Received: 27 August 2018 | Revised: 16 December 2018 | Accepted: 30 January 2019

DOI: 10.1002/sys.21479

REGULAR PAPER

WILEY

A game-theoretic model for resource allocation with deception and defense efforts

Xiaoxiong Zhang[1,2,5] | Keith W. Hipel[2,3,4] | Bingfeng Ge[5] | Yuejin Tan[5]

[1]The Sixty-third Research Institute, National University of Defense Technology, Nanjing, Jiangsu, China

[2]Department of Systems Design Engineering, University of Waterloo, Waterloo, ON, Canada

[3]Centre for International Governance Innovation, Waterloo, ON, Canada

[4]Balsillie School of International Affairs, Waterloo, ON, Canada

[5]College of Systems Engineering, National University of Defense Technology, Changsha, Hunan, China

Correspondence
Bingfeng Ge, College of Systems Engineering, National University of Defense Technology, Changsha, Hunan 410073, China.
Email: bfge.nudt@gmail.com

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 71690233, 71501182, 71571185

Abstract

This paper develops a strategy for assisting two players in allocating multiple resources in a strategic sequential game. The defender first needs to allocate deception and defense efforts among targets to deceive the attacker and strengthen the target, respectively. Then, the attacker chooses a type of threat and a target to attack. The defender aims at mitigating the possible damage to the targets, whereas the attacker strives to cause maximum damage to the targets. Traditional modeling approaches typically focus only on the defender's homogeneous resource in defense and are not well suited to effectively capture the complex interplay between players. Given scarce resources, a game-theoretic model is proposed for determining optimal strategies for both players. The key novel features of this model include: (1) the attacker's learning and the defender's counter-learning efforts are considered; (2) trade-offs between deception and defense efforts among different targets for the defender are investigated; and (3) sensitive analysis is carried out to see how different parameters can affect the equilibrium results. An illustrative example is presented to demonstrate the procedure of this game-theoretic model and show its effectiveness. The results can provide additional insights for defense and deception strategies.

KEYWORDS

deception and defense, game-theoretic model, learning and counter-learning, resource allocation, sequential game, trade-off

1 | INTRODUCTION

Efficient resource allocation reflects proficiency and requires prompt decisions while managing the available resources, especially in a military environment. Since September 11, 2001, studies of various models associated with national security have rapidly proliferated.[1] In general, these studies are mainly about a two-player game between a defender (she) and an attacker (he). The defender needs to allocate resources among targets to protect herself from possible terrorism or attacks. The attacker, on the other hand, aims to attack targets to cause possible damage. Therefore, appropriate resource allocations can greatly protect the defender from possible attacks, whereas improper decisions could lead to a waste of resources or even unprecedented damages to the defender's interest. Thus, knowing how to make the best use of resources is highly important, especially under circumstances of limited resources.[2,3]

To date, many researchers have addressed the attacker-defender game, where each player seeks to maximize a single objective function under certain constraints. Game theory and the concept of Nash equilibrium have been recognized as suitable tools for studying such strategy-interaction resource allocation problems for a long time.[4–6] For example, Zhuang and Bier[7] utilized game theory to identify the best defensive strategy with endogenous attacker effort for countering terrorism and natural disasters. Bier et al[8] explored a rigorous computational model for the optimal allocation of resources among potential terrorist targets. Subsequently, Golany et al[9] investigated the problem of allocating multiple defensive resources to protect multiple sites as a two-person zero-sum game with piecewise linear utility functions and polyhedral action sets. Paulson et al[10] studied a strategic game-theoretic model for resource allocation among countermeasures with multiple attributes. In summary, various modifications to game-theoretic models by adding complexities in defender-attacker situations have been proposed for the purposes of better representing real-world situations.[11–13]

The resource management in the attacker-defender game has also increasingly become relevant with the interdisciplinary field of systems engineering. In fact, many systems engineering authors are considering the role of humans in the design and development of complex systems, as well as the broader sociotechnical context of systems.[14–16] To that end, various game-theoretic models have been proposed. The

theoretical game between players, in this paper, can also be treated as a kind of system—one that calls for increasing attention as such. Based on the definitions, a system carries the following characteristics[17]: (1) consisting of multiple elements interacting with each other, (2) following an established or organized procedure, and (3) aiming to accomplish certain objectives. In fact, from a system perspective, the resource allocation game between two players matches these specific characteristics. More specifically, taking the two players game as a system, the attacker and defender are then considered to be ingredients constituting the system, satisfying the first characteristic. Both players take their own actions either simultaneously or sequentially, following an organized pattern. Therefore, the second characteristic is satisfied. As for the last characteristic, each player focuses on maximizing their own benefits by taking into account the other player's actions. When an equilibrium is obtained, no player has the incentive to deviate from their current strategies. The aim of a system is to achieve stability, which is similar with that of obtaining the equilibrium solution of a strategic game. In other words, the goal of the players essentially equals the goal of the system, especially when the elements of the systems are highly interrelated and affect each other.

In reality, defenders may be better off utilizing secrecy or deception rather than disclosure in military strategies for homeland security.[18] Some studies have responded to this idea by allowing for secrecy or deception for the defender's strategy in a game. For example, Hausken and Levitin[19] analyzed the optimal distribution of the defense resources between protecting the genuine system elements and deploying false elements in a defender-attacker game. Zhuang et al[20] used game theory to model strategies of secrecy and deception in a multiperiod resource allocation and signaling game with two players under an incomplete information environment. Such a model is complicated and entails great computational costs in identifying mixed-strategy equilibrium. The recent work by Zhang et al[21] presented a multiobjective optimization approach for facility location problems considering intentional attacks using secrecy. Thus, with deception efforts deployed, the attacker may need to take great efforts to learn the target before launching an attack in the decision-making process. The aforementioned literature focuses on the effect of secrecy or deception in a game, especially on how the deception can mislead the attacker from attacking certain targets. The issue is that they ignore the attacker' learning behavior before launching an attack, which is realistic and important. Later, Xu and Zhuang[22] analyzed the strategic interactions of a terrorist's costly learning and defender's counter-learning and defense strategies in a game with private defender information. However, they still leave open the question: how to consider the trade-off between different kinds of resources for the defender in a strategic game.

