Neurocomputing 148 (2015) 158–166

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

Immune cooperation mechanism based learning framework

Pengtao Zhang, Ying Tan*

Key Laboratory of Machine Perception (MOE), Peking University, Department of Machine Intelligence, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China

ARTICLE INFO

Article history:
Received 7 April 2012
Received in revised form
25 July 2012
Accepted 31 August 2012
Available online 31 July 2014

Keywords:
Immune cooperation mechanism
Learning framework
Feature extraction
Malware detection
Artificial immune system

ABSTRACT

Inspired from the immune cooperation (IC) mechanism in biological immune system (BIS), this paper proposes an IC mechanism based learning (ICL) framework. In this framework, a sample is expressed as an antigen-specific feature vector and an antigen-nonspecific feature vector at first, respectively, simulating the antigenic determinant and danger features in the BIS. The antigen-specific and antigen-nonspecific classifiers score the two vectors and export real-valued Signal 1 and Signal 2, respectively. With the cooperation of the two signals, the sample is classified by the cooperation classifier, which resolves the signal conflict problem at the same time. The ICL framework simulates the BIS in the view of immune signals and takes full advantage of the cooperation effect of the immune signals, which improves the performance of the ICL framework. It does not involve the concept of the danger zone and further suggests that the danger zone is considered to be unnecessary in an artificial immune system (AIS). Comprehensive experimental results demonstrate that the ICL framework is an effective learning framework. The ICL framework based malware detection model outperforms the global concentration based malware detection approach and the local concentration based malware detection approach for about 3.28% and 2.24% with twice faster speed, respectively.

1. Introduction

With the development of the biological immunology, more and more immune mechanisms become clear. One of the most important achievements is the danger theory (DT) which overcomes the drawback of the traditional self–nonself (SNS) model in defining the harmfulness of self and nonself [1,2]. The DT believes that the immune system reacts to danger instead of nonself, and the internal conversation between the tissues and the cells in the immune system controls immunity. It explains the autoimmunity problem perfectly and has been one of the most important immune theories.

Many immune based artificial immune systems (AIS) have been proposed and applied to the field of computer security in the past few years. Forrest et al. applied the immune theory to computer abnormality detection for the first time in 1994. They proposed a negative selection algorithm on the basis of the SNS model to detect the abnormal modification of protected data [3], and later to monitor UNIX processes [4]. In the last decade, lots of the DT based learning approaches were proposed with some success, most of which involved a danger zone. The danger zone defines the spread range of a danger signal and the way of different signals to interact with each other. It has been one of the most important components in the DT based artificial immune systems.

According to the study of the adaptive immune system, a danger signal is considered to spread in the global space of the immune system rather than a local zone in this paper. Although an immune signal could spread only among adjacent cells physically, the cells are able to move in the immune system. This mechanism breaks the assumption of a danger zone which limits the spread range of a danger signal in a local zone. Hence this paper suggests that the danger zone is considered to be unnecessary in AIS.

The immune cooperation (IC) mechanism in the biological immune system (BIS) is crucial for producing an effective immune response to an antigen precisely and avoiding the autoimmunity. Introducing this mechanism into AIS is considered to be helpful for improving the performance of AIS. Taking inspiration from the IC mechanism and simulating BIS in the view of immune signals provide new ideas for constructing better AIS. Now how to introduce the IC mechanism into AIS and make full advantage of the cooperation effect of the immune signals become valuable works.

Malware is a general term for all the malicious codes that is a program designed to harm or secretly access a computer system without the owners' informed consent, such as computer virus,

* Corresponding author. Tel./fax: +86 10 62767611.
E-mail addresses: pengtaozhang@gmail.com (P. Zhang), ytan@pku.edu.cn (Y. Tan).

http://dx.doi.org/10.1016/j.neucom.2012.08.076
0925-2312/© 2014 Elsevier B.V. All rights reserved.

Trojan and worm. It has been one of the most terrible threats to the security of the computers worldwide [5]. How to detect malware efficiently is one of the hottest research points.

A variety of malware detection approaches have been proposed so far, which can be classified into two categories: static techniques and dynamic techniques. As the static techniques usually work on the binary string or application programming interface (API) calls of a program without running the program, they are portable and can be deployed on personal computers. The dynamic techniques keep watch over the execution of every program during run-time and stop the program once it tries to harm the system. The dynamic techniques bring too much extra loads and significantly degrade the performance of the computer system, so they are usually used to analyze malware in companies instead of detecting malware in personal computers.

Inspired from the BIS, an IC mechanism based learning (ICL) framework is proposed in this paper. This framework expresses a sample as an antigen-specific feature vector and an antigen-nonspecific feature vector at first, respectively, simulating the antigenic determinant and danger features in the BIS. The antigen-specific and antigen-nonspecific classifiers score the two vectors and export real-valued Signal 1 and Signal 2, respectively, corresponding to the signals in the BIS. With the cooperation of the two signals, the sample is classified by the cooperation classifier, which resolves the signal conflict problem at the same time. In order to incorporate the ICL framework into the whole procedure of malware detection, an ICL framework based malware detection (ICL-MD) model is further proposed in this paper.

The ICL framework simulates the BIS in the view of immune signals. And it introduces the IC mechanism into the AIS successfully and makes full use of the cooperation effect of the immune signals. What is more, it does not involve the concept of the danger zone and further suggests that the danger zone is considered to be unnecessary in the AIS. Experimental results suggest that the ICL framework is an effective learning framework.

The remainder of this paper is organized as follows. In Section 2, the related works are introduced. Section 2 describes the proposed ICL framework in detail. In Section 4, the ICL-MD model is presented. Section 5 gives the detailed experimental setup and results. Finally, we conclude the paper with some discussions.

2. Related work

The SNS model has been accepted to describe how the immune system works for over 50 years. Although it fails to explain a plenty of new findings, the SNS model based AIS were still applied to a wide range of fields successfully.

Li proposed an immune based dynamic detection model for computer viruses [6]. Through dynamic evolution of ‘self’, an antibody gene library and detectors, this model reduces the size of the ‘self’ set, raises the generating efficiency of detectors, and resolves the problem of detector training time being exponential with respect to the size of ‘self’.

A malware detection model based on a negative selection algorithm with penalty factor (NSAPF) was proposed [7]. The NSAPF punishes the features of nonself which match the features of self instead of deleting them directly. It tries to overcome the drawback of the SNS model in defining the harmfulness of self and nonself by retaining all the nonself features in this way. Later they further proposed a danger feature based negative selection algorithm which divides the danger feature space into four parts and reserves all the self and nonself danger features [8]. Both the two models gave good results.

