Risk Evaluation for Security Network Based on Protection Model and Risk Entropy

Haitao Lv
National Engineering Research Center for Multimedia Software Wuhan University
Lvhaitao0301@gmail.com

Ruimin Hu
Scholl of Computer Wuhan University
National Engineering Research Center for Multimedia Software Wuhan University
Hurm1964@gmail.com

Abstract— **A security network is considered as a diagram of security systems deployed in different places in a guard zone. For a security network, its risk is an important metric to judge whether its protection effectiveness is good or not. How to evaluate the risk of a security network? In this paper, the protection coverage area of a security system is considered. We put forward the protection model that can be used to determine the protection coverage of a security system and define the protection probability on a grid-modeled field. According to the Shannon Information Theory, we propose the risk entropy, which can be used to quantitatively evaluate the risk of arbitrary position in an area. We use Dijkstra's shortest path algorithm to find the weakest protection path. The protection probability on the weakest protection path is considered as the risk measure.**

Keywords-Security Network; Risk Entropy; Protection Model; Risk Evaluation

I. INTRODUCTION

Since 911 events, public safety has emerged as an urgent and serious social problem. In China, in order to improve social public safety, a lot of security systems have deployed in cities.With the rapid development of information technology, multiple security systems such as the intrusion alarm system, the video surveillance system, the access control system, the explosion-proof security check system, etc, make up of a network. For a security network, the protection coverage area of a security network may exist vulnerable paths. The probability that an adversary traverses an area through the most vulnerable path to attack assets gives insight about the risk level of a security network. Some of risk evaluation challenges of a security network may be listed as follows:

- How could the protection probability and the protection coverage of a security system be modelled and determined?
- How to find the vulnerable paths of a security network?
- How to quantificationally evaluate the risk of a security network.

In this paper, we assume that security systems are randomly deployed over an area. We bring forward the protection model of security systems and risk entropy, which can be used to calculate the protection probability and determine the protection coverage. We also provide a method to find the most vulnerable path, which is defined by the breach protection probability of an adversary passing through an area.

The reminder of this paper is organized as follows. In Section 2, the related work about risk evaluation of security systems is introduced. In Section 3, risk entropy and protection model of a security system are put forward. How to find the most vulnerable path problem is described. In Section 4, the model and algorithm are simulated. Finally, we conclude our paper in Section 5.

II. RELATED WORK

Security systems are different from ordinary information systems. A security system is made up of persons, buildings and electronic instruments. Security systems come from physical protection systems. In 1970's, the concepts of a physical protection system [1] was firstly introduced by Sandia National Laboratories of U.S. Department. Subsequently, the adversary sequence diagram (ASD) [2] was brought forward by U.S. Department of Energy to evaluate the vulnerability of a security system by analyzing the probability of assets being attacked by adversaries. The path that is most easily broken through is considered weakest. In 1997 Kobza and Jacobson [3] have presented probability models for access security systems with particular applications to aviation security. In 1998, Hicks etal. [4] Presented a cost and performance model to analyze the vulnerability of physical protection systems. He considered the vulnerability is risk, which is defined as follows.

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

After 911 events, 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 vulnerability of security systems through risk analysis.In 2004, Fischer [5] used a probability matrix and criticality matrix to rank the threats faced by a security system, and then he constructed the risk matrix according to the levels of threats. In 2009, Jonathan Pollet and Joe Cummins [6] proposed a risk assessment framework of Security Systems according to the characteristics of the system itself and the external environment factors. In 2011, Xu peida [7] used the Dempster-Shafer (D-S) evidence theory to analyze the vulnerability of a security system. In recent years, some methods[8] such as bounded intervals, exogenous dynamics,

etc, were also put forward to resolute the risk evaluation of a security system. But all in all, the current risk evaluation models are all aimed at a single independent system, so the models cannot be used to evaluate the risk of a security network made of multiple security systems.