In this paper, we analyze the strategic sequential game between a defender and an attacker. The defender needs to allocate resources among potential targets with deception and defense efforts, and the attacker chooses a type of threat and a target to attack. As an extension of previous game-theoretic models, the strategic interactions between the attacker's learning and defender's counter-learning efforts are modeled. Given scarce resources, the defender needs to do trade-offs between deception and defense efforts among different targets. The attacker, on the other hand, needs to decide which target to learn and subsequently whether to launch an attack or not. We aim to achieve an equilibrium that not only provides optimal resource allocations within each target for the defender, but also provides the best strike strategy for the attacker. Meanwhile, we admit that in certain circumstances such as where targets are networked, the payoffs rely heavily on the connectivity and inherent synergy effect between various targets.[23] Comparative studies are also carried out in this paper, and one of the crucial findings is how the equilibrium depends on various parameters. The model enables players making better decisions to support a variety of purposes, including how best to carry out trade-offs between different resources and choose proper attack strategies. In addition, the game-theoretic model can also be expanded in other negotiation and decision-making problems associated with multiple players in system engineering fields, such as project scheduling, business negotiations, and international conflict resolution. To the best of our knowledge, no previous study has been carried out which is similar to the contributions in this paper.

The remainder of this paper is organized as follows. Section 2 introduces the basic notation and model for the game. Section 3 explores the equilibrium solution and some theoretical findings. Section 4 studies a number of illustrative examples to demonstrate how the game-theoretic model works. Conclusions and suggestions for further research are given in Section 5.

2 | MODEL FORMULATION

In this section, a game-theoretic model is proposed for investigating the resource allocation problem with two players. Section 2.1 gives the notations used throughout this paper. Section 2.2 introduces the basic description of this problem. Last, Section 2.3 presents the mythology to demonstrate the calculations for determining the payoff of each player.

2.1 | Notation

The notations used in this paper are first explained, including parameters, functions, and decision variables, as shown in Table 1.

2.2 | Description

Consider a resource allocation game having two players, referred to as the defender and the attacker, along with the following assumptions:

1. The defender has a limited resource to allocate among targets.
2. The attacker chooses a type of threat and a target to attack.
3. The defender can use the resources either in deception or defense among targets.
4. The deception resource can mislead the attacker, whereas the defense resource can decrease the probability of a successful attack.
5. The attacker needs to learn the target before attacking once deception resources are deployed.
6. Certain costs will be incurred when learning or attacking targets.

7. Each target and each attack are independent of each other.
8. The defender moves first, allocating deception and defense resources among targets under resource constraints. The attacker moves second, learning and choosing a proper target to attack.
9. Both players have complete information of this game.
10. The defender aims to minimize her losses, whereas the attacker attempts to cause damage to the most extent.

2.3 | Methodology

In this section, the methodology used to tackle this model and how to obtain the payoff (utility or disutility) for each player is investigated. We aim to determine the best resource allocation strategy for the defender, and the best attack strategy for the attacker.

To begin with, the probability of a successful attack j at a target i varies based on the defense effort and the vulnerability of targets. Assume that if no defense effort is used on a target, the attacker can successfully destroy this target with certainty. On the contrary, when the defense effort approximates positive infinity, the probability of a successful attack should be around zero. Meanwhile, even the same attack can have different impacts on attacking different targets. Based on the above assumptions, the resulting probability of a successful attack at one target is formulated as in (1):

$$P_{ji}(l) = e^{-\alpha_{ji} l_i}; \tag{1}$$

where α_{ji} is a coefficient representing the effectiveness of attack j on target i, and l_i is the defense effort deployed at target i.

The attacker's learning cost is highly correlated with the deception efforts deployed at target i. The greater efforts the defender spends in deceiving the attacker, the more cost it will incur associated with the attacker's learning on this target. Herein, learning refers to obtaining knowledge with respect to attacking targets, such as obtaining the true locations of targets and exploring new skills to attack targets. The learning cost is formulated based on the deception efforts as in (2):

$$C_i(d) = k_i d_i, \tag{2}$$

where k_i is a coefficient denoting the unit cost of learning target i related with the deception effort.

For a given threat j at a given target i, the defender's expected disutility can be determined using

$$L_D(d, l, y) = P_{ji} f_D(\beta_{ji}), \tag{3}$$

where P_{ji} is the probability of the success of an attack for a given threat j against a given target i, and $f_D(\beta_{ji})$ denotes the disutility arising from the corresponding attack.

As for the attacker, he faces a set of choices: which threat to use and which target to attack. However, we assume that the attacker needs to learn before launching any attacks once deception efforts are deployed. In general, the more destructive a threat is, the greater cost it consumes. The attacker needs to balance the gain from attacking and the cost in learning and attacking. Accordingly, for a given threat j at a given target i, the attacker's utility is defined as the expected damage to the target subtracting the cost in terms of learning and launching attacks.

$$U_A(d, l, y) = f_A(P_{ji}\beta_{ji} - C_i - W_j), \tag{4}$$

where $P_{ji}\beta_{ji} - C_i - W_j$ is the total expected payoff on the attacker's side.

Herein, the attacker and defender utility functions $f(x)$ are assumed to be differentiable with the following properties: $f(x) = 0; f(x)' > 0$. In other words, both players' utility is nonnegative and increasing in total damage. Both players are allowed to be risk averse, risk neutral, or risk seeking, and we explore the implications of different risk preference levels in Section 4.2.3.

Let y^* be the attacker's best strategy in response to the defender's resource allocation. We try to minimize the defender's loss as

$$\min L_D(d, l, y^*) \tag{5}$$

$$s.t. \begin{cases} \sum_{i=1}^{I} d_i + l_i \le B \\ d_i, l_i \ge 0 \qquad \forall i \end{cases}, \tag{6}$$

where objective (5) focuses on minimizing the loss for the defender given the attacker's best strategy. Inequality (6) limits the amount of deception and defense resources spent in total and guarantees that the amount of resources used in each target is not negative.

