Journal of Electronic Research and Application
OPEN

Simulation of Attack Signal Path Identification in Radio Network Information

He Gaofeng, Ma Yuanyuan, Zhang Bo

Abstract: It is possible to improve the safety performance of the radio network by accurately identifying the attack signal path in the radio network information. When the attack signal path identification is carried out, it is necessary to calculate the vulnerability of the attack signal path, obtain the time series sample set of the network attack path, train the sample set for different vulnerabilities, and complete the path recognition. The traditional method is to establish the attack graph model. It cannot calculate the vulnerability of the attack signal path and cannot carry out the training, which leads to the limitation of the path recognition and the low efficiency. An improved identification method of attack signal path in radio network information with improved attack graph is proposed. Firstly, the attack map of the traditional method is transformed according to the theory of graph theory, and the concept of vulnerability factor is introduced into the improved attack graph. The vulnerability of the attack route is improved, and then the sliding time window is used to construct the network attack path recognition Time series sample set, Ada-Boosting method is used to train the sample sets with different vulnerabilities, and the regression matrix is obtained by using the training results. Finally, the attack signal path identification in the radio network information is completed. The simulation results show that the improved method has high accuracy and can guarantee the smooth operation of the radio network.

Key words: Radio network; attack path; identification method

(School of Management Science and Engineering, Global Energy Internet Research Institute, Nanjing 210003)

1 Introduction

With the continuous improvement of radio network technology, as the core network of modern society, radio network has become a high-value target of network attacks [1-3]. Because of the complexity of the attack on the radio network, the existing radio network security technology can only provide real-time power network attack detection information, has been unable to meet the security needs of the network [4-6]. Using the results of training to form a radio network attack path identification regression matrix, the use of the matrix of the radio network to identify the future security status, can effectively solve the problem [7].

In [8], the basic principle of Bayesian network is used to identify the attack signal path in the radio network information. This method firstly defines the resource state and operation sequence occupied by the historical attacker as attack evidence, constructs the Bayesian network attack graph, combines the risk probability of the Bayesian network theory to calculate the threat of radio network attack, The identification of the attack signal path in the radio network information is completed, the recognition accuracy of the method is high, but the operation process is difficult to realize. In [9], an attack graph model is established, the attack signal path identification in the radio network information. The transition process is defined by different types of network intrusion. On this basis, the probability of the next network intrusion path selection is calculated to complete the attack signal path identification in the radio network information. However, when the current method is used to identify the attack path, the attack model cannot estimate the future security situation of the power network, and the limitation of the method

is very important. In [10], a random game model is established for the radio Identification of Attack Signals in Network Information. This method introduces the game theory into the radio network attack path identification process, sets up the radio network attack and defense model, calculates the average attack time and the weak node of the radio network, and uses the calculated result to complete the recognition of the attack signal path in the radio network information. The method is simple to implement, but there is a problem that the recognition accuracy is poor.

In this paper, an improved attack path identification algorithm for radio network information based on improved attack graph is proposed.

2. Principle Model of Attack Signal System in Radio Network Information

In the radio network information attack signal system, the first access to the history of the network attack path samples, and the sample based on the formation of radio network attack map, the definition of attack path and network attack type, the use of network state transition probability between the invasion of the most may select the attack path, and calculate the probability of the attack by the intruder is successful, the principle of the attack signal system in the radio network information model, the specific steps are as follows:

Assuming that V_0 is a representative of the network attack, T is a representative of the network, on behalf of the network attack map, then use the following formula to map the network attack map for the radio network state transition system

$$T = \frac{S \otimes t \cdot s_0 \times S_G}{V_0} \quad (1)$$

Where, *S* is the network attack state of the collection, *t* is the network attack state transition relationship between the collection,S_0 representing the initial state of the network, S_G representing the target state of the attack set.

