TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 12, No. 8, August 2014, pp. 6354 ~ 6360
DOI: 10.11591/telkomnika.v12i8.5082

A Dynamic Selection Algorithm on Optimal Auto-Response for Network Survivability

Jinhui Zhao*[1,2], Yujia Sun[1], Liangxun Shuo[1]
[1]Network Information Security Laboratory Shijiazhuang University of Economics,
No.136, Huai'an East Road, Shijiazhuang, China, 0311-87207577
[2]School of Mechanical Electronic and Information Engineering China University of Mining and Technology,
Beijing,10083, China, 18630129615
*Corresponding author, e-mail: zhaojh9977@sohu.com[1], sunyujia@sjzue.edu.cn[2],
shuoliangxun@sjzue.edu.cn[3]

Abstract

In the selection process of survival strategies, it is a challenging work to automatically choose the optimal measure for the survival event. A dynamic selection algorithm is proposed, based on feedback control. According to the feature of survival strategy, the strategy model is presented, which includes fuor specific attribute. The dynamic update process of attribute vector is described in detail. Combining the weight of preference and attributes of strategy, the TOPSIS evaluation is employed to select optimal measure. Experiments and analysis show that optimal measure selected by proposed algorithm is appropriate and wishful, which enriches the research content in this field.

Keywords*: network survivability, dynamic update, active response, TOPSIS (technique for order preference by similarity to ideal solution), evaluation*

1. Introduction

After or when survival incidents occur in information system, auto-response technology is to take a series of measures or actions to ensure the confidentiality, integrity and availability of critical services. Cohen's [1] study, about the capabilities of network managements, the response time and the number of successful defense, shown that timely response is essential in preventing survival incidents. In reality, because the capabilities of administrators are uneven and the timeliness of the response is difficult, timely and reasonable auto-response technology is one of the important means to improve the system viability. How to select emergency measures and how to ensure the effectiveness of the measures is key step in auto-response technology.

There have been several strategic choice models to achieve a quick and timely automatic response, which are mainly the following categories:

Static Mapping Model: The specific type of alarms associated with the specific response measures in this model. When there are alarms, specific response measures are selected from response decision table according to alarm type. This method is simple to implement, easy to operate and maintain, which is a good solution to the problems of timely response, administrator capacity and so on. But, this method did not consider the credibility and severity of the attacks, the survival condition of attacked object, and the response measures are easy to guess by attackers. It is not suitable for large-scale systems [2].

Dynamic Mapping Model [3]: according to the characteristics of attack and system, this model selects suitable measures to response the attack. Because the model considers the various factors, the response strategies are more suitable for the actual situation. However, this method is less consideration in the negative impact of response; it is the loss outweighs the gain sometime.

Cost-sensitive Model: the goal of auto-response is to minimize the cost in exchange for maximum security. Therefore, the researchers propose the cost-sensitive model by analyzing the relationship between the pay and the benefit of response, and to select the appropriate response measures, for example reference [4, 5]. This model can ensure that the cost of response is less than the loss of survival incident. But there are many factors in calculated the

Received November 9, 2013; Revised April 1, 2014; Accepted April 15, 2014

cost of response and the loss in survival incident, and how to determine and quantify these factors is a new challenge. Moreover, the cost of response is uncertain. Sometime, the cost of response is high at the beginning of survival incident, but the cost is low for the whole event. How to calculate the cost of the survival incident and the response is a problem in the interaction process.

Real-time Intrusion Risk Assessment Model [6, 7]: this model automatically select response measures according to the risk assessment of survival incident. It has a good anti-jamming capability, and synthetically considers the performance and the negative impact of response, which is the latest model at present.

The goal of automatical response is to judge current survival situation by survival detection, risk assessment, situational awareness, and implement active safeguard procedures according to the judgement [8]. The content of situational awareness was detailed in reference [9], which didn't present for space. This work focus on strategy selection, which propose a dynamic evaluation and selection method of survival strategy based on dynamic update of attribute vector. And, the accuracy of proposed method is tested by simulated experiment.

