A Defense-Attack Game under Multiple Preferences and Budget Constraints with Equilibrium

Nadia Niknami, Abdalaziz Sawwan, and Jie Wu
Department of Computer and Information Sciences
Temple University, Philadelphia, PA, USA

Abstract*—Cyber-security research often focuses on attack-defense games where a strategic attacker seeks to destroy the defender's targets or kill him. In such a game there is a defender who just try to protect himself. In the real world, players can choose to protect themselves as well as kill their opponents to maximize their overall gain. In this case, the player allocates their budget for both defending and attacking actions and decides how well to attack and how well to defend against others. Players should allocate their budgets appropriately for each action throughout multiple rounds when playing such a game. The probabilities of surviving and killing in each round are determined by what happened in the previous rounds and the amount of the remaining budget. Players can continue playing until they die or run out of money. It is possible for the player not to be aware of everything his opponent does. Despite knowing that his opponent is playing according to one of the possible types, he cannot see which action exactly he is taking. Likewise, it may be the case that the player only sees the opponent's action, but does not know what its objective is. To meet this challenge, this paper develops a game where players decide how to allocate resources when they have partial information. For a model with complete information, equilibrium can be found and, as an extension, models with incomplete and imperfect information are also discussed. Our simulation examines how utility changes based on prior beliefs, total budgets, costs, and uncertainty.

***Index Terms*—Defender-attacker games, (in)complete information, (im)perfect information, repeated games, sequential games.**

I. Introduction

The attack and defense game is a game in which an attacker has an incentive to destroy the defender's targets and a defender wants to protect it. Game theory is widely used to study this conflict between the players. In theory, each player should aim to maximize their gains by devising an optimal strategy according to their preference. In [1], Hausken analyzed the attack and defense strategies of systems according to different probabilities of detection by the attacker. It is not only each player's own actions that affect their welfare, but also those of others. Generally, players in the security domain prefer to attack their opponents or defend themselves against them. Consider a situation where players have both attacking and defending preferences, i.e. defending themselves and at the same time trying to kill opponents. The players must determine how they will allocate their limited budget for defending and attacking throughout multiple rounds of a sequential game.

This research was supported in part by NSF grants CPS 2128378, CNS 2107014, CNS 2150152, CNS 1824440, CNS 1828363, and CNS 1757533.

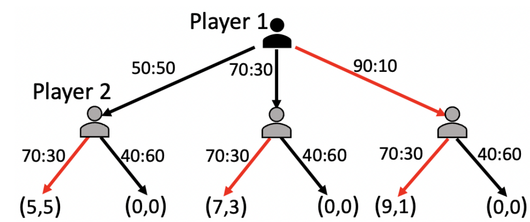


Fig. 1. Possible budget allocations and associated payoffs in a game with two players. Red line shows path of the best strategy in case of expected payoff.

In such a scenario, a proper resource allocation can protect players against possible attacks, while improper decisions result in a waste of resources, some damages, and even death. As a player tends to deploy more budget on attacking, he prefers to kill other players instead of defending himself. While spending more of his budget on defense, he prefers to survive even if he cannot kill the opponent. Consequently, balancing the allocation of budgets plays a crucial role in the interactions between players and their utilities. In other words, it is imperative to know how to manage defensive and offensive resources under budget constraints.

To facilitate this explanation, consider a game G in Fig. 1; the player set consists of Player 1 and Player 2 where the total budget is \$100 for both. For simplicity, suppose that there are three possible actions for Player 1 and two possible actions for Player 2. There is also a predefined payoff function. Player 1 can allocate \$70 for defending and \$30 for attacking. Additionally, he can allocate \$90 of his budget for defending and the remainder of his budget for attacking. Third action, this player can split his budget for defending and attacking evenly. Player 2's actions are \$70 : \$30 and \$40 : \$60. The tree structure shows the order of playing. The values in leaf nodes are obtained as the gain after the sequence of actions. The red lines in Fig. 1 show the best actions for players based on the obtained gain. For Player 2, by considering Player 1's possible actions, the action \$70 : \$30 has a higher gain value than \$90 : \$10. For Player 1, \$40 : \$60 has a higher gain value which is 9 against 5 and 7.

As in the real world, players are unaware of all information about the opposing side. They can see what the other side's reactions are. However, they cannot find out what kind of reaction it is and for what purpose the opponent took such an action. In incomplete information games, players need to learn from opponents' actions in order to devise the most effective strategy against them. Similarly, in a similar situation, the player will know all possible payoffs in each case of all possible actions, but they will not know what the specific action is. They have imperfect information about others. Players have trouble selecting the most useful action and allocating the proper budget due to such a lack of information. Therefore, it is essential to analyze the equilibrium allocation of defenders or attackers for different information availability scenarios and under budget constraints.

In the case of multiple players with different preferences in a game, each player should decide on their own budget. If a player dies during the game, the game will continue with the remaining ones and may involve multiple stages. We assume that staying in the game even without any investment for attacking has some base cost and gain for the player. In other word, there is a base cost for staying in the game. To ensure that the game will not continue forever, a measurement of cost is introduced. By considering the cost, player will stop playing when there is not enough budget for him to pay for the cost. If the cost of continuing the game is more than its benefits for the remaining players, it will stop. This cost value is considered in the utility function. In summary, we make the following contributions:

- We introduce a new game with two players who have preferences of both protection and destruction. As a result of their preferences and intentions, players allocate their resources to actions against their opponents. Based on how much they prefer attacking or defending, these players can be described as attacker-minded or defender-minded.
- We define the new utility function that includes both gains from staying in the game and gains from killing the opponents. Each player's incentive determines the amount of gain associated with their actions.
- We propose modeling the behaviors of players under budget constraints when players have incomplete or imperfect information at the time of decision making.
- We analyze the effects of the players' preferences, budget, and cost/expenditure on the model. Finding equilibrium involves balancing budget allocations with satisfying preferences.

The remainder of the paper is organized as follows: Section II describes related works on different approaches to model the interactions between attackers and defenders. Section III explains modeling a two-player game with two possible preferences of defending and attacking. In Section IV, we elaborate a little about incomplete and imperfect information game. In Section V, we evaluate our proposed algorithm by conducting experiments. This section contains some simulation results to evaluate our model. Section VI summarizes the results of experiments. Finally, we conclude our paper in Section VII and provide some suggestions for future work.

II. Related Works

This section presents related works on different approaches to modeling a game in a security domain. Most of the work on algorithms for finding an equilibrium has focused on the non-repeated game [2]–[5]. Hausken and Zhuang in [6] analyze allocating resources for a defender and attacker in a two-stage sequential game. Guan *et al.* in [7] analyze the equilibrium allocation of defenders and attackers based on a budget constraint in a multi-target attacker–defender game, but only for a one-shot game. Nevertheless, most of the interactions between agents are repeated many times.

