Communications and Network, 2013, 5, 578-583
http://dx.doi.org/10.4236/cn.2013.53B2104 Published Online September 2013 (http://www.scirp.org/journal/cn)

Protection Model of Security Systems Based on Neyman-Person Criterion

Haitao Lv, Ruimin Hu, Jun Chen, Zheng He
National Engineering Research Center for Multimedia Software, Wuhan University, Wuhan, China
Email: lvhaitao@gmail.com, hurm1964@gmail.com

Received May 2013

ABSTRACT

In this paper security systems deployed over an area are regarded abstractly as a diagram of security network. We propose the Neyman-Pearson protection model for security systems, which can be used to determine the protection probability of a security system and find the weakest breach path of a security network. We present the weakest breach path problem formulation, which is defined by the breach protection probability of an unauthorized target passing through a guard field, and provide a solution for this problem by using the Dijkstra's shortest path algorithm. Finally we study the variation of the breach protection probability with the change of the parameters of the model.

Keywords: Security System; Protection Probability; Security Network; Breach Protection Probability; Breach Path

1. Introduction

The society security problem has been attached importance by national governments. In order to maintain social public safety, many security systems have been constructed in cities in the world. With the rapid development of information technology, especially the Internet of Things and cloud computing, the security system is getting more and more complex, which consists of the intrusion alarm system, the video surveillance system, the access control system, the explosion-proof security check system, etc. Security systems are deployed at different positions in an area, which can communicate and share data each other through the internet, and complete protection tasks cooperatively. In this paper, a large and complex security system is regarded as abstractly as a diagram of a security network. As shown in **Figure 1**, there is a security network consisted of some security systems in the guard zone, where each of yellow filled circles represents a security system, and every triangle represents a protection target.

For a security network, depending on the protection ranges and the protection coverage schemes of security systems, as well as the deployment-density of the guard field, the protection coverage area may contain vulnerable paths. The probability that an unauthorized target traverses the region through a vulnerable path gives insight about the level of security provided by the security network. In this paper, the protection model of security systems based on Neyman-Pearson Criterion is proposed. The protection probability at any position in a guard field, which is provided by a security system, can be calculated by the model. The weakest breach path of a security network, which is defined by the breach protection probability of an unauthorized target passing through a guard field, can be found.

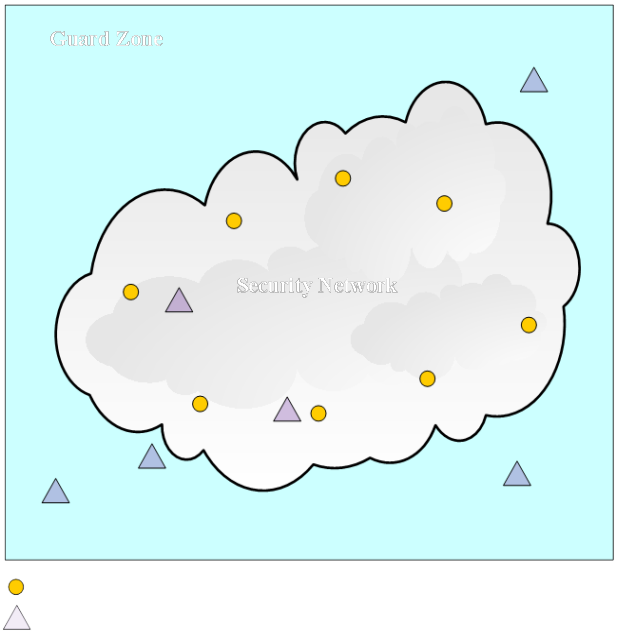

Figure 1. The abstract diagram of a security network.

The reminder of this paper is organized as follows: In the next section, the related work about seurity systems is introduced. In Section 3, the protection model is proposed, the weakest breach path of a security network is described and the method based on Dijkstra's shortest path algorithm to find the weakest breach path is put forward. After presenting the details of the problems formally, the results are simulated and analyzed in Section 4. Finally, conclusions are drawn in Section 5.