Assuming that $[S_1, S_2, \ldots S_{n-1}]$ represents a group of state sequences exist from the original state of the network, which S_n represents a network intrusion target state, satisfying the condition of $(S_i, S_{i+1}) \in t$, then the following formula $[S_1, S_2, \ldots S_{n-1}]$ will be defined as the path of the network intrusion

$$[S_1, S_2, \ldots S_{n-1}] = \frac{[S_n \in S_G] \otimes T}{(S_i, S_{i+1}) \in t} \quad (2)$$

In the formula, (S_i, S_{i+1}) represents any set of states in the attack graph.

The action against cyber attacks can be expressed as

$$\upsilon_{id} = \frac{(src\_host, dst\_hos)}{(S_1, S_2, \ldots, S_{n-1})} \quad (3)$$

Where, src_host is the attacking host ID, dst_hos is the victimized host,

Assuming that S_i is a certain type of state in the attack graph, ac_i represents the complexity of the path attack, assuming that the attacker arrives S_i, then select the *SUB_S* represented by the representative attack, using the following formula to identify the next step of the network attack target

$$\kappa_{im} = \frac{S_i \otimes ac_i \cdot S_i}{SUB\_S} \otimes \upsilon_{id} \times \frac{[S_1, S_2, \ldots S_{n-1}]}{T} \quad (4)$$

Assuming that the *L* is the attack path, *li* is represented by the attack path set, the rational model of the attack signal system in the radio network information is

$$C_i = \frac{L \otimes l_i}{} \times \frac{L \cdot \kappa_{im} \times \upsilon_{id}}{} \quad (5)$$

In order to identify the attack signal path by using the principle model of the attack signal system in the radio network information, it is necessary to calculate the vulnerability of the attack signal path, obtain the time series sample set of the network attack path identification, train the sample set for different vulnerabilities, and complete the path recognition. The traditional method is to establish the attack graph model, identify the attack path of the network signal, cannot calculate the vulnerability of the attack signal path, which cannot be targeted training, resulting in the path recognition of the limitations of large, low efficiency. An optimization method of radio network attack path identification based on improved attack graph is proposed.

3 Identification of Attack Signals in Radio Network Information Based on Improved Attack Graph

3.1 Calculation of the vulnerability of each attack signal path

In the process of identifying and identifying the attack signal path in the radio network information, the transformation of the current attack map is carried out, and the concept of vertex vulnerability factor is introduced to describe the transformation process. The network disturbance, node fault, In order to improve the vertex set of the attack graph,

the logical relationship between the vertices is deduced, and the vulnerability of each attack signal path is obtained. The concrete steps are as follows:

Assuming that *G* is the attack map created by the traditional method abstracts all the attack targets into the root node, abstracts all kinds of attacks into leaf nodes, adds all the root nodes and leaf nodes to the *V* representative collection, and sets up the vertices. All feasible edges are added and added to the collection, *A* , which can be calculated

$$G = V \times A \quad (6)$$

Assuming that L_1 is the first layer of the attack graph is represented, the leaf nodes with all degrees of entry 0 are added to the first set, and all vertices with tangential edges are found in the vertices of the set, and the collection, L_2, is formed until the traversal, to the last layer set L_n, using the following formula

$$L_n = \frac{\left[L_1, L_2 \ldots L_P\right]}{G \times n} \quad (7)$$

Assumption, C_i by representing the vertex vulnerability factor, C_i will be introduced into the transformation of the attack graph, using equation (8) to express C_i:

$$c_i = \frac{\left(I_i^+ + I_i^-\right) \cdot \alpha_i \cdot \beta_i}{\vec{G} \otimes \left[L_{l+1}, L_{l-1}\right] \times L_{l+1} \times v_i} \otimes \left[L_{l+1}, L_{l-1}\right] \quad (8)$$

In the formula, $I_i^+$and I_i^- represent the relative distribution in the vertex, L_{l+1} and L_{l-1} represent the vertex distribution of each vertex in the vertex represents the probability that the vertex,v_i, will trigger the representative of the vertex set,L_{l+1}, which B_i represents the attack event represented by the vertex,v_i, under different external conditions of a_i.

