Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnline CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 52-20 (2019) 351–356

On Security Games with Additive Utility ⋆

Hamid Emadi * **Sourabh Bhattacharya** **

* *Department of Mechanical Engineering, Iowa State University, Ames, IA 50010 USA (e-mail: emadi@iastate,edu).*
** *Department of Mechanical Engineering and Department of Computer Science Iowa State University, Ames, IA 50010 USA (e-mail: sbhattac@iastate.edu).*

Abstract: In this work, we investigate a security game between an attacker and a defender. We formulate a zero-sum game in which the payoff matrix has a special structure which results from the *additive property* of the utility function. The combinatorial nature of security games leads to a large cost matrix. We present structural properties of the optimal attacker strategy. Based on the structural properties, we propose a polynomial-time algorithm to compute the value of the large-scale zero-sum game.

Keywords: Security Game, Zero-Sum Game, Nash Equilibrium, Computational Complexity.

1. INTRODUCTION

Security of networks has become ubiquitous in modern large networking infrastructures. There has been a significant improvement in the efficiency and reliability of systems due to enhanced interconnection of intelligent devices. However, this has opened the door for strategic adversaries to exploit the vulnerabilities of the network and cause damage. This gives rise to important questions regarding the security of the network, for example, what are the potential threats to the network, or what are the cost-efficient defense strategies. In this work, we investigate an asset protection game between an adversary and a network provider.

In order to minimize the impact of a malicious attack on a large-scale system, resources need to be efficiently allocated to protect "high-value" targets. Since attackers can exploit the vulnerabilities of the network to launch a high-impact low-frequency attack, it is necessary to examine the security of the network from a mathematical perspective in order to obtain optimal defense strategies. Game theory (Basar and Olsder (1999)) is a useful tool to model adversarial scenarios. *Security games* model attack scenarios wherein an attacker attacks a number of targets while the defender allocates its resources to protect them to minimize the impact. The payoff for the attacker and the defender is based on the successfully attacked and protected targets, respectively. Traditionally, attacker-defender games have been modeled as zero-sum games, and the resulting saddle-point strategies are assumed to be optimal for both players.

The combinatorial nature of a security games renders the problem of obtaining optimal strategies for the players computationally infeasible. Kiekintveld et al. (2009) proposed an algorithm for randomized security resource allocation by introducing a compact representation for Stackelberg security game with multiple resources based on a mixed-integer programming formulation. They consider an attacker that attacks one target, and a defender that has multiple resources to defend the targets. Bhattacharya et al. (2011) propose an approximation algorithm to compute Stackelberg strategy for a security game in which the defender tries to minimize the total cost of the resources. Korzhyk et al. (2011c) show that under a natural restriction on security games (subsets of defense sets are defense sets), any Stackelberg strategy is also a Nash equilibrium strategy. Brown et al. (2012) consider a security game with multiple attackers, and provide approximate algorithms to compute optimal solutions.

Although, Stackelberg models have been used in real world applications (Pita et al. (2008), Jain et al. (2010)), one of their major drawbacks is the fact that the defender cannot be sure that the attacker is aware of the defender's mixed strategy before his/her decision. Yin et al. (2010) and Korzhyk et al. (2011b) model the uncertainty of the attacker's knowledge about the defender's mixed strategy as part of the game, and propose an iterative algorithm based on alternating between Nash equilibrium solver and a Stackelberg solver. Another remedy for Strong Stackelberg solutions is proposed by Guo et al. (2018) which introduces the solution concept of the inducible Stackelberg equilibrium to avoid overoptimism. In the past, there has been some work to connect equilibrium computation in security games to combinatorial optimization. Xu (2016) and Wang and Shroff (2017) reduced the security game to a combinatorial optimization problem which can be characterized by a set consisting of the defenders pure strategies. Moreover, their framework captures most of the characteristics of the security game models.

In the past decade, there has been extensive research on the complexity of computing the equilibrium of security games due to their combinatorial nature. Korzhyk et al. (2010) show that computing the optimal Stackelberg strategy in security resource allocation game, when attacker

⋆ This work was supported in part by NSF CPS grant ECCS 1739969.

10.1016/j.ifacol.2019.12.180

attacks one target, is NP-hard in general. However, when resources are homogeneous and cardinality of protection set is at most 2, polynomial-time algorithms have been proposed by the authors. Korzhyk et al. (2010) propose an LP formulation similar to Kiekintveld's formulation, and present a technique to compute the mixed strategies in polynomial time. In the presence of multiple attackers with limited resources, solving the security game becomes significantly more challenging. Korzhyk et al. (2011a) propose a polynomial-time algorithm for computing Nash equilibrium in security games modeled as a non-zero game with multiple attacker resources. Our work lies in a similar vein. In contrast to the iterative procedure proposed in Korzhyk et al. (2011a), we derive structural properties of the optimal solution to arrive at a polynomial-time algorithm to compute the value of a zero-sum security game.

