A New Fault-node Location Strategy

Li Qianmu,† *and Xu Manwu2*††,

Nanjing University, State Key Laboratory for Novel Software Technology, Jiangsu, China
Nanjing University of Science and Technology, Computer Science Department, Jiangsu, China

Summary
In order to overcome the defects of the traditional network fault Location methods, according to the immunology principles of bionics, a new type of node-fault detection system is presented. In this paper event detection sequences are viewed as analogous to peptide. According to the principle of positive selection in Immunology, the system builds up its event database. The behavior model whose frequency is higher will be analyzed and processed first. It improves the speed and effectiveness of fault detection. The experiment system implemented by this method shows a good diagnostic ability.

Key words:
Fault-node location, detection sequences, immunology, network troubleshooting

Introduction

With the development of the network, information globalization becomes the tendency of human development. But the network has some characteristics, such as the diversity of coupling form, the asymmetry of terminal distributing, network's opening and interlink age, which Lead the network faced with faults emerged one after another. So locating the fault node in time is very important to guarantee the integrality and usability of the network system.

At present, network fault detection methods can be sorted into two parts: misuse fault detection and anomaly fault detection. The principle of misuse fault detection is: network fault can be always expressed as form of model or characteristic. Beforehand, system defines network fault manner whose weakness is known, through monitoring the specific activity of the specific target and matching the model which is set in advance to detect network fault. Like in the network fault detection expert system [1], network fault model which is known is coded into expert system rule by expert, using the known network fault form through expert system matching. The main shortcoming of this method is that it is nail-biting to the unknown model network. The difficulty is how to distil and compile characteristic from the known network fault and let it express network fault phenomenon but will not match the normal activity. Misuse network fault detection method has these problems mentioned, so most of network fault detection system adopt anomaly network fault detection method. Anomaly network fault detection assumes that network fault activity is subclass of anomaly activity, using the normal behavior model of the network to detect network fault .The first step of this method is to set normal behavior model, then when system runs, anomaly detection program compares real time behavior model with normal behavior model, it can be considered as network fault once the notable departure happens. Like network fault detection system which bases on NN[2] , it distills characteristic of user's normal behavior sample to build characteristic contour of user's normal behavior ; It uses NN to scan system and compare the detection sample resulted from audit note with user's characteristic contour , using the deviation of them as evidence to detect network fault . The difficulty of this method is how to set up normal behavior characteristic and how to design detection arithmetic. Traditional anomaly network fault detection method like network fault detection technology which bases NN, their normal behavior characteristic are mainly from audit note of network, thus system's adaptability is not good, that is when network changes (such as the user deletes or updates network and so on), system will possibly regard sudden change which is legal as the abnormity and give an alarm, and it enlarges system's proportion of misinformation.

Network is made up of equipments and subsystems, different equipment and subsystem detects sequences with each other. Equipment produces fault and that it may influences many other equipments which are connected with it or the subsystems, even it will cause paralysis of network, this phenomenon is called network diffusion. The diffusion nature of fault makes the fault diagnoses much difficult to find fountainhead of the fault quickly from a number of fault phenomenon. Fault diffusion is the important characteristic of network fault, and it is similar to biology pathological changes mechanism. This paper puts forward a new type of network fault detection system which bases on immunology through studying the comparability between biology immunity system and network fault detection system. Immunity network is similar to human body immunity system, immunity network distinguishes normal behavior and anomaly behavior according to event detection sequences, similarly, immunity system distinguishes oneself matter and non-self matter on the basis of peptide (the segment of protein).

Manuscript received September 5, 2006.
Manuscript revised September 25, 2006.

According to the characteristic of network fault, this paper which bases on the principle of immunology puts forward integrate fault node detection arithmetic .This arithmetic finds the fountainhead of fault by the drive relationship among the faults, and it can availably make the function of fault filtration and orientation .The second and third segment of this paper present the structure of system and set the mathematic model. The forth segment presents formalization description of the status messages and the method to capture information. The fifth segment aims at the diffusion of the fault, simulating immunity mechanism to define the drive relationship of event detection sequences, and base on that it presents fault node detection arithmetic. The sixth segment uses example to validate the arithmetic.