III. PROTECTION MODEL AND RISK ENTROPY

A. *Protection Model of a Security System*

Security system share one common fact, which is that protection ability diminishes as distance increases. We assume that the protection probability that a security system protects assets on arbitrary grid point is nonnegative. According to this, for a security system s_i , the protection model is defined as follows.

$$P_{vi} = \begin{cases} 0 & if\ r+r_e \le d_{vi} \\ e^{-\lambda\alpha^{\beta}} & if\ r_e > |r-d_{vi}| \\ 1 & if\ r-r_e \ge d_{vi} \end{cases} \quad (1)$$

Where P_{vi} is the protection probability on grid point v .

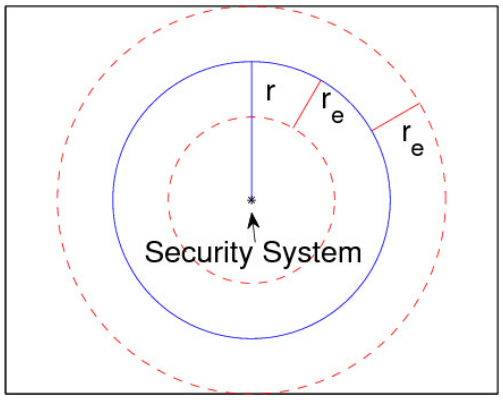

Figure 1. The relationship of r and r_e

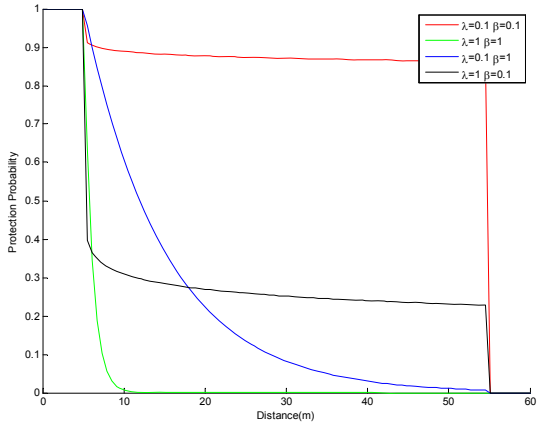

Figure 2. Sample security systems protection probabilities with r=30m and $r_e = 25m$

$r_e\,(r_e < r)$ is a measure of uncertainty in protection of a security system. λ and β are parameters that represent different characteristics of security systems. d_{vi} is the distance between a security system and the grid point v and $\alpha = d_{vi} - r + r_e$. The parameters r , r_e , λ and β are adjusted on the basis of the physical properties of security systems. In particular, r and r_e affect the threshold distances of target protection. When the distance d_{vi} is smaller than $r - r_e$,the assets are absolutely protected. When d_{vi} is larger than $r + r_e$, the assets can not be protected. r and r_e are shown in Fig.1. Sample security systems protection probabilities are depicted in Fig.2.

B. *Risk Entropy*

The risk of a security network is usually related to 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. In order to quantitatively evaluate uncertain factors, similar to Shannon entropy, risk entropy is proposed in this article. Suppose that the protection probability of a grid point v_i provided by a security system S_i is p_{vi} . We use P_v to represent the protection probability provided by a security network.

$$P_v = \sum_{i=1}^{n} p_{vi}, if\ \ P_v \ge 1, P_v = 1$$

The risk entropy of arbitrary point can be defined as:

$$I_v = \log(P_v) \quad (2)$$

For a security network, the most vulnerable path is considered to measure the risk. In order to simplify the problem, a guard field is considered as a cross-connected grid. A sample field which is 8m length and 4m width is shown in Fig.3..

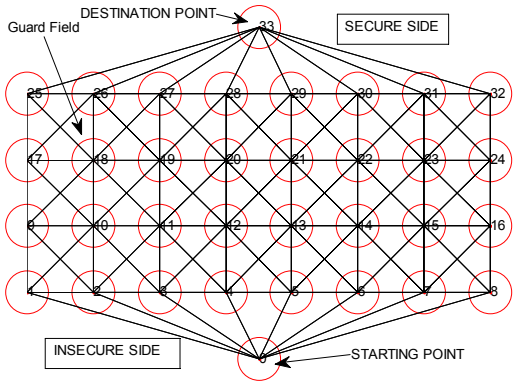

Figure 3. A sample field model and the grid size is 1m.

