Journal of Electronic Research and Application
OPEN

Research on Generating and Visualizing Display Method of Power Optical Network Attack Path

Li Wei Wei, Ma Yuan Yuan, Zhou Cheng, Li Qian Mu

Abstract: When an intruder attacks an object in an electric power network, it is necessary to successfully invade the target node along an attack path. However, as the number of target power optical network nodes increases gradually, the attack path will be exponential growth, resulting in path redundancy, affecting the overall performance of the generated path. To this end, a new power optical network attack path generation and visual display method, introduced the atomic attack, attack map and attack path definition. Based on the analysis of the cost and benefit of the attack path, the intrusion feasibility model is proposed, and the intruder's choice of the attack path becomes the problem of the feasibility of the invasion. When the POS set contains all the directional edges of the power optical network attack map, generate the attack path of the power optical network by traversing the POS collection element. The process of generating the attack path of the electric power network is displayed. The experimental results show that there is no redundant phenomenon in the proposed method, and the generated attack path is effective and the reliability is high.

Key words: Power optical network; attack path generation; visual display

1 Introduction

The power optical attack path is a description of the sequence of intrusion behavior that causes the state of the power grid to change [1,2]. Power optical network attack path to help power optical network security researchers more fully understand and deal with power optical network attacks [3]. In addition, it can speed up the speed of optical intrusion detection and defense, for power optical security personnel to develop strategies to prevent further optical network intrusion to provide important data support [4,5]. Therefore, it is of great significance to study the generation and visualization of the attack path of the electric power network, which has become the focus of research on related scholars [6,7].

In [8], a Bayesian network-based method for generating the attack path of the optical network is proposed. The Bayesian network is used to find the intrusion evidence of intrusion. Along with the intrusion path attack target with the above intrusion behavior, the node confidence degree Attack path to predict, in order to achieve the attack path generation. The method is simple to implement, but it also leaves evidence of intrusion in the case of intruder intrusion. However, the intruder will not attack the target along the path, resulting in path redundancy. [9] This method considers that the intruder is based on the cost to determine the intrusion strategy, so it uses the intruder's subjective selection to realize the generation of the power optical network attack path and reduce the redundant path, but the method Ignoring the invasion of income, resulting in the generation of the attack path is not reliable; [10] proposed a Petri net based on the power network attack path generation method to build the attack model, based on the model to establish a Petri net-based optical network attack map, In order to achieve the attack path generation. The method is efficient, but the construction of the model requires a lot of prior knowledge and is not easy to realize.

A new method of generating and visualizing the attack path of the electric power network is proposed, and the definition of atomic attack, attack map and attack path is introduced. The intruder on the attack path selection problem into the feasibility of the invasion of the problem, by traversing the POS set of elements to generate power optical network attack path. The process of generating the attack path of the electric power network is displayed. The experimental results show that there is no redundant phenomenon in the proposed method, and the generated attack path is effective and the reliability is high.

(Global Energy Internet Research Institute, Nanjing 210003)

2 Research on Generation and Visual Display of Attack Path of Electric Power Network

2.1 Power Optical Network Attack Map Description

For ease of analysis, this section calls a single vulnerability attack as an atomic attack, as shown in Figure 1.

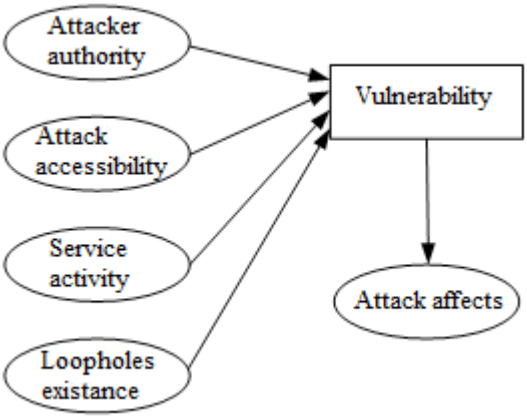

Figure 1 Atomic attack

Fig. 1 Atomic attack

The atomic attack described in Figure 1 is essentially a CPN network structure. The following is a formal definition of atomic attack based on CPN. The formula is described as follows:

$$AAG = \langle P_{Ao}, t, P_{Ad} \rangle \quad (1)$$

Where P_{AO} is used as a prerequisite for describing an atomic attack; t is used to describe a transition and is a vulnerable behavior of an atomic attack; P_{Ad} is used to describe a set of successful atomic attacks.

