Optimal preventive strike strategy vs. optimal attack strategy in a defense-attack game

Di Wu
School of Management
Xi'an Jiaotong University
Xi'an, China
wd_0824@stu.xjtu.edu.cn

Xiangbin Yan
Donlinks School of Economics and Management
University of Science and Technology Beijing
Beijing, China
xbyan@ustb.edu.cn

Rui Peng
School of Economics and Management
Beijing University of Technology
Beijing, China
pengruisubmit@163.com

Shaomin Wu
Kent Business School
University of Kent
Canterbury CT2 7FS, United Kingdom
S.M.Wu@kent.ac.uk

Kaiye Gao*
School of Economics and Management
Beijing Information Science & Technology University
Beijing, China
gaokaiye1992@qq.com

***Abstract*—This paper analyzes an attack-defense game between one defender and one attacker. Among, the defender moves first and allocates its resources to three different methods: employing a preventive strike, founding false targets, and protecting its genuine object. The preventive strike may expose the genuine object, and different from previous literature, a false target may also be detected to be false. The attacker, observing the actions taken by the defender and allocating its resources to three methods: protecting its own base from the preventive strike, founding false bases, and attacking the defender's genuine object. Similarly, a false base may be correctly identified. Different from previous methods in evaluating the potential outcome, for each of the defender's given strategies, the attacker tries to maximize its cumulative prospect value considering different possible outcomes. Similarly, the defender maximizes its cumulative prospect value, assuming that the attacker chooses the strategy to maximize the attacker's cumulative prospect value. Numerical examples are presented to illustrate the optimal number of bases to attack by preventive strike, and the optimal number of targets to attack by attacker.**

Keywords- Imperfect false target; preventive strike; vulnerability; attack-defense game; cumulative prospect

I. INTRODUCTION

Launching preventive strike and deploying false targets are two efficient methods for the defense of genuine objects against intentional attacks. Recently, more publications have started considering the attacker's risk attitude and analyzing the cases where both the attacker and the defender allocate different resource on different strategies [1], [2], [3]. The defender may employ the strategies of preventive strike to gain the initiative, use false targets to distract the attention of the attacker, and protect the genuine object to reduce its vulnerability in case it is attacked. The attacker, in response, may protect its base against preventive strike, deploy false bases to distract the defender, and attack the defender's genuine object. The vulnerability of the attacker's base and the defender's genuine object is usually characterized by the Tullock model in an attack-defense game [4]. One common assumption of the existing work is that employing preventive strike will expose the true object and thus there is no need to deploy false targets in case the preventive strike strategy is applied. In reality, nevertheless, the defender may choose to launch preventive strike from a location different from where the genuine object is located or even require a third party to launch the preventive strike. As a result, the genuine object may be exposed only with some probability and deploying false targets may still be an effective strategy.

In this paper, we consider the employment of both preventive strike and false targets (i.e., camouflages). It assumes that the preventive strike may expose the genuine object with some probability. In addition, a false target is assumed imperfect in the sense that it may be detected. While the defender may launch a preventive strike, protect the genuine object, or deploy false targets, the attacker may protect its genuine base against preventive strike, deploy false bases, or

National Nature Science Foundation of China(71671016)

launch attacks aiming to destroying the defender's genuine object. There may therefore be three different outcomes of the contest: 1) the attacker's base is destroyed by a preventive strike; 2) The attacker's genuine base survives a preventive strike, and the defender's genuine object also survives the attacker's attack; 3) The attacker's genuine base survives a preventive strike and successfully destroys defender's genuine object. We should further note that once the base is destroyed by the preventive strike, the attacker cannot attack the object. In order to consider both the defender's and the attacker's risk attitudes, the Cumulative Prospect Theory (CPT) is used to calculate their cumulative prospect value of both parties considering all possible outcomes of the contest [5]. Typically, the defender moves first with the aim to maximize its cumulative prospect value, assuming that the attacker maximizes its own cumulative prospect value for any defender's strategy. The major contributions of this paper conclude: 1) the false target of the defender and the false base of the attacker may be correctly identified; 2) the cumulative prospect value is employed to evaluate the potential outcome of both the defender and the attacker. Section 2 presents the general model for solving the optimal defense and attack strategies. Section 3 presents numerical examples to illustrate the optimal number of attacks bases by preventive strike, and the optimal number of attacked targets by attacker. Section 4 concludes.