2. The Model of Dynamic Strategic Selection

The model of dynamic strategic selection is shown in Figure 1.

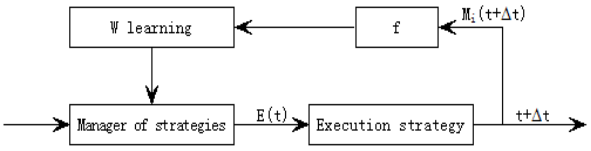

Figure 1. The Process of Dynamic Strategic Selection

In the model of dynamic strategic selection, manager of strategies is responsible for classification and storage of strategies, evaluation and choice; when survival events have detected or survivability need enhance, the survival module send request and the weight of preference to manager of strategies; the manager of strategies select the strategy in the set, which has the same function, according to the preference of user and the attribute vectors of strategy; the manager of strategies adjusts weight vector of strategies according to the feedback information by the feedback module. The core is how to select the right survival strategies. The strategic selection system, in survival system, must meet the timeliness, the accuracy, the rationality, self-adaptive, security and so on.

Define 1: the set, in which the strategies have the same function, is described as:

$$S_f = \{s_i \mid 1 \le i \le n\} \tag{1}$$

Where n is the number of strategies; each s_i has the same function, but its implementation technique, operating conditions and so on may vary.

In order to distinguish different strategies, we describe in detail strategies by attributes. According to the special requirements in survival system, the attribute vector is defined as:

Define 2: the attribute vector of s_i at t moment is as:

$$A^{(i)}(t) = \{A_a^{(i)}(t), A_e^{(i)}(t), A_t^{(i)}(t), A_c^{(i)}(t)\} \tag{2}$$

When the strategy (s_i) is selected at the moment (t), the attribute vector is changed according to the feedback $M_i(t+\Delta t)$. Δt

$$A^{(i)}(t+\Delta t) = f(A^{(i)}(t), M_i(t+\Delta t)) \quad (3)$$

The feedback includes the start time, the end time, the survival states, and so on.

Define 3: The vector of preference indicates the user's preference for properties of measures.

$$\vec{W} = \{w_i \mid \sum_{i=1}^{4} w_i = 1\} \quad (4)$$

Where w_i is the weight of element in $A^{(i)}(t)$.

Define 4: According to the vector of preference, at the moment t the selection process of optimal survival strategies can express as:

$$P: \{(A^{(i)}(t), \vec{W}) \mid i = 1,2,\cdots,n\} \to E(t) \quad (5)$$

$E(t)$ is the comprehensive evaluation index set of s_i at the moment t, according to $A^{(i)}(t)$ add $\vec{W}$.

3. Dynamic Update of Attribute Vector

3.1. Availability ($A_a^{(i)}(t)$)

The available status of strategy can be acquired by feed back and monitor. At the moment t, the availability of s_i can estimate by the online probability, which can calculate as:

$$a_a^{(i)}(t) = \frac{T_u^{(i)}(t)}{T_u^{(i)}(t) + T_d^{(i)}(t)} \quad (6)$$

Where: $T_u^{(i)}(t)$ is the summation of s_i available time at period $[t-l, t]$ by the moment t; $T_d^{(i)}(t)$ expresses the summation of s_i unusable time.