Tan et al. proposed a global concentration (GC) based feature construction (CFC) approach for spam detection by taking inspiration from the human immune system [9,10]. The GC is defined as a two-element concentration vector, consisting of ‘self’ concentration and ‘nonself’ concentration. The experimental results suggested that the GC was effective to characterize a sample. The GC was latter applied to detect malware [11] and achieved good results.

A feature named the local concentration (LC) was proposed based on the GC which was considered to be able to extract position-correlated information from a sample and brought down the dilute risk of the GC to a certain extent [12,13]. The LC based feature extraction (LCFE) approach works on the local areas in a sample to collect the detailed local information of the sample. Experimental results suggested that it outperformed the GC based approaches. The LCFE approach for malware detection is imported in for comparison.

The DT believes that the immune system is more concerned with danger than nonself [2]. It explains a lot of new findings successfully, therefore many researchers have tried to introduce this new theory into AIS which has developed into a new branch of AIS [14].

Aickelin et al. proposed the concept of the danger zone to translate the DT into the field of computer security for the first time [15,16]. From then on, many DT based AIS have been proposed [17].

A DT inspired artificial immune algorithm for online supervised two-class classification problem was proposed [18]. The size of the danger zone in this algorithm is decreased with the increase of the accumulated intensity of the antibody. The better antibodies would proliferate and live longer by using the clonal selection algorithm, while a suppression mechanism is utilized to control the antibody population. Experimental results suggested that this algorithm performed well with good generalization capability.

Zhu and Tan proposed a DT based learning model for combining classifier and applied it to detect spam [19]. There are three components in this model: binary-valued Signal 1, Signal 2 and danger zone. If the Signal 1 and Signal 2 make the same classification for a sample, the sample is classified directly. Otherwise, a self-trigger process has to be done to solve the signal conflict problem. The classifiers used to emit immune signals are supposed to be conditionally independent, in order to get different trained classifiers from the same data source.

An agent-based intrusion detection system (ABIDS) inspired by the DT was proposed [20], where agents coordinate one another to calculate mature context antigen value and update activation threshold for security responses. The ABIDS works on the dual detection of dendritic cell agents for signals and T-cell agents for antigens. It combines advantages from the dendritic cell algorithm, multi-agent systems and AIS to provide a better intrusion detection mechanism for unknown host behaviors.

Kolter and Maloof proposed a method to detect malware based on the relevant N-Grams selected by the IG [21], and achieved good results. They clearly identified that using the techniques from machine learning and data mining to detect malware is feasible. Later they extended this method to classify malware based on the function of their payload [22]. This method is in fact the method M_2 involved in the proposed ICL-MD model which will be introduced in Section 4.

3. Immune cooperation mechanism based learning framework

3.1. Immune cooperation mechanism

The adaptive immune system is one of the most important parts of BIS. It allows for a stronger immune response as well as immunological memory [23]. There are two kinds of immunities in the adaptive immune system, humoral immunity and cellular immunity. The humoral immunity is mediated by antibodies secreted in the B lymphocytes (B cell), which can be found in the body fluids, while the cellular immunity is the immunity mediated by cells, involving the macrophages, natural killer cells, T lymphocytes (T cell), and cytokines [24].

In the adaptive immune system, the cooperation mechanism between the first signal (Signal 1) and the second signal (known as co-stimulation signal, referred to as Signal 2 in this paper), which are antigen specific and nonspecific respectively, is usually crucial for BIS to produce an effective immune response to an antigen. This mechanism is called the immune cooperation (IC) mechanism in this paper. From the perspective of the IC mechanism, there are not remarkable differences between the humoral immunity and the cellular immunity in the procedure of antigen recognition. Hence this paper illustrates the IC mechanism by using the humoral immunity.

The danger model is shown in Fig. 1, which illustrates an immune response in the humoral immunity [2]. Firstly, the naive B cell recognizes the antigenic determinant of an antigen, which is able to identify a specific kind of antigen, by using the antibody molecule in its surface and sends Signal 1 to activate these kinds of B cells. At the same time, the normal cells intruded by the antigens die abnormally and release the intracellular products, which are believed to be danger features. These danger features are considered to be able to send a danger signal, which is antigen nonspecific, to their neighboring antigen present cells (APCs). After receiving the danger signal, the APCs move into immune tissues and transform it to corresponding helper T cells (Th, for short), CD4+ Th1 in this case, as the co-stimulation signal, referred to as Signal 2. Then the helper T cells release various kinds of cytokines, which act as Signal 2, to activate the corresponding B cells. Finally, under the cooperation of the two signals, the B cell is fully activated and secretes antibodies to produce an effective immune response.

It is easy to see that there are two signals acting on the lymphocytes, B cell and T cell, in an effective immune response: antigen-specific Signal 1 provided by the antibody molecular of B cell or T cell receptor, and antigen-nonspecific Signal 2 which is able to stimulate the antigen-specific lymphocytes to proliferate and differentiate. Since both the signals are considered to own two states, presence or absence, in an immune response, the two signals are regarded as binary-valued signals. A lymphocyte could be fully activated if and only if the two signals cooperate with each other and work on it. Although there are many differences between the danger signal and Signal 2, taking different senders and receivers as an example, Signal 2 is considered to come from the danger signal and could be regarded as a danger signal in another form. Hence this paper merges the danger signal into Signal 2. The IC mechanism drops down the probability of the autoimmunity in BIS, and helps us to recognize and clear antigens more precisely. It is one of the most important mechanisms to keep BIS working stably and effectively.

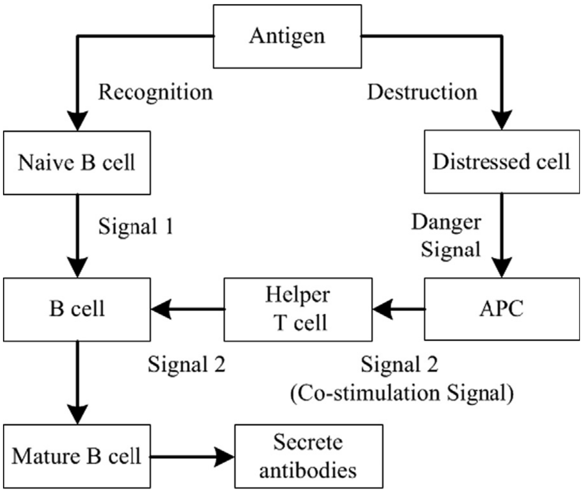

Fig. 1. The danger model.

