Risk Assessment and Vulnerable Path in Security Networks Based on Neyman-Pearson Criterion and Entropy

Ruimin Hu[ba], Haitao Lv[a*], and Jun Chen[a]
[a]National Engineering Research Center for Multimedia Software, Wuhan University, Wuhan, China
[b]School of Computer, Wuhan Univeristy, Wuhan, China

Abstract: In this paper, the protection coverage area of a security system is considered. The protection coverage is determined by applying the protection model of security systems, which is brought forward according to Neyman-Pearson Criterion. The protection model can be used to define the protection probability on a grid-modeled field. The security systems deployed in a guard field are regarded abstractly as a diagram. On the basis of the entropy theory, we propose the risk entropy, which can be used to quantificationally evaluate the risk of arbitrary position in an area. Using a graph model for perimeter, we use Dijkstra's shortest path algorithm to find protection breach paths. The protection probability on the vulnerable path is considered as the risk measure of a security network. Furthermore, we study the effects of some parameters on the risk and the breach protection probability and present simulations. Ultimately, we can gain insight about the risk of a security network.

Keywords: Risk Entropy, Neyman-Pearson Criterion, Security Network, Protection Breach Path.

1. INTRODUCTION

Security is surely not a new concept. The idea of protecting cities through the construction of fortifications dates back thousands of years. Following the excavation of Jericho and analysis of the fortifications and artifacts located there, Kenyon[1] found that the earliest walls and towers of that ancient city dated prior to 6000 B. C. The walls of Jericho indicate that as long as mankind has been protecting people and propery from adversaries have existed as a motivation to provide protection. As threats change, so must the safeguards. The events of September 11, 2001 came as a shocking announcement that the threats against the world had changed. Security has emerged as a pressing social concern. Currently, the society security problem has been attached importance by many countries. In order to maintan social public safety, many security systems have been constructed in cities in the world. A security system can be considered as a complex physical protection system, which is made up of securities or guards, architectures and electronic devices and consists of some subsystems, such as the intrusion alarm system, the video surveillance system, the access control system, the explosion-proof security check system, etc. Securtiy 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 the security systems deployed in a guard field are regarded abstractly as a diagram of security network as shown in Figure 1. Each of yellow filled circle represent a security system, and every triangle represents a protection target.

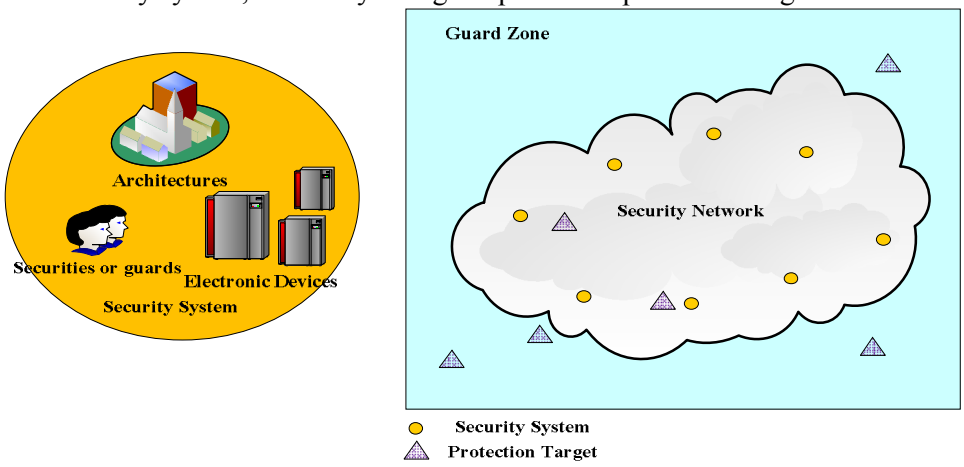


Figure 1. The abstract diagram of a security network

The reminder of this paper is organized as follows: In the next section, the related work about risk assessment of security systems is introduced. In Section 3, the risk entropy based on the Shannon information theory and Neyman-Pearson protection model are put forward. We describe the most vulnerable path problem and present how to use the model to find the most vulnerable path of a security network. Dijkstra's shortest path algorithm is introduced as a solution to this problem by defining a grid-based guard field. After presenting the details of the problem formally, the results are stimulated and analyzed in Section 4. Finally, we draw our conclusions in Section 5.

