International Journal of Security and Its Applications
Vol. 10, No. 9 (2016), pp.301-308
http://dx.doi.org/10.14257/ijsia.2016.10.9.29

Research on Network Security Situation Prediction Based on Markov Game Theory

Wang Yong

Information Management Department, Xuzhou College of Industrial Technology, Xuzhou 221140, China
wangfengqi1981@163.com

Abstract

The prediction problem of network security should be studied facing the Massive malicious attacks, the information should be alarmed in time, then the network security can be ensured. The network security situation prediction is necessary to ensure safety of network, therefore the Markov game theory is applied in predicting the network security situation. Firstly, the network security situation prediction model is constructed based on coarse grained treatment. Secondly, the prediction model of network security situation based on Markov game theory is established, the basic procedure of network security situation prediction is established. Finally, the simulation of network security situation based on Markov game is carried out, and results show that the Markov game theory is an effective method for predicting the network security situation.

Keywords*: network security situation; prediction; Markov game theory*

1. Introduction

With rapid development of Internet technology, all kinds of network security events are emerging in an endless stream. Network security is the highest level of technology for the whole network situation awareness. The situation prediction can predict the security status of network for some time in the future based on the current situation of network, and then the corresponding measurements can be taken when the network is attacked. Because a series situation values can reflect the security status of network after situation evaluation, and the situation values equate to a series of time series, therefore the situation prediction is actually the time series prediction problem. The time series prediction belongs to regression problem, the network security situation generally has the characteristics of nonlinearity and time degeneration, the traditional predicting method cannot obtain high predicting precision and computing commutating efficiency, therefore it is necessary to find out an advanced method for predicting the network security situation. The Markov game theory can analyze the game relationship between threat transmission and loophole amendment, which can carry out dynamic analysis for security situation of network, and the approximate processing is carried out for attack threat and vulnerability information, then the status space is shortened, and the inputting scale of model can be reduced greatly, the network security situation predicting efficiency can be improved greatly [1-3].

The security situational awareness is put forward by Endsley firstly, the elements in environment are perceived from two dimensions of space and time, the knowledge is comprehensively understood and future status is predicted, the situation awareness is firstly applied in aviation, military and emergency services. In 1999, Bass et al. combined the situation awareness and network security technology, then the situation awareness is introduced into network security, then the network security situation evaluation and network security prediction are studied by many scientists. The vulnerability research of network is concerned by some scientists, some scientists put forward AML model, and

ISSN: 1738-9976 IJSIA

the vulnerability prediction of network is amended from the aspects of software multi version, multi cycle. The framework TANDI and SGIF were put forward to trace the attack, and the graph theory and probability method are all used in these framework. The existing achievements can not reflect the effect of changes of future security element value on future network security situation, and the interaction effect between different elements are ignored, therefore the new prediction method of network security situation is proposed in this research.

2. Network Security Situation Prediction Model

The coarse grained treatment of security situation value can achieve the symbolization of time series for security situation. The static symbolization can divide the security situation value R_L into five intervals, which is expressed as follows [4]:

$$S_R = \begin{cases} E, R_i > \varepsilon + \sigma \\ O, \varepsilon + \frac{1}{2}\sigma < R_i < \varepsilon + \sigma \\ Y, \varepsilon - \frac{1}{2}\sigma < R_i < \varepsilon + \frac{1}{2}\sigma \\ B, \varepsilon - \sigma < R_i < \varepsilon - \frac{1}{2}\sigma \\ G, R_i < \varepsilon - \sigma \end{cases} \quad (1)$$

where ε is the average value, σ is the variance, E , O , Y , B , G are the red, orange, yellow, blue and green early warning status of network, which are corresponding to serious, high risk, medium risk, low risk, and safety. Based on this idea, the safety situation series R_L can be transferred to the symbol series, which are expressed as follows:

$$S_R = (s_1, s_2, s_3, \cdots, s_n), \ s_i = E, O, Y, B, G \quad (2)$$

The whole system interval can be divided into finite sub intervals, and every sub space is given a string, then the whole system interval can be transferred to a symbol sequences.

The symbol sequence S_R obtained using continuous two strings $((S_{2i-1}, S_{2i}), i = 1,2,\cdots)$ as node to express the security situation in this time, and the corresponding expression is listed as follows:

$$\{EE, EO, EY, EB, OE, \cdots\} \quad (3)$$

The network security situation dimension of this security situation model is equal to twenty five. Using EY as example, where E denotes that the network security situation is in the state of serious risk in a certain time point, Y denotes that the network security situation is in the state of medium risk in another time point, therefore EY denotes the network security situation changes between the two time points. Then the network security situation can be modeled by network structure, which is shown in Figure 1 [5].

