Safety Science 65 (2014) 125–137

Contents lists available at ScienceDirect

Safety Science

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

An evidential approach to physical protection system design

Peida Xu [a], Yong Deng [b,c,*], Xiaoyan Su [a], Xin Chen [a], Sankaran Mahadevan [c]

[a] School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[b] School of Computer and Information Science, Southwest University, Chongqing 400715, China
[c] Department of Civil and Environmental Engineering, Vanderbilt University, Nashville, TN 37235, USA

ARTICLE INFO

Article history:
Received 15 May 2013
Received in revised form 23 October 2013
Accepted 13 January 2014
Available online 13 February 2014

Keywords:
Information fusion
Dempster–Shafer evidence theory
Risk analysis
Physical protection system
Optimization design

ABSTRACT

A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent intruder attacks. The physical protection components (detection, delay, and response) within a facility interact with each other and their locations significantly affects the effectiveness of PPS. This paper proposes a method based on an evidential approach to evaluate the risk level of PPS and optimally locate the physical protection components to balance cost and performance. Each individual component of the system is modeled in a simulated plane. Then, the risk level distribution of each component is determined based on its actual environment. The comprehensive risk level distribution is obtained by combining information from multiple sources within the framework of Dempster–Shafer evidence theory. Finally, optimization algorithms are used to find the optimal locations. A hypothetical example is discussed which demonstrates the usefulness of the developed methodology.

© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent intruder attacks. The design of an effective PPS requires a systematic approach in which the designer weighs the objectives of the PPS against available resources, and then evaluates the proposed design to determine how well it meets the objectives. Without this kind of careful assessment, the PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points of the facility. A PPS can be seen as a typical man-in-the-loop system. The system includes not only the physical equipment to detect, delay and respond, but also guards to monitor and protect the system, where human factors analysis plays an important role.

Many studies have been reported on PPS-related research (Kobza and Jacobson, 1997; Garcia, 2001; Jaeger, 2003; Garcia, 2005; Moore et al., 2007; Scaparra and Church, 2008; Jang et al., 2009; Hester and Mahadevan, 2010; Hester et al., 2010; Xu et al., 2010; Berle et al., 2011). Garcia provided detailed discussion on models and methods to guide the design, evaluation and vulnerability assessment of PPS (Garcia, 2001, 2005). The main functions of PPS are detection, delay and response. For an effective system there must be awareness of an intruder (detection) and slowing of progress of the intruder to the target (delay), thus allowing a response force to interrupt or stop the adversary in time (response). Therefore, the effectiveness of a PPS can be calculated in terms of its degree of success in achieving detection, delay and response.

Several vulnerability assessment methods for security systems have been proposed (Moore et al., 2007; Scaparra and Church, 2008; Jaeger, 2003; Berle et al., 2011; Xu et al., 2010). One of the commonly used methods to evaluate the effectiveness of a PPS is pathway analysis of potential outside attack (Garcia, 2001, 2005), focusing on delay time. For example, one can use a simulation code to find the highest risk pathway of the PPS, then some improvements such as adding a new delay unit in the pathway can increase the effectiveness of the system. However, as pointed out in Jang et al. (2009), Garcia's work (Garcia, 2001, 2005) does not use a two-dimensional map for pathway analysis and thus has limitations in representing the structure of a PPS.

Besides the problem above, other issues also need attention. There are many sources of uncertainty in a PPS. Probability theory has been applied for uncertainty modeling and vulnerability assessment. In some situations, however, the uncertainty is not randomness but fuzziness. Fuzzy set theory and Dempster–Shafer evidence theory have been shown to be effective in dealing with both aleatory and epistemic uncertainty in many applications of decision making and risk analysis. The PPS consists of many different kinds of sensors which provide subjective or objective data. A data fusion method is desired to combine various types of data.

* Corresponding author at: School of Computer and Information Science, Southwest University, Chongqing 400715, China. Tel./fax: +86 023 68254555.
E-mail address: ydeng@swu.edu.cn (Y. Deng).

http://dx.doi.org/10.1016/j.ssci.2014.01.003
0925-7535/© 2014 Elsevier Ltd. All rights reserved.

Then how to efficiently represent and propagate the available information in the evaluation procedure?

Probability theory, fuzzy set theory, rough set theory and evidence theory, have been proposed to deal with uncertainty. For example, Bajpai et al. (2010) use fuzzy numbers to analyze security risk. However, among these tools, evidence theory is able to model not only probabilistic data but also fuzzy data. In addition, the Dempster's rule in evidence theory provides an effective method to combine evidence from different sources (Deng et al., 2011a,b,c; Deng and Chan, 2011; Basir and Yuan, 2007). Therefore, evidence theory is seen to be a reasonable tool to handle uncertainty in PPS evaluation.

