TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.4, April 2014, pp. 2797 ~ 2807
DOI: http://dx.doi.org/10.11591/telkomnika.v12i4.4245

An Enhanced Safety Algorithm for Network QoS Multicast Routing Optimization

Liu Wei*[1], Cui Yong-Feng, Li Ya
School of Science and Technology, Zhoukou Normal University, Zhoukou Henan 466001, China
*Corresponding author, e-mail: zknucyf@qq.com

Abstract

In the traditional QoS multicast network routing algorithm, when the node encounters abnormal traffic network data, the node data overflows. The current protocol is lack of directional guidance for overflow, which causes abnormal data jitter and disorder, the data path planning of traditional Qos protocol blocked and network delay. In order to solve this problem, this paper presents an enhanced safety algorithm for QoS multicast network routing optimization. The constraint relationship between security level of input parameters of network service request and trust level of network service is set, in order to judge and screen the traffic overflow nodes generated by abnormal operation. Then filtered set of network services is used to construct a multi-path network services digraph and converts it into web services selection tree in use of pointing relationship between sub-services. Finally, it sorts the paths and according to the size of Qos path selects the optimal one to carry out through tracing method. Simulation results show the new algorithm has optimum network quality of service and lower complexity.

Keywords: *multicast routing, data overflow checking, algorithm optimization*

1. Introduction

As the Internet continues to grow, the function of network are also increasingly powerful, a variety of network service modes are emerging, the network business has expanded from the simple e-mail and other business to multimedia and distributed real-time business like video conferencing, video on demand, distance education [1], thus, people are increasing demand for new multimedia processing technology. The emergence of these businesses makes communication mode of the traditional unicast and broadcast cannot meet the requirements of network information transmission. The characteristic of new business is the transmission mode from point to multipoint or multipoint to multipoint, so multicast applications are paid more and more attention, multicast can effectively reduce bandwidth requirements of the overall network, lessen the load on servers and networks, which make information transmission accurate and efficient. Because most of the real-time business has a high requirement for quality of service (QoS), the needs of QoS multicast become the research hotspot of Internet-related technology. Qos multicast routing technology is one of the key technologies for network support QoS guarantee, so high efficient QoS multicast routing algorithm is vital.

A lot of research has been done by many scholars in this field, and a number of algorithms are put forward. Traditional QoS multicast routing algorithm is divided into the shortest path tree algorithm and the minimum Steiner tree algorithm, Su, et al first proposed a delay-constrained shortest path tree algorithm (CKMB algorithm) [2], while there are more algorithms related to the minimum Steiner tree algorithm. BSMA algorithm is used to solve the delay-constrained minimum Steiner tree optimization problems [3]; Rouskas, et al first proposed QoS multicast routing algorithm which satisfies delay and delay variation constraints [4]; Sheu, et al put forward DDVCT algorithm based on the core tree (CBT) and minimum delay path algorithm [5]. In recent years, QoS multicast routing algorithm based on intelligent algorithm is developing rapidly. The algorithm has been used, such as genetic algorithm, ant colony algorithm, simulated annealing algorithm, particle swarm optimization(PSO), etc., although these algorithms has its own advantages, disadvantages are also obvious. Genetic algorithm is easy to fall into local optimum, while the ant colony algorithm converges more slowly, simulated annealing algorithm and PSO have its own shortcomings, so it is difficult to completely solve multi-constrained QoS multicast routing problems by using a single intelligent algorithm.

Received August 5, 2013; Revised October 20, 2013; Accepted November 18, 2013

Therefore, many researchers combined several intelligent algorithms to solve QoS multicast routing selection problem, made use of their respective advantages, and achieved some results. ESbensen utilized the genetic algorithm which have high usage rate at present to solve the multicast routing problem [6-8]; Xiang.F gives a new genetic algorithm based on process to solve the QoS routing problem [9, 10]; Wang Xinhong, et al put forward a delay constrained least cost multicast routing selection method based on immune genetic algorithms [11-13]; Zhao Xiuping, et al raised a multiple constrained QoS multicast routing selection method based on immune genetic algorithm.

