A Study on Bayesian Approach for Intrusion Detection in Physical Protection System of Nuclear Power Plants

Minho Kang [a], Moonsung Koh [a]*
[a]Korea Institute of Nuclear Nonproliferation and Control, 1418 Yuseong-daero, Yuseong-gu, Daejeon 34101
[*]Corresponding author : mhkang@kinac.re.kr

1. Introduction

Scientific detection devices play an important role in a physical protection system. They can detect unauthorized intrusion in real time through the CCTV or sensors installed in the fence around the protected area in nuclear power plants. The intrusion detection strengthens the monitoring inside and outside the protected area. If a blind spot is present in the monitoring through CCTVs, a serious problem for protection can occur. Thus, this study aims to propose a methodology that can estimate the detection probability of unauthorized actions through the Bayesian approach when a person(s) moves into the blind spot, which is outside the detection area.

2. Methods and Modeling

In this section, we present an intrusion detection model using Bayesian approach based on human behavior pattern analysis.

2.1 Method that detects abnormal actions based on the Bayesian approach

The probability calculation according to the Bayesian approach consists of prior probability, posterior probability, and likelihood function. The uncertainty of intrusion detection for the target (person) can be expressed with probability using given data as presented in Eq. (1).

$$P(I \mid E) = \frac{P(E \mid I)P(I)}{P(E)} = P(I)\frac{P(E \mid I)}{P(E)} \quad (1)$$

A specific event occurred already with probability of *P(E)* and the probability with regard to the cause of the event occurrence, that is, posterior probability *P(I|E)* can be calculated using information that is already known prior to event occurrence, that is, prior probability *P(I)*. The most likely intrusion and event information can be obtained within a probability between 0 and 1 according to prior information and the maximum likelihood function *P(E|I)*. The closer the posterior probability *P(I|E)* to 1, the more the intrusion becomes evident.

2.2 Construction of Bayesian network

In this study, the Bayesian inference introduced in the previous section is extended to a network model to propose the detection probability of abnormal activities. It is necessary to construct a profile consisting of two patterns: frequently occurring normal behavior pattern and infrequently occurring abnormal behavior pattern. The construction process is as follows:

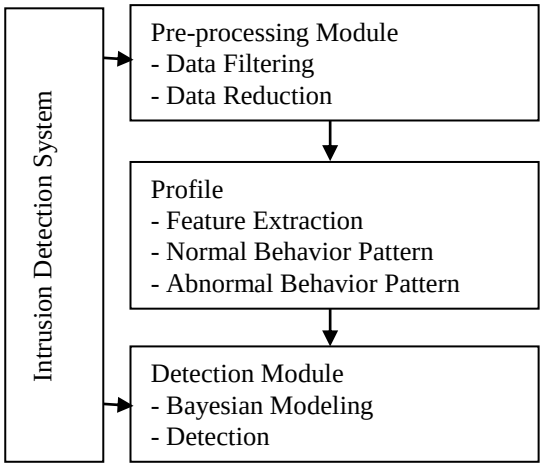

Fig. 1. Overview of Intrusion Detection System

Until now, safeguards sees CCTV monitors in the CAS(Central Alarm System) room during 24 hours in day and night shifts to check if there is an intruder. Through the methodology presented in this paper, it is possible to analyze the probability of the intruder moving to the blind spot and the probability of detection based on the human movement pattern analysis.

2.2.1 Construction of behavior patterns

The following variables are defined to construct the behavior patterns.

CC_i = *i*-th CCTV, $i=1,2,\ldots,l$
NBP_j = *j*-th normal behavior pattern, $j=1,2,\ldots,m$
ABP_k = *k*-th abnormal behavior pattern, $k=1,2,\ldots,n$

A pattern can be defined as a path where a person moves from an arbitrary location cell to the next adjacent cell when the screen in the CCTV is divided into cells of fixed size. A moving path from the time a person is discovered in a single monitor of the CCTV to

an arbitrary time is defined as a normal behavior pattern, which can be expressed with a probability chain type. A path that passes through a blind spot in Fig. 2 is defined as an abnormal behavior pattern, which can be also be expressed with a probability chain type.

