Research Article

A Cyber-Attack Synergy Model Considering Both Positive and Negative Impacts from Each Attacker

Yu-Shun Wang, Lun-Ping Hung, Hsiao-Hsien Rau, and Frank Yeong-Sung Lin

1Department of Information Management, National Taiwan University, No. 1, Section 4, Roosevelt Road, Taipei 106, Taiwan
2Department of Information Management, National Taipei University of Nursing and Health Sciences, Taipei, Taiwan
3Graduate Institute of Biomedical Informatics, Taipei Medical University, Taipei, Taiwan

Correspondence should be addressed to Frank Yeong-Sung Lin; yslin@im.ntu.edu.tw

Received 3 November 2014; Accepted 27 February 2015

Academic Editor: Neil Y. Yen

Copyright © 2015 Yu-Shun Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

An emerging attack strategy, collaborative attack, is considered the next generation type of attack. There are only a few models quantifying the synergy of a collaborating attack. Further, previous models consider only positive effects regardless of potential disharmonious factors which are common in the real world. Contributions of this work are summarized as follows: first, this paper introduces a mathematical formulation measuring synergy which takes both positive and negative effects into consideration. This model can not only be applied in measuring collaborative attack effectiveness, but also be used to describe the synergy in other teamwork scenarios. The scenario of an applicable cyber-warfare can take place in a wired network, wireless network, or sensor network. Secondly, a meaningful connection between contest success function and Cobb-Douglas function is proposed and integrated in a cyber-attack scenario. Both the contest intensity of the contest success function and the sum of exponents of Cobb-Douglas function reflect an environmental factor regarding whether it encourages investing or not. Lastly, comparisons between the proposed model and the Cobb-Douglas function are also presented with a subsequent discussion of implications. The behavior of the proposed model is closer to reality and less coupled to another exogenous variable, contest intensity.

1. Introduction

Information security has become an important topic whether in academic or industrial domain. According to the report of Symantec in 2011 [1], businesses are worrying about a variety of threats. Specifically, their top worry is cyber-attacks, followed by IT incidents caused by well-meaning insiders and internally generated IT-related threats. Because of the risks caused by cyber-attacks, enterprises have to invest more resources to protect their systems and the information on them.

In a traditional network attack and defense scenario, most attacks are launched individually. But science collaborative attack is more powerful and efficient; it has become a new strategy for attackers recently. In [2], the authors describe that the collaborative attacks are launched by multiple attackers, who might be human beings or organizations, of specialized expertise. The characteristic of collaboration makes the decisions and behavior more sophisticated. Further, in [2], the authors use a high-level abstract framework and classification to evaluate its effectiveness. The scenario of a cyberwarfare can take place in a wired network, a wireless network, or a sensor network.

By cooperating with other members in an attack group, sharing information about the target network with each other can significantly increase the effectiveness of an attack. Furthermore, synergy can be created through collaboration and thus achieves the following advantages mentioned in [3]. (1) Coordinated attacks could be designed to avoid detection. (2) It is difficult to differentiate between decoy and actual attacks. (3) There is a large variety of coordinated attacks. Nevertheless, there are certainly some drawbacks regarding collaborations, for example, inefficiency caused by personal preferences, which is also considered in this work.

In this paper, one of the contributions is to propose a generic model which quantified the interrelationships between group members. This model can be applied not only in an attack and defense scenario, but also in other
collaborations. In the real world, relationships among individuals or organizations play an important role in collaborative work. Friendship and political alliances, for example, may positively influence the outcome of group work. Negative emotions and attitudes toward other people on the same team can cause disagreements that can significantly derail the performance of a team. Workers in the same group construct an informal social network, in which people who trust each other can exchange relevant information and allocate different resources. According to the above truisms, individuals can be seen to influence others in a group.