Then use the following formula to calculate the $\vec{G}$ representative of the improved attack map

$$\vec{G} = \frac{(V, A, X, Y, C)}{c_i \times L_n} \quad (9)$$

Where, *X* is the source attack path set, *Y* represents the intersection between the different sets of layers, *C* representing the set of vulnerability factors,C_i, for each vertex.

Assuming that s represents the total number of external condition categories of the attack path, P_k represents the probability of occurrence of the *k*th attack path attack condition, and R_k represents the determination of whether or not all vertices of L_{l+1} in the next set of vertices occur when the *k*th attack condition occurs Threshold, the following formula is used to calculate R_k

$$R_K = \frac{p_k \times R_K \times (C)}{L_{l+1} \times L_n} \geq 1 \quad (10)$$

In the formula, if v_i can trigger L_{l+1}, then R_k is 1, otherwise Rk is 0.

Suppose that the vertex data of the attack graph is represented by *m*, and the vulnerability of each attack path in the improved attack graph represented by $\vec{G}$ is calculated.

$$\overrightarrow{G(c_i)} = m \times \frac{L_n}{R_K \times \vec{G}} \quad (11)$$

In the formula, $\overrightarrow{G(c_i)}$ is the product of the vulnerability factor representing each vertex, the higher the product value indicates that the attack path is more harmful.

In summary, it can be explained that in the process of optimizing the identification of radio network attack path, the current attack map is transformed and the concept of vertex vulnerability factor is introduced to describe its transformation process. The network attack, power equipment failure and steady state the node perturbation mapping is used to improve the vertex set of the attack graph, the logical relationship between the vertices is deduced, the vulnerability of each attack path is obtained, which lays the foundation for the optimal identification of the attack path of the radio network.

3.2 Optimization of attack path identification based on recognition regression matrix

In the process of optimizing the identification of radio network attack path, the time series sample set is identified by using the sliding time window to construct the network attack path based on the vulnerability of the attack path obtained in the improved attack pattern obtained in section 3.1, and the sample is trained by Ada Boosting method Set the radio network attack path identification regression matrix using the results of the training to carry on the detailed identification to the future security state of the radio network, the concrete steps are as follows:

It is assumed that the recognition of each time point *i* is a time series based on the $\overrightarrow{G(c_i)}$ obtained by the 3.1 section at the respective time points identified by *i* for the radio network attack path, and the sliding time window size 4, the sliding step is 1, and obtains a number of time series composed of S_i to form a sample set

$$D(i) = \frac{D \times i}{\overrightarrow{G(c_i)}} \oplus S_i \quad (12)$$

The training set of the representative data of D is input into the AdaBoosting method. Assuming that T'' represents the maximum number of iterations, the training error δ of the tth sub-regression analysis matrix h_t is calculated by using equation (13)

$$\delta_t = \frac{w_t(i)}{D(i) \times S_i} \times h_t \mp T''(t) \quad (13)$$

Where, $w_t(i)$represents the weighting factor of the sample.

The weight of the sub-regression analysis matrix,h_t, is calculated using equation (14)

$$\lambda_t = \frac{1}{3} \frac{w_t(i)}{\delta_t} \times D(i) \times h_t \quad (14)$$

Assumptions, $w_{t+1}(t)$ by representing the sample weight of each sample in the next generation of training, use the following formula to calculate

$$w_{t+1}(t) = \frac{w_t(i) e^{-\lambda_t v_i h t(x_i)}}{E_t} \quad (15)$$

Where $h_t(x_i)$ represents the recognition value of the sub-analysis analysis matrix based on the input quantity x_i, v_i represents the true value of the recognition, and E_t represents the normalization coefficient.