Many researches have shown that Signal 2 plays an important role in an adaptive immune response [25–28]. It is necessary for the proliferation, differentiation and survival of the lymphocytes. It is also able to increase the immunological effect dramatically in an adaptive immune response.

It is important to note that the APCs send Signal 2 to corresponding helper T cells by moving in BIS, rather than its neighboring helper T cells physically. For example, after receiving a danger signal, an APC delivers itself to the lymphatic tissue through lymphatic channels in cellular immunity. In the lymphatic tissue, it transforms the danger signal to corresponding helper T cells in the form of Signal 2. The helper T cells further transform this signal to corresponding effector T cells to activate these T cells.

Many DT based AIS assumed that there is a danger zone in an AIS. It indicates the spread range of a danger signal and defines a specific way for a danger signal to interact with other signals. According to the BIS, this assumption is considered to be unreasonable. As we know, the APC, which is antigen nonspecific and could engulf a wide range of antigens, has lower diversity. It is different from the B cells and T cells, which are antigen specific and own lots of classes. As there are plenty of APCs which could be found everywhere in the BIS, it is reasonable to assume that any danger signal is able to be sent to any kind of APCs. After receiving a danger signal, an APC would load the information of the antigen into its major histocompatibility complex (MHC) molecule and further send this information to corresponding helper T cells in the form of Signal 2. As mentioned above, these helper T cells need not come near the APC physically. The APC could move in the immune system with the information of the antigen and find the appropriate helper T cells. That is to say, although the immune signals only spread among adjacent immune cells, the immune cells with the antigen information are able to move in the immune system. This mechanism breaks the assumption of the danger zone which suggests that the danger signal spreads itself in a local zone. Hence this paper regards the danger signal, referred to as Signal 2, as a global signal. There is no need to define a danger zone in AIS which simplifies the framework of AIS dramatically.

Let us illustrate the above analysis using an example. When the same antigens intrude an immune system from any position, the immune system almost always produces an effective immune response. This phenomenon suggests that there is not a danger zone in the immune system and the danger signal, Signal 2 in this paper, could be regarded to spread in the whole immune system. In an AIS, every APC usually has only one copy, which represents a kind of APC. No matter how far an antigen is from an APC logically, a danger signal activated by the antigen is hoped to be sent to all the APCs.

3.2. ICL framework

Inspired from the IC mechanism in BIS, this paper proposes a novel IC mechanism based learning (ICL, for short) framework. The definitions of the concepts used in the ICL framework are given below:

- *Antigen-specific feature* is the antigen feature that only occurs in antigens, simulating the basic unit of the antigenic determinant of a biological antigen. It is obviously antigen-specific and is able to identify a kind of antigen.

- *Antigen-nonspecific feature*, also called danger feature, is able to measure the danger of a sample and discriminate antigens from non-antigens. As it appears in both antigens and non-antigens, it is antigen-nonspecific, simulating the basic element of the danger features in BIS.

The flowchart of the ICL framework is shown in Fig. 2. Firstly, the ICL framework expresses a sample as an antigen-specific feature vector by using the antigen-specific feature library L_1. This feature vector simulates the antigenic determinant of a biological antigen and is considered to contain the antigen-specific information of the sample. It is taken as the input of the antigen-specific classifier C_1, in which the antigen-specific information contained in the sample is measured. At the same time, the sample is further expressed as an antigen-nonspecific feature vector based on the antigen-nonspecific feature library L_2. This feature vector simulates the danger features in BIS, and is used to measure the danger information of the sample by the antigen-nonspecific classifier C_2.

Secondly, the classifiers C_1 and C_2 score their input features. The scores of the two features are taken as the real-valued Signal 1 and Signal 2 in this paper, corresponding to the binary-valued Signal 1 and Signal 2 in BIS. The two signals here are real numbers in the interval $[0, 1]$. They are taken as the input of the cooperation classifier C_3.

Finally, according to the cooperation information of Signal 1 and Signal 2, the cooperation classifier C_3 classifies a sample into a class. In this phase, the classifier C_3 resolves the classification problem and the immune signal conflict problem at the same time on the basis of the knowledge learned in its training procedure. It increases the efficiency of the ICL framework greatly. Furthermore, the IC mechanism used here helps us to drop down the false positive rate and the false negative rate, and improves the performance of the proposed ICL framework.

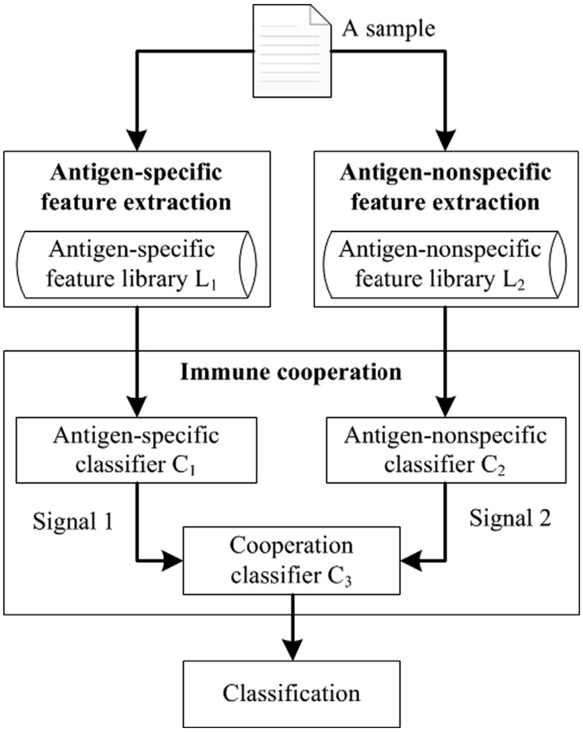
A sample
Antigen-specific feature extraction
Antigen-specific feature library L1
Antigen-nonspecific feature extraction
Antigen-nonspecific feature library L2
Immune cooperation
Antigen-specific classifier C1
Antigen-nonspecific classifier C2
Signal 1
Signal 2
Cooperation classifier C3
Classification

Fig. 2. The flowchart of the ICL framework.