TABLE I
Main notations

Symbol	Meaning
B/B'	Total budget of the Player $1/2$
D_i/D'_i	Defensive efforts of the Player $1/2$ at round i
A_i/A'_i	Attacking efforts of the Player $1/2$ at round i
k_i/k'_i	Probability that Player $1/2$ kills the opponent exactly at round i
d_i/d'_i	Probability that Player $1/2$ gets killed exactly at round i
$U(\mathbf{K})/U'(\mathbf{K})$	The Utility functions of Player $1/2$
α/α'	The reward for staying in the game for Player $1/2$
G/G'	The reward of killing the opponent for Player $1/2$
C	General cost of being in the game
$\mathcal{B}$	Player's belief
θ/θ'	Type of Player $1/2$
$S_\theta/S'_{\theta'}$	Strategy of Player $1/2$ when his type is θ/θ'

There are some interesting papers that consider analyzing multiple rounds of the game, but most of them neglect the possibility of the lack of information about the game. Z. Xu *et al.* in [8] design a sequential game with complete information between one defender and multiple attackers. Wu *et al.* in [9] propose a model for a game with one defender and two attackers. When both players have complete information and common knowledge, they consider the effect of risk attitude on their decisions. Zhai *et al.* in [10] introduce asymmetric utilities when there is no consistency between the attack target and the defense target. These papers all made some unrealistic assumptions. They do not cover scenarios in which players do not have enough information about the actions or preferences of other players. There is not complete information about the opponent's side in the real world.

In the approach of [11], an attacker and a defender play a signaling game. They suppose that there is incomplete information about the type of defender for the attacker. Attackers may attack immediately or wait until they are stronger against defenders. The authors in [12] consider multiple strategies and targets in a sequential defender-attacker game. With the zero-sum game, they model a scenario in which the defender is the first mover, and both players have the same preferences, without additional rewards. Zhang *et al.* in [13] compare this model with the traditional game where the attacker behaves rationally to study how the attacker's rationality affects the defender's optimal defense. Aziz *et al.* in [14] study a sequential game-theoretical resource allocation model where there are multiple defensive budget allocations among multiple potential targets. The idea is that the defender and attacker believe that the different types of resources are independent, but there are complementary effects between them. Neither of them

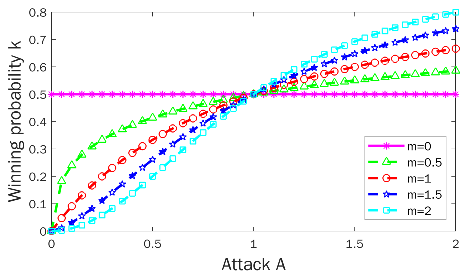


Fig. 2. The relation between k and A with varying values of m and $D = 1$.

take into account a situation where players with preferences for attacking and defending have incomplete or imperfect information.

To address these research gaps, we analyze the model on budget constraints with the possibility of different preferences for players in a repeated game. Players can have both preferences of attacking and defending. The model of this paper is more practical since it considers limited budget, time, and limited information in a repeated game. In the case of computing the value of the utility function, we take into account gain for players in the case of protecting themselves or terminating the opponent. There is a constant gain for survival and staying in the game, but the gain of killing is based on the probability of winning for the players.

III. The Defend-Attack Model

We model a two-player game where each player has two possible preferences: protecting itself and killing the opponent. When a player has more preference for defending in comparison to attacking, we can call him a defender-minded (D-minded). Similarly, a player who prefers to allocate more resources to attacking would be called attacker-minded (A-minded). By considering this, possible type of players in this game are the following: both players are D-minded, both players are A-minded, and one of the players is A-minded while another player is D-minded.

A. Contest Success Function and Utility

In order to find the player's success in obtaining their objective, A Contest Success Function [15] is used. Success probability of a player is determined not only by the amount he invests, but also by the opponent's investment. That is why it is a game. It helps to measure the interplay between the players in case of attacking and protection efforts. The Contest Success Function (CSF) is defined as:

$$k = \frac{A^m}{A^m + D^m}, \tag{1}$$

where A refers to the amount of effort that the player makes toward his objective and D is the effort of opponent's side. In the case of attacker and defender, A represents the amount of attack and D represents the amount of defense. If the player has attacking investment A and his opponent has defense investment D, the probability of a successful defense k decreases by the defensive investment D, and increases by the offensive investment A. The decisiveness parameter m

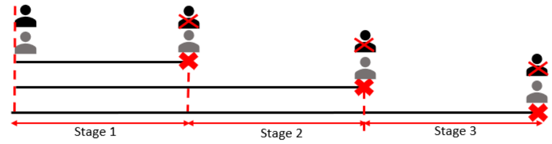


Fig. 3. Attack-defense game in three rounds.

should be set based on the contest intensity. It reflects how the survival of the opponent depends on the resources extended. The higher m expresses high intensity, whereas a low m expresses low intensity [16]. Fig. 2 illustrates how the level of decisiveness m affects the success probability of k for different values of the effort. We can see that with $A = 1.6$ there is success probability 0.7 when $m = 2$.

We can generalize the Eq. (1) to a multiple rounds game with two players who both are interested in maintaining a defense system against the opponent as well as spending some resources on killing the other side. For sake of simplicity, we consider $m = 1$ from so on. In this ratio form of CSF, A_i, D_i, A'_i, and D'_i refer to the attacking and defending efforts of Player 1 and 2 during round i respectively. The values of k_i and k'_i are the probability of killing the opponent for Player 1 and Player 2, respectively. In fact, by considering B and B' as the total budget of Player 1 and Player 2, D_i and D'_i are equal to some portion of total budget B and B' associated with defending at round i, A_i and A'_i is equal to some portion of total budget B and B' associated with attacking at round i. In this multiple rounds game, we can rewrite Eq. (1) as the probability that Player 1 kills Player 2 exactly at round i:

$$k_i = \frac{A_i}{A_i + D'_i}. \tag{2}$$

As well as the probability that Player 2 kills Player 1 exactly at round i:

$$k'_i = \frac{A'_i}{A'_i + D_i}. \tag{3}$$

The expected utility function for Player 1 is based on the gain of remaining in the game as well as killing the opponent. It should be noted that the number of rounds is based on the total budget and the probability of killing the opponent. There is constant gain α for surviving or staying in the game and G which is the gain of killing the opponent. The value G is the amount of reward that the player will receive if he can kill the opponent, which depends on the probability of wining, k_i, exactly at round i which is shown in Eq. (2). The value α represents the amount of reward that Player 1 obtains by surviving for a round. Based on the preference of the player between A-minded or D-minded strategy, there are different values for G and α. For example, if there is a higher value for the gain of surviving in comparison with the gain of killing, then players prefer to allocate more budget on defending. Therefore, a D-minded player finds higher α than an A-minded player for surviving in a given round. Suppose that the game ends after the first round. The utility for Player 1 would be:

$$U_1 = \alpha + G\frac{A_1}{A_1 + D'_1}. \tag{4}$$

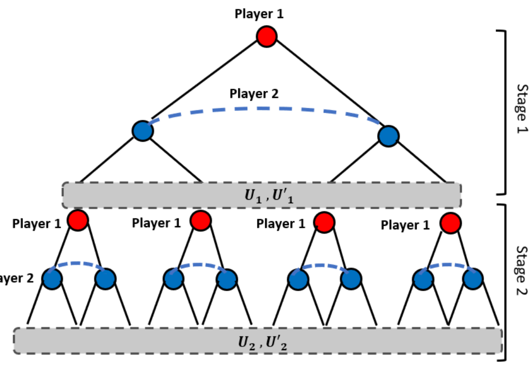


Fig. 4. Attack-defense game in two rounds.