However, as users and applications continues to increase, the existing QoS multicast routing technology saves network bandwidth resources and increases the scalability of group communication system, meanwhile exposes a number of security issues. Due to lack of effective support for traffic management, billing, reliability and security, application of QoS multicast has been limited. Obviously, previous QoS multicast routing algorithms cannot meet the needs of network security, it is necessary to develop a safety enhanced QoS multicast routing algorithm aiming at the problems.

Based on the starting point that access requests and network services are required to be protected, the hierarchical security policies are embedded in the multi-path structure, we propose a network QoS multicast routing optimization algorithm based on probabilistic principal component analysis (PPCA). First, constrained relationship between the security level of input parameters in network service request and trust level of network service is set, and the traffic overflow nodes generated by abnormal operation are judged and screened. Then, the filtered set of network services are built into a multi-path network services digraph, and convert it into web services selection tree by making use of pointing relationship between sub-services, it sorts the paths and according to the size of Qos path selects the optimal one to carry out through tracing method. Finally, the superiority and effectiveness of the new algorithm are analyzed by simulation and comparison, so as to provide a theoretical reference for the QoS multicast routing security enhancements.

2. Qos Multicast Routing Overview

The main goal of QoS multicast routing is to better achieve multicast under the condition of meeting the requirement of quality of service. A brief introduction to the basic concept of QoS multicast routing is as below.

2.1. The concept of QoS Multicast Routing

Quality of Service (QoS) is a composite indicator designed to measure satisfaction with services. The main purpose of QoS is to meet the measurement technique of delay and jitter in the network, its purpose is to provide user with end-to-end quality assurance.

Multicast is network connection which can achieve point to multipoint between the sender and multiple receivers. If a sender sends data to multiple receivers, the traditional unicast should pass the data in each link, which will lead to a common link transmit the same data several times, however, the multicast is based on the idea of node replication, which means the same data only need to be copied once to be transmitted efficiently, so as to reduce the pressure on the backbone network and optimize the network, improve the utilization of network resources.

QoS multicast routing is a routing mechanism based on stream QoS requests and network available resources f, which is a dynamic routing protocol, and the QoS parameters like network available bandwidth, link utilization and usage rate of end-to-end path, delay, jitter, cost and so on, should be taken into consideration when draw up the path selection criteria. The goal is to dynamically determine a feasible path, optimize the use of resource and impact on network performance as small as possible. The purpose of QoS multicast routing is to seek an optimal multicast tree under the condition of satisfy the QoS constraints, the tree must contain all the multicast members, and lessen network costs to a minimum. QoS multicast routing problems in general contain multiple constraints, delay, jitter and bandwidth is necessary to ensure efficient transmission of real-time multimedia, the cost is an important indicator of network efficiency evaluation.

2.2. Measurement of QoS Multicast Routing

QoS provided by the network to the user includes delay, jitter, bandwidth and packet loss rate and other parameters. If network operators want to meet customer requirements, it must meet QoS parameters required by the user.

(1) Bandwidth

The number of packets transmitted in unit time. In the case of sufficient bandwidth, network data transmission delay, jitter, etc. will be less than the bandwidth is insufficient. Under the condition of meet customer demand, network resources are used rationally to manage bandwidth.

(2) Delay

The time interval of data packets transmitted and received between two points. Delay including the transmission time of data packet in the transmission medium, the processing time of the routing device, the wait queue time in the routing device. Fixed delay mainly refers to the delay in packet forwarding and spread on the transmission link, the variable delay of the data packets caused by waiting in the queue of the network node. Real-time services is sensitive to delay, so the delay takes more significant position in the QoS constraints.

(3) Jittery

Jitter is delay variation, the difference of time interval between adjacent two packets arrives at the receiver and sent by the sender. When a packet arrives at a switch device, if no other packet waiting in the queue, it will be forwarded at a fixed time delay. However, if there are other packets waiting in the queue, then it may need to wait, the fixed delay plus the waiting time in the queue is equal to the delay when packet is switched. The impact of delay jitter for real-time business is great, if the jitter is too large, the buffer is empty, real-time business don't obtain the data, the link will be interrupted.

