An Artificial Immune-based Feature Interaction Detection Method

Wei WEI, Fangchun YANG
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
buptweiwei@163.com, fcyang@bupt.edu.cn

Abstract

Based on analyzing the similarities of the Feature Interaction Detection System and Artificial Immune System, an artificial immune-based feature interaction detection method is proposed to detect all kinds of feature interactions in the next generation network, which references the multi-layer protection of the immune system and some immune principles, including the immune recognition, co-stimulation, immune learning, clone selection and self tolerance. The simulation and research show that this method is capable of detecting all kinds of feature interactions neatly, enhancing the detection ratio and efficiency dynamically, and adapting to multi-network with high expansibility and universality.

1. Introduction

Features function well solely, but their combined behavior may exhibit undesired characteristics, which is known as Feature Interaction (FI) [1, 2]. For example in telecommunication system, a user who subscribes to Call Waiting (CW) and Call Forward when Busy (CFB) is engaged in a call, then what will happen when there is a further incoming call? If the call is forwarded, then the CW feature is clearly compromised, and vice versa. In either case, the user will not have their expectations met.

In the Next Generation Network (NGN), with the openness of the networks capabilities, a great deal of independent service providers can access the network to develop and deploy the services. With the rapid growth of the numbers and kinds of services, FI will become much severer. Because features are packages of incrementally added function to services, we will use term feature and service interchangeably in this paper.

There have been plenty of works on the prevention, detection and resolution of FI in the telecommunication systems [1, 2]. But the traditional run-time detection method can only detect several kinds of FI, especially lack in the gradual recognition for the unknown FI. Artificial Immune System (AIS) [3-6] has good capability of immune learning, immune recognition and immune memory, and AIS has been researched and applied in many fields. Based on the AIS and the feature interaction manager (FIM) method between the service layer and control layer in NGN, an Artificial Immune-based Detection method (AID) for FI is proposed to detect all kinds of FI. The detection ratio and efficiency of AID is enhanced by the separation of the innate immune and the adaptive immune in the AIS. The AID combines the antigen recognition and the reinforcement immune learning to detect the unknown FI gradually, uses clone selection to accelerate the coverage of FI, and decreases the Fault Positive (FP) by self tolerance. The simulation shows that AID can not only detect the known FI, but also get the knowledge of the unknown FI gradually. Also, AID adapts to multi-network with high expansibility and universality.

2. Related Work

According to its lifecycle, the feature interaction management includes offline method and online method. Offline means that the method is applied during design time of features, in contrast to online method which is applied while the features are actually running. Offline method is limited in use because it needs the detail of feature implementation [2]. Online method is mainly divided into negotiation method and FIM method. The negotiation method [7,8] regards the components of the networks (user, terminal and value-added service, etc.) as different intelligent entities, detects and resolves FI by exchanging intentions of those entities. The negotiation method is not suitable for the NGN because the entities in NGN have no such intelligence. The FIM method [9-14] adds a FIM into the network to detect and resolve FI. These methods are capable of detecting and resolving one or

0-7695-2650-0/06/$20.00 (c) IEEE

several kinds of FI efficiently, but they can not be combined together efficiently because their adaptability and expansibility are not good. There are also some limitations in these methods. For example, Ref.[9] ignores the semantic info in messages and matches the feature behavior just by syntactic info of the messages; the efficiency of the resolution process in Ref.[12,13] is a little low. Immunology-based Service Interaction Management System (ISIMS) [15] was proposed to detect all kinds of FI in NGN. ISIMS describes all kinds of feature behavior as antigen in AIS. The detection rules in ISIMS will detect the FI by matching with feature behavior. So ISIMS can detect FI in a universal way based on immune cells recognizing the antigen. But for high detection ratio, ISIMS needs enumerate all possible combinations of the feature behavior, too many detection rules in ISIMS result in low efficiency. Also ISMIS is lack in favorable learning mechanism, and the weak detection rules generated by the single parent generation algorithm can not detect the unknown FI efficiently.

The AID method is an enhancing method for ISIMS, so AID can detect all kinds of FI in NGN.

3. The mapping of the AID system and AIS

Compared the similarities of the feature interaction management system with the AIS, the function entities mapping and the detection process mapping relations are shown as Table 1 and Table 2.