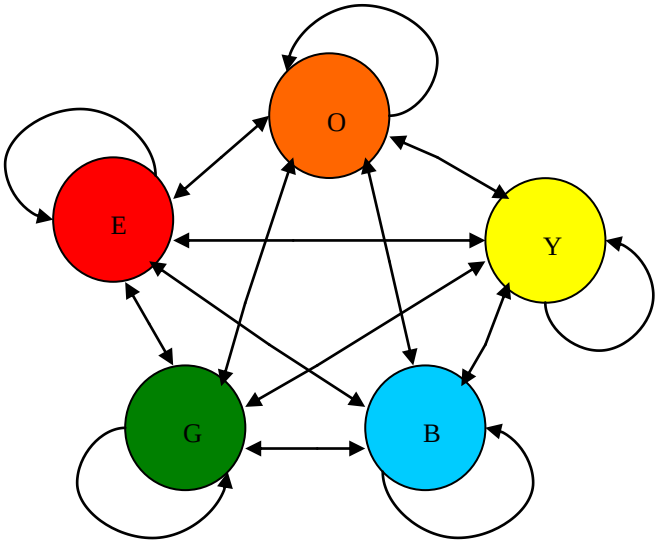

Figure 1. Diagram of Network Security Situation Dimension

The arrow in the figure denotes the change from a time point to another time point. a situation status dimension can not appear in the simulation process because the algorithm situation dimension. Therefore twenty four status dimensions are used to construct the weighted network that the network security situation changes with time, and the directed line denotes the modal connection from front time slot to backward time slot.

The out-degree of node is considered in this research, the relationship between probability $p(k)$ of node k and node degree k can be expressed as follows [6]:

$$p(k) = \frac{N_i}{N} \tag{4}$$

where N_i denotes the number of nodes, N denotes the total number of nodes.

The distance between node i and node j is defined by d_{ij}, and the average route length L is defined by the following expression:

$$L = \frac{1}{N(N-1)} \sum_{i \neq j} d_{ij} \tag{5}$$

The cluster coefficient can reflect the close degree of network, the cluster coefficient of single node is calculated by the following expression:

$$C_i^{\omega} = \frac{1}{s_i(k_i - 1)} \sum_{(i,j)} \frac{\omega_{ij} + \omega_{ik}}{2} a_{ij} a_{ik} a_{jk} \tag{6}$$

where ω_{ij} denotes the weighted value of connection line between two nodes, $s_i = \sum_j \omega_{ij}$ denotes the strength of node i, $\sum_{k>j} a_{ij} a_{ik} a_{jk}$ denotes the total number of triangles concluding node i.

3. Prediction Model of Network Security Situation based on Markov Game Theory

The network security situation prediction belongs to system engineering, and the basic procedure is shown in Figure 2.

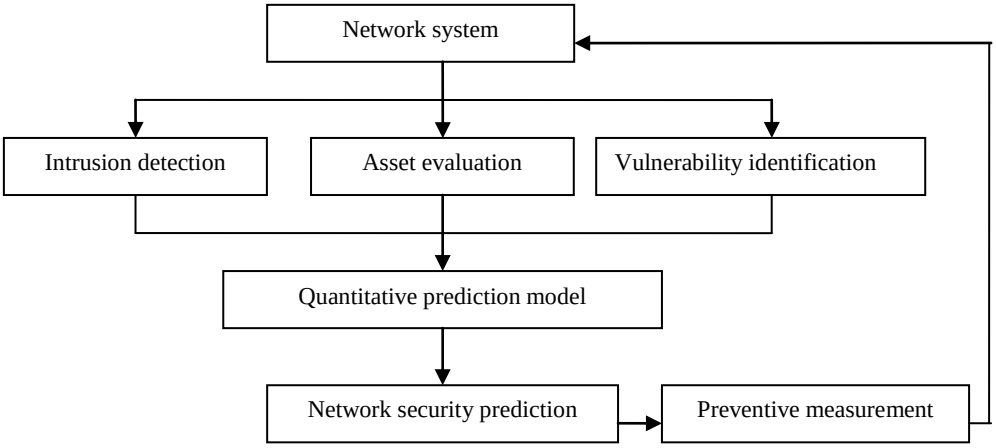

Figure 2. Basic Procedure of Network Security Situation Prediction

The security situation prediction should cover the whole network. Firstly, the status information is collected, which concludes basic structure of network, capital evaluation, node loophole information and so on, the prediction model is constructed according to Markov game theory based on the information collected. And finally the prediction of the network security situation is carried out, and the corresponding preventive measurements are put forward.