In order to rapidly reflect the changing state of measures, we join the detection of adjacent states in the calculation of the online probability.

$$\begin{cases} T_u^{(i)}(t) = T_u^{(i)}(t-1) + (1-\mu^{(i)}(t)) \times \Delta T^{(i)}(t) \\ T_d^{(i)}(t) = T_d^{(i)}(t-1) + \mu^{(i)}(t) \times \Delta T^{(i)}(t) \end{cases} \quad (7)$$

Where $\Delta T^{(i)}(t)$ is the difference for completion of application or detection between t-1 and t. $\mu^{(i)}(t)$ is related to the result of feedback and detection, which can get by:

$$\mu^{(i)}(t) = \begin{cases} 0, & U^{(i)}(t-1) = up \wedge U^{(i)}(t) = up \\ 1, & U^{(i)}(t-1) = down \wedge U^{(i)}(t) = down \\ \varphi & (U^{(i)}(t-1) = up \wedge U^{(i)}(t) = up) \vee (U^{(i)}(t-1) = down \wedge U^{(i)}(t) = down) \end{cases} \quad (8)$$

Where $\varphi \in [0,1]$.

3.2. Effectiveness ($A_e^{(i)}(t)$)

The effectiveness of s_i at the moment t can present as:

$$a_e^{(i)}(t) = 1 - \frac{N_f^{(i)}(t)}{N^{(i)}(t)} \tag{9}$$

Where $N^{(i)}(t)$ indicates s_i's frequency of use in $[t-l,t]$ by the time t; $N_f^{(i)}(t)$ expresses the frequency without the desired result. The value of l is obtained according to the s_i's intensive of use. When l is large enough, $a_e^{(i)}(t)$ can represent the effectiveness of s_i at the moment t+1.

3.3. Timeliness ($A_t^{(i)}(t)$)

$A_t^{(i)}(t)$ represents the time interval of dealing survival event, which includes request of user, choice of strategy, execution and taking effect. Some factors affect this attribute, such as bandwidth, transmission rate, congestion, failure and so on.

$$a_t^{(i)}(t) = (1-a)\cdot a_t^{(i)}(t-1) + a\cdot T^{(i)}(t) \tag{10}$$

Where $T^{(i)}(t)$ is the time for execution of s_i, which is employed or detected at moment t; a is the weighted average factor.

3.4. Cost ($A_c^{(i)}(t)$)

$A_c^{(i)}(t)$ includes two parts: negative impact and resource consideration.

$$a_c^{(i)}(t) = Ic + Ne \tag{11}$$

Where Ic indicates the forecast for consume of different resource; Ne is the value of negative impact.

The value of Ic is confirmed by specialist, according to service condition and repository. Ne can calculate by:

$$Ne = P\cdot S_t \cdot \frac{T^{(i)}(t)}{T} \tag{12}$$

Where P presents the value of source; S_t express the intension, which is classed three or more different grades levels and map into interval [0, 1]; $T^{(i)}(t)$ means the execution time of measure; T present the time period, which was used in assessment asset.

4. The Dynamic Selected Process of Survival Strategic

According to the description of define 4, we select optimal strategy by TOPSIS(Technique for Order Preference by Similarity to an Ideal Solution), the steps are following:

1) It is need to establish decision matrix of attributes.

$$X = \begin{pmatrix} a_a^{(1)}(t) & \cdots & a_c^{(1)}(t) \\ \vdots & \ddots & \vdots \\ a_a^{(n)}(t) & \cdots & a_c^{(n)}(t) \end{pmatrix} \tag{13}$$

Where n is the number of measures, which have the same function.

2) There are cost indexes and performance indexes. The cost indexes are as small as possible, while performance indexes are the bigger the better; the dimensions are different for each index. For ease of comparison, indexes are normalized by following:

$$\begin{cases} r_{ij} = a_j^{(i)}(t) / a^{(i)}(t)^{\max} & (Performanc\ \ e) \\ r_{ij} = a_j^{(i)}(t)^{\min} / a^{(i)}(t) & (Cost\ ) \end{cases} \tag{14}$$

3) The weighted normalized matrix is obtained by W and X.

$$Y = (y_{ij}) = (w_j \cdot r_{ij}) \tag{15}$$

4) According to the matrix of Y, the optimal and worst decision schemes are brought out.

$$\begin{cases} A^+ = \{\max(\ y_{i1}, \cdots, y_{in})\} = \{y_1^{\max}, \cdots, y_n^{\max}\} \\ A^- = \{\min(\ y_{i1}, \cdots, y_{in})\} = \{y_1^{\min}, \cdots, y_n^{\min}\} \end{cases} \tag{16}$$