2. Related Work

In 1970's, U.S. Department of Energy's Sandia National Laboratories [1] first introduced the basic concepts of the Physical Protection System, from which the security system evolved. Subsequently, the U.S. Department of Energy put forward a model named adversary sequence diagram (ASD) [2], which was applied to the field of nuclear facilities protection. ASD can recognize vulnerability of physical protection systems by analyzing how hypothetical enemies might achieve their objects through various barriers. The path that is most easily broken through is considered weakest.

In 1981, Doyon [3] presented a probabilistic network model for a system consisting of guards, sensors, and barriers. He determined analytic representations for determining probabilities of intruder apprehension in different zones between site entry and a target object. In 1997 Kobza and Jacobson [4] have presented probability models for access security systems with particular applications to aviation security. In 1998, Hicks *et al.* [5] Presented a cost and performance analysis for physical protection systems. He considered the systems-level performance metric is risk, which is defined as follows.

$$Risk = p(A)\times\left[1-p(E)\right]\times C \quad (1)$$

where $p(A)$ is Probability of Attack, $p(E)$ is Probability of System Effectiveness, and C is Consequence.

After the events of September 11, 2001, public safety becomes the issue concerned by countries in the world. The concept of Physical Protection System has been changed. Some researchers from USA and Australia considered that a physical protection system is made up of people, architectures and electronic devices. So the concept of Security System was born. Many researchers were interested in assess the protection effectiveness of security systems through risk analysis. In 2004, Fischer [6] presented a very subjective risk analysis approach to rank threats using a probability matrix, criticality matrix, and vulnerability matrix. In 2006, Zhihua Chen [7] in Chinese People's Public Security University has proposed performance evaluation index and evaluation methods of crime prevention system for the assessment of the effectiveness and vulnerability of crime prevention system. This method is a qualitative assessment to the crime prevention system based on management science. In 2007, Garcia [8] gave an integrated approach for designing physical security systems. The protection effectiveness of a physical protection system was defined as the cumulative probability of detection from the start of an adversary path to the point determined by the time available for response. In 2009, Jonathan Pollet and Joe [9] Cummins put forward a performance assessment framework of the Security Systems, which considered not only the characteristics of the system, also the risk outside the system.

In recent years, some researchers considered that there were enormous uncertainty in the vulnerability evaluation of security systems, and they put forward some methods to reduce uncertainty. In 2011, Xu peida [10] thought that each individual component of the security system was modeled, and he used the Dempster-Shafer (D-S) evidence theory to analyze potential threats. Some literatures also proposed methods such as bounded intervals [11], exogenous dynamics [12], games of imperfect information [13-15], to characterize uncertainty in vulnerability analysis.

3. Protection Model and the Weakest Breach Path Problem Formulation

3.1. Neyman-Pearson Protection Model

In our research, there is a basic assumption that is a security system can eliminate any threat as long as a threat is detected. If a security system finds a threat, it will sound alarm. So each security system has its own false alarm rate, and it is regarded abstractly as the process of decision. The optimal decision rule that maximizes the detection probability subject to a maximum allowable false alarm rate α that is given by the Neyman-Pearson lemma [16]. Two hypotheses that represent the absence and presence of an unauthorized object are set up. The model computes the likelihood ratio of the respective probability density functions, and compares it against a threshold which is configured, and the false alarm constraint is satisfied. The process of a security system finding threats can be considered as the process signal reception. Suppose that an unauthorized object is a passive signal reception that happens in the presence of additive white Gaussian noise (AWGN) with zero mean and variance σ_n^2, as well as path-loss with path loss exponent η. Every breach protection decision is based on the processing of L data samples. If samples are collected fast enough, the distance between a security system and a object can be considered constant throughout the observation period. Let d_{vi} be the Euclidean distance between the grid point v and the security system i. Based on Neyman-Pearson Criterion with false alarm rate α, the protection probability of an unauthorized object at grid point v by the se-

curity system i is defined as follows.