Table 1. Function entities Mapping

Telecommunication system	Body
Feature Interaction Management System	Artificial Immune System
Feature Behavior	Antigen
Feature Interaction	Nonself Cell
Normal Feature behavior/ Feature collaboration	Self Cell
Feature Interaction Detection Rule	Immune Cell
Feature Interaction Detection Information	Antigen determinant
Information Preprocess	Skin and physical environment
Special Memorial Feature Interaction Detection Rule	Macrophage
Universal Memorial Feature Interaction Detection Rule	Lymphocyte
Feature Interaction Detection Rule Generator	Backbone Lymphoid Organs
Feature Interaction Resolution Policy	Bacteriolysin/ Antibody
Known Feature Interaction Detection Rule	Bacterin

Table 2. Detection process mapping

Happen of Feature Interaction	Antigen Inbreak
Collection and Preprocess of the Feature Messages	Antigen Presentation
Detection of Feature Interaction	Antigen Recognition
Resolution of Feature Interaction	Antigen Clearup
Affirm of Feature Interaction	Co-stimulation
Storage of Feature Interaction Detection Information	Immune Memory
Input of the Detection Rules for the known Feature Interaction	Inoculate Bacterin

4. AID method

4.1. Some definitions

Firstly, we make several definitions based on AIS:

Def. 1 Detection Rule Set *B*, *B*={*b*|*b*=[<messages>][<datas>][<rules>]<capability><interval>={[<message>^{m}][<data>^{n}][<rule>^{k}]<capability><interval>| capability, interval ∈ N}, messages represent the response messages of the feature, datas represent the info to aid FI detection, rules represent the constraint of FI, each part of them could be empty, but could not be all empty; *m*, *n*, *k* represent the number of the message, data and rule separately, capability represents the times of *b* detecting the FI successfully, interval represents *b*'s lifecycle.

B is composed of Memorial Detection Rule Set M_b, Mature Detection Rule Set T_b, and Immature Detection Rule Set I_b. The rules having detected FI successfully are stored in M_b. The rules having not detected FI are stored in T_b, and those of which expired lifecycles will be deleted. The new detection rules will be added to the I_b. There are following relations among them: $B = M_b \cup T_b \cup I_b$, $M_b \cap T_b \cap I_b$ =NULL. $M_b = S\_M_b + U\_M_b$, S_M_b represents the special detection rules in M_b, U_M_b represents the universal detection rules in M_b.

Def. 2 Feature behavior Set *Ag*, *Ag* = {*ag* | *ag* = [<messages>][<datas>]}, the service behaviors are described by the messages and datas. *Ag* includes two subsets: *Nonself* and *Self*, $Self \cup Nonself = Ag$, $Self \cap Nonself$=NULL.

Def. 3 *Nonself*, *Nonself* represents the FI.

Def. 4 *Self*, *Self* represents the normal feature behavior or feature collaboration.

4.2. AID system

There are three layer protections in the AIS, as shown in Figure 1.

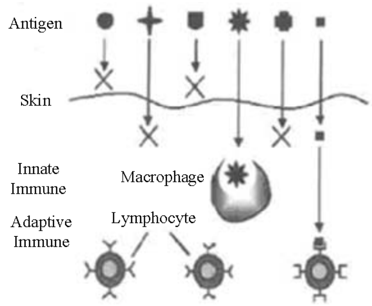

Figure 1. Model of multi-layer protection in AIS

Similarly, the AID system is set up as Figure 2. The dashed means that the function model is new added model than ISIMS. The Special Feature Interaction Detection (sFID) model is added to enhance the detection ratio, and the Generate Detection Rule (GDR) submodel is added to generate the new detection rules for unknown FI. AID system exists between the service layer and control layer of the NGN, and it is independent of the concrete network architecture. AID system can apply not only between the Parlay Application Server and Parlay Gateway, but also between the Application Server and Serving Call Session Control Function(S-CSCF) of IP Multimedia Subsystem (IMS).