2. Network Fault Detection Model Based on Immunology

The modern immunology considers: there is an integrate physiological mechanism with responsibility for immunity function called immunity system, it likes other systems such as nerve and incretion has a self-running mechanism, it can cooperate with other systems and restrict each other to maintain the economy 's total balance and stability on the life process . Immunological defense is a kind of functions of immunity protects to exclude external matter with the nature of antigen. The key of immunological defense is to distinguish the health cell (innocuity cell in the economy) and the bad cell (pathological molecule and baneful pathological subject). Protein is the basic component of life matters, and different proteins have different cells, so it has the good nature of identification. Immunity system identifies bad cells on the basis of peptide (a kind of protein segments).

With immunity network's biology simulation, network node can be viewed as molecule, local network in the same layer with several nodes running can be viewed as organism with many cells and the whole network can be viewed as organism tissues. Network fault reorganization mainly bases on network's event sequences which are similar to peptide. In the system, setting up a monitor program which is similar to lymphocyte to find the abnormity of network node in time. When this lymphocyte finds certain node run abnormally, the node can be thought that it have been destroyed, which is the same as differentiation mechanism.

Immunity cyber-biology simulation relationship shows in the table("immunity network's biology simulation")

Table 1: Immunity network's biology simulation

Life activity	***Network fault detection system***
Molecule	Node
Organism with more cells	The same layer network
Organism organization	The whole network
Lymphocyte	Monitor program in network
Peptide	Event detection sequences

The basic thought of event detection sequences is that filtrating unnecessary or irrelevant event for a certain single conception event through detecting several fault events, thus it can reduce fault information provided for network manager to quickly and accurately find the fountainhead of fault. Basing on the characteristic of event detection sequences, we puts forward fault orientation model showed in the figure ("Fault orientation model")and status messages collection is the anomaly events which happen in monitor and collect network. Event pretreatment is to format and filtrate the collected events. Event detection sequences analysis is to detect sequences, reduce and analyze for the events. Fault orientation is to get the fountainhead of fault through speculating. Lastly, system can remove the fault in the equipments and get the network running right through collocating manage tools or the network managers.

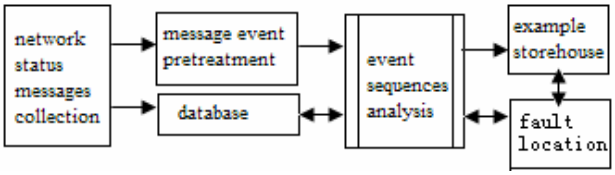

Fig. 1 Fault orientation model.

Immunity network executes two functions: detecting system network system fault and self-learning functions. Detecting system network fault is mainly to matching according on event detection sequences. System's self-learning function is similar to again response of biology immunity system's again-responsion. Namely, when immunity network detects the new fault mode, it does not only give an alarm but also stores the behavior mode of the network fault into system. When it happens again, system may give network fault signals to users directly rather than to do network fault analysis and give an alarm. The first time response and the again response of simulation biology extremely promote the reaction speed and reliability of system.

3. Event detection sequence and its model

Fault event is the sent message due to the state changing of the network object at a certain time. Network object can be viewed as a n dimensional vector, every vector represents attribute of network event and also it is time function. When some attribute of the network object under the given value of system, it will produce an event. The event can be produced directly by network object and also can be produced by network detection system.

We use a group with six members to describe the certain fault event:

Event = （EventName, EventID, Source, Type, TimeStamp, Severity）

EventName means the name of the event; EventID means the unique sign of the event; Source means the position of the event; Type means the type of the event; EventID means the time of the event, that is time thrust; Severity means the serious degree of the warning, that is cleared, normal, warning, major, critical.

Event sequence is the fault event composed by multi-events according to definite rules.

Network event detection sequences can be described as a directed graph G= (V, E). Among them, graph's vertexes express faults; graph's sides express event detection sequences.

(1) If $\forall e_1, e_2 \in E$ and $e_1 \Rightarrow e_2$, express in graph G for $e_2 \to e_1$, that is mean there is a side from e_2 to e_1.

(2) $\forall e, e_1, e_2 \in E$ and $e = e_1 \cap e_2$, express in graph G for $e \to e_1$ and $e \to e_2$, that is mean there are a side from e to e_1 and a side from e to e_2.

(3) $\forall e, e_1, e_2 \in E$ and $e = e_1 \cup e_2$, express in graph G for $e \to e_1$ and $e' \to e_2$, $\forall a \in E, a \to e,$ so that $a \to e'$, That is mean there are a side from e to e_1 and a side from e' to e_2.

(4) $\forall e_1, e_2 \in E$ and $e_1 \Leftrightarrow e_2$, mean in graph G for e_1, e_1 instead of e_2

Therefore, fault sequences contain four kinds of basic combination operations: $\cap$、$\cup$、$\Rightarrow$、$\Leftrightarrow$.

