attacker will move to another station until gives up or finds a new target. We assume that the crime occurs at the station where there are many people and the probability of successful crime is high. SSG theory is not suitable for this kind of situation due to the long-term planning of the attacker. [27] presents a more flexible model OSG based on the Markov strategy and gives the algorithm EOSG to allocate defender's resource. p_{ij} in Markov transition matrix is the probability of attacker is at station i and defender is at station j at the same time. Obviously if the number of stations grows exponentially, the Markov transition matrix can be very complicated. They also use the COPS algorithm which simplifies the transition matrix to solve the large-scale OSG problems, but the scalability of COPS algorithm is still limited. Previous studies have shown that the performance of OSG with Markov models can be affected by the size of the problem, and we can find another abstract method to simulate the transition with reducing the size of the transition matrix.

Actually, the machine learning methods such as decision tree and cluster have been used in crime prediction [11]. To some extent, these methods are viable, because criminals have certain regularity in committing crimes, and different criminals have their own delinquency proneness. We can collect these crime data and train model to predict the crime hotspot. However, generalization of the model in machine learning is closely related to the data set. We must consider the difficulty of collecting criminal data. [8] points out that in wildlife protection there is a large amount of unlabeled data, and very little labeled data. If we train the model with a small amount of labeled data, it may lead to overfitting.

[23] have provided the basis for our study of the attacker's cooperation mechanism, and they use SUQA to model the behavior of boundedly rational adversaries. In SUQA, a new utility function called subjective utility is defined, which is a linear combination of key features. Experiments show that the SUQA model performs better than the QA model. In this paper, considering the impact of the boundedly rational adversaries, we apply the SUQA model and the cooperative strategy in the OSG to propose a new framework COSG.

4 COSG Model

In this section, we discuss the novel cooperative opportunistic security game model. For convenience, we call the vendor in the free market as attacker and the ranger as defender. We assume that: (1) The entire area is divided into grids of the same size and each grid is called zone. Time is divided into time steps of the same size. (2) Each zone is a target and an attacker can commit opportunistic crime in specific zones. If the attacker finds that there is no defender in the current target, the attacker commits a crime (**S**uccess). Otherwise, the attacker does not commit crime(**F**ailure) and utility is zero. (3) Multiple attackers will share their total utility fifty-fifty if attackers agree to cooperate. (4) COSG is zero-sum game. The defender's utility is non-positive, and the attacker's utility is non-negative. For simplicity, we explain the model with two attackers and one defender.

4.1 Utility

The SSG has two players, an attacker and a defender, and in the COSG we have multiple attackers $\Psi_1, \Psi_2, ..., \Psi_N$ and one defender Θ with M resources. The defender can cover M targets and each attacker can attack a target at the same time. The attacker chooses which target to move to at the next time step based on the expected utility of cooperation and non-cooperation and the probability that the defender will appear in this position. When the target is already protected by a defender's resource, the attacker does not attack and the attacker's utility is zero. Attackers and defender's resources can move to the adjacent zone of the current position at the next time step or stay in the current zone. Attackers cannot observe the coverage distribution of the defender and only when an attacker and a defender's resource move to the same position, the attacker will observe the defender. Similarly, defender cannot observe the positions of attackers, only know the attackers are opportunists. Attackers have a possible initial distribution of defender based on their historical experience and they can use this distribution to measure the attractiveness of a target, but this distribution is not the true distribution of the defender. Defender's transition strategy is the common knowledge of all the players.

To discuss this model more specifically, let T be a set of targets and T_1, T_2 are two subsets of all the targets T, where $T_2 = T - T_1$. T_1 is available to the first attacker Ψ_1 and T_2 is available to the second attacker Ψ_2. At any