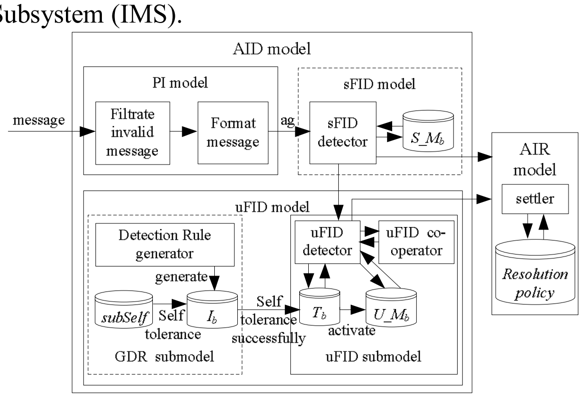

Figure 2. Model of AID system

4.3. AID description

The AID is based on multi-layer protection of the AIS, whose detection process is divided into three parts:

4.3.1. First Layer: Preprocess Information

The first layer of AIS is the skin and physical environment, which protects body from the virus intrusion and kills the bacillus.

Similarly, the first layer in AID is the Preprocess Information (PI) model, which filtrates the invalid interactive messages from the control entity or the service logic, collects and formats the messages for the further use. The messages are formatted as formula 1:

<message>={<SessionID><Event><ServiceID> <msgName>[<msgPara>|…]<Times>} (1)

<SessionID>=N, SessionID represents a unique session;

<Event>={Address_Analyzed|tBusy|…},Event represents the trigger event;

<ServiceID>=N, SessionID represents a unique service satisfied by the current Event in the session;

<msgName>={<routeReq>|<release>|…}, msgName represents the name of the message;

<msgPara>={<origAddress>|<destAddress>|…}, msgPara represents the important parameters of the message;

<Times>=N, Times represents the times interacted with the AID system in the session, and its value increases gradually.

4.3.2. Second Layer: Innate Immune

The second layer of AIS is the innate immune composed by Macrophage. Macrophage can eliminate the intrude Bacterium quickly, and its secondary response is not enhanced because it can not memory the intruded Bacterium.

Similarly, the second layer of the AID is the sFID model, which is composed of a detector and a sFID database stored S_M_b. The detection rules in S_M_b are simple and independent on the concrete services, and they can detect a special kind of FI efficiently. For example, the rule for the shared trigger interaction named m_{b1} is stored in S_M_b.

m_{b1}:

<messages>=NULL;

<datas>=NULL;

<rules>=<$\forall$ *i*,*j*><message$_i$.Event=message$_j$.Event> <message$_i$.SessionID = message$_j$.SessionID> <message$_i$.ServiceID != message$_j$.ServiceID> <message$_i$.Times = message$_j$.Times>.

If the FI is detected successfully by this layer, it will be resolved by the Artificial Immune-based Resolution (AIR) model; otherwise, it will be passed to the third layer.

4.3.3. Third Layer: Adaptive Immune

The third layer of AIS is the adaptive Immune composed of Lymphocyte. Lymphocyte can memorize the Bacterium encountered before, and produce much faster secondary response.

Similarly, the third layer of the AID is the Universal Feature Interaction Detection (uFID) model, which includes GDR submodel and uFID submodel. The

GDR submodel is used to generate the new detection rules, which is composed of a Detection Rule generator; two databases stored the subset of *Self* and I_b respectively. The uFID submodel is composed of a detector, a co-operator and two uFID databases stored T_b and U_M_b respectively. The rules in T_b and U_M_b are dependent on the concrete services, and can be used by the detector to detect all kinds of FI using the antigen recognition of AIS. After the antigen is recognized by the detector, the co-stimulation will be executed to determine whether it is a FI.

If the FI is detected successfully by this layer, it will be resolved by the AIR model; otherwise, it will be regarded as the *self*.

Some immune principles are implemented in the uFID model:

(1) Antigen Recognition

Antigen Recognition is the main function of the AIS. The *Self* and *Nonself* can be distinguished according to the affinity between the lymphocyte and the antigen.

Similarly, the uFID is implemented by matching the m_b in the U_M_b or t_b in the T_b with *ag*. The detector calculates the match degree of the detection rules and the *ag*. The recognition function is shown as formula 2:

$$f_{match}(b, ag) = \begin{cases} 1, & aff(b, ag) \geq \tau \\ 0, & otherwise \end{cases}, \forall b \in U\_M_b \cup T_b \quad (2)$$

In formula 2, *aff* is the function of calculating the affinity, τ is the match threshold value. The system will send the alert signal when m_b or t_b mathes *ag*.

