Anti-virus Security and Robustness of Heterogeneous Immune Static Network

Tao Gong

Abstract—**Unknown viruses are dangerous for networks, but traditional approaches for recognizing the features of viruses are not good at detecting the unknown viruses. To overcome the bottleneck, a normal model and an immune computation model were proposed with self/non-self representation to detect recognize and eliminate worms in a heterogeneous e-learning network. Inspired from the natural immune system, the immune computation included the steps of detecting self/non-self, recognizing known non-self, learning unknown non-self and eliminating non-self. The self/non-self detection was based on querying in the self database and the self database was built on the normal model of the static network system. After the detection, the recognition of known non-self was based on querying in the non-self database and the recognition of unknown non-self was based on learning unknown non-self. The learning algorithm was designed on the neural network or the learning mechanism from examples. The last step was elimination of all the non-self and failover of the damaged Web system. The immunization of the static network system was programmed with Java to test effectiveness of the approach, after the static network system was infected by some worms. The results of the immunization simulations show that, the immune program can detect all the worms, recognize all known worms and most unknown worms, and eliminate the worms. Moreover, the damaged files of the static network system can all be repaired through the normal model and immunization. Therefore, the normal model and the immune computation model of the static network system are effective in some anti-virus applications.**

Key words: immune model, immune network, security, anti-virus

I. Introduction

THE artificial immune system is a tri-tier adaptive system, inspired from biological immune system, and the adaptive immune tier is the most important tier for keeping the system adaptive, intelligent and robust [1]. The adaptive immunity of the immune system can transform the primary immune respond for unknown viruses into the secondary immune response by adjusting the knowledge information about the known viruses in some immune cells [2]. The antibodies can learn unknown viruses and some immune cells can memorize the results of learning [3-5]. The adaptive immunity of the system is useful for recognizing and eliminating unknown viruses so that the normal state of the system can be repaired in time to keep robust [6].

The adaptive immunity of the immune system may be understood by some scientists and immunologists with some famous immunological theories and models, such as immune learning [7], immune tolerance [8], immune memory [9], theory of clonal selection [10], immune network model [11] and so on. Among the theories and models of adaptive immunity, evolution is a basic mechanism for the immune system and its immune cells to process the immune response against some viruses [12]. Inspired from the adaptive immunity of the biological immune system, some similar models are built in the artificial immune to simulate the immune system, and the models are designed and tested with immune evolutionary algorithms and neural networks [13-18].

On the modern network like the Internet, many viruses such as worms often do great harm to the information society. Since 1988, the worms of Morris have made surprising loss on the Internet servers, and Orman summarized the history of the worms of Morris [19]. Staniford Paxson and Weaver analyzed the anti-worm problem on the Internet, and for example some uncontrolled worms could infect the whole Internet in about 30 second [20]. The whole network would be terminated or destroyed by the worms, and Balthrop Forrest and Newman analyzed how harmful spread of the worms was to the technological networks [21].

To detect and stop the worms, some network techniques were used. Levy analyzed the types of propagation and attack for some worms [22]. Gray and Berk designed a rapid approach for detecting Worms using ICMP-T3 Analysis [23]. Dasgupta and González presented a technique inspired by the negative selection mechanism of the immune system that can detect foreign patterns in the non-self space [24]. Zou Gong and Towsley built and analyzed a propagation model of the Code Red worm [25]. Madhusudan and Lockwood presented the design and implementation of a system that automatically detected new worms in real time by monitoring all traffic on a network [26]. But the traditional detection techniques could not detect all worms especially such as unknown worms because traditional approaches depend on matching the features of non-selfs. To overcome the bottleneck of the incomplete detection, a normal model was proposed on space- time properties and a new immune algorithm for detecting all selfs and all non-selfs was proposed on the normal model. The new detection approach was on matching the space-time properties, so unknown non-selfs were detected by detecting the known selfs.

This work was supported in part by the National Natural Science Foundation of China under Grant 60404021, the Shanghai Educational Development Foundation under Grant 2007CG42 and Donghua Univ. Foundation under Grant #104-10-0044017.

Tao Gong is with the College of Information Science and Technology, Donghua University, Shanghai 201620, China (phone: 86-21-67792312; fax: 86-21-67792312; e-mail: taogong@dhu.edu.cn).