2. Related Works

There is little research [4–10] discussing the synergy effects among different people in the same organization. In [4], the authors focused on measuring state-society synergy but did not model it as a formulation. As for [5], three broad classes of resources that contribute to the creation of value were compared, but no quantified model was offered. A framework that integrated theoretical perspectives in a process-oriented model was proposed in [6]; however, while this framework provided several insights into synergy, it mainly focused on mergers and acquisitions and lacked a generic modeling of human collaboration. The authors of [7] introduced a method for strengthening the collaborative benefits specifically in a health domain. Although a model of motivational synergy as the positive combination of intrinsic and extrinsic motivation was presented in [8], the scenario focused on employee inspiration rather than effectiveness.

A new measure called partnership synergy assessing the degree of a partnership’s collaborative process was illustrated in [9]. This process, which is conceptually related to this study, was derived from conclusions the authors made from questionnaire data rather than formulations. Nonetheless, the conclusions of [9] which discusses important factors influencing synergy are considered in this study.

In [10], a mathematical formulation measuring collaborative synergy is proposed. Specifically, the well-known Cobb-Douglas model from economics was applied to describe synergy effects. This formulation can not only represent the synergy effects but also reflect the economic environment by summing the exponents. However, this model does not consider the synergy effect among different personal interests. For example, in a group where the project manager leads the members to achieve a specific goal, those members who like the leader are more likely to contribute more whereas those who dislike the leader might take an apathetic attitude. It may also turn out that one person may have different influences on other people in the same group or organization. In our study, we consider the above effects and formulate them. The comparisons are demonstrated in simulation results.

For any team work, without losing generality, there are three parties: the leader, participants, and external forces. Though some scenarios do not contain external forces, for rigourousness, when choosing a proper scenario to demonstrate synergy effects, all three parties should be considered. Further, with the rapid development of the Internet and information technology, organizations are more likely to suffer from malicious attacks, thus making information security a major concern for enterprises [1, 3]. In the real world, the adversaries might form a group with a commander who coordinates members to launch attacks collaboratively. Each attacker has a different capability and relationship among members. The scenario perfectly fits the condition of the previous descriptions, where the leader is the commander, participants are the attackers, and the network work administrator plays the role of external force against malicious behaviors. Consequently, the network attack and defense scenario is chosen to demonstrate the synergy models.

3. Problem Description

3.1. Synergy Modeling. In light of the above discussion and to the best of our knowledge, it is clear that the Cobb-Douglas function, which was developed from the economic domain to evaluate the synergy of workers, matches closely the proposed model both conceptually and in terms of quantified methods. Consequently, it is necessary to introduce this formulation before our proposed model. Consider

\[ Y = AL^αK^β \]  

subject to

\[ p_1L + p_2K \leq B, \]  

where \( Y \) is the total utility (the monetary value of all goods produced in a year), \( L \) is the labor invested (e.g., total number of person-hours), \( K \) is the capital invested (e.g., the monetary worth of all machines), \( A \) is the total factor productivity, where the value is influenced by environment or progress of technology, \( p_1 \) is the unit price of labor, \( p_2 \) is the unit price of capital, and \( B \) is the total budget.

In this model, parameters \( \alpha \) and \( \beta \) have specific physical meaning which represents the marginal effects of labor and capital, respectively. The summation of these two exponents also stands for whether there exist economies of scale in the given environment. There are three value domains with respect to the summation of \( \alpha \) and \( \beta \) given as follows.

(i) \( \alpha + \beta > 1 \): this represents investing in more capital and labor returns more output. In other words, the external environment encourages investing.

(ii) \( \alpha + \beta = 1 \): this production function is directly proportional to scale; in other words, if investing is double capital \( K \) and labor \( L \), the return is double output \( Y \).

(iii) \( \alpha + \beta < 1 \): this represents investing in equal capital and labor returns less output; there is a decreasing return to scale of production. In other words, the external environment discourages investing.

Apart from the standard form of the Cobb-Douglas function, there is an extended form that allows this function to take into consideration diverse elements. Consider

\[ U(x_1, x_2, x_3, \ldots) = Ax_1^αx_2^βx_3^γ \ldots \]  

(3)
For modeling synergy effects in a more comprehensive way, the corresponding proposed model is presented in the following. The given parameters and variables are shown in Table 1. This synergy model can be applied to various aspects of decision making problems and measures the synergy effects considering both positive and negative factors, thus making this formulation closer to reality.