As this is a sequential game where the defender moves first, based on which the attacker decides his own move. We assume that both players have complete information and are given full rationality. In other words, the best response for the attacker is to maximize his utility given the defender's possible resource allocations, as

$$y^* = \arg max_y U_A(d^*, l^*, y). \tag{7}$$

3 | EQUILIBRIUM SOLUTION

In this section, the definition of an equilibrium solution in a sequential model is given. In particular, we show how the subgame perfect nash equilibrium (SPNE) in this circumstance can be obtained by solving a transformed model. The pseudocode for the game-theoretic model is tabulated as well. Lastly, some lemmas are presented and explained.

Definition 1. A solution (d^*, l^*, y^*) is an equilibrium (SPNE) if and only if the following conditions are satisfied:

$$(d^*, l^*) = \arg \min_{(d,\, l)} L(d, l, \hat{y}(d, l)),\ y^* = \hat{y}(d^*, l^*), \tag{8}$$

where $\hat{y}(d, l)$ is the attacker's strategy that can maximize his utility given the defender's allocation strategy (d, l). Among all the pairs of $(d, l, \hat{y}(d, l))$, the defender finds the strategy (d^*, l^*) that results in the minimum loss for her. Then, $\hat{y}(d^*, l^*)$ is the corresponding attack strategy. At equilibrium, the loss and gain for the defender and attacker are $L_D(d^*, l^*, y^*)$ and $U_A(d^*, l^*, y^*)$, respectively.

To compute the SPNE for this two-stage game with perfect information, the game model can be transformed to

$$\min_{m=1,2,\ldots,M} \min_{(d,l)} L_D(d,l,y_m) \quad s.t. \begin{cases} U_A(d,l,y_m) \geq U_A(d,l,y_k) & \forall k = 1,2,\ldots,M \\ \text{other constraints on } d,\ l,\ \text{and } y \end{cases}. \tag{9}$$

As the attacker strategy is a combination of threats and targets, there are finitely many strategies (say M) for the attacker, and the attacker strategy must be pure. For each potential strategy y_m, the first condition in Equation 9 ensures that y_m is the attacker's response to the defender's resource allocation (d, l) that maximizes his gain. Then, we find the defender's best response that minimizes her loss, given that y_m is the attacker's best response, ie, $\min_{(d,l)} L_D(d,l,y_m)$. Subsequently, the above model can be solved for $k = 1, 2, \ldots, M$ to find the strategy that minimizes the defender's loss, ie, $\min_{m=1,2,\ldots,M} \min_{(d,l)} L_D(d,l,y_m)$.

A pseudocode is given below to compute the SPNE for the two players. At the outset, we list all the feasible combinations of threats and targets for the attacker. Then, for each feasible attacker strategy y_m, line 4 first calculates the best resource allocation strategy (d, l) that can result in the minimum loss for the defender, under the constraint that y_m is the attacker's best response resulting in the maximum gain for him. Given the current resource allocation (d, l) and y_m, the algorithm calculates the loss and gain for the defender and attacker, respectively. The minimum loss for the defender is updated through the cycle, as well as the gain for the attacker, and the strategies for both players. Finally, the outputs of the algorithm are the resource allocation strategy for the defender, the combinations of threats and targets for the attacker, along with the payoffs for both players.

Lemma 1. *An output from Algorithm 1 is an SPNE, due to the fact that* (d^*, l^*, y^*) *satisfy the two conditions of* (8).

Lemma 2. *A pure equilibrium solution must exist for this model.*

Algorithm 1. Solving for equilibrium solution

1: **Input**: input all related parameters, including I, J, α_{ji}, β_{ji}, k_i, λ_A, λ_D, W_j, and B;
2: **List all the feasible solutions for the attacker**: M ($M = I * J$) strategies exist for the attacker, denoted as y_m ($m = 1, 2, \ldots, M$);
3: **for** $m \leq M$ **do**
4: **Solve** $(d,l) = \arg\min_{d,l} L_D(d,l,y_m)$, *s.t.* $\sum_{i=1}^{I} d_i + l_i \leq B$, $y_m = \hat{y}(d,l)$, $d_i, l_i \geq 0$;
5: **Compute** $L = L_D(d,l,y_m)$, and $U = U_A(d,l,y_m)$, if one exists;
6: **if** $m = 1$, **then**
7: $L^* \leftarrow L; U^* \leftarrow U$;
8: $d^* \leftarrow d; l^* \leftarrow l; y^* \leftarrow y_m$;
9: **else**
10: **if** $L < L^*$ **then**
11: $L^* \leftarrow L; U^* \leftarrow U$;
12: $d^* \leftarrow d; l^* \leftarrow l; y^* \leftarrow y_m$;
13: **end if**
14: **end if**
15: **end for**
16: **return** d^*, l^*, y^*, L^*, U^*.

Proof. Based on Algorithm 1, the attacker's strategy is finite. In particular, given each defender's allocation strategy, there exists a maximum gain for the attacker. Both players have complete knowledge of the other's preference. That is, the defender can predict the attacker's strategy given her allocation strategy, which would, in turn, determine her own loss. Thus, there has to be a pure equilibrium solution for this model. In fact, the design of Algorithm 1 constitutes a sufficient condition for the existence of a local minimum. □

Note that if there is more than one strategy, which are indifferent to the attacker, we assume that the attacker would play certain strategy that is favorable for the defender as the defender could slightly alter her resource allocations to induce the attacker to follow her desired strategy.

Lemma 3. *The following conditions are necessary if* (d^*, l^*, y^*) *is an equilibrium solution.*

$$\begin{cases} U(d^*,l^*,y^*) \geq U(d^*,l^*,y) \\ \dfrac{dL(x^*,y^*)}{dx} = 0, x = (d^*,l^*) \\ \dfrac{d^2L(x^*,y^*)}{dx^2} > 0 \end{cases}. \tag{10}$$

Proof. The first condition satisfies Definition 1, and the last two represent the necessary conditions for the existence of a local minimum.

