Game-theoretic Resource Allocation with Real-time Probabilistic Surveillance Information

Wenjun Ma, Weiru Liu, and Kevin McAreavey

School of EEECS, Queen's University Belfast
{w.ma, w.liu, kevin.mcareavey}@qub.ac.uk

Abstract. Game-theoretic security resource allocation problems have generated significant interest in the area of designing and developing security systems. These approaches traditionally utilize the Stackelberg game model for security resource scheduling in order to improve the protection of critical assets. The basic assumption in Stackelberg games is that a defender will act first, then an attacker will choose their best response after observing the defender's strategy commitment (e.g., protecting a specific asset). Thus, it requires an attacker's full or partial observation of a defender's strategy. This assumption is unrealistic in real-time threat recognition and prevention. In this paper, we propose a new solution concept (i.e., a method to predict how a game will be played) for deriving the defender's optimal strategy based on the *principle of acceptable costs of minimax regret*. Moreover, we demonstrate the advantages of this solution concept by analyzing its properties.

1 Introduction

Recently, the problem of allocating limited security resources for protecting critical infrastructure and the general public has attracted significant research interest. In the literature, most existing work deals with this problem in the Stackelberg game framework [10, 14]. That is, a defender selects their strategy based on the assumption that an attacker can observe and understand the defender's strategy. As a result, the Stackelberg game framework mainly focuses on the effective scheduling of limited security resources through past experience or knowledge.

Example 1 *A surveillance system in an airport has detected that a person has been loitering in the shopping area excessively. A combination of metal detection and body-shape image capture at the entrance to the shopping area suggest that the person may be carrying a gun and a bag. Moreover, there are three critical assets in the shopping area: a Foreign Currency Exchange office, a Supermarket and a Jewelry Shop. Suppose there is currently only one security team available, where should the security team protect?*

In this example, using information obtained by the surveillance system and the event inference method in [7, 15], we can infer the suspect's motivation, e.g., detonating a bomb in a public place, carrying out a robbery, etc. Malevolent motivations such as these can be used to model subsequent attack preferences

(e.g., a robber may be more likely to target a bank than a shopping mall, while a bomber may be more likely to target a shopping mall than a bank). Thus, we can make use of such motivations as indicators of different types of attacker. Given that there may be multiple potential targets for an attacker and that a defender has limited resources for protecting these targets, it is essential for the defender to determine which target an attacker is most likely to attack. This type of problem is called a Surveillance Driven Security Resource Allocation (SDSRA) problem.

Since, in SDSRA problems, security teams act after detecting a potential threat, it suggests that an attacker and a defender actually execute their actions simultaneously. This contrasts with the type of security games addressed in [14], where a security manager assigns a patrol schedule for the security team first and the attacker then makes their decision based on the observation of the defender's strategy. As a result, current solution concepts based on the Stackelberg game framework, such as the Strong Stackelberg equilibrium [14], robust non-equilibrium solutions [11] and worst-case approaches for interval uncertainty [4], are not well-suited for modelling SDSRA problems. Moreover, in such games, since an attacker cannot know a defender's payoff value as well as a defender's probability distribution over different attacker types (motivations), traditional solution concepts, such as the Bayes-Nash equilibrium [5], cannot handle these problems either. Therefore, a natural direction is to consider a new game framework and solution concept for handling these SDSRA problems.

In this paper, we propose a *principle of acceptable costs of minimax regret* for the SDSRA game model based on three assumptions: (i) influence of loss-aversion for each player; (ii) minimax regret and loss-aversion based strategy selection for each player; (iii) knowledge of payoff matrices.[1] With this principle, we propose a method to predict the strategy which will be selected by each type of attacker and to determine the defender's optimal strategy. Finally, we analyze the properties of this new solution concept to justify our framework and suggest a linear programming implementation. Our main contributions are as follows: (i) we extend the application of security games to the SDSRA problem; (ii) with our solution concept, we dynamically predict an attacker's target/goal based on information gathered and inferred from an intelligent surveillance system; (iii) according to an attacker's strategy, we flexibly determine a defender's optimal strategy by balancing the expected payoff for successful threat prevention and for unaffordable losses caused by failure; and (iv) we validate our method by analyzing its properties.