As mentioned before, $A_1/(A_1+D'_1)$ represents the probability of killing Player 2 when Player 1 has A_1 amount of investment for attacking and Player 2 has D'_1 amount of investment for defending at round 1. If there are two rounds, the utility function for Player 1 includes the gain of staying in the game for two rounds, which is 2α, and the gain of killing the opponent in the first round or in the second round. We need to consider the probability of killing Player 2 in the first round, which is k_1, as well as the probability of killing Player 2 in the second round $(1-k_1)k_2$. It is important to consider the conditional probability for each round based on what happened during the previous rounds. Therefore, the utility function for Player 1 when the game ends in two rounds is as follows:

$$U_2 = 2\alpha + G\Big(\frac{A_1}{A_1+D'_1} + \big(1-\frac{A_1}{A_1+D'_1}\big)\times\frac{A_2}{A_2+D'_2}\Big). \quad (5)$$

According to Eq. (2), it can be written as :

$$U_2 = 2\alpha + G(k_1 + (1-k_1)k_2). \quad (6)$$

If there are three rounds, Player 1's utility function includes the gain of staying in the game for three rounds, which is 3α. In addition, it includes the gain of killing the opponent during the first round, during the second round, or during the third round. Here, we need to consider the probability of killing Player 2 at round 1 or 2 or 3. Accordingly, Player 1 can benefit from the utility function as follows when the game is over after three rounds:

$$U_3 = 3\alpha + G(k_1 + (1-k_1)k_2 + (1-k_1)(1-k_2)k_3). \quad (7)$$

To find the expected utility function for Player 1, we must consider the probability of ending the game in the first round, the probability of ending the game in the second round, the third round, etc., and the probability of ending the game in round T. Based on the total amount of the budget, T represents the number of rounds that are possible. Another variable is defined to represent the probability that Player 1 gets killed exactly at round i, which is called d_i. The probability of death for Player 1 at the very beginning of the game is $d_0 = 0$. The probability that Player 1 gets killed at rounds 1, 2, and 3 are as follows:

$$d_1 = k'_1, \quad d_2 = (1-k'_1)k'_2, \quad d_3 = (1-k'_1)(1-k'_2)k_3. \quad (8)$$

Algorithm 1 Multi-round Attack-defense Game

Require: B, B', C
$i = 1$
while $B > C$ **do**
  Players allocate budget for (A_i, D_i) and (A'_i, D'_i).
  Calculating k_i and k'_i
  Calculating U_i and U'_i.
  if Player 1 killed player 2 at round i **then**
    while $B > 0$ **do**
      Player 1 continues game with spending C
      Update remaining budget B.
    Break
    Go to round $i+1$
  return $U(K)$

Therefore, the probability that Player 1 gets killed exactly at round i is as follows:

$$d_i = \big(\prod_{x=1}^{i-1}(1-k'_x)\big)k'_i.$$

Utility Function for Player 1:

$$U(\mathbf{K}) = \alpha\sum_{x=1}^{T}((x-1)d_x) + G\sum_{x=1}^{T}\big(k_x\big(\prod_{j=1}^{x-1}(1-k'_j)\big)\big), \quad (9)$$

where $\mathbf{K}$ is the vector of parameters $k_1, k'_1, k_2, k'_2, \ldots$ and x stands for number of rounds. We consider the subspace of strategies where

$$k_1 \geq k_2 \geq \cdots \geq k_T \quad and \quad k'_1 \geq k'_2 \geq \cdots \geq k'_T.$$

Suppose that Player 1 and Player 2 are supposed to protect themselves and attack the opponents, respectively, to maximize their utility value with limited resources B and B'. The utility can be formulated by considering C as the base cost of staying in the game:

$$\begin{aligned} \max \quad & U(\mathbf{K}) \\ \text{subject to} \quad & \sum_{1\leq i\leq T}(A_i + D_i) \leq B \\ & D_i, D'_i \geq C \end{aligned} \quad (10)$$

Theorem 1. The utility function in Eq. (9) is a concave function for all budget allocations. Moreover, there is at least one *Nash equilibrium* for a game with a concave utility function.

Proof: An equilibrium point exists for every concave n-person game [17]. We need to investigate the concavity of the utility function in Eq. (9). In Appendix A, we prove the concavity of utility function. ■

IV. (In)complete and (Im)perfect Information

As with any repeated game, the key to analyzing the outcome is to analyze how much information is available about the game, because how the game proceeds will be determined by the result of each round. Each decision made early affects the decisions made by others later. Depending on the information that has been provided in previous stages,

Algorithm 2 Backward Induction

Require: Decision node n

if $n \in$ Leaf **then**
  return $U(n)$
Best-Utility $\leftarrow -\infty$
for each action $a \in S(n)$ **do**
  U $\leftarrow$ Backward Induction(n, a)
  if U $>$ Best-Utility **then**
    Best-Utility $\leftarrow$ U
return Best-Utility

Algorithm 3 Perfect Bayesian Equilibrium

Require: $S, S', \mathcal{B}$

The Player 1 starts with S.
Calculates updated $\mathcal{B}$ about Player 2 by using Bayes rule.
Calculates the Player 2's optimal action based on $\mathcal{B}$.
if S is the best response to the Player 2's strategy **then**
  PBE has been found.
return $(S^*, \mathcal{B})$

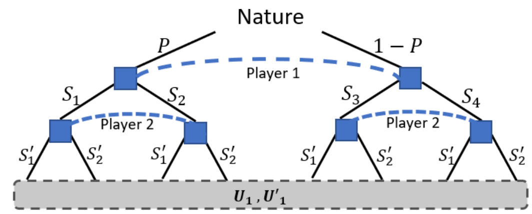


Fig. 5. Partial information for Player 1's preference.

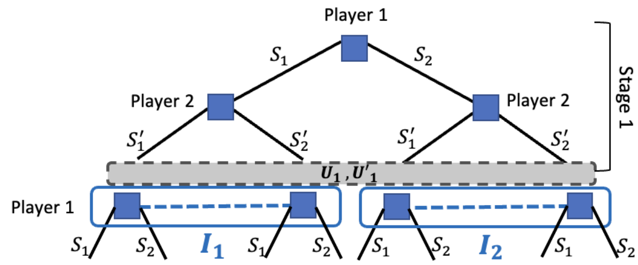


Fig. 6. Game with imperfect information for one of the players.

players can adjust their play accordingly. Information can be categorized into complete information, incomplete information, and imperfect information.