Lemma 4. *The defender is better off when the resource constraint* B *increases.*

Proof. Based on Definition 1, given each resource allocation (d, l), the attacker would choose the strategy $\hat{y}(d,l)$ to maximize his utility. Then, the defender would find the strategy resulting in the minimum loss for her among all pairs of $(d, l, \hat{y}(d,l))$. As B increases, more feasible allocation strategies exist for the defender from which she can choose. In other words, the optimal resource allocation under a lower resource constraint must be a feasible option for the defender under a higher resource constraint. Thus, the disutility for the defender under a higher resource constraint is no worse than that under a relatively lower resource constraint. □

Next, we present some theoretic results related with equilibrium solutions in the most general cases. To begin with, we give the definition of a tied attack.

Definition 2. Given two strategies y' and y'', assume that $\max U_A(d,l,\hat{y}(d,l)) = \max U_A(d^*,l^*,y') = \max U_A(d^*,l^*,y'')$. In other words, the defender allocates resources in such a way that the attacker is indifferent between more than one attack. Then, these two attacks are called tied attacks.

Corollary 1. *For a given threat* j, *the defender would allocate resources in defense on target* i *rather than deception as long as the defense resource is no greater than an allocation threshold.*

Proof. The resources spent in defense and deception can lower the probability of a successful attack and consume the attacker's learning cost, respectively. For a given threat j against a given target i, the marginal return to investing in defense can be obtained by differentiating the utility in terms of a successful attack. Similarly, the marginal

return to investing in deception can be derived by differentiating the utility in terms of the learning cost. Assume that these two marginal returns are equal, we have $\frac{\partial(e^{-\alpha_{ji}l}\times\beta_{ji})}{\partial l} = \frac{\partial(k_i d)}{\partial d}$. Solve this equation, we can get $\hat{l}_i = \ln \frac{k_i}{\alpha_{ji}\times\beta_{ji}}/(-\alpha_{ji})$. Thus, for any target i, the margin return in defense is greater than that in deception when $l < \hat{l}_i$. In other words, for a given threat j at any target i, the defender would not allocate resources in deception as long as $l_i < \hat{l}_i$. We call $\hat{l}_i$ as the allocation threshold in allocating resources between defense and deception on target i. Note that $\hat{l}_i$ is related with three other parameters as k_i, α_{ji}, and β_{ji}. The greater β_{ji} is, the greater $\hat{l}_i$ is. On the contrary, the greater α_{ji} or k_i is, the smaller $\hat{l}_i$ is. □

Corollary 2. *For a given scenario, the equilibrium resource allocation would result in two situations: (1) only one target having none-zero resource allocation or (2) a tied attack across certain targets with nonzero resource allocations.*

Proof. For the proof of this corollary, it would be easier to consider the resources as a whole, instead of differentiating between deception and defense resources. If there is no resource allocated on any target, the attacker could attack targets successfully with certainty. Then, targets can be indexed based on the attacker's expected utility from attacking different targets in descending order, denoted as target 1, target 2, and so on. Thus, target 1 is the most attractive one that could offer the highest utility for the attacker. The defender therefore should first allocate resources in this target to lower her loss. As this allocation process continues, the attacker's expected utility from attacking target 1 declines until the utility of attacking target 1 just equals the utility of attacking the second most attractive target (target 2). From now on, the defender must allocate resources in both targets 1 and 2 in such a way that the attacker's utilities of attacking these two targets are equal. Otherwise, the attacker would choose to attack certain targets that could produce higher utility for him. The defender continues allocating resources in this way until these two targets are no more attractive than target 3. This allocation process continues on and on until all resources are used up. Based on the above explanation, when there are insufficient resources, the first situation occurs in an equilibrium as all resources go to the most important target. Otherwise, the defender must divide resources in such a way that the attacker is indifferent to multiple attacks, as implied in the second situation. □

4 | ILLUSTRATIVE EXAMPLE

The following illustrative example illustrates the procedure for applying the proposed model to the problem. Additionally, comparative studies are carried out to show how the values for the parameters can affect the optimal strategies and the payoffs for both players.

4.1 | Basic model

Assume that an attacker wants to strike three potential targets to inflict damage. The attacker can choose from three different threats—destroying high buildings, paralyzing transportation, and attacking infrastructure—referred to as threat 1, threat 2, and threat 3, respectively. The three potential targets are one big city, one middle-sized town, and one small village, referred to as target 1, target 2, and target 3, respectively. The defender can deploy altogether $B = 100$ resources among targets. The attacker's unit costs of learning different targets are set as $k_1 = 0.4$, $k_2 = 0.6$, $k_3 = 0.5$, respectively. The costs of launching the three attacks are $W_1 = 4$, $W_2 = 5$, and $W_3 = 3$, respectively. The destructiveness of the damage and the coefficients associated with attack success probability are given in Table 2. Both players' risk preference levels are set as $\lambda_A = \lambda_D = 1$, ie, the utility function for both players is set as $f(x) = x^\lambda = x$. All target valuations and the costs are measured in millions of dollars. Note that these values are used for illustrative purposes and have no absolute meanings. In realistic applications, however, such parameters could be estimated based on historical data,[24] expert elicitation,[25] or experiments.[26]

After all these parameters have been obtained, we can use Algorithm 1 to obtain the equilibrium solution for both players. The

TABLE 1 Notations used in this paper

Parameters	
I	number of targets
J	number of threats
α_{ji}	coefficient denoting the effectiveness of attack j on target i
β_{ji}	destructiveness of damage caused by attack j on target i
k_i	unit cost of learning target i related with the deception efforts
λ_A	risk preference of the attacker
λ_D	risk preference of the defender
W_j	cost of launching threat j by the attacker
B	resource constraint for the defender
Functions	
$C(d)$	attacker's cost of learning, which depends on d
$P_0(l)$	probability of a successful attack on targets, which depends on l
$f(x)$	utility function
$L_D(d, l, y)$	expected disutility (loss) for the defender
$U_A(d, l, y)$	expected utility (gain) for the attacker
Decision variables	
d_i	deception effort used on target i by the defender, $0 \le d_i \le B$ $(i = 1, 2, \ldots, I)$
l_i	defense effort used on target i by the defender, $0 \le l_i \le B$ $(i = 1, 2, \ldots, I)$
y	strategy for the attacker