The rest of this paper is organized as follows: Section 2 introduces three assumptions underpinning the new solution concept for the SDSRA problem; Section 3 predicts the optimal mixed strategy for each possible type of attacker and analyzes the properties of our attacker strategy prediction method; Section 4 discusses the selection of the optimal strategy for the defender; and Section 5 discusses related work and concludes the paper with future work proposals.

[1] A defender's knowledge of both players' payoff matrices and an attacker's knowledge of their own payoff matrix.

2 Rationalizability in SDSRA

When a security manager obtains real-time probabilistic surveillance information [15][2], we can describe the security game for SDSRA as follows:

Definition 1 *A security game of SDSRA is a 6-tuple of* $(N, \Theta, A, \Psi, M, U)$*:*

- $N = \{1, 2\}$*, where* 1 *stands for a defender and* 2 *stands for an attacker.*
- $\Theta = \{t_1, \ldots, t_n\}$*: set of potential types of an attacker.*
- $A = \{A_i \mid i = 1, 2\}$*:* A_i *is a pure strategies set of player* i*. Here, a pure strategy is an action executed by a player.*
- $\Psi = \{(a_k, b_l) \mid a_k \in A_1$ *and* $b_l \in A_2\}$*: set of all pure strategy profiles.*
- $P = \{p(t) \mid p(t)$ *is a probability value for each element* t *of* $\Theta\}$*.*
- $U = \{u_{i,t}(X) \mid i \in N,\ t \in \Theta,\ X \in \Psi\}$*,* $u_{i,t}(X)$ *is a payoffs function* $u_{i,t} : \Psi \rightarrow R\}$*.*

The probability distribution P *and the defenders utilities (i.e.,* $u_{1,t}(X)$ *for each* $t \in \Theta$ *and* $X \in \Psi$*) are known only to the defender.*

For each player a mixed strategy s_i is a probability distribution over his set of pure strategies. The differences between the security game of SDSRA and the traditional security game are: (i) an attacker and a defender actually take their actions simultaneously; (ii) a defender's payoff value for each pure strategy profile is unknown by an attacker; (iii) an attacker is unlikely to know the defender's probability distribution over potential attacker types (motivations). The first difference is the reason that solution concepts for Stackelberg games are not applicable, while the second and the third differences are the reasons that the Bayes-Nash equilibrium is not applicable. As a result, we introduce a new solution concept, called the *principle of acceptable costs of minimax regret*, which exploits two factors in decision making under uncertainty: loss-aversion and regret[3]. These factors have been identified in the literature and have been observed in psychological experiments [6, 12]. Similar to the idea of the rationalizability in the Nash equilibrium [9], we provide three constraints on players for our solution concept: **A1:** Each player considers the influence of loss-aversion (i.e., people's tendency to strongly prefer ensuring a sufficient minimum payoff rather than seeking potential maximum utility in decision making). **A2:** Each player minimizes their maximum regret based on their attitude towards loss-aversion and the strategic choices of others. **A3:** The attacker's payoffs matrix is known by the defender and each player knows his own payoff matrix.

Consider assumption **A1** first. This idea of loss-aversion has been discussed extensively in the literature. An example in [12] is, perhaps, the most well-known. Consider the game in Table 1, where player 1 is the row player and player 2 is the column player. Clearly, in this game, the payoffs for the unique Nash equilibrium $((\frac{3}{4}A, \frac{1}{4}B), (\frac{1}{2}A, \frac{1}{2}B))$ for each player can be guaranteed by their maximin strategy, i.e., $(\frac{1}{2}A, \frac{1}{2}B)$ for player 1 and $(\frac{1}{4}A, \frac{3}{4}B)$ for player 2. In the literature [3, 12], many have argued over what strategy should be selected

[2] While surveillance information can be represented by some imprecise probability theories [7], due to space restrictions, in this paper we focus on probability theory.

[3] Regret is an emotion associated with decisions which yield undesirable outcomes.

Table 1. Aumann and Maschler Game

	A	B
A	1,0	0,1
B	0,3	1,0

by each player: Nash equilibrium or maximin strategies? Some researchers, such as Harsanyi [3], have further argued that the players should indeed choose their maximin strategies, since the Nash equilibrium means a player would risk losing their maximin value without gaining a higher expected utility.