In this work, we assume that the utility function has an *additive property* i.e., the total utility of successfully attacking multiple targets is equal to the sum of utilities of the individual targets. In several practical problems, it is possible to approximate the utility function with an additive utility function (Soltan et al. (2018), Korzhyk et al. (2011c)). However, one may also consider non-additive utility functions to capture the interdependency between targets. Wang and Shroff (2017) and Wang et al. (2017) examine the security game with non-additive utilities and multiple targets. They use the framework proposed by Xu (2016) which shows that a security game is equivalent to a combinatorial optimization problem over the pure strategies of the defender. They prove that computing optimal strategies is NP-hard in general, and under some constraints they propose polynomial-time algorithms.

In this work, we address a security game between resource-constrained players in which the utility function has an additive property. In Section 2, we present the problem formulation. In Section 3, we present structural properties of the optimal attacker strategy. In Section 4, we present a polynomial-time algorithm to compute the value of a large-scale zero-sum game. In Section 5, we present our conclusions along with some future work.

2. PROBLEM FORMULATION: SECURITY GAME

Consider a two-person zero-sum game on a graph $G(\nu, \epsilon)$ containing n vertices and m links, where $\nu = \{1, \ldots, n\}$ and $\epsilon = \{1, \ldots, m\}$ are the vertex set and the edge set, respectively. We assume an attacker (player 1) chooses k_a-links to attack. So, there are $n_a = \binom{m}{k_a}$ actions for player 1. On the other hand, protection budget of links is limited, and we assume that only k_d links will be protected by the defender. So, there are $n_d = \binom{m}{k_d}$ actions for player 2. The defender (Player 2) has no knowledge about the links chosen by player 1. In order to find the optimal strategy for the players, we formulate a strategic security game $(\mathcal{X}, \mathcal{Y}, A)$, where $\mathcal{X}$ and $\mathcal{Y}$ denote the action sets for attacker and defender, respectively, and $\text{card}(\mathcal{X}) = n_a, \text{card}(\mathcal{Y}) = n_d$. Every element of $\mathcal{X}$, denoted by x_i, is defined as the attacked links. Similarly, $y_i \in \mathcal{Y}$ is defined as the protected links. Let $\mathcal{I} = \{1, \ldots m\}$. Each $x_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$ is a k_a-tuple, and k_d-tuple subset of $\mathcal{I}$, respectively. The attacker has no information about the links that are protected by the defender. Let ϕ_i denote the cost associated to link i, and each link is labeled such that

$$\phi_i \geq \phi_j \quad \text{for} \quad i > j.$$

We consider an additive property for the utility function i.e., entries of the cost matrix A are defined as follows:

$$a_{ij} = \sum_{\{l | l \in x_i \cap y_j^c\}} \phi_l. \tag{1}$$

A represents the game matrix or payoff matrix for player 1. Since we consider a zero-sum game, the payoff matrix for player 2 is $-A$.

Let p, q be the probability vectors representing the mixed strategies for player 1 and player 2, respectively. The expected utility function is

$$v = p^T A q.$$

According to the minimax theorem, every finite two-person zero-sum game has a saddle point with the value, v^*, in mixed strategy $p^* = \left[p_1^*, \ldots, p_{n_a}^*\right]^T$ for player 1, and mixed strategy $q^* = \left[q_1^*, \ldots, q_{n_d}^*\right]^T$ for player 2, such that player 1's average gain is at least v^* no matter what player 2 does. And player 2's average loss is at most v^* regardless of player 1's strategy, that is

$$p^T A q^* \leq {p^*}^T A q^* \leq {p^*}^T A q.$$

In the next section, we present an algorithm to compute v^* which is polynomial in m, k_a and k_d.

3. STRUCTURAL PROPERTIES OF THE OPTIMAL SOLUTION

Since v^* denote the value of the game, the following holds:

$$v^* = \max_p \min_{1 \leq i \leq n_d} (p^T A)_i = \min_q \max_{1 \leq j \leq n_a} (Aq)_j$$

Let $(p^T A)_i$ denote the i^{th} element of $p^T A$. From (1), $(p^T A)_i$ can be written in the following form,

$$(p^T A)_i = \sum_{j=1}^{n_d} p_j a_{ji} = \sum_{j=1}^{n_d} p_j \sum_{l \in x_j \cap {y_i}^c} \phi_l = \sum_{j \in y_i^c} \alpha_j \phi_j,$$

where,

$$\alpha_j = \sum_{\{i | j \in x_i\}} p_i. \tag{2}$$

Note that $(p^T A)_i \geq v^*, \forall i$, and minimum value of $(p^T A)_i$ is v^*. We say $p_l \in \alpha_j$ when p_l is present in the R.H.S of (2) (i.e. $j \in x_l$).