2. RELATED WORKS

In 1970's, U.S. Department of Energy's Sandia National Laboratories[2] 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)[3], which was applied to the field of nuclear facilities protection. ASD can recognize vulnerability of physical protection systems by analyzing how hypothetical adversaries might achieve their objects through various barriers. The path that is most easily broken through is considered weakest. In 1981, Doyon[4] 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[5] presented probability models for access security systems with particular applications to aviation security. In 1998, Hicks etal.[6] put forward a cost and performance analysis for physical protection systems. He considered the systems-level performance metric was risk, which was defined as follows.

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

where $p(A)$ is the probability that the attack on a facility will occur, $p(E)$ is the probability that a physical protection system prevents an adversary from making an attack successfully, and C is the extent of consequence.

After the events of September 11, 2001, public safety becomes the issue concerned by many countries. The concept of Physical Protection System began to change and some researchers from USA and Australia considered that a physical protection system should consist of guards, architectures and electronic devices. Since then a physical protection system is also called a security system and many researchers have been interested in assessing the protection effectiveness of security systems through risk analysis. In 2004, Fischer[7] developed a very subjective risk analysis approach to rank threats using a probability matrix, a criticality matrix, and a vulnerability matrix. In 2006, Zhihua Chen[8] evaluate the protection effectiveness of a security system through establishing the corresponding indexs based on expert opinions. In 2007, Garcia[9] gave an integrated approach for designing physical security systems. The risk 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[10] Cummins put forward a risk 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 risk evaluation of secrutiy systems, and they put forward some methods to reduce uncertainty. In 2011, Xu peida[11] thought that each individual component of the security system was modelled, and he used the Dempster-Shafer (D-S) evidence theory to analyse potential threats. Zhuang Jun and his colleagues also proposed methods such as bounded intervals[12], exogenous dynamics[13], games of imperfect information[14-16], to characterize uncertainty in risk analysis, and in 2013 they[17, 18] presented an approach based on game theory and considered the cases where the defender had resource constraints. In considering series systems, they differentiated between cases where atttackers had perfect knowledge of the system's defenses or no prior knowledge of the defensive configuration. All in all, the above methods or models are still on the basis of probability.

3. Risk ENTROPY, NEYMAN-PEARSON PROTECTION MODEL, VUNLNERABLE PATH PROBLEM

The security level of a security network can be described by the breach protection probability, which is defined as the maximum protection probability of an unauthorized target passing through a field via the most vulnerable path which can be defined as finding the breach protection probability of the most vulnerable path in a security network. The protection probability on the most vulnerable path is consedered as the risk measure of a security network. In this section, the risk entropy and Neyman-Pearson protection model are put forward. Then a grid-based field method is introduced. Finally, we present how to formulate and solve the most vulnerable path problem.

3.1. Risk Entropy

Entropy, which was brought forward by French scientist Rudolf Clausius[19] in 1865, is a state function of the second law of thermodynamics. Austrian physicist Boltzmann [20]firstly used entropy to solve some statistical problems. Frome then on, entropy becomes a measure of disorder or uncertainty of systems. In 1948, American scientist Shannon[21] proposed the concept of information entropy, which can be used to measure the average information amount in the process of communication. Information entropy is also called Shannon entropy denoted by $H(X)$, which is defined as follows:

$$H(X) = E\left[\log_2 \frac{1}{p(x_i)}\right] = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \qquad (2)$$

Where $p(x_i)$ is the probability of the discrete random variable x_i.

Due to the uncertainty of information transmission, Shannon entropy is used to measure the amount of information. The risk of a security system is usually judged by the ratio of completion of a protection task. So there are a lot of uncertain factors to affect the risk of a security system. The higher the ratio of completion protection task is , the less the uncertainty associated with the risk of a security system is. Similar to Shannon entropy, the uncertain factors can be measured by entropy.

In order to quantitatively evaluate uncertain factors, Risk entropy is proposed in this article. Suppose that there are n independant factors that affect the protection ability of a security system. The completing task probability of each factors is expressed as $R_i(i=1,2,\cdots,n)$, and the weight of every factor is $\omega_i(i=1,2,\cdots,n)$. The risk entropy can be defined as:

$$I_{s_i} = -\sum_{i=1}^{n} \omega_i R_i \ln R_i \qquad (3)$$

Where I_{s_i} is the risk entropy of a security system.