TABLE 2 Example parameters

	Coefficient α_{ji}			Destructiveness β_{ji}		
	Target I			Target I		
Threat J	1	2	3	1	2	3
1	0.15	0.1	0.2	75	80	65
2	0.1	0.08	0.12	80	90	70
3	0.08	0.05	0.1	70	70	60

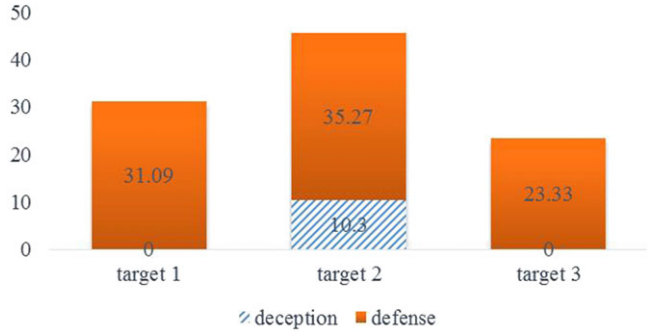

FIGURE 1 Resource allocation for the basic setting

TABLE 3 Payoffs for both players for the basic setting

Defender disutility				Attacker utility			
	Target 1	Target 2	Target 3		Target 1	Target 2	Target 3
Threat 1	0.71	2.35	0.61	Threat 1	−3.29	−7.83	−3.39
Threat 2	3.57	5.36	4.26	Threat 2	−1.43	−5.83	−0.74
Threat 3	**5.82**	12.00	**5.82**	Threat 3	**2.82**	**2.82**	**2.82**

defender's optimal resource allocation on each target, categorized by deception and defense efforts, is shown graphically in Figure 1. Note that the top part of each pillar denotes the defense resources allocated on each target, and the bottom part refers to the deception resources allocated on each target.

We can find that target 2 has the greatest level of protection in terms of both defense and deception because, unprotected, it would be the most valuable target for both players. By allocating nearly half of the resources on target 2, the attacker has to attack other targets instead of target 2 to maximize his own utility. In addition, the defender allocates no deception efforts on targets 1 and 3, as it would not be beneficial to allocate deception efforts owing to their marginal returns as Corollary 1 suggests.

The corresponding utilities for both players under the equilibrium solution are given in Table 3. Note that these values in Table 3 are meaningful when compared with each other. For instance, the defender would suffer less if the attacker uses threat 1 to attack target 1 compared with attacking target 2 as 0.71 <2.35. From the utilities tabulated in Table 3, we find that given the resource allocations as shown in Figure 1, the attacker could use threat 3 to attack either target, resulting in the same highest utility of 2.82. However, the defender is not indifferent between these three targets as the disutility varies. As explained in Lemma 2, we assume that under a tied-attack, the attacker would choose certain attacks that yield the smallest disutility for the defender. Otherwise, the defender could alter her resources slightly to induce the attacker toward her desired situation.

In this case, the defender is also indifferent between two targets (target 1 and target 3), leading to a disutility of 5.82. The tied attacks are shown in bold and shaded cells in the payoff tables. In other words, using threat 3 to attack either target 1 or 3 could result in the same utility (disutility) for the attacker (defender). The utility for each player is constant no matter what the attacker chooses, any mixed strategy included. Thus, the utility set for the two players in this case is (5.82, 2.82) for the equilibrium solution, where the first entry is the loss for the defender and the second is the gain for the attacker. Note that this solution is also used as a basis of comparison for each succeeding example.

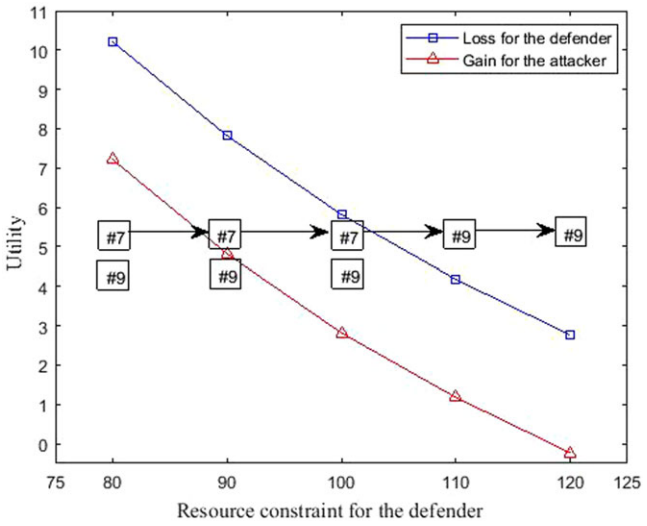

FIGURE 2 Equilibrium utilities and attack strategies under different resource constraints

4.2 | Sensitive analysis

To explore how the results of the proposed model depend on various parameters, comparative studies are carried out. More specifically, resource constraint for the defender, unit costs of learning targets, and players' risk preference levels are changed individually. We aim to determine how the strategies for the two players might vary in each scenario.

4.2.1 | Equilibrium under different resource constraints

Resource constraint is an important factor for the defender. When this constraint exists, the defender needs to balance the resources spent in deceiving the attacker and strengthening targets in order to minimize her disutility, which, in turn, affects the attacker's strategy. In this section, we change the resource constraint for the defender from 80 to 120 in increments of 10. The equilibrium utilities for both players under different resource constraints are depicted in Figure 2.