QShine 2008, July 28-31, 2008, Hong Kong, Hong Kong.
 ISBN 978-963-9799-26-4
DOI 10.4108/ICST.QSHINE2008.4265

II. IMMUNE COMPUTING MODEL OF ANTI-WORM NETWORK

A. Tri-tier Immune Model of Artificial Immune System

The adaptive immune tier is the second tier of the tri-tier immune model for the artificial immune system, and the first tier is the innate immune tier and the third tier is the parallel immune tier [27-30], shown in Fig. 1.

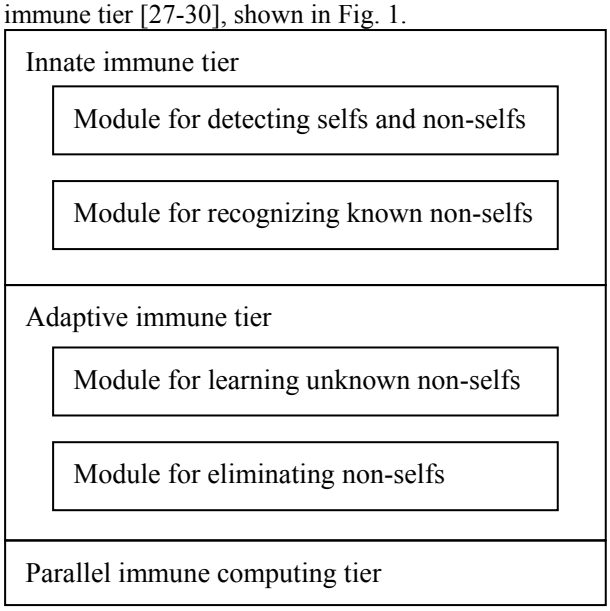

Fig. 1. Tri-tier immune model of artificial immune system.

The innate immune tier is comprised of two modules. The first module is used to detect the selfs and the non-selfs in the system that the artificial immune system protects. The second module is used to recognize the features of known non-selfs and classify the types of the known worms. The approach for detecting the non-selfs is based on the approach for detecting the selfs, and the approach for detecting the selfs is based on the normal model of the selfs.

The adaptive immune tier is comprised of two modules. The first module is used to learn features and types of the unknown worms with the knowledge about all the known worms. The second module is used to eliminate the non-selfs that have been detected.

The parallel immune computing tier is a parallel computer, which is used to increase efficiency and load balance in the artificial immune system.

Definition 1 The self/non-self detection of the artificial immune system S is represented with the random event D, and the probability that the random event D occurs is called as the probability of self/non-self detection, denoted as $P(D)$. Suppose the sum of the detected selfs is represented with n_s, the sum of the detected non-selfs is represented with n_n, the sum of the selfs is represented with s_s, and the sum of current non-selfs is represented with s_n, then the probability of self detection is represented as such.

$$P(D_s) = \frac{n_s}{s_s}, \tag{1}$$

And the probability of non-self detection is represented as such.

$$P(D_n) = \frac{n_n}{s_n}. \tag{2}$$

Theorem 1 On the condition that the time property is correct, based on the normal model and the tri-tier immune computing model of the static Web system, the probability of detecting selfs is 100% and the probability of detecting non-selfs is also 100%.

Proof The normal state of all the files in the static Web system is represented with their space-time properties according to the normal model of the system. Thus, when the normal model of the system is used to detect the normal files of the system, the normal files will be all matched in the self database so that all the normal files can be detected. The other files of the system are all regarded as the non-self. Therefore, no one normal file is detected as a non-self, and no one abnormal file is detected as a normal file. All in all, 100% self of the system is detected and 100% non-self is also detected.

$$P(D_s) = \frac{n_s}{s_s} = \frac{\sum_{i=1}^{n+m} N(s(c_i))}{s_s} = \frac{s_s}{s_s} = 1, \tag{3}$$

$$P(D_n) = \frac{n_n}{s_n} = \frac{k + l - s_s}{s_n} = \frac{s_n}{s_n} = 1. \tag{4}$$

Here, c_i represents a component of the system; $N(x)$ represents the normal function of the variant x and its value is 1 when the variant x is normal; $s(o)$ represents the state function of the object o; k represents the sum of files in the current system; l represents the sum of the directories in the current system.

Hence, the probability of detecting the selfs and the probability of detecting the non-selfs are 100%.

After the antigen was determined as a non-self, pattern recognition of the non-self was started in two ways. One was matching the features of the non-self, and the other was learning the non-self. The former was useful at recognizing known worms through querying in the non-self database, where the features of all known worms were stored. The latter was useful at learning unknown worms with neural networks such as the BP neural network. If the worm was known for the artificial immune system and its features matched a record in the non-self database, the destroyer was called to eliminate the worm. For example, the deletion command of operating systems was a kind of destroyer. Otherwise, for the unknown worm, neural network or learning mechanism from examples was used to learn the worm.