According to the dependence of different atomic attacks on the power of optical network attack map to establish the power optical network attack diagram formula described as follows:

$$AG = \langle P_0 \bigcup P_d, T_0 \bigcup T_d, E \rangle \quad (2)$$

Where P_0 is used to describe the initial set of the initial library, which contains the initial state of the power optical network and the intrusion behavior; P_d is used to describe the set of reachable libraries that record the reachability of the power optical and intruders; T_0 is used to describe the set of independent transforms; T_d is used to describe the dependency set; E is used to describe the directional arc of the library in the connected CPN attack map.

According to the attack map definition to obtain the attack path definition: $Path = t_1 \to t_2 \to \cdots \to t_n$ describe the power optical network with a transition sequence in Figure AG, then meet the following conditions of the transition sequence as a power optical network attack path: Change t_i is independent type change; the set of output t_i and the set of key nodes intersect.

2.2 Power optical network attack path generation method

In this paper, the cost of the attack path analysis, on the basis of the proposed feasibility of the invasion model, the intruder on the attack path selection problem into the feasibility of the invasion of the problem, resulting in power optical network attack path.

The cost of the attack path, $Cost(e_{ji})$, mainly includes the risk cost and the operation cost, among which the operating cost is:

$$Cost(e) = \alpha \times cost(meta-operations) + \beta \times cost(sequence) \quad (3)$$

Where, $cost(meta-operations)$ representing the cost of operation; $cost(sequence)$ representing the cost of the operation sequence; e used to describe the directional edge, $e = \langle a_j, v_i \rangle$; α, β is the normal number.

The risk cost can be determined by:

$$cost = \cos t(e) \times X(e)^{time-1} \times \theta(e) \quad (4)$$

Where $X(e)$ is the intruder experience coefficient; $time$ is used to describe the number of invasions; $\theta(e)$ is the risk factor used to describe the risk factor can be obtained through expert experience.

The cost of the attack path $Cost(e_{ji})$ is:

$$Cost(e_{ji}) = \varepsilon Cost(e) + \mu \cos t \quad (5)$$

Where, ε, μ are used to describe the weight of operating costs and risk costs.

The following is based on the cost of the attack path cost of the proposed feasibility of the invasion model. The intruder along the attack path to the target invasion will pay the corresponding attack costs, will get the corresponding benefits, with m to describe. In the invasion of the power optical network, the intruder will judge the target value, when the target value to meet the requirements of the intruder will attack. The invasive feasibility can be described as:

$$\Delta = \frac{m - cost\left(e_{ji}\right)}{cost\left(e_{ji}\right)} \quad (6)$$

Analysis of the above equation can be seen, Δ is essentially a net income, that is, when $\Delta > 0$, the intruder will get the benefits.

The definition of a partial order relation set is given below: for a two adjacent nodes, if there is a tangential edge between the two, then there is a partial order relation between them, and the set of partial order relations is the partial order the relationship set is described by POS.

Through the above analysis we can see that when the POS set contains all the directional edges of the power optical network attack graph *AG*, it can obtain the power optical network attack path by traversing the POS collection element.

2.3 Power optical network attack path visualization display

In order to demonstrate the generation process of the attack path of the power optical network, this section first assigns the weight ϖ according to the mathematical model proposed in the previous section and the expert experience. Then the root node v_0 as the initial node, cut it as a node edge, into the collection POS_i. And then according to the topological order $\psi = \{v_1, v_2, v_3, a_1, a_2, v_4, v_5, v_6, a_3, a_4, v_7\}$ to obtain all the nodes between the partial order relationship set POS. Figure 2 shows the attack pattern after giving the weight ϖ.

