Entropy **2012**, *14*, 571-580; doi:10.3390/e14030571

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Benefit-Cost Analysis of Security Systems for Multiple Protected Assets Based on Information Entropy

Jingjing Dai [1], Ruimin Hu [1,2,*], Jun Chen [1] and Qing Cai [1]

[1] National Engineering Research Center for Multimedia Software, Wuhan University, Wuhan 430072, China; E-Mails: dianadai2002@gmail.com (J.D.); chenj@whu.edu.cn (J.C.); caiqing75@gmail.com (Q.C.)

[2] School of Computer, Wuhan University, Wuhan 430072, China

* Author to whom correspondence should be addressed; E-Mail: hrm1964@163.com.

Received: 18 January 2012; in revised form: 27 February 2012 / Accepted: 29 February 2012 / Published: 14 March 2012

Abstract: This article proposes a quantitative risk assessment for security systems which have multiple protected assets and a risk-based benefit-cost analysis for decision makers. The proposed methodology consists of five phases: identification of assets, security unit and intrusion path, security unit effectiveness estimation, intrusion path effectiveness estimation, security system risk assessment and benefit-cost estimation. Key innovations in this methodology include its use of effectiveness entropy to measure the degree of uncertainty of a security system to complete a protection task, and the fact it measures risk like information theory measures the amount of information. A notional example is provided to demonstrate an application of the proposed methodology.

Keywords: security system; effectiveness estimation; entropy; multiple assets; benefit-cost

1. Introduction

Physical security systems are deployed to prevent or mitigate loss of valuable assets (e.g., property or life) [1]. According to the Department of Homeland Security National Infrastructure Protection Plan of United States, benefit-cost analysis is the hallmark of homeland security decision making [2]. Benefit-cost analysis requires quantification of the risk after and before implementation of a risk reduction strategy. The basic theory of risk evaluation for security systems is still lacking in China. Scientists mainly rely on qualitative assessments of management science to determine the risk of the

system [3–6]. However, if an evaluation system does not have a deep, comprehensive understanding of the security system, risk evaluation based on management science will result in deviations. On an international scope, scientists have made some significant progress on the basic theory for risk evaluation of security systems. In 1970s, the U.S. Department of Energy's Sandia National Laboratories [7] first introduced the basic concepts of physical protection systems. At that time, it proposed the idea that this system can be applied to the field of nuclear facilities protection. Subsequently, the U.S. Department of Energy put forward a model of adversary sequence diagram (ASD) [8]. This model can identify deficiencies in physical protection systems by analyzing how hypothetical adversaries might achieve their objectives through various barriers. The model identified the weakest path in a physical protection system where an opponent has the highest probability of attacking the system. Subsequently, the U.S. Department of Energy put forward a comprehensive path analysis model based on single-path analysis that has a significant limitation in that only one adversary attack path is analyzed [9]. The top ten weakest paths will be found from among hundreds of probable attack paths. In 2007, Garcia [10] gave an integrated approach for designing physical security systems. The measure of effectiveness employed for a physical protection system is the probability of interruption, which is defined as "the cumulative probability of detection from the start of an adversary path to the point determined by the time available for response". Hicks *et al.* [11] presented a cost and performance analysis for physical protection systems at the design stage. Their system-level performance measure is risk, which they define as follows: Risk = P(A) × [1 − P(E)] × C where, P(A) is Probability of Attack, P(E) is Probability of System Effectiveness, = P(I) × P(N), P(I) is Probability of Interruption, P(N) is Probability of Neutralization, C is Consequence. Their discussion of the cost-performance tradeoff is limited and heavily weighted toward cost as a driver in the decision [1]. Fischer and Green [12] present a qualitative risk analysis approach to ranking threats using a probability/criticality/vulnerability matrix. Cost effectiveness is discussed as a possible measure of system evaluation. Oak Ridge National Laboratory [13] established a CSG (Combination Solid Geometry) model, which is a powerful descriptive model facility. This model is based on the use of image processing, distributed computing, geometric aspects of technology, using computer-aided design methods to establish facilities in three-dimensional simulation model. This three-dimensional simulation model is close to the actual installations of the model, calculated by dedicated software; the system can do the most detailed analysis.