Lemma 1. Let $\Gamma = \{\alpha_{i_1}, \ldots, \alpha_{i_{k_a}}\}$ be an arbitrary set of α_i's with cardinality k_a.

(1) $\exists p_c \quad \text{s.t.} \quad p_c \in \alpha_{i_1}, \ldots, \alpha_{i_{k_a}}$ and $p_c \notin \alpha_{i_{k_a+1}}, \ldots, \alpha_{i_m}$
(2) Given any $\alpha_r \notin \Gamma$, there exists $\alpha_j \in \Gamma$ such that p_i's can be perturbed to reduce α_r by $\delta > 0$, and increase α_j by δ without any change in α_i's for $i \in \mathcal{I} \setminus \{r, j\}$.

Proof. 1) We prove for the special case when $\Gamma = \{\alpha_1, \ldots, \alpha_{k_a}\}$. From (2), it is clear that p_1 is common in $\alpha_1, \ldots, \alpha_{k_a}$. Moreover, p_1 does not appear in $\alpha_{k_a+1}, \ldots, \alpha_m$ because none of $k_a+1, \ldots, m$ lie in x_1. For the general case, it is possible to relabel ϕ_i's such that $\Gamma = \{\alpha'_1, \ldots, \alpha'_{k_a}\} = \{\alpha_{i_1}, \ldots, \alpha_{i_{k_a}}\}$. Therefore, p'_1 lies in $\alpha'_1, \ldots, \alpha'_{k_a}$, and we can define $p_c = p'_1$.

2) In order to prove this claim, we assume that $p_c \in \alpha_r$. From part 1, there exists α_j, such that $p_c \notin \alpha_j$. From part 1, there exist p'_c such that $p'_c \in \alpha_j$, and p'_c belongs to all α_i's which contain p_c except α_r. So by reducing p_c by δ and increasing $p_{c'}$ by δ, we are able to reduce α_r and increase α_j without affecting other α_i's. □

Theorem 1. For $k_a + k_d \leq m$, the optimal solution p^* and v^* satisfy the following properties:

(1) $\alpha^*_i \phi_i \geq \alpha^*_j \phi_j$ for $i > j$,
(2) $v^* = \alpha^*_1 \phi_1 + \cdots + \alpha^*_{m-k_d} \phi_{m-k_d}$,
(3) $\alpha^*_i \phi_i = \alpha^*_j \phi_j \ \forall\ i, j \in \{m-k_d, \ldots, m\}$.

Proof. 1) We prove by contradiction. Assume that there exists i and j such that $\alpha_i \phi_i < \alpha_j \phi_j$ for $i > j$ for the optimal solution. Since $\phi_i \geq \phi_j$, $\alpha_j > \alpha_i$. From property 2 in Lemma 1, $p_d, p'_d > 0$ exist such that $p_d \in \alpha_j$ ($p_d \notin \alpha_i$) and $p'_d \in \alpha_i$ ($p'_d \notin \alpha_j$). We show that if p_d is decreased by δ, and p'_d is increased by δ, v^* either increases or remains constant. As a consequence, the first assumption is not correct, and we conclude that $\alpha_i \phi_i \geq \alpha_j \phi_j$. In order to show that v^* is not decreasing, we analyze an arbitrary $(p^T A)_r$. Since we know that $(p^T A)_r \geq v^*$, v^* can be decreased only when $(p^T A)_r$ is decreased for $(p^T A)_r = v^*$. If $(p^T A)_r$ contains both $\alpha_i \phi_i$ and $\alpha_j \phi_j$, the value of $(p^T A)_r$ is increased by reducing α_j and increasing α_i. If $(p^T A)_r$ only contains $\alpha_i \phi_i$, it will increase as well. If $(p^T A)_r$ contains only $\alpha_j \phi_j$, there exists another $(p^T A)_{r'}$ such that

$$(p^T A)_{r'} = (p^T A)_r - \alpha_j \phi_j + \alpha_i \phi_i. \tag{3}$$

Since we assumed that $\alpha_j \phi_j > \alpha_i \phi_i$, $(p^T A)_r > (p^T A)_{r'} \geq v^*$. Therefore, we can pick δ such that by reducing α_j, v^* is not reduced. The last case is when $(p^T A)_r$ does not contain $\alpha_i \phi_i, \alpha_j \phi_j$. In this case v^* is not affected. Hence the first property holds.