The mathematical model of the proposed ICL framework could be written as

$$f(V_S, V_N) = f_{C_3}(f_{C_1}(V_S), f_{C_2}(V_N)) \tag{1}$$

where V_S and V_N denote the antigen specific and nonspecific feature vectors of a sample, respectively. And f_{C_1}, f_{C_2} and f_{C_3} represent the classifiers C_1, C_2 and C_3, respectively.

Different from the method proposed in [19], there is not uncorrelated requirement for the machine learning classifiers used in the classifiers C_1 and C_2 as their data sources are considered to be independent. That is to say, any machine learning classifier is able to be used in the classifiers C_1 and C_2. Their training feature vectors determine their properties, antigen-specific and antigen-nonspecific.

The proposed ICL framework utilizes the real-valued signals instead of the binary-valued signals in BIS. The real-valued signals are believed to bring many advantages, which are listed below:

- The real-valued signals are able to transform the characterization information of a sample more precisely to the cooperation classifier C_3 without information loss. Base on this property, the real-valued signals have the potential ability to improve the performance of the ICL framework.
- The ICL framework need not set the binary thresholds for the classifiers C_1 and C_2, which brings down the number of parameters in this framework.
- With the help of the real-valued signals, there is no need to resolve the immune signal conflict problem here, which further simplifies the structure of this framework.

The Signal 1 and the Signal 2 in the proposed ICL framework are emitted based on the antigen-specific and antigen-nonspecific feature vectors of a sample by the classifiers C_1 and C_2, respectively. The data sources of the two signals almost exactly correspond to those in BIS. It makes the emission of the signals more natural. Table 1 lists the mapping between the BIS and the ICL framework. Inspired from BIS, the ICL framework simulates the BIS in the view of immune signals reasonably and makes full advantage of the IC mechanism. It is believed to be able to measure the danger of a sample more precisely and make a better classification.

In the ICL framework, Signal 1 and Signal 2 cooperate with each other. The cooperation effect is considered to be able to help the ICL framework express and measure the class information of a sample more accurately and precisely. Actually the two branches in the ICL framework, i.e. the classifiers C_1 and C_2 which emit Signal 1 and Signal 2, could be regarded as two independent learning methods, written as M_1 and M_2 respectively. The mathematical models of M_1 and M_2 are $f(V_S) = f_{C_1}(V_S)$ and $f(V_N) = f_{C_2}(V_N)$. With the cooperation of the immune signals, the ICL framework is expected to outperform both M_1 and M_2, and further exceed the sum of the two methods. The sum of M_1 and M_2 is written as $M_{1\bigcup 2}$ in this paper, the mathematical model of which is $f(V_S, V_N) = f_{C_1}(V_S) \bigcup f_{C_2}(V_N)$.

Table 1
The mapping between the BIS and the ICL framework.

BIS	ICL framework
Antigenic determinant	Antigen-specific feature vector
Danger feature	Antigen-nonspecific feature vector
Binary-valued Signal 1	Real-valued Signal 1
Binary-valued Signal 2	Real-valued Signal 2
B cell, T cell	Antigen-specific classifier C_1
APC, helper T cell	Antigen-nonspecific classifier C_2
B cell, T cell	Cooperation classifier C_3

In this paper, $F(M_i)$ is used to denote the performance of the method M_i, where $i = 1, 2, 1\bigcup 2, 3$. In particular, $F(M_3)$ indicates the performance of the ICL framework. According to the IC mechanism, we hope

$$F(M_3) > F(M_{1\bigcup 2}) \tag{2}$$

$$F(M_{1\bigcup 2}) > = F(M_1) \tag{3}$$

$$F(M_{1\bigcup 2}) > = F(M_2) \tag{4}$$

The area under the receiver operating characteristic (ROC) curve (AUC), which is widely used to evaluate the classification performance in the field of machine learning, is utilized as the performance evaluation criteria in this paper. Let $f_i(x)$ denote the ROC curve of the method M_i, where x is the false positive rate and $f_i(x)$ is the true positive rate, then

$$F(M_i) = \int_0^1 f_i(x)\, dx \tag{5}$$

We define

$$F(M_{1\bigcup 2}) = \int_0^1 \max\{f_1(x), f_2(x)\}\, dx \tag{6}$$

From the above definition of the $F(M_{1\bigcup 2})$, it is easy to see that Formula (3) and Formula (4) are always true. We will verify Formula (2) in the experiments, thereby proving that the IC mechanism helps us to improve the performance of the ICL framework.

4. ICL framework based malware detection model

In order to incorporate the ICL framework into the procedure of malware detection, a novel ICL framework based malware detection (ICL-MD) model is proposed in this paper. This model involves two modules, feature extraction and classification. In the malware detection problem, malware are taken as antigens, while benign programs are non-antigens.

In the ICL-MD model, the 4-Grams are taken as the candidate features which are binary strings of length 4 bytes. N-Gram is a concept from text categorization, which indicates N continuous words or phrases. Kolter and Maloof took 4-Grams as candidate features in their previous works [21,22]. They believed that the 4-Gram is able to capture not only binary strings of length 4 bytes, but also longer strings.

The way to extract the feature libraries L_1 and L_2 is introduced below. Firstly, the ICL-MD model collects the statistical information of the 4-Grams by traversing the training set. It is the data basis to evaluate the goodness of a 4-Gram. Secondly, the goodness of every 4-Gram is measured by using a feature goodness criteria. The information gain (IG) is taken as the feature goodness criteria in this paper. Other feature goodness criteria such as document frequency, mutual information, χ^2 statistic and term strength [29] could also be used. Then all the 4-Grams are sorted in the descending order based on their IG values. Finally, the ICL-MD model traverses the ordered 4-Grams orderly. If a feature f only occurs in malware, it is considered to be antigen-specific and added to L_1. Otherwise, we regard it as an antigen-nonspecific feature and add it to L_2. Iterate this process until there are N_1 features in the L_1 and N_2 features in L_2. Until now, the two feature libraries are generated.

It is easy to see that the features in L_1 only occur in malware which are antigens, hence they are considered to be antigen-specific. However, the features in the L_2 appear in both malware and benign programs with high IG value, so they are believed to be antigen-nonspecific features and have the ability to discriminate malware from benign programs.

In the procedure of feature extraction, a sample is expressed as a binary feature vector of length N_1, which consists of 0 s for the absence of the features in L_1 and 1 s for the presence of the features in L_1. This feature vector is the antigen-specific feature vector which is taken as the input of the classifier C_1. In a similar way, the antigen-nonspecific feature vector of length N_2 is extracted on the basis of L_2.