Those researches are mainly focused on the risk evaluation of security system by using probability statistics methods and simulation methods. Probabilistic statistics methods experiment with small statistical samples of events to get the probability of attack of a security system and make debatable assumptions about fixed values for detection and delay elements [14]. These methods only describe scenarios of one asset, and don't extend to collocated assets [14]. In practice, there are many security systems that protect multiple assets, such as museums or schools. Risk assessment for security systems for multiple assets is needed. Simulation experiments are applied to assess the effectiveness of security systems must establish completely different facilities models for different facilities, so the complexity of computation is very large and the development process is extremely complex.

The historical data on attacks is limited. There are enormous uncertainties in risk evaluation of security systems. The most uncertain is the threat itself [15]. A number of researchers have used bounded intervals [16], game theory [17–19], exogenous dynamics [20], to characterize uncertainty in

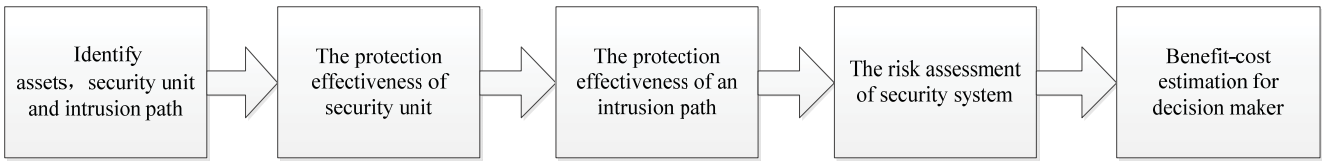
terrorism risk analysis. There is some important recent literature considering both adaptive and non-adaptive threats [18,21]. Despite the fact a contribution on this issue is not within the scope of this article, we take the position that credible expert opinion can compensate for the lack of data to support quantitative risk assessments and only consider non-adaptive threats.

The primary objective of this article is to reference the Information Theory of Shannon. Like information entropy, we use entropy to measure the effectiveness uncertainty degree of a security system's protection capability with regard to protection of multiple assets. With a simple illustrative example, we demonstrate the application of security system risk assessment and benefit-cost estimation with different strategies.

2. Benefit-Cost Estimation of Security Systems Based on Information Entropy

This section develops a quantitative risk assessment for security systems and benefit-cost estimation for decision makes when the security system protects multiple assets. The proposed risk-based benefit-cost estimation method for security system consists of five phases (Figure 1).

Figure 1. Risk-based benefit-cost estimation for decision maker.