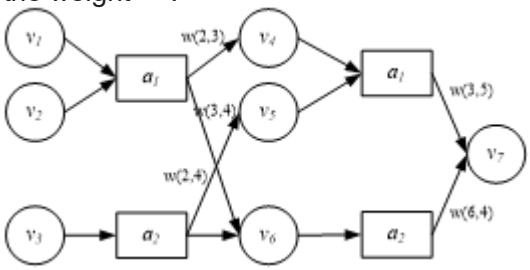

Figure 2 Gives the weight of the power after the optical network attack map

Fig. 2 Give weight after power optical network attack graph

Power optical network attack path generation process is as follows:

(1) cut off $v_1 \to a_1$, $POS_1 = \{\langle v_1, a_1\rangle\} \cup \{v_1 \wedge v_2\}$;

(2) cut off $v_2 \to a_1$, $v_3 \to a_2$, $POS_2 = POS_1 \cup \{\langle v_2, a_1\rangle\} \cup \{v_3 \wedge a_2\}$;

(3) cut off $a_1 \to v_4$: $POS_3 = POS_1 \cup \{\langle a_1, v_4\rangle\} \cup \{a_1 \wedge a_2\}$, judge $\langle a_1, v_4\rangle$: $\Delta = (3-2)/2 > 0, f_{14} = \oplus$;

(4) in accordance with the order of $a_1 \to a_6$, $a_2 \to v_5$, $a_2 \to v_6$, $a_3 \to v_7$, $a_4 \to v_7$ cut and judge, to get $f_{16} = \oplus$, $f_{25} = \oplus$, $f_{26} = \oplus$, $f_{37} = \oplus$, $f_{47} = \otimes$;

(5) Traverse the POS, get $Path_i$, find out all $\langle a_j, v_i\rangle$ of the state flag $\otimes$, and the path corresponding to the flag to give up the attack path;

(6) output power optical network attack path $Path_i$.

3 Experimental results analysis

3.1 Experimental environment

The method proposed in this paper is compared with Bayesian network method and Petri net

method to verify the validity of power grid attack path generation and visual display method proposed in this paper.

The experimental results show that the effectiveness of the proposed method is validated. Power network system topology shown in Figure 3.

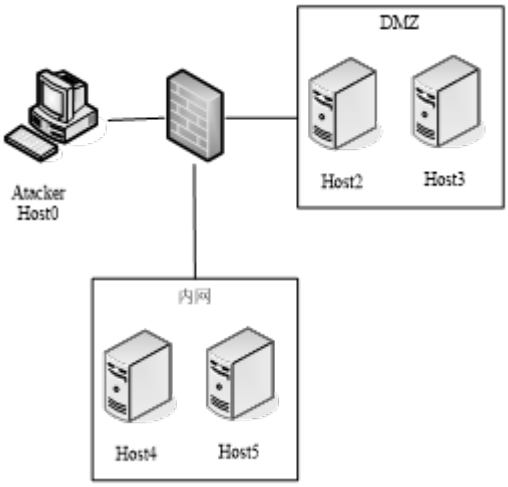

Figure 3 Power network system topology

Fig. 3 Electric power system optical network topology

As shown in Figure 3, the firewall divides the power network into the inner network area, the DMZ area and the external network area. The software configuration and vulnerability information for each application terminal is shown in Table 1.

Table 1 Software configuration and vulnerability information

Table 1 The software configuration and vulnerability information

The experimental site is shown in Figure 4.