B. Model for Learning Unknown Worms

The model for learning unknown worms is comprised of the feature space of known worms, the algorithm for reading the features of non-selfs, the algorithm for searching the most similar non-self, the unknown worm that is being recognized, and the result set of learning. Let C be a set of q-dimensional vector features vectors c_j, which represents a type of worms. Define $c_j = (u_{j1}, u_{j2}, \cdots, u_{jq})$, where u_{ji} is the ith feature of worm c_j. Assuming that there are M known words, we have

$C = \{c_j\}, j = 1,2,...,M$. For example, o-dimension features of the unknown worm c_u are measured, and the known features are represented with $(u_{ji_1}, u_{ji_2}, \cdots, u_{ji_o})$, but the other features $(u_{jl_1}, u_{jl_2}, \cdots, u_{jl_{q-o}})$ are unknown. Suppose the most similar known worm to the unknown worm c_u is c_k, the algorithm for searching the most similar worm is denoted with A_s, then the process for learning the unknown worm can be represented as such.

$$c_k = A_s((u_{ji_1}, u_{ji_2}, \cdots, u_{ji_o})), \quad (5)$$

$$u_{jl_h} = u_{kl_h}, h = 1,2,\cdots, q-o \text{。} \quad (6)$$

During the process for learning the unknown worm, the non-self is classified into the type of the most similar known worm to the unknown one, according to the feature vector of the unknown worm. The types of known worms are known and the amount of the known worms is limited. However, the unknown worm can not be classified into any type of known worms, and a new type must be created for the unknown one at that time. With creation of new type repeated, the types of unknown worms may be unlimited but numerable, as shown in Fig. 2. The dimension coordinate of the feature space for the worms is represented with $u_i, i = 1,2,\cdots, q$, small balls are used to denote the non-selfs, and the big circles represent the type of the worms. For the problem for learning unknown worms with unlimited type, current approaches of machine learning are not quite suitable, so that the type of unknown worms is regarded as a limited variable.

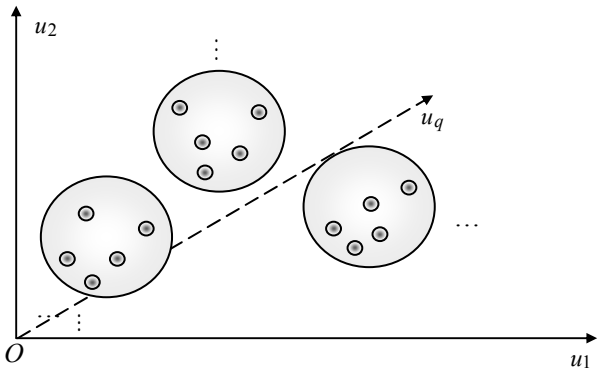

Fig. 2. Feature space of worms with unlimited type expending.

III. Random Searching Algorithm with Immunity and Evolutionary Computation

Suppose the current system that the artificial immune system protects has k components, among which the algorithm for recognizing known worms has regarded k_2 components as unknown non-selfs. There is some feature information for K known worms in the storage of worms, and each worm has q features that are coded in some tables. The problem for recognizing the unknown worms can be solved by finding the most similar known worm to unknown worm and/or creating a new type for the unknown worm, and the problem for finding the most similar known worm to the unknown worm is a constrained optimization problem. Suppose the difference between the unknown worm and a known worm is represented with $f(c_u, c_i) = |c_u - c_i|$, the constrained optimization problem is described as such [31].

$$\text{minimize} \quad f(c_u, c_i) \quad c_u = (u_{u1}, x_{u2}, \cdots, x_{uq}) \in \Re^q \quad (7)$$

$$c_i = (u_{i1}, x_{i2}, \cdots, x_{iq}) \in \Re^q$$

$$\text{subject to:} \quad f(c_u, c_i) < r$$

Here, r represents the threshold that is used to detemine if the unknown worm belongs to any type of known worms.

The constrained optimization problem for finding the most similar known worm to the unknown worm can be solved with some evolutionary algorithms, and the algorithm for recognizing the unknown worms is designed with immune memory, shown in Fig. 3.