As shown in figure 1, a security network is made up of multiple security systems. The risk of a security network is associated with the most vulnerable path from starting point to destination. In this paper, each security system is hypothesized to be independent. Suppose that there are n security systems in a guard zone, the risk entropy of a security network can be expressed as follows:

$$I = \sum_{i=1}^{n} I_{s_i} \qquad (4)$$

3.2. 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, so that 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 security system i is defined as follows.

$$p_{vi} = 1 - \Phi\left(\Phi^{-1}(1-\alpha) - \sqrt{\gamma L d_{vi}^{-\eta}}\right) \tag{5}$$

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

3.3. Vulnerable Path Problem

In order to simplify the problems of risk assessment, we consider the guard field as a cross-connected grid. A sample field model is presented in Fig.2.

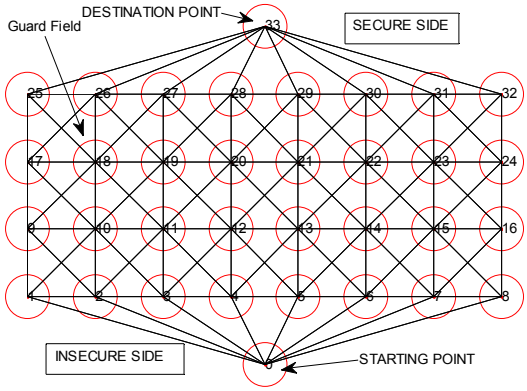


Figure 2. A sample field model constructed to find the vulnerable path for the guard field where the length is 8 m, the width is 4 m, and the grid size is 1 m (N=8, M=4)

The guard field model consists of the grid points and two auxiliary nodes which are the staring and the destination points. The aim of the target is to go through the guard field from the staring 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 of the grid points. The matrix $c_{v,w}$ is defined as defined in (6).

$$c_{v,w}=\begin{cases}1 \ if \ 0<v,w<NM+1 \ and \ (x_v-x_w, y_v-y_w)\in D\\ 1 \ if \ v=0 \ and \ y_w=0\\ 1 \ if \ w=NM+1 \ and \ y_v=M-1\\ 0 \ otherwise\end{cases} \tag{6}$$

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

The most vulnerable 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 protection probability. The nodes v_{i-1} and v_i are connected to each other where $c_{v_{i-1},v_i}=1$. The miss protection probability p of the most vulnerable path V is defined as follows.

$$p=\prod_{v_i\in V}\left(1-p_{v_i}\right) \tag{7}$$

Where p_{vi} is the protection probability associated with the grid point $v_i\in V$, n is the number of v_i. The most vulnerable path can be find by solving the following optimization problem

$$\begin{aligned}&\max\prod_{v_i\in V}\left(1-p_{v_i}\right)x_{ij} \ subject\ to\\ &\sum_{(s,j)\in C}x_{sj}=1;\ \sum_{(i,d)\in C}x_{id}=1;\forall i=1,2,\cdots,NM\\ &\sum_{(i,j)\in C}x_{ij}-\sum_{(k,i)\in C}x_{ki}=0\ \forall i=1,2,\cdots,NM,\\ &x_{ij}=\begin{cases}1 \ if \ ith \ and \ \ jth \ nodes \ are \ on \ the \ path \ and \ c_{ij}=1\\ 0 \ otherwise\end{cases}\end{aligned} \tag{8}$$

Where 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 (6). In this formulation, the aim is to maximize the miss probability P defined in (8).

4. SIMULATION AND ANALYSIS

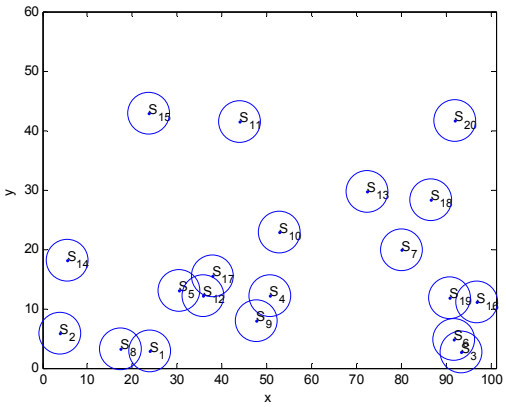
4.1. The Most Vulnerable Path

Table 1: The coordinates of the security systems deployed in an area

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}
X	23.81	3.88	93.2	50.62	30.33	91.64	80.02	17.26	47.61	52.69
Y	2.95	5.82	2.68	12.24	13.01	4.74	19.87	3.2	7.97	22.81
	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}
X	43.92	35.76	72.32	5.57	23.51	96.7	37.83	86.44	90.59	91.79
Y	41.48	12.22	29.76	18.1	42.88	11.11	15.53	28.28	11.78	41.72