Because the network security situation changes with time, therefore the prediction of network security situation is a dynamic cycle process, then the periodic prediction should be carried out for network security situation, and the problems existing in the network can be found out in real time, and the effective preventive measurements can be taken in time.

The game theory is the mathematical model on conflict and cooperation among intelligent decision makers, and the Markov decision process is an good tool for studying the multi stage decision process optimization problem under random environment, Markov game theory is constructed through combing the game theory and Markov decision process, and the corresponding prediction model is constructed based on Markov game theory.

The Markov game model is constructed, which is listed as follows:

(1) Game three parties: the attacker exists in threat form, which can cause damage to system through threat transmission. Defender uses administrator as deputy, which can reduce the vulnerability to threats and cut off the transmission route of threat, then the security of the system can be improved. The neutral party uses the normal customer as represent, which can affect the performance of network through visiting network resources, and then the statistical characteristics of all normal customers can be considered as an entity. The aim of attacker is to cause great damage of network, the aim of defender is opposite, the neutral party only concern itself benefit, and does not consider the status of network.

(2) The status space is defined as follows: the status space made up of all possible status is defined by $TPN(t)$, the status at t moment is defined as follows [7]:

$$TPN(t,k)=\{s^i(k),e^j(k)\},\ i=1,2,\cdots,M,\ j=1,2,\cdots,N \tag{7}$$

where M is the transmission node, N is transmission route.

The status of i th transmission node at k moment is defined as follows:

$$s^i(k)=(id_i,valua_i,\rho_{aik},t_{fik},v_{fik}) \tag{8}$$

The status of j th transmission route at k moment is defined as follows:

$$e^j(k)=(id_{js},id_{jd},valua_{ej},\rho_{ejk},p_{ejk}) \tag{9}$$

(3) The strategy collection is the all possible activity collection of game three parties, the activity of attacker u^t is the first step transmission of threat t, the activity of defender u^v is the reinforcement scheme executed by the administrator, the activity of neutral party u^c is the fluctuation changing rate of access statistics of normal customer.

(4) Transferring probability: with activity chose of every game party, the status of system changes constantly, the changing rules of system status is described by:

$$p(TPN(t,k+1)\mid TPN(t,k),u_k^t,u_k^v,u_k^c) \tag{10}$$

where $TPN(t,k+1)$ and $TPN(t,k)$ are the system status at $k+1$ and k moment, u_k^t,u_k^v,u_k^c are the activities of all parties at k moment.

(5) Reward function can describe the gain and loss of all parties after game.

The basic procedure of game is listed as follow using a network with four nodes and five directed lines, for a threat t in this network the TPN of t is constructed, and the game three par ties are threat, administrator, and normal customer, the activity of attacker is to transmit t to uninfected node based on TPN, and the activity of defender is that the administrator amend the vulnerability of system node utilized by t, the activity of neutral party is the visiting rate of network when the normal customers add or reduce, the system status is all possible status of TPN relating to t, the every game party can choose the activity itself according to system status and reward function dynamically, the system can turn to next status with a certain probability according to the effect of every party's activity [8].

Step 1: At k moment, t is only inspected in node 1, the system is in the state A;

Step 2: At $k+1$ moment, t spread to node 3, and the administer can fix the node 3, the visiting rate of normal customer does not change, if the system jumps to status B, the fixing plan does not get success, and t has transmitted successfully, if the system jumps to status C, the fixing plan is success, and t transmission is failure.

Step 3: at $k+2$ moment, using status B as example, t transmit to node 4, node 2 and node 1, the administrator fixes the node 1, the visiting rate of normal customer does not change, if the system jumps to status D, t transmit to node 2 and node 4 successfully, and the fixing plan of node 1 is success, or transmission of t in this direction is failure.

The Markov game process is shown in Figure 3.