For Assumption **A2**, it means in our games players will minimize their maximum regret based on a threshold, rather that maximize their expect utility based on the correct subjective beliefs about another player's strategy. In fact, many behavioral studies (e.g., [1]) show that human decisions under uncertainty are strongly influenced by the emotion of regret. The *minimax regret* principle suggested in [13] says that a choice is admissible if this choice minimizes the maximum difference between the outcome of a choice and the best outcome that could have been obtained in a given state.

Finally, assumption **A3** is accepted by solution concepts in the Stackelberg game framework [14]. Such an assumption is more realistic than the Nash equilibrium concept when applied to real-world applications, since this concept assumes that all player strategies and all player payoffs are common knowledge. Hence, according to these assumptions, our solution concept should satisfy:

A player is willing to select a strategy with a lower maximum regret, after considering whether the minimum expected payoff of such a strategy is an acceptable reduction of their maximin expected payoff.

Actually, this principle has two advantages. Firstly, it avoids the overly pessimistic (worst case) approach of the maximin strategy. For example, suppose a lottery sells tickets for \$1 with a 99% chance of winning \$5000, then the maximin strategy would reject the offer. Clearly this violates our intuition. In our principle, however, if losing \$1 is acceptable to a player then this risk will be tolerated. Secondly, it avoids the potential for unaffordable losses resulting from the minimax regret strategy. For example, suppose a lottery sells tickets for \$1000 with a 1% chance of winning \$5000, then the minimax regret strategy would always accept the offer. Clearly this violates our intuition also. In our principle, a player will consider whether \$1000 is an acceptable loss and may or may not accept the offer. These advantages are useful in real-world security applications, since some losses are unaffordable (e.g., people's lives) while an overly pessimistic approach may mean that a player loses the chance to act.

3 Solution Concept for SDSRA Problem

First, we consider the prediction of the attacker's strategy. Formally, we have:

Definition 2 *Let* $S_2 = \{s_2^1, \ldots, s_2^m, \ldots\}$ *be a set of mixed strategies for the attacker, which each mixed strategy is a probability distribution over* A_2. $\sigma_{2,t} \in [0, 1]$ *is the threshold of acceptable cost which an attacker of type* t *can tolerate*

and $a_t \in A_1$ is a pure strategy of a defender. Then the optimal strategy for the attacker of type t, denoted as $s^*_{2,t} \in S_2$, is given by:

$$s^*_{2,t}=\text{argmin}\{\overline{r}(s^i_2)\,|\,\overline{r}(s^i_2)=\max_{a_h}\{\max_{j\neq i} u_{2,t}(a_h, s^j_2)-u_{2,t}(a_h, s^i_2)\}\}, \tag{1}$$

where

$$\min_{a_s} u_{2,t}(a_s, s^i_2) \geq \max_{s^k_2}\min_{a_r} u_{2,t}(a_r, s^k_2) - \varsigma_{a,t}, \tag{2}$$

$$\varsigma_{a,t} = \sigma_{2,t}(\max_{s^k_2}\min_{a_r} u_{2,t}(a_r, s^k_2) - \min_{s^l_2}\min_{a_w} u_{2,t}(a_w, s^l_2)). \tag{3}$$

Eq. 1 in Def. 2 means that an attacker will select, as their optimal strategy, a mixed strategy which can minimize their maximum regret. Hence, Eq. 2 limits the acceptable cost for a given attacker when adopting the minimax regret strategy. That is, the minimum expected utility of the strategy should be higher than an acceptable reduction of the maximin value. Eq. 2 shows how to calculate the acceptable reduction, where $\varsigma_{a,t}$ denotes the maximum loss that a type t attacker might pay in a SDSRA security game. Moreover, $\sigma_{2,t}$ in Eq. 3 is determined by an attacker's type. That is, some attackers will accept a choice with a lower minimum utility in order to reduce the maximum regret, while some attacker will refuse a high loss of their minimum utility. In short, the higher the value of $\sigma_{2,t}$, the higher the tolerance for loss of the minimum utility. In real-world applications, $\sigma_{2,t}$ can be obtained for each type of attacker from historical data or from criminology experts. Clearly, different types of attackers will have different attitudes for loss of the minimum utility. For example, a politically motivated terrorist usually shows higher tolerance for loss of the minimum utility than a robber, who is normally more concerned about their own safety.