In the classification module, the three classifiers C_1, C_2 and C_3 adopt the same machine learning classifier: the support vector machine (SVM) with the same parameters realized in LibSVM. Other classifiers, such as k-nearest neighbor, naive Bayes and decision tree, can also be used.

In the malware detection field, M_2 is actually the method proposed in [21,22], which is imported in for comparison.

5. Experiments

5.1. Experimental setup

Comprehensive experiments are conducted on three public malware datasets in this paper: CILPKU08 dataset, Henchiri dataset and VXHeanvens dataset, which can be download from www.cil.pku.edu.cn/resources/.

The benign program dataset used here consists of the files in portable executable format from Windows XP and a series of applications, which are the main punching bag of malware.

This paper optimizes the following two parameters for the SVM, the gamma g in kernel function and the cost c, by traversing the whole combinations of g and c, where $g = 0.005, 0.010, \ldots, 1$ and $c = 1, 2, \ldots, 64$. According to the experimental results, the parameters of the SVM used in this paper are finally set as follows: $g = 0.125, c = 4$. We did not emphasize on optimizing the SVM parameters because the parameters optimization of the SVM is not our main focus.

In the experiments in Section 5.3, eight groups of experiments are carried out on the three public malware datasets using 5-fold cross validation, and the 95% confidence intervals are computed to look into the stability of the proposed ICL-MD model. As both the CILPKU08 and Henchiri datasets mainly consist of computer viruses, two experiments are exploited in the two datasets, ignoring the categories of malware. There are six categories of malware in the VXHeavens dataset, so it is split into six smaller datasets: backdoor, constructor, trojan, virus, worm and “Others”. The “Others” includes DoS, Nuker, Hacktool and Flooder, while the malware in the other five smaller datasets fall into a category. Six groups of experiments are taken in the six smaller datasets.

There is no overlap between a training set and a test set in all the experiments. For a training set, the malware in a test set are the unseen malware. This setting increases the reliability of the experiments.

In the experiments, we will verify that the IC mechanism plays the cooperation effect and improves the performance of the proposed ICL-MD model. What is more, the immune global concentration based malware detection (GC-MD) approach [11] and the immune local concentration based malware detection (LC-MD) approach [13], which perform very well, are imported in for comparison.

The average detecting time for a sample is very important for a real-time system, hence it will be given and discussed in Section 6.2. The detailed information of the experimental platform is listed in Table 2.

5.2. Selection of parameters

The two parameters in the ICL framework, N_1 and N_2, are selected by using the grid search in this section, where $N_1, N_2 = 100, 200, \ldots, 1000$. The larger N_1 and N_2 are not considered as the higher dimension of the feature vectors.

The dataset used here consists of 1048 benign programs, randomly selected from the benign program dataset, and 1048 computer viruses from the VXHeavens dataset. The benign programs were randomly split into two sets with 524 programs for each set, one for training and the other one for testing. The same partition was done to the computer viruses. The 524 benign programs and 524 viruses made up the training set, and the test set consisted of the remaining benign programs and viruses.

The experimental results on the above dataset are further processed using cubic spline interpolation method and plotted in Fig. 3 which illustrates the influence of the two parameters, N_1 and N_2, to the performance of the ICL-MD model. It is easy to see that N_1 has a greater influence on the performance of the ICL-MD model, so selecting a proper N_1 would help the ICL-MD model perform better. With the increase of N_1, more and more discriminating antigen-specific features are included in L_1 which are considered to help us to improve the performance of the ICL-MD model, whereas more misleading information are also brought which lead to the decrease of the performance of the ICL-MD model at last. According to the experimental results, N_1 is set to 400 as the ICL-MD model performs well and stably with this parameter. The influence of N_2 is less than that of N_1. With $N_1 = 400$, we set $N_2 = 400$.

Table 2
The experimental platform.

CPU	Core 2 Duo 3.00 GHz
RAM	8 GB
Operating System	Win 7 64-bit

5.3. Experimental results

Eight groups of experiments are conducted on the three public malware datasets in this section. Table 3 lists the experimental results of the $M_1, M_2, M_{1\bigcup 2}$, and the proposed ICL-MD model, in which the bold font indicates the best results of the four models.

Table 3 suggests that the ICL-MD model outperforms both M_1 and M_2 in all the experiments. It performs better than M_1 and M_2 for about 13.46% and 0.58% on average in the experiments taken in the VXHeavens dataset. Since both M_1 and M_2 achieved good results in the CILPKU08 and Henchiri datasets, the ICL-MD model outperforms M_1 and M_2 slightly in the two datasets.

The ICL-MD model also outperforms $M_{1\bigcup 2}$, which indicates the sum of M_1 and M_2, with minor superiority in the experiments on the CILPKU08 and Henchiri datasets, while it is better than $M_{1\bigcup 2}$ for about 0.42% on average in the other six groups of experiments. In the experiment to detect worm, the ICL-MD model outperforms $M_{1\bigcup 2}$ for about 0.92%, which proves that the IC mechanism in the ICL framework plays the cooperation effect effectively.

The proposed ICL-MD model characterizes and analyzes a sample from the antigen-specific perspective and the antigen-nonspecific perspective at the same time, which lays a good foundation for the classification later. The ICL-MD model achieves excellent performance with the help of the cooperation of the two immune signals, which are considered to help us to drop down the false positive and false negative rates.

The experimental results of the GC-MD and LC-MD approaches are given in Table 4. It is easy to see that the proposed ICL-MD model outperforms the GC-MD and LC-MD approaches for about 3.28% and 2.24% on average, respectively, in the experiments taken in the VXHeavens dataset, while it is a little better than the two approaches in the other two experiments. These experimental results suggest that the ICL framework is an effective immune based learning framework and introducing the IC mechanism into AIS has the potential ability to improve its performance.

The 95% confidence intervals in all the experiments of the ICL-MD model are relatively small from Table 3, and they are less than that of the M_1, M_2 and $M_{1\bigcup 2}$ in most cases. These results suggest that the proposed ICL-MD model is very stable.