As B increases, the model produces less loss for the defender as $2.77 < 4.18 < 5.82 < 7.82 < 10.22$ (the corresponding disutilities for the defender when B varies from 120 to 80), whereas the gain for the attacker also decreases in different situations since $-0.23 < 1.18 < 2.82 < 4.82 < 7.22$ (utilities for the attacker when B varies from 120 to 80). When B is sufficient enough, it would not be beneficial for the attacker to implement any attacks as when B equals 120, in which case any attack would produce a negative utility for the attacker. As mentioned above, nine (3*3) possible combinations of attacks and targets exist for the attacker in this case, denoted as y_1 (using threat 1 to attack target 1), y_2 (using threat 1 to attack target 2), …, y_9 (using threat 3 to attack target 3). As Figure 2 shows, when B is less than 100, the attacker would either use strategy y_7 (using

TABLE 4 The equilibrium utilities and solutions for both players under different resource constraints

B metric	Target	*d*	*l*	Attacker strategy	Defender's expected disutility	Attacker's expected utility
80	Target 1	0	24.05	y_7 (y_9)	10.22	7.22
	Target 2	2.97	**35.27**			
	Target 3	0	17.70			
90	Target 1	0	27.39	y_7 (y_9)	7.82	4.82
	Target 2	6.96	**35.27**			
	Target 3	0	20.37			
100	Target 1	0	31.09	y_7 (y_9)	5.82	2.82
	Target 2	10.30	**35.27**			
	Target 3	0	23.33			
110	Target 1	2.06	32.99	y_9	4.18	1.18
	Target 2	13.04	**35.27**			
	Target 3	0	26.65			
120	Target 1	5.58	32.99	y_9	2.77	−0.23
	Target 2	15.39	**35.27**			
	Target 3	0	30.77			

threat 3 to attack target 1) or y_9 (using threat 3 to attack target 3). As *B* increases, the optimal attack strategy shifts to only y_9.

To more clearly study the trade-offs between the deception and defense efforts in different situations, we list the equilibria in different situations as *B* varies, as shown in Table 4. The defender allocates most resources on target 2, because this target is the most important to him, followed by target 1 and target 3. Meanwhile, the defender increases the deception resources on target 2 as *B* increases. Interestingly, we find that the defender allocates the same amount of defense resources (35.27, in this case) on target 2. This is because it would not be beneficial for the defender to allocate more defense resources on this target, as proven in Corollary 1. That is, the allocation threshold for target 2 between defense and deception is 35.27, which can be obtained using the following relation as $\ln \frac{k_2}{\alpha_{32}\times\beta_{32}}/(-\alpha_{32}) = \ln \frac{0.6}{0.05\times 70}/(-0.05) = 35.27$. The defender first cares more about strengthening the target than misleading the attacker on different targets before reaching the threshold. However, when the resource spent in defense reaches this threshold, the defender would begin to allocate resources in deception. The same situation occurs when the defense effort on target 1 reaches 32.99.

Note that as the resource constraint *B* increases, both the disutility for the defender and the utility for the attacker decrease. Especially when *B* is 120, the optimal utility for the attacker is negative (−0.23, in this case). As a reasonable player, the attacker would choose not to attack in this case. In fact, given more resources for the defender, more options (feasible allocation strategies) exist for her from which she can choose. Thus, any equilibrium for the defender under a higher resource constraint is no worse than that under a relatively lower resource constraint.

4.2.2 | Equilibrium under different unit costs of learning

To analyze the trade-off between defense and deception efforts, the attacker's unit cost of learning *k* changes, while the other parameters are fixed. We execute the model to obtain different solutions. The utilities and SPNE solutions for both players under different situations are tabulated in Table 5.

When *k* is low (k = [0.1 0.2 0.1]), the defender allocates all resources in defense among three targets, and the attacker is indifferent between three strategies in this case. As *k* increases, the defender allocates a certain amount of deception resources among these targets. More specifically, the defense resources on target 1 first increase and then decrease, whereas the deception resources on this target increase in *k*. As for target 2, the defense resources decrease, whereas the deception resources increase in *k*. As *k* increases, the threshold between allocating different resources in terms of defense and deception decreases. The defender allocates relatively the same amount of defense resources on target 3 in difficult situations as *k* increases, mostly because this target is the least important to both players. In a word, when *k* increases, the defender would allocate relatively less resources in defense, whereas more resources in deception. Both the defender's disutility and the attacker's utility decrease in *k* because the defender could benefit more by allocating more deception resources in misleading the attacker.

4.2.3 | Equilibrium under different risk preference levels

Player's risk preferences play an import role in the decision process. Based on utility theory, a player possesses risk aversion, risk neutral, or risk seeking if and only if the utility function is concave ($f'' < 0$), linear ($f'' = 0$), or convex ($f'' > 0$). Figure 3 shows different curves in terms of utility functions associated with different risk preference levels. When λ is less than 1, it denotes that the player is risk-averse; when λ equals 1, the player is risk neutral; and when λ is greater than 1, the player is risk seeking.

In the basic setting, both players are risk neutral toward targets. In this subsection, we focus on both players' risk preferences to see how they can affect the equilibrium results. λ_A and λ_D are set as 0.5,

TABLE 5 The equilibrium utilities and solutions for both players under different unit costs of learning

k metric	Target	*d*	*l*	Attacker strategy	Defender's expected disutility	Attacker's expected utility
[0.1, 0.2, 0.1]	Target 1	0	29.87	y_7 (y_8, y_9)	6.42	3.42
	Target 2	0	47.78			
	Target 3	0	22.35			
[0.2, 0.4, 0.3]	Target 1	0	30.01	y_7 (y_9)	6.34	3.34
	Target 2	4.14	43.38			
	Target 3	0	22.47			
[0.4, 0.6, 0.5]	Target 1	0	31.09	y_7 (y_9)	5.82	2.82
	Target 2	10.30	35.27			
	Target 3	0	23.33			
[0.6, 0.8, 0.7]	Target 1	4.09	27.92	y_9	5.04	2.04
	Target 2	13.70	29.52			
	Target 3	0	24.77			
[0.8, 1, 0.9]	Target 1	7.51	24.32	y_9	3.99	0.99
	Target 2	16.01	25.06			
	Target 3	0	27.10			

