Reliability Engineering and System Safety 169 (2018) 76–80

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Object defense with preventive strike and false targets

Di Wu [a], Hui Xiao [b], Rui Peng [a,*]

[a] Donlinks School of Economics & Management, University of Science & Technology Beijing, Beijing, China
[b] School of Statistics, Southwestern University of Finance and Economics, Chengdu, China

ARTICLE INFO

Keywords:
Defense
False target
Intentional impact
Optimal strategy
Preventive strike
Vulnerability

ABSTRACT

In this paper, optimal strategies for the defender and the attacker are studied. The defender moves first, allocating its limited resources into three diverse measures: launching a preventive strike, building false targets, and protecting the genuine object. It is assumed that launching a preventive strike will expose the genuine object, thus during this measure the defender will not simultaneously build false targets. The attacker moves after observing the actions taken by the defender, allocating its resources into three measures: protecting its own base from a preventive strike, building false bases, and attacking the genuine object. For each of the defender's given strategies, the attacker tries to maximize the destruction probability of the genuine object. Comparing the expected vulnerability of the object, the defender decides whether to launch a preventive strike or build false targets. The strategies of the attacker and the defender are illustrated with numerical examples, and the optimal strategies are found.

1. Introduction

Defense strategies against intentional impacts have attracted tremendous attention, in order to enhance the system survivability [1,2]. In the case of defending a single object against a strategic attacker, protecting the genuine object and deploying false targets are two effective methods [3]. Since the attacker can always observe the defender's investment in security and adapt its choice of strategy accordingly, game theory is one of the most effective methods to analyze this kind of problem [4]. Numerous studies have concentrated on the optimal strategy for the attack-defense contest from different perspectives. For example, in [5], game theory was applied to identify the equilibrium strategies for both the attacker and the defender in a fully endogenous model of resource allocation, [6] employed the game-theoretic analysis into cyber-physical network infrastructures, and [7] considered a system against intentional attacks in a two-stage game with incomplete information.

Many researchers have studied the tradeoff between the protection of genuine system elements and the deployment of false targets [8–10]. [11] also analyzed the efficiency of deploying false targets, and obtained the optimal number of false targets and attacked objects. [3] further studied the optimal tradeoff where the false targets are imperfect. A defense system with variable attackers was studied in [12]. [13] introduced the false target concept in a Markov game and used the new model to solve the attack-defense of power networks under possible misinformation. [14] considered a system combining genuine elements and objects that cannot be distinguished or detected by the attacker's observation. [15] incorporated a risk-seeking attitude into the false target defense strategy and solved the optimal resource allocation in this case. [16] considered the foundation of the detection system that can be used by the attacker to detect the real object. [17] studied the cases where the attacker tries to detect a subset of false targets. [18] introduced this concept in multiple cyber-attacks and discussed the characterization and optimization of an object with observation errors.

Nonetheless, in some cases, the defender may attempt to destroy the attacker's base preventively – to neutralize the threat of being attacked – instead of defending passively using genuine object protections and false targets. [19] analyzed the balance between protecting an object and striking preventively against an attacker seeking to destroy the object. [20] focused on a T-period game. [21] conducted a survivability quantitative analysis and [22] concentrated on the perverse effects on counterterrorism. [12] and [23] discussed mixed strategies between a preventive strike and protections in an attack-defense game. [24] presented a two-stage game where the emphasis is on the interaction between the preemptive and defensive measures. Their 'preemptive measure' is synonymous with our term 'preventive strike' . [25] considered the resource allocation between offense and defense in a duel where two participants exchange attacks in each round. See [26] for a comprehensive review on several defensive strategies applied in system attack-defense problem. [27] formulated the attack-defense scenario as a mathematical model where the defender applies both proactive and reactive defense mechanisms against the attacker. [28] proposed an algorithm considering external attacks and self-defense to solve the optimization problem of the

* Corresponding author.
E-mail address: pengrui1988@ustb.edu.cn (R. Peng).