Figure 4 Experimental site map

Fig. 4 The experiment site map

3.2 Attack path redundancy test

In this paper, we use the method, the Bayesian network method and the Petri net method to generate the attack path for the attack target, and get the number of attack paths and the actual attack. For the five different root nodes, the number of paths is compared, and the results obtained are described with reference to Fig. 5

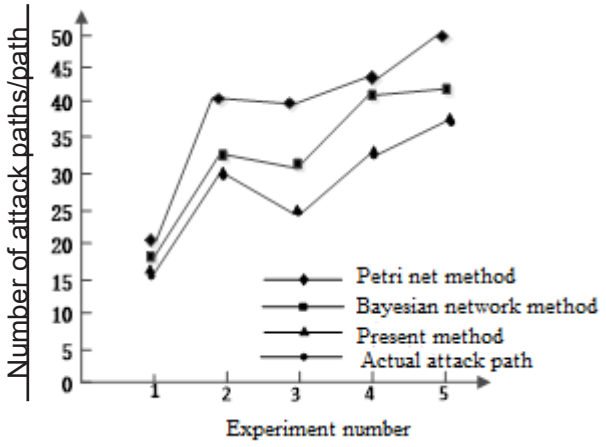

Figure 5 Comparison of the number of attack paths and the actual number of the three methods

In the five experiments, the number of attack paths generated in this method is equal to the number of actual attack paths. The number of attack paths and the number of actual attack paths generated by Bayesian network method and Petri net method exist. Very different, indicating that the path generated by this method does not exist redundant phenomenon.

3.3 Attack test

The evaluation results of the attack effect are obtained by the weighted average method. The index is used as an index to evaluate the attack effect of the three methods. The formula is described as follows:

$$Q = \sum_{i=1}^{5} \omega_i \sum_{j=1}^{n_i} \omega_j^{(i)} I_{ij} \quad (7)$$

Where n_i is used to describe the number of evaluation indicators for the *i*-th attack; I_{ij} is used to describe the normalized value of the *j*th evaluation index for the *i*-th attack; ω_i is used to describe the weighting factor. *Q* in the range of [0,1], the greater the value of *Q*, the better the effect of the generated attack path.

Figure 6 describes the results of the comparison of the attack results of the attack path generated by the method, the Bayesian network method and the Petri net method for the five experiments.

Host	The network segment	Service Provided	Vulnerability to use the results authority
H0	External network	Network attack	0
H2	DMZ	Network services	1
		Location service	2
H3	DMZ	Communication services	2
		Location service	1
H4	Intranet	Transmission service	2
		Network services	2
H5	Intranet	Communication services	1

Fig. 5 Three ways of attack path quantity and actual quantity comparison results

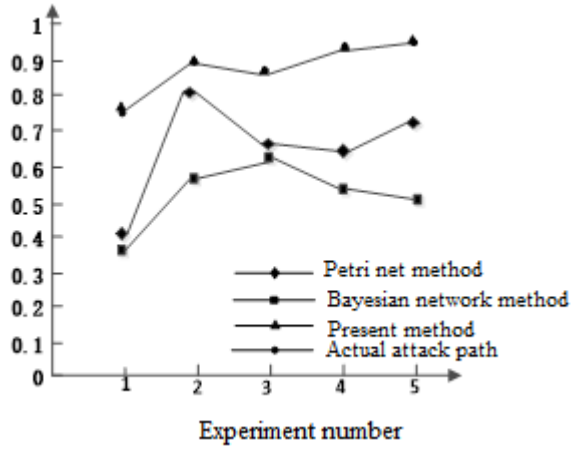

Figure 6 Comparison of the attack results of the attack paths generated by the three methods

Fig. 6 three ways to generate the attack value comparison results of evaluation the effect of the path

It can be seen that in the five experiments, the attack effect evaluation of the attack path generated by this method is obviously higher than that of the Bayesian network method and Petri net method, and the curve is more stable, which shows that the attack generated by this method The path works best.

3.4 Reliability testing

This section evaluates the reliability of the generated network attack path by averaging time-free and availability. The mean time between failures can be determined by:

$$MTBF_j = \frac{\left(1-\sum_{i=1}^{m_i} p_i\right)\times T}{\sum_{i=1}^{m_i} g_i} \quad (8)$$

Where T is used to describe the total experiment time; p_i is used to describe the probability of failure of the library; m_j is used to describe the number of libraries; g_i is used to describe the number of failures in the library.

Availability can be obtained by:

$$A = \left(1-\sum_{i=1}^{m_i} p_i\right)\times 100\% \quad (9)$$

The shorter the average trouble-free time, the higher the availability, the more reliable the attack path is generated.