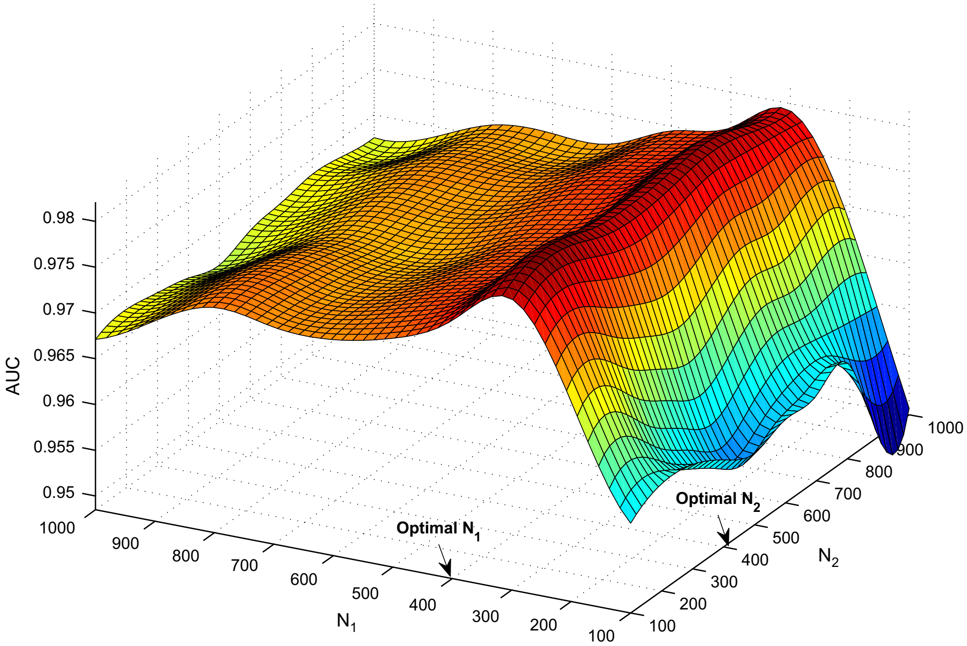

Fig. 3. The AUC in the selection of parameters.

Table 3
The AUCs of the $M_1, M_2, M_{1\bigcup 2}$, and the ICL-MD model.

Datasets	M_1	M_2	$M_{1\bigcup 2}$	ICL-MD model
CILPKU08	0.9564 ± 0.003228	0.9992 ± 0.000910	0.9995 ± 0.000410	$\mathbf{0.9997 \pm 0.000249}$
Henchiri	0.9606 ± 0.006053	0.9990 ± 0.000862	0.9994 ± 0.000361	$\mathbf{0.9995 \pm 0.000276}$
Backdoor	0.8509 ± 0.004976	0.9794 ± 0.003280	0.9825 ± 0.003355	$\mathbf{0.9846 \pm 0.002036}$
Constructor	0.8996 ± 0.047044	0.9794 ± 0.014825	0.9808 ± 0.013594	$\mathbf{0.9820 \pm 0.014933}$
Trojan	0.7741 ± 0.036341	0.9644 ± 0.005274	0.9665 ± 0.005665	$\mathbf{0.9702 \pm 0.004172}$
Virus	0.8439 ± 0.023959	0.9770 ± 0.004391	0.9775 ± 0.004147	$\mathbf{0.9833 \pm 0.002757}$
Worm	0.8691 ± 0.035813	0.9708 ± 0.006525	0.9726 ± 0.006626	$\mathbf{0.9818 \pm 0.002969}$
Others	0.8282 ± 0.025178	0.9676 ± 0.007042	0.9688 ± 0.006974	$\mathbf{0.9717 \pm 0.006097}$

Table 4
The AUCs of the GC-MD approach and LC-MD approach.

Datasets	GC-MD approach	LC-MD approach
CILPKU08	0.9976 ± 0.000526	0.9973 ± 0.000559
Henchiri	0.9970 ± 0.001283	0.9966 ± 0.001944
Backdoor	0.9711 ± 0.007953	0.9740 ± 0.006196
Constructor	0.9651 ± 0.011248	0.9672 ± 0.009040
Trojan	0.9525 ± 0.004842	0.9527 ± 0.003589
Virus	0.9650 ± 0.009839	0.9692 ± 0.008283
Worm	0.8942 ± 0.032133	0.9322 ± 0.016678
Others	0.9288 ± 0.014902	0.9438 ± 0.009501

Table 5
The ANOVA/*P*-value Table.

Source	SS	df	MS	*F*	*P*
Experiments	0.00338	2	0.00169	4.27	0.034
Error	0.00592	15	0.00039		
Total	0.00930	17			

The SS denotes the sums of squares, and the df is the degrees of freedom. The MS represent the mean squares (SS/df) and the *P* is the *P*-value.

5.4. Statistical analysis

In order to ensure that the experimental results are reliable and the proposed ICL-MD model outperforms the GC-MD and LC-MD approaches statistically, an analysis of variance (ANOVA) has been done followed by two *t* hypothesis tests (t-test).

As the malware in the CILPKU08 and Henchiri datasets come from the Disk Operating System (DOS) which are easier to be detected, all the GC-MD approach, the LC-MD approach and the proposed ICL-MD model perform well on the two datasets. Here all the statistical analysis has been done with the six groups of experiments on the VXHeavens dataset.

We regard the performances of the three malware detection models as a random variable which is distributed normally with the same variance. According to the six groups of independent experimental results, the ANOVA/*P*-value table is given in Table 5.

Table 5 suggests that the *P*-value is 0.034, which is less than the default $\alpha = 0.05$ significance level. It indicates that the performances of the three malware detection models are not the same statistically. Hence the null hypothesis that all the three models have a common performance is rejected and the three models are considered to perform statistically different.

In order to make sure that the proposed ICL-MD model outperforms the GC-MD and LC-MD approaches statistically, two t-tests have been further carried out. There are six groups of independent experimental results, written as (X_i, Y_i, Z_i) where X_i, Y_i, Z_i are the AUCs of the GC-MD, LC-MD and ICL-MD models respectively, $i = 1, 2, \ldots, 6$. Let $D^i_{xz} = X_i - Z_i$ and $D^i_{yz} = Y_i - Z_i$. As there is only a factor, the different malware detection models, which affect the values of the D^i_{xz} and D^i_{yz}, the D^i_{xz} and D^i_{yz} are considered to be distributed normally, respectively. Suppose that $D^i_{xz} \sim N(\mu_{D_{xz}}, \sigma^2_{D_{xz}})$, $i = 1, 2, \ldots, 6$. Three hypothesis tests are needed to be exploited based on the samples D^{xz}_i, which are shown as

$$H_0 : \mu_{D_{xz}} = 0, H_1 : \mu_{D_{xz}} \neq 0 \tag{7}$$

$$H_0 : \mu_{D_{xz}} \leq 0, H_1 : \mu_{D_{xz}} > 0 \tag{8}$$

$$H_0 : \mu_{D_{xz}} \geq 0, H_1 : \mu_{D_{xz}} < 0 \tag{9}$$

According to the t-test, $t_{0.05/2}(5) = 2.5706, t_{0.05}(5) = 2.0150$, the critical region of the three hypothesis tests are $(-\infty, -2.5706]\bigcup]2.5706, +\infty), [2.0150, +\infty), (-\infty, -2.0150]$.

