Research on Bio-inspired Multi-net Paralleling Mechanism Based on Web Application

Ruijuan Zheng, Huiqiang Wang, and Yonggang Pang

College of Computer Science and Technology, Harbin Engineering University,
Harbin 150001, China
`rjwo@163.com`

Abstract. With the rapid development of network technologies and deteriorating of network environment, traditional single-net security system can't satisfy the security requirement. Excellent security performance of biological systems impels bio-inspired network security theory to be a hot topic currently. We advance Bio-inspired Multi-Net Security (B-MNS) system which implements the functional distributary of different subnets by state transition in Multi-Net Paralleling (MNP) mechanism. Firstly, concept model of B-MNS and MNP mechanism are outlined; secondly, parameter estimation and modifying algorithms are introduced to construct the mathematical model of B-MNS; at last, the practicability and high efficiency are proved by a simulation.

Keywords: bio-inspired; multi-net paralleling; hidden Markov; LoadRunner.

1   Introduction

With the development of network technologies and the deterioration of network entironment, traditional security system can't satisfy the security requirement. Similar security mechanisms between biology and computer network make it possible to solve the network security problems inspired by biology. Bio-inspired research started in the middle of 1990s[1, 2]. In current, bio-inspired research mainly focuses on computer immune system[3], anti-virus immune system[4] and bio-inspired fault tolerance computing[5], which are all limited in the immune system. We are inspired by the "Multi-Net" security mechanism and apply them into the design of B-MNS. The paper is organized as follows: Based on BMNSM[6], section 2 presents the concept model of B-MNS. Section 3 constructs the mathematical model. By a simulation, section 4 compares the performance of B-MNS and traditional security system. Section 5 presents some conclusions and proposes future work on B-MNS.

2   Concept Model for B-MNS

In the intricate and mutable survival environment, biological systems keep high security performance and implement the normal running, which owe to the perfect security system of biology. The key mechanisms can be summarized as follows: (1)

Multi layers. (2) Multi time sequences. (3) Multi nets. Close cooperating with each other, several independent "Nets" complete the security of system. So, the core of security system in specific biological population scale is MNP mechanism.

Inspired by this, B-MNS is divided into three angles: Population Scale, Time Stage and Subnet Type. Monitoring subnet monitors the data transmitted by data transmission subnet and implements precaution, detection and response. Recovery subnet deals with the abnormal information and recovers the network state. Corresponding mechanism takes charge of synchronization and information transfer between three subnets. MNP is embodied as "Three-Net-Paralleling"(Figure 1).
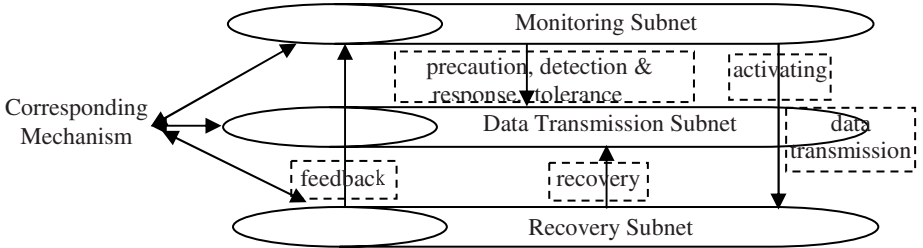

Fig. 1. Three-Net-Paralleling mechanism

3   Mathematical Model

To a given observation sequence $O = O_1, O_2, …, O_T$, Baum-Welch algorithm will find out a $\lambda=(\Pi, A, B)$ which maximizes $P(O/\lambda)$.We select O= (C, C, C) as the example sequence, so the final estimation results are showed in table 1.

Table 1. Estimation results

$P(O/\lambda)$	Π	A				B		
0.33333	(1,0,0,0)	4.46357e-007	0.327284	0.672715	0	0	0	1
		0	1.93327e-007	4.22823e-007	0.999999	0	0	1
		0	0	3.249e-007	1	0	0	1
		0	0	0	1	0	0	1

The modifying procedure is:

a.   Initialization: $\delta_1(i) = \pi_i b_{ii}(O_i), 1 \le i \le N$ (1)

$\varphi_1(i) = 0, 1 \le i \le N$ (2)

b.   Recursion: $\delta_t(j) = \max\limits_{1 \le i \le N}[\delta_{t-1}(i)a_{ij}]b_{ij}(O_t), 2 \le t \le T, 1 \le j \le N$ (3)

$\varphi_t(j) = \operatorname*{argmax}\limits_{1 \le i \le N}[\delta_{t-1}(i)a_{ij}], 2 \le t \le T, 1 \le j \le N$ (4)

c.   Result:

$$P^* = \max_{1 \le i \le N} [\delta_T(i)] \tag{5}$$

$$q_T^* = \operatorname*{argmax}_{1 \le i \le N} [\delta_T(i)] \tag{6}$$

d.   Optimal state sequence: $q_t^* = \varphi_{t+1}(q_{t+1}^*), t = T - 1, T - 2, ..., 1$ $\tag{7}$