**Table 1: Parameter explanations.**

| Notation | Description |
|----------|-------------|
| $W$      | Set of workers |
| $T$      | Set of tasks |
| $P_{wt}$ | The productivity rate of worker $w$ on task $t$, where $w \in W$ and $t \in T$ |
| $r_{wt}$ | Basic productivity rate of worker $w$ on task $t$, where $w \in W$ and $t \in T$ |
| $l_{iwt}$ | Leadership factor (inference) of worker $i$ on worker $w$ for task $t$, where $w \in W$ and $t \in T$ |
| $d_{iwt}$ | Discount rate of worker $i$ on worker $w$ for task $t$, where $i \in W$, $w \in W$, and $t \in T$ |
| $v_i$    | Relative value out of the productivity rate for task $t$, where $t \in T$ |

**Decision variable**

| Notation | Description |
|----------|-------------|
| $x_{iwt}$ | A decision variable which is the portion of worker $w$'s resources allocated to task $t$, where $t \in T$ |
| $b_i$    | The number of workers participating in task $t$, where $t \in T$ |
| $h_{iwt}$ | The number of workers whose leadership is greater than discount effect on worker $w$ when accomplishing task $t$, where $w \in W$ and $t \in T$ |

subject to

$$p_1 x_1 + p_2 x_2 + p_3 x_3 + \cdots \leq B,$$

where $x_i$ is type $i$ resource, $p_i$ is unit price of $x_i$, exponents are marginal effect regarding $x_i$, and $A$ is total factor productivity.

In the extended form, resources are not restricted to only labor and capital and can include other types of elements. In this work, “resources” stand for not only money, but also time, human resource, and other types of possible form. A generic form is applied to hopefully include most attack and defense scenarios. The defender can quantify “resource” adaptively based on features of attack and defense scenario. This makes the extended model flexible. Corresponding modifications are also applied to the budget constraint. The original model takes the point of view from a high level, which can be seen as a “top-down” concept since it treats all human resources as the one factor of “labor.” With the help of the extended form, the granularity of resource type can be modified as needed.

After a brief introduction to the Cobb-Douglas model, it is clear that an instance of team work can be modeled in the extended form where each member can be treated as one type of resource since every participant has a different value of attributes, such as salaries, working hours, and shifts. Also, the marginal effects, which are represented by exponents, can be different from each other. Nevertheless, it can be observed that although external negative effects can be considered by the summation of exponents, this is still an implicit way. Moreover, the internal disharmonious factors which are within the group are neglected.

For modeling synergy effects in a more comprehensive way, the corresponding proposed model is presented in the following. The given parameters and variables are shown in Table 1. This synergy model can be applied to various aspects of decision making problems and measures the synergy effects considering both positive and negative factors, thus making this formulation closer to reality.
When the proportion becomes large, the penalty which decreases productivity also becomes greater.

After measuring one worker's productivity, the total efficiency of the system is modeled by the summation of individual preferences on working subjects $t$, $v$, and $P_{ue}$.

3.2. Scenario. As mentioned before, the network attack and defense scenario is quite suitable for demonstrating the synergy effects of the Cobb-Douglas function and proposed model. Not only does the scenario contain all the important features needed in a collaborative work, but information security is also a significant issue [1, 3].

In a network attack and defense scenario, there is a service provider (defender) who provides network service (e.g., HTTP, FTP services) to users. In addition to the secure private information collected from customers, maintaining the quality of services is also the provider’s responsibility. However, there are adversaries trying to steal secret information or disrupt network services. For the emerging attack type [2] of collaborative attacks, adversaries are subordinate to a commander who makes decisions on choosing the victims and the proper targets. Under this type of attack, synergy effects play an important role since they directly influence the outcome of a battle. The attackers are assumed to have only incomplete information about the network. In other words, the attackers can only acquire neighboring information. They cannot compromise the core nodes directly. Therefore, the topology type has influences on attack performance.