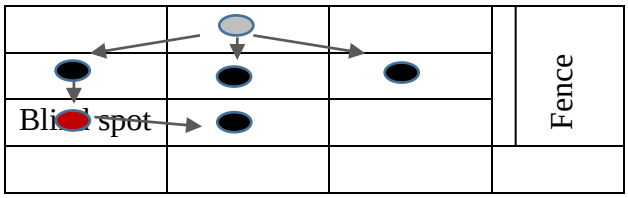

Fig. 2. Recognition of moving pattern through CCTV monitor

2.2.2 Bayesian network modeling

X_i consisting of moving path patterns of people in the *i*-th CCTV is dependent on previous moving path patterns in the CCTV (X_1, X_2, X_3,..,X_{i-1}) and *Ab* that represents an occurrence of abnormal behavior (blind spot passing or hiding). Thus, a continuous moving path pattern of people in the CCTV can be expressed via the Bayesian network shown in Fig. 3.

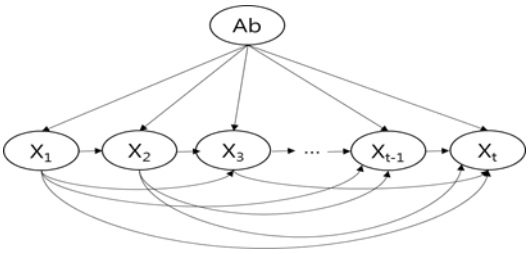

Fig. 3. Bayesian network of behavior patterns

2.2.3 Abnormal behavior detection

Based on the Bayesian approach, the probability of occurrence of abnormal behavior can be calculated via Eq. (2) using conditional probabilities that represent the dependence between prior probability *P*(*Ab*) of abnormal behavior (blind spot passing or hiding) and X_i.

$$P(Ab \mid X) = \frac{P(X \mid Ab)P(Ab)}{P(X)} = P(Ab)\frac{P(X \mid Ab)}{P(X)} \quad (2)$$

$$X = X_1, X_2, X_1, \ldots, X_l$$

That is, the number of patterns that pass through the blind spots from the number of cases of all possible moving patterns inside individual CCTVs can be calculated as shown in Fig. 2. Through this calculation, prior probability *P*(*Ab*) can be determined. Furthermore, since abnormal behaviors in each of the CCTVs is independent with one another, likelihood function *P*(*X*|*Ab*) can be calculated. When a behavior pattern is detected in an arbitrary CCTV based on the above two probability distributions, that is, the posterior probability *P*(*Ab*|*X*) of possible event occurrence, whether this behavior is abnormal or not (blind spot passing or hiding), can be suggested with a probability value.

3. Conclusions

The scientific detection equipment are an important component in a physical protection system but the blind spot of a CCTV makes the protection of facilities in nuclear power plants vulnerable. Accordingly, this study can calculate the detection probability of abnormal behavior and estimate the vulnerable path of protection by using the Bayesian approach proposed in the present study based on prior information about blind spots in individual CCTVs. However, there is a limit to develop a probabilistic model and to simulate using the methodology presented in this paper by using CCTV information installed in a protected area of a nuclear power plant. Nuclear power plants are not only difficult to obtain such detailed information as a national important facility, but also difficult to collect data through simulations in the field. Research is underway to overcome these limitations by carrying out R&D projects such as identification of vulnerable paths that make the most use of plant information.

For the future study, time information about how long a person remains in each divided cell on the screen of the CCTV will be added to expand the network model to raise the reliability of detection probability. And also, as future research subject, it will be possible to further enhance the reliability of the intrusion detection system by database of human characteristics inherent to big data analysis as well as behavior pattern analysis.

REFERENCES

[1] B. M. Choi, J. S. Lee, M. M. Han, “IDS Model using Improved Bayesian Network to improve the Intrusion Detection Rate”, Journal of Korean Institute of Intelligent Systems, Vol.24(5), p.495-503, 2014.

[2] B. R. Cha, K. W. Park, J. H. Seo, “Modified Intrusion Pattern Classification Technique based on Bayesian Network”, Korean Society for Internet Information, Vol.4(2), p.69-80, 2003.

[3] M. G. Chi, H. S. Lim, M. S. Kim, "Development of Physical Protection System Design Process for New Nuclear Power Plants", The Korean Institute of Electrical Engineers, Vol.24(7), p.1621-1622, 2014.

[4] S. J. Seo, S. S. Jang, H. S. Yoo, "Analysis on Physical Protection Vulnerability Assessment Programs Using Different Modeling Methods", Korean Society of Hazard Mitigation, Vol.16(6), p.221-230, 2016.

[5] J. D. Williams, "Physical protection system design and evaluation", PROCEEDINGS SERIES STI/PUB, Vol.11, p.267-274, 1997.