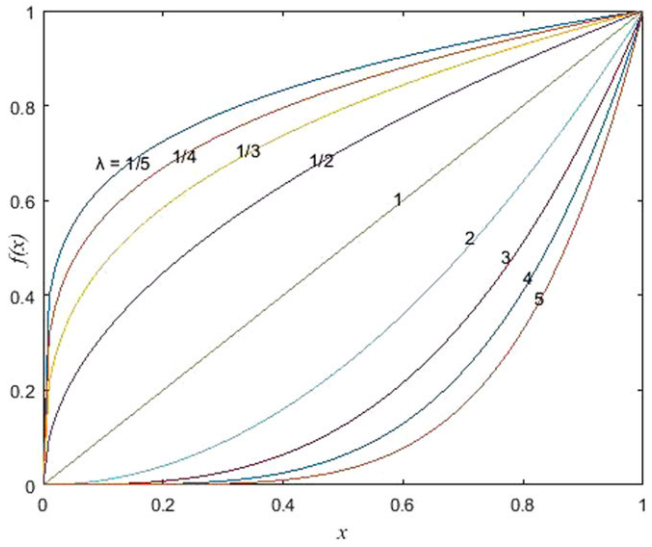

FIGURE 3 Utility functions with different risk preference levels

TABLE 6 The equilibrium utilities under different risk preferences

Scenario	λ_A	λ_D	Attacker strategy	Defender's expected disutility	Attacker's expected utility
Scenario 1	**0.5**	**0.5**	**y_7 (y_9)**	**2.41**	**1.68**
Scenario 2	0.5	1	y_7 (y_9)	5.82	1.68
Scenario 3	0.5	2	y_7 (y_9)	33.86	1.68
Scenario 4	**1**	**0.5**	**y_7 (y_9)**	**2.41**	**2.82**
Scenario 5	1	1	y_7 (y_9)	5.82	2.82
Scenario 6	1	2	y_7 (y_9)	33.86	2.82
Scenario 7	**2**	**0.5**	**y_7 (y_9)**	**2.41**	**7.94**
Scenario 8	2	1	y_7 (y_9)	5.82	7.94
Scenario 9	2	2	y_7 (y_9)	33.86	7.94

1, and 2, respectively, representing different risk preference levels. As for the first three scenarios in Table 6, assume that the attacker is risk-averse ($\lambda_A = 0.5$), changing the defender from being risk-averse to risk-seeking. The middle three scenarios denote that the attacker is risk-neutral, and the last three represent that the attacker is risk-seeking.

The attacker's optimal strategy and both players' equilibrium utilities under these nine scenarios are shown in Table 6. Interestingly, we find that both players' risk preference levels do not affect their equilibrium strategies, no matter whether they are risk-averse, risk-neutral, or risk-seeking. The reason could be that the alteration in λ could change the utility value of taking various strategies, but not the ordinal rankings of different strategies for both players. Thus, the attacker could either use strategy y_7 (using threat 3 to attack target 1) or y_9 (using threat 3 to attack target 3). As for the defender, her optimal strategy is the same as depicted in Figure 1, allocating a certain amount of deception resources on target 2 and most resources in defense among three targets. Fixing one of the player's risk preference level, we find that the defender's disutility increases in λ_D and the attacker's utility increases in λ_A. In addition, each player's risk preference level does not affect the other player's utility. Take scenarios 1, 4, and 7, for example, the defender's disutility is constant (2.41) under these three scenarios, but the attacker's utility increases from 1.68 to 7.94 as λ_A changes from 0.5 to 2.

The sensitivity analysis allows the evaluation of how the optimal solutions for both the defender and attacker can change with the parameters of the model. For example, the resource constraint is an important factor that can influence the equilibrium solutions for both players. Given limited resources, the defender should focus more on strengthening targets than misleading the attacker. Both players' risk preference levels do not affect the equilibrium solutions. However, it is worth pointing out that all these results and conclusions are based on

the hypothetical scenario and the values of the parameters used in this paper.

5 | CONCLUSIONS

Resource allocation is a crucial process in military and nonmilitary applications. Improper decisions could lead to a waste of resources or even unprecedented consequences to national interests. In this context, a game-theoretic model is proposed, aimed at resource allocation for both the defender and attacker. As an extension to existing models, we take into account the attacker's learning and defender's counter-learning (deception) efforts. The trade-off between deception and defense efforts for the defender is also investigated.

Our numerical results indicate that (1) a defender's resource allocation and an attacker's attack strategy are very sensitive to the values of the parameters. For example, the resource constraint is an important factor that can directly influence the solutions and payoffs for both players; (2) the equilibrium solution under a higher resource constraint is no worse than that under a relatively lower resource constraint; (3) the defender is better off allocating resources in defense among targets as long as the defense resources do not reach certain thresholds, whose value is highly related with the unit costs of learning targets; and (4) both players' risk preference levels do not affect the equilibrium strategies and their corresponding utilities. This study could provide military decision makers with more insights on: (1) how the equilibrium solution depends on various system parameters; and (2) how to carry out the trade-off between deception and defense for the defender; eg, the defender would know when she should increase (decrease) her defense (deception) effort to achieve certain goals.

Due to the characteristics of the model, it can also be extended to other negotiation and decision-making problems associated with multiple players, such as project scheduling, international conflict resolution, and multiattribute bilateral negotiations, in which cases the possibility of reaching agreements and "Win-Win" situations for two parties are allowed. An extensive literature has been devoted to this kind of problems in various fields. Thus, it should not be difficult to modify and extend our model by allowing for richer assumptions. Future research directions include considering uncertainty in player's preferences, allowing for nonadditive utilities and multiple attacker resources, and enabling dynamic resource distribution strategy over a time horizon. These challenges will certainly contribute to the expansion of this methodology for tackling a broader range of problems.

ACKNOWLEDGMENTS

This work was supported in part by the National Natural Science Foundation of China under Grants 71690233, 71501182, and 71571185. The authors would like to thank the editor and three anonymous referees for their constructive comments that helped us to improve the quality of this paper.