2) Since $v^* = \min_i (p^T A)_i$, and $(p^T A)_i$'s are constructed from all $m - k_d$ combinations of $\alpha_j \phi_j$ the second property holds.

3) We prove by contradiction. Assume that $\exists i \in \{m-k_d+1, \ldots, m\}$ such that $\alpha_i \phi_i > \alpha_{i-1} \phi_{i-1}$. Since $k_a + k_d \leq m$,there exists $\Gamma = \{\alpha_{i_1}, \ldots, \alpha_{i_{k_a}}\}$ such that $i_1, \ldots, i_{k_a} \leq m - k_d$, and from property 2 in lemma 1, there exists an $r \in \{1, \ldots, k_a\}$ such that we can reduce α_i and increase α_r without affecting the other α's which in turn increases the v^*. Since v^* is the value of the game, we reach a contradiction. Therefore, the assumption at the beginning cannot hold as a result of which the property holds. □

Corollary 1.1. If $k_a + k_d \leq m$, the optimal solution satisfies the following:

$$\alpha^*_m \phi_m = \cdots = \alpha^*_s \phi_s \geq \cdots \geq \alpha^*_{s-k_a+1} \phi_{s-k_a+1}, \quad s \in \{k_a, \ldots, m-k_d\}. \tag{4}$$

The proof of the above corollary follows from Theorem 1 and Lemma 1. From Lemma 1, we can conclude that any $\alpha_j \neq 0$ for $j = 1, \ldots, \alpha_{s-k_a}$ can be reduced to increase v^*. Therefore $\alpha^*_1 = \cdots = \alpha^*_{s-k_a} = 0$.

Let $\mathcal{U}_a$ and $\mathcal{U}_d$, called active sets of attacker and defender, denote the union of x_i's and y_i's corresponds to the support sets of p^* and q^*, respectively.

Corollary 1.2. In a security game $(\mathcal{X}, \mathcal{Y}, A)$, $\mathcal{U}_a = \{i, i+1, \ldots, m\}$, where $i \in \{1, \ldots, m-k_a\}$.

4. COMPUTATION OF THE VALUE

We consider the game from the attacker's perspective. For $\mathcal{U}_a = \{i, \ldots, m\}$, the following holds:

$$(p^{*T} A)_j > v^* \quad \forall j \quad \text{s.t.} \qquad x_j \cap \mathcal{U}_a = \emptyset.$$

Consequently,

$$q^*_j = 0 \quad \forall j \quad \text{s.t.} \qquad x_j \cap \mathcal{U}_a = \emptyset,$$

otherwise, $p^{*T} A q > v^*$. Hence, $\mathcal{U}_d \subseteq \mathcal{U}_a$.

According to Corollary 1.2, both players choose strategies that involve set of links with highest impacts (ϕ_i). We use this property to reduce the possible scenarios for the attacker by constructing an $(m-k_d) \times (m-k_d)$ matrix U such that its element $(i, i+r)$, denoted as $U_{i,i+r}$, is associated with the following condition:

$$\alpha_m \phi_m = \cdots = \alpha_s \phi_s > \alpha_{s-1} \phi_{s-1} \geq \cdots \geq \alpha_{s-r} \phi_{s-r}$$
$$s = m - k_d - i + 1 \tag{5}$$
$$r \in \{0, \ldots, k_a\}, i \in \{1, \ldots, m-k_d\}. \tag{6}$$

The above condition can be interpreted as $\mathcal{U}_a = \{s-r, s-r+1, \ldots, m\}$, and $\mathcal{U}_d = \{s, s+1, \ldots, m\}$ for cell $U_{i,i+r}$. Since $\mathcal{U}_d \subseteq \mathcal{U}_a$, we consider that $U_{i,j}$ is not a candidate for the solution of the security game, when $j < i$.

The following theorem relates v^* to elements of U.

Theorem 2. $v^* = \max\{U_{i,j}\}$. Elements of U are defined as follows:

- $U_{i,i} = \frac{k_a i}{c_i}$ when $c_i \phi_s \geq k_a$.
- $U_{i,i+r} = \sum_{l=s-r}^{s-1} \phi_l + \frac{(k_a - r) i}{c_i}$, when $c_i \phi_{s-r} > i$, and $c_i \phi_s \geq k_a - r > c_i \phi_{s-1}$
- $U_{i,i+r} = (k_a - r - c_{i-1} \phi_s) \phi_{s-r} + \sum_{l=s-r+1}^{s-1} \phi_l + i \phi_s$ when $c_i \phi_{s-r} \leq i$, and $c_i \phi_s \geq k_a - r > c_i \phi_s - 1$,
- Otherwise(i.e. when the above conditions are not satisfied), $U_{i,j}$ is not a candidate for the solution, and this entry is not considered in max.

where $c_i = \sum_{j=s}^{m} \frac{1}{\phi_j}$.