2.1. Identify Assets, Security Unit and Intrusion Path

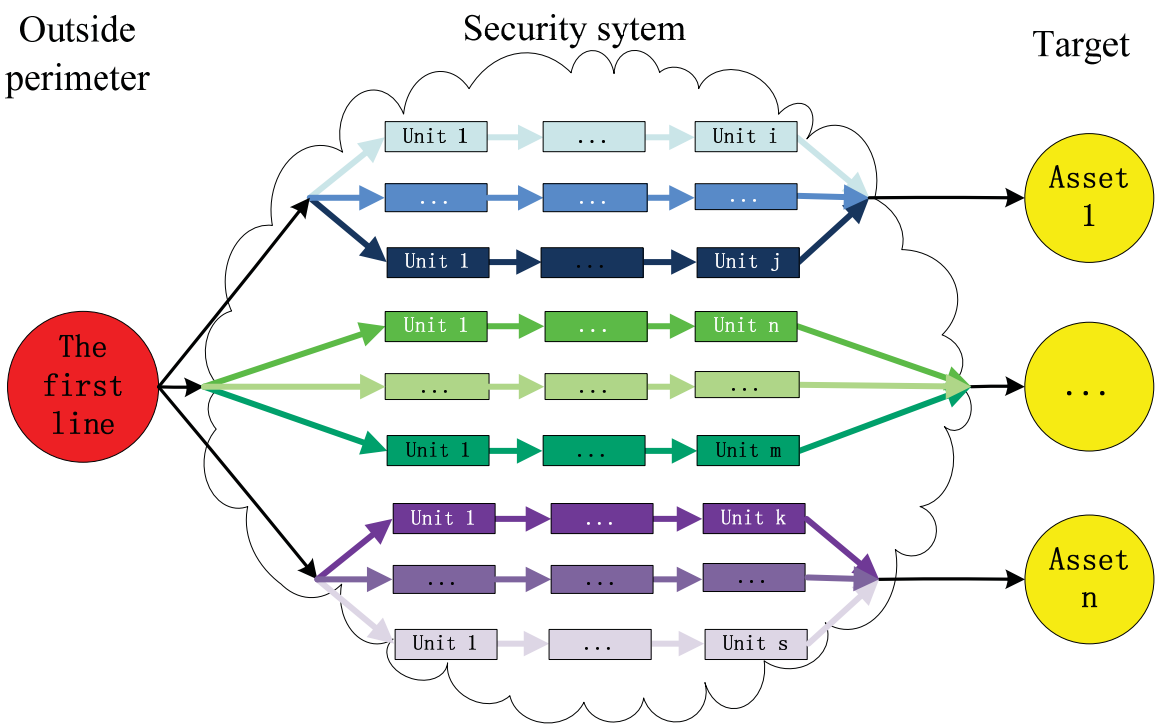
The first phase begins by identifying the key assets which need protection and a complete set of plausible intrusion paths leading to each key asset. Each intrusion path begins at the outside perimeter of a security system since it is the first line that must be crossed by an intruder to gain access to a protected asset [22]. A sequence of discrete security units composes an intrusion path. Security units have protection capability; they may be either a barrier or a path. The security system is abstracted into a security network diagram which is shown in Figure 2. We make some assumptions as follows:

(1) Attackers start from the outside and treat one of protected assets as a target of attack;
(2) There exists at least one path can get to the protected asset;
(3) All units in the path have protection capability values; the attacker needs to pay a cost to pass through the security unit.

2.2. Security Unit Effectiveness Assessment

Entropy is a state function which was proposed to solve the quantity problem of the second law of thermodynamics by French scientist Rudolf Clausius in 1865 [23]. Later, entropy became a measure of disorder or uncertainty about system after Austrian physicist Boltzmann's statistical interpretation [24].

Figure 2. The security network diagram.



In 1948, American scientist Shannon used information entropy to represent the average uncertainty of an information source and the amount of information is a measure of uncertainty that is missing before reception [25]. Information entropy is often obtained from a given probability distribution $p = \{p_i\}$ of messages or symbols. For a random variable X with n outcomes $\{x_i{:}i = 1,\ldots,n\}$, the Shannon entropy, a measure of uncertainty and denoted by H(X), is defined as:

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_b p(x_i) \tag{1}$$

where $p(x_i)$ is the probability mass function of outcome x_i. Due to the source uncertainty, information entropy is used to measure the amount of information in information theory [26]. Similar to information theory, we use entropy to measure the degree of effectiveness uncertainty of the protection capability of a security system. The value of effectiveness is measured by the degree of protection capability that reduces the uncertainty of the security system. In a security system, the effectiveness is usually measured by the ratio of completion of a task. The larger the ratio of completion protection task, the less the uncertainty associated with the effectiveness of the security system is. That means the higher the effectiveness of the security system, the lower the degree of failures to accomplish a protection task will be. Suppose a unit has n-factors for a certain protection task. The ratio is 1 when fully meeting the task. The ratio is 0 when absolutely not meeting the task. The ratio of n factors on a unit can be expressed as R_i $(i = 1,2,\ldots,n)$, the weight of each factor is ω_i $(i = 1,2,\ldots,n)$. For a particular task, the protection effectiveness of one unit j can be determined as:

$$U_j = \sum_{i=1}^{n} \omega_i \log \frac{1}{1-R_i} \, (j = 1,2,\cdots,m; i = 1,2,\cdots,n) \tag{2}$$

where U_j is the protection effectiveness of unit j. R_i is the degree of accomplishing a protection task of factor i. $1 - R_i$ is the degree of fail to accomplish protection task of factor i. As different factors have different impacts on the security system protection effectiveness, ω_i denotes the effect weight of factor-i, and $\sum_{i=1}^{n} \omega_i = 1$.