Assuming that $\hat{U}_{J+4}$ is the true value of the radio network attack path at the $j + 4$th time point, U_{J+4} represents the radio network attack path identification value obtained by using the tth sub-regression analyzer h_t, then the constraint condition is

$$\sum_n w_{t+1}(i) = \frac{\hat{U}_{J+4}}{U_{J+4}} [h_t] \times \frac{[j+4]}{w_{t+1}(t)} \quad (16)$$

(h1, h2, ... ht) is multiplied by the corresponding weight represented by λ_t and the radio is calculated from the following equation: (h1, h2, ... ht) Network attack signal path optimization identification regression analysis matrix

$$H = \sum_n w_{t+1}(i) \times \frac{\lambda_t \otimes H}{[h_1, h_2, \ldots h_T]} Sign \lambda_t h_t(x) \quad (17)$$

Where *Sign* represents a symbolic function

Using the formula (17) to calculate the radio network attack path optimization identification regression analysis matrix, you can complete the radio network attack signal path optimization and identification.

4. Simulation results and analysis

In order to prove the validity of the proposed method of attack signal path identification in the radio network information based on improved attack graphs, an experiment is required. In this paper, the radio network field data of 214 days in 2012 is used as the experimental data source, and the radio network attack signal path recognition experiment environment is set up in MATLAB7.0 environment.

4.1 Different methods to identify the effectiveness of contrast

Respectively, using this method and literature [8] method for radio network attack signal path identification experiment. The error rate of the signal recognition of the radio network attack signal is compared with two different methods, and the effectiveness of the radio network attack signal path identification is measured by comparing the different results.

It can be concluded from Fig. 1 that the effectiveness of using the method to identify the signal path of the radio network is far superior to that of the radio network attack signal path identification by using [8] method, which is mainly due to the use of this method When the radio network attack signal path identification is carried out, the attack map of the traditional method is modified based on the theory of graph theory, and the concept of vulnerability factor is introduced into the improved attack graph to calculate the vulnerability of the attack signal path, Thus ensuring the effectiveness of the proposed method for radio network attack signal path identification.

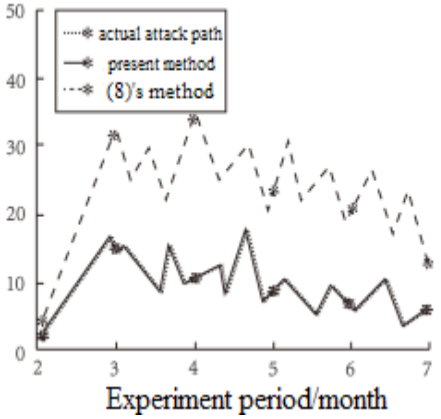

Figure 1 Comparison of error rates for different methods

4.2 Comparison of the overall superiority of different methods

Respectively, using this method and literature [8] method for radio network attack signal path identification experi-

ment. False alarm rate(%), error alarm rate (%) and stability (%) of the radio network attack signal path identification are compared. The effectiveness of different methods for radio network attack signal path identification is measured by comparing the results. The results are shown in Fig. 2 and Fig. 3 and Fig. 4.