A 3-D visual threat distribution map of a PPS can be constructed using a mathematical model based on evidence theory (Xu et al., 2010). This model integrates multiple sensor information and facility layout information within the framework of the Dempster–Shafer evidence theory. By this method, a simplified PPS model, as shown in Fig. 1, can be evaluated as a 3-D visual threat distribution map, as shown in Fig. 2. Following Garcia's work (Garcia, 2001, 2005), we can calculate the delay time corresponding to the path lengths and the additional delay that the delay equipments bring about. One can easily find two paths with the same delay time but significantly different threat distribution along each path.

Based on this model, this paper aims to solve the following two problems:

1. Can the PPS designer optimally locate the sensors based on this visual mathematical model? In other words, are there some optimal solutions of the corresponding optimization problem?
2. How to solve the corresponding optimization problem?

This paper proposes solutions to the above problems and shows an approach to finding a global optimal solution in an efficient manner. The designer can also consider different objectives and their weights in the overall objective function using the proposed method.

In summary, this paper proposes a method to optimally design the PPS under the framework of evidence theory. The proposed method is helpful not only in mathematical modeling and visualization but also provides potential guidance to engineering practice with respect to PPS.

The organization of the rest of this paper is as follows. Section 2 gives a brief introduction to some necessary related concepts. The proposed method is presented in Section 3. Section 4 investigates the effectiveness of the proposed method for optimization of PPS using a hypothetical facility example. The paper is concluded in Section 5.

2. Preliminaries

In this section, some related concepts are briefly introduced, including evidence theory, the evidence distance, and the modified averaging approach to combine evidence. These concepts are used to handle uncertainty and obtain the risk level in the PPS evaluation.

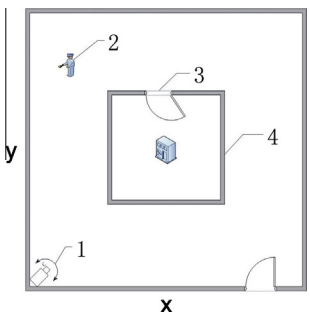

Fig. 1. System model.

2.1. Dempster–Shafer evidence theory

The mathematical theory of evidence, as introduced by Dempster (1967) and extended later by Shafer (1976), is concerned with the question of belief in a proposition and systems of propositions. 'Belief' in a proposition conceptually does not necessarily mean the 'chance' of the proposition being true. Evidence can be considered in a similar way when forming propositions, and as such, the Dempster–Shafer theory (D–S theory) is concerned with evidence, weights of evidence and belief in evidence (Shafer, 1976). Thus, this theory can be viewed as a generalization of the classic probability theory. Due to its ability to handle uncertainty or imprecision embedded in the evidence, the D–S theory has been increasingly applied in many fields (Andersen and Hooker, 1996; Murphy, 2000; Liu and Shenoy, 2004; Deng et al., 2004; Hilhorst et al., 2008; Xu et al., xxxx). Formally, the evidence theory consists of the following basic concepts:

(1) *Frame of discernment*:
Evidence theory starts with the definition of a set of hypotheses θ called the frame of discernment, defined as:

$$\theta = \{H_1, H_2, \ldots, H_N\} \tag{1}$$

The set θ is composed of N exhaustive and exclusive hypotheses. Denote $P(\theta)$, the power set composed of 2^N propositions of θ as:

$$P(\theta) = \{\emptyset, \{H_1\}, \{H_2\}, \ldots, \{H_N\}, \{H_1 \cup H_2\}, \{H_1 \cup H_3\} \ldots \theta\} \tag{2}$$

where $\emptyset$ denotes the empty set. The N subsets containing only one element each are called singletons.

(2) *Mass functions, focal elements, and kernel elements*:
When the frame of discernment is determined, the mass function m is defined as a mapping of the power set $P(\theta)$ to a number between 0 and 1, i.e.,

$$m: \ P(\theta) \to [0, 1] \tag{3}$$

and which satisfies the following conditions:

$$\sum_{A \in P(\theta)} m(A) = 1, \tag{4}$$

$$m(\emptyset) = 0 \tag{5}$$

The mass function m is also called the basic probability assignment (BPA) function. $m(A)$ expresses the proportion of all relevant and available evidence that supports the claim that a particular element of θ belongs to the set A but to no particular subset of A. Any subset A of θ such that $m(A) > 0$ is called a focal element; $C = \cup_{m(A) \neq 0} A$ is called a kernel element of mass function m in θ.

(3) *Rule of evidence combination*:
Suppose m_1 and m_2 are two mass functions formed based on the information obtained from two different information sources in the same frame of discernment θ; the Dempster's rule of combination (also called orthogonal sum), denoted by $m = m_1 \oplus m_2$, combines two BPAs m_1 and m_2 to yield a new BPA:

$$m(A) = \frac{\sum_{B \cap C = A} m_1(B) m_2(C)}{1 - k} \tag{6}$$

$$k = \sum_{B \cap C = \emptyset} m_1(B) m_2(C) \tag{7}$$

Download English Version:

https://daneshyari.com/en/article/6976343

Download Persian Version:

https://daneshyari.com/article/6976343

Daneshyari.com