In the proposed attack and defense scenario, the method of determining the outcome of an attack is governed by the contest success function, which was initially put forward in economic theory for solving rent seeking problems [11]. The result is in a probabilistic form, which is influenced by resources invested from both sides. This function has been widely used in the literature addressing various economics-related activities, as well as international and civil wars [12, 13]. In recent years, this theory has also been applied to the determination of the success probability for the attacker to compromise a system [14–17]. The form of contest success function is as follows:

$$v = T^m / (T^m + t^m).$$

In (7), $v$ stands for adversaries’ winning probability, $T$ represents the attack resources invested on the victim node, whereas $t$ is the defense resources deployed on the node. As for the parameter $m$, it is named contest intensity which has a specific physical meaning regarding the nature of the contest. Some value intervals of $m$ can be described as follows.

(i) $0 < m < 1$: this represents a “fight to win or die” circumstance. In other words, resources invested by both sides have little influence on the success probability.

(ii) $m = 1$: the investments of both sides have proportional impacts on the probability.

(iii) $1 < m < \infty$: the effectiveness of the resources each player invested exponentially increases since contest intensity is the exponent of the contest success function.

(iv) $m \to \infty$: this depicts a “winner takes all” circumstance. In other words, as long as one side invests one unit resource more than the other, there is almost a 100% success probability.

For measuring the synergy effects in an attack and defense scenario, there are certain modifications that need to be made for both the Cobb-Douglas function and proposed model. First, for the Cobb-Douglas function, the extended form is applied to measure the attack resources ($T$) after taking synergy into consideration (8). Moreover, each attacker (worker) is treated as one type of resource since there are always some differences between people. Everyone is unique in the world. Further, the exponent of each resource type represents the marginal effect. In (9), it is suitable to measure an attacker's marginal contribution through his/her capability. And according to the previous discussion, the concept of economies of scale is very similar to contest intensity in terms of not only the value range but also the physical meaning. Consequently, we can make connections between the contest success function and the Cobb-Douglas function via contest intensity. Table 2 illustrates the modified Cobb-Douglas function and proposes the method of combination. Consider

$$T = A_1 \prod_{i=1}^{N} x_i^{a_i},$$

$$\sum_{i=1}^{M} a_i = \sum_{i=1}^{M} \left( \frac{c_i}{\sum_{j=1}^{M} c_j} \times m \right) = m,$$

$$\sum_{i=1}^{M} x_i \leq B.$$
Table 2: Parameter explanation of the modified Cobb-Douglas function.

| Notation | Description |
|----------|-------------|
| $N$      | The total number of attackers involved in an attack event |
| $M$      | The total number of attackers subordinated to one commander |
| $c_i$    | Attacker’s capability |
| $\alpha_i$ | The marginal effect of attacker $i$, which is measured by the ratio of attacker capability since this metric directly influences the attack results |
| $A$      | A parameter whose value is related to attackers’ capability |
| $m$      | Contest intensity |

Table 3: Parameter explanation of the proposed model in the attack and defense scenario.

| Notation | Description |
|----------|-------------|
| $N$      | The index set of all nodes |
| $P$      | The index set of all attackers |
| $r_{um}$ | Basic attack performance rate of attacker $l$ on compromising node $m$, where $w \in P$, $m \in N$ |
| $l_{um}$ | Leadership of attacker $l$ on worker $w$ for compromising node $m$, where $l \in P$, $w \in P$, $m \in N$, and $l \neq w$ |
| $d_{lm}$ | Discount rate of worker $l$ on worker $w$ for compromising node $m$, where $l \in P$, $w \in P$, $m \in N$, and $l \neq w$ |

| Notation | Description |
|----------|-------------|
| $a_{um}$ | A decision variable is the portion of attacker $l$’s efforts allocated to compromising node $m$, where $l \in P$ and $m \in N$ |
| $Y_{um}$ | The synergy effect of attacker $w$ on compromising node $m$, where $w \in P$ and $m \in N$ |
| $T_m$    | Quantity of attack resources allocated on node $m$ after considering synergy effects, where $m \in N$ |
| $b_m$    | The number of attackers participating in compromising node $k$, where $k \in N$ |
| $h_{um}$ | The number of attackers whose leadership is greater than discount effect on attacker $w$ when compromising node $m$, where $w \in N$, $m \in P$ |

