The Vulnerability Assessment Code for Physical Protection System

Sung Soon Jang and Hosik Yoo
Korea Institute of Nuclear Non-proliferation and Control
119 Munji-Ro, Yuseong, Daejeon, Korea, 305-732

1. Motivation

To neutralize the increasing terror threats, nuclear facilities have strong physical protection system (PPS). PPS includes detectors, door locks, fences, regular guard patrols, and a hot line to a nearest military force. To design an efficient PPS and to fully operate it, vulnerability assessment process is required.

Evaluating PPS of a nuclear facility is complicate process and, hence, several assessment codes have been developed. The estimation of adversary sequence interruption (EASI) code analyzes vulnerability along a single intrusion path. To evaluate many paths to a valuable asset in an actual facility, the systematic analysis of vulnerability to intrusion (SAVI) code was developed. KAERI improved SAVI and made the Korean analysis of vulnerability to intrusion (KAVI) code.

Existing codes (SAVI and KAVI) have limitations in representing the distance of a facility because they use the simplified model of a PPS called adversary sequence diagram. In adversary sequence diagram the position of doors, sensors and fences is described just as the locating area. Thus, the distance between elements is inaccurate and we cannot reflect the range effect of sensors.

In this abstract, we suggest accurate and intuitive vulnerability assessment based on raster map modeling of PPS. The raster map of PPS (shown in Fig. 3) accurately represents the relative position of elements and, thus, the range effect of sensor can be easily incorporable. Most importantly, the raster map is easy to understand.

2. Physical Protection System

We will briefly introduce a physical protection system before to go further. PPS is consisted of detection, delay and response. Suppose we should protect a valuable asset from intruders. First of all, we would build heavy fences to delay them. However, delay is not enough; we should know the intrusion (detection) and take actions to turn them out (response). As a response, we probably ask help to a police office, because intruders are dangerous. In this circumstance, the condition of interrupting intruders is that a response fore arrives before intruders take the asset and run.

Hence the probability of interruption is a function of detection probabilities and delay times along a specific path, and a response force time [1-3].

$$P_I = f(detection, delay, response)_{path} \qquad (1)$$

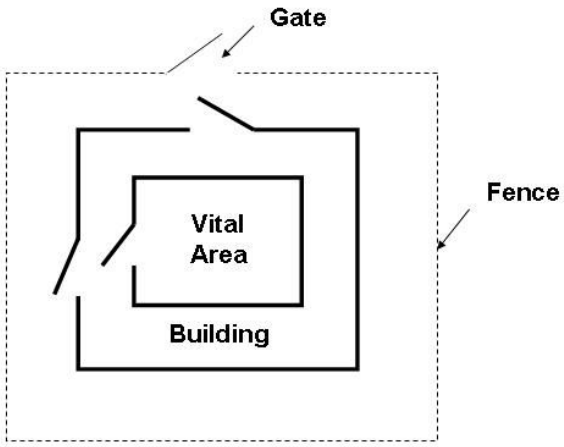

Fig. 1 An example of a physical protection system

	Probability of detection	Delay time (seconds)
Gate	0.99	120
Fence	0.5	10
Door (3 ea)	0.9	90
Wall (2 ea)	0.3	300
Sabotage Target	No detection	120

Fig. 2 The detection and delay of the protection elements in the example (Fig. 1)

The detailed calculation is written in the cited references.

Figure 1 and 2 shows an example of detection and delay elements of PPS. The dangerous nuclear material in vital area is protected by a fence, walls and doors. To detect adversaries, sensors and CCTV are located at a gate, doors, and around walls. Figure 2 shows detection probability and delay times of protection elements. These elements with a response force constitute PPS of a facility.

3. Raster map representation of a PPS

Rasterizing a facility is to divide 2D-map of the facility by meshes of a finite size square shown in Fig. 3. Each mesh has probability of detection and delay time of the corresponding elements on the mesh. For example if an element on a mesh is a fence, detection probability is 0.5 and delay time is 10. Because of evaluation speed, the size of mesh can not be arbitrary small. Therefore, the evaluation has errors depending on the mesh size.