(4) Packet Loss Rate

Packet loss rate refers to the ratio of the packet loss to transmitted data packets when data packets transmitted in the network. The main reason for this problem is network congestion, the queue is full at a node, a lot of new data packets waiting in the queue, but there is not much space to store these packets, resulting in packet loss caused by transmission errors.

(5) Cost

Certain resources are used in data transmission, the consumption of resources produce cost, the cost can be understood as some consume resources, like management costs and some routing nodes.

In the typical measurement of QoS, delay, jitter, and hop count metric has additive; packet loss rate, error rate, etc. have multiplicative; costs, traffic and bandwidth etc. have minimum and maximum.

2.3. Algorithm of of QoS Multicast Routing

The multicast routing algorithm with QoS constrained, that is, according to some routing policy, make use of network status information to construct a multicast routing tree includes all multicast members, so as to determine the packet transmission path, while meeting a variety of QoS requirements and realizing optimization of network resources. From the network user's perspective, QoS-based multicast routing algorithm should first meet the user's QoS requirements, namely looking for an end-to-end transmission path which meets a variety of requirements. From the service provider's point of view, QoS-based multicast routing algorithm should be able to make optimum use of network resources.

QoS multicast routing algorithm is divided into single-path algorithm and multi-path algorithm according to the number of paths provided, Single-path routing algorithm (single path routing, SPR) provides a single path for the new members to connect to the multicast tree, while the multi-path routing algorithm (multi path routing, MPR) provides multiple paths for new members to choose, so as to determine the path which is most suitable to meet their requirements and connect it to the tree. MOSPF, CBT and PIM-SM and other agreements have adopted the single path routing algorithm. Algorithm used in Spanning-Join QoS multicast routing protocol is a typical representative of MPR.

The process of their work is: first, new member broadcasts join-request message in neighbor node to find the on-tree-node. Then, when the on-tree-node receives the join-request message, it sends a response message (ACK) to the new member. The ack transmission path determined by the unicast routing protocol is a candidate for multicast path. New members can receive multiple response messages, and each response corresponds to a candidate path. Response messages collect QoS attributes of the path it passes in the transmission process, so the new member can select a best path according to QoS information carried by response message. When the new member is relatively far from the multicast tree, Spanning-join method needs to broadcast continuously join-request messages until it encounters the on-tree-node, so this method can significantly increase the overhead of network bandwidth. QoSMIC is another multi-path routing protocol which is paid more attention, the search of candidate path are constituted by the two processes, namely local search and tree search. Local Search is same to Spanning-join, the only difference is that the range of search is smaller. When the local search failed to find the on-tree-code, the agreement adopts tree search. Tree search makes the new member send a so-called M-JOIN to designated manager node (designated manager node, DMN), DMN select a subset of the on-tree-node in the multicast tree. The node in the subset subsequently sent the BID message to the new member. The path which the BID message experienced is determined by unicast routing protocols, and constitute the candidate paths. The scalability of QoSMIC is better than Spanning-Join agreement, but how to choose the DMN and the consequent increase in the volume of traffic is still a problem which cannot be ignored. QMRP is another new proposed QoS multicast routing protocol, it will be a combination of single path routing and multi-path routing. QMRP first makes use of SPR search, if that failed, the search back to the predecessor node of failure point and shift to multi-path search. It is obvious that the effectiveness of QMRP protocol depends on the condition of single path search, if part of the path formed by the single path search has high latency, then the probability of failure of multi-path search will be great. Thus, QMRP protocol cannot support additive QoS well, like additive such as delay.

3. Path-Policy Composition Algorithm

3.1. Related Definitions

Synthesis of execution path Global QoS calculations is aimed at addressing the problem that how to calculate the whole service quality of e ach quality dimension in the path by a single service quality. Different quality dimensions and different synthesis structure lead to the Global QoS calculation algorithm is different.A new algorithm combined path and policy is adopted in the paper. To clearly describe the proposed algorithm, the definitions related to web service are presented at first.