(1) $\forall e, e_1, e_2 \in E$ and $e = e_1 \cap e_2$, that is if fault e_1 and fault e_2 take place simultaneously it would then cause fault e's occurrence.

(2) $\forall e, e_1, e_2 \in E$ and $e = e_1 \cup e_2$, that is whenever fault e_1 or fault e_2 take place it would cause fault e's occurrence.

(3) $\forall e_1, e_2 \in E$ and $e_1 \Rightarrow e_2$, that is if fault e_1 takes place it would then cause fault e_2's occurrence.

(4) $\forall e_1, e_2 \in E$ and $e_1 \Leftrightarrow e_2$, that is fault e_1 and fault e_2 are the duplicate fault sent by the same managerial object.

If $A(e) = \{e_1 \mid e_1 \in E, e_1$ is the fault caused by fault $e\}, e$ is the root fault of all the faults in $A(e)$. Grant E is the fault set, obviously, E is the finite set. Physical layer fault orientation issue is a process to find the root fault among a mass of faults, it can express as $R = f[E, CE]$, E is the managerial fault set; CE is the fault set in the current network, $CE \subset E$; function f is the arithmetic to find the root fault; R is the root fault set of all faults in current network after operating by f.

4. Formalization analyses of node fault status messages

Status messages collection is the precondition of constructing event detection sequences. This model takes two kinds of ways to collect information: network event that the equipment reports the key to the manage system and driving polling. General equipments will produce many syslogs towards network node fault, and the syslog has serious grade sign itself. It can be read directly and it has five grades. For the information about performance polling, we just can set the valve value according to experiences. Like the utilization ratio of CPU, it can be set that: 30% is normal, 30%-60% is warning, 60%-80% is serious grade, over 80% is over loading and giving an alarm urgently.

We also need to colligate the parameters of the performance besides this information.

1 Bit Error Rate: $BError = \dfrac{BadbitsofTrans}{TotolbitsofTrans}$;

2 Block Error Rate: $F_{BL} = \dfrac{BlockofInvalid}{TotolBlockofSends}$

3 Signal distortions:

Excursion distortion $\delta_e = \dfrac{T - T'}{T + T'} \times 100\%$; The biggest signal excursion $\delta_P = \dfrac{\Delta t_{\max}}{T_N} \times 100\%$; The peak value excursion $\delta_P = \dfrac{\Delta t_{\max} - \Delta t_{\min}}{T_N} \times 100\%$.

4 attenuation/strand trouble ratio:

$ACR = NEXT - AttenuationofLine$

5 Signal-to-Noises $SNR = \dfrac{SignalFrame}{NoiseFrame}$;

6 Interface utilization: get through inquire about disposed bytes in the X moment and Y moment,

$$U = \frac{(iInOs_y - iInOs_x) + (iOutOs_y - iOutOs_x)}{(y-x) * iSpeed}$$

7 Corresponding receiving rate

$$Percent..\mathrm{Re}ceive = \frac{ifIn\,\mathrm{Re}ceives}{Total.Intput.Packets}$$

8 Receiving error rate

$$Per.In.Er = \frac{Indis + InHdrErs + InAddrErs}{In\,\mathrm{Re}ceives}$$

9 Data report transmitting rate: get through inquire about entity transmitted data packages' number in the X moment and Y moment.

$$F.Rate = \frac{ForwDgrams_x - ForwDgrams_y}{y-x}$$

10 time delay in chain line e

$$Delay(p) = \sum_{e \in p} D(e) \qquad D(e): E \to R^+$$

11 cost of chain line e

$$Cost(p) = \sum_{e \in p} C(e) \qquad C(e): E \to R^+$$

12 bottleneck bandwidth

$$Width(p) = \min_{e \in p}\{B(e)\} \qquad B(e): E \to R^+$$

In a certain network, if $e_{i,i+1} \in E_i$ (thereunto=1,2,… s-1), mark the attribute J of $e_{i,i+1}$ as $f_{i,i+1}^j$, the attribute J of P as f_p^j, thus it can define three measurements according to the characteristics of network status:

1 addition measurements. If $f_p^j = \sum_{i=1}^{s-1} f_{i,i+1}^j$, the attribute J of P is addition measurement. (For example, received number, send number, jump number, time delay, time delay dithering and cost.)

2 multiply measurements. If $f_p^j = \prod_{i=1}^{s-1} f_{i,i+1}^j$, the attribute J of P is multiply measurement.