$$p_{vi} = 1 - \Phi\left(\Phi^{-1}(1-\alpha) - \sqrt{\gamma L d_{vi}^{-\eta}}\right). \quad (2)$$

Where $\Phi(x)$ is the cumulative distribution function of the zero-mean, unit-variance Gaussian random variable at point x.

$$\gamma = \frac{A\psi}{\sigma_n^2}. \quad (3)$$

γ controls the per-datum signal-to-noise power ratio where the security system transmits information with power ψ, and A is a constant, which is regarded as signal propagation losses, emergency resources, information communication, etc.

3.2. Grid-Based Guard Field

In order to simplify the formulations, we consider the guard field as a cross-connected grid. A sample field model is presented in **Figure 2**.

The guard field model consists of the grid points and two auxiliary nodes which are the starting and the destination points. The aim of the target is to go through the guard field from the starting point that represents the insecure side to the destination point that represents the secure side. The horizontal axis is divided into $N-1$ and the vertical axis is divided into $M-1$ equal parts. Thus, there are $N \times M$ grid points plus the starting and destination points. For the sake of simplifying the notation, instead of using two dimensional grid point indices (x_v, y_v) where $x_v = 0,1,\cdots,N-1$ and $y_v = 0,1,\cdots,M-1$, we utilize a kind of one dimensional grid point index v which is calculated as $v = y_v N + x_v + 1$. The index of the starting point is defined as $v = 0$, and the index of the destination point is $v = NM + 1$. We use the connection matrix $c_{v,w} \in C_{(NM+2)\times(NM+2)}$ to represent the connections

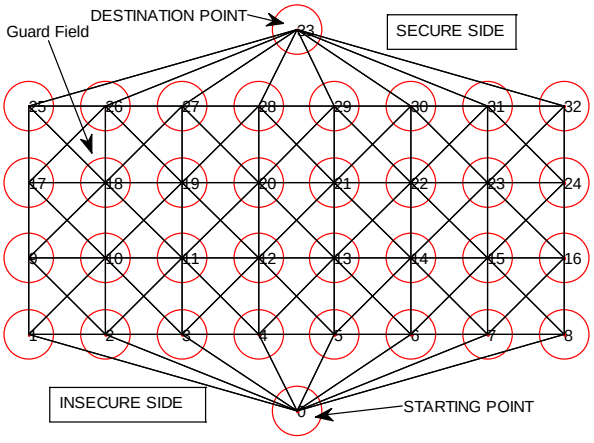

Figure 2. A sample field model constructed to find the vulnerable path for the guard field where the length is 8 m, the width is 4 m, and the grid size is 1m (N = 8, M = 4).

of the grid points. The matrix $c_{v,w}$ is defined as defined in Equation (4).

$$c_{v,w} = \begin{cases} 1 \text{ if } 0 < v, w < NM+1 \text{ and } (x_v - x_w, y_v - y_w) \in D \\ 1 \text{ if } v = 0 \text{ and } y_w = 0 \\ 1 \text{ if } w = NM+1 \text{ and } y_v = M-1 \\ 0 \text{ otherwise} \end{cases}. \quad (4)$$

$D = \{\{-1,0,1\} \times \{-1,0,1\}\} - \{(0,0)\}$ which is the set of possible difference-tuples of the two-dimensional grid point indices excluding $v = w$.

Using the grid-based field model above, the protection probabilities can be computed for every grid point through the Neyman-Pearson Protection Model of security systems.