2.3. Intrusion Path Effectiveness Assessment

The higher the performance of the unit protection, the greater cost the attacker must pay through the unit, so we define unit cost as the value of unit protection effectiveness. The value of unit cost denoted by $C(U_j)(j = 1, 2, \cdots, m)$ is equal to the unit effectiveness:

$$C(U_j) = U_j (j = 1, 2, \cdots, m) \tag{3}$$

We assumed that there are k units $U_i (j = 1, 2, \cdots, k)$ in a path, $C\left(Path(U_1, U_2, \cdots, U_i)\right)(i = 1, 2, \cdots, k)$ denotes the path cost. The value of the path cost is equal to the sum of unit costs.

$$C\left(Path(U_1, U_2, \cdots, U_i)\right) = C(U_1) + C(U_2) + \cdots + C(U_i) \quad (i = 1, 2, \cdots, k) \tag{4}$$

2.4. Security System Risk Assessment

DHS (U.S. Department of Homeland Security) uses reasonable worst-case conditions to assess terrorism risks because intelligent adversaries can choose circumstances where targets are vulnerable and consequences are maximized. The worst-case condition of a security system is intelligent adversaries who can choose the most vulnerable paths to each asset and destroy all assets. The most vulnerable path is the minimum cost of intrusion paths for each asset. So the protection effectiveness for each asset can be determined as:

$$E(asset) = Min\left(C(Path_1), C(Path_2), \cdots, C(Path_n)\right) \tag{5}$$

The value of risk of the security system can be defined as follows, based on the risk definition of security system that Hicks proposed:

$$Risk = P(A) * P(r) * C \tag{6}$$

where P(A) is the probability of attack against a critical asset during the time frame of the analysis which can be assessed by experts. C is consequence, P(r) is the probability of successful attack, that is also called the probability of protection invalidation. In this formula, P(r) is related to the protection effectiveness of security system. The higher the protection effectiveness, the lower the probability of successful attack P(r). The relationship between the two concepts can be expressed as:

$$E(asset) = \log \frac{1}{P(r)} \tag{7}$$

Suppose a security system has n protected assets, so the risk of security system can be determined as:

$$Risk = \sum_{i=1}^{n} \left(P(A)_i * \frac{1}{e^{E(asset_i)}} * C_i \right) \tag{8}$$

where $E(asset_i)$ is the protection effectiveness value of asset i, $P(A)_i$ is the probability of attack for asset i, it can be determined as the annual rate of occurrence of attack, C_i is the value of the protection asset i.