time step, the positions of the two criminals are t_1 and t_2 respectively. The two attackers determine their targets through the pay-off of cooperation and non-cooperation and Table 1 summarizes the players' pay-off in all cases. $U^u_{\Psi_1}(t_1)$ indicate the pay-off of Ψ_1 at uncovered target t_1 and $U^u_{\Psi_2}(t_2)$ is the pay-off of Ψ_2 at uncovered target t_2 respectively. Similarly, $U^c_{\Psi_1}(t_1)$ indicate the pay-off of Ψ_1 at covered target t_1 and $U^c_{\Psi_2}(t_2)$ is the pay-off of Ψ_2 at covered target t_2. The defender's pay-offs in uncovered targets t_1, t_2 are $U^u_{\Theta}(t_1)$ and $U^u_{\Theta}(t_2)$ respectively. $U^c_{\Theta}(t_1)$ and $U^c_{\Theta}(t_2)$ are the pay-offs of defender in covered targets. In order to introduce a cooperative mechanism, we use ϵ to represent the reward factor, and the reward factor will motivate two attackers to cooperate. If attackers successfully cooperate with each other they will share all of their pay-offs fifty-fifty and they will receive the reward ϵ.

Table 1. Pay-offs for attacks.

Attackers: Ψ_1, Ψ_2	Crime success status	Cooperation status
$U^u_{\Psi_1}(t_1)$, $U^u_{\Psi_2}(t_2)$	Ψ_1 S, Ψ_2 S	Noncooperation
$U^u_{\Psi_1}(t_1)$, $U^c_{\Psi_2}(t_2)$	Ψ_1 S, Ψ_2 F	Noncooperation
$U^c_{\Psi_1}(t_1)$, $U^u_{\Psi_2}(t_2)$	Ψ_1 F, Ψ_2 S	Noncooperation
$U^c_{\Psi_1}(t_1)$, $U^c_{\Psi_2}(t_2)$	Ψ_1 F, Ψ_2 F	Noncooperation
$(U^u_{\Psi_1}(t_1) + U^u_{\Psi_2}(t_2) + 2\epsilon)/2$	Ψ_1 S, Ψ_2 S	Cooperation
$(U^u_{\Psi_1}(t_1) + U^c_{\Psi_2}(t_2) + \epsilon)/2$	Ψ_1 S, Ψ_2 F	Cooperation
$(U^c_{\Psi_1}(t_1) + U^u_{\Psi_2}(t_2) + \epsilon)/2$	Ψ_1 F, Ψ_2 S	Cooperation
$(U^c_{\Psi_1}(t_1) + U^c_{\Psi_2}(t_2))/2$	Ψ_1 F, Ψ_2 F	Cooperation

Ψ_i is opportunistic criminal, and does not attack when defender's resource cover the current target, so the pay-off of Ψ_i is zero in this case. The COSG is zero-sum game, and the pay-off of defender Θ is $-(U_{\Psi_1}(t_1) + U_{\Psi_2}(t_2))$. In our COSG model, the two factors that affect the probability of the attacker committing a crime are the utility $U_{\Psi_i}(i = 1, 2)$ and the probability that the police will protect a specific target. The two attackers compare their expected utility in case of non-cooperation or cooperation and choose the optimal strategy. If the best choices for both attackers are cooperation, they will attack cooperatively and share the pay-offs. Otherwise, one of attackers is not willing to cooperate, they will commit crime individually.

4.2 Transition and Diffusion

In order to simulate the scenario of opportunistic crime in real life, we introduce the transition and diffusion of the opportunistic crime. The whole area where crime may occur is divided into zones of the same size. The criminals Ψ_1, Ψ_2 and defender Θ can move in the specific zones. We have a more compact division of

time steps so that the players can only move to the adjacent zones or stay in the same zone at each time step, e.g. moving from one zone to a neighboring zone, is assumed to take one time step. At each time step, Θ and Ψ_1, Ψ_2 firstly move at the same time, and then Ψ_1 and Ψ_2 commit crimes at their current targets (or not commit) at this time step, the defender Θ protects the target where they are currently simultaneously. At the next time step, the three players develop their own optimal strategy and repeat the previous process. We explain the transition and diffusion mechanism of players by two 4×4 zones T_1, T_2 (see Fig. 2).

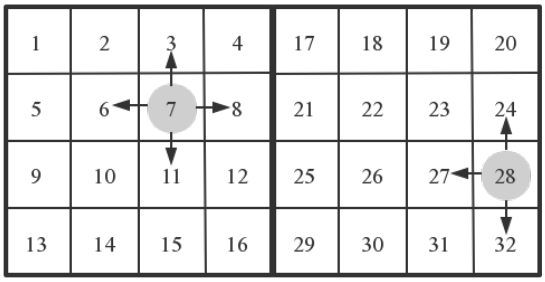


Fig. 2. Distribution of two attackers at time unit t, and they can move to a neighboring zone at next time step $t + 1$.