The grid-based field can be regard abstractly as a graph, so Dijkstra's shortest path algorithm can be employed to solve the most vulnerable path problem too. The protection probability associated with the grid points can not 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 most vulnerable path. We assume that twenty security systems, which have same parameters, are randomly deployed in a rectangular area, of which the length and width are respectively 100 m and 60 m. The coordinates of the starting point and the destination are (50,-1) and (50,61). The coordinates of the security systems

are shown in Table1. The distribution of the security systems in the field is shown in Fig. 3. A sample security systems coverage graph and the weakest breach path is shown in Fig. 4. Using the two-dimensional field model and adding the protection probability as the third axis.



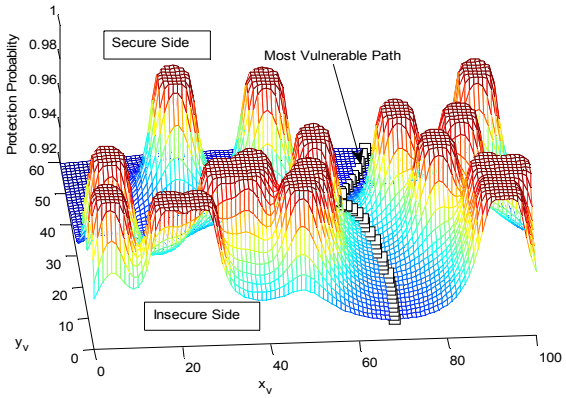


Figure 3. The distribution of the security systems deployed in a guard field

Figure 4. 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 $L=100, R=9, \alpha=0.01, \eta=2, \gamma=20db$. The breach probability is 0.0639

4.2. Effects of Parameters on the Risk and Protection Probability

In this section, the effects of the Neyman-Pearson Protection Model parameters on the risk and breach protection probability are analyzed. The deployment of security systems is random with uniform distribution. The parameters are shown in Table 2. 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 risk of a security network.

Table 2: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	20db
L	100

Ten security systems are deployed in a field where the parameters are same as in Table Ⅱ . The effect of the false alarm rate, α , on therisk and breach protection probability P is shown in Fig. 5, 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. As shown in Fig. 5, the false alarm rate α has a great effect on the breach protection probability and risk. As α increases, the breach probability decreases, which reflects the protection probability p_v of an unauthorized object at grid v increases.

p_{vi} is as defined in (5). When α increases, the risk entropy decreases after temporarily increasing. Large false alarm rate α represents that a security system is very sensitive to risks. So the false alarm rate of a security system is configured an appropriate value, which can improve the protection ablility of a security system.

Although α is very influential on the risk and the 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 and risk as shown in Fig. 6. 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 $\eta \le 4$. The risk and breach protection probability will tend to stabilize. According to the scenario shown in Table 1, as η increases the breach protection probability approximates 0.35 and the risk approximates 11.4495. As shown in Fig. 7, when the signal noise ratio γ increases, the breach protection probability and risk decreases, which indicates that the protection probability of the security network improves and the protection performance increases so that the risk of a security system decreases. If targets are closer to security systems, signal noise ratio has more influence on the protection probability and the risk. When the parameter $\eta \ge 3$, the effect of the signal noise ratio γ becomes very small.