Definition 1 User demands AQ. AQ=<ARGI, ARGO, QoS>, ARGI and ARGO are the input and output parameter of the network generated in form of <VAL, SL>, VAL represents the parameter value and SL is the security level of corresponding parameter; QoS is the users' demand of the web service quality, QoS=<cost, runtime, reliability, availability>, abbreviated as QoS=<c, rt, rty, aty>.

Definition 2 Network services call graph WSIG=<WS, AR>. Wherein, WS as an alternative network services set that can be decomposed into a plurality of sub-network service. AR is the set of <wsi, wsj> means that wsj is executed after wsi. Non-special case, ws0 is service requests node, wsn is service execution node, and all paths from ws0 to wsn are executable paths. Parameters of any network service are described in the form of <ND, TL>, ND is the node on a network service execution path, and TL is the trust level of the network execution node.

3.2. Judgement of Node Overflow

The rapid development of network technology has brought a rapid consumption of bandwidth and network congestion problems, and the multicast is a effective method for reducing bandwidth consumption. However, after 20 years of development, IP multicast in Internet has not achieved the desired success. The major factor that hinders the business development of IP multicast is that large-scale development of multicast technology on Internet is lack of an effective congestion control. Among that, the capacity of bandwidth is insufficient, the overflow of network nodes is one of the direct cause of congestion. According to Shannon information theory, the maximum value of any channel bandwidth is the channel capacity. If the entire source transmission rate is greater than the channel capacity, bandwidth bottleneck is formed at network low link, when it cannot satisfy the bandwidth requirements of all source passed it , the network congestion occurs. Therefore, in order to improve network multicast QoS, determine whether there is an overflow node is very necessary.

The judgment is on the foundation of the attribute characteristics of network-based IP data and concepts of the theory, combining the probabilistic planning system to determine the overflow of network node channel. If there is no correlation between every two in the m feature items $X_1, X_2, \cdots, X_m$ compose $\vec{X}$, the IP data attribute feature vector, the link between feature items should be removed, and then a simplified probabilistic model is obtained. If $c_1, c_2, \cdots, c_m$ represent the arranging condition of m types IP data and $X_1, X_2, \cdots, X_m$ indicate the m IP data feature items in the vector area, every two feature items X_p and X_q of channels X_p and X_q randomly selected are independent from each other. Therefore $U(\vec{X} = \vec{x} \mid z_j)$ the conditional probability of probabilistic classification models is:

$$U(X_1 = x_1, X_2 = x_2, \cdots, X_e = x_e \mid d_j)$$
$$= \prod_{i=1}^{e} U(X_i = x_i \mid d_j) \quad (1)$$

Probabilistic classification model is adopted to manage the data rationally. If $\vec{x} = \{x_1, x_2, \cdots, x_e\}$ is the eigenvector of IP data g, and $x_1, x_2, \cdots, x_e$ represent the eigenvalues. Therefore, according to the probability specification that:

(1) The probability that g belongs to classification z_l is ($l = 0$ indicates the conflict data and $l = 1$ means valuable IP data), which can be described by formula (2):

$$U(z_l \mid g) = U(z_l \mid \vec{X} = \vec{x}) = \frac{U(\vec{X} = \vec{x} \mid z_l) W(z_l)}{U(\vec{X} = \vec{x})}$$
$$= \frac{U(X_1 = x_1, X_2 = x_2, \cdots, X_e = x_e \mid z_l) U(z_l)}{\sum_{l=0}^{1} U(z_l) Q(X_1 = x_1, X_2 = x_2, \cdots, X_e = x_e \mid z_l)}$$
$$= \frac{U(z_l) \prod_{i=1}^{e} U(X_i = x_i \mid z_l)}{\sum_{l=0}^{1} U(z_l) \prod_{i=1}^{e} U(X_i = x_i \mid z_l)} \quad \text{u=0,1} \quad (2)$$

(2) The maximum posterior probability classifying IP data d is :

$$z_{MAP} = \arg\max_{z_{l=0,1}} U(z_l \mid g) = \arg\max_{z_{l=0,1}} U(z_l \mid \vec{X} = \vec{x})$$
$$= \arg\max_{z_{l=0,1}} U(\vec{X} = \vec{x} \mid z_l) U(z_l)$$
$$= \arg\max_{z_{l=0,1}} U(z_l) \prod_{i=1}^{z} U(X_i = x_i \mid z_l) \quad (3)$$

Wherein, formula (3) can be used to calculate priori probability $U(z_l)$. When feature items $X_1, X_2, \cdots, X_e$ independent from each other, classifying IP data to analyze whether the abnormal condition such as overflow and vibration appears or not.