As opposed to perfect information games in which all players are aware of previous actions taken by others, imperfect information games tend to have one or more players unaware of previous actions. A game with complete information has strategies and payoffs that are known by all players. In an incomplete information game, at least one player does not know the strategies and rewards of their opponents [18]. In what follows, we review each of the types in turn.

A. *Complete and Perfect Information*

In games with complete and perfect information, players are fully aware of everything that has happened. Players are aware of their opponents' behavior and their preferences. The equilibrium paths of the game in such a case are determined by backward induction. It begins at the end of the game and moves backwards one stage at a time.

Definition 1 (Backward Induction)**.** A Nash equilibrium strategy can be derived from backward induction for every finite game of perfect information [19]. With the help of backward induction, the equilibrium path can be found.

Algorithm 2 presents the steps of the backward induction when n is a node in the tree of the game and a shows the action (branch in the tree). The results of backward induction are used to find the best utility value. To capture the notion of backward induction, we need to define the subgame. According to the Subgame Perfect Nash Equilibrium, the selected strategy of all players should be rational not only at the beginning of the game, but also in all subgames.

Theorem 2. The pair of strategies $S^* = (A, D)$ and $S'^* = (A', D')$ is a Subgame Perfect Nash Equilibrium (SPNE) in the extensive form game G, if it induces a Nash in every subgame with the following conditions:
1. Player 1 chooses S to maximize her expected utility U by assuming that Player 2 will choose his best response S'. That is, $S^* = \text{argmax}_S\, U(S, S')$.
2. Player 2 chooses his best response S' against S^* to maximize his expected utility U'. That is, $S'^* = \text{argmax}_{S'}\, U'(S, S')$.

Proof: At any point in the game, the players' subsequent behavior should reflect the Nash equilibrium of the continuation game (of the subgame), regardless of what has happened before. Each player will attempt to respond to the other side as effectively as possible [20]. ■

According to Theorem 2, in every part of the game, players are going to choose their actions optimally based on what others did. It should be noted that the order of the players in case of taking actions is important. It is obvious that the second mover can see what the action of the first mover was, and then select the proper action. This advantage applies only to a game with complete information. When there is not complete information for the players about the other players' action, the order of the playing the game would not be important. In fact, such a sequential game should be considered as a simultaneous game. In the subsections IV-B and IV-C, this type of game will be explained in detail. In the real world, we need to model games where complete information is not available. In such a scenario, there is partial information about the strategy and target of other players.

B. *Incomplete Information*

Most of the stochastic game models are composed of matrix game and Markov decision, which assumes that the player has known the opponent's information. This assumption does not conform to the actual situation. The uncertainty of the opponent's income can be converted to the indeterminacy of the player type, and an incomplete information game. When a player does not know all the information about the other players, e.g. their type, strategies, payoffs, or preferences, the game

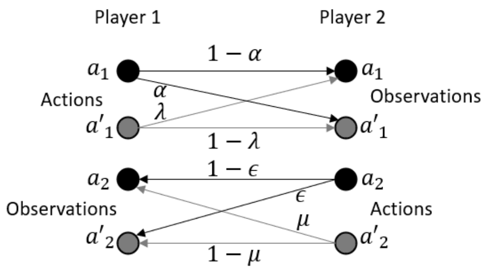


Fig. 7. A player observes his or her opponent's actions with error probabilities $\alpha, \lambda, \epsilon$, and μ.

is called incomplete/asymmetric information or Bayesian [21]. A Bayesian game considers incomplete information scenarios where players have beliefs about unknown factors and seek to maximize their expected utility. The reason for this is that players are not given enough information about what is happening in the game [22].

Each player in a game of complete information has a utility function that maps action or strategy into payoffs. As they observe one another's actions, they adjust their strategies accordingly. They may not be accurate with their observations, however. In a game of incomplete information, each player may have one of many possible utility functions. Players can form beliefs about one another based on their common knowledge. Different types of players are categorized according to their preferences. Although they know their own types (i.e. their preferences), they are unsure about the other player's types (i.e. their preferences). Despite this, there is a common understanding of the types of the other players. The setup of the game is shown in Fig. 7. Without loss of generality, it is assumed that $0 \leq \alpha, \lambda, \epsilon, \mu \leq 0.5$.

According to Harsanyi, in [23], the game begins after a move by chance that selects the different preferences or types of players. In the game, each player can observe his own type, but not those of the other players, so he or she needs to make predictions about their types. Based on the probability distribution over the different possible types of players, players should form beliefs about the strategies of the others. Such an equilibrium is known as Bayesian Nash equilibrium. It is a straightforward extension of Nash equilibrium. All types of players choose a strategy that maximizes expected utility based on the actions of all other types and their beliefs about other types. By predicting other types' behavior, players can maximize their own utility.

Definition 2. A game G with incomplete information is a tuple $< N, A, \Theta, S, U >$ where N is the number of players, A is the set of actions, Θ is the set of types of players, S is the set of possible strategies, and U is the utility function.

For such a game, perfect Bayesian equilibrium, or PBE, is the solution. AS mentioned above, Bayes-Nash equilibrium is a generalization of Nash equilibrium for incomplete information games. The result of PBE is a pair $(S, \mathcal{B})$ such that strategy S is sequentially rational given beliefs $\mathcal{B}$. Algorithm 3 presents the steps of PBE. Let $P(\theta'|\theta)$ denotes the probability that Player 2 has the type θ' given that Player 1 has type θ. If S_θ and $S'_{\theta'}$ stand for the strategy of players with types of θ and θ', the expected utility for Player 1 can be defined as:

$$U(S, S'|\theta) = \sum\nolimits_{\theta'} P(\theta'|\theta) \cdot U(S_\theta, S'_{\theta'}) \tag{11}$$

Definition 3. For the player with type θ, the strategy S is a Bayesian Nash equilibrium if:

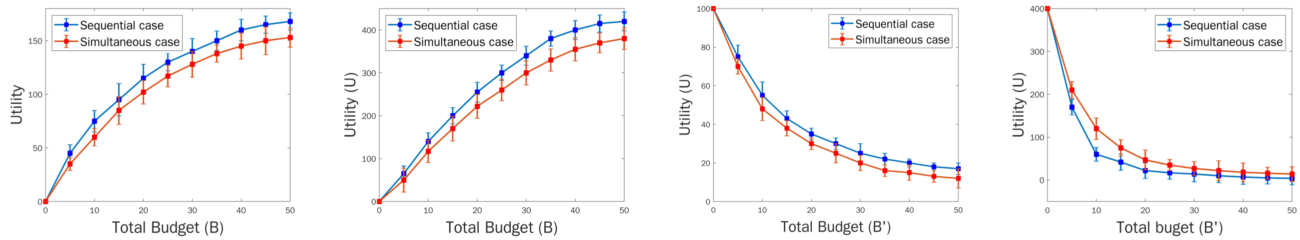
$$S_\theta = \arg\max\nolimits_S \sum\nolimits_{\theta'} P(\theta'|\theta) \cdot U(S_\theta, S'_{\theta'}). \tag{12}$$

The idea underlying this definition is identical to that for existence of Nash equilibrium in the complete information game. Consider game a G where there are two possible types, θ_1 and θ_2. Suppose that player 2 is not aware of the type of player 1. Based on his belief, the type of player 1 is θ_1 with probabilities P and θ_2 with probability $(1-P)$ [24]. Fig. 5 displays such an incomplete information game. After taking strategy S, a player needs to update his belief based on the Bayesian rules if it is possible. Suppose that $P = 0.5$ for the player 1 to be a D-minded player. Also suppose that as prior knowledge player 2 knows that player 1 with the probability of 0.75 allocates 70% of his budget for protection. If player 2 observes a large amount of protection investment, say D, he can update his belief about $P(\theta_1|D)$ with the help of the Bayesian rule of $P(D|\theta_1) \times P(\theta_1)/P(D)$.