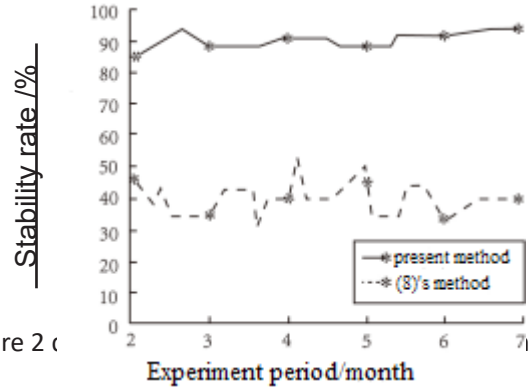

Figure 2 c iparison

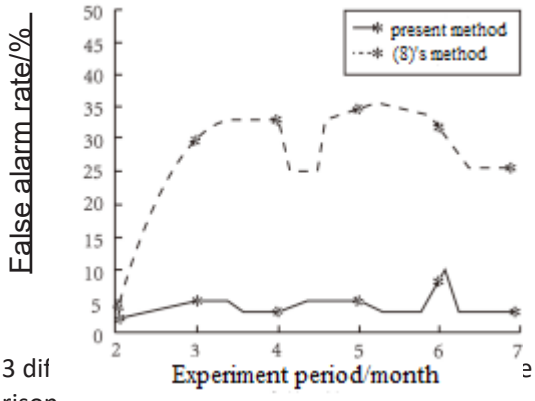

Figure 3 dif e comparison

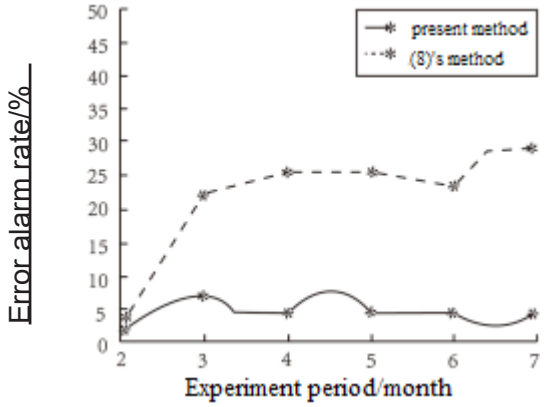

Figure 4 different methods to identify error alarm rate comparison

From the analysis in Fig. 2 to Fig. 4, it can be concluded that the overall superiority of the radio network attack signal path identification using this method is obviously higher than that of using the literature [8] method to realize the overall superiority of the radio network attack signal path recognition. Because the radio network attack signal path identification is used in this paper, the time series sample set is identified by the sliding time window, and the sample set is trained by Ada Boosting method. The radio network attack signal path identification Matrix, which guarantees the overall superiority of this method in the identification of radio network attack path.

5 Conclusion

This paper presents an optimization method of radio network attack path identification based on improved attack graph. The simulation results show that the method has high accuracy and can guarantee the smooth operation of the radio network.

References:

(1) Tian Guan Wei, ZHOU De Rong. Study and Simulation of Attack Path Marking Technology after Network Intrusion [J]. Computer Simulation, 2014,31 (12): 292-295.

[2] Zhang Feng Bin, Sun Gang, Zhang Bin. Study on Attack Path Marking Based on Immune Intrusion Detection [J]. Application Research of Computers, 2014,31 (1): 217-221.

[3] Teng Cui, Liang Chuan, LIANG Bi Zhen. Study on Intrusion Attack Recognition Technology Based on Attack Path Map [J]. Modern Electronics Technique, 2016,39 (7): 93-96.

[4] Zhai Ji Qiang, et al. Using DDT to Identify DDoS Attack Path [J]. Journal of Harbin University of Science and Technology, 2014,19 (5): 76-82.

[5] Liu Pei Peng, et al. Security Analysis of Anonymous Network I2P Path Selection [J]. Journal of Computer Research and Development, 2014,51 (7): 1555-1564.

[6] Chen Xiao Jun, et al. Study on Intrinsic Attack Inference Algorithm Based on Probability Attack Graph [J]. Journal of Computers, 2014,37 (1): 62-72.

[7] Huang Hui Ping, Xiao Shi De, Meng Xiang Ying. Information Security Risk Assessment of Industrial Control System Based on Attack Tree [J]. Application Research of Computers, 2015,32 (10): 3022-3025.

[8] We Zhi Jun, Cui Yi, Yue Meng. On the Cloud Computing Routing Platform Based on Virtual Hash Access Path VHSAP Defense DDoS Attack Method [J]. Journal of Communications, 2015,36 (1): 30-37.

[9] Huang Lujuan, et al. Combining DDoS Attack Packet Tag Deployment Scheme [J]. Computer Engineering and Applications, 2014,50 (5): 74-78.

[10] Lu Minfeng, Yang Liang. Standardized P2P Network Loan Platform Growth Path [J]. Southern School: Nanyang Teachers College Humanities and Social Sciences, 2016,36 (2): 105-109.