II. THE MODEL

Consider a defender who owns a single genuine object subjected to intentional attacks by an attacker. The defender distributes its resource r into three different measures: $rx(0 \le x \le 1)$ for preventive strike with unit strike effort cost c_{ps}, $r(1-x)y(0 \le y \le 1)$ for building false targets with unit cost c_{ft}, and $r(1-x)(1-y)$ for protecting the genuine object with unit protection effort cost c_{pt}. The attacker also distributes its resource on three measures: $RX(0 \le X \le 1)$ for protecting its own base from the preventive strike with unit protection effort cost C_{bp}, $R(1-X)Y(0 \le Y \le 1)$ for building false bases with unit cost C_{fb}, and $R(1-X)(1-Y)$ for attacking the genuine object with unit attack effort cost C_{at}. The probability of correctly detecting a false target is denoted by d_{ft}, whereas the probability of correctly detecting a false base is denoted by D_{fb}.

In an attack-defense game considering perfect information, the defender takes action first and the attacker moves only after observing the resource allocation of the defender. Specifically, the CPT is used and both the defender and the attacker are assumed to try to maximize their own respective cumulative prospect by considering different possible outcomes in this paper. That is, the attacker chooses its attack strategy to maximize its cumulative prospect value for any given defense strategy; and the defender maximizes its cumulative prospect value anticipating that the attacker always chooses the attack strategy to maximize the attacker's cumulative prospect value. It is assumed that the preventive strike may uncover its genuine object with a probability d_{ex}.

As the attacker deploys false bases, the defender will distribute its preventive resource evenly into Q_d ($1 \le Q_d \le \lfloor R(1-X)Y / C_{fb} \rfloor + 1 - k_{fb}$) bases to maximize the vulnerability of the genuine base in case where k_{fb} false bases are detected to be false. The vulnerability of the genuine base can be modeled by the contest success function proposed by Tullock given the attacked bases:

$$\tilde{v_b} = \frac{\left(rx / Q_d c_{ps}\right)^{m_p}}{\left(RX / C_{bp}\right)^{m_p} + \left(rx / Q_d c_{ps}\right)^{m_p}}, \quad (1)$$

Among, m_p is the contest intensity of the game, the numerator represents the contest effort the defender takes, and $\left(RX / C_{bp}\right)$ denotes the contest effort of the attacker by considering base protection. Further, we should note that the contest intensity is assumed to be exogenous since it relies on the behavior of neither the attacker nor the defender.

As such, the vulnerability of the base given that k_{fb} false bases are detected is

$$v_b(Q_d, k_{fb}) = \frac{Q_d}{\lfloor R(1-X)Y / C_{fb} \rfloor + 1 - k_{fb}} \times \tilde{v_b}. \quad (2)$$

The fraction in Eq. (2) illustrates the ratio of the attacked bases to the undetected bases, and the defender chooses $Q_d^*(k_{fb}) = \arg\max(v_b(Q_d, k_{fb}))$.