In this scenario, $v_i$ of the generic model does not influence the productivity rate. The synergy regarding attack resource $T$ can be measured by (12). Consider

$$Y_{um} = a_{um} r_{um} \left( \frac{\sum_{l \in P \setminus w} a_{um} l_{um} d_{um} h_{um}}{l_{um} b_m} \right) \times \sum_{l \in P \setminus w} a_{um} l_{um} d_{um}$$

(11)

$$\forall w \in P, \forall m \in N,$$

$$T_m = \sum_{w \in P} Y_{um} \quad \forall m \in N.$$  

(12)

4. Computational Simulations

In this section, simulations are constructed to evaluate the Cobb-Douglas function and proposed synergy model. A scale-free network, which is a network with a power law tail in the degree distribution, is applied as the defender’s network. In [18], the authors proposed that the presence of scale-free emerging properties in many “real-world” networks provides initial evidence that these self-organizing phenomena not only depend on the characteristics of individual systems, but also are general laws of evolving networks. As such, this type of network is chosen to demonstrate the results to make conclusions closer to reality.

In the attack and defense scenario, the defender is responsible for the survivability of services including one confidential and personal data storage service and two quality-sensitive services. For the data storage service, once the core node is compromised, the information is leaked. As for quality-sensitive services, if the defender fails to maintain the quality of service, this is considered as being compromised. Table 4 lists the defender parameters.

Regarding commanders, they group up a team with many attackers, each of whom has different attributes including influences toward the other group members. Normal distributions are applied to describe budget, capability, and the
| Parameter                  | Value                                      |
|----------------------------|--------------------------------------------|
| Topology type              | Scale-Free                                 |
| Number of nodes            | 25                                         |
| Number of services         | 2                                          |
| Number of total core nodes | 3                                          |
| Total budget for network construction and defense | 1.5 M |

Table 5: Commander parameters (M = millions).

| Parameter                  | Value                                      |
|----------------------------|--------------------------------------------|
| Total budget               | Normal distribution with interval (0.3 M–1.5 M) |
| Leadership                 | Normal distribution with interval (0–1)    |
| Discount                   | Normal distribution with interval (0–1)    |
| Number of attackers per group | Uniform distribution with interval (5–14) |

impacts between attackers (leadership and discount factor). Table 5 presents the commander parameters.

4.1. Convergence Test. Before explaining the simulation results, it is important to discover a proper number of simulation times for each experiment, insofar nonconverged results lead to incorrect conclusions. This section thus introduces the method of determining the proper number of simulation times that gives converged results.

We constructed a series of simulations for a network attack and defense scenario that applies the Cobb-Douglas function and the proposed model to measure their respective synergy effects. Figure 1 shows the service compromise probability of applying the Cobb-Douglas function to measure the synergy effects while Figure 2 presents the corresponding results of applying the proposed model. For illustration purposes, 50 simulation results are summarized as one unit in both Figures 1 and 2. The vertical axis represents the service compromise probability while the horizontal axis stands for the number of units. As for the criterion to determine the proper time, the rule is as follows.

For ith simulation, if the difference between the probability of this one and the average probability of all previous simulations is less than 0.1%, it is believed that the number of simulations currently is big enough to yield a converged result.

According to the results, for the Cobb-Douglas function in Figure 1, the number of units that achieved the above condition was 109, which represented 5,450 commanders. As for the proposed model in Figure 2, the corresponding number of units was 136, which represented 6,800 commanders. For rigorousness, the proper number of simulations, which is also the proper number of commanders, was set to 7,500 commanders for the Cobb-Douglas function and 10,000 commanders for the proposed model.