3.3. Steps of the Algorithm

Based on the access request and network services required protection, considering the information leakage and the path relocation cost, an enhanced safety algorithm for QoS multicast network routing optimization based on PPCA is designed.

Among the statistical method based on non-supervision, principal component analysis (PCA) is the method used widely, PCA extract information from the explicit variables which can be observed to compose the implicit variables which cannot be directly observed. It is a linear mapping method, the principle adopted is to make the largest variance, to preserve as much of the information contained in the original variable, while using as little of main component instead of the original variables, so as to achieve the purpose of dimension reduction. Probability PCA is an extension of the traditional PCA, which is first proposed by Tipping and Bishop, its purpose is to define an appropriate probability model for PCA. In the traditional PCA, the information outside subspace is simply discarded, but in PPCA, this information will be estimated as Gaussian noise. Due to PPCA defines the probability model, it can be easily extended to hybrid model, and the parameters of model can be obtained by EM algorithm training.

Implementation process of PPCA can be attributed to three steps: create a network service digraph, access to network services selection tree and determine network services path.

Steps 1: Create a network service digraph

For each network service request, there may be multiple paths from the service launched node to service performed node. When the execution of network service failed, it is flexible to choose the best alternative path. Algorithm 1 shows how to create a web service call graph.

Algorithm 1 Input: WS, RQ Output: WSIG

```
for ∀ WSi ⊆ WS
AQ.ARGI= ws0, AQ.ARGO= wsi, 1 ≤ i ≤ n-1
add a ar=<ws0,wsi> to WSIGi.AR;
  for ∀ wsi ⊆ WSi
     if Max(wsi.ARGI.sl-wsi.tl) ≥ δ
     for ∀ wsj ⊆ WSi, i ≠ j
       if AQ.ARGOi ⊆ AQ.ARGIj
         add a ar=<wsi,wsj> to WSIGi.AR;
     end for;
   end if;
  end for;
add a ar=<wsj,wsn> to WSIGi.AR;
end for;
return WSIG
```

The above algorithm completes security access by comparing the security level of request parameters and trust level of the network service. δ represents the settable parameters of the user decision threshold access success rate which satisfy the Equation (4).

$$\varphi == \begin{cases} 0, k < -\delta \\ \dfrac{k+\delta}{2\delta}, -\delta \le k < \delta, k = ws_i.tl - Max(ws_i.ARGI.sl) \\ 1, k \ge \delta \end{cases} \tag{4}$$

The range of φ is [0, 1].

Steps 2: Access to network services selection tree

The logical relationship between the associated nodes of the network service can be described with WSIG. But due to the multi-path, the WSIG cannot clearly present the sequence of the network path. Therefore, to determine the execution path, it must be converted into logical tree, that is WSIG→WSIT.

Algorithm 2 Input: WSIG Output: WSIT

```
for NDi in WSIG sizeof(WSIGi.AR) is N
  if(N>1)
    Duplicate N sub-WSIGi in the NDi;
    for every sub-WSIGi
      While(N>=2)
        Let every incoming arrow point to NDi;
        N--;
      end while;
    end for;
  end if;
end for
return WSIT
```

The typical example of the method is shown as Figure 1. According to algorithm 1, the graph of network service is obtained, ND11 is the service request node, ND41 and ND42 are service execution nodes. Each path from request node to execute node is an executable path pth. WSIG is converted into WSIT by algorithm 2, and then we obtain the number of executable paths: I1×I2. The executable path set can be expressed as PTH={pthi| 1≤i≤I1×I2}, I1and I2are the nodes number product of each level between request nodes and execution nodes of the network service.

