Applied Mechanics and Materials Vols 380-384 (2013) pp 2728-2731 *Online: 2013-08-30*
© (2013) Trans Tech Publications, Switzerland
doi:10.4028/www.scientific.net/AMM.380-384.2728

A New Research on Instrusion Detection System based on Artificial Immune

Lan Shi[a], Yanrui Zhang[b]

College of Information Science and Engineering, Northeastern University,

Shenyang, 110819, China

[a]email: shilan@ise.neu.edu.com, [b]email: zhangyanrui_dbdx@foxmail.com

Keywords: Intrusion Detection System; Mature Detector; Co-evolution Method; Widely Application

Abstract. The paper proposed a new model by applying biological immune into intrusion detection system, in this new model, generated algorithm of the mature detection get improved, the self-et realized dynamic, co-evolution module can effectively find the system potential vulnerabilities and generate the corresponding patch to strengthen the system. As of result, simulation experiment for this new model is did, through the analysis of the result for simulation experiment, it shows that the new model and method has higher rate in making matured detector than the traditional model and method, and new model also has higher detecting rate on intrusion detection. To sum up, the co-evolution method is able to strengthen the system effectively.

Introduction

Jerne [1] proposed the first model of the immune system in 1974, and because of its excellent features of diversity, tolerance, self-learning, self-organizing, adaptive, distributed parallel processing, immunological memory, the robustness etc, biological immune system [2] is to be studied and applied to other fields, especially computer security field. Many researchers have proposed intrusion detection model based on artificial immune system, but from the current research situation, most of them are still in the exploratory stage. A new immune based dynamic intrusion detection model [3] [4] is proposed in this paper. In this model, the immaturity detector is made by this method has stronger pertinence and higher rate of survival. The new model adopt the method with integrate of detect based on misuse and detect based on abnormity, it overcome the defect of used single technique, and improves the detect efficiency of system. In addition the definition of self-used [5] a dynamic process, and this self-set can reflect the normal data of network more all-sided, and it overcome the low percentage of coverage detect for self-muster. Under the inspiration of phenomenon of co-evolution in the nature, co-evolution [6] method is developed to strengthen the system. In this thesis, a new model of IDS based on AIS is proposed in view of questions exist in current research. And co-evolution method is also proposed to strengthen the system.

Design Module

The system structure of the model is described from the flow of the detector in Figure 1.

Dynamic self-set and dynamic non-self-set through the variation to produce immature detection cells [7]. Immature detection cells must pass a fixed number of self-tolerance, if matched with any self during tolerance, it will be death, or it will successfully evolved into mature cell, and thus into the life cycle of the mature cell. In this life cycle, if immature detection cell do not match sufficient number antigen or the matching antigen is normal self-antigen (if a match does not get assistance stimulation signal, i.e. the erroneous detection occurred), the immature detection cell goes to dying. Conversely, if matched enough antigens and got synergistic stimulation signal, the immature detection cell will evolve for memory detection cell. Memory detection cell will have infinite life value until they're error matching the normal antigens (matched an antigen, but did not get the synergistic stimulation signal, which produce a false detection) or replace by other memory detection cell.

The system uses a new kind of mature detector generation algorithm. The algorithm has the following steps:

Step one: Generate the self set and non-self set and coding.

Step two: Random select self or non-self and evolve its variation (according to the length of the binary string 1en to get variation and match value r to select suitable variation bits) become mature detector set.

Step three: Match the non-mature detector generated by variation with self, if exist any self can match with it, then remove it.

Step four: Repeat the second step and the third step until generate a mature detector.

The flow of generating mature detectors is shown in Figure 2.