2.5. Benefit-Cost Estimation

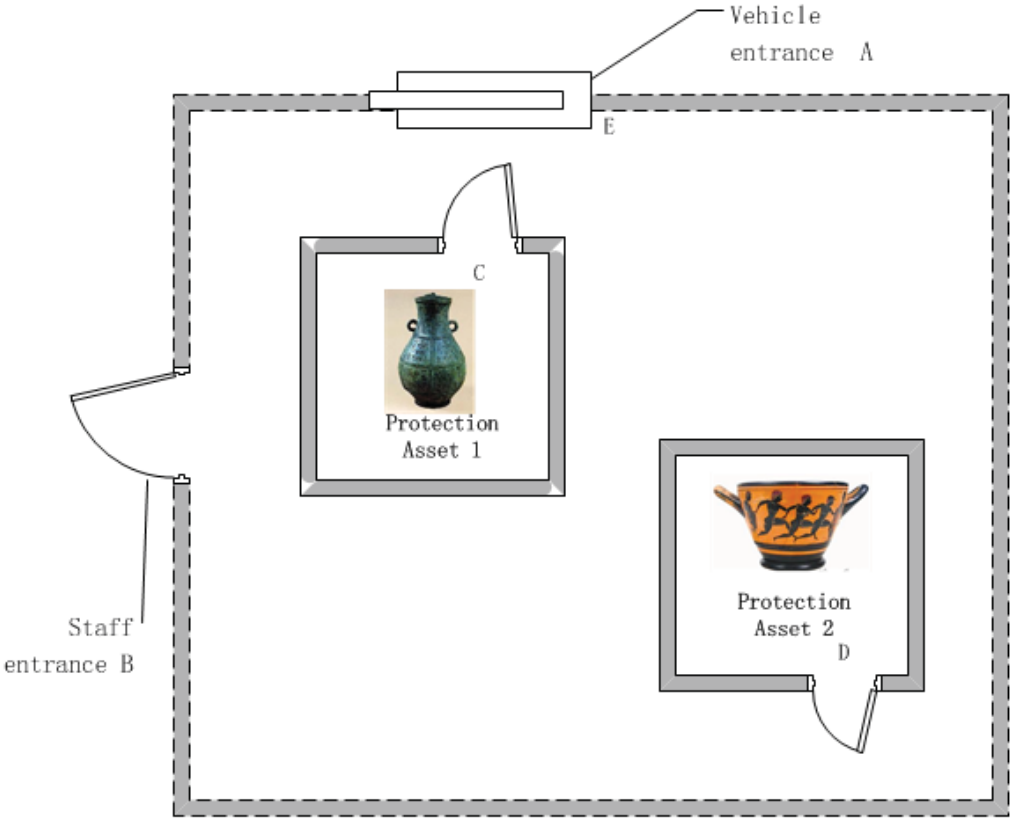
Benefit-cost analysis determines the cost effectiveness of proposed countermeasures and consequence mitigation strategies for reducing the risk associated with an asset or portfolio of assets. The benefit-to-cost ratio for a given investment alternative can be calculated as:

$$\frac{Benefit}{Cost} = \frac{Risk \quad after \quad applied \quad strategy - Risk \quad before \quad applied \quad strategy}{Cost \quad of \quad strategy} \tag{9}$$

3. An Application of a Museum Scenario

To illustrate a simple application of the proposed method, consider the notional museum with two key ancient porcelain assets as shown in Figure 3. Note that all values used throughout this example are purely notional.

Figure 3. Diagram of security system in a museum scenario.



3.1. Identify Assets, Security Unit and Intrusion Path

There are two assets in this example. Consider the example where the adversary intends to sabotage the target as shown in Figure 2, there are two paths to the asset 1. Path one: The adversary intends to

penetrate the vehicle entrance A, travel to the appropriate room, force open the door C, destroy the protected asset 1. Path two: The adversary intends to penetrate the staff entrance B, travel to room, force open the door C, and destroy the protected asset 1. There are two paths to the asset 2. Path one: the adversary intends to penetrate the vehicle entrance A, travel to the room, force open the door D, destroy the protected asset 2. Path two: the adversary intends to penetrate the staff entrance B, travel to room, force open the door D, and destroy the protected asset 2. The protection units of each intrusion path are shown in Table 1.

Table 1. The protection units of each intrusion path.

Intrusion Path	Protection element of Unit 1	Protection element of Unit 2
Path 1 for asset 1	Vehicle entrance A	Door C
Path 2 for asset 1	Staff entrance B	Door C
Path 1 for asset 2	Vehicle entrance A	Door D
Path 2 for asset 2	Staff entrance B	Door D

3.2. The Protection Effectiveness of Security Unit

A security system is a complex configuration of detection, delay, and response elements [27]. So suppose each unit has three factors for the protection task: detection, delay and response. Detection is the discovery of an adversary action which must be followed by an assessment of the alarm to verify whether there is an actual intrusion. Delay is the function of slowing down adversary progress during an intrusion to give the guards more time to respond. Response is the actions taken by the response force to prevent adversary success [28]. The ratio is 1 when the protection task is fully met. The ratio is 0 when the task is absolutely not met. The effect weights of each factor are the same. The ratio of each factors on a unit are shown in Table 2. From Equation (2), the effectiveness of each unit can be determined as listed in Table 2.

Table 2. The effectiveness for each unit.