5) The distance of each strategy to A^+ and A^- is calculated.

$$\begin{cases} D_i^+ = [\sum_{j=1}^{4} (y_{ij} - y_j^{\max})^2]^{1/2} \\ D_i^- = [\sum_{j=1}^{4} (y_{ij} - y_j^{\min})^2]^{1/2} \end{cases} \tag{17}$$

6) To build the comprehensive evaluation index set, and select optimal strategy.

$$E(t) = \left(e_i(t) \mid e_i(t) = \frac{D_i^-}{D_i^- + D_i^+} \right) \tag{18}$$

5. Experiments

In order to test the effectiveness of this model, the experimental environment is putted up. The topological structure shows as Figure 2. If an intruder wants to attack the nodes in the inner network from Internet, the firewall is the first protective barrier. A switchboard connects all the servers and PC. The super intrusion detection system (SIDS) is the second shielding, which monitor the survival events and select automatic response measures. There are monitors in each server, which detect the service failures or the results of response and send the state to the SIDS.

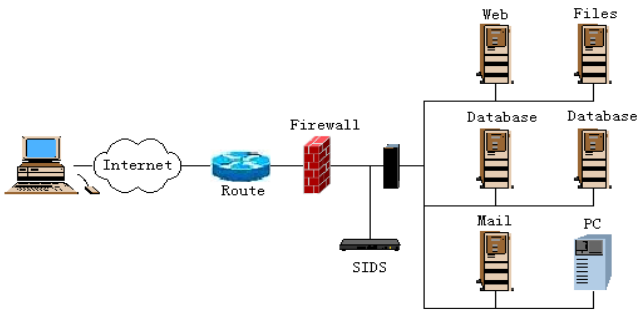

Figure 2. The Network Environment of Experiment

Attack classification is the base of strategy choice, which is divided into two categories: failure events, security events. Progressive failures and unexpected accidents are taken as one class, and take corresponding response measures. Based on the attack classification method of MIT Lincoln laboratory, there are four major types attacks: Probes, R2L, U2R and DoS. Accordingly, automatic response strategies are divided into record, analysis, alarming, backup, refuse, isolation, beat back and cancel. Each response strategy includes several measures. According to above, the SIDS selects response method, when survival event take place.

According to the situation awareness, the SIDS select the application strategies. In order to analyze the process of choice, we simulate the offensive and defensive behavior for four hours. In the first hour, there are only malicious attacks, whih have low frequency; in the second hour, the frequency of malicious attacks is high, and the malicious attacks include some more harmful; there are malicious attacks with failure of service in the third hour; some service crashe in the fourth hour. The Table 1 shows the specific.

Table 1. Survival Events and Response Strategies

	Time	Position	Type of Threat	Strategy Description
1	0:03	Route	Portsweep scan	Checked out
2	0:07	Server	Satan scan	Checked out
3	0:15	Mail	Trojan	Checked out
4	0:23	PC	Trojan	Authentication Filter
5	0:29	WEB	Apache mod_ssl buffer overflow	IP Access Restrictions
6	0:31	Route	Worms	Successful survival
7	0:36	WEB	Worms	Tolerance
		……	……	……
		……	……	……
53	3:43	WEB	DOS	Shutdown
54	3:47	Database	Heap-based buffer overflow	Patch
55	3:50	Database	failure	Switch to Backup

According to different function, each node has different survival purposes, so it has distinct preference of response strategy. For example, the service of Web focus on providing information, the attribute of cost is more important in its choice of strategy; because in the files service, confidentiality is most important, the effectiveness is a priority. In order to provide the continuous service, the server of database design dual hot standby,but the initial value of negative impact is high. In the experiment, the preference weight vectors are as Table 2.