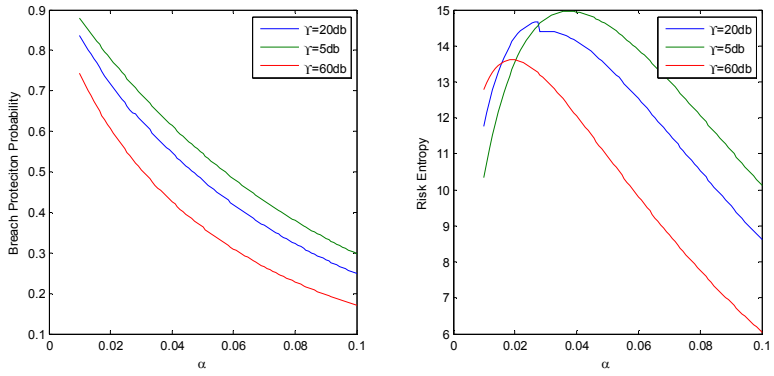


Figure 5. The effect of α on the risk and the breach protection probability

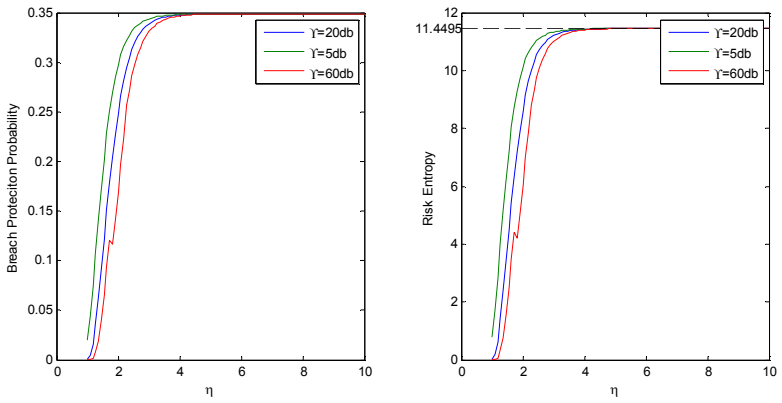


Figure 6. The effect of η on the risk and the breach protection probability

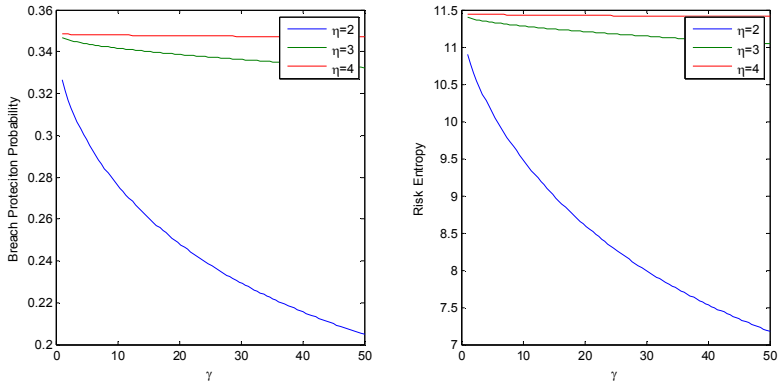


Figure 7. The effect of γ on the risk and the breach protection probability

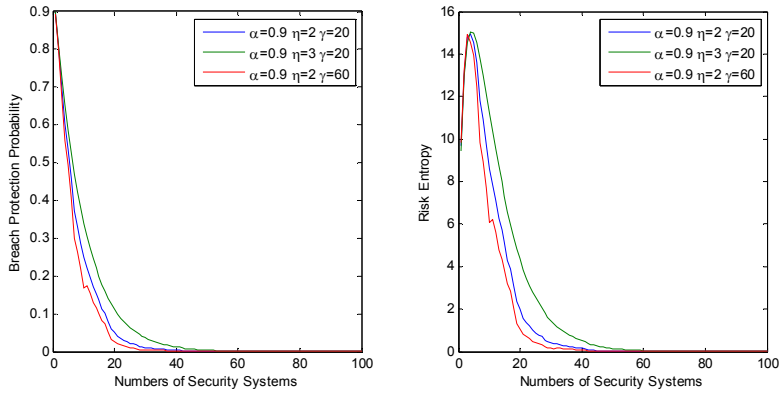


Figure 8. The effect of numbers of security systems on the breach protection probability and the risk entropy

4.3. Effects of Number of Security Systems on the Risk and the Protection Probability

While analyzing the required number of security systems for a given breach probability or a level of risk, 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 risk and the breach protection probability is shown in Fig. 8. As the density of security systems increases in a field, the breach protection probability and the risk tend to stabilize, which approximate the zero. The results suggest that there is a 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 and the risk more than η (see Fig. 5 and 6), so the false alarm rate α is more influential here too. The rapid decrease in the risk and 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 risk and the breach protection probability considerably, however, once the saturation is reached, the affection of numbers of security systems is not so large anymore.