As $t_{xz} = -2.7839$, t_{xz} refuses the hypothesis H_0 in (7) and (9), but accepts the hypothesis H_0 in (8). These results suggest that the ICL-MD model outperforms the GC-MD approach at the $\alpha = 0.05$ significance level. In a similar way, we know that $t_{yz} = -3.7712$, which also demonstrate that the ICL-MD model outperforms the LC-MD approach at the $\alpha = 0.05$ significance level. On the basis of the above t-tests, the improvement of the ICL-MD model is considered to be statistically significant, and the experimental results in this paper are reliable.

6. Discussions

6.1. Advantages of the ICL framework

Inspired from BIS, the danger zone is considered to be unnecessary in AIS in this paper. Based on this idea, the proposed ICL framework does not define a danger zone. It is different from the previous danger theory based learning models which almost always define a danger zone to limit the spread range of the danger signal. Hence the ICL framework need not optimize the size of the danger zone. It drops down the complexity of the ICL framework. Compared to the BIS, the ICL framework without danger zone is more natural.

The proposed ICL framework takes advantage of the real-valued signals instead of the binary-valued signals in BIS. It makes the ICL framework not to define the binarization thresholds for the classifiers C_1 and C_2, and not to resolve the signal conflict problem here. The complexity of the ICL framework is brought down dramatically in this way. What is more, the real-valued signals are able to be sent to the cooperation classifier C_3 more precisely without information loss which lay a good foundation for the cooperation of the immune signals later.

The ICL framework defines a new way to emit the immune signals. The antigen-specific classifier C_1 sends out Signal 1 based on the antigen-specific feature vector of a sample, while Signal 2 is emitted by the antigen-nonspecific classifier C_2 according to the sample's antigen-nonspecific feature vector. The different properties of the two immune signals, that is, antigen-specific and antigen-nonspecific, do not rely on the uncorrelated machine learning classifiers used in the classifiers C_1, C_2 and C_3. In fact, they come from the two different and independent training data sources: antigen-specific and antigen-nonspecific feature vector sets.

The IC mechanism is introduced into AIS successfully by the ICL framework in this paper. The ICL framework characterizes a sample more precisely from the antigen-specific and antigen-nonspecific perspectives with the help of the IC mechanism, which is believed to help us to reduce the false positive and false negative rates. With the cooperation effect of the immune signals, the ICL framework outperforms the M_1, M_2 and $M_{1\bigcup 2}$, and it further outperforms the GC-MD and LC-MD approaches statistically.

6.2. Time complexity

The time complexity of the ICL framework is the same as the GC-MD and LC-MD approaches: $O(N)$, where N is the length of a sample. There are N 4-Grams at most in a sample of length N. In the procedure of feature extraction, every 4-Gram needs to be queried in a hash table, the capacity of which is a constant, N_1+N_2 in this context. The query complexity in the hash table is $O(1)$. Hence the time complexity to extract the antigen-specific and antigen-nonspecific feature vectors of a sample is $O(N)$. Compared to the time complexity of the feature extraction, the time complexity of the classification module in the ICL framework is very low which could be ignored. Hence the time complexity of the proposed ICL framework is $O(N)$.

The average detecting time for a sample of the ICL-MD model is measured in the virus dataset of the VXHeavens dataset, where the average size of the samples is 104 KB. The average detecting time is given in Table 6.

Table 6 shows that the average detecting time for a sample of the four models is almost the same. In the feature extraction procedure, the ICL-MD model and the $M_{1\bigcup 2}$ store the feature libraries L_1 and L_2 in a hash table, respectively, the capacity of which is N_1+N_2, while the capacity of the hash tables used in the M_1 and M_2 are N_1 and N_2, respectively. Actually a query in these hash tables consumes nearly the same time. Compared to the time used in the feature extraction procedure, the time of classification is quite short. Hence the ICL-MD model runs as fast as the M_1, M_2 and $M_{1\bigcup 2}$.

The proposed ICL-MD model is twice faster than the GC-MD and LC-MD approaches which consume 0.16 and 0.15 s for a sample on average respectively. It basically meets the requirement of a real-time system.

7. Conclusions

Inspired from BIS, this paper has proposed a novel IC mechanism based learning framework. It characterizes a sample from both the antigen-specific and antigen-nonspecific perspectives, and classifies the sample by using the immune cooperation effect of the immune signals. Extended experimental results suggest that the ICL framework is an effective learning framework. The ICL-MD model outperforms the GC-MD and LC-MD approaches for about 3.28% and 2.24% on average, respectively, with twice faster speed. This work makes two contributions:

Table 6
The average detecting time for a sample (seconds).

M_1	M_2	$M_{1\bigcup 2}$	ICL-MD model
0.07179	0.06968	0.07236	0.07256

- This paper introduces the IC mechanism into AIS and constructs an IC mechanism based learning framework.
- This paper illustrates that the danger zone is considered to be unnecessary in AIS.

Future work includes strengthening the cooperation effect of the immune signals by introducing different machine learning classifiers.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant nos. 61170057 and 61375119.

