# Vulnerability Evaluation of Security Network Based on Neyman-Pearson Criterion

Haitao Lv, Ruimin Hu, Jun Chen
National Engineering Research Center for Multimedia Software,
Wuhan University,
Wuhan, 430072, China

***Abstract*—What is a security network? In this paper, a security network is considered as a diagram of security systems deployed in different places in a guard zone. For a security network, its vulnerability is an important metric to judge whether its protection effectiveness is good or not. How to evaluate the vulnerability of a security network? We bring forward a protection model of a security system based on Neyman-Pearson criterion. According to the model, we propose methods to determine the most vulnerable path of a security network. The protection probability of the most vulnerable path is used to assess the vulnerability of a security network. Ultimately, we can gain insight about the vulnerability of a security network.**

***Keywords-security network; vulnerability evaluation; neyman-pearson criterion; protection probability.***

## 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, many security systems deployed in different places can communicate and share data in any time easily. So 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, which is called security network as shown in Figure 1, where each of yellow filled circles represents a security system and every triangle represents a protection target.

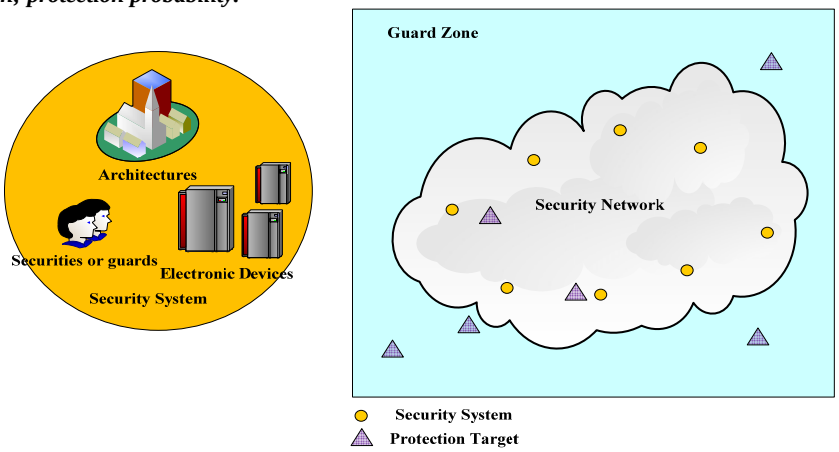


Figure 1. The abstract diagram of a security network

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 analysing 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] presented probability models to assess the vulnerability of access security systems in an airport. 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.

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

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

© 2015. The authors - Published by Atlantis Press

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 vulnerability matrix according to the levels of threats. In 2009, Jonathan Pollet and Joe Cummins [6] proposed a vulnerability 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 analyse the vulnerability of a security system. In recent years, some methods such as bounded intervals, exogenous dynamics, etc, were also put forward to resolute the vulnerability evaluation of a security system. But all in all, the current vulnerability evaluation models are all aimed at a single independent system, so the models cannot be used to evaluate the vulnerability of a security network made up of multiple security systems.

For a security network, its vulnerability depends on the protection ranges and the protection coverage schemes of its security systems. The protection coverage area of a security network may contain paths with weakest protection, which is called vulnerable paths. The protection probability of an unauthorized target traversing through a vulnerable path can reflect the vulnerability of a security network. In this paper, we will construct a protection model of a security system based on Neyman-Pearson criterion to calculate the protection probability provided by arbitrary security system. Using the model, the most vulnerable path of security network can be found and used to evaluate its vulnerability.

The paper is organized as follows. In the next section, we propose the protection model of a security system on the basis of Neyman-Pearson Criterion. In Section 3, the most vulnerable path problem is described, and how to find the most vulnerable path using Dijkstra's shortest path algorithm is proposed as a solution by defining a grid-based guard field. The model and algorithm are stimulated in Section 4. Finally, we conclude our paper in section 5.

## II. 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 is to maximize the probability that attackers are found by a security system. The protection probability provided by a security system is subjected to a maximum allowable false alarm rate $\alpha$, which can be got by the Neyman-Pearson lemma. The process of a security system finding threats can be considered as the process signal reception.

An unauthorized object is supposed to be a passive signal that subjects to additive white Gaussian noise with zero mean and variance $\sigma_n^2$. With the increase of the distance between an unauthorized object and a security system, the intensity of signals drops off. Path loss exponent is supposed to be $\eta$. Every breach protection decision is on the basis of the processing of L data samples. If the samples are collected fast enough, the distance between the security system and the object can be considered constant during 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 $\alpha$, the protection probability of an unauthorized object at grid point $v$ by the security system $i$ is defined as follows.

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

## III. VULNERABILITY EVALUATION OF SECURITY NETWORK

The security level of a security network is related to the breach protection probability, which is equal to the maximum protection probability of an unauthorized target passing through a guard field via the most vulnerable path. In this section, we will provide a method to calculate the protection probability of arbitrary point in a guard field, and then we construct the vulnerability evaluation model of a security network according to the most vulnerable path.

### A. Grid-Based Guard Field

A guard field is considered as a cross-connected grid. A sample field which is 8m length and 4m width is shown in Figure 2.

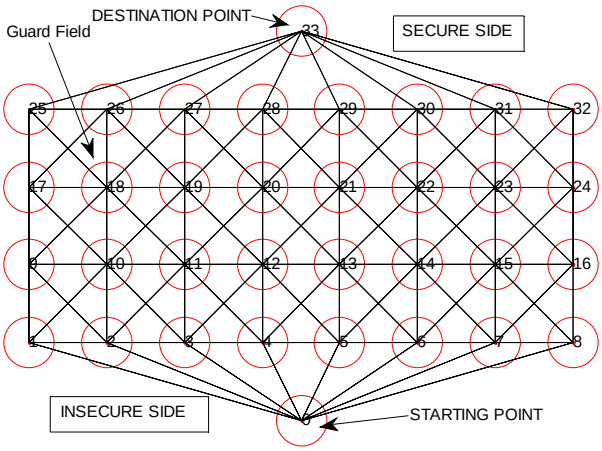


Figure 2. A sample field and the grid size is 1m.