4.4. Effects of Field Shape on the Risk and the Protection Probability

According to the application, the shape of grid-based fields may vary. Thus, the effect of the field shape on the breach protection probability will provide useful insights for designing better security network. While analyzing the effect of a field's shape on the breach protection probability, three cases are considered. The first case is a field where the length is 50 m and the width is 40 m. The second case is a field where the length is 100 m and the width is 20 m. The last case is that a field where the length is 200 m and the width is 10 m. Every case employs two kinds of random deployment of security systems. One is that the security systems are uniformly distributed along both the vertical and horizontal axes. The other is that the security systems are deployed uniformly along the horizontal axis and normally distributed along the vertical axis with mean $M/2$ and standard deviation of 10% of the width of the field. The three cases have same area, and the parameters are shown in Table3.

Table 3:Parameter values used in the simulations for the effect of the shape of fields

Parameters	Case1	Case2	Case3
Length	50 m	100 m	200 m
Width	40 m	20 m	10 m
Grid Size	1 m	1 m	1 m
α	0.1	0.1	0.1
η	2	2	2
γ	20db	20db	20db
L	100	100	100

As shown in Fig. 9, the effect of the field shape on the breach protection probability and risk entropy are depicted on the basis of uniformly and normally distributed y-axis schemes, respectively. For a given number of security systems, the breach protection probability and the risk entropy are larger for narrow and long fields compared to the thicker and short fields. As the field gets shorter and thicker, the difference between the required numbers of security systems for the uniformly and normally distributed schemes is more and more obvious.

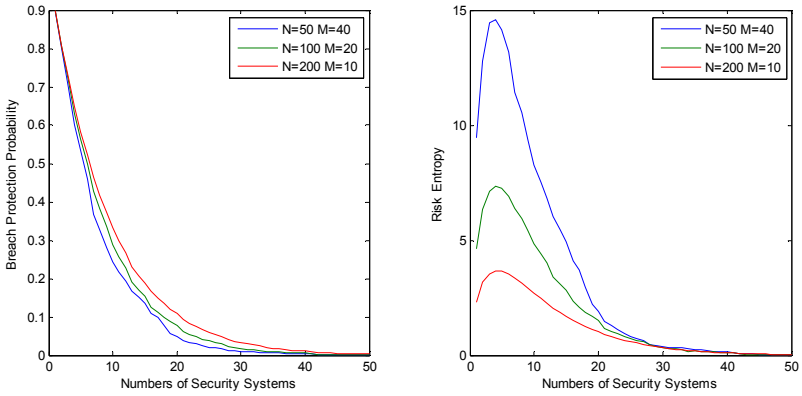


Figure 9. The effect of the shape of a field on the risk and the breach probability

Table 4:Comparisons of breach protection probabilities between uniform distribution and normal distribution in case 1.

Numbers	Uniform Distribution	Normal Distribution
1	0.895434	0.894791
2	0.803099	0.802583
3	0.698366	0.687385
4	0.600218	0.579151
5	0.534645	0.513832
6	0.458572	0.432987
7	0.368046	0.358656
8	0.327027	0.309101
9	0.280573	0.266564
10	0.244496	0.221933

Table 5:Comparisons of risk entropy between uniform distribution and normal distribution in case 1.

Numbers	Uniform Distribution	Normal Distribution
1	9.443946	9.478494
2	12.79884	12.81545
3	14.44238	14.51576
4	14.16493	13.97594
5	13.1877	12.83587
6	11.43323	11.04486
7	10.53394	10.38812
8	9.353526	9.235092
9	8.276395	7.52695
10	7.529026	6.822215

As shown in Table4 and Table5, when the numbers of security systems are less than four, the risk entropy of uniform distribution is less than the risk entropy of normal distribution, but as the numbers of the security systems increases, the normally distributed scheme is more effective on the required number of security systems, because it produces a deployment where many security systems are placed near the center line of the field along the horizontal axis. This deployment scheme produces a well-secured barrier in the middle of a field.

5. CONCLUSIONS

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 network, 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. Considering a security network, some of the design challenges may be listed as follows: How to find the most vulnerable path of a security networks? How to quantitatively assess the risk of security systems? how many security systems are to be deployed to provide a required security level ? In this paper, we analyze the above challenges and put forward a model, which is on the basis of entropy theory and Neyman-Pearson criterion, to quantitatively assess the risk of a security system. We assume that security systems are randomly deployed over an area. Utilizing the model, we can find the most vulnerable path of a security network that consists of the security systems and evaluate the risk of the security network that is defined by the breach protection probability of an unauthorized target passing through the guard field. We propose a method to determine the required number of security systems to provide a predetermined security level in different fields. Finally we study the variation of the breach protection probability and the risk with the change of the parameters of the model.