Since the probability of correctly detecting k_{fb} false bases is

$$p_{fb}(k_{fb}) = \begin{pmatrix} \left\lfloor \frac{R(1-X)Y}{C_{fb}} \right\rfloor \\ k_{fb} \end{pmatrix} D_{fb}^{\,k_{fb}} (1 - D_{fb})^{\left\lfloor \frac{R(1-X)Y}{C_{fb}} \right\rfloor - k_{fb}}, \quad (3)$$

the unconditional vulnerability of the base is

$$v_b(Q_d, k_{fb}) = \sum_{k=0}^{\left\lfloor \frac{R(1-X)Y}{C_{fb}} \right\rfloor} p_{fb}(k_{fb}) v_b(Q_d^*(k_{fb}), k_{fb}). \quad (4)$$

In the case where the base of the attacker survives the preventive strike, the attacker will try to destroy the genuine object of the defender. Considering that the genuine object may (or may not) be uncovered by the preventive strike, the vulnerability of the genuine object can be obtained by

$$v_g = (1-v_b(Q_d^*))[d_{ex} \frac{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a}}{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a}+\left(r(1-x)(1-y)/c_{pt}\right)^{m_a}} + (1-d_{ex}) \sum_{0}^{\left\lfloor \frac{r(1-x)y}{c_{ft}} \right\rfloor} p_{ft}(k_{fb}) v_g(Q_a^*(k_{fb}), k_{fb})], \quad (5)$$

where $(1-v_b(Q_d^*))$ is the survival probability of the attacker, and $\frac{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a}}{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a}+\left(r(1-x)(1-y)/c_{pt}\right)^{m_a}}$ is the destruction probability of the genuine object in case where it is exposed by the preventive strike. In addition, the probability to detect k_{ft} as false targets is

$$p_{ft}(k_{ft}) = \begin{pmatrix} \left\lfloor \frac{r(1-x)y}{c_{ft}} \right\rfloor \\ k_{ft} \end{pmatrix} d_{ft}^{\,k_{ft}} (1-d_{ft})^{\left\lfloor \frac{r(1-x)y}{c_{ft}} \right\rfloor - k_{ft}}, \quad (6)$$

and

$$v_g(Q_a(k_{ft}), k_{ft}) = \frac{Q_a(k_{ft})}{\lfloor r(1-x)y/c_{ft} \rfloor + 1 - k_{ft}} \cdot \frac{\left(R(1-X)(1-Y)/Q_a^*(k_{ft})C_{at}\right)^{m_a}}{\left(R(1-X)(1-Y)/Q_a^*(k_{ft})C_{at}\right)^{m_a}+\left(r(1-x)(1-y)/c_{pt}\right)^{m_a}} \quad (7)$$

is the vulnerability of the genuine object if k_{ft} false targets are detected and $Q_a^*(k_{ft})$ is the $Q_a(k_{ft})$ that maximizes $v_g(Q_a(k_{ft}), k_{ft})$ and m_a is the contest intensity.

For any given defender's and attacker's resource allocation and a given number of detected false bases, the defender will choose the optimal number of bases to attack in order to maximize the base destruction probability. In addition, for any given defender's and attacker's resource allocation, the attacker always chooses the optimal number of targets to attack in order to maximize the destruction probability of the defender's object, given any number of false targets detected and that the attacker survives the preventive strike. Nonetheless, for a given defense strategy, the attacker chooses its resource allocation strategy to maximize its cumulative prospect value considering all possible outcomes of the contest, including: 1) its base is destructed; 2) its base survives and the genuine target of the defender is not destructed too; 3) its bases survives and the defender's genuine target is destructed. The attacker's monetary outcomes corresponding to the three possible outcomes of the contest are denoted as x_{a1}, x_{a2} and x_{a3}, respectively. Moreover, the defender chooses its resource allocation strategy in order to maximize its cumulative prospect value, given that the attacker always chooses the attacking strategy to maximize the attacker's cumulative prospect value. Similar to the attacker, the defender's monetary outcomes corresponding to the above mentioned three possible outcomes of the contest are denoted as x_{d1}, x_{d2} and x_{d3}, respectively. The probabilities for the three outcomes of the contest are denoted as p_1, p_2 and p_3. Thus, the prospect value of each party is given by