Unit	Detection	Delay	Response	Effectiveness
Vehicle entrance A	0.7	0.8	0.9	0.74
Staff entrance B	0.8	0.8	0.6	0.60
Door C	0.9	0.6	0.8	0.70
Door D	0.7	0.6	0.9	0.64

3.3. The Protection Effectiveness of an Intrusion Path

From Equation (4), the effectiveness of each intrusion path can be determined as Table 3.

Table 3. The effectiveness for each intrusion path.

Intrusion Path	Effectiveness
Path 1 for asset 1	1.44
Path 2 for asset 2	1.30
Path 1 for asset 1	1.38
Path 2 for asset 2	1.24

3.4. The Risk Assessment of the Security System

From Equation (5), the effectiveness of the security system can be calculated: $E(asset_1) = 1.30$, $E(asset_2) = 1.24$. Suppose that the annual rate of occurrence of attack for the asset 1 is 0.6 and for asset 2 it is 0.4, so $P(A)_1 = 0.6$, $P(A)_2 = 0.4$. The value of the asset 1 is 100,000 dollars, the value of the asset 2 is 200,000 dollars，so C_1 = 100,000, C_2 =200,000. From Equation (8), the risk for each asset can be shown as in Table 4.

Table 4. The risk of each asset.

Parameter	i = 1	i = 2
$E(asset_i)$	1.30	1.24
$P(A)_i$	0.6	0.4
C_i	100,000	200,000
$Risk_i$	1.6×10^4	2.32×10^4

From Equation (8), the risk he risk of the museum security system can be calculated as Risk = 3.92×10^4.

3.5. Benefit-Cost Estimation

To reduce the total risk associated with this security system, three countermeasure strategies were considered: first, improve the response factor of Staff entrance B to 0.7. Second, improve the delay factor of Door C to 0.7. Third, improve the detection factor of Door D to 0.8. Suppose that the costs for each strategy are the same, that is 1,000 dollars.

The higher benefit-cost value means the better the strategy is. From the benefit-cost value of each strategy in Table 5, we can know that strategy 1 and strategy 2 are the same, and the third strategy is better than the first and second strategy.

Table 5. The benefit-cost value for each strategy.

Strategy	Risk Reduction Value	Benefit-Cost Value
1	3×10^3	30
2	3×10^3	30
3	1.4×10^3	1.4×10^2

4. Conclusions

This article proposes a quantitative risk analysis method and benefit-cost estimation for security systems that must protect multiple assets. Following four steps of development, including using effectiveness entropy to measure the degree of uncertainty of the security system, and measuring risk like information theory measures the amount of information, a general formula for security system risk assessment was obtained. Benefit-cost estimation analyses the relationship between proposed countermeasure strategies for reducing risk and cost. As the environments of security system are more complex in general, the proposed model is not comprehensive enough to analyze all the factors. As an exploration of benefit-cost estimation of security systems, this method can help security system

technical staff to carry out quantitative risk assessment of security systems which have multiple protected assets and make decisions about the choice of countermeasure strategies.

Acknowledgments

Thanks for the assistance from National Science Foundation of China (61170023), the major national science and technology special projects (2010ZX03004-003-03), National Nature Science Foundation of China (No. 60832002) and National Natural Science Foundation of China (61172173). We would also like to thank knowledgeable reviewers for their constructive and thoughtful comments.