References

[1] P. Matzinger, Tolerance, danger, and the extended family, Annu. Rev. Immunol. 12 (1) (1994) 991–1045.
[2] P. Matzinger, The danger model: a renewed sense of self, Science 296 (5566) (2002) 301.
[3] S. Forrest, A. Perelson, L. Allen, R. Cherukuri, Self-nonself discrimination in a computer, in: Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy, IEEE, 1994, pp. 202–212.
[4] S. Forrest, S. Hofmeyr, A. Somayaji, T. Longstaff, A sense of self for unix processes, in: Proceedings of the 1996 IEEE Symposium on Security and Privacy, IEEE, 1996, pp. 120–128.
[5] C. F-Secure, F-secure Reports Amount of Malware Grew by 100% during 2007, 2007.
[6] T. Li, Dynamic detection for computer virus based on immune system, Sci. China Ser. F: Inf. Sci. 51 (10) (2008) 1475–1486.
[7] P. Zhang, W. Wang, Y. Tan, A malware detection model based on a negative selection algorithm with penalty factor, Sci. China Inf. Sci. 53 (12) (2010) 2461–2471.
[8] P. Zhang, Y. Tan, A danger feature based negative selection algorithm, Adv. Swarm Intell. (2012) 291–299.
[9] Y. Tan, C. Deng, G. Ruan, Concentration based feature construction approach for spam detection, in: International Joint Conference on Neural Networks, IJCNN 2009, IEEE, 2009, pp. 3088–3093.
[10] G. Ruan, Y. Tan, A three-layer back-propagation neural network for spam detection using artificial immune concentration, Soft Comput. A Fus. Found. Methodol. Appl. 14 (2) (2010) 139–150.
[11] W. Wang, P. Zhang, Y. Tan, An immune concentration based virus detection approach using particle swarm optimization, Adv. Swarm Intell. (2010) 347–354.
[12] Y. Zhu, Y. Tan, A local concentration based feature extraction approach for spam filtering, IEEE Trans. Inf. Forensics Secur. 6 (2) (2011) 486–497.
[13] W. Wang, P. Zhang, Y. Tan, X. He, An immune local concentration based virus detection approach, J. Zhejiang Univ. Sci. C 12 (6) (2011) 443–454.
[14] D. Dasgupta, S. Yu, F. Nino, Recent advances in artificial immune systems: models and applications, Appl. Soft Comput. 11 (2) (2011) 1574–1587.
[15] U. Aickelin, C. S., The danger theory and its application to artificial immune systems, Artif. Immune Syst. (2002) 141–148.
[16] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, J. McLeod, Danger theory: the link between AIS and IDS? Artif. Immune Syst. (2003) 147–155.
[17] M. Vella, M. Roper, S. Terzis, Danger theory and intrusion detection: possibilities and limitations of the analogy, Artif. Immune Syst. (2010) 276–289.
[18] C. Zhang, Z. Yi, A danger theory inspired artificial immune algorithm for on-line supervised two-class classification problem, Neurocomputing 73 (7–9) (2010) 1244–1255.
[19] Y. Zhu, Y. Tan, A danger theory inspired learning model and its application to spam detection, Adv. Swarm Intell. (2011) 382–389.
[20] C. Ou, Host-based intrusion detection systems adapted from agent-based artificial immune systems, Neurocomputing 88 (2012) 78–86.
[21] J.Z. Kolter, M.A. Maloof, Learning to detect malicious executables in the wild, in: Proceedings of the tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '04, 2004, pp. 470–478.
[22] J. Kolter, M. Maloof, Learning to detect and classify malicious executables in the wild, J. Mach. Learn. Res. 7 (2006) 2721–2744.
[23] Z. Pancer, M. Cooper, The evolution of adaptive immunity, Annu. Rev. Immunol. 24 (2006) 497–518.
[24] P. Travers, M. Walport, Charles A. Janeway, Jr, M.J. Shlomchik, Immunobiology: The Immune System in Health and Disease, no. 2.
[25] T. Golovina, T. Mikheeva, M. Suhoski, N. Aqui, V. Tai, X. Shan, R. Liu, R. Balcarcel, N. Fisher, B. Levine, et al., Cd28 costimulation is essential for human t regulatory expansion and function, J. Immunol. 181 (4) (2008) 2855–2868.
[26] F. Vincenti, Costimulation blockade in autoimmunity and transplantation, J. Allergy Clin. Immunol. 121 (2) (2008) 299–306.
[27] R. Nurieva, X. Liu, C. Dong, Yin–yang of costimulation: crucial controls of immune tolerance and function, Immunol. Rev. 229 (1) (2009) 88–100.

[28] M. Ford, C. Larsen, Translating costimulation blockade to the clinic: lessons learned from three pathways, Immunol. Rev. 229 (1) (2009) 294–306.

[29] Y. Yang, J. Pedersen, A comparative study on feature selection in text categorization, Int. Conf. Mach. Learn. 23 (1997) 412–420.

Pengtao Zhang received a Bachelor of Science in Computer Science from Dalian University of Technology, Liaoning, China, in 2008. He is currently majoring in Computer Science and working towards the Ph.D. degree at Key Laboratory of Machine Perception (Ministry of Education) and Department of Machine Intelligence, EECS, Peking University, Beijing. His research interests include artificial immune system, intelligent information processing algorithm, computer information security, pattern recognition, machine learning and data mining.

Ying Tan (M'98, SM'02) received the B.S. degree in 1985, the M.S. degree in 1988, and the Ph.D. degree in signal and information processing from Southeast University, Nanjing, China, in 1997. Since then, he became a postdoctoral fellow then an associate professor at University of Science and Technology of China. He was a full professor, advisor of Ph.D. candidates, and director of the Institute of Intelligent Information Science of his university. He worked with the Chinese University of Hong Kong, in 1999 and in 2004–2005. He was an electee of 100 talent program of the Chinese Academy of Science, in 2005. Now, he is a full professor, advisor of Ph.D. candidates at the Key Laboratory of Machine Perception (Ministry of Education), Peking University, and department of Machine Intelligence, EECS, Peking University, and he is also the head of Computational Intelligence Laboratory (CIL) of Peking University. He has authored or coauthored more than 200 academic papers in refereed journals and conferences and several books and book chapters. His current research interests include computational intelligence, artificial immune system, swarm intelligence and data mining, signal and information processing, pattern recognition, and their applications. He is an Associate Editor of International Journal of Swarm Intelligence Research and IES Journal B, Intelligent Devices and Systems, and Associate Editor-in-Chief of International Journal of Intelligent Information Processing. He is a member of Advisory Board of International Journal on Knowledge Based Intelligent Engineering System and The Editorial Board of Journal of Computer Science and Systems Biology and Applied Mathematical and Computational Sciences. He is also the Editor of Springer Lecture Notes on Computer Science, LNCS 5263, 5264, 6145 and 6146, and Guest Editor of Special Issues on Several Journals including Information Science, Soft computing, International Journal of Artificial Intelligence, etc. He was the General Chair of International Journal on Swarm Intelligence (ICSI 2010, ICSI 2011) and the Program Committee Chair of ISNN2008. He was honored the 2nd-class prize of National Natural Science Award of China in 2009. He is a senior member of the IEEE.