The attackers Ψ_1, Ψ_2 and defender Θ move within their specific zones. We define that Ψ_1 moves in the left area T_1, and Ψ_2 moves in the right area T_2 and Θ can move in the $T = T_1 \cup T_2$. At this time step t, Ψ_1 is in target 7 of T_1, and Ψ_2 is in target 28 of T_2. If the two attackers commit crimes in their current zones based on if they observe defender Θ at time step t. At the next time unit $t + 1$, all the players can move to an adjacent zone to commit opportunistic crime or protect the target. For example, Ψ_1 only can move to the target $3, 6, 8, 11$ or stay in the target 7 at time step $t + 1$. For an attacker, which target to be chosen depends on the utility of the target when cooperation and non-cooperation and the probability of this target is protected, so we can give the transition matrix of Ψ_1, Ψ_2 and Θ. To the attacker Ψ_1, transition matrix of Ψ_1 is T_{Ψ_1}, and T_{Ψ_1} is a $5 \times (4 \times 4)$ matrix. The (4×4) represents each target number in T_1, and the 5 represents a strategy choice to move up, down, left, right or stay. So each element $x_{i,j}$ in row i and column j is the probability of moving to a neighboring zone when Ψ_1 is in zone j.

In the transition matrix (see Fig. 3), the vector in column 2 is $(0, \frac{1}{4}, \frac{1}{3}, \frac{1}{6}, \frac{1}{4})^T$, so when attacker Ψ_1 is in target 2, the probability of moving down to target 6 is $\frac{1}{4}$, and the probability of moving left to target 1 is $\frac{1}{3}$, and the probability of moving right to target 3 is $\frac{1}{6}$, and the probability of staying in target 2 is $\frac{1}{4}$. There is no target for attacker to move up when in target 2, the probability of moving up is 0. The attacker can move from target 1 to target 2 and also move

from target 2 to target 1, So these two probabilities are equal in T_{Ψ_1} and they are $\frac{1}{3}$.

$$T_{\Psi_1} = \begin{array}{c} \begin{array}{cccc} 1 & 2 & \dots & 16 \end{array} \\ \begin{pmatrix} 0 & 0 & \dots & \frac{3}{7} \\ \frac{1}{3} & \frac{1}{4} & \dots & 0 \\ 0 & \frac{1}{3} & \dots & \frac{1}{7} \\ \frac{1}{3} & \frac{1}{6} & \dots & 0 \\ \frac{1}{3} & \frac{1}{4} & \dots & \frac{2}{7} \end{pmatrix} \end{array} \begin{array}{l} \text{move up} \\ \text{move down} \\ \text{move left} \\ \text{move right} \\ \text{not move (stay)} \end{array}$$

Fig. 3. Transition matrix of attacker Ψ_1.

The probability that Ψ_1 moves from zone i to zone j and Ψ_2 moves from zone m to zone n at next time step is

$$\begin{aligned} & p(j,n) = p_{\Psi_1}(i,j) \cdot p_{\Psi_2}(m,n) \\ & s.t. \quad i,j \in T_1, \quad j \in Adj(i) \\ & \qquad m,n \in T_2, \quad n \in Adj(m) \end{aligned} \tag{1}$$

where Adj is the set of all adjacent zones of a specified zone. Let $p_{\Psi_1}(i,j)$ denotes the probability of Ψ_1 in target i and choose to attack target j at next time step. Similarly, $p_{\Psi_2}(i',j')$ denotes the probability of Ψ_2 in target i' and choose to attack target j' at next time step. $p_{\Psi_1}(i,j)$, $p_{\Psi_2}(m,n)$ can be obtained from attackers' transition matrix T_{Ψ_1} and T_{Ψ_2} respectively. We give the equation of $p_{\Psi_1}(i,j)$, and $p_{\Psi_2}(m,n)$ is calculated similarly to Equation (2).

$$p_{\Psi_1}(i,j) = \max\{(1 - \overrightarrow{c_{b,t}(j)}) \cdot Att(j)\} \tag{2}$$