References and Notes

1. Graves, G.H. Analytical foundations of physical security system assessment. Ph.D. Thesis, Texas A&M University: College Station, TX, USA, August 2006.
2. US Department of Homeland Security. National infrastructure protection plan. Available online: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed on 20 February 2009).
3. Chen, Z.H. Research and practice of effectiveness evaluation of security system (in Chinese). *China Security & Protection* **2007**, *11*, 16–20.
4. Sun, Y.-H.; Li, S.-J.; Li, B. Quantitative assessment of physical protection system for nuclear power plant (in Chinese). *Nuclear Power Engineering* **2009**, *30*, 20–25.
5. Wu, Q.; Yan, L.L. The risk assessment model for enterprise security (in Chinese). *Safety & Security Technology* **2010**, *10*, 10–14.
6. Li, J.-S. Inquiry on the design of museum building security prevention system (in Chinese). *Shanxi Architecture* **2011**, *37*, 29.
7. Bennett, H.A. The EASI approach to physical security evaluation; SAND76-0500; Sandia Labs.: Albuquerque, NM, USA, 1 January 1977; pp. 1–35.
8. Chapman, L.D.; Harlan, C.P. EASI estimate of adversary sequence interruption on an IBM PC; SAND-85-1105; Sandia Labs.: Albuquerque, NM, USA, 1 October 1985; pp. 1–66.
9. Matter, J.C. SAVI: APC-based vulnerability assessment program; SAND 88-1279; Sandia Labs.: Albuquerque, NM, USA, 1 July 1988; pp. 1–19.
10. Garcia, M.L. *Design and Evaluation of Physical Protection Systems*; Butterworth-Heinemann: Burlington, MA, USA, 2007.
11. Hicks, M.J.; Snell, M.S.; Sandoval, J.S.; Potter, C.S. Physical protection systems—Cost and performance analysis: A case study. *IEEE Aero. Electron. Syst. Mag.* **1999**, *14*, 9–13.
12. Fischer, R.J.; Green, G. *Introduction to Security*, 7th ed.; Elsevier: Boston, MA, USA, 2004.
13. Shen, N. Design and development of physical protection system. Master Thesis, China Institute of Atomic Energy, Beijing, China, July 2003.
14. Cummings, M.C.; Mcgarvey, D.C.; Vinch, P.M. Homeland security risk assessment. Volume Ⅱ. Methods, techniques, and tools. RP05-024-01a. Homeland Security Institute: Arlington, VA, USA, 16 June 2006; pp. 1–160.
15. Keeney, R.L. Modeling values for anti-terrorism analysis. *Risk Anal.* **2007**, *27*, 585–596.
16. Nikoofal, M.; Zhuang, J. Robust allocation of a defensive budget considering an attacker's private information. *Risk Anal.* **2011**, doi:10.1111/j.1539-6924.2011.01702.x.

17. Golalikhani, M.; Zhuang, J. Modeling arbitrary layers of continuous level defenses in facing with a strategic attacker. *Risk Anal.* **2011**, *31*, 533–547.
18. Zhuang, J.; Bier, V.M. Balancing terrorism and natural disasters—Defensive strategy with endogenous attack effort. *Oper. Res.* **2007**, *55*, 976–991.
19. Zhuang, J., Bier, V.M.; Alagoz, O. Modeling secrecy and deception in a multiple-period attacker-defender signaling game. *Eur. J. Oper. Res*. **2010**, *203*, 409–418.
20. Hausken, K.; Zhuang, J. The timing and deterrence of terrorist attacks due to exogenous dynamics. *Eur. J. Oper. Res*. **2011**, doi:10.1057/jors.2011.79.
21. Hao, M.; Jin, S.; Zhuang, J. Robustness of optimal defensive resource allocations in the face of less than fully rational attackers. In Proceedings of the 2009 Industrial Engineering Research Conference, Miami, FL, USA, 30 May–3 June 2009; pp. 886–891.
22. Fisscher, R.J.; Green, G. *Introduction to Security*, 7th ed.; Elsevier: Burlington, MA, USA, 2004.
23. Clausius, R. *The Mechanical Theory of Heat—With Its Applications to the Steam Engine and to Physical Properties of Bodies*; John van Voorst: London, UK, 1986.
24. Sandler, S.I. *Chemical and Engineering Thermodynamics*, 3rd ed.; Wiley: New York, NY, USA, 1999.
25. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423, 623–656.
26. Golan, A.; Maasoumi, E. Information theoretic and entropy methods: An overview. *Economet. Rev.* **2008**, *27*, 317–328.
27. Davies, S.J.; Minion, R.R. *Security Supervision: Theory and Practice of Asset Protection*, 3rd ed.; Butterworth-Heinemann: Jordan Hill, Oxford, UK, 2008.
28. Rico, G.; Beasley, J.S. Physical protection systems: Concepts, analysis, and practice in the ET classroom. Available online: http://spacegrant.nmsu.edu/NMSU/2006/rico.pdf (accessed on 27 September 2006).