$$V_a = \sum_{k=a_3} v(x_k)\pi_k^+ + \sum_{k=a_1,a_2} v(x_k)\pi_k^-; \quad (8)$$

$$V_d = \sum_{k=d_1,d_2} v(x_k)\pi_k^+ + \sum_{k=d_3} v(x_k)\pi_k^-, \quad (9)$$

respectively, where $v(x_k)$ is the value of the possible outcome of the game, π_k^+ is the specific weight for the value of the potential gain, and π_k^- is the specific weight for the value of the potential loss. According to [5] and [6], $v(x_k)$ can be represented by

$$v(x_k) = \begin{cases} x_k{}^g & x_k > 0, \\ -\lambda(-x_k)^l & otherwise, \end{cases} \quad (10)$$

Among, parameters g and l are exponential and λ is further denoted as the loss parameter. Moreover, the loss-aversion factor λ should be always greater than or equal to one since the individuals are essentially more sensitive to losses than gains. On the other hand, the decision weights for the payoffs can be expressed by

$$\pi_k^+ = w^+(\sum_{j=k}^{n} p_j) - w^+(\sum_{j=k+1}^{n} p_j); \quad (11)$$

$$\pi_k^- = w^-(\sum_{j=1}^{k} p_j) - w^-(\sum_{j=1}^{k-1} p_j), \quad (12)$$

respectively, where w^+ and w^- represent the weighting functions for specific values, respectively. They are represented by

$$w^+(p) = \frac{p^\chi}{[p^\chi + (1-p)^\chi]^{1/\chi}}, \quad (13)$$

and

$$w^-(p) = \frac{p^\delta}{[p^\delta + (1-p)^\delta]^{1/\delta}}, \quad (14)$$

where both χ and δ are model parameters and can also be estimated through experiments. Note that $w^+(p)$ and $w^-(p)$ are monotonic and exhibit inverse S-shapes for some specific ranges [7].

Throughout our deduction and model foundation, it is easy to find that

$$p_1 = v_b(Q_d^*), \quad (15)$$

$$p_2 = 1 - v_b(Q_d^*) - v_g\left(X^*, Y^*\right), \tag{16}$$

$$p_3 = v_g\left(X^*, Y^*\right). \tag{17}$$

In reality, it is reasonable to assume that $x_{a1} < 0 < x_{a3}$ and $x_{d3} < 0 < x_{d1}$. However, it is hard to say whether x_{a2} and x_{d2} are positive or not and we will discuss different cases to obtain the optimal strategies. We can then rewrite the function of prospect value of each party as

$$V_a = \begin{cases} {x_{a3}}^g \pi_3^+ - \lambda(-x_{a2})^l \pi_2^- - \lambda(-x_{a1})^l \pi_1^-, & x_{a2} < 0 \\ {x_{a3}}^g \pi_3^+ - \lambda(-x_{a1})^l \pi_1^-, & x_{a2} = 0, \\ {x_{a3}}^g \pi_3^+ + {x_{a2}}^g \pi_2^+ - \lambda(-x_{a1})^l \pi_1^-, & x_{a2} > 0 \end{cases} \tag{18}$$

$$V_d = \begin{cases} {x_{d1}}^g \pi_1^+ + {x_{d2}}^g \pi_2^+ - \lambda(-x_{d3})^l \pi_3^-, & x_{d2} > 0 \\ {x_{d1}}^g \pi_1^+ - \lambda(-x_{d3})^l \pi_3^-, & x_{d2} = 0. \\ {x_{d1}}^g \pi_1^+ - \lambda(-x_{d2})^l \pi_2^- - \lambda(-x_{d3})^l \pi_3^-, & x_{d2} < 0 \end{cases} \tag{19}$$

For any given (x, y), the attacker chooses its decision variables $(X^*, Y^*) = \arg\max(V_a)$. The defender chooses $(x^*, y^*) = \arg\max(V_d(X^*, Y^*))$.