A security network will be prone to fail if some security systems in the network die due to their limited enery resources. Therefore, the failures of security systems shall be modelled and incorporated into the most vulnerable path problem. As a future work, we will consider the failures of security systems and simulate the reliability of a network throughout the entire life of a security network. Furthermore, when the number of security systems in a field is very limited, we will consider the mobile character of security systems to construct a scheme to get an acceptable security level.

Acknowledgements

Thanks for the assistance from National Science Foundation of China (No. 61170023), the Major National Science and Technology Special Projects of China (2010ZX03004-003-03), National Nature Science Foundation of China (No. 61231015). The authors would like to thank Ren Pin teaching assistant Department of Electrical Engineering and Computer Science, Northwestern University USA, for his thoughtful comments.

References

[1] Kenyon KM. *Digging up Jericho / Kathleen M. Kenyon*, 1957, London: Benn.

[2] Bennett HA, Olascoaga MT. *Evaluation Methodology For Fixed-Site Physical Protection Systems,* Nuclear materials management, 9:pp.403-410(1980).

[3] Darby JL, Simpkins BE, Key BR. Seapath, *A Microcomputer Code For Evaluating Physical Security Effectiveness Using Adversary Sequence Diagrams*, Nuclear materials management, 15:pp.242-245(1986).

[4] Doyon LR. *Stochastic modeling of facility security-systems for analytical solutions*, Computers & Industrial Engineering, 5:pp.127-138(1981).

[5] Kobza JE, Jacobson SH. *Probability models for access security system architectures*, Journal of the Operational Research Society, 48:pp.255-263(1997).

[6] Hicks MJ, Snell MS, Sandoval JS, Potter CS. *Physical protection systems cost and performance analysis: a case study*, Aerospace and Electronic Systems Magazine, IEEE. 14:pp.9-13(1999).

[7] Robert Fischer EH, David Walters. *Introduction to Security, Ninth Edition*: ELSEVIER; 2012.

[8] Chen Z. *The research and practice on the evalation of effectiveness on security system*. China Security. pp.11-13(2007).

[9] M.L.Garcia. *The Design and Evaluation of Physical Protection Systems*. 2011, Boston: Butterworth-Heinemann.

[10] Pollet J, Cummins J. *All hazards approach for assessing readiness of critical infrastructure. Technologies for Homeland Security*, 2009 HST '09 IEEE Conference on2009. pp. 366-372(2009).

[11] Xu P, Su X, Wu J, Sun X, Zhang Y, Deng Y. *Risk analysis of physical protection system based on evidence theory*. Journal of Information and Computational Science. 7:pp.2871-2878(2010).

[12] Nikoofal ME, Zhuang J. *Robust Allocation of a Defensive Budget Considering an Attacker's Private Information*. Risk Analysis. 32:pp.930-943(2012).

[13] Hausken K, Zhuang J. *The timing and deterrence of terrorist attacks due to exogenous dynamics*. Journal of the Operational Research Society. 63:pp.726-735(2012).
[14] Golalikhani M, Zhuang J. *Modeling Arbitrary Layers of Continuous-Level Defenses in Facing with Strategic Attackers*. Risk Analysis. 31:pp.533-547(2011).
[15] Zhuang J, Bier VM, Alagoz O. *Modeling secrecy and deception in a multiple-period attacker-defender signaling game*. European Journal of Operational Research. 203:pp.409-418(2010).
[16] Zhuang J, Bier VM. *Balancing terrorism and natural disasters-defensive strategy with endogenous attacker effort*. Operations Research. 55:pp.976-991(2007).
[17] Shan X, Zhuang J. *Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender¨Cattacker game*. European Journal of Operational Research. 228:pp.262-272(2013).
[18] Shan X, Zhuang J. *Subsidizing to disrupt a terrorism supply chain[mdash]a four-player game*. 2013,J Oper Res Soc..
[19] Clausius R. *The Mechanical Theory of Heat: With Its Application to the Steam-engine and to the Physical Properties of Bodies*: 1867,Van Voorst.
[20] Sandler SI. *Chemical, Biochemical, and Engineering Thermodynamics:* 2006,Wiley.
[21] Shannon CE. *A mathematical theory of communication*. SIGMOBILE Mob Comput Commun Rev. 5pp.:3-55(2001).