ORCID

Bingfeng Ge https://orcid.org/0000-0002-0331-7260

REFERENCES

1. Krause ME. The 9/11 Commission Report: Final report of the National Commission on terrorist attacks upon the United States. *Air Space Power J*. 2004;18:117–120.
2. Guan P, He M, Zhuang J, Hora SC. Modeling a multitarget attacker–defender game with budget constraints. *Decis Anal*. 2017;4:87–107.
3. Kujawski E. Accounting for terrorist behavior in allocating defensive counterterrorism resources. *Syst Eng*. 2015;18:365–376.
4. Golany B, Goldberg N, Rothblum U. A two-resource allocation algorithm with an application to large-scale zero-sum defensive games. *Comput Oper Res*. 2017;78:218–229.
5. Bai C, Sarkis J. Supplier development investment strategies: A game theoretic evaluation. *Ann Oper Res*. 2016;240:583–615.
6. Kujawski E. A probabilistic game-theoretic method to assess deterrence and defense benefits of security systems. *Syst Eng*. 2016;19:549–566.
7. Zhuang J, Bier VM. Balancing terrorism and natural disasters-defensive strategy with endogenous attacker effort. *Oper Res*. 2007;55:976–991.
8. Bier VM, Haphuriwat N, Menoyo J, Zimmerman R, Culpen AM. Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Anal*. 2008;28:763–770.
9. Golany B, Goldberg N, Rothblum UG. Allocating multiple defensive resources in a zero-sum game setting. *Ann Oper Res*. 2015;225:91–109.
10. Paulson EC, Linkov I, Keisler JM. A game theoretic model for resource allocation among countermeasures with multiple attributes. *Eur J Oper Res*. 2016;252:610–622.
11. Zhang L, Reniers G. A game-theoretical model to improve process plant protection from terrorist attacks. *Risk Anal*. 2016;36:2285–2297.
12. Zhang J, Zhuang J, Jose VRR. The role of risk preferences in a multi-target defender-attacker resource allocation game. *Reliabil Eng Syst Saf*. 2018;169:95–104.
13. Ding T, Yao L, Li F. A multi-uncertainty-set based two-stage robust optimization to defender-attacker-defender model for power system protection. *Reliabil Eng Syst Saf*. 2018;169:179–186.
14. Heydari B, Pennock MJ. Guiding the behavior of sociotechnical systems: the role of agent-based modeling. *Syst Eng*. 2018;21:210–226.
15. Kordova S, Katz E, Frank M. Managing development projects—the partnership between project managers and systems engineers. *Syst Eng*. 2018;21:1–16.
16. Reis A, Siddiqi A, de Weck O. Evolution stages of aircraft manufacturing firms. *Syst Eng*. 2019;22:1–16.
17. Tyson R, Browning EF, Negele H. Key concepts in modeling product development processes. *Syst Eng*. 2006;9:104–128.
18. Zhuang J, Bier VM. Reasons for secrecy and deception in homeland-security resource allocation. *Risk Anal*. 2010;30:1737–1743.
19. Hausken K, Levitin G, Protection V. False targets in series systems. *Reliabil Eng Syst Saf*. 2009;94:973–981.
20. Zhuang J, Bier VM, Alagoz O. Modeling secrecy and deception in a multiple-period attacker–defender signaling game. *Eur J Oper Res*. 2010;203:409–418.
21. Zhang C, Ramirez-Marquez JE, Li Q. Locating and protecting facilities from intentional attacks using secrecy. *Reliabil Eng Syst Saf*. 2018;169:51–62.
22. Xu J, Zhuang J. Modeling costly learning and counter-learning in a defender-attacker game with private defender information. *Ann Oper Res*. 2016;236:271–289.
23. Wang S, Shroff N. Security game with non-additive utilities and multiple attacker resources. *Proc ACM Meas Anal Comput Syst*. 2017;1:13.

24. Shan X, Zhuang J. Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game. *Eur J Oper Res*. 2013;228:262–272.
25. Wang C, Bier VM. Expert elicitation of adversary preferences using ordinal judgments. *Oper Res*. 2013;61:372–385.
26. Shan X, Zhuang J. Cost of equity in homeland security resource allocation in the face of a strategic attacker. *Risk Anal*. 2013;33:1083–1099.

AUTHORS' BIOGRAPHIES

Xiaoxiong Zhang received the BE degree in systems engineering and the ME and PhD degrees in management science and engineering from the National University of Defense Technology, Changsha, Hunan, China, in 2012, 2014, and 2018, respectively. He is currently an assistant professor of the Sixty-third Research Institute at the National University of Defense Technology. He was a visiting scholar with the Conflict Analysis Group, Department of Systems Design Engineering, University of Waterloo, Waterloo, ON, Canada. His current research interests include multiple-person, multiple-objective decision analysis including game theory.

Keith W. Hipel received the BASc degree in civil engineering, the MASc degree in systems design, and the PhD degree in civil engineering from the University of Waterloo, Waterloo, ON, Canada, in 1970, 1972, and 1975, respectively. He is currently a University Professor of systems design engineering with the University of Waterloo, where he is the Coordinator of the Conflict Analysis Group. He has authored or coauthored four books, 12 edited books, over 305 journal papers, as well as many conference and encyclopedia articles. His current research interests include the development of conflict resolution, multiple criteria decision analysis, time series analysis, and other decision-making methodologies for addressing complex system of systems engineering problems lying at the interface of science, technology, and the environment with application to water resources management, hydrology, environmental engineering, energy, and sustainable development.

Bingfeng Ge received the BE degree in systems engineering and the ME and PhD degrees in management science and engineering from the National University of Defense Technology, Changsha, Hunan, China, in 2006, 2008, and 2014, respectively. He is currently an associate professor of management science and engineering at the National University of Defense Technology. He was a visiting scholar with the Conflict Analysis Group, Department of Systems Design Engineering, University of Waterloo, Waterloo, ON, Canada. His research interests include system-of-systems architecting and engineering management, portfolio decision analysis, and conflict resolution. Dr. Ge is a Member of the IEEE Systems, Man, and Cybernetics Society, the IEEE Internet of Things Technical Community, and the International Council on Systems Engineering.

Yuejin Tan received the BE degree in the Department of Mathematics from Hunan Normal University, Changsha, China, in 1981, and the ME degree in the Department of System Engineering and Mathematics from National University of Defense Technology, Changsha, China, in 1985. He is currently a professor in College of Systems Engineering, National University of Defense Technology. His research interests include various areas such as robust, reliability, and comprehensive of complex networks; armament system of systems requirement analysis; and structure design. He has been awarded first-class prize of Military Technology Progress Award twice, secondary prize of Military Technology Progress Award seven times, secondary prize of National Teaching Achievement Award once, and secondary prize of provincial Teaching Achievement Award four times.

How to cite this article: Zhang X, Hipel KW, Ge B, Tan Y. A game-theoretic model for resource allocation with deception and defense efforts. *Systems Engineering*. 2019;22:282–291. https://doi.org/10.1002/sys.sys21479