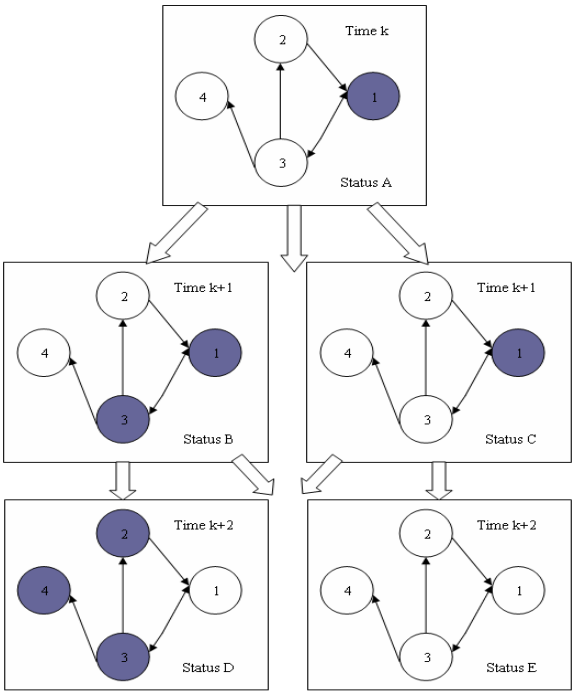

Figure 3. Diagram of Markov Game Process for Predicting Network Security Situation

4. Simulation of Network Security Situation based on Markov Game

In order to verify the effectiveness of this prediction method, the certain network is constructed , and the simulation programmer is compiled by MATLAB software, and the security guard log of computer security from January 1 2015 to March 30, 2015 are collected eight times per day, then 823 security situation value are obtained, which is transferred to security situation symbol sequences based on coarse granulation method, which is REEOYOBBYOBB…, and then the Markov game theory is used to predict the security situation of this network, and the prediction results are shown in Table 1.

Table 1. Simulation Prediction Results of Network Security Situation

Real value	Situation	Prediction	Error/%
11.84	B	B	3.18%
12.89	Y	Y	6.93%
19.54	O	O	4.96%
21.44	O	O	6.74%
18.36	O	Y	12.52%
12.43	Y	Y	8.92%
10.88	B	B	7.10%
12.06	B	B	3.97%

As seen from Table 1, the Markov game theory can predict the network security situation correctly, and the correct rate is 87.5%, and the prediction error ranges from 3.18% to 12.52%, the prediction results are simple to be understand by administrator, then the safety measurements can be taken in time, and the network security can be ensured.

5. Conclusions

The network security situation prediction is an new technology of achieving the network security monitoring, and the potent and malicious attack can be found out, and the harm brought out by attack can be decreased. Currently the network security situation is more complex, it is necessary to offer correct network security situation information for administrator of network. The traditional prediction method of network security situation has bigger error, and has difficulty in confirming the parameter and other disadvantages. Therefore the Markov game theory is applied in network security situation prediction, and the simulation results show that the Markov game theory has high prediction precision, which can offer an effective method for safe operation of network. The prediction results can be benefit for taking proper measurements for dealing with the future network security event.

References

[1] Z. Shu, L. Lixia and Q. Xiaohua, "Cloud Prediction of Network Security Situation", Telecommunications Science, vol. 29, no. 12, **(2013)**.
[2] H. Tong-qing and Z. Yi, "An Approach to Real-time Network Security Situation Prediction", Journal of Chinese Computer Systems, vol. 35, no. 2, **(2014)**.
[3] C. Hong, W. Fei, X. Zhenjiu and S. Lina, "Method of network security situation prediction based on IHS_LSSVR", Computer Engineering and Applications, vol. 50, no. 23, **(2014)**.
[4] G. Chun-xiao and S. Yang, "A New Optimized Algorithm Based on Quantum Eolutionary Strategy for Network Security Situation Prediction", Journal of Chinese Computer Systems, vol. 35, no. 6, **(2014)**.
[5] X. Hanjie and S. Xiuli, "Network security situation prediction based on hyper parameter optimization of relevance vector machine", Journal of Computer Applications, vol. 35, no. 7, **(2015)**.
[6] L. Ji-zhen, M. Xiang-ru, W. Xiang-xi and K. Qiao-yan, "Network security situation prediction based on Gaussian process optimized by glowworm swarm optimization", Systems Engineering and Electronics, vol. 37, no. 8, **(2015)**.
[7] H. He, H. Changzhen and Y. Shuping, "Decision Model of Optimal Active Response for Network Security Using Partial Observable Markov Game", Journal of Xi'an Jiaotong University, vol. 45, no. 4, **(2011)**.
[8] Ma C.Y.T., Yau D.K.Y., X. Lou and Rao N.S.V., "Markov game analysis for attack-defense of power networks under possible misinformation", IEEE Transactions on Power Systems, vol. 28, no. 2, **(2013)**.