Proof. The diagonal element $U_{i,i}$ corresponds to the following case:

$$\alpha_m \phi_m = \cdots = \alpha_s \phi_s, \tag{7}$$
$$\alpha_j = 0 \quad \text{for} \qquad j \in \{1, \ldots, s-1\}$$

Substituting the above condition in the expression for v^* in Theorem 1, we obtain the following:

$$v = \sum_{l=s}^{m-k_d} \alpha_l \phi_l = i \alpha_j \phi_j \implies \alpha_j = \frac{v}{i \phi_j}, \quad j \in \{s, \ldots, m\}$$

From Lemma 1, every p_i is present in k_a α_i's. Since $\sum_{j=1}^{n_a} p_j = 1$, $\sum_{j=1}^{m} \alpha_j = k_a$. Substituting (8) into $\sum_{j=1}^{m} \alpha_j$, we obtain the following:

$$\sum_{j=s}^{m} \frac{v}{i\phi_j} = k_a \implies v = \frac{k_a i}{\sum_{j=s}^{m} \frac{1}{\phi_j}} \tag{8}$$

Let $c_i = \sum_{j=s}^{m} \frac{1}{\phi_j}$. Substituting v in (8) leads to the following:

$$\alpha_j = \begin{cases} \frac{k_a}{\phi_j c_i} & j \in \{s, \dots, m\} \\ 0 & j \in \{1, \dots, s-1\} \end{cases}$$

Since ϕ_j's are in ascending order, $\alpha_s \leq 1$ implies that $\alpha_j \leq 1$ for $j > s$. $\phi_s c_i < k_a$ implies that $\alpha_s > 1$ which contradicts the definition of α in (2). Hence, in this case the maximum value of α_s is 1. Therefore,

$$\alpha_j \phi_j c_i < k_a, \qquad \text{for} \qquad j = s, \dots, m,$$

which implies that $\sum_{l=1}^{m} \alpha_l = k_a$ cannot be satisfied. In other words, $U_{i,i}$ cannot be the optimal solution when $\phi_s c_i < k_a$, and this cell is not a candidate for the solution of the game. Hence we can put this entry equal to 0, when $c_i \phi_s < k_a$.

The off-diagonal entry $U_{i,i+r}$ corresponds to the following condition:

$$\alpha_m \phi_m = \dots = \alpha_s \phi_s > \alpha_{s-1}\phi_{s-1} \geq \dots \geq \alpha_{s-r}\phi_{s-r}$$

$$s = m - k_d - i + 1 \tag{9}$$

$$r \in \{1, \dots, k_a\}, i \in \{1, \dots, m - k_d - 1\}. \tag{10}$$

Substituting $\alpha_j \phi_j$'s from (5) in $v = \sum_{j=1}^{m-k_d} \alpha_j \phi_j$ leads to the following expression for v:

$$v = \sum_{l=s-r}^{s-1} \alpha_l \phi_l + i\alpha_j \phi_j \quad j \in \{s, \dots, m\}$$

$$\implies \alpha_j = \frac{v - \sum_{l=s-r}^{s-1} \alpha_l \phi_l}{i\phi_j} \quad j \in \{s, \dots, m\} \tag{11}$$

Since $\sum_{l=1}^{m} \alpha_l = k_a$, we obtain the following:

$$\sum_{l=s-r}^{s-1} \alpha_l + \sum_{l=s}^{m} \frac{v - \sum_{j=s-r}^{s-1} \alpha_j \phi_j}{i\phi_l} = k_a \tag{12}$$

$$\implies v = \sum_{l=s-r}^{s-1} \frac{(c_i \phi_l - i)}{c_i} \alpha_l + \frac{k_a i}{c_i}, \tag{13}$$

where $c_i = \sum_{j=s}^{m} \frac{1}{\phi_j}$. Next, we consider two cases based on the coefficients of α_l in the above expression.