3.3. The Weakest Breach Path Problem

The weakest breach path problem can be defined as finding the permutation of a subset of grid points $V = \{v_1, v_2, \cdots, v_k\}$ with which an object traverses from the starting point to the destination point with the least probability of being detected. The nodes v_{i-1} and v_i are connected to each other where $c_{v_{i-1},v_i} = 1$. The miss probability p of the most vulnerable path V is defined as follows.

$$p = \left(\sum_{v_i \in V}\left(1 - p_{v_i}\right)\right) \Big/ n. \quad (5)$$

Where p_{vi} is the breach protection probability associated with the grid point $v_i \in V$, n is the number of v_i.

The weakest breach path can be find by solving the following optimization problem as defined in Equation (6). x_{ij} denotes the edge which originates from the ith node and sinks in the jth node, s is the starting node and d is the destination node and C is as defined in Equation (4). In this formulation, the aim is to maximize the miss probability P defined in Equation (6). By using the logarithm function the optimization problem defined in Equation (7) can be changed to a linear program, where the aim is to find the minimum value.

$$\begin{aligned} &\max \sum_{v_i \in V}\left(1 - p_{v_i}\right) x_{ij} \text{ subject to} \\ &\sum_{(s,j)\in C} x_{sj} = 1; \sum_{(i,d)\in C} x_{id} = 1; \forall\, i = 1,2,\cdots,NM \\ &\sum_{(i,j)\in C} x_{ij} - \sum_{(k,i)\in C} x_{ki} = 0 \;\forall\, i = 1,2,\cdots,NM, \\ &x_{ij} = \begin{cases} 1 \text{ if } ith \text{ and } jth \text{ nodes are on the path and } c_{ij} = 1 \\ 0 \text{ otherwise} \end{cases} \end{aligned} \quad (6)$$

$$\min \sum_{(i,j)\in C} -\log(1 - p_i) x_{ij} \quad (7)$$

4. Simulation and Analysis

The grid-based field can be regard abstractly as a graph, so Dijkstra's shortest path algorithm can be employed to solve the weakest breach path problem too. The protection probability associated with the grid points cannot be used as weights of the grid points. Consequently, the weights of the grid points need be converted to a new measure d_v, which is defined as $d_v = -\log(1-p_v)$. This algorithm finds the path with the smallest negative logarithm value that is equal to be the weakest breach path. A sample security systems coverage graph and the weakest breach path is shown in **Figure 3**. Using the two-dimensional field model and adding the protection probability as the third axis.

Valleys and hills of protection probabilities are shown in **Figure 3**. The weakest breach path follows the valleys because the valleys denote the low protection probabilities.

4.1. Effects of Parameters on the Protection Probability

In this subsection, the effects of the Neyman-Pearson Protection Model parameters on the breach protection probability are analyzed. The deployment of security systems is random with uniform distribution. The parameters are shown in **Table 1**. The figures, which are presented in the following are the averages of 100 runs, depict how the environmental properties and the tolerance to the false alarms affect the vulnerability of a security network.

Ten security systems are deployed in a field where the parameters are same as in **Table 1**. The effect of the false alarm rate, α, on the breach protection probability P is shown in **Figure 4**, which essentially represents the network operating characteristics. With greater tolerance to false alarms, the P performance improves, and hence the protection range becomes larger. Sufficiently high signal noise ratio is necessary for an acceptable level of breach protection probability, which is relatively insensitive to the false alarm rate.