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 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.

$$p=\left(\sum_{v_i\in V}\left(1-p_{v_i}\right)\right)\Big/n \tag{3}$$

The risk entropy of a security network is defined as:

$$I=-\log\left(1-p\right) \tag{4}$$

IV. SIMULATION AND ANALYSIS

A. The Most Vulnerable Path

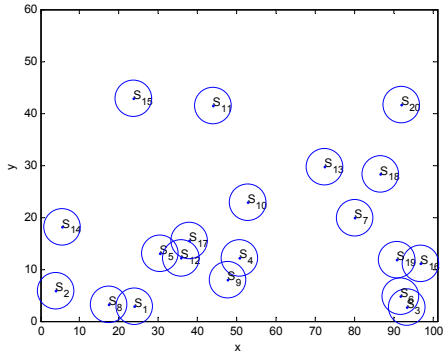

Figure 4. The random distribution of the security systems deployed in a guard field

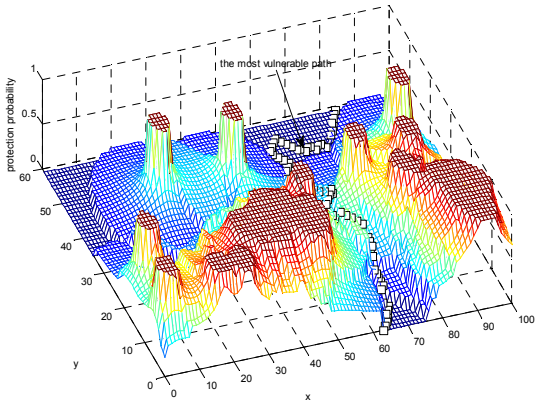

Figure 5. A sample of a guard field and vulnerable path where the length is 101 m, the width is 60 m, and grid size is 1m.

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 weights of the grid points need be converted to a new measure, which is defined as $-\log\left(1-p_v\right)$. 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 that are $\lambda=1$ and $\beta=0.3$, are randomly deployed in a rectangular area, of which the length and width are respectively 100m and 60m. The coordinates of the starting point and the destination are (50,-1) and (50,61). The distribution of the security systems in the field is shown in Fig. 4. Using the two-dimensional field model and adding the protection probability as the third axis, a sample security systems coverage graph and the weakest breach path is shown in Fig. 5.

B. Effect of the Security System Placement Strategies on the Risk of a Security Network

Except for the random placement, some regular, deterministic placement strategies have influence on the risk of a security network. We assume that thirty six security systems are placed in an area with three deterministic rules respectively and spaced along the horizontal and vertical line that split the area.The three rules are the cross deployment scheme, the square deployment scheme, and the triangle deployment scheme. The related parameter values are listed in Table 1.

TABLE I. PARAMETER VALUES USED IN THE SIMULATIONS FOR THE DETERMINISTIC SECURITY SYSTEM PLACEMENT STRATEGIES

Parameters	Values
λ	1
β	0.3
Width of Area	40m
Length of Area	100m
r	10m
r_e	6m

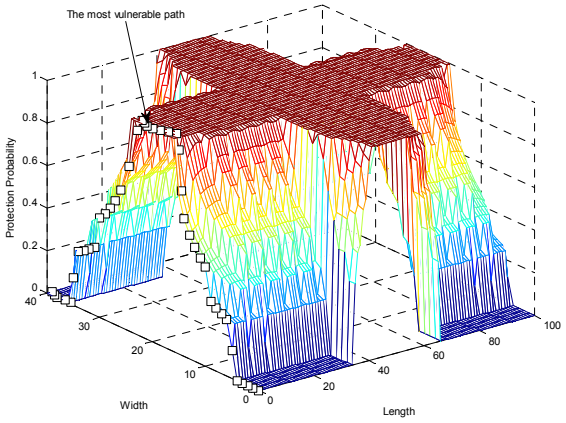

Figure 6. The most vulnerable path of the security network under the cross deployment rule

Using the cross deployment rule, the most vulnerable path of the security network is shown in Fig.6. Using the square deployment rule, the most vulnerable path is shown in Fig.7. Using the triangle deployment rule, the most vulnerable path is shown in Fig.8. According to (4), the risk

of the security network can be calculated. The experiment results are shown in Table 2.