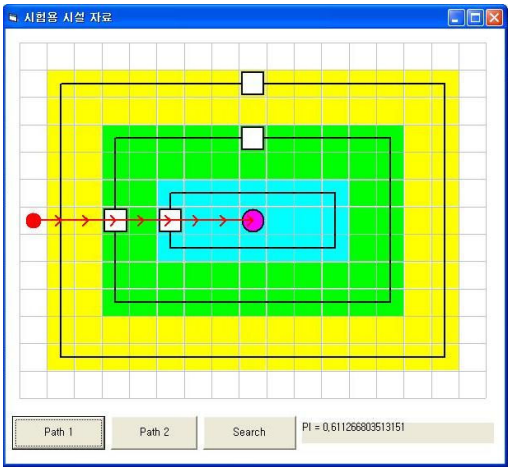

Fig. 3 Raster map of a PPS

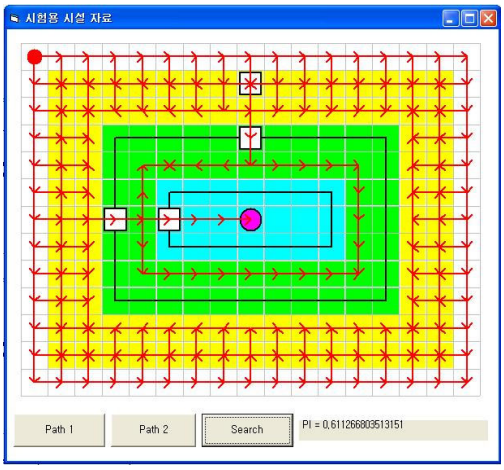

Fig. 4 Search of the most vulnerable path

Using the raster map of a facility to represent PPS has the following advantages;

- representation of PPS and an adversary path is easy to understand, and
- the relative position of elements is accurately reflected.

Given the raster map of a PPS, a response force time, and an adversary path, we can calculate the probability of interruption of the path. Meshes along the path contain required probability of detection and delay time. Thus, the probability of interruption is calculated by equation (1). In Fig. 3, the lower right corner shows the probability of interruption.

4. Searching the most vulnerable path

We represent the vulnerability of a PPS by the probability of interruption of the most vulnerable path to a target, because we assume the worst case where adversaries know the whole details of PPS. Hence, we should search all possible paths to find the most vulnerable one.

We use the best-first search algorithm [4] to find a path which has the lowest probability of interruption. Instead of random search, the best-first search algorithm uses a rough estimation, called *heuristics*, to pick out more possible paths. Figure 4 displays searched paths till the target. In this figure, an inner most wall is bypassed because penetrating wall consumes much time (see, Fig. 2), which is predicted by the heuristics.

Even though the algorithm is very similar to the fastest path finding algorithm, the most vulnerable path finding has a big difference; the latter must consider not only fast intrusion but also covert intrusion. The trade off between these speed and covertness is judged by the equation (1).

5. Results & Discussion

We are developing vulnerability assessment code based on 2D raster map of PPS. Figure 3 and figure 4 shows capture screens of the code. We are writing the code by Visual Basic, and plan to complete the development until the end of this year.

For the code to be useful, the most important work is collecting data regarding to sensor detection and barrier delays used in PPS. Without proper input data, the code would give useless results. Currently we use only the old testing data from USA and cannot access to the latest test data because they are secret. We recommend installing and operating test-bed of sensors and barriers.

Conclusively, we suggest accurate and intuitive vulnerability assessment code based on raster map modeling of PPS. The code will help to assess of a PPS and, thus, to build robust protection against terror.

Acknowledgement

This work has been carried out under the Nuclear Research and Development program supported by the MOST

REFERENCES

[1] Mary Lynn Garcia, *The Design and Evaluation of Physical Protection Systems,* Butterworth-Heinemann (2001).

[2] Mary Lynn Garcia, *Vulnerability Assessment of Physical Protection Systems*, Butterworth-Heinemann, (2005).

[3] IAEA, *Physical Protection of Nuclear Facilities and Materials*, The materials of the nineteenth international training course on physical protection, May (2006).

[4] S. J. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach 2nd edition*, Prentice Hall (2002)