For example, error rate, lost package rate and node utilization.

3 the maximum and the minimum measurement. If $f_p^j = \min_{i=1,2,...,s-1}\{f_{i,i+1}^j\}$, the attribute J of P is the minimum measurement. If $f_p^j = \max_{i=1,2,...,s-1}\{f_{i,i+1}^j\}$, attribute J of P is the maximum measurement. Such as making mistakes rate, consume, jump number are the minimum measurement; interface utilization, flux, bandwidth are the maximum measurement.

This text uses the method of adding authority to counterchange to the maximum/the minimum measurement; for multiply state, changing the corresponding status value, becoming addition measurement. So it only includes addition state in network status fault detection, network status fault detection problems can be changed as addition multi- decision-making problems, we introduce immunology mechanism to simulate addition fault diffusion.

5. Design of fault node detection algorithm

Faults have two routes to transmit in the network: transverse transmission and longitudinal transmission. Transverse transmission means that faults transmit horizontally along the physical connected or logical connected equipments. Longitudinal transmission means that faults transmit along agreement stack from lower layer to higher layer in the interior of the equipment. According to the routes of fault transmission, fault diagnosis is separated into two parts: transverse diagnosis and longitudinal diagnosis. Thus it can improve the veracity of fault diagnosis. Meanwhile, it designs event storeroom according to the masculine choice principle of biology immunology, and it does prior analysis and disposal to high frequency behavior mode, thus it will promote the detection's speed and efficiency.

Grant fault graph G= （V, E） has n vertexes （n≥1） , now set $A[i,j] = \begin{cases} 1 & (v_i, v_j) \in E \\ 0 & (V_i, V_j) \notin E \end{cases}$, that we use n factorial matrix to express graph G, this matrix A is called fault graph G's fault matrix. According to literature [3], we use the Depth-First Traversal arithmetic of matrix, and connect all the related sides to many non-closed sides' linear list until the connected sides' number is n-1.

According to sides' linear list, we divide fault graph into k connected child graphs, k≤n. using V_i , $i \in [1,\cdots,k]$ expresses vertexes set of child graphs. Get rid of the vertex with' in V_i, and add the elements in the duplicate fault which are not showed in the graph, which is called event detection sequence class, namely, $E = \bigcup_{i=1}^{k} S_i$, $S_i \cap S_j = \phi$, $i, j \in [1,2,\cdots,k], i \neq j$, S_i divides fault set E into multi-detection sequence classes, faults in every detection sequence class have detection sequence nature, faults in different event detection sequence classes do not have detection sequence nature.

For the current fault set CE, $\forall$ a ∈ CE, if a ∈ S_i , a belongs to CE. Supposing that the result is $CE_1, CE_2, \cdots, CE_k$, thus CE_i , $i \in [1,\cdots,k]$,and

$CE=\bigcup_{i=1}^{k}CE_i$, $CE_i \cap CE_j=\phi$, $i,j\in[1,k], i\neq j$ .Supposing that $R_i(i=1,2,3,\cdots,k)$ is the fault set of CE_i $(i=1,2,3,\cdots,k)$,thus the root fault set R_{CE} of CE can be expressed as $R_{CE}=\bigcup_{i=1}^{k}R_i$.

So we get the every root fault set R_i of CE_i separately, and then seek their combination set, thus we can get the root fault set R_{CE} of CE. When seeking the every root fault set R_i of CE_i , it can get the fault matrix according to the fault graph of CE_i ,if one row's elements are all 0, the corresponding vertex is the root fault. So CE_i 's fault graph is a directed graph, if one row's elements in adjoining matrix are all 0, the corresponding vertex has no forward vertex which is root fault. So we get the detection arithmetic as follows:

STEP1. To eliminate redundancy stylebook through seeking the boundary subclass of stylebook set $E=|e_1,e_2,\cdots,e_k|$. According to the principal of coarseness set, the boundary set of E is $R(Y)=R^*(Y)-R_*(Y)$ .In the formula, $R^*(Y)$和$R_*(Y)$ is the above approximation's subclass and down approximation's subclass of conclusion fault reasons' subclass $Y=\{y_1,y_2,\cdots,y_k\}$, they can be described by these formulas (X and Y are the equal classes to R):

$$R^*(Y)=\bigcup\{X\in E/R: X\subseteq Y\};$$

$$R_*(Y)=\bigcup\{X\in E/R: X\cap Y\neq\Phi\}$$

STEP2. To build the fault graph G of E, using the Depth-First Traversal arithmetic of matrix to get the connected child graph of G and using V_i , $i\in[1,\cdots,k]$ to express k connected child graphs' vertexes' set of fault graph G.