(2) Reinforcement Immune Learning

The AIS covers the *Nonself* by the reinforcement learning process. The lymphocyte's primary response for *ag* is very slow. After the first successful matching, the lymphocyte memorizes the *ag*, and it's secondary response will be much faster. The co-stimulation mechanism of the AIS judges whether $ag \in Nonself$ for further avoidance of the FP.

In the process of antigen recognition in AID, when $aff(t_b, ag) > \tau$, the co-stimulation mechanism is needed to judge whether $ag \in Nonself$. If $ag \in Nonself$, the co-operator will integrate the data and rule into the t_b and send a signal to detector, and then the t_b will be added to U_M_b, with its capability is set as 1. So the *ag* will be recognized quickly for the next time. Otherwise, if $ag \in Self$, the t_b will be deleted from T_b and the *ag* will be added to the *Self* for the self tolerance.

(3) Clone Selection

The lymphocyte will clone and mutate itself to resist much more *ag* after it recognizes the *ag* successfully.

When t_b or m_b in the AID detects an *ag* successfully, it will be added into the *Parent* set. When the count of *Parent* set reaches a threshold value or the threshold timer is expired, the *Parent* set will produce the *Child* generation by crossover and mutation operator, as shown in Figure 3. *Child* is added to the I_b as i_b. The crossover point and mutation point are acquired by an average distribution.

By the clone selection, new detection rules, especially for unknown FI, are generated. Those i_b will become t_b after self tolerance successfully.

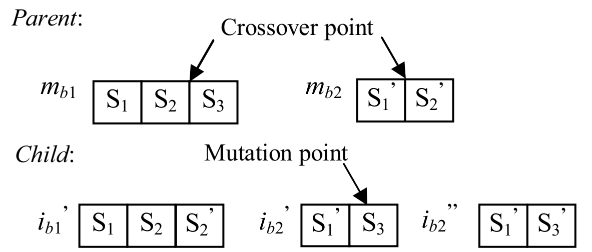

Figure 3. Crossover and mutation operator

(4) Self Tolerance

There are lots of self cells in the thymus and medulla of the body, which tolerance the fresh lymphocyte by the negative selection. The fresh lymphocyte will be killed if it recognizes the self cell, the left fresh lymphocyte will become mature lymphocyte to detect antigen.

In AID, the FP of new detection rules in I_b were decreased by the negative selection progress of self tolerance. The initial *Self* are some normal service behaviors in the network. The i_b passed through the self tolerance will become t_b. The function of self tolerance is shown as Formula 3:

$$f_{selfTolerance}(I_b) = I_b - \{ i_b \mid i_b \in I_b \cap ag \in Self \cap f_{match}(i_b, ag) = 1 \} \quad (3)$$

The process of AID method is shown as Figure 4:

The artificial immune-based feature interaction detection method.

(1) Initialize *Self*, M_b, T_b, I_b, *time*, τ;
(2) Filtrate the invalid message, and preprocess the message to *ag* by formula 1;
(3) Does one of the rules in S_M_b match *ag*? If matched, goto(6), otherwise goto(4);
(4) Does m_b in U_M_b or t_b in T_b match *ag*? If $aff(m_b, ag) > \tau$, $m_b.capability$++, goto(6); otherwise if $aff(t_b, ag) > \tau$, goto(5);otherwise goto(9);
(5) Judge whether $ag \in Nonself$ by co-operator, if it is, delete t_b from T_b and add t_b with integrated data and rule to U_M_b, $capability = 1$; otherwise, delete t_b from T_b and add t_b to *Self*;
(6) Resolve the feature interaction;
(7) Insert the m_b or t_b to *Parent*. If the genetic condition is met, *Child* will be generated by crossover and mutation and inserted into I_b;
(8) I_b will undergo self tolerance by formula 3;
(9) If the method should not be finished, goto(2).

Figure 4. Main process of AID

5. Simulation and Results

In order to inspect the validity of the method, the AID method is simulated in the experiment platform of state key laboratory of networking and switching technology in Beijing University of Posts and Telecommunications. It is supposed that the service trigger point is 5, and there are 5 services in each trigger point. The user arrival rate is an exponential distribution whose average interval is 1 second. For simpleness, it is assumed that only one key message is reserved in each service, and the data and rule of the message are ignored. Once FI is detected in a session, the session will be released.