4.2. Effectiveness Comparison. In this section, the effectiveness of the Cobb-Douglas function and proposed model is discussed. Simulations are constructed under different levels of attack budget. The data is shown in Table 6. Corresponding trends can be observed in Figure 3 where the vertical axis means service compromise probability. It can be observed in Figure 3 that the Cobb-Douglas function appears as an increasing trend toward synergy effects, which is in contrast to the proposed model that only reveals a slight increase in service compromising probability. At the first glance, it seems that the behavior of Cobb-Douglas function is reasonable. However, the reason of this significant improvement is because the proposed model takes into consideration both positive and negative effects between each participant whereas the Cobb-Douglas function considers only the positive ones. Thus, with the increasing total budget, there is a significant monotonic increasing trend.

In an attack and defense scenario, since a mistake made by one group member can jeopardize the whole operation, budget is not the only factor influencing the outcome of the battle. Any disharmonious factor has a great effect on total performance. Consequently, in the proposed model, the
impacts between each participant play an important role in measuring synergy.

As for the real world, increasing resources may have a positive effect on inciting group members. But there is a more influential factor, which is the relationship between members. Good relationships help make projects successful more easily than just the investment of more resources. This feature is reflected by the proposed model in contrast to the Cobb-Douglas function that mainly focuses on the quantity of resources invested.

4.3. The Relationship between Synergy Effectiveness and the Numbers of Participants. After comparing the effectiveness of the two models, the sensitivity regarding the number of participants is the next item that needs discussion. As can be seen from the simulation results listed in Table 7, the proposed model is more sensitive than the Cobb-Douglas function when the number of participants increases.

As shown in Figure 4, the improvement rate of the proposed model increases 24.8% when the number of participants increases from 4 to 7. On the other hand, the improvement rate of the Cobb-Douglas function only increases 11.7%. The reason is that in proposed model, with more participants, the influences caused by each pair of members grow rapidly while in Cobb-Douglas function, this effect is neutralized by the exponentiation. Unless the new entrant has a negative impact on all existing group members, recruiting people contributes more good than harm. Consequently, the trend is less significant in the Cobb-Douglas function.

Considering the situation in the real world, increasing the size of a group usually has a positive effect on performance as long as the new member can cooperate with the team smoothly. Of course there are situations in which adding a new member decreases the whole productivity. But in small- and middle-sized groups, like the size in the simulations, positive effects are more likely to be observed unless there exists a member who has a very bad influence on all the others.

4.4. The Relationship between Synergy Effectiveness and Contest Intensity. In this section, relationships regarding synergy effectiveness and contest intensity are examined. As is evident in Table 8, the value of contest intensity determines the nature of a battle. However, there should be no obvious trend for network compromise probability based on the different values of contest intensity [14–17]. In other words, the value of contest intensity prefers neither the defender nor the commanders.

With the help of synergy, there is an increasing trend on attack performance with the application of the Cobb-Douglas function. But in the proposed model, there is no significant regularity. This can be explained as follows: for the Cobb-Douglas function, since the summation of exponents is connected to the contest intensity, the synergy effect becomes more significant when the value of contest intensity increases. As for the proposed model, the synergy effect is governed by the impacts between each participant, such that modifying the value of contest intensity does not give consistent results on attacks. Different values of contest intensity only influence the nature of a battle, not the outcome of a contest (Figure 5).
The relationship between synergy effectiveness and contest intensity


type of synergy model

| Contest intensity | m = 0.5 | m = 2 | m = 1 |
|-------------------|---------|-------|-------|
| Compromise probability (%) | | | |
| 0                  |         |       |       |
| 20                 |         |       |       |
| 40                 |         |       |       |
| 60                 |         |       |       |
| 80                 |         |       |       |
| 100                |         |       |       |

Figure 5: The relationship between synergy effect and contest intensity.

