Reliability Engineering and System Safety 142 (2015) 68–77

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

# Risk assessment of security systems based on entropy theory and the Neyman–Pearson criterion

Haitao Lv*, Chao Yin, Zongmin Cui, Qin Zhan, Hongbo Zhou

*School of Information Science and Technology, Jiujiang University, 332005 Jiujiang, China*

ARTICLE INFO

*Article history:*
Received 14 June 2013
Received in revised form
30 April 2015
Accepted 30 April 2015
Available online 9 May 2015

*Keywords:*
Security system
Risk entropy
Neyman–Pearson criterion
Security network
Vulnerable path

ABSTRACT

For a security system, the risk assessment is an important method to verdict whether its protection effectiveness is good or not. In this paper, a security system is regarded abstractly as a network by the name of a security network. A security network is made up of security nodes that are abstract functional units with the ability of detecting, delaying and responding. By the use of risk entropy and the Neyman–Pearson criterion, we construct a model to computer the protection probability of any position in the area where a security network is deployed. We provide a solution to find the most vulnerable path of a security network and the protection probability on the path is considered as the risk measure. Finally, we study the effect of some parameters on the risk and the breach protection probability of a security network. Ultimately, we can gain insight about the risk assessment of a security system.

## 1. Introduction

### 1.1. Motivation

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 property 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 gaining importance by many countries. In order to maintain 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. Security systems are deployed at different positions in an area, which can communicate and share data with 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 Fig. 1. Each of yellow filled circle represent 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 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?

### 1.2. Contribution

In this paper, we analyze the above challenges and put forward a model, which is on the basis of entropy theory and the 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

* Corresponding author. Tel.: +86 15070271446; fax: +86 792 8311046.
*E-mail addresses:* lvhaitao0301@gmail.com (H. Lv), 956075578@qq.com (C. Yin), 5171419@qq.com (Z. Cui), 908480624@qq.com (Q. Zhan), 63027046@qq.com (H. Zhou).

http://dx.doi.org/10.1016/j.ress.2015.04.023
0951-8320/© 2015 Elsevier Ltd. All rights reserved.

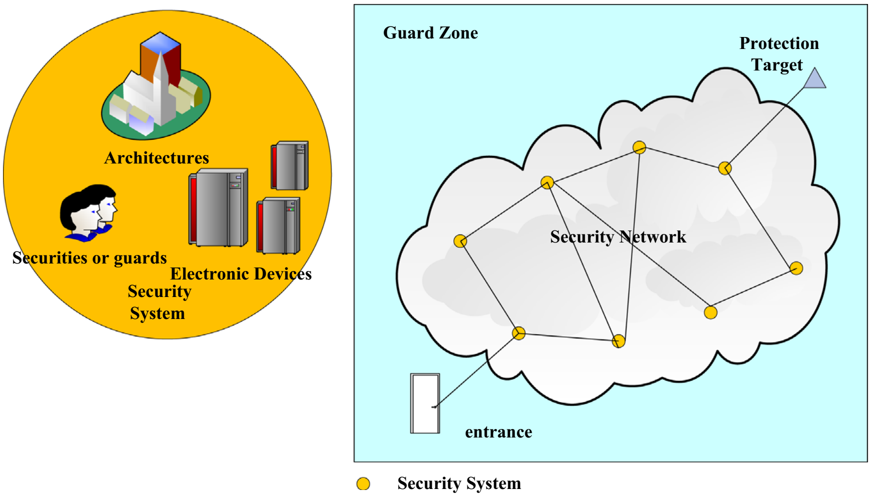

**Fig. 1.** The abstract diagram of a security network.

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. In the next subsection, the related studies about security systems are presented.

### 1.3. Related work

In 1970s, 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 et al. [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 :

$$\text{Risk} = p(A) \times [1 - p(E)] \times C. \qquad (1)$$

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, Chen [8] evaluated the protection effectiveness of a security system through establishing the corresponding indexes 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, Pollet and Cummins [10] put forward a risk assessment framework of the Security Systems, which considered not only the characteristics of the system, but also the risk outside the system.

In recent years, some researchers considered that there were enormous uncertainty in the risk evaluation of security systems, and they put forward some methods to reduce uncertainty. In 2011, Xu [11] 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. Zhuang 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 attackers 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.

### 1.4. Paper organization

The remainder of this paper is organized as follows: in the next section, 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 3. Finally, we draw our conclusions in Section 4.

## 2. Risk entropy and vulnerable path problem formulation

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 considered as the risk measure of a security network. In this section, the risk entropy and Neyman–Pearson protection