III. Optimal Numbers of Bases and Targets to Attack

Due to space limit, we only illustrate the optimal numbers of bases and targets to attack. In particular, we use the same parameters setting as those in [8] as:

$$r = R = 10, C_{bp} = C_{fb} = C_{at} = c_{ps} = c_{ft} = c_{pt} = 2, m_p = m_a = 2, D_{fb} = d_{ft} = d_{ex} = 0.5.$$

We first analyze the optimal number of attacked bases of the defender. To avoid the tedious calculation, here we only consider two different values for each decision parameter: 0.3 for low resource allocation and 0.7 for high resource allocation. In the calculation of attacked bases, the related decision parameter of the defender is the portion of resource spent on preventive strike and the related decision parameters of the attacker are the portions of resources spent on protection and false bases, which makes eight possible cases.

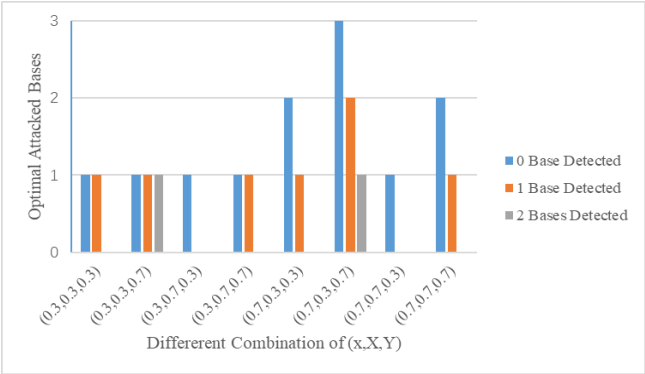

Figure 1. Optimal Attacked Bases under Different Combination of (x, X, Y)

With different possible numbers of detected bases, we perform the optimal number of attacked bases for the defender in the Fig. 1. From Fig. 1, one can find that only when the resource of the defender spent on preventive strike is high and the resource of the attacker spent on false bases deployment is high $(x, X, Y) = (0.7, 0.3, 0.7)$, the optimal number of attacked bases will reach three if no false bases are detected to be false. Actually, in this case, the amount of resource spent on false bases deployment is $R(1-X)Y = 4.9$. Given that the unit cost for each false base is 2, the attacker is able to deploy 2 false bases. Since the defender spends 70% of its resource for preventive strike, it has enough resource to attack all the three bases, one genuine base and two false bases, if no false base is detected to be false. On the other hand, when the defender's resource allocated into preventive strike is low ($x = 0.3$), it always attacks one base no matter how many false bases are deployed by the attacker. Actually, when the resource spent on preventive strike is low, further spreading the resources on multiple bases would lead to a low strike effort on each base under strike. Thus, even the genuine base is under strike, it is difficult to destroy it.

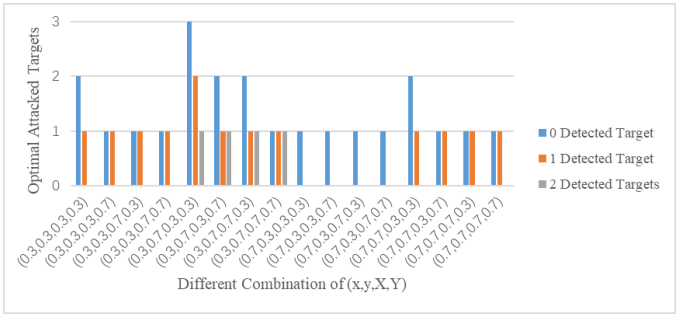

Figure 2 Optimal Number of Attacked Targets under Different Combination of (x, y, X, Y)