5. Conclusions and Future Works

In this paper, a different synergy model is well-formulated and its features are compared with the widely applied Cobb-Douglas function. A network attack and defense scenario is proposed to evaluate the behavior of these two models. According to the simulation results, the proposed model is more sensitive to the number of participants rather than the total budget, which is reasonable and more closely approximates reality. In contrast, the Cobb-Douglas function performs a proportional trend according to total budget. Also, contest intensity has a monotonic influence on the performance of the Cobb-Douglas function while there is not an obvious trend in the proposed model. For future work, other types of modeling techniques or a hybrid form of different models may be considered to measure synergy effects.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] Symantec, State of Security Survey, Symantec, 2011.
[2] S. Xu, “Collaborative attack vs. collaborative defense,” in Collaborative Computing: Networking, Applications and Worksharing, vol. 10 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, part 2, pp. 217–228, Springer, 2009.
[3] S. Braynov and M. Jadliwala, “Representation and analysis of coordinated attacks,” in Proceedings of the ACM Workshop on Formal Methods in Security Engineering (FMSE ’03), pp. 43–51, October 2003.
[4] P. Evans, “Government action, social capital and development: reviewing the evidence on synergy,” World Development, vol. 24, no. 6, pp. 1119–1132, 1996.
[5] S. Chatterjee, “Types of synergy and economic value: the impact of acquisitions on merging and rival firms,” Strategic Management Journal, vol. 7, no. 2, pp. 119–139, 1986.
[6] R. Larsson and S. Finkelstein, “Integrating strategic, organizational, and human resource perspectives on mergers and acquisitions: a case survey of synergy realization,” Organization Science, vol. 10, no. 1, pp. 1–26, 1999.
[7] R. D. Lasker, E. S. Weiss, and R. Miller, “Partnership synergy: a practical framework for studying and strengthening the collaborative advantage,” Milbank Quarterly, vol. 79, no. 2, pp. 179–205, 2001.
[8] T. M. Amabile, “Motivational synergy: toward new conceptualizations of intrinsic and extrinsic motivation in the workplace,” Human Resource Management Review, vol. 3, no. 3, pp. 185–201, 1993.
[9] E. S. Weiss, R. M. Anderson, and R. D. Lasker, “Making the most of collaboration: exploring the relationship between partnership synergy and partnership functioning,” Health Education & Behavior, vol. 29, no. 6, pp. 683–698, 2002.
[10] G. Fandel, A. Giese, and B. Mohn, “Measuring synergy effects of a public social private partnership (PSPP) project,” International Journal of Production Economics, vol. 140, no. 2, pp. 815–824, 2012.
[11] S. Skaperdas, “Contest success functions,” Economic Theory, vol. 7, no. 2, pp. 283–290, 1996.
[12] G. Levitin and K. Hausken, “False targets efficiency in defense strategy,” European Journal of Operational Research, vol. 194, no. 1, pp. 155–162, 2009.
[13] F. Y.-S. Lin, Y.-S. Wang, H.-Y. Chung, and J.-L. Pan, “Maximization of network survivability under malicious and epidemic attacks,” in Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA ’12), pp. 412–417, IEEE, Fukuoka, Japan, March 2012.
[14] K. Hausken and G. Levitin, “Protection vs. false targets in series systems,” Reliability Engineering and System Safety, vol. 94, no. 5, pp. 973–981, 2009.
[15] F. Y.-S. Lin, Y.-S. Wang, and M.-Y. Huang, “Effective proactive and reactive defense strategies against malicious attacks in a virtualized honeynet,” Journal of Applied Mathematics, vol. 2013, Article ID 518213, 11 pages, 2013.
[16] L. Wang, S. Ren, K. Yue, and K. Kwiat, “Optimal resource allocation for protecting system availability against random cyber attacks,” in Proceedings of the 3rd International Conference on Computer Research and Development (ICCRD ’11), pp. 477–482, March 2011.
[17] J. E. Ramirez-Marquez, C. M. Rocco, and G. Levitin, “Optimal network protection against diverse interdictor strategies,” Reliability Engineering & System Safety, vol. 96, no. 3, pp. 374–382, 2011.
[18] A. Tolba, “Scale free networks; a literature review,” in Proceedings of the International Conference on Complex Systems, September 2007.