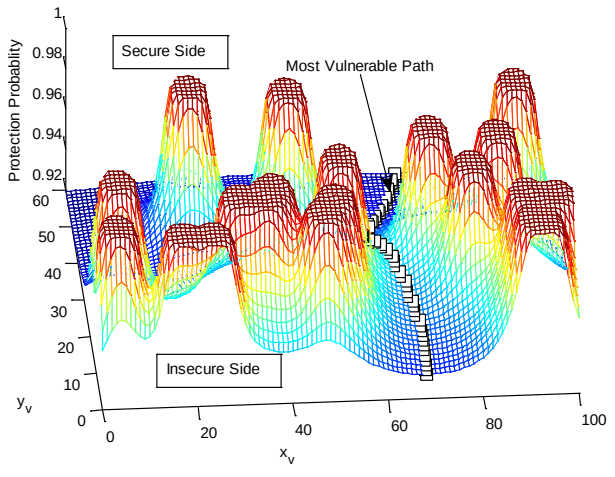

Figure 3. A sample of a guard field and vulnerable path where the length is 101 m, the width is 60 m, and grid size is 1 m. Twenty security systems are deployed in this field randomly. The Neyman-Pearson Protection Model is configured with L = 100, R = 9, α = 0.01, η = 2, γ = 20 *db*. The breach probability is 0.0639.

As shown in **Figure 4**, the false alarm rate α has a great effect on the breach protection probability P, and as α increases, the breach probability decreases, which reflects the protection probability p_v of an unauthorized object at grid v increases.

Although α is very influential on breach protection probability, η does not have an appreciable impact when the signal noise ratio is small. When the values of γ become large, η significantly increases the breach protection probability as shown in **Figure 5**.

This is due to the fact that the protection probability is inversely proportional to the distance on the order of η. The effect of η is very significant when $\eta \le 4$.

As shown in **Figure 6**, when the signal noise ratio γ increases, the breach protection probability decreases,

Table 1. Parameter values used in the simulations for Neyman-Pearson Protection Model.

Parameters	Value
Length of the field	51 m
Width of the fileld	41 m
Grid Size	1 m
Numbers of Security Systems	10
α	0.1
η	2
γ	20 db
L	100

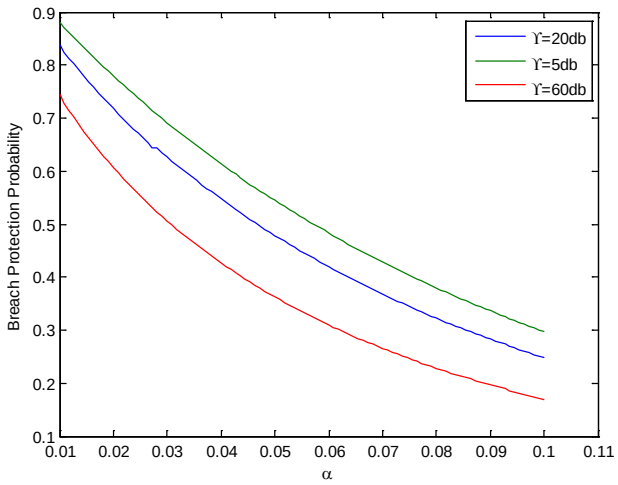

Figure 4. The effect of α on the breach protection probability.