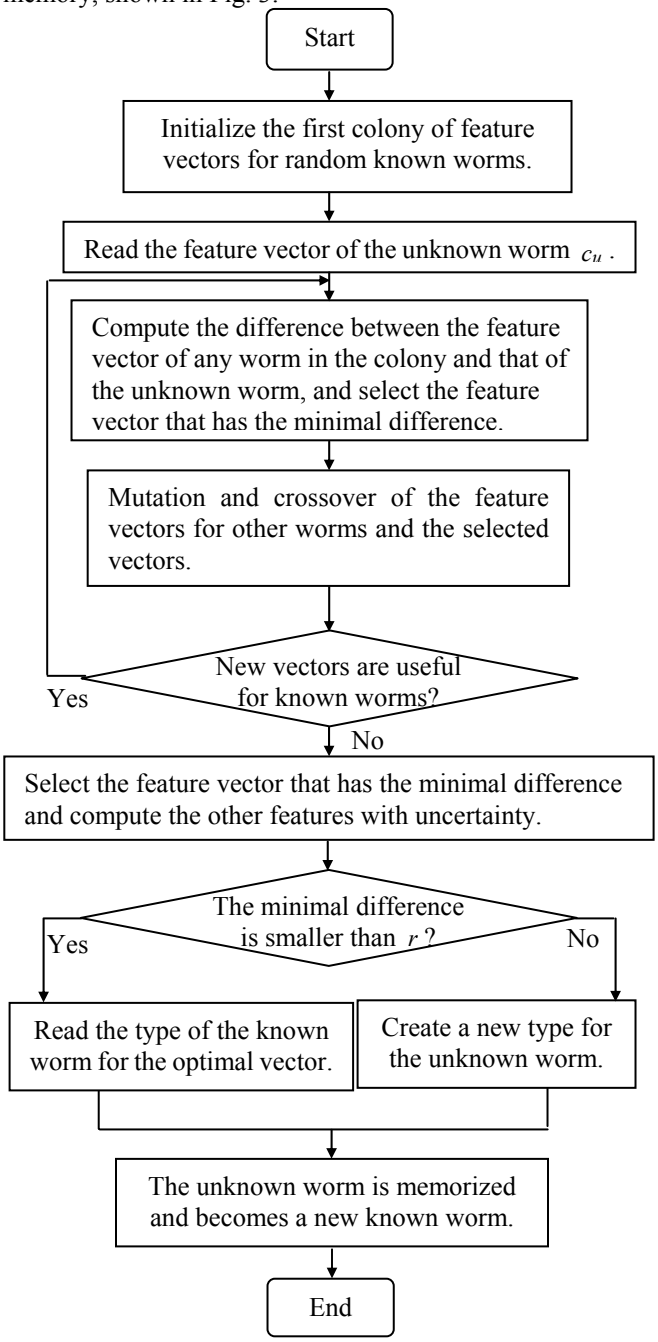

Fig. 3. Algorithm for recognizing the unknown worms with evolutionary computation and immune memory.

The immune memory means that the unknown worm can be transformed into a known one after learning, and the immune learning is enhanced. Before the algorithm for recognizing the unknown worms is used, the unknown worms must be detected. The algorithm for detecting selfs and non-selfs on the normal model is used to detect whether the object is a self or non-self, and the algorithm for recognizing the known worms is used to determine whether the non-self is a known worm or unknown worm. For recognizing more unknown worms, the stage for detecting selfs and non-selfs is very crucial and the stage for recognizing known worms is relatively simple.

With the space properties and the time properties of the components, the normal model uniquely identifies the normal state of each component and the normal state of the whole system that the artificial immune system protects. Therefore, the following two theorems show the advantages of the normal model to the algorithm for recognizing the unknown worms.

Theorem 1 On the condition that the time properties are correct, based on the normal model and the tri-tier immune model of the artificial immune system, the probability for detecting selfs is 100% and the probability for detecting non-selfs is also 100%.