C. *Imperfect Information*

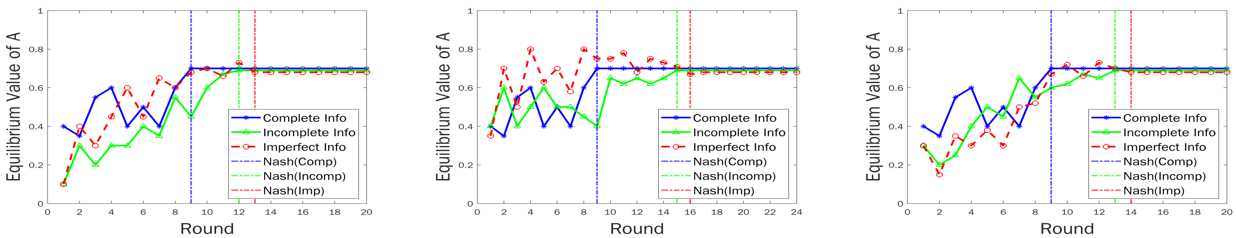
With perfect information, a player is able to perfectly observe every action they have taken in the past. Nevertheless, in the absence of perfect information, players cannot see the actions taken by their adversaries [25]. A game with imperfect information represents games where a player does not know what actions other players have taken at a given time. Consequently, it is computationally challenging to follow the history of actions during a multistage game. Nevertheless, all players may know their opponents' types, strategies, and payoff functions, which may create a complete, imperfect information game. In cybersecurity games, both the attacker and the defender are considered to be playing an imperfect information game [26] [27]. A game of imperfect information is an extensive-form game in which each player's choice nodes are divided into information sets. This information set I contains all the nodes that the player may be at. A player cannot distinguish between nodes in an information set. Player i's information sets are $I_{i1}, ..., I_{im}$ for some m, where $\{I_{i1} \cup ... \cup I_{im}\}$ is all nodes where it's player i's move. For all $j \neq k$ there is $I_{ij} \cap I_{ik} = \varnothing$.

All players know who the other players are, what their possible strategies/actions are, and what their preferences/rewards are. As a result, in an imperfect information game, the information about the other players is complete. Each player's decision node is located in an information set. The authors in [28] presented a repeated game with finite steps or infinite steps based on imperfect information. When two decision nodes are in the same information set, the player cannot distinguish between them and needs to rely on his beliefs to make a decision.



(a) $B' = 20$, $C = 10$ (b) $B' = 20$, $C = 1$ (c) $B = 20$, $C = 10$ (d) $B = 20$, $C = 1$

Fig. 8. Utility of Player 1 in the case of simultaneous and sequential games with varying budgets.



(a) Initial Belief:(10%:90%) (b) Initial Belief:(50%:50%) (c) Initial Belief:(30%:70%)

Fig. 9. Speed of convergence in the case of different belief. Dashed lines show the time of converging to the Nash equilibrium.

Consider the game in Fig. 6. In the first round, Player 1 starts the game and takes his action. Then Player 2 should make a decision based on observing what Player 1 did. Suppose that at the beginning of the second round, Player 1 cannot observe what Player 2 has done in the last round; however, Player 1 knows what the payoff is. Dashed lines in Fig. 6 shows the uncertainty of Player 1 in realizing where he is. The blue box represents information set I_1 and I_2. The two nodes in each of the information sets show imperfect information for Player 1. In this case, Player 1 has to consider all possible actions and find Nash equilibrium for each information set. The imperfect information game can be converted to a normal form and finding the Nash equilibrium is possible [29].

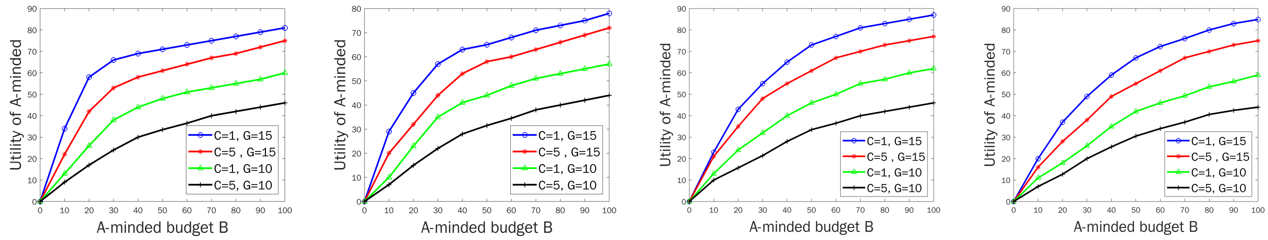
If we assume that players are not informed about their payoffs until the end of the final round, the repeated game can be modeled by a hidden Markov chain and can be classified as imperfect information. Such a game can be called a hidden Markov Bayesian game [30]. Using a hidden Markov model to group opponents into types and learn models for each type is helpful in case of imperfect information.

V. Evaluation

In this section, we present the results of analyzing optimal strategies of players and show the impacts of different parameters on interactions between players. Preference of players in the cases of attacking and defending, level of knowledge, amount of budget, cost, and m are parameters that can have an impact on the decision-making processes of players and their utility. We model a finite repeated game with limited budget for players. We investigate the trend of players in the case of complete and partial information and analyze the convergence to the Nash equilibrium. In a complete information game, each player has complete information about the total budget, taken actions, and preference of the other players. In a partial information game, the player cannot observe the actions or preferences of the other players and needs to learn about the game. We suppose that there are two players, one attacker-minded (A-minded) player and one defender-minded (D-minded) player in the game with complete information, incomplete information, or imperfect information. Without loss of generality, it is assumed that there are different values for α, c, and G in different scenarios. The value of $\alpha = 1$ or 5, $C = 1$ or 10, and $G = 10$ or 15.