Now, we consider how to find an optimal strategy for the defender based on the optimal mixed strategy $s^*_{2,t}$ for each type of attacker and the probability distribution over the attacker's possible types. In contrast to traditional security games, in real-time surveillance systems a defender needs to decide how to act in order to prevent further actions from the attacker. As a result, since only one pure strategy will be adopted by one security resource of the defender, we only need to consider the minimax regret with respect to pure strategies. Thus, using the same idea as our principle of acceptable costs of minimax regret, we can select the optimal strategy for the defender by:

Definition 3 *Let $a_i \in A_1$ be a defender's pure strategy, Θ be the set of possible types of an attacker, $p(t)$ be the probability value of attacker type t, $\sigma_1 \in [0, 1]$ be the threshold of acceptable cost that a defender can tolerate, and $s^*_{2,t}$ be the optimal mixed strategy for each type of attacker. Then the defender's optimal strategy, denoted as a^*, is given by:*

$$a^*_1 = \arg\max\{EU(a_i) \mid EU(a_i) = \sum_{t\in\Theta} p(t)u_{1,t}(a_i, s^*_{2,t})\}, \tag{4}$$

where

$$\min_{a_{2,t}} \sum_{t\in\Theta} p(t)u_{1,t}(a_i, a_{2,t}) \geq \max_{a_h}\min_{a_{2,t}} \sum_{t\in\Theta} p(t)u_{1,t}(a_h, a_{2,t}) - \varsigma_d, \tag{5}$$

$$\varsigma_d = \sigma_1(\max_{a_h}\min_{a_{2,t}} \sum_{t\in\Theta} p(t)u_{1,t}(a_h, a_{2,t}) - \min_{a_l}\min_{a_{2,t}} \sum_{t\in\Theta} p(t)u_{1,t}(a_l, a_{2,t})). \tag{6}$$

The reason we adopt the same formula as the maximum expected utility in Eq. (4) is that the defender already knows the attacker's optimal mixed strategy $s^*_{2,t}$ and the probability distribution over the attacker's possible types. As a result, according to Assumption 2 and Def. 2, the minimax regret strategy is the same as the maximum expected utility strategy for the defender. Moreover, since the attacker's strategy is based on a judgement of the attacker's payoff matrix, the threshold of acceptable cost assumption for each type of attacker, and imperfect information obtained by surveillance system, there is a chance that the attacker may play a different strategy than the strategy predicted by the defender. Thus, Eq. (5) and (6) together guarantee the minimum expected utility for a given pure strategy is acceptable for the defender.

In fact, a security manager can fine-tune the value of σ_1 to reflect different (real-time) situations for different applications. In this way, our method is more flexible in balancing the possibility of unaffordable losses caused by the failure of prevention and the expected payoff for successfully preventing an attack.

4 Properties and Linear Programming

Since the correctness of the defender's optimal strategy in our method is based on a prediction of the attacker's strategy, we consider properties of Def. 2 to justify the attacker's strategy prediction method. Moreover, given these properties, the whole process in our solution concept can be interpreted as an optimization problem for which there exists efficient methods of computation.

Theorem 1 *The maximin strategy of an attacker for our SDSRA security game is an unique equalizer*[4]*.*

Proof. Suppose $A_1 = \{a_1, \ldots .a_n\}$ is the set of defender's pure strategies; $\{q_1, \ldots, q_n\}$ is a set of probability values over the set of attacker's pure strategy $A_2 = \{b_1, \ldots, b_n\}$. By the definition of an equalizer, our game has a unique equalizer if and only if for linear equations $Aq = u$, where

$$A = \begin{bmatrix} u_2(a_1,b_1) & \cdots & u_2(a_1,b_n) \\ \vdots & \ddots & \vdots \\ u_2(a_n,b_1) & \cdots & u_2(a_n,b_n) \\ 1 & \cdots & 1 \end{bmatrix}, q = \begin{bmatrix} q_1 \\ \vdots \\ q_n \end{bmatrix}, u = \begin{bmatrix} c \\ \vdots \\ c \\ 1 \end{bmatrix},$$

there exists a unique solution q. Thus, $rank(A) = n$. In other word, it requires: (i) no convex combination of some rows in A dominating convex combinations of other rows; (ii) the payoff matrix satisfies $|A_1| = |A_2| = n$. Since there does not exist any dominated strategy for the attacker, item (i) holds in our game. Hence, since the defender and attacker share the same set of targets, item (ii) also holds in our game. □

[4] Formally, in a two-player game, a probability distribution p for the pure strategies of a given player i ($A_i = \{a_1, \ldots, a_n\}$) is an equalizer if and only if there exists $c \in \Re$ ($\Re$ is the set of real numbers) and any pure strategy b_j for their opponent, s.t. the following equation holds $\Sigma_{t=1}^{n} p(a_t) u_i(a_t, b_j) = c$.