Table 2. Preference Weight Vectors

Server	Availability	Effectiveness	Timeliness	Cost
Web	0.3	0.1	0.1	0.5
Files	0.3	0.3	0.3	0.1
Database	0.2	0.3	0.2	0.3
Mail	0.2	0.3	0.2	0.3
PC	0.25	0.25	0.25	0.25

At the moment t, the optimal measure (s_i) is employed, the attributes of s_i are adjusted according to feedback $M_i(t+1)$ at the moment $t+1$. The update method is as the above.

The last row in Table 1 shown the response methods in the experiment. As shown, web server usually adopt the method of tolerance, because the weight of cost is high, which has more attention on the impact of survial event; only when the attack of DOS leaded to failure, the web server restarted. the restricted access for IP of attacker has high frequency in files server for its effectiveness and timeliness. Database prefer to delete the suspicious user, and the server would switch to backup when there is a critical fault. Presented approache not only takes into the cost of the response, but also consider the other properties and dynamic properties. the rationality and accuracy of presented approaches is significantly better than the traditional methods. Experiments also verify the results.

4. Conclusion

Survival situational awareness is the base of automatic response; automatic response is the important method to improve the viability of system. Strategy choice is the key step in utomatic response. This paper foucs on selection of optimal strategy for the same survival event, according to non-functional property. The structure of strategy evaluation is given, based on dynamic update Qos of survival strategy, which elaborated the dynamic update process of attributes vector based on information feedback and process of assessment based on TOPSIS algorithm. Experiments indicate that selected results were appropriate and desired, and the proposed algorithm was suitable for the real network environment.

Acknowledgements

The authors would like to acknowledge shijiazhuang university of economics in support with the initial fund of scientific research after our doctorate and Hebei province's science and technology plan project (13210702D).

References

[1] Cohen F.Simulating Cyber Attacks, Defenses and Consequenees. http://all.net/joumal/ntb/simulate/simulate.html, 1999-3/2009-3.
[2] Thomas Toth, Christopher Kruegel. *Evaluating the impact of automated intrusion response mechanisms*. Porc of the 18th Annual Computer Security Application Conference Washington DC. IEEE Computer Society. 2002: 301-310.
[3] CA Carve, U pooch. *A Methodology for Using Intelligent Agent to Provide Automated Intrusion Response. New York:* IEEE Sysetms, Man and Cybemetics Inofmration Assurance and Securiyt Workshop. West Point. 2000; 163-175.
[4] GUO Yu, SUN. Intrusion response based on SVM cost-sensitive decision model. 2007: 27(11): 2704-2706.
[5] Wu Hongrun, Qin Jun, Zheng Bojin. Anti-attack Ability Based on Costs in Complex Networks. 2012; 39(8): 224-227,255.
[6] Hu He, Hu Changzhen, Yao Shuping. Decision on Optimal Active Response Based on Intrusion Graph. *Journal of Beijing University of Technology*. 2012; 38(11): 1659-1664.
[7] WuWen, Meng Xiangru Ma Zhiqiang, Chen Duolong. Network Sruvivability Situation Tracking Based on Modulariaed Dynamic Game. *Journal of XIAN Jiaotong University*. 2012; 46(12): y1-y6.
[8] Zhang Yongzheng, Fang Binxing, Chi Yue, etal. Risk propagation model for assessing network information systems. *Journal of Software*. 2007; 18(1): 137-145.
[9] Zhao Jinhui, Zhou Yu, Shuo Liangxun. A Situation Awareness Model of System Survivability Based on Variable Fuzzy Set. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(8): 1701-1708.
[10] Zhao Jinhui, Wang Xuehui, Xu Qian. Variable Weights in Assessment of Survival System. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(5): 2284-2290.
[11] Lin Wangqun, Wang Hui, Liu Jiahong, et al. Research on active defense technology in network security based on non-cooperative dynamic game theory. *Journal of Computer Research and Developmen*t. 2011; 48(2): 306-310.