In Equation (2) $\overrightarrow{c_{b,t}}$ represents the attacker's belief states of defender's place at next time step, so $\overrightarrow{c_{b,t}(j)}$ is the probability distribution that the police Θ may appear in the target j to the attacker Ψ_1. Att is the attractiveness of the neighboring zones to the attacker. The attractiveness of targets Att is attacker's probability distributions of choosing target at next time step based on the subjective utility and Att is calculated as Equation (3).

$$Att(j) = \max\{p^{nc}_{\Psi_1}(j), p^{c}_{\Psi_1}(j)\} \tag{3}$$

We have known that Ψ_1 and Ψ_2 both are bounded rational, so we use the SUQR model to describe the probability that they choose their own targets and whether they prefer to cooperate. The SUQR extends the classic quantal response model by replacing the excepted utility with a subjective utility function. In the case of cooperation and non-cooperation, the probabilities that Ψ_1 will

choose the zone j at next time step are shown in Equation (4), and the equation of Ψ_2 can be generated likewise.

$$\begin{aligned} p^{nc}_{\Psi_1}(j) &= \frac{e^{SU^{nc}(j)}}{\sum\limits_{I \in T_1} e^{SU^{nc}(I)}} \\ p^{c}_{\Psi_1}(j) &= \frac{e^{SU^{c}(j)}}{\sum\limits_{I \in T_1} e^{SU^{c}(I)}} \end{aligned} \tag{4}$$

where the SU^c and SU^{nc} are the subjective utility functions of an attacker in an zone when the two sides cooperate successfully (c) or cooperate unsuccessfully (uc). If one's best choice is to cooperate but another's optimal choice is not to cooperate or both attackers choose not to cooperate, we refer to these situations as cooperation failed. In this case, Ψ_1 and Ψ_2 commit crimes individually. Only when the best choices for criminals both are cooperation, they will attack cooperatively and share their pay-offs.

For the defender Θ, we do not need to consider whether to cooperate, and the defender arranges resources based on the subjective utility, so the probability of Θ will protect target y in next time step is

$$p_\Theta(y) = \frac{e^{SU(y)}}{\sum_{X \in T} e^{SU(X)}} \tag{5}$$

where $y \in T$. Let $p_\Theta(x, y)$ denotes the probability that a defender's resource in zone x and move to zone y at next time step, and $p_\Theta(x, y)$ is an element in the transition matrix T_Θ.

$$p_\Theta(x, y) = p_\Theta(y) \tag{6}$$

The two opportunistic criminals can attack target j and target n at next time step when the target is not covered. Thus, we only pay attention to if the two targets which will be attacked are protected by the defender's resources. The probability distribution of Θ covers the two targets after t time steps is shown as Equation (7) where $\overrightarrow{c_0}$ is the initial state distribution of the resources.

$$\overrightarrow{c_t}(j, n') = T^t_\Theta \cdot \overrightarrow{c_0}(j, n) \tag{7}$$

4.3 Optimal Resource Allocation Strategy

In our model, we can obtain the combination of the attackers' locations and the defender's locations at each time step. Attackers make choices on account of defender's place and the attractiveness of the neighboring zones. Defender dispatches m resources based the initial state distribution and the transition matrix. We have described the behavior of the attackers and defender in COSG model, and in this section we give the formulas to find the optimal patrol strategy. We focus on the interaction between attackers Ψ_1, Ψ_2 and defender Θ.

Our optimal resource allocation strategy is to minimize the loss of defender in each state. We consider the locations where the attackers appeared, and whether the defender can protect these targets timely. The attackers are opportunists, and they do not take action if they notice the defender in the same zone, so the defender's loss will be reduced. We have

$$U_p(k) = V_p \cdot X_k \tag{8}$$

where $U_p(k)$ is the defender's expected utility at kth time step. V_p represents the utility for the two targets where the attackers in and we can get the utility based on the probability of the attackers launch crimes in the two targets accordingly. X_k is the probability of defender cover the targets at kth time step.