This theorem reveals that an attacker can always find a unique strategy that guarantees their expected payoff regardless of any mixed strategy of the defender.

Theorem 2 *In a SDSRA security game, the expected payoff of the maximin strategy will not be less than a completely mixed Bayes-Nash equilibrium.*

Proof. Since in a completely mixed bimatrix game, each player can guarantee the expected payoff from a completely mixed equilibrium by playing a maximin strategy if and only if such a strategy is an equalizer [12]. By Theorem 1, and the fact that a Bayesian game in which the type space is finite can be redefined as a normal form game in which the strategy space is finite dimensional [9], this result can be obtained directly. □

Since our games satisfy that no pure or mixed strategy of an attacker or defender is strictly or weakly dominated by a convex combination of their other strategies, Theorem 2 shows that in many cases, an attacker can guarantee that their expected payoff is not less than the completely mixed Bayes-Nash equilibrium by selecting a maximin strategy.

Theorem 3 *Suppose a_h is a pure strategy for the defender, b_k is a pure strategy for the attacker, then the maximin regret $\overline{r}_t(s_2^i)$ for the attacker's (of type t) strategy s_2^i in a SDSRA security game can also be obtained as follows:*

$$\overline{r}_t(s_2^i)=\max_{a_h}\{\max_{b_k} u_{2,t}(a_h,b_k)-u_{2,t}(a_h,s_2^i)\}$$

Proof. Given the linearity of payoff functions and the fact that there does not exist any dominated strategy for the attacker, we obtain this result directly. □

This Theorem means that we only need to consider the pure strategy of the attacker when considering the maximin regret strategy of the attacker.

Theorem 4 *Suppose a_h is a defender's pure strategy, b_k is an attacker's pure strategy, and the payoff value of successfully attacking each target is the same for an attacker with a given type t ($u_{2,t}(a_i,b_j)=u_{2,t}(a_s,b_r),\ i\neq j,\ s\neq r$), then the minimax regret strategy is the same as the maximin strategy for the attacker.*

Proof. Suppose the maximin strategy for an attacker of a given type t is $\overline{s}_2$. By Theorem 1, for any defender's pure strategies a_i and a_s, we have $u_{2,t}(a_i,\overline{s}_2)=u_{2,t}(a_s,\overline{s}_2)$. Then, by Theorem 3 and $u_{2,t}(a_i,b_j)=u_{2,t}(a_s,b_r)>u_{2,t}(a_k,b_l)$, for any $i\neq j$, $s\neq r$, $k=l$,[5] we have

$$\overline{r}_t(\overline{s}_2)=u_{2,t}(a_h,b_k)-u_{2,t}(a_h,\overline{s}_2),\ \ for\ any\ h\neq k.$$

Suppose there exists a minimax regret strategy $s_2^*\neq\overline{s}_2$, then we have $\overline{r}_t(s_2^*)\leq\overline{r}_t(\overline{s}_2)$. Given the uniqueness of the equalizer (Theorem 1) and $u_2(a_i,b_j)=u_2(a_s,b_r)$, $i\neq j,\ s\neq r$, we have $\overline{r}_t(s_2^*)\neq\overline{r}_t(\overline{s}_2)$. Moreover, by $\overline{r}_t(s_2^*)<\overline{r}_t(\overline{s}_2)$, for

[5] $k=l$ means that both players select the same target (i.e., the attacker loses), while $i\neq j$ and $s\neq r$ mean that players select different targets (i.e., the attacker wins).

a given defender's pure strategy a_i, we have $u_{2,t}(a_i, b_k) - u_{2,t}(a_h, s_2^*) < u_{2,t}(a_i, b_k) - u_{2,t}(a_i, \overline{s}_2),\ i \neq k$. Then, we have $u_{2,t}(a_h, s_2^*) > u_{2,t}(a_i, \overline{s}_2)$. Since $\overline{s}_2$ is a maximin strategy, there exists a pure strategy a_s, such that $u_{2,t}(a_s, s_2^*) < u_{2,t}(a_s, \overline{s}_2)$. So, we have $u_{2,t}(a_s, b_k) - u_{2,t}(a_s, s_2^*) > u_{2,t}(a_s, b_k) - u_{2,t}(a_s, \overline{s}_2),\ s \neq k$. It violates our assumption that $\overline{r}_t(s_2^*) \leq \overline{r}_t(\overline{s}_2)$. So, $s_2^* = \overline{s}_2$. □