The system performance could be evaluated by the False Positive Ratio (FPR, *self* is recognized as *nonself*) and False Negative Ratio (FNR, *nonself* is not recognized). A favorable system should detect FI with low FNR, low FPR, and high detection efficiency. Ref. [9-14] could only cover one or several kinds of FI, so the AID is compared with ISIMS because they can both cover all kinds of FI. Assume that the knowledge for the known FI is similar; the detection rule number for a special kind of FI in S_M_b of AID is 1, while the detection rule number for a special kind of FI in ISIMS is relative with the service, so the detection rule number in AID is less than that in ISIMS. The single parent genetic algorithm in ISIMS and clone selection in AID are both based on similar knowledge for known FI.

The emulational results are shown as Figure 5, Figure 6, and Figure 7:

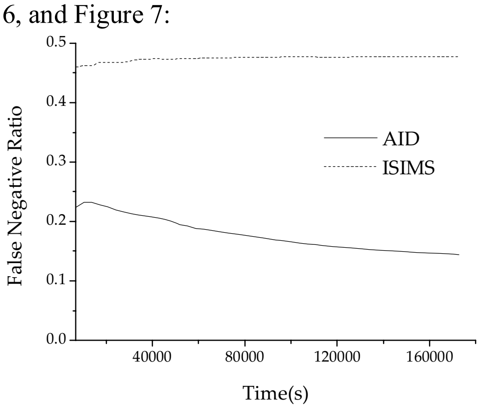

Figure 5. Comparison of FNR

Figure 5 shows that the FNR of AID is much lower than that of ISIMS. AID has good mechanism of producing the new detection rules by clone selection and nice reinforcement learning process, so the unknown FI can be recognized after some time. But in ISIMS, since the new detection rules generated by the single parent genetic algorithm, the diversities of these new rules are not good enough to cover the much more unknown FI. So, the FNR of AID is decreased gradually, while that of ISIMS is always high. When the original knowledge for known FI is similar, the detection rule number in AID is less, but it can detect much more FI.

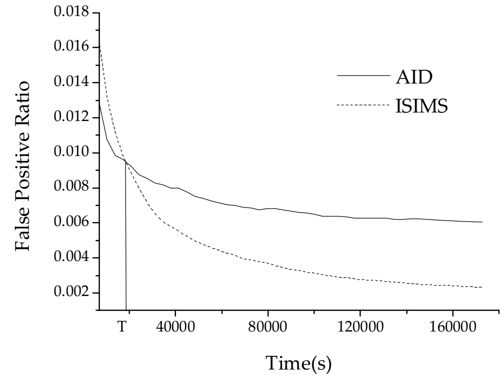

Figure 6. Comparison of FPR

Figure 6 shows that FPR of AID is decreased gradually and it is lower than that of ISIMS in the period from 0 to T. This is because clone selection process generates the new detection rule continuously, and self tolerance deletes i_b recognized by *Self* in AID. But not all the normal feature behaviors are added into the *Self*, so the FPR in AID always exists. The FPR of ISIMS decreased sharply and it is much lower than that of AID after T. This is because the detection ratio of ISIMS is very low, the number of new detection rules generated by the single parent genetic algorithm is very little, and the diversity of them is bad too. Along with some detection rules with FP are deleted, the FPR of ISIMS is less and less, even near to 0.

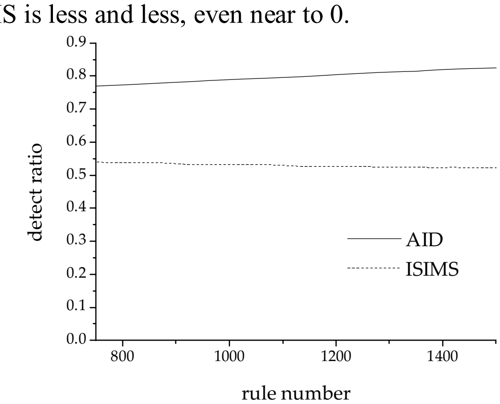

Figure 7. Relation between rule number and detection ratio

Figure 7 shows that the AID could cover much more *Nonself* with same detection rule number in contrast to the ISIMS. This is because the innate immune and adaptive immune of AIS are implemented in AID, the detection rules in S_M_b are independent on the concrete services, they can detect a special kind of FI efficiently. With the increasing detection rule number, the detection ratio of AID is enhanced gradually, while that of ISIMS is always low.