Table 2 describes the reliability test results of the attack paths generated by the three methods.

Table 2 Three methods to generate the reliability of the attack path test results

Experiment number	Present method		Bayesian network method		Petri net method	
	Mean time between failures / s	Reliability /%	Mean time between failures / s	Reliability /%	Mean time between failures / s	Reliability /%
1	3.2	92.8	6.2	91.5	8.1	73.5
2	4.7	95.7	7.3	88.6	7.6	79.2
3	5.1	96.5	5.1	82.7	8.5	82.5
4	3.8	98.1	6.9	85.8	8.3	83.7
5	4.6	96.3	7.8	82.6	7.2	81.9

Table 2 The reliability of the three methods to generate the attack path test results

As shown in Table 2, it can be seen that compared with the Bayesian network method and the Petri net method, the average failure time of the attack path generated by this method is the shortest and the highest availability, which means that the method has the highest reliability.

4 Conclusion

This paper presents a new method for generating and visualizing the attack path of electric power network, and introduces the definition of atomic attack, attack graph and attack path. The cost of the attack path analysis, the intruder on the attack path selection problem into the feasibility of the invasion of the problem, by traversing the POS set of elements to generate power optical network attack path. The experimental results show that there is no redundancy phenomenon in the power optical network attack path generated by the proposed method, and the effect is good and the reliability is high.

References

[1] Wang J, Wang J, Wu C, et al. Anonymous communication with network coding against traffic analysis attack.[J].Proceedings-IEEE INFOCOM,2011,28(6):1008-1016.

[2] Zhang Y F, Ren S, Juan L I, et al. Research on High Power Inter-Channel Crosstalk Attack in Optical Networks[J]. Journal of Shanghai Jiaotong University,2015,51(1):7-13.

[3] Alenazi M J F, Çetinkaya E K, Sterbenz J P G. Cost-efficient algebraic connectivity optimisation of backbone networks[J]. Optical Switching&Networking,2014,14(4):107-116.

[4] Skorinkapov N, Jirattigalachote A, Wosinska L. An ILP Formulation for Power Equalization Placement to Limit Jamming Attack Propagation in Transparent Op-

tical Networks[J]. Procedia-Social and Behavioral Sciences,2015,199(2):137-142.

[5] Jiao Jian, Chen Xin. Analysis of network security system using stochastic Petri net [J]. Computer Science, 2014,41 (7): 119-121.

[6] Manousakis K, Ellinas G.Attack-aware planning of transparent optical networks [J]. Optochemical Switching & Networking, 2015, 19 (2): 97-109.

[J]. Signal Processing, 2016,32 (1): 91-97 [J]. Signal Processing, 2016,32 (1): 91-97. [7] Jia Renqing, Wu Xiaofu, Zhu Weiping.

JIA Ren-qing, WU Xiao-fu, ZHU Wei-ping.Double-Eavesdroppers Cooperative Attack on iJam [J]. Journal of Signal Processing, 2016,32 (1): 91-97.

[8] Manandhar K, Cao X, Hu F, et al. Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter [J]. IEEE Transactions on Control of Network Systems, 2014,1 (4): 370-379.

[9] ZHU Ya-dong. Study on Dynamic Mutation Suppression Model of Network Virus Based on Random Vector Resonance [J]. Electronic Design Engineering, 2016,24 (6): 26-28.

ZHU Ya-dong. Network virus dynamic parallel suppression model based on random vector resonance [J]. Electronic Design Engineering, 2016, 24 (6): 26-28.

[10] Tong Ming, Tian Weijuan. An INMF Resistant Strong Geometric Attack Video Watermarking Framework [J]. Journal of Xi'an Engineering University, 2016,30 (1): 58-65.

TONG Ming, TIAN Weijuan.A video watermark framework resistant to strong geometric attacks using incremental non-negative matrix factorization [J]. Journal of X'an Polytechnic University, 2016,30 (1): 58-65.