Similarly, we obtain the optimal number of attacked targets by the attacker under different combinations of resource allocation and different numbers of detected false targets. The results are as shown in Fig. 2. It can be seen that, only for the case (0.3, 0.7, 0.3, 0.3), the number of attacked targets reaches three given that no false targets are detected. In fact, the amount of resource spent on deploying false targets is $r(1-x)y = 4.9$ in this case, which means that two false targets are deployed. On the other hand, the amount of resource

spent on attack by the attacker is $R(1-X)(1-Y)=4.9$, which is almost half of the attacker's resource. Thus, even no false targets are detected to be false, the attacker has enough resource to attack all the three targets, one genuine object and two false targets. It can also be seen that, when $x=0.7$, the number of attacked targets is almost always 1 except for (0.7, 0.7, 0.3, 0.3). In fact, when *x* is big, the amount of resource left for false targets deployment is low. In case $y=0.3$, the resource left for false targets deployment is $r(1-x)y=0.9$, which is not enough for even a single false target. Thus, the attacker only needs to focus on the genuine object. In case $y=0.7$, the resource left for false targets deployment is $r(1-x)y=2.1$, which is just enough for a single false target. For the case (0.7, 0.7, 0.3, 0.3), the attacker's resource on attack is $R(1-X)(1-Y)=4.9$. Thus, the attacker can afford to attack both the genuine object and the false targets. For the three different cases (0.7,0.7,0.3,0.7), (0.7,0.7,0.7,0.3), (0.7,0.7,0.7,0.7), the attacker's resources on attack are respectively 2.1, 2.1, 0.9. For these cases, focusing on one target gives the attacker a big chance to destroy the defender's object.

IV. Conclusions and Future Research

In this study, we analyze the optimal attacked objects. The defender may choose to protect the genuine object, set up false targets, and employ preventive strike. Similarly, the attacker may choose to protect genuine base, set up false bases, and employ attack after surviving the preventive strike. A preventive strike may expose its own genuine object. To be more general, the false targets/bases are imperfectly camouflaged in the sense that they may be detected by the attacker/defender. By employing cumulative prospect theory, we consider players' risk attitude in the traditional Tullock model, which provides a better depiction of the behavior of both parties under different risk parameters. Numerical examples are presented to illustrate the methods.

This work can be further extended in the future. First, the optimal attack and defense strategy could be obtained through backward induction. Since the theoretical solution is hard to obtained, people can perform the characteristic of the solution by employing simulation. Sensitivity analysis should also be conducted on the risk parameters.

Acknowledgment

The research was supported by the National Nature Science Foundation of China under grant numbers 71671016.

References

[1] G. Levitin, and K. Hausken, "Resource distribution in multiple attacks against a single target." Risk. Anal, vol.30(8), pp.1231-1239, August 2010.

[2] G. Levitin, and K. Hausken, "Defense resource distribution between protection and redundancy for constant resource stockpiling pace." Risk. Anal, vol.31(10), pp.1632-1645, October 2011.

[3] R. Peng, G. Levitin, M. Xie, and S. H. Ng, "Optimal defense of single object with imperfect false targets."" J. Oper. Res. Soc, vol.62(1), pp.134-141, January 2011.

[4] G. Tullock. "Efficient Rent Seeking". Springer, Boston, MA. 2011.

[5] Y. Liu, Z. P., Fan, and Y. Zhang, "Risk decision analysis in emergency response: A method based on cumulative prospect theory." Comput Oper Res, vol.42(2), pp.75-82, February 2014.

[6] Z. Wang, R. Y. K. Fung, Y. L. Li, and Y. Pu, "An integrated decision-making approach for designing and selecting product concepts based on QFD and cumulative prospect theory." Int. J. Prod. Res, vol.7, pp.1-16, December 2017.

[7] A. Jamshidi, S. Faghihroohi, Hajizadeh S, A. Nunez, R. Babuska, R. Dollevoet, Z. L. Li, and B. De Schutter, "A Big Data Analysis Approach for Rail Failure Risk Assessment." Risk. Anal, vol.37(8), pp.1495-1507, August 2017.

[8] D. Wu, H. Xiao, and R. Peng, "Object defense with preventive strike and false targets." Reliab. Eng. Syst. Safe, vol.169, pp.76-80, January 2018.