The defender's goal is to minimize the total expected utility of all time steps. The more time steps we set, the more we can simulate opportunistic crimes in reality. Therefore, the objective of defender is

$$\begin{aligned} Obj &= \lim_{K\to\infty} \sum_{k=0}^{K} U_p(k) \\ &= \lim_{K\to\infty} \sum_{k=0}^{K} V_p \cdot ((1-\alpha)\cdot T_\Theta)^k \cdot X_1 \end{aligned} \tag{9}$$

Only unknown variable in equation (9) is T_Θ, and it can be denoted as the defender's decision.

5 Experiments

We evaluate the performance of our approach based on extensive experiments. We use Jupyter Notebook (version 5.7.6) and all results are performed on a 64-bit PC with a 3.30 GHZ CPU and a 16.0 GB RAM. Each data point we report is an average of 50 different samples.

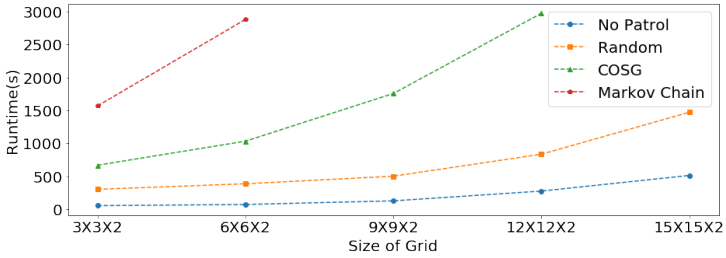
5.1 Data Sets

In our experiments, we simulate the cooperative opportunistic crime in real life, and simplify the model of real-world. In our model, the whole area is divided into zones of the same size, and we set the entire area to two $N \times N$ zones. Time is divided into continuous and equal time steps, and player moves from one zone to a neighboring zone at one time step. Defender has m resources and the initial distribution of these resources which the two attackers do not know is set based on the importance of targets. The two attackers know a possible distribution of police based on their historical experience. The defender's transition matrix is the common knowledge of all players. We randomly set the attractiveness function Att of each target i, so the attacker's route is more random and difficult to predict. The defender's utility of not covering at least one target is $U_\Theta < 0$ and $U_\Theta = 0$ is covering both two targets in our experiments. Similarly, the criminal's

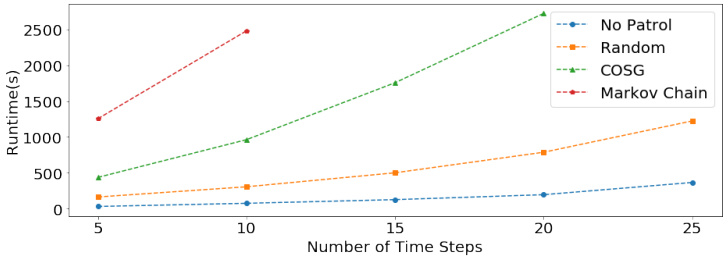
utility of attacking a target successfully is $U_{\Psi_i} > 0$ and $U_{\Psi_i} = 0$ is giving up committing crime. The attacker decides whether to cooperate according to the utility in case of noncooperation and cooperation. We set the exit rate of the attacker $\alpha = 0.1$.

5.2 Results

The experiment involves four models and there are COSG model, Markov chain model, random patrol model, and no patrol model. Players in our model decide how to move based on the subjective utility. In the random patrol model, defender chooses the next target to protect randomly and we set the value of each element in the transition matrix to $\frac{1}{5}$. To the no patrol model, the defender does not cover any targets, so the attackers commit the crime arbitrarily. In the Markov chain model, the players can move to any zones at a time step.



$(a) : m = 3, \gamma = 15$



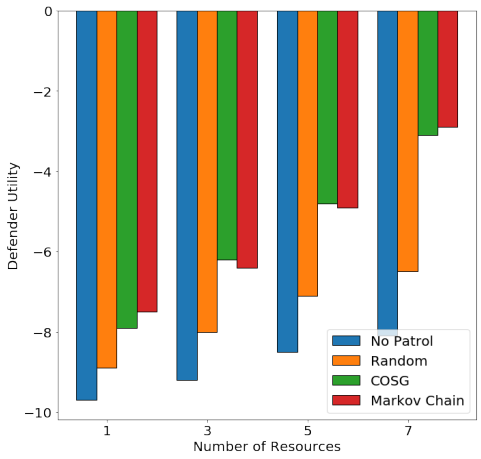
$(b) : m = 3, |G| = 9 \times 9 \times 2$

Fig. 4. Runtimes analysis.