[Proof] The normal states of the components in the system that the artificial immune system protects are represented with their space-time properties according to the normal model of the system. Thus, when the normal model of the system is used to detect the normal files of the system, the normal components will be all matched in the storage of the selfs so that all the normal components can be detected. The other objects in the system are all regarded as the non-selfs. Therefore, no normal component is detected as a non-self, and no abnormal object is regarded as a normal component. All in all, 100% selfs of the system is detected and 100% non-self is also detected.

$$P(D_s)=\frac{n_s}{s_s}=\frac{\sum_{i=1}^{n+m}N(s(c_i))}{s_s}=\frac{s_s}{s_s}=1, \tag{8}$$

$$P(D_n)=\frac{n_n}{s_n}=\frac{k+l-s_s}{s_n}=\frac{s_n}{s_n}=1. \tag{9}$$

Here, D_s represents the event that the selfs are detected, D_n represents the event that the non-selfs are detected, n_s represents the amount of the selfs that have been detected, D_n represents the event that the non-selfs are detected, n_n represents the amount of the non-selfs that have been detected, s_s represents the amount of the selfs in the current system that the artificial immune system protects, s_n represents the amount of the non-selfs in the current system that the artificial immune system protects, $s(c_i)$ represents the state of the component c_i, $N(\cdot)$ represents the normal function and the function value 1 means that the system is normal, while the function value 0 means that the system is abnormal.

Hence, the probability for detecting the selfs and the probability for detecting the non-selfs are both 100%. ■

Theorem 2 Suppose the event that the artificial immune system detects the non-selfs by matching the features of the non-selfs is denoted with D_T, the event that the artificial immune system detects the non-selfs is denoted with D_N, the probability for recognizing the unknown worms based on the normal model is represented with $P(R|D_N)$, the probability for recognizing the unknown worms only based on matching the features of the non-selfs is represented with $P(R|D_T)$, then $P(R|D_N)>P(R|D_T)$.

[Proof] The artificial immune system recognizes the unknown worms after the system detects the unknown worms as unknown non-selfs. Thus, the probability for recognizing the unknown worms is a conditional probability $P(R|D)$, which is the probability of the event that unknown worms are recognized on the condition that the worms are detected.
$\because P(D_N)=1$, $P(D_T)<1$, $\therefore P(D_N)>P(D_T)$.
$\therefore P(R|D_N)=P(R)>P(R|D_T)$. ■

IV. Experiments

To test the approach for learning unknown worms with evolutionary computation and immune memory, a web demo system is immunized and infected by some unknown worms. The unknown worms mean that the worms can not be matched in the storage of worms for the artificial immune system, and there are three variants of known worms and two complete-unknown worms among the unknown worms. The three variants are respectively modified from the loveletter worm, the happy-time worm and the Jessica worm [32-34].

The selfs of the web demo system are represented with the normal model, and the normal model is uniquely identified by the space-time properties of the components when the initial system is normal, shown in Fig. 4.

The system is a part of web-based e-learning system, which is developed by some web programming languages such as HTML JSP, Java and JDBC. The system is used to show how a fire-fighting robot searches a path to find the fire and put out the fire, and the initial system is normal. Therefore, at the initial normal state the normal model of the system is built and used to represent the selfs.

The immune memory is a kind of rote learning, and the memory part can be regarded as a function $m(\cdot)$ in mathematics. The input vector of the memory function is $(u_{ji_1},u_{ji_2},\cdots,u_{ji_o})$, and the output vector of the memory function is the combination of unknown features and unknown type of the unknown worm, as denoted with $(u_{jl_1},u_{jl_2},\cdots,u_{jl_{q-o}},T)$. The immune memory can be searched directly and easily, and no repeated immune computation is needed for learning unknown features and type, when the memory function $m(u_{ji_1},u_{ji_2},\cdots,u_{ji_o})$ is called [35].

$$\begin{aligned}&(u_{ji_1},u_{ji_2},\cdots,u_{ji_o})\xrightarrow{m}(u_{jl_1},u_{jl_2},\cdots,u_{jl_{q-o}},T)\\&\xrightarrow{\text{storing}}((u_{ji_1},u_{ji_2},\cdots,u_{ji_o}),(u_{jl_1},u_{jl_2},\cdots,u_{jl_{q-o}},T))\end{aligned} \tag{10}$$