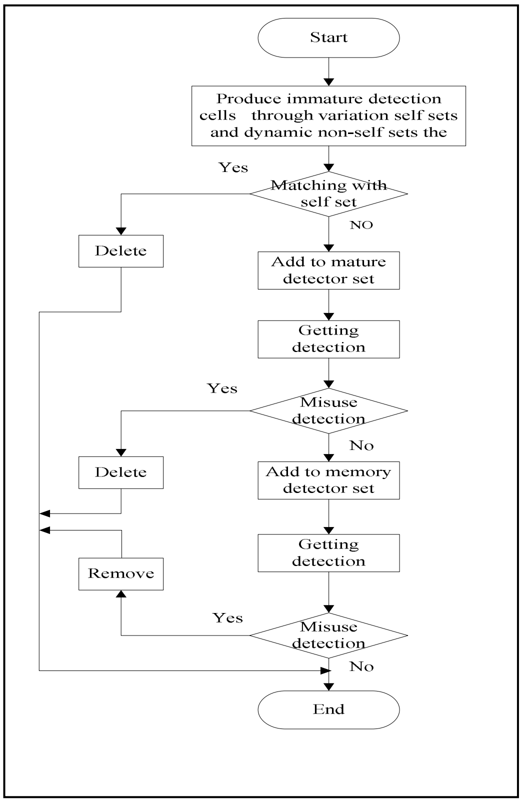
Start
Produce immature detection cells through variation self sets and dynamic non-self sets the
Yes
Matching with self set
NO
Delete
Add to mature detector set
Getting detection
Yes
Misuse detection
No
Delete
Add to memory detector set
Getting detection
Remove
Yes
Misuse detection
No
End

Fig.1. Flow of detectors' generating

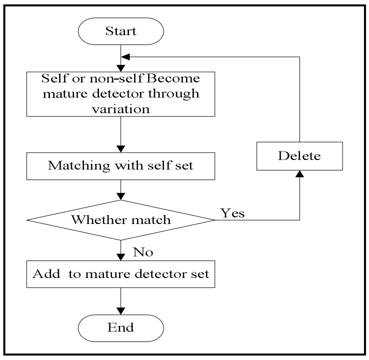
Start
Self or non-self Become mature detector through variation
Matching with self set
Delete
Whether match
Yes
No
Add to mature detector set
End

Fig.2. Flow of generating mature detectors

Co-evolution Method Strengthening System Module

A. Finding bugs module

The model finds potential bugs through the evolution of a group of malicious non-self-antigens. This evolution requires misuse detection module to provide the fitness value of any given non-self (non-self) antigen. Our system is unable to detect the percentage of the detector. If a non-self-antigen whose fitness value is 1, it will potentially on behalf of a bug in the system. Intuitively speaking, an IDS system is very robust, it will cost more in order to find the bugs. Here, the price is iterations, iterations is required to find a bug. We will prove this point of view in the back of the simulation experiments.

B. Developing patches module

The goal of this module is to make the system more robust, it uses a set of FHM find bugs to create a group of additional detector set to overwrite vulnerability is found. This additional detector set will combine with detector set in misuse detector module, and generating a larger detector set. The process of generating additional detector includes the following steps, as shown in Figure 5.

Step one: Randomly select a set of candidate detector from vulnerability set, if not enough, random generate detector to complement. And set each candidate detector fitness value is 0.

Step two: Determine whether vulnerability set is empty, if empty, end the process, and otherwise enter the third step.

Step three: Use static genetic algorithm to evolve the set of candidate detector, use each candidate detector to match vulnerability set, if matched one, the fitness value of this candidate detector plus 1. And self set to do the matching operation, if matched, the fitness value of the candidate detector is set to 0.

Step four: Determining iterations is equal to 0, if equal, enter the fifth step, otherwise, iterations plus 1, enter the third step.

Step five: Choose the maximum fitness value detector that is detector can match the most bugs, remove, and add to the misuse detection detector set. Remove the bug which matched with the detector from the bug set, so the detector generated by the present method will have a different coverage. Randomly select one from the bug set add to the candidate detector set. Iterations is set to 0, go to step two.

Simulation Experiment

A. Mature detector generation

In this experiment, taking r = 8, sf_s = 1000, nsf_s = 1000, sf_b = 60, nsf_b = 5, and the number of generated mature detector (mature_detector_num) takes 500, 1000, 1500, 2000. The experiment results as shown in Table1.

Table.1. Time using table of new algorithm and old algorithm

Mature detector number	**Cost time**	
	Time1(ms)	**Time2(ms)**
500	9814	8945
1000	20131	18905
1500	45934	42157
2000	96212	90571

Time1 is traditional algorithms cost, time2 is improved algorithm cost. Clearly can be seen from the table that the improved algorithm requires the time significantly shorter than the traditional algorithms requires, which means the improved algorithm is more efficient.