Theorem 3 demonstrates that if the payoff value of successfully attacking each target is the same for an attacker with a given type, then he can choose their maximin strategy to guarantee their minimum payoff value as well as to reduce their maximum regret in our games. Also, the relationship between Def. 2 and the decision rule of minimax regret [13], as well as that of Γ-maximin [9] is as follows:

Theorem 5 *Let $\sigma_{2,t} \in [0, 1]$ be the threshold of acceptable cost that an attacker of type t can tolerate, and $s_{2,t}^*$ be the optimal strategy for attacker type t, according to the principle of acceptable costs of maximum regret:*

(i) if $\sigma_{2,t} = 1$, then $s_{2,t}^*$ is also an optimal choice according to the rule of minimax regret; and

(ii) if $\sigma_{2,t} = 0$, then $s_{2,t}^*$ is also an optimal choice according to the rule of Γ-maximin.

Proof. (i) From Eq. (2) and (3) and the fact $\sigma_{2,t} = 1$, a mixed strategy s_2^i can be any element in the set of mixed strategies S_2. Then, from Eq. (1), $s_{2,t}^*$ is also an optimal choice according to the rule of minimax regret. (ii) From Eq. (1), (2), and (3), with $\sigma_{2,t} = 0$, $s_{2,t}^*$ can only be an element with the maximin utility in the set of mixed strategies $S_{2,t}$. Thus, $s_{2,t}^*$ is also an optimal choice according to the Γ-maximin rule. □

Actually, given Def. 2 and 3 as well as Theorems 1 and 3, the whole process of finding a defender's optimal strategy based on the strategy selected by each possible type of attacker can be solved by two Linear Programs as follows[6]:

$$
\begin{aligned}
\min_{\{q_j^t\}} \quad & \overline{r}_{2,t}(\{q_j^t\}) \\
\text{s.t.} \quad & \overline{r}_{2,t}(\{q_j^t\}) \geq (u_{2,t}(a_h, b_k) - \sum_{i=1}^{n} q_j^t u_{2,t}(a_h, b_j))(\forall a_h, \forall b_k) \\
& \sum_{j=1}^{n} q_j^t u_{2,t}(a_h, b_j) \geq (1 - \sigma_{2,t}) C_{2,t} + \sigma_{2,t} V_{2,t} \qquad (\forall a_h) \\
& C_{2,t} = \sum_{l=1}^{n} \overline{q}_l^t u_{2,t}(a_s, b_k) \qquad (a_s \in A_1) \\
& V_{2,t} = \min\{u_{2,t}(a_h, b_k)\} \qquad (\forall a_h, \forall b_k) \\
& \sum_{j=1}^{n} q_j^t = 1, q_j^t \in [0, 1]
\end{aligned}
$$

[6] Since a defender may have multiple available security resources, our Linear Programs will also consider this situation based on Def. 3

$$\max_{\{x_i\}} \quad \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{t\in\Theta} p(t)x_i u_{1,t}(a_i,b_j)q_j^t$$

$$\text{s.t.} \quad \sum_{i=1}^{n}\sum_{t\in\Theta} p(t)x_i u_{1,t}(a_i,b_j) \geq (1-\sigma_1)C_1 + \sigma_1 V_1$$

$$C_1 = \max\{\sum_{t\in\Theta} p(t)u_{1,t}(a_i,b_j)\}$$

$$V_1 = \min\{\sum_{t\in\Theta} p(t)u_{1,t}(a_i,b_j)\}$$

$$\sum_{i=1}^{n} x_i^* = k, x_i^* \in \{0,1\}$$

The first LP aims to find the mixed strategy selected by each possible type of attacker $\{q_t^j\}$ based on our principle while the second LP aims to find the defender's optimal strategy $\{x_i\}$. For the first LP, the objective function and the first constraint represent Eq. 1, the second, third and fourth constraints represent Eq. 2 and 3 (where $\{\overline{q}_1^t, \ldots, \overline{q}_n^t\}$ is the probability distribution for a type t attacker's unique equalizer strategy), the fifth constraint limits the set $\{q_j^t\}$ as a probability distribution over the set of actions A_2. For the second LP, the objective function represents Eq. 4, the first, second and third constraints represent Eq. 5 and 6, and the fourth constraint limits the strategies selected by a defender being a pure distribution over A_1 (that is, $p_i = 1$ or $p_i = 0$) and the amount of available security resources.