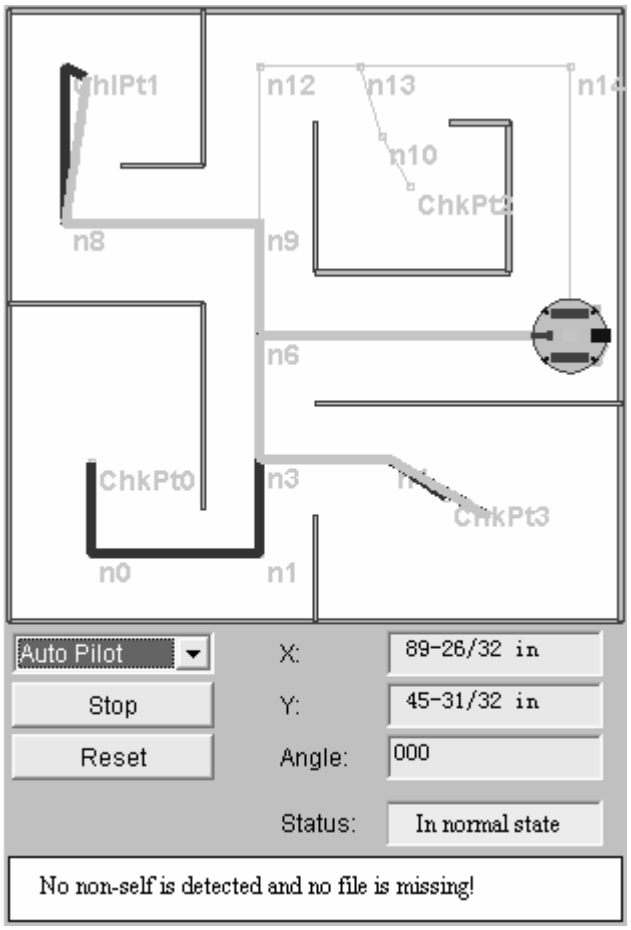

Fig. 4. Initial web demo system when the system is normal.

In this example, the three variants v_1, v_2, v_3 are recognized to belong to three classes of the loveletter worms, the happy-time worms, and the Jessica worms respectively, and the three classes are known, shown as the real-line circle in Fig. 5. The other unknown worms w_1, w_2 are recognized as two brand-new unknown worms, and two new classes are created for them, shown as the dashed circle in Fig. 5.

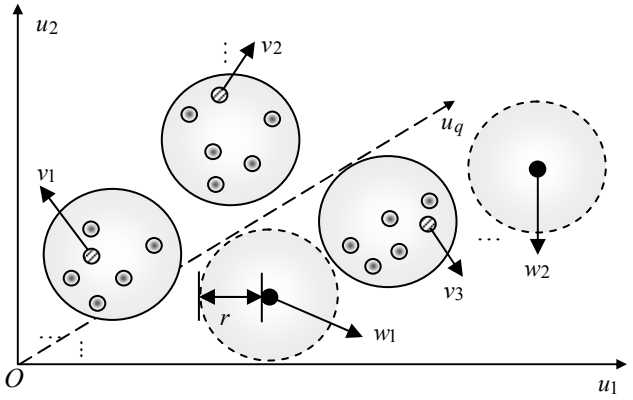

Fig. 5. Learning results of the unknown worms in the feature space.

The web demo system is immunized by the artificial immune system and is now immune from some worms. When many known worms and the unknown worms attack the demo system that the artificial immune system protects, the innate immune tier is activated to detect the worms and recognized the known worms. Detection of all the worms and recognition of the unknown worms are both quick because of the normal model and the storage of known worms, shown as the curve from the time point 0 to t_2 in Fig. 6. After the innate immune tier confirms that the unknown worms are not any known worms, the adaptive immune tier begins to learn the unknown worms with random evolutionary search, shown as the curve from the time point t_2 to t_3 in Fig. 6, and the most similar known worm is found to decide whether the unknown worms belong to any type of known worms or are really new type of worms. The learning results are memorized so that the unknown worms are transformed into new known worms in the end. If another variant of the loveletter worm attacks the demo system, the artificial immune system recognizes the variant as a known worm now and the immune response is quick from the time point t_4 to t_5 in Fig. 6. Here, m_{wd} represents the sum of the worms that have been processed, and t represents the time coordinate.

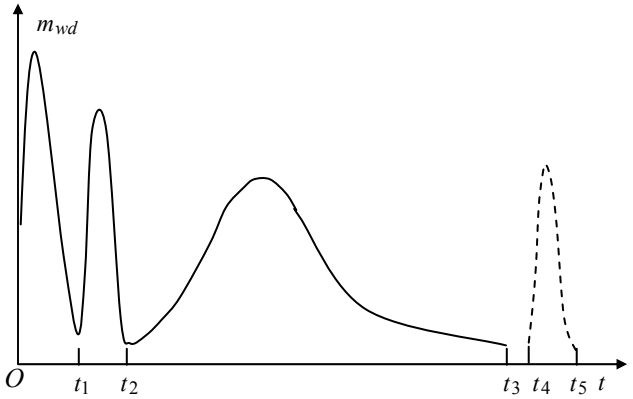

Fig. 6. Immune response to the known worms and the unknown worms.