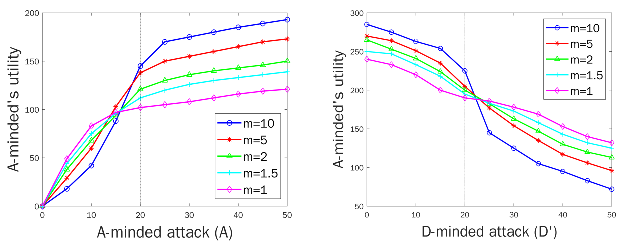
A. Impact of Different Amounts of Budget and Different Costs

In this section, we analyze the trend of players' behavior in case of different amounts of budget. Players need to spend their budget for the attack and defense as well as cost. More budget helps the player to more investments and it increases the chance of having a successful result. Fig. 8 shows the change in utility for Player 1 who is A-minded and Player 2 who is D-minded while keeping the budget of one side constant and varying the budget of other side. The A-minded player's expected gain increases when the total budget $B' = 20$ and there is increasing total amount of budget B. The result is similar when there are different base cost $C = 1$ and $C = 10$. There are decreasing values for utility of an A-minded player in a scenario with a constant amount of budget $B = 20$ for the A-minded player and increasing budget for D-minded. Therefore, the amount of budget plays an important role in the game. In addition, Fig. 8 compares the results for sequential and simultaneous game. In the simultaneous game, both players cannot find any information about the action and preference of another player before making a decision about their action. Hence, there is higher gain for the player in the sequential game compared to the simultaneous one.



(a) $B' = 20, \alpha = 1$ (b) $B' = 40, \alpha = 1$ (c) $B' = 20, \alpha = 5$ (d) $B' = 40, \alpha = 5$

Fig. 10. The effect of different values of cost and gain on utility.



(a) $D' = 20$ (b) $A = 20$

Fig. 11. Effect of m on utility with varying amount of attack and defend.

B. Convergence in Different Information and Initial Beliefs

Availability of information is an effective item in the process of decision-making for players. When there is complete information for the player about the action and intention of the opponent side, the player can select the best action without a doubt. In the case of partial information, players cannot see what the exact actions of opposing sides are or cannot find what the exact intentions are. After any observation, if it is possible, they update their prior belief about the other sides and find what the best action against these opponents is. In this section, we want to investigate the speed of convergence to the Nash equilibrium equilibrium in different availability of information for players. As Fig. 9 illustrates, the speed of converging to the Nash in the complete information game is higher than one with partial information. Similarly, in an imperfect information game, player needs to spend more time to reach the Nash equilibrium in comparison to an incomplete information. With different initial beliefs, predict other players' behavior, eventually the game will converged.

C. Impact of Different Amounts of Gain and Cost

In this part of the evaluation, we evaluate the effect of different values for cost of staying in the game which is presented by C, gain of staying in the game α, and gain of killing the opponent G on the utility function. As mentioned before, we need to consider a base cost for staying in the game, otherwise the final remaining player can be in the game forever. The value of C helps us to estimate the total number of rounds in a game if there is a budget limitation for the players. Fig. 10 shows the utility value for an attacker-minded player in four scenarios that are based on the total amount of budget and the value of α. We consider a fixed amount of budget for the opponent, then evaluate the utility value with a varying amount of budget for the attacker-minded player. It is obvious that the lower cost C helps the player to keep more budget for attacking and increase the probability of staying in the game. Also, as a result of the higher gains, players can find higher utility at the end of the game. The total amount of budget belonging to the opponent has a significant effect on the result of the game as well. The more budget, the more chance of winning for the player.

D. Impact of Different Values of m

In CSF, m represents the intensity of the contest. Fig. 11 illustrates the effect of different values of m on the utility of Player 1 when there is a fixed amount of investment for one of the players and a varying investment for another one. It turns out that a higher value for m corresponds to a higher intensity. An A-minded player will have a smaller amount of investment for attacking than D', or in this case 20, so that a large m will have a lower utility value than a small m. However, when the amount of attack against D' is greater, the utility value of a large m is greater than a small m. Similar results are obtained when we consider fixed attack A for the A-minded player and different investments from the D-minded player, D', for defending. Fig. 11 (b) represents the effect of m on decreasing utility for the A-minded player when he has lower or higher effort against the D-minded player.

VI. Discussion

It is evident from the results above that the overall budget and cost of remaining in the game play an important role in the outcome of the game. The result of analyzing the effect of m on the utility turns out that with a higher value for m, there is a higher intensity and higher impact related to the opponent's investment. An important factor determines the result of the game and the amount of utility that can be obtained is the amount of total budget and the ratio of budgets between players. Taking into account the imperfectness of the observations for both players and the lack of information about the opponent's motivations, players need to update their prior belief about the other side after any observation, and then find the best way to deal with these opponents. When each player believes correctly about his opponent, he eventually reaches the Nash Equilibrium, which is the point at which the player maximizes the gain against all of the opponent's strategies. The cost of remaining in this game is another significant factor. In the case of the lower cost C and high gain α, there is a possibly greater utility for an attacker-minded player who receives a higher reward G for killing the opponent.

VII. Conclusion

Among studies on defense-attack games, no previous approaches have explicitly considered both attacking and defending preference in the resource allocation alongside the constraints of partial information and restricted budget. In this paper, we investigated how optimal defense and offense could change when both players are rational and their strategy relies on strategic interactions, in which both players benefit from defending and killing. Possibly one of them would prefer designing a defense system against an attack, while the other would rather kill another player. By considering budget constraints, finding equilibrium and optimizing solutions and their respective payoffs is an interesting challenge. Verifying the influences of various parameters on the equilibrium helps to better understand the attacker's activities and obtain a better defensive strategy. As a future work, we can evaluate a game with more than two players. Different preferences determine the priorities and order of actions in such a game. Additionally, players can share their budgets with one another.

References

[1] G. Levitin and K. Hausken, "Defence and attack of systems with variable attacker system structure detection probability," *Journal of the Operational Research Society*, vol. 61, no. 1, pp. 124–133, 2010.

[2] X. Liu, X. Di, J. Li, H. Wang, J. Zhao, H. Yang, L. Cong, and Y. Jiang, "Allocating limited resources to protect a massive number of targets using a game theoretic model," *Mathematical Problems in Engineering*, vol. 2019, 2019.

[3] O. Baron, O. Berman, and A. Gavious, "A game between a terrorist and a passive defender," *Production and Operations Management*, vol. 27, no. 3, pp. 433–457, 2018.

[4] A. Yolmeh and M. Baykal-Gürsoy, "Two-stage invest–defend game: Balancing strategic and operational decisions," *Decision Analysis*, vol. 16, no. 1, pp. 46–66, 2019.

[5] N. Niknami and J. Wu, "A constraint partially observable semi-markov decision process for the attack–defence relationships in various critical infrastructures," *Cyber-Physical Systems*, pp. 1–26, 2021.

[6] K. Hausken and J. Zhuang, "Governments' and terrorists' defense and attack in a t-period game," *Decision Analysis*, vol. 8, no. 1, pp. 46–70, 2011.

[7] P. Guan, M. He, J. Zhuang, and S. C. Hora, "Modeling a multitarget attacker–defender game with budget constraints," *Decision Analysis*, vol. 14, no. 2, pp. 87–107, 2017.