We could draw a conclusion from the emulational results that the FNR and FPR of AID are much less than those of ISIMS, and the AID could cover much more *Nonself* with less detection rules, so it is more helpful to sustain the system stable and improve the users' satisfaction.

6. Conclusion and Future Work

An artificial immune-based feature interaction detection method named AID was proposed in this paper. Compared with the traditional detection method[9-15], AID can detect all kinds of FI in NGN with low FNR, low FPR and high efficiency. The multi-layer protection mechanism and some immune principles of AIS, including the immune recognition, co-stimulation, reinforcement immune learning, clone selection and self tolerance are implemented in AID. The simulation and research show that AID is capable of detecting FI neatly and efficiently, and adapting to multi-network with high expansibility and universality dramatically.

The shortage of AID is that the experimental results are got in the emulational environment, not in the real telecommunication system.

The further work is to research the artificial immune-based resolution method for FI.

7. Acknowledgement

This work is jointly supported by: the National Basic Research and Development Program (973 program) of China (No. 2003CB314806); Program for Changjiang Scholars and Innovative Research Team in University.

8. References

[1] D. O. Keck, P. J. Kuehn, "The feature and service interaction problem in telecommunications systems: a survey", *IEEE Transactions on Software Engineering*, 24 (10), Oct. 1998, pp. 779 -796.

[2] M. Calder, M. Kolberg, E. H. Magill, et al., "Feature Interaction: a critical review and considered forecast", *Computer Networks*, 41(1), Jan. 2003, pp.115-141.

[3] D. Dasgupta, N. Attoh-Okine, "Immunity-based systems: a survey", Proc IEEE International Conference on Systems, Man, and Cybernetics, Florida, Oct. 1997, pp.369-374

[4] Licheng JIAO, Haifeng DU, "Development and Prospect of the Artificial Immune System", *Acta Electronica Sinica*, Beijing, 31 (10), Oct. 2003, pp.1540-1549.

[5] Tao LI, Computer Immunology [M], Beijing, Electronics Industy Press, 2004.

[6] Renbin XIAO, Lei WANG, "Artificial Immune System: Principle, Models, Analysis and Perspectives", *Chinese Journal of Computers*, Beijing, 25(12), Dec. 2002, pp. 1281-1293.

[7] N. D. Griffeth, H. Velthuijsen, "The negotiating Agents approach to runtime interaction resolution", Feature Interactions in Telecommunication and Software Systems, IOS Press, Amsterdam, 1994, pp.217-235.

[8] M. Amer, A. Karmouch, T. Gray, et al, "An Agent Model for the Resolution of Feature Conflicts in Telephony", *Journal of Network and Systems Management*, 8(3), Mar. 2000, pp.419-437.

[9] S. Tsang, E. H. Magill, "Behaviour Based Run-Time Feature Interaction Detection and Resolution Approaches for Intelligent Networks", Feature Interactions in Telecommunications Systems IV, IOS Press, Montreal, 1997, pp.254-270.

[10] I. Aggoun, P. Combes, "Observers in the SCE and SEE to Detect and Resolve Feature Interactions", Feature Interactions in Telecommunications Systems IV, IOS Press, Montreal, 1997, pp.198- 212.

[11] S. Homayoon, H. Singh, "Methods of Addressing the Interactions of Intelligent Network Services with Embedded Switch Services", *IEEE Communications*, 26(12), Dec. 1998, pp.42-70.

[12] D. Marples, E. H. Magill, "The use of Rollback to prevent incorrect operation of Features in Intelligent Network Based Systems", Feature Interactions in Telecommunications and Software Systems V, IOS Press, Amsterdam, 1998, pp. 115-134.

[13] S. Reiff-Marganiec, Runtime Resolution of Feature Interactions in Evolving Telecommunications Systems, Ph.D Dissertation, University of Glasgow, Glasgow, 2002.

[14] Jiuyun XU, Fangchun YANG, Hua ZOU, "An approach to runtime detecting and resolving service interactions in next generation intelligent network", *Journal of china institute of communications*, 25(3), Mar. 2004, pp. 126-133.

[15] Wenjian XIONG, An Immunology-based service interaction detection method in NGN, Ph.D Dissertation, Beijing University of Posts and Telecommunications, Beijing, 2005.