Cyber-attack path suggestion system by using markov model and Dijkstra's algorithm

Young Ho Chae [a*], Chanyoung Lee [a], Poong Hyun Seong [a]
[a] *Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea*
[*] *Corresponding author: cyhproto@kaist.ac.kr*

1. Introduction

Since nuclear power plant (NPP) is safety critical infrastructure, to enhance the safety I&C systems are converted from analog to digital. As a result of conversion safety and availability of nuclear power plant are enhanced. However, at the same time, the system becomes vulnerable to cyber-attack. At the early stage, the NPP is thought to be safe from the cyber-attack due to the air-gap. However, Davis-Besse NPP was attacked and also Iranian uranium enrichment facility was attacked. As the series of attacks, it is figured that the air-gap cannot guarantee safe from cyber-attack.

The best way to protect NPP is protect every component in NPP with unlimited resources. However, it is impossible in reality. Therefore for the efficient protection, the priority should be defined. However, prioritization is difficult because there are numerous components and links. For instance, the I&C system of APR-1400 has 173 communication nodes and 416 links.

Therefore, in this paper we suggested an attack path proposal system based on markov model that maximizes the attack impact. We assumed that the attack impact is large when the components communicating with multiple devices is compromised.

2. Attack path finding system

2.1 Page-rank algorithm

To quantifying the importance of a component, page-rank algorithm is utilized. The page-rank algorithm which is based on markov model is suggested by L. Page et.al. [1]. The key idea of their methodology is as follow: If the web site is highly cited, the probability that the random web surfer stays will increase because the web page is connected to many other web pages. The algorithm worked successfully and became the basic algorithm of the google search engine. In this paper, we assumed that the attack impact can be increased when the component that communicate with multiple components is compromised. Therefore, in the same manner, the importance of each component can be calculated by using page-rank algorithm.

2.2 Attack resistance concept

In order to maximize the impact of cyber-attacks from the perspective of an attacker, it is desirable to compromise components with high importance. Therefore, the attacker will feel less attack resistance when attacking a component with high importance. The concept can be expressed as following equation (Eq. 1).

$$\mathrm{R} = \frac{1}{\mathrm{Importance}} \quad \text{Eq. 1}$$

In the same manner, link resistance can be defined as follows (Eq. 2).

$$\mathrm{R(i,j)} = \frac{1}{Importance(i,j)} = \frac{1}{Importance(i) + Importance(j)} \quad \text{Eq. 2}$$

If there is an additional security measure, it can be expressed as adding additional resistance to the corresponding link (Eq. 3).

$$\mathrm{R(i,j)} = \frac{1}{Importance(i) + Importance(j) + R_{security\ measure}} \quad Eq. 3$$

Therefore, the attack path that can maximize the attack impact is same as the path with smallest resistance.

2.3 Dijkstra's algorithm

To figure out possible attack path automatically, Dijkstra's algorithm is applied. Dijkstra's algorithm is firstly proposed by Dijkstra E. W. [2]. Dijkstra's algorithm is an algorithm for finding the shortest paths between nodes in a graph. The algorithm works with following sequences.

1. Define unvisited set
2. Assign to every node a tentative distance value and set initial node as current node
3. Calculate tentative distance from the current node
4. Compare the newly calculated tentative distance to the current assigned value and then assign the smaller one.
5. Remove current node from unvisited set when all of the unvisited neighbors of the current nodes are marked.
6. Finish the algorithm when the destination node has been marked.

With Dijkstra's algorithm the attack path that can maximize the attack impact can be figured.

3. Conclusions

When there is an attack starting point and target, there can be many different ways to reach the target. Therefore, if the defense against components that can increase the impact of the attack in the possible attack path can be helpful in reducing the impact of the attack.

Therefore, in this study, the page rank algorithm, attack resistance concept, and Dijkstra's algortihm were used to quantify component and link importance. And by identifying the shortest path, we designed a system that suggests the path that the attacker can take from the attack starting point and the attack target. By using proposed methodology, the effective preparation for the cyber-attack can be conducted.

ACKNOWLEDGEMENT

This research was supported by the National R&D Program through the National Research Foundation of Korea (NRF) funded by the Korean Government. (MSIP: Ministry of Science, ICT and Future Planning) (No. NRF-2016R1A5A1013919)

REFERENCES

[1] Page, Lawrence, Brin, Sergey, Motwani, Rajeev and Winograd, Terry, “The PageRank Citation Ranking: Bringing Order to the Web”, Technical Report. Stanford InfoLab (1999)
[2] Dijkstra, E. W. “A note on two problems in connexion with graphs” Numerische Mathematik 1, pp.269-271 (1959)