[8] Z. Xu and J. Zhuang, "A study on a sequential one-defender-n-attacker game," *Risk Analysis*, vol. 39, no. 6, pp. 1414–1432, 2019.

[9] D. Wu, X. Yan, R. Peng, and S. Wu, "Optimal defence-attack strategies between one defender and two attackers," *Journal of the Operational Research Society*, pp. 1–17, 2019.

[10] Q. Zhai, R. Peng, and J. Zhuang, "Defender–attacker games with asymmetric player utilities," *Risk Analysis*, vol. 40, no. 2, pp. 408–420, 2020.

[11] X. Zhou, J. Huang, and G. Cheng, "Attacker-defender signaling game in multi-period based on technology accumulation and bayesian learning," in *In Proc. of Machinery, Materials and Information Technology Applications*. Atlantis Press, 2015.

[12] X. Zhang, S. Ding, B. Ge, B. Xia, and W. Pedrycz, "Resource allocation among multiple targets for a defender-attacker game with false targets consideration," *Reliability Engineering & System Safety*, vol. 211, p. 107617, 2021.

[13] J. Zhang, Y. Wang, and J. Zhuang, "Modeling multi-target defender-attacker games with quantal response attack strategies," *Reliability Engineering & System Safety*, vol. 205, p. 107165, 2021.

[14] R. A. Aziz, M. He, and J. Zhuang, "An attacker–defender resource allocation game with substitution and complementary effects," *Risk Analysis*, vol. 40, no. 7, pp. 1481–1506, 2020.

[15] K. Hausken, "Choosing what to protect when attacker resources and asset valuations are uncertain," *Operations Research and Decisions*, vol. 24, 2014.

[16] S. Skaperdas, "Contest success functions," *Economic theory*, vol. 7, no. 2, pp. 283–290, 1996.

[17] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica: Journal of the Econometric Society*, pp. 520–534, 1965.

[18] M. Zhu, A. H. Anwar, Z. Wan, J.-H. Cho, C. Kamhoua, and M. P. Singh, "Game-theoretic and machine learning-based approaches for defensive deception: A survey," *arXiv preprint arXiv:2101.10121*, 2021.

[19] U. Schwalbe and P. Walker, "Zermelo and the early history of game theory," *Games and economic behavior*, vol. 34, no. 1, pp. 123–137, 2001.

[20] M. J. Osborne *et al.*, *An introduction to game theory*. Oxford university press New York, 2004, vol. 3, no. 3.

[21] A. Kajii and S. Morris, "The robustness of equilibria to incomplete information," *Econometrica: Journal of the Econometric Society*, pp. 1283–1309, 1997.

[22] E. Dekel, D. Fudenberg, and D. K. Levine, "Learning to play bayesian games," *Games and Economic Behavior*, vol. 46, no. 2, pp. 282–303, 2004.

[23] J. C. Harsanyi, "Games with incomplete information played by "bayesian" players, i–iii part i. the basic model," *Management science*, vol. 14, no. 3, pp. 159–182, 1967.

[24] N. Ben Amor, H. Fargier, R. Sabbadin, and M. Trabelsi, "Possibilistic games with incomplete information," 2019.

[25] D. Koller and A. Pfeffer, "Generating and solving imperfect information games," in *IJCAI*. Citeseer, 1995, pp. 1185–1193.

[26] T. Başar and G. J. Olsder, *Dynamic noncooperative game theory*. SIAM, 1998.

[27] L. Phlips, *The economics of imperfect information*. Cambridge University Press, 1988.

[28] T. Alpcan and T. Basar, "A game theoretic analysis of intrusion detection in access control systems," in *In Proc. of CDC*, vol. 2. IEEE, 2004, pp. 1568–1573.

[29] S. Shiva, S. Roy, H. Bedi, D. Dasgupta, and Q. Wu, "A stochastic game model with imperfect information in cyber security," in *The 5th International Conference on i-Warfare and Security*. Citeseer, 2010, pp. 308–318.

[30] W. He and J. Gao, "Hidden markov bayesian game with application to chinese education game," *Journal of Uncertainty Analysis and Applications*, vol. 4, no. 1, p. 4, 2016.

Appendix

Proof of Theorem 1: An equilibrium point exists for every concave n-person game [17]. We need to investigate the concavity of the utility function in Eq. (9). Here we prove the concavity of the utility function for Player 1:

$$U(\mathbf{K}) = \alpha \sum_{x=1}^{T}((x-1)d_x) + G\sum_{x=1}^{T}(k_x(\prod_{j=1}^{x-1}(1-k'_j))),$$

where $\mathbf{K}$ is the vector of parameters $k_1, k'_1, k_2, k'_2, \ldots$ and x stands for number of rounds. We consider the subspace of strategies where $k_1 \geq k_2 \geq \cdots \geq k_T$ and $k'_1 \geq k'_2 \geq \cdots \geq k'_T$. As we mentioned before, k_i is the probability that Player 1 kills Player 2 exactly at round i.

$$k_i = \frac{A_i^m}{A_i^m + D_i'^m}, \quad k'_i = \frac{A_i'^m}{A_i'^m + D_i^m}.$$

By considering B and B' as the total budget of Player 1 and Player 2, D_i and D_i' are equal to some portion of total budget B and B' associated with defending at round i, as well as A_i and A_i' is equal to some portion of total budget B and B' associated with attacking at round i. We do prove the concavity of $U(\mathbf{K})$ by the following statement:

$$U(\lambda\mathbf{K}^1 + (1-\lambda)\mathbf{K}^2) \geq \lambda U(\mathbf{K}^1) + (1-\lambda)U(\mathbf{K}^2),$$

where $\mathbf{K}^1$ are the parameters of the first game $(k_1^1, k_1^{'1}, k_2^1, k_2^{'1}, \dots)$ and $\mathbf{K}^2$ are the parameters of the second game $(k_1^2, k_1^{'2}, k_2^2, k_2^{'2}, \dots)$, when $\forall\lambda \in [0,1]$. Without loss of generality, we consider the case $k_1^1 \geq k_1^2, k_2^1 \geq k_2^2, \dots$. We start from the left hand side and replace $\mathbf{K}^1$ and $\mathbf{K}^2$ with the parameters of the attack-defense game:

$$\begin{aligned}
&U(\lambda\mathbf{K}^1 + (1-\lambda)\mathbf{K}^2)\\
&= \alpha(1-(\lambda k_1^{'1} + (1-\lambda)k_1^{'2}))(\lambda k_2^{'1} + (1-\lambda)k_2^{'2})\\
&+ 2\alpha(1-(\lambda k_1^{'1} + (1-\lambda)k_1^{'2}))(1-(\lambda k_2^{'1} + (1-\lambda)k_2^{'2}))\\
&(\lambda k_3^{'1} + (1-\lambda)k_3^{'2}) + \dots\\
&+ G\sum_{x=1}(\lambda k_x^1 + (1-\lambda)k_x^2)(\prod_{j=1}^{x-1}(\lambda k_j^{'1} + (1-\lambda)k_j^{'2}))\\
&= \alpha\lambda k_2^{'1} + \alpha(1-\lambda)k_2^{'2} - \alpha\lambda^2 k_1^{'1}k_2^{'1}\alpha\lambda(1-\lambda)k_1^{'1}k_2^{'2}\\
&- \alpha\lambda(1-\lambda)k_1^{'2}k_2^{'1} - \alpha(1-\lambda)^2 k_1^{'2}k_2^{'2} + \dots\\
&+ G\sum_{x=1}(\lambda k_x^1 + (1-\lambda)k_x^2)(\prod_{j=1}^{x-1}(\lambda k_j^{'1} + (1-\lambda)k_j^{'2}))
\end{aligned}$$