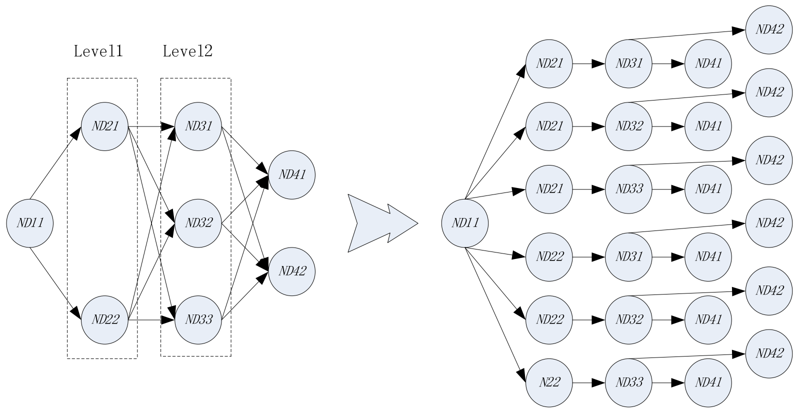

Figure 1. WSIG to WSIT

Steps 3: Determine network services path

When the WSIT is obtained, all of the execution paths can be backtracked from leaf node of WSIT. At the same time, the QoS between neighbor nodes can be calculated. The equation (5) is used to estimate the service performance of the current path.

$$\nabla\left(pth_i\right)=\frac{\varphi}{\eta} \tag{5}$$

η and φ are used to assess the quality of network services and access success rate of an executable path, which are determined separately v=by Equation (6).

$$\eta=\prod_{i=0}^{n}\left(\frac{1}{\sqrt{c^2\left(ws_i\right)+rt^2\left(ws_i\right)+1/rty^2\left(ws_i\right)+1/aty^2\left(ws_i\right)}}\right) \tag{6}$$

Wherein, c represents the resources consumption, rt is the running time, rty stands for the reliability, aty is the resource availability. The smaller η is, the higher the network service quality is leaf nodes in the tree diagram are network service execution nodes, from which backtracking can determine the execution path and its integrated service performance. According to the Qos order from high in the end, each node in the execution path is stored in the stack STK. If the high QoS execution path failed, the neighbor highest path QoS will be automatically selected to instead. The way from WSIT to determine PTH is shown as follow

Algorithm 3 Input: WSIT Output: PTH

```
cnode= NDend;
for every NDend in WSIT
  if ∃ WSIT.AR=<NDi,cnode>
   Push(cnode, stkj);
   if NDi=NDst;
     Generate a pthj and add to PTH;
end for;
```

Leaf node NDlf in WSIT is the final network execution node NDed.

4. Simulation and analysis

The PPCA algorithm considering access service information leakage and failure path re-election, so the simulation analysis can be based on two parts: 1) the network service quality evaluation. 2) Path service integrated performance and complexity analysis under certain network service success rate. Experimental environment is ThinkPad E50 Intel i3 2GHz processor, 2GRAM Windows7 operating system, and compiler is Microsoft Visual C + +2010.

Three group of network service testing data are given, formula (6) is used to compute the network quality of service assessment parameter η. Compared with the optimization method and the average value of the set of feasible solutions, the results are shown in Table 1.

Table 1. Testing Results of η

The group number of the test data	PPCA method	Optimal method	Average value
1	0.51	0.46	0.25
2	0.64	0.59	0.37
3	0.89	0.88	0.56

From the testing results of Table1 we can obtain that the η of proposed PPCA method is higher than that of optimal method. It is obviously that the PPCA is more suitable for selecting service path.

Network service access success rate is more difficult to assess due to the need to consider the relationship between the security level of the input parameters and trust level of network services. If $ws_i.tl - Max(ws_i.ARGI.sl) \geq \delta$ can be ensured, the access success rate is 100%. Actually, use the same test data, set δ=1, wsi.tl and wsi.ARGI.sl are randomly selected in range [0, 5]. $\nabla\left(pth_i\right)$ of executable path can be assessed by equation (6), the comparison results with optimal method are shown as Table 2.