First, we consider the case in which the coefficients of α_l are positive (i.e. $c_i \phi_{s-r} > i$). From (13), we can conclude that the maximum value of v occurs at the following values of α's:

$$\alpha_j = \begin{cases} 0 & j \in \{1, \dots, s-r-1\} \\ 1 & j \in \{s-r, \dots, s-1\} \\ \frac{k_a - r}{c_i \phi_j} & j \in \{s, \dots, m\} \end{cases} \tag{14}$$

If $\frac{k_a - r}{c_i \phi_s} \leq 1$, then entry of $U_{i,i+r}$ is a candidate for the solution of the security game. Substituting (14) in (13) leads to the following expression for v:

$$v = \sum_{l=s-r}^{s-1} \phi_l + \frac{(k_a - r)i}{c_i} \tag{15}$$

If $\frac{k_a - r}{c_i \phi_s} > 1$, the constraint of $\alpha_j \leq 1$ is violated, and consequently this cell of U cannot be the solution for the security game.

Next, we consider a case in which some coefficients of α_l in (13) are negative, and $\frac{k_a - r}{c_i \phi_s} > 1$. In this case, α_s should be modified, and the only case which can be a candidate for the solution of the game is

$$\alpha_j = \begin{cases} 0 & j \in \{1, \dots, s-r-1\} \\ \delta & j = s-r \\ 1 & j \in \{s-r+1, \dots, s\} \\ \frac{\phi_s}{\phi_j} & j \in \{s+1, \dots, m\}, \end{cases} \tag{16}$$

where $\delta = k_a - r - c_{i-1}\phi_s$, which is resulted from $\sum_{j=1}^{m} \alpha_j = k_a$. Since $0 < \delta \leq 1$, $k_a - r - c_{i-1}\phi_s > 0$, which is equivalent to $c_i \phi_s - 1 < k_a - r$.

Moreover, v can be computed from Theorem 1, second part, which is given by the following expression:

$$v = \delta \phi_{s-r} + i\phi_s + \sum_{l=s-r+1}^{s-1} \phi_l. \tag{17}$$

From definition of U, in $U_{i,i+r}$, the active sets are $\mathcal{U}_a = \{s-r, s-r+1, \dots, m\}$, and $\mathcal{U}_d = \{s, s+1, \dots, m\}$. Each column and row of U, corresponds to the attacker and defender's active set, respectively. □

Corollary 1.3. v^* can be computed in $\mathcal{O}((m - k_d)^2)$.

The above corollary can be concluded from the fact that U has $(m - k_d)^2$ entries. Algorithm 1 gives the value of the game and active links for the attacker and the defender.

Next, we show the feasibility of each cell of U i.e., there exists a p which satisfies the values of α in each cell of U obtained in the previous analysis. In other words, we show that in each cell of U that can be a candidate for the value of the game, there exists $p \geq 0, \sum_{j=1}^{N} p_j = 1$ such that $Mp = \alpha$, where $\alpha = [\alpha_1, \dots, \alpha_m]^T$ is obtained from the analysis in proof of Theorem 2. M is a matrix of dimension $\binom{m}{k} \times m$, and each column has k entries equal to 1 and rest of the entries equal to 0. In other words, M is a matrix constructed from $\binom{m}{k}$ combinations of k one in an m dimensional vector. We refer to M as a *combinatorial matrix*, and denote it as $M_{[m,k]}$.

Lemma 2. Let $\alpha = [\alpha_1, \dots, \alpha_m]^T$, and $\sum_{j=1}^{m} \alpha_j = k$, and $0 \leq \alpha_j \leq 1$. α lies in the convex-hull of columns of $M_{[m,k]}$. In other words, there exists $p \geq 0, \sum_{j=1}^{N} p_j = 1$, such that $Mp = \alpha$.

Proof. The proof is by induction. We assume that the lemma is true for $m' = m - 1$ and $k' = 1, \dots, k - 1$. Moreover, $M_{[m,k]}$ can be written as

$$M_{[m,k]} = \begin{bmatrix} \mathbf{1}^T & \mathbf{0}^T \\ M_{[m-1,k-1]} & M_{[m-1,k]} \end{bmatrix}. \tag{18}$$