A guard field model includes grid points and two auxiliary nodes. The two auxiliary nodes are respectively the starting and the destination points. The starting point represents the unsafe side and the destination point represents the safe side. The aim of an unauthorized object is supposed to travel through a guard field. The horizontal axis is assumed to be divided into N-1 and the vertical axis is assumed to be divided into M-1 equal parts. Thus, there are $N \times M$ grid points plus the starting and destination points. In order to simplify the notation, a kind of one dimensional

grid point index $v$ which is calculated as $v = y_v N + x_v + 1$ is used to replace the two dimensional grid point indices $(x_v, y_v)$ where $x_v = 0,1,\cdots,N-1$ and $y_v = 0,1,\cdots,M-1$.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

$$c_{v,w} = \begin{cases} 1 \ if \ 0 < v, w < NM+1 \ and \ (x_v - x_w, y_v - y_w) \in D \\ 1 \ if \ v = 0 \ and \ y_w = 0 \\ 1 \ if \ w = NM+1 \ and \ y_v = M-1 \\ 0 \ otherwise \end{cases} \quad (3)$$

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

### B. Vulnerability Evaluation Model

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.

$$p = \left( \sum_{v_i \in V} \left(1 - p_{v_i}\right) \right) \Big/ n \quad (4)$$

$p_{vi}$ is the breach 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 that is defined as follows.

$$\max \sum_{v_i \in V} \left(1 - p_{v_i}\right) x_{ij} \ subject \ to$$
$$\sum_{(s,j) \in C} x_{sj} = 1; \ \sum_{(i,d) \in C} x_{id} = 1; \ \sum_{(i,j) \in C} x_{ij} - \sum_{(k,i) \in C} x_{ki} = 0 \ \forall \ i = 1,2,\cdots,NM, \quad (5)$$
$$x_{ij} = \begin{cases} 1 \ if \ ith \ and \ jth \ nodes \ are \ on \ the \ path \ and \ c_{ij} = 1 \\ 0 \ otherwise \end{cases}$$

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 Eq. (3).

## IV. 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 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, which is 100m length and 60m width. The parameters of the Neyman-Pearson Protection model of the security systems are supposed to be configured with $L = 100, R = 9, \alpha = 0.01, \eta = 2, \gamma = 20db$ . The coordinates of the twenty security systems are shown in Table I. The distribution of the twenty security systems in the field is shown in Figure 3. A sample security network coverage graph and the most vulnerable path is shown in Figure 4. Using the two-dimensional field model and adding the protection probability as the third axis.

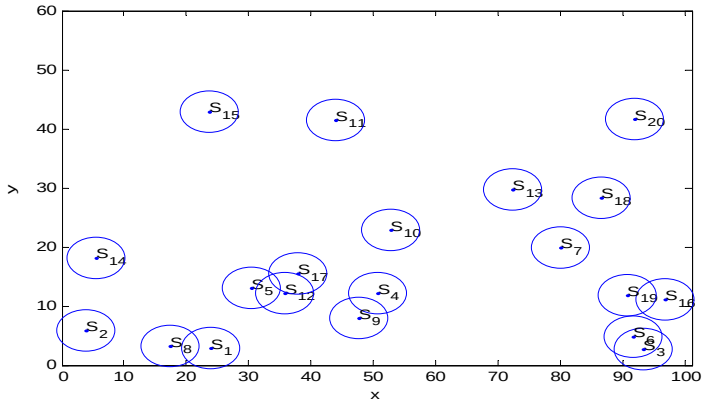


Figure 3. The distribution of the security systems deployed in a guard field

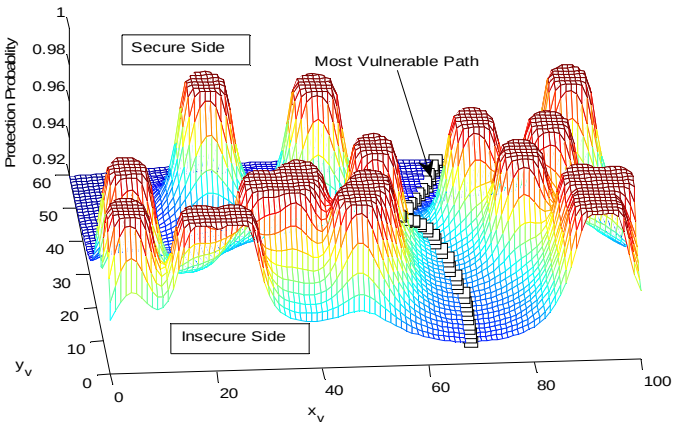


Figure 4. A sample of a guard field and the most vulnerable path

TABLE I. 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 |

## V. CONCLUSIONS

In this paper, the Neyman-Pearson protection model of a security system is put forward. On the basis of the Neyman-Pearson protection model, we provide a method to calculate the protection probability of arbitrary point in a guard field, which is employed to find the most vulnerable path of a security network. Finally, how to use the most vulnerable path to evaluate the vulnerability of a security network is simulated.

A security network will tend to fail if some security systems among the network die due to their limited energy resources. Therefore, as a future work, the failures of security systems will be considered and incorporated into the vulnerability evaluation of a security network.

## VI. 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).

## REFERENCES

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

[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*. 15, pp.242-245 ,1986.

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

[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*. 14, pp.9-13, 1999

[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*, pp. 366-372.2009.

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