In Fig. 6, the primary immune response includes the self/non-self detection and recognition of the known worms, and the detection is accomplished from the time point 0 to t_1. The secondary immune response is from the time point t_2 to t_3, which is much longer than the primary immune response. In fact, the hypothetic immune response from the time point t_4 to t_5 is a part of the primary immune response after the secondary immune response.

The experiments are made on the web-based course system, and the web demo system is a part. Over a hundred of worms attack the web system, and many files are infected. The artificial immune system detects all the worms successfully with the normal model and the approach for detecting selfs and non-selfs. But only with some intelligent techniques such as the artificial neural network, the probability for detecting the non-selfs is smaller, and such result affects the process of recognizing the worms. With the immune learning algorithm after detecting the worms with the normal model, the artificial immune system recognizes the unknown worms with the higher probability than the result with the artificial neural network with the BP algorithm.

The immunization simulation was developed and visualized with Java to test the immune model with the static network system and worms in 1200 experiments. Some

non-self files are recognized as the infected files of happy-time worms, which are unknown for the anti-worm immune static Web system; 90 non-self files are recognized as the infected files of love worms, which are known for the artificial immune system, according to the string features of 'loveletter' and '.copy' etc. After the worm recognition, the infected files are eliminated immediately through the deletion command of the operation system.

V. CONCLUSIONS

Adaptive immunity is very important for the biological immune system, and the adaptive immune tier is also very crucial for the artificial immune system. The approach for learning many unknown worms with evolutionary computation and immune memory is a useful and effective new technique, and the normal model is useful for increase the probability for recognizing the unknown worms.

The web system is a good test-bed for investigating the anti-worm problem with the artificial immune system, and the adaptive immune approach is helpful for establishing an active defending system to keep the web system safe, normal and robust. In the future, more intelligent techniques should be used for improving the artificial immune system.

REFERENCES

[1] L. N. de Castro, J. Timmis, *Artificial Immune Systems: A New Computational Intelligence Approach*. London: Springer-Verlag, 2002.

[2] N. K. Jerne, "Towards a network theory of the immune system," *Ann. Immunol.*, 1974, 125C, pp. 373–389.

[3] L. N. de Castro, F. J. von Zuben, "Learning and optimization using the clonal selection principle," *IEEE Trans. on Evolutionary Computation*, 2002, vol. 6, no. 3, pp. 306–313.

[4] H. Bersini, F. Varela, "Hints for adaptive problem solving gleaned from immune network," *Parallel Problem Solving from Nature*. Heidelberg: Springer-Verlag, 1991, pp. 343–354.

[5] A. Perelson, R. Hightower, S. Forrest, "Evolution (and learning) of v-region genes," *Research in Immunol.*, 1996, vol. 147, pp. 202–208.

[6] T. Gong, "Research on Modeling and Robustness Analysis of Immune Computation," *Ph.D. Thesis.*, Central South University, 2007.

[7] H. D. Kim, J. J. Jin, J. A. Maxwell, et al., "Enhancing Th2 immune responses against amyloid protein by a DNA prime-adenovirus boost regimen for Alzheimer's disease", *Immunology Letters*, 2007, vol. 112, no. 1, pp. 30–38.

[8] L. W. Collison, C. J. Workman, T. T. Kuo, et. al., "The inhibitory cytokine IL-35 contributes to regulatory T-cell function," *Nature*, 2007, vol. 450, no. 7169, pp. 566–9.

[9] L. J. Guo, X. J. Zhang, B. Zheng, et al., "IgM-mediated signaling is required for the development of a normal B cell memory response," *Mol Immunol*, 2008, vol. 45, no. 4, pp. 1071–7.

[10] P. Ghia, C. Scielzo, M. Frenquelli, et al., "From normal to clonal B cells: Chronic lymphocytic leukemia (CLL) at the crossroad between neoplasia and autoimmunity," *Autoimmun. Rev.*, 2007, vol. 7, no. 2, pp. 127–31.

[11] Z. Q. Yan, G. K. Hansson, "Innate immunity, macrophage activation, and atherosclerosis," *Immunological Reviews*, 2007, vol. 219, pp. 187–203.

[12] A. Perelson, R. Hightower, S. Forrest, "Evolution (and learning) of v-region genes," *Research in Immunology*, 1996, vol. 147, pp.202–208.

[13] M. A. Nowak, C. R. Bangham, "Population dynamics of immune responses to persistent viruses," *Science*, 1996, vol. 272, no. 5258, pp. 74–79.