5 Conclusion

Related Work: Recently, security games have received increasing attention when aiming to solve security resource allocation problems [14]. Much of the work deals with this problem within the Stackelberg game framework [5, 8, 10]. That is, a defender commits to a strategy first and an attacker chooses their strategy based on the defender's commitment. The typical solution concept is the Strong Stackelberg Equilibrium, which assumes that an attacker will always break ties in favor of a defender in the case of indifference [5]. However, it is not always intuitive in real-world applications: how can an attacker observe the defender's strategy in a real-time, interactive environment? Thus, our work provides a more reasonable solution concept based on the principle of acceptable costs of minimax regret. On the other hand, in recent years there has been an increase in the deployment of intelligent surveillance systems, largely in response to the high demand for identifying and preventing threats for public safety, e.g., suspect object tracking [2] and anti-social behavior analysis [7]. However, to the best of our knowledge, little work of this kind focuses on how to allocate security resources to prevent possible attacks based on incomplete information in a surveillance system.

Conclusion: This paper proposed a new solution concept to handle SD-SRA security games based on the principle of acceptable costs of minimax regret. Firstly, we discussed the rationalizability assumptions of our principle: loss-aversion, minimax regret, and knowledge of the payoff matrix. Then, based on this principle, we proposed a method to predict the attacker's strategy and to determine the optimal strategy for the defender. Finally, we validated our method with some properties and provided a Linear Program for our solution concept.

References

1. H. F. Chua, R. Gonzalez, S. F. Taylor, R. C. Welsh, and I. Liberzon. Decision-related loss: Regret and disappointment. *NeuroImage*, 47(4):2031–2040, 2009.
2. S. Gong, C. Loy, and T. Xiang. Security and surveillance. In *Visual Analysis of Humans*, pages 455–472. Springer London, 2011.
3. J. C. Harsanyi. *Rational behaviour and bargaining equilibrium in games and social situations*. CUP Archive, 1986.
4. C. Kiekintveld and V. Kreinovich. Efficient approximation for security games with interval uncertainty. In *Proceedings of the AAAI Spring Symposium on Game Theory for Security, Sustainability, and Health GTSSH*, 2012.
5. D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe. Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. *Journal of Artificial Intelligence Research*, 41(2):297–327, 2011.
6. C. M. Kuhnen and B. Knutson. The neural basis of financial risk taking. *Neuron*, 47(5):763–770, 2005.
7. J. Ma, W. Liu, and P. C. Miller. Event modelling and reasoning with uncertain information for distributed sensor networks. In *Scalable Uncertainty Management - 4th International Conference, SUM 2010, Toulouse, France, September 27-29, 2010. Proceedings*, pages 236–249, 2010.
8. W. Ma, X. Luo, and W. Liu. An ambiguity aversion framework of security games under ambiguities. In *IJCAI 2013*, pages 271–278, 2013.
9. M. J. Osborne. *An introduction to game theory*. Oxford University Press New York, 2004.
10. J. Pita, M. Jain, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus. Using game theory for Los Angeles airport security. *AI Magazine*, 30(1):43–57, 2009.
11. J. Pita, M. Jain, M. Tambe, F. Ordóñez, and S. Kraus. Robust solutions to stackelberg games: Addressing bounded rationality and limited observations in human cognition. *Artificial Intelligence*, 174(15):1142–1171, 2010.
12. V. Pruzhansky. Some interesting properties of maximin strategies. *International Journal of Game Theory*, 40(2):351–365, 2011.
13. L. J. Savage. The theory of statistical decision. *J. of the Amer. Stat. Asso.*, 46(253):54–67, 1951.
14. M. Tambe. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*. Cambridge University Press, Cambridge, 2011.
15. S. Wasserkrug, A. Gal, and O. Etzion. Inference of security hazards from event composition based on incomplete or uncertain information. *Knowledge and Data Engineering, IEEE Transactions on*, 20(8):1111–1114, 2008.