After modifying, we get L= (1/5,1/5,1/5,1/3), U= (1/3,1/3,2/3,3/5).
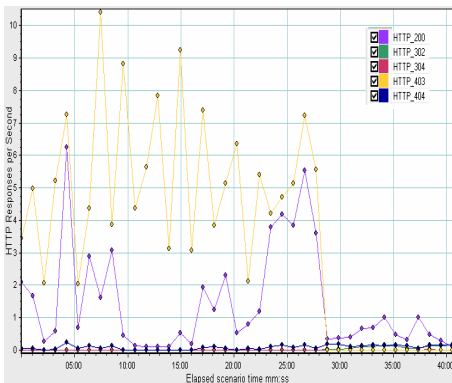
4   Simulation

Figure 2(a) and 2(b) respectively describes the changing of Hits-Throughput in single-net system and B-MNS. The average Hits and throughput in single-net system respectively is 5.206 times/second (t/s) and 25815.54 Bytes/second (B/s); the average Hits and throughput in B-MNS respectively is 10.851 t/s and 52443.666 B/s.
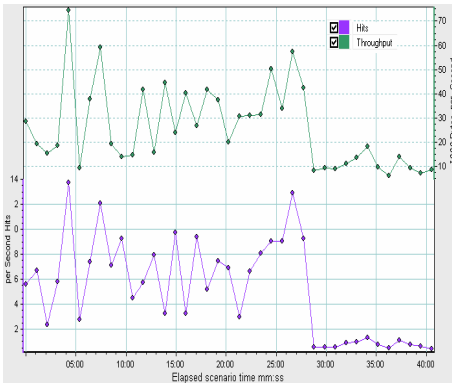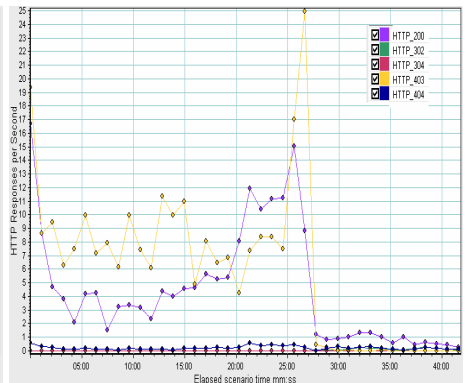

Fig. 2(a). Hits-Throughput per second in single-net system
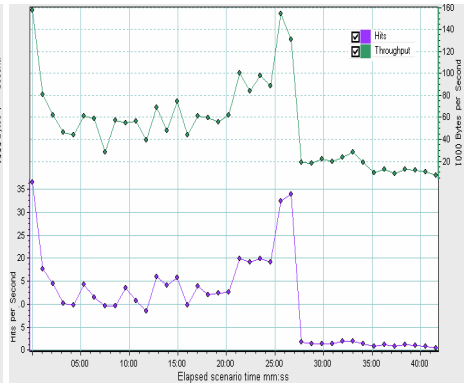
Fig. 2(b). Hits-Throughput per second in B-MNS

Fig. 3(a). Http responses per second in single-net system

Fig. 3(b). Http responses per second in B-MNS

During the simulation, Http response ability of single-net system is common, which is showed in figure 3(a). In B-MNS, under the help of corresponding mechanism, three subnets in B-MNS implement the functional distributary. The Http response in B-MNS is showed in figure 3(b).

Comparing of Http responses is showed in table 2.

Table 2. Http responses

Responses/s	Http_200	Http_302	Http_304	Http_403	Http_404
single-net	1.455	0.027	0	3.727	0.083
B-MNS	4.569	0.045	0.001	6.168	0.224

5 Conclusion

Traditional single-net security system can't adapt to the increasing user requirement and aggravating network environment. Inspired by multi-net security mechanism of biological system, we advanced MNP mechanism. In this paper, we put forward B-MNS. Simulation results prove that the performance of B-MNS improves 3-4 times than that of single-net system. In the future work, we'll integrate the security methods and technologies in time stages of B-MNS.

References

1. Forrest, S., Perelson, A., Allen, L., et al: Self-nonself Discrimination in a Computer. Proceedings of the IEEE Symposium on Research in Security and Privacy. LOS Alamilos: IEEE Computer Society Press (1994)
2. Kephart, J.O.: A Biologically Inspired Immune System for Computers. Proceedings of the 4th International Workshop on the Synthesis and Simulation of Living Systems and Artificial Life (1994) 130–139
3. Forrest, S., Hofmeyr, S.A., Somayaji, A., Longstaff, T.A., et al: A Sense of Self for Unix Processes. Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy. IEEE Computer Society Press. (1996) 120–128
4. MAO, X.Y., Liang, Y.W.: Research on the Model of Immune Firewall. Computer Engineering. (2004.8), 25(8):1282–1285
5. Bradley, D.W., Ortega-sanchez, C., Tyrrell, A.M., et al: Embryonics + Immunotronics: A Bio-Inspired Approach to Fault Tolerance. Proceedings of the 2nd NASA/DoD Workshop on Evolvable Hardware (2000.7)
6. Wang, H.Q., Zheng, R.J., Li, X.Y., Liu. D.X.: A Bio-inspired Multidimensional Network Security Model. Proceedings of the 2006 International Multi-Symposiums of Computer and Computational Sciences (2006.6) Vol (2):3–7