By separating p into $\bar{p}_1$ and $\bar{p}_2$,

Algorithm 1 Computation of the value, and active links

Input: $\phi_1, \dots, \phi_m$ and k_a, k_d
Output: v^*,$\mathcal{U}_a$,$\mathcal{U}_d$
Construct U based on Theorem 2
for $i = 1 : m - k_d$ **do**
  if $c_i\phi_s \geq k_a$ **then**
    $U_{i,i} = \frac{k_a i}{c_i}$
  else
    $U_{i,i} = 0$
  end if
  for $r = 1 : k_a$ **do**
    if $c_i\phi_{s-r} > i$, and $c_i\phi_s \geq k_a - r > c_i\phi_{s-1}$ **then**
      $U_{i,i+r} = \sum_{l=s-r}^{s-1} \phi_l + \frac{(k_a - r)i}{c_i}$,
    else if $c_i\phi_{s-r} \leq i$, and $c_i\phi_s \geq k_a - r > c_i\phi_s - 1$ **then**
      $U_{i,i+r} = (k_a - r - c_{i-1}\phi_s)\phi_{s-r} + \sum_{l=s-r+1}^{s-1} \phi_l + i\phi_s$
    else
      $U_{i,i+r} = 0$
    end if
  end for
end for
$v^* \leftarrow \max U_{i,j}$
$(i^*, j^*) \leftarrow \arg\max U_{i,j}$
$\mathcal{U}_a \leftarrow \{m - k_d - j^* + 1, \dots, m\}$
$\mathcal{U}_d \leftarrow \{m - k_d - i^* + 1, \dots, m\}$

$$M_{[m,k]}p = \begin{bmatrix} \mathbf{1}^T & \mathbf{0}^T \\ M_{[m-1,k-1]} & M_{[m-1,k]} \end{bmatrix} \begin{bmatrix} \bar{p}_1 \\ \bar{p}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{1}^T\bar{p}_1 \\ M_{[m-1,k-1]}\bar{p}_1 + M_{[m-1,k]}\bar{p}_2 \end{bmatrix}. \quad (19)$$

Second entry of the above matrix can be written in the following form:

$$\alpha_1 M_{[m-1,k-1]}{p'}_1 + (1 - \alpha_1)M_{[m-1,k]}{p'}_2, \quad (20)$$

where, $\bar{p}_1 = \alpha_1{p'}_1, \bar{p}_2 = (1-\alpha_1){p'}_2$. Since we assumed that the lemma is true for $m' = m - 1$ and $k' = 1, \dots, k - 1$, there exists ${p'}_1$ and ${p'}_2$ in a simplex such that the following hold:

$$M_{[m-1,k-1]}{p'}_1 = \frac{k-1}{k - \alpha_1} \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix}, \quad (21)$$

$$M_{[m-1,k]}{p'}_2 = \frac{k}{k - \alpha_1} \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix}. \quad (22)$$

By substituting the above expressions in (19), we conclude that $M_{[m,k]}p = \alpha$, where p lies on a simplex. In other words, α lies in a convex-hull of columns of M. In order to complete the proof, we need to show that the lemma holds for arbitrary $M_{[k+1,k]}$ and $M_{[m,1]}$.

Note that $M_{[m,1]} = I_{m\times m}$. Therefore $p = \alpha$, and $\sum_{j=1}^m p_j = \sum_{j=1}^m \alpha_j = 1$. Next,

$$M_{[k+1,k]}p = (\mathbf{1}\mathbf{1}^T - I)p = \alpha \quad (23)$$

$$p = (\mathbf{1}\mathbf{1}^T - I)^{-1}\alpha = (\frac{\mathbf{1}\mathbf{1}^T}{k} - I)\alpha = \mathbf{1} - \alpha. \quad (24)$$

Consequently, lemma holds for base cases, which completes the proof. □

Finally, we consider the case when $k_a + k_d > m$. When $k > \frac{m}{2}$, the optimal solution satisfies the following:

$$\alpha_m\phi_m = \dots = \alpha_{k_a+1}\phi_{k_a+1} \geq \alpha_{k_a}\phi_{k_a} \geq \dots \geq \alpha_1\phi_1,$$

As in the case of $k_a + k_d \leq m$, we can construct a matrix U with i^{th} entry on the diagonal as follows:

$$\begin{aligned} &\alpha_m\phi_m = \dots = \alpha_s\phi_s, \\ &\alpha_j = 0, \qquad j \in \{1, \dots, s-1\} \\ &s = k_a - i + 2 \\ &i \in \{1, \dots, k_a + 1\}, \end{aligned} \quad (25)$$

Since $v = \sum_{j=1}^{m-k_d} \alpha_j\phi_j$,

$$v = 0 \qquad \text{for} \qquad i = 1, \dots, k_a + k_d - m + 1,$$

which implies that these cells cannot be a candidate for the value of the game. For $i \geq k_a + k_d - m + 2$, we obtain the following:

$$\alpha_j = \frac{k_a}{c_i\phi_j}, \quad v = \frac{k_a(i - k_a - k_d + m - 2)}{c_i}. \quad (26)$$

and off-diagonal entry $(i, i+r)$ corresponds to the following condition:

$$\begin{aligned} &\alpha_m\phi_m = \dots = \alpha_s\phi_s > \alpha_{s-1}\phi_{s-1} \geq \dots \geq \alpha_{s-r}\phi_{s-r}, \\ &s = k_a - i + 2 \\ &r \in \{1, \dots, k_a\}, i \in \{1, \dots, k_a\}. \end{aligned} \quad (27)$$

For $i \leq k_a + k_d - m + 1$, all entries corresponding to the first $k_a + k_d - m + 1$ columns are a candidate for the value of the game. For other off-diagonal elements, we have an analysis similar to the off-diagonal entries for $k_a + k_d \leq m$.