We compare the scalability of our model. The result is shown as Figure 4(a) where the x-axis represents the size of grid and the y-axis indicates runtime. γ denotes the number of time step. Our model is greatly affected by the size of grid and cannot scale up to the size of grid larger than 12×12×2 with the runtime cap of 3000 seconds. Random strategy and no patrol strategy are always faster than our model, because they do not need to consider the subjective

utility of the defender. The Markov chain model requires the maximum runtime, because the transition matrix of it is more complicated than the other three models. In our experiments, we also compare the runtime of our strategy with different time length. The result is shown in Fig.4(b) and $|G|$ denotes the size of grid. Runtime rises faster as the number of time steps increase, because more boundary constraints are considered. We deal with small-scale issues in this paper, and we can find that scalability is still a major challenge.

Fig.5 shows that the number of defender's resources m can influence the defender's utility. When we set the number of time steps $\gamma = 15$ and the size of grid $|G| = 9 \times 9 \times 2$, the defender's utility rises as the number of resources increases. The random patrol model and no patrol model cannot give a more satisfactory patrol strategy, because the two models do not consider too much bounded rationality of the players. Our COSG model and Markov chain model perform better than the previous two models.



$\gamma = 15$, $|G| = 9 \times 9 \times 2$

Fig. 5. Different resources of problem.

6 Summary

In this paper, we propose an innovative model for cooperative opportunistic and boundedly rational criminals. Furthermore, we introduce a compact form of transition matrix representation unlike previous opportunistic security game which used Markov chain to describe players' diffusion. Traditional Stackelberg game models require attacker to make decision in advance, but the attacker in our model reacts to real-time information. As shown in our experimental results, the runtime of our model is better than the Markov chain model. However,

scalability is still a major challenge, and the current model is only suitable for small-scale problems. In future work, we can use the abstract method or constraint generation to compress the scale of the problem. In addition, it is also feasible to construct the opportunistic security game model by using neural networks.

References

1. Abbasi, Y. D., Short, M., Sinha, A., Sintov, N., Zhang, C., Tambe, M.: Human numes in opportunistic crime security games: Evaluating competing bounded rationality models. In: Proceedings of the Third Annual Conference on Advances in Cognitive Systems ACS. (2015)
2. Abbasi, Y., Kar, D., Sintov, N., Tambe, M., Ben-Asher, N., Morrison, D., Gonzalez, C.: Know Your Adversary: Insights for a Better Adversarial Behavioral Model. In: CogSci. (2016)
3. Bondi, E., Fang, F., Hamilton, M., Kar, D., Dmello, D., Choi, J., Nevatia, R.: Spot poachers in action: Augmenting conservation drones with automatic detection in near real time. In: Thirty-Second AAAI Conference on Artificial Intelligence. (2018)
4. Fang, F., Stone, P., Tambe, M.: When security games go green: Designing defender strategies to prevent poaching and illegal fishing. In: Twenty-Fourth International Joint Conference on Artificial Intelligence. (2015)
5. Fang, F., Jiang, A. X., Tambe, M.: Optimal patrol strategy for protecting moving targets with multiple mobile resources. In: Proceedings of the 12th International Conference on Autonomous Agents and Multiagent Systems. (2013)
6. Gholami, S., Zhang, C., Sinha, A., Tambe, M.: An extensive study of Dynamic Bayesian Network for patrol allocation against adaptive opportunistic criminals (2015)
7. Gholami, S., Wilder, B., Brown, M., Sinha, A., Sintov, N., Tambe, M.: A game theoretic approach on addressing cooperation among human adversaries. In: Proceedings of the 15th International Conference on Autonomous Agents and Multiagent Systems. (2016)
8. Gurumurthy, S., Yu, L., Zhang, C., Jin, Y., Li, W., Zhang, X., Fang, F.: Exploiting Data and Human Knowledge for Predicting Wildlife Poaching. In: In Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies. (2018)
9. Halvorson, E. D., Conitzer, V., Parr, R.: Multi-step multi-sensor hider-seeker games. In: Twenty-First International Joint Conference on Artificial Intelligence. (2009)
10. Kahneman, D., Tversky, A.: Prospect theory: an analysis of decision under risk. Econometrica **47**(2), 263-292 (1979)
11. Kar, D., Ford, B., Gholami, S., Fang, F., Plumptre, A., Tambe, M., Mabonga, J.: Cloudy with a chance of poaching: Adversary behavior modeling and forecasting with real-world poaching data. In: Proceedings of the 16th International Conference on Autonomous Agents and Multiagent Systems. (2017)
12. Li, M., Cao, Y., Qiu, T.: Optimal patrol strategies against attacker's persistent attack with multiple resources. In: IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation. (2017)
13. Laan, C. M., Barros, A. I., Boucherie, R. J., Monsuur, H., Timmer, J.: Solving partially observable agent-intruder games with an application to border security problems. Naval Research Logistics **66**(2), 174-190 (2019)