Table 2. The Comparison Results of $\nabla\left(pth_i\right)$ Assess Results

The group number of the test data	PPCA method	Optimal method	Average value
1	8.7	8.4	7.9
2	11.3	10.9	8.8
3	19.2	15.7	13.6

From the testing results of $\nabla\left(pth_i\right)$, it can be obtained that the PPCA algorithm has the highest integrated assessment value in certain access success rate. That is to say PPCA algorithm chooses the best from queuing perform queue instead of reconstructing network access path when access failed, which reduce the complexity of the algorithm. The three groups of test data request can be divided into four categories {C2, C3, C4, C5} which means that the number of execution nodes meet network service request are 2-5. The algorithm complexity comparison test results are shown in Figure 2. The conclusion can be acquired that in the same condition, PPCA has the lowest compute complexity.

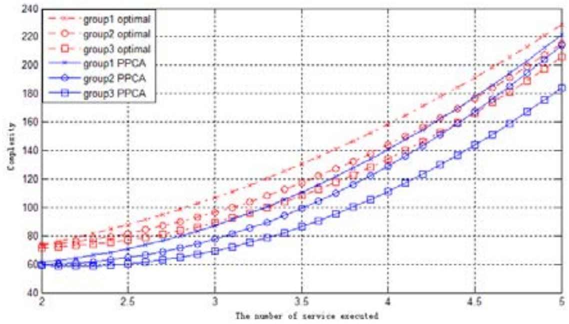

Figure 2. Comparison of the Complexity of the Algorithm

5. Conclusion

The current Internet provides only best-effort (best-effort Service) delivery service and sent it as soon as possible, there is no clear time and reliability guarantee. With the rapid development of multimedia technology of network, Internet multimedia applications are on emerging, such as IP telephony, video conferencing, and video on demand (VOD), distance education and other multimedia real-time services as well as e-commerce on the Internet transmission. Internet has gradually from a single data transmission network evolution to the integrated transmission network for data, voice, images and other multimedia information.

The development of the network also accelerated the development of the network multicast technology. It has been to a hot research field that multicast network because of its high efficiency, high scalability, saving the sender resources, etc., in these years. Multicast is between sender and multiple receivers to achieve multipoint network connection. If a sender to multiple receivers simultaneously transmit the same data, only a copy of the same data packet needed. It improves the data transmission efficiency and reduces the likelihood of backbone network congestion, and thus efficiently uses the network resources. Compared with unicast and broadcast technologies, multicast has the following advantages: (a) it saves the server load that the client-side who requires same data stream join to the same group to share a data stream, and have the advantages which broadcast possess. (b) Since the copy and forwarding of data stream in the multicast protocol is based on the needs of the recipient, the total bandwidth of the server's service is not limited by the access bandwidth of client-side, and their services can be very rich. (c) Multicast protocol like unicast protocol, they all allow the Internet transmission. Multicast applications can be divided into three categories: real-time interactive applications such as video conferencing systems; real-time but non-interactive applications such as datagram broadcast; non-real-time applications such as electronic document distribution.

However, the ensuing security issues of multicast have become the focus. Many factors that affect IP multicast security methods and mechanisms, which led to the network communication is very vulnerable to attack. If we do not protect the network service requester, it may reveal its own sensitive information. Based on this, we propose a security-enhanced access path - Strategy synthesis algorithm. It sets the constraints relationship between the security level of the input parameters of network service request and the trust level of network service, constructs directed multi-path network services graph. After converting WSIG to network service selection tree, the algorithm sorts and selects the best execution of all network services path according to the QoS size of paths through backtracking method. Comparing the simulation results with that of the traditional optimal path selection methods, the proposed algorithm has higher service quality and lower complexity level that can provide protection service composition to embedded network.

Principal component analysis (PCA) is a method which commonly used in multivariate statistical analysis. It does not depend on accurate mathematical model. It is mainly based on the original data space. In PCA, the process data and quality data from the high-dimensional data space projected onto a low-dimensional feature information space, the factors