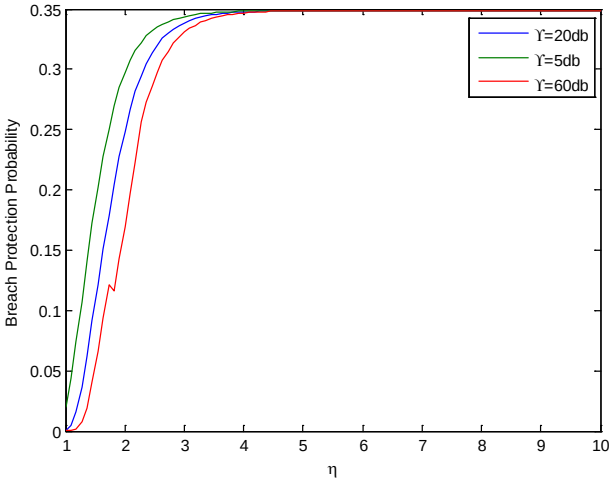

Figure 5. The effect of η on the breach protection probability,

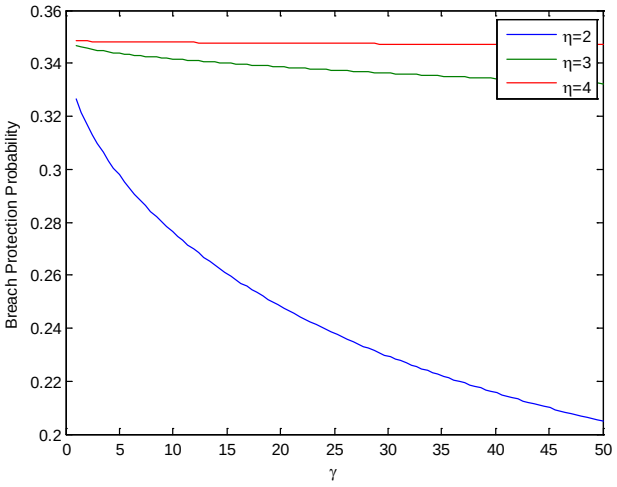

Figure 6. The effect of γ on the breach protection probability.

which indicates that the protection probability of the security network improves and the protection performance increases. If targets are closer to security systems, signal noise ratio has more influence on the protection probability. When the parameter $\eta \geq 3$, the effect of the signal noise ratio γ becomes very small.

4.2. Effects of Number of Security Systems on the Protection Probability

While analyzing the required number of security systems for a given breach probability, one case of random deployment is considered. The case is assumed that security systems are uniformly distributed along both the vertical and horizontal axes. The effect of numbers of security system in a field on the breach protection probability is shown in **Figure 7**.

As the density of security systems increases in a field, the breach protection probability tends to stabilize, which approximates the zero. The results suggest that there is a

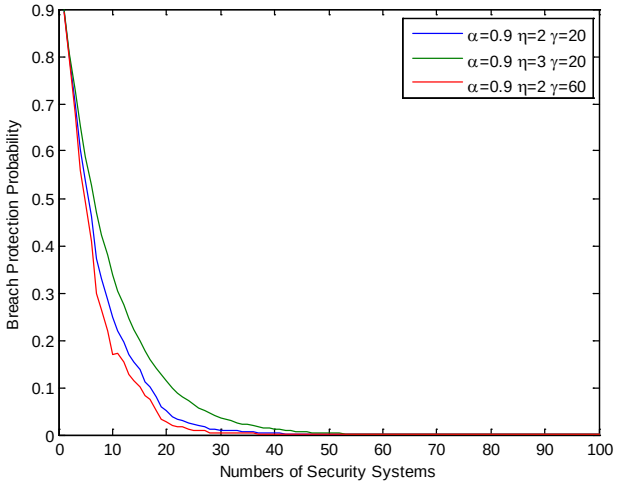

Figure 7. The effect of numbers of security systems on the breach protection probability.

saturation point after which randomly placing more security systems does not significantly impact the breach protection probability of a security network in a field.

When the signal noise ratio is same, α affects the breach protection probability more than η (see **Figures 4** and **5**), so the false alarm rate α is more influential here too. The rapid decrease in the breach protection probability can be explained by the fact as the density of security systems is saturated in a field, grid points are covered with high protection probabilities. Consequently, at the beginning, an additional security system decreases the breach protection probability considerably, however, once the saturation is reached, the affection of numbers of security systems is not so large anymore.

5. Conclusion

In this paper, we put forward the Neyman-Pearson protection model of security systems that can be employed to find the weakest breach path of a security network. In order to find the weakest breach path, we apply Dijkstra's shortest path algorithm by using the negative log of the breach protection probability as the grid point weights. Finally, the effect of parameters of Neyman-Pearson protection model on breach protection probability is studied by MATALAB simulation. The simulation experiments show that the false alarm rate is the most influential parameter on the breach protection probability.