14. McKelvey, R. D., Palfrey, T. R.: Quantal response equilibria for normal form games. Games and economic behavior **10**(1), 6-38 (1995)
15. Nguyen, T. H., Yang, R., Azaria, A., Kraus, S., Tambe, M.: Analyzing the effectiveness of adversary modeling in security games. In: Twenty-Seventh AAAI Conference on Artificial Intelligence. (2013)
16. Pita, J., Jain, M., Ordóñez, F., Tambe, M., Kraus, S., Magori-Cohen, R.: Effective solutions for real-world stackelberg games: When agents must deal with human uncertainties. In: Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems. (2009)
17. Shieh, E., An, B., Yang, R., Tambe, M., Baldwin, C., DiRenzo, J., Meyer, G.: Protect: A deployed game theoretic system to protect the ports of the united states. In: Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems. (2012)
18. Sinha, A., Fang, F., An, B., Kiekintveld, C., Tambe, M.: Stackelberg Security Games: Looking Beyond a Decade of Success. In: Twenty-Seventh International Joint Conference on Artificial Intelligence. (2018)
19. Tsai, J., Kiekintveld, C., Ordonez, F., Tambe, M., Rathi, S.: IRIS-a tool for strategic security allocation in transportation networks. (2009)
20. Tayebi, M. A., Ester, M., Glässer, U., Brantingham, P. L.: Crimetracer: Activity space based crime location prediction. In: Proceedings of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. (2014)
21. Varakantham, P., Lau, H. C., Yuan, Z.: Scalable randomized patrolling for securing rapid transit networks. In: Twenty-Fifth IAAI Conference. (2013)
22. Wang, X., An, B., Strobel, M., Kong, F.: Catching Captain Jack: Efficient time and space dependent patrols to combat oil-siphoning in international waters. In: Thirty-Second AAAI Conference on Artificial Intelligence. (2018)
23. Wang, B., Zhang, Y., Zhou, Z. H., Zhong, S.: On repeated stackelberg security game with the cooperative human behavior model for wildlife protection. Applied Intelligence **49**(3), 1002-1015 (2019)
24. Yin, Z., Jiang, A. X., Johnson, M. P., Kiekintveld, C., Leyton-Brown, K., Sandholm, T., Sullivan, J. P.: Trusts: Scheduling randomized patrols for fare inspection in transit systems. In: Twenty-Fourth IAAI Conference. (2012)
25. Yang, R., Ford, B., Tambe, M., Lemieux, A.: Adaptive resource allocation for wildlife protection against illegal poachers. In: Twenty-Fourth International Joint Conference on Artificial Intelligence. (2015)
26. Yang, Z., Zhu, J., Teng, L., Xu, J., Zhu, Z.: A double oracle algorithm for allocating resources on nodes in graph-based security games. Multimedia Tools and Applications **77**(9), 10961-10977 (2018)
27. Zhang, C., Jiang, A. X., Short, M., Brantingham, P. J., Tambe, M.: Modeling Crime diffusion and crime suppression on transportation networks: An initial report. In: 2013 AAAI Fall Symposium Series. (2013)
28. Zhang, C., Sinha, A., Tambe, M.: Keeping pace with criminals: Designing patrol allocation against adaptive opportunistic criminals. In: Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems. (2015)