B. Activation threshold on system

Here take r = 10, ma_s = 200, me_s = 200, sf_s = 200, nsf_s = 200, age = 20, sf_b = 65, nsf_b = 5, and respectively take th = 5, 8, 12, 15, each of 5 experiments and get the average results. The experiment results as shown in Figure 3.

We can see from the Figure that as the mature detector activation closing value increases, the probability of the mature detector detects exception reduces, while the probability of mature detector turn into memory detector also will be reduce, causing the number of memory testing set in detector set is relatively less. Thus, lr false negative rate of the system detects becomes larger with the increase of the threshold value th and simultaneously wr decreases.

C. Co-evolution method

Here carry out the following experiment on the basis of 400 detectors in misuse detection.

Figure 4 shows the running of this experiment. The x-axis is the scale of detector set in current misuse detection module.

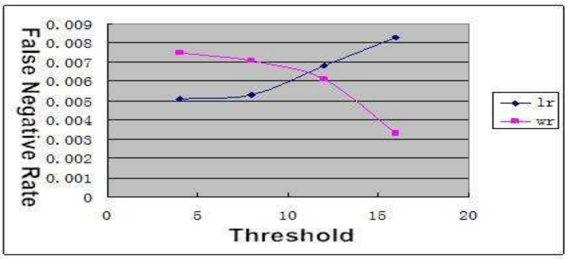

Fig.3. Diagram of activating threshold’s affection to detection result

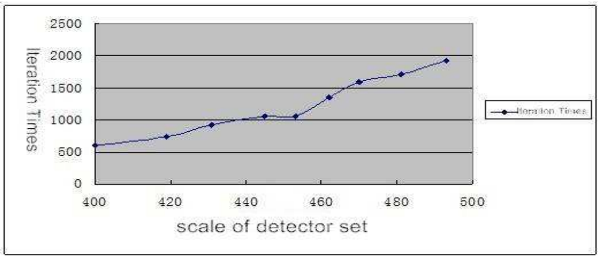

Fig.4. Diagram of scale of detector set’s affection to FHM’s iteration times.

The y-axis is iterations of the FHM. The curve in the chart shows iterations FHM find a bug required, we can see from this chart, the cost FHM looking for bugs significant increases when newly create detector is added to the system. Some might say, the more detectors rightly bring greater coverage, so FHM needs more iteration to find the bugs. This is correct in the general case.

Conclusion

This paper proposes a new method for generating mature detector, it is able to improve the mature detector generating efficiency. Through the simulation of co-evolutionary phenomena on ecology, this paper proposes a co-evolutionary model to find the system vulnerabilities, and to patch their systems. This method is significant to strengthen the system.

Acknowledgement

In this paper, the research was sponsored by the Nature Science Foundation (Project No. 61100182).

References

[1] United states general accounting office. Information security: computer attacks at department of defense pose increasing risks[J]. GAO/AIMD-96-84,USA,1996.

[2] CERT Coordination Center [EB/OL], http://www.cert.org/encyc_article/tocencyc.html.

[3] T. Verwoerd, R. Hunt. Intrusion detection techniques and approaches [J], Computer Communications, 2002, 25:1356-1365.

[4] K. L. Fox, R. R. Ilenning, J. H. Reed, R. Simonian. An Neural Network Approach Towards Intrusion detection[A], In Proceedings of the 13th National Computer Security Conference[C], 1990.

[5] W. Lee, S. J. Stolof, K. W. Mok. A Data Mining Framework for Building Intrusion Detection Models [J], IEEE Symposium on Security and Privacy, 1999,

[6] Goldberg D, Deb. K. A Comparative Analysis of Selection Schemes Used in Genetic Algorithms[J], Foundations of Genetic Algorithms, 1991:69-93.

[7] L. J. Eshelman, J. D. Schaffer. Real-Coded Genetic Algorithms and Interval Schemata[J], Foundations of Genetic Algorithms, 1993, 2:187-202.

Vehicle, Mechatronics and Information Technologies
10.4028/www.scientific.net/AMM.380-384

A New Research on Instrusion Detection System Based on Artificial Immune
10.4028/www.scientific.net/AMM.380-384.2728