6. Acknowledgements

Thanks for the assistance from National Science Foundation of China (No. 61170023), the Major National Science and Technology Special Projects of China (2010ZX 03004-003-03, 2010ZX03004-001-03), National Nature Science Foundation of China (No. 60832002). The authors would like to thank Ruimin Hu. IEEE Member, pro-

fessor of School of Computer, Wuhan University, Ren Pin teaching assistant Department of Electrical Engineering and Computer Science, Northwestern University USA, for their thoughtful comments.

REFERENCES

[1] H. A. Bennett and M. T. Olascoaga, "Evaluation Methodology for Fixed-Site Physical Protection Systems," *Nuclear Materials Management*, Vol. 9, 1980, pp. 403-410.

[2] J. L. Darby, B. E. Simpkins and B. R. Key, "A Microcomputer Code for Evaluating Physical Security Effectiveness Using Adversary Sequence Diagrams," *Nuclear Materials Management*, Vol. 15, 1986, pp. 242-245.

[3] L. R. Doyon, "Stochastic Modeling of Facility Security-Systems for Analytical Solutions," *Computers & Industrial Engineering*, Vol. 5, No. 2, 1981, pp. 127-138. http://dx.doi.org/10.1016/0360-8352(81)90020-6

[4] J. E. Kobza and S. H. Jacobson, "Probability Models for Access Security System Architectures," *Journal of the Operational Research Society*, Vol. 48, 1997, pp. 255-263.

[5] M. J. Hicks, M. S. Snell, J. S. Sandoval and C. S. Potter, "Physical Protection Systems Cost and Performance Analysis: A Case Study," *IEEE Aerospace and Electronic Systems Magazine*, Vol. 14, No. 4, 1999, pp. 9-13. http://dx.doi.org/10.1109/62.756078

[6] E. H. Robert Fischer and D. Walters, "Introduction to Security," 9th Edition, Elsevier, 2012, p. 544.

[7] Z. Chen, "The Research and Practice on the Evalation of Effectiveness on Security System. *China Security*, 2007.

[8] M. L. Garcia, "The Design and Evaluation of Physical Protection Systems," Butterworth-Heinemann, Boston, 2001.

[9] J. Pollet and J. Cummins, "All Hazards Approach for Assessing Readiness of Critical Infrastructure," *IEEE Conference on Technologies for Homeland Security*, Boston, 11- 12 May 2009, pp. 366-372.

[10] P. Xu, X. Su, J. Wu, X. Sun, Y. Zhang, Y. Deng, "Risk Analysis of Physical Protection System Based on Evidence Theory," *Journal of Information and Computational Science*, Vol. 7, 2010, pp. 2871-2878.

[11] M. E. Nikoofal and J. Zhuang, "Robust Allocation of a Defensive Budget Considering an Attacker's Private Information," *Risk Analysis*, Vol. 32, 2012, pp. 930-943. http://dx.doi.org/10.1111/j.1539-6924.2011.01702.x

[12] K. Hausken and J. Zhuang, "The Timing and Deterrence of Terrorist Attacks Due to Exogenous Dynamics," *Journal of the Operational Research Society*, Vol. 63, 2012, pp. 726-735. http://dx.doi.org/10.1057/jors.2011.79

[13] M. Golalikhani and J. Zhuang, "Modeling Arbitrary Layers of Continuous-Level Defenses in Facing with Strategic Attackers," *Risk Analysis*, Vol. 31, 2011, pp. 533-547. http://dx.doi.org/10.1111/j.1539-6924.2010.01531.x

[14] J. Zhuang, V. M. Bier and O. Alagoz, "Modeling Secrecy and Deception in a Multiple-Period Attacker-Defender Signaling Game," *European Journal of Operational Research*, Vol. 203, 2010, pp. 409-418. http://dx.doi.org/10.1016/j.ejor.2009.07.028

[15] J. Zhuang and V. M. Bier, "Balancing Terrorism and Natural Disasters-Defensive Strategy with Endogenous Attacker Effort," *Operations Research*, Vol. 55, 2007, pp. 976-991. http://dx.doi.org/10.1287/opre.1070.0434