STEP3. To get rid of vertexes with ' inV_i , and add the elements in the duplicate fault which are not showed in the graph, we use S_i to express, and then get all the fault relationship classes $S_1,S_2,S_3,\cdots,S_k$.

STEP4. Basing on regulation: " ∀ a∈CE, f a∈ S_i , a belongs to CE_i ", sorting CE. The result is $CE_1,CE_2,\cdots,CE_k$,and $CE=\bigcup_{i=1}^{k}CE_i$, $CE_i\cap CE_j=\phi$, $i,j\in[1,k], i\neq j$;

STEP5. Setting the beginning root fault set $R_{CE}=\phi$, get the fault matrix according to CE_i 's fault graph, if the elements in a certain row are all 0 in matrix, the vertex corresponding to this row is root fault. Seeking root fault set R_i of all$V_i, i\in[1,k]$, get all the fault set $R_{CE}=\bigcup_{i=1}^{k}R_i$ of the current network fault.

6. Simulation and analysis

In order to test the validity of this method as well as the universality, we choose an experiment circumstance which has ten nodes and two regional chain ways, we open interface block's CDMA/CD CMOS chip U2 of equipment 5 and equipment 6, equipment 2 is under the estate of maintenance. Like figure 2 status message collection equipment finds 1283 bit error's event messages.

If equipment i loses connection with network, we use a_i to express. If cable loses efficacy, we use bi to express. Detection sequences among faults is $b_1\rightarrow a_1$, $a_2=b_2\cup a_1$, $a_2\rightarrow a_3$, $a_4\rightarrow a_5$, $a_4\rightarrow a_6$, $a_7=a_5\cap a_6$, $a_6\rightarrow a_9$, $a_7\rightarrow a_8$, $a_9\rightarrow a_{10}$.

The fault matrix of fault graph after conversion:

b_1	b_2	a_1	a_2	a_2'	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
0	0	1	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0
1	0	0	1	0	0	0	0	0	0	0	0	0
0	0	1	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	0	0	0	0
0	0	0	1	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	1	0	0	0	0
0	0	0	0	0	0	1	0	0	1	0	0	0
0	0	0	0	0	0	1	0	0	1	0	1	0
0	0	0	0	0	0	0	1	1	0	1	0	0
0	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	0	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	1	0

We can get the sides' liner list of fault graph according to matrix depth traversal arithmetic:

(a_8 , a_7)→(a_7 , a_5)→(a_5 , a_4)→(a_4 , a_6) →(a_6 , a_9)→(a_9 , a_{10})(b_1 , a_1)→(a_1 , a_2)→(a_2 , a_3)→(a_3 , a_2') →(a_2' , b_2)

According to liner list, fault graph can be divided into two connected child graphs. The vertexes set of the two connected child graphs are V_1 and V_2 , $V_1=\{a_4,a_5,a_6,a_7,a_8,a_9,a_{10}\}$, $V_2=\{b_1,b_2,a_1,a_2,a_2',a_3\}$。 V_1 is expressed as S_1 , V_2 is expressed as S_2 after throwing off a_2' , $S_1=\{a_4,a_5,a_6,a_7,a_8,a_9,a_{10}\}$, $S_2=\{b_1,b_2,a_1,a_2,a_3\}$。 S_1 and S_2 is the two fault event sequence classes of fault set E. if managed equipment do not response, managed equipment loses connection with

network, so the fault set in network now is CE={ a_2 *, a_3 , a_6 , a_7 , a_8 , a_9 , a_{10} }. If managed equipment 2 is maintaining a_2 , it should add *. Sorting CE as CE_1 ={ a_6 , a_7 , a_8 , a_9 , a_{10} } and CE_2 ={ a_2 *, a_3 }。

Finding the root fault of CE_1 and CE_2 through the method of adjoining matrix, we can find the fountain of fault.