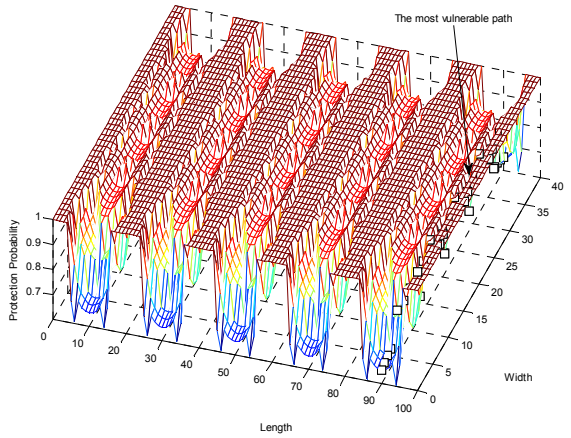

Figure 7. The most vulnerable path of the security network under the square deployment rule

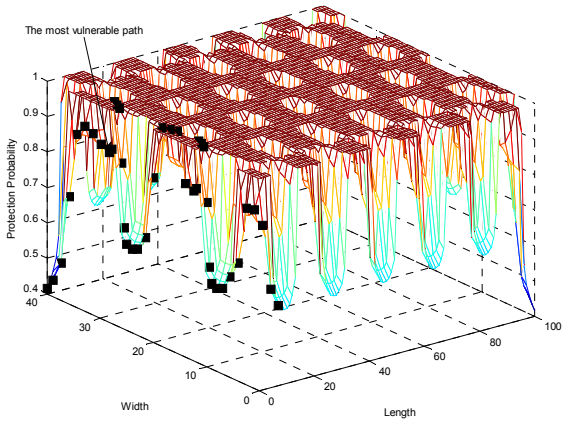

Figure 8. The most vulnerable path of the security network under the triangle deployment rule

TABLE II. THE RISK OF SECURITY NETWORKS UNDER THE DIFFERENT DEPLOYMENT RULES

Deployment Rule	Risk
Cross Rule	0.5593
Square Rule	1.6854
Triangle Rule	1.4146

V. CONCLUSION

In this paper, we propose the risk entropy and the protection model to quantitatively assess the risk of a security system or a security network. We apply the Dijkstra's shortest path algorithm, which uses the negative log of the breach protection probabilities as the grid point weights to find the most vulnerable path that is considered as the risk measure of a security network.

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.

ACKNOWLEDGMENT

Thanks for the support from National Science Foundation of China (No. 61170023, No. 61231015) and the Major National Science and Technology Special Projects (2010ZX03004-003-03).

REFERENCES

[1] Bennett, H.A.; Olascoaga, M.T. Evaluation Methdology For Fixed-Site Physical Protection Systems. *Nuclear materials management*,1980,9, pp.403-410.

[2] Darby, J.L.; Simpkins, B.E.; Key, B.R. Seapath, A Microcomputer Code For Evaluating Physical Security Effectiveness Using Adversary Sequence Diagrams. *Nuclear materials management*,1986 15, pp.242-245.

[3] Kobza, J.E.; Jacobson, S.H.: Probability models for access security system architectures. Journal of the Operational Research Society,1997,48, pp.255-263 .

[4] Hicks, M.J.; Snell, M.S.; Sandoval, J.S.; Potter, C.S.: Physical protection systems cost and performance analysis: a case study. Aerospace and Electronic Systems Magazine, IEEE.1999, 14, pp.9-13.

[5] Robert Fischer, E.H., David Walters: *Introduction to Security, Ninth Edition*. ELSEVIER.pp.203-207,2012

[6] Pollet, J.; Cummins, J.In All hazards approach for assessing readiness of critical infrastructure. Technologies for Homeland Security, 2009,pp. 366-372.

[7] 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. 2010,7, pp.2871--2878 .

[8] Nikoofal, M.E.; Zhuang, J.: Robust Allocation of a Defensive Budget Considering an Attacker's Private Information. Risk Analysis,2012, 32, pp:930-943.