5. CONCLUSION

In this work, we investigated a security game. We formulated a zero sum-game in which the payoff matrix of the game has a special structure which results from the *additive property* of the utility function. We presented structural properties of the optimal attacker strategy. Based on the structural properties, we proposed a polynomial-time algorithm to compute the value of the large-scale zero-sum game.

There are several directions of future research. One direction is to use the proposed structural property to formulate a network design problem to minimize the impact of attacks. Another direction of future research is to generalize the results of this work to nonzero-sum games with different utility functions for attacker and defender. Finally, we plan to extend our analysis to games with non-additive utility functions by using perturbation analysis.

ACKNOWLEDGEMENTS

We acknowledge NSF CPS grant ECCS 1739969. We also thank Prof. Manimaran Govindarasu, Burhan Hyder and Srayashi Konar for useful discussions about this topic.

REFERENCES

Basar, T. and Olsder, G.J. (1999). *Dynamic noncooperative game theory*, volume 23. Siam.

Bhattacharya, S., Conitzer, V., and Munagala, K. (2011). Approximation algorithm for security games with costly resources. In *International Workshop on Internet and Network Economics*, 13–24. Springer.

Brown, M., An, B., Kiekintveld, C., Ordóñez, F., and Tambe, M. (2012). Multi-objective optimization for security games. In *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 2*, 863–870. International Foundation for Autonomous Agents and Multiagent Systems.

Guo, Q., Gan, J., Fang, F., Tran-Thanh, L., Tambe, M., and An, B. (2018). On the inducibility of stackelberg equilibrium for security games. *arXiv preprint arXiv:1811.03823*.

Jain, M., Tsai, J., Pita, J., Kiekintveld, C., Rathi, S., Tambe, M., and Ordónez, F. (2010). Software assistants for randomized patrol planning for the lax airport police and the federal air marshal service. *Interfaces*, 40(4), 267–290.

Kiekintveld, C., Jain, M., Tsai, J., Pita, J., Ordóñez, F., and Tambe, M. (2009). Computing optimal randomized resource allocations for massive security games. In *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1*, 689–696. International Foundation for Autonomous Agents and Multiagent Systems.

Korzhyk, D., Conitzer, V., and Parr, R. (2010). Complexity of computing optimal stackelberg strategies in security resource allocation games. In *Twenty-Fourth AAAI Conference on Artificial Intelligence*.

Korzhyk, D., Conitzer, V., and Parr, R. (2011a). Security games with multiple attacker resources. In *Twenty-Second International Joint Conference on Artificial Intelligence*.

Korzhyk, D., Conitzer, V., and Parr, R. (2011b). Solving stackelberg games with uncertain observability. In *The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 3*, 1013–1020. International Foundation for Autonomous Agents and Multiagent Systems.

Korzhyk, D., Yin, Z., Kiekintveld, C., Conitzer, V., and Tambe, M. (2011c). Stackelberg vs. nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. *Journal of Artificial Intelligence Research*, 41, 297–327.

Pita, J., Jain, M., Marecki, J., Ordóñez, F., Portway, C., Tambe, M., Western, C., Paruchuri, P., and Kraus, S. (2008). Deployed armor protection: the application of a game theoretic model for security at the los angeles international airport. In *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track*, 125–132. International Foundation for Autonomous Agents and Multiagent Systems.

Soltan, S., Loh, A., and Zussman, G. (2018). Analyzing and quantifying the effect of k-line failures in power grids. *IEEE Transactions on Control of Network Systems*, 5(3), 1424–1433.

Wang, S., Liu, F., and Shroff, N. (2017). Non-additive security games. In *Thirty-First AAAI Conference on Artificial Intelligence*.

Wang, S. and Shroff, N. (2017). Security game with non-additive utilities and multiple attacker resources. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 1(1), 13.

Xu, H. (2016). The mysteries of security games: Equilibrium computation becomes combinatorial algorithm design. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, 497–514. ACM.

Yin, Z., Korzhyk, D., Kiekintveld, C., Conitzer, V., and Tambe, M. (2010). Stackelberg vs. nash in security games: Interchangeability, equivalence, and uniqueness. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: volume 1-Volume 1*, 1139–1146. International Foundation for Autonomous Agents and Multiagent Systems.