We replace $\mathbf{K}^1$ and $\mathbf{K}^2$ with in the parameters of the attack-defense game in right hand side statement, therefore we have:

$$\begin{aligned}
&\lambda U(\mathbf{K}^1) + (1-\lambda)U(\mathbf{K}^2)\\
&= \alpha(\lambda(1-k_1^{'1})k_2^{'1} + (1-\lambda)(1-k_1^{'2})k_2^{'2})\\
&+ 2\alpha(\lambda(1-k_1^{'1})(1-k_2^{'1})k_3^{'1}\\
&+ (1-\lambda)(1-k_1^{'2})(1-k_2^{'2})k_3^{'2}) + \dots\\
&+ G\lambda\sum_{x=1}(k_x^1(\prod_{j=1}^{x-1}(1-k_j^{'1})))\\
&+ G(1-\lambda)\sum_{x=1}(k_x^2(\prod_{j=1}^{x-1}(1-k_j^{'2})))\\
&= \alpha\lambda k_2^{'1} + \alpha(1-\lambda)k_2^{'2} - \alpha\lambda k_1^{'1}k_2^{'1} - \alpha(1-\lambda)k_1^{'2}k_2^{'2} + \dots\\
&+ G\lambda\sum_{x=1}(k_x^1(\prod_{j=1}^{x-1}(1-k_j^{'1})))\\
&+ G(1-\lambda)\sum_{x=1}(k_x^2(\prod_{j=1}^{x-1}(1-k_j^{'2})))
\end{aligned}$$

Now, we need to show that

$$U(\lambda\mathbf{K}^1 + (1-\lambda)\mathbf{K}^2) - (\lambda U(\mathbf{K}^1) + (1-\lambda)U(\mathbf{K}^2)) \geq 0$$

To do so, subtracting the corresponding terms yields:

$$\begin{aligned}
&U(\lambda\mathbf{K}^1 + (1-\lambda)\mathbf{K}^2) - (\lambda U(\mathbf{K}^1) + (1-\lambda)U(\mathbf{K}^2))\\
&= \alpha\lambda k_2^{'1} + \alpha(1-\lambda)k_2^{'2} - \alpha\lambda k_2^{'1} - \alpha(1-\lambda)k_2^{'2}\\
&- \alpha\lambda^2 k_1^{'1}k_2^{'1} + \alpha\lambda k_1^{'1}k_2^{'1} - \alpha\lambda(1-\lambda)k_1^{'1}k_2^{'2}\\
&- \alpha\lambda(1-\lambda)k_1^{'2}k_2^{'1} - \alpha(1-\lambda)^2 k_1^{'2}k_2^{'2} + \alpha(1-\lambda)k_1^{'2}k_2^{'2}\\
&+ \dots\\
&+ G\sum_{x=1}(\lambda k_x^1 + (1-\lambda)k_x^2)(\prod_{j=1}^{x-1}(\lambda k_j^{'1} + (1-\lambda)k_j^{'2}))\\
&- G\lambda\sum_{x=1}(k_x^1(\prod_{j=1}^{x-1}(1-k_j^{'1})))\\
&- G(1-\lambda)\sum_{x=1}(k_x^2(\prod_{j=1}^{x-1}(1-k_j^{'2}))) = 0
\end{aligned}$$

We can rewrite this statement as:

$$\begin{aligned}
&U(\lambda\mathbf{K}^1 + (1-\lambda)\mathbf{K}^2) - (\lambda U(\mathbf{K}^1) + (1-\lambda)U(\mathbf{K}^2))\\
&= \alpha\lambda(1-\lambda)k_1^{'1}k_2^{'1} - \alpha\lambda(1-\lambda)k_1^{'1}k_2^{'2}\\
&- \alpha\lambda(1-\lambda)k_1^{'2}k_2^{'1} + \alpha\lambda(1-\lambda)k_1^{'2}k_2^{'2} + \dots\\
&+ G\sum_{x=1}(\lambda k_x^1 + (1-\lambda)k_x^2)(\prod_{j=1}^{x-1}(\lambda k_j^{'1} + (1-\lambda)k_j^{'2}))\\
&- G\lambda\sum_{x=1}(k_x^1(\prod_{j=1}^{x-1}(1-k_j^{'1})))\\
&- G(1-\lambda)\sum_{x=1}(k_x^2(\prod_{j=1}^{x-1}(1-k_j^{'2}))) = 0
\end{aligned}$$

Then:

$$\begin{aligned}
&U(\lambda\mathbf{K}^1 + (1-\lambda)\mathbf{K}^2) - (\lambda U(\mathbf{K}^1) + (1-\lambda)U(\mathbf{K}^2))\\
&= \alpha\lambda(1-\lambda)(k_1^{'1}k_2^{'1} + k_1^{'2}k_2^{'2} - k_1^{'1}k_2^{'2} - k_1^{'2}k_2^{'1}) + \dots\\
&+ G\sum_{x=1}(\lambda k_x^1 + (1-\lambda)k_x^2)(\prod_{j=1}^{x-1}(\lambda k_j^{'1} + (1-\lambda)k_j^{'2}))\\
&- G\lambda\sum_{x=1}(k_x^1(\prod_{j=1}^{x-1}(1-k_j^{'1})))\\
&- G(1-\lambda)\sum_{x=1}(k_x^2(\prod_{j=1}^{x-1}(1-k_j^{'2}))) = 0
\end{aligned}$$

Now, since $k_1^1 \geq k_1^2, k_2^1 \geq k_2^2, \dots$, and $k_1 \geq k_2 \geq \dots$ as well as $k_1' \geq k_2' \geq \dots$, we conclude that:

$$(k_1^{'1}k_2^{'1} + k_1^{'2}k_2^{'2} - k_1^{'1}k_2^{'2} - k_1^{'2}k_2^{'1}) \geq 0.$$

The same would apply for the remaining $2\alpha, 3\alpha, \dots$ terms. Furthermore, the last three G terms reduce to the exact formula except that while replacing the factor k_i' by k_i. Hence, the inequality applies. By that, we have proven the concavity of U in $k_1, k_1', k_2, k_2', \dots$. Now, since both $-k_i(A_i)$ and $k_i'(D_i)$ are convex $\forall i, m \geq 1$, and U^a is nonincreasing in each of the arguments in $\mathbf{K}$. Hence, U is concave on $A_1, D_1, A_2, D_2, \dots$. ■