Fig.1 status messages captured by bit error test

Event detection sequence graph G_1 of CE_1 is like fig. 3

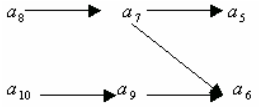

Fig. 3 event detection sequence graph G_1 of CE_1

Fault matrix of event detection sequence graph G_1 is:

$$\begin{array}{c} a_5\ a_6\ a_7\ a_8\ a_9\ a_{10} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

The elements in adjoining matrix's first low and second row of event detection sequence graph G_1 are all 0, so a_5 and a_6 are the root faults, that is R_1 ={ a_5 , a_6 }。 Next we will find the root fault of CE_2 .Event detection sequence graph G_2 of CE_2 likes fig. 4:

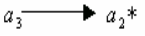

Fig. 4 event detection sequence graph G_2 of CE_2

The fault matrix of event detection sequence graph G_2 is

$$\begin{array}{c} a_2\ *\ a_3 \\ \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \end{array}$$

Fig. 5 adjoining matrix of event detection sequence graph G_2

The elements in first row of matrix G_2 are all 0, corresponding a_2 but a_2 is under the maintain estate, it is not root fault, that is R_2 =Φ. CE's root fault is R= R_1 ∪ R_2 = { a_5 , a_6 }. We find the fountain of fault, managed equipment 5 and managed equipment 6 disconnected with network through fast orientation algorithmic, we eliminate detection sequence event, and to detect bit error event which is related to equipment 5 and equipment 6.(like fig. 6.)

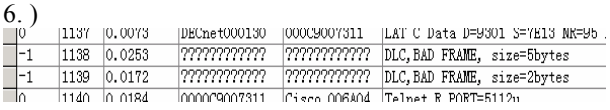

Fig. 6 related abnormal event

7. Conclusion

This paper aims at the diffusion of network fault, bases on the principal of immunology, uses event detection sequences, and it puts forward fault detection arithmetic, to take the function of fault filtration and orientation. Antitype system approves that it is available to detect the fountain fault on the basis of event detection sequences, and makes famous experiment results. The next work is to take more parameters to characteristic, to improve detection arithmetic through immunology mechanism, it can reduce the rate of misinformation and lost information, and it can improve integral capability of detection system.

References

[1] Jacobson V. Congestion Avoidance and Control. IEEE/ACM Transaction Networking, 2000, 6(3):314-329
[2] Caserri C, Meo M. A new approach to model the stationary behavior of TCP connections. In: Proc IEEE INFOCOM2000, Tel Aviv, Israel, CA: IEEE Computer Society, 2000
[3] Veres A, Boda M. The chaotic nature of TCP congestion control. In: Proc INFOCOM2000, Tel Aviv, Israel, CA:IEEE Computer Society 2000
[4] Floyd S, Fall K. Promoting the use of End-to-End congestion control in the Internet. IEEE/ACM Transaction Networking, 2002, 7(4): 458-472
[5] Harris B, Hunt R. TCP/IP security threats and attack methods. Computer Communications, 2004,22(10): 885-897
[6] Christoph L, Schuba, Ivan V, Krsul. Analysis of denial of service attack on TCP. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy 2000
[7] Hamann T, Walrand J. A new fair window algorithm for ECN capable TCP(New-ECN). In: Proc IEEE INFOCOM2000, Tel Aviv, Israel, CA: IEEE Computer Society, 2000
[8] Yager R. OWA neurons: A new class of fuzzy neurons. In:Proc IEEE-FUZZ, 1992. 2316-2340
[9] Glorennec Pierre-Yves. Neuro-fuzzy logic. In: ProcIEEE-FUZZ, 2003. 512-518
[10] Witold Pedrycz. Fuzzy neural networks and neuro computations. Fuzzy Sets and Systems. 1992, 56(1):1-28
[11] Witold Pedrycz. Logic-based neurons: Extensions, uncertainty representation and development of fuzzy controllers. Fuzzy Sets and Systems, 2004, 66(1): 251-266
[12] Bailey S A, Chen Ye-Hwa. A two layerd network using the OR/AND neuron. In: Proc IEEE-FUZZ, 1999. 1566-1571
[13] Averkin A N. Decision making based on multivalued logic and fuzzy logic, architectures for semiotic modeling and situation analysis in large complex systems . In: Proc ISIC Workshop, Monterey, 2001. 871-875
[14] He Hua-Can et al. Generalized logic in experience thinking. Science in China(E), 1996, 39(3): 225-234
[15] Buckley J J, Siler W. A new t-norm. Fuzzy Sets and Systems,2004,16(1):283-290

Li Qianmu received the B.S. and Ph.D. degrees in Computer Science and Technology from Nanjing University of SCI. and TECH. in 1999 and 2005, respectively. His research interests include wireless LAN, ad hoc networks, network troubleshooting and quality of service.

Xu manwu received the Ph.D. degree in Computer Science and Technology from Nanjing University in 1980. His research interests include wireless networks, quality of service and network performance.