http://dx.doi.org/10.1016/j.ress.2017.08.006
Received 10 April 2017; Received in revised form 30 July 2017; Accepted 3 August 2017
Available online 5 August 2017
0951-8320/

resource management system in grid computing systems. See [29] for some real cases that occurred in Iran. However, although these research works concentrated on the preventive strike, none of them considered the strategy of deploying false targets. In another stream of literature, [23,30,31] have considered preventive strike and false targets together, however, they just allow the defender to deploy false targets. In practice, the attacker may also deploy some false bases to distract the defender in case it launches preventive strike. For a real life example, imagine that when a group of bomber jets perform a task to blow down a military facility, the radar may detect their track and use antiaircraft missiles in order to destroy them. For the attacker, there may be only one jet carrying the bomb which can cause the greatest damage. Therefore, the other jets in the group can be taken as the false bases to reduce the vulnerability of the genuine base, in other words, the jet carrying the bomb. Moreover, the anti-radar system can be considered as the protection of the genuine base.

In this paper, the defense of a single object is studied, where the defender can choose between the strategies of striking preventively or deploying false targets. In response, the attacker can allocate part of its resources into protecting its own base against the preventive strike and building some false bases to distract the preventive strike. The behavior of the defender and the response of the attacker are studied. In the literature, [30,31] analyzed how a defender determines a balance between defending an object passively and striking preventively against an attacker equipped with one or more attack facilities for the sake of destroying the base of the attacker. In their following work, [23] assumed that the attacker cannot distinguish the genuine object, and the defender determines the balance between striking preventively and deploying false targets to distract the attacker. We address the scenario where the attacker can also build false bases to distract the defender's preventive strike effort away from the genuine base. By considering the false bases, we model each participant of the game with three analogous strategies: building false targets or bases, protecting the genuine object or base, and attacking the other side (which is known as a preventive strike for the defender and an attack for the attacker).The extension is meaningful since, if the defender can put some effort into building false targets, the attacker, in practice, may also build false bases.

The rest of this paper is organized as follows. In Section 2, we describe the model. In Sections 3 and 4, the optimal strategies are solved for the respective scenarios of launching a preventive strike and deploying false targets. In Section 5, we make it flexible to the defender whether to initiate a preventive strike or build false targets, and solve the optimal strategies. Sensitivity analysis is also performed to show the influence of different parameters. Section 6 provides our conclusions and gives possible directions for future work.

2. The model

Consider a single genuine object subjected to intentional attacks. The defender distributes its resource r into three different measures: rx for preventive strike, $r(1-x)y$ for building false targets, and $r(1-x)(1-y)$ for protecting the genuine object. The attacker also distributes its resource into three measures: RX for protecting its own bases from the preventive strike, $R(1-X)Y$ for building false bases, and $R(1-X)(1-Y)$ for attacking the genuine object. The false targets are assumed to be perfect and cannot be detected by the opponent.

The cost of each false target for the defender is c_{ft}, whereas the cost for each false base for the attacker is C_{fb}. The cost of unit effort for a preventive strike is c_{ps}, whereas the cost of unit protection effort is c_{pt}. The cost of unit effort for base protection is C_{bp}, whereas the cost of unit attack effort is C_{at}.

In this two-period game of perfect information, the defender moves first and the attacker moves only after knowing the resource allocation of the defender. In this game, the most conservative strategy of the defender is studied. That is, the defender always assumes the attacker to use the most harmful strategy and the defender makes its reaction based on the attacker's optimal strategy. It is assumed that the defender will expose its genuine object if a preventive strike is made. Thus, the defender will not simultaneously choose to initiate a preventive strike and deploy false targets. If the preventive strike is chosen by the defender, it does not waste resources on false targets, and $y=0$. As the attacker uses false bases, the defender distributes its preventive strike effort evenly into Q_d $(1 \le Q_d \le \lfloor R(1-X)Y/C_{fb} \rfloor + 1)$ bases to maximize the vulnerability of the genuine base, where $Q_d = \lfloor R(1-X)Y/C_{fb} \rfloor$ is the number of attacked bases. The vulnerability of the genuine base, given it is in the Q_d attacked bases, can be modeled by the contest success function [32]:

$$\upsilon_{1b}^{\sim} = \frac{\left(rx/Q_d c_{ps}\right)^{m_p}}{\left(RX/C_{bp}\right)^{m_p} + \left(rx/Q_d c_{ps}\right)^{m_p}} \tag{1}$$

where mp is the contest intensity, $(rx/Q_d c_{ps})$ represents the contest effort the defender takes by spending the corresponding resources on a preventive strike, and (RX/C_{bp}) denotes the contest effort of the attacker in base protection. The contest intensity here is an exogenous variable which does not rely on the action of the attacker nor the defender. In fact, the contest intensity derived from the history of warfare, represents the impact on the vulnerability, where low intensity occurs if neither players can get a significant advantage and high intensity results from the enormous difference between the participants. When $0<m<1$, exerting more effort than one's opponent gives less advantage. When $m=1$, the efforts remain proportional impact on the vulnerability. When $m>1$, exerting more effort than one's opponent gives more advantage. And $m=\infty$ will result in a winner-takes-all situation [32].

Therefore, the unconditional vulnerability of the base is

$$\upsilon_{1b} = \frac{Q_d}{\lfloor R(1-X)Y/C_{fb} \rfloor + 1} \times \frac{\left(rx/Q_d c_{ps}\right)^{m_p}}{\left(RX/C_{bp}\right)^{m_p} + \left(rx/Q_d c_{ps}\right)^{m_p}}. \tag{2}$$

The defender chooses $Q_d^* = \arg\max(\upsilon_{1b}(Q_d))$. The first term of the right side in equation illustrates the ratio between attacked bases and founded bases.

The vulnerability of the genuine object is

$$\upsilon_{1g} = (1-\upsilon_{1b}(Q_d^*))\frac{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a}}{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a} + \left(r(1-x)/c_{pt}\right)^{m_a}} \tag{3}$$

where m_a is the contest intensity. The first term of the right side represent the probability that the attacker survives after the preventive strike. For any given x, the attacker chooses its decision variables $(X^*, Y^*) = \arg\max(\upsilon_{1g})$. The defender chooses $x^* = \arg\min(\upsilon_{1g}(X^*, Y^*))$.

In the case where a preventive strike is not chosen by the defender, it does not waste resources on it, i.e., $x=0$. As the defender does not use a preventive strike, the attacker does not need to protect its base, and thus $X=0$. It also does not use false bases, thus $Y=0$. As the defender uses false targets, the attacker distributes its attack effort R evenly into Q_a objects to maximize the vulnerability of the object. The vulnerability of the genuine object in cases where it is among the Q_a attacked objects can be modeled by the contest success function as

$$\upsilon_{2g}^{\sim} = \frac{\left(R/Q_a C_{at}\right)^{m_a}}{\left(r(1-y)/c_{pt}\right)^{m_a} + \left(R/Q_a C_{at}\right)^{m_a}} \tag{4}$$

Therefore, the unconditional vulnerability of the genuine object is

$$\upsilon_{2g} = \frac{Q_a}{\lfloor ry/c_{ft} \rfloor + 1} \times \frac{\left(R/Q_a C_{at}\right)^{m_a}}{\left(r(1-y)/c_{pt}\right)^{m_a} + \left(R/Q_a C_{at}\right)^{m_a}} \tag{5}$$

For any given y, the attacker chooses its optimal decision $Q_a^* = \arg\max(\upsilon_{2g})$. The first term of the right side in equation illustrates the ratio between attacked targets and the total number of targets. The defender chooses $y^* = \arg\min(\upsilon_{2g}(Q_a^*))$ to maximize the vulnerability. By comparing the vulnerabilities of the two cases, the defender decides to use a preventive strike if $\upsilon_{1g}^* = \upsilon_{1g}^*(x^*) < \upsilon_{2g}^*(y^*) = \upsilon_{2g}^*$; otherwise, the defender chooses to build false targets to decrease the vulnerability of the genuine object.