[14] D. D. Ho, A. U. Neumann, A. S. Perelson, et al., "Rapid turnover of plasma virions and CD4 lymphocytes in HIV-1 infection," *Nature*, 1995, vol. 373, no. 6510, pp. 123–126.

[15] B. F. Dibrov, M. A. Livshits, M. V. Volkenstein, "Mathematical model of immune processes," *J. Theor. Biol.*, 1977, vol. 65, no. 4, pp.609–631.

[16] G. I. Bell, "Mathematical model of clonal selection and antibody production," *J. Theor. Biol.*, 1970, vol. 29, no. 2, pp. 191–232.

[17] J. Balthrop, S. Forrest, M. E. J. Newman, et al., "Technological Networks and the Spread of Computer Viruses," *Science*, 2004, vol. 304, no. 5670, pp. 527–529.

[18] S. Sarafijanovic, J. Y. Le Boudec, "An artificial immune system approach with secondary response for misbehavior detection in mobile ad hoc networks," *IEEE Trans. Neural Networks*, 2005, vol. 16, no. 5, pp. 1076–1087.

[19] H. Orman, "The Morris Worm: A Fifteen-Year Perspective," IEEE SECURITY & PRIVACY, 2003, 1(5): 35-43.

[20] S. Staniford, V. Paxson, N. Weaver, "How to Own the Internet in Your Spare Time," Boneh D. (ed.), Proceedings of the 11th USENIX Security Symposium, Berkeley: USENIX, 2002. 149-167.

[21] J. Balthrop, S. Forrest, M. E. J. Newman, et al, "Technological Networks and the Spread of Computer Viruses," Science, 2004, 304(5670): 527- 529.

[22] E. Levy, "Worm Propagation and Generic Attacks," IEEE Security and Privacy, 2005, 3(2): 63-65.

[23] R. S. Gray, V. H. Berk, "Rapid Detection of Worms Using ICMP-T3 Analysis," Carapezza E M. (ed.), Proceedings of SPIE, Bellingham: SPIE Press, 2004, 89-101.

[24] D. Dasgupta, F. González, "An immunity-based technique to characterize intrusions in computer networks," IEEE Transactions on Evolutionary Computation, 2002, 6(3): 281-291.

[25] Chang-chun Zou, Wei-bo Gong, D. Towsley, "Code Red Worm Propagation Modeling and Analysis," Atluri V. Proceedings of the 9th ACM Conference on Computer and Communications Security, New York: ACM Press, 2002, 138-147.

[26] B. Madhusudan, J. W. Lockwood, "A hardware- accelerated system for real-time worm detection," IEEE Micro, 2005, 25(1): 60-69.

[27] R. Medzhitov, C. A. Jr.Janeway, "Decoding the Patterns of Self and Nonself by the Innate Immune System," *Science*, 2002, vol. 12, no. 296, pp. 298–300.

[28] T. Gong, Z. X. Cai, "Tri-tier Immune System in Anti-virus and Software Fault Diagnosis of Mobile Immune Robot Based on Normal Model," Journal of Intelligent and Robotic Systems, 2008, 51(2): 187–201.

[29] T. Gong, Z. X. Cai, "An Immune Agent for Web-based AI Course," *International Journal on E-Learning*, 2006, vol. 5, no. 4, pp. 493–506.

[30] T. Gong, Z. X. Cai, Natural Computation Architecture of Immune Control Based on Normal Model, *Proceedings of the 2006 IEEE International Symposium on Intelligent Control*, Munich, 2006, pp. 1231–1236.

[31] E. Levy, "Worm Propagation and Generic Attacks," *IEEE Security and Privacy*, 2005, vol. 3, no. 2, pp. 63–65.

[32] I. Arce, E. Levy, "An analysis of the Slapper worm," *IEEE SECURITY & PRIVACY*, 2003, vol. 1, no. 1, pp. 82–87.

[33] C. C. Zou, W. Gong, D..Towsley, "Code Red Worm Propagation Modeling and Analysis," In: Atluri V. eds. *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ACM Press, New York, 2002, pp. 138–147.

[34] S. Tsutsui, M. Yamamure, T. Higuchi, "Multi-parent recombination with simplex crossover in real coded genetic algorithms," in *Proc. Genetic and Evol. Comput. Conf.*, 1999, pp. 657–664.

[35] Z. X. Cai, G. Y. Xu, *Artificial Intelligence: Principles and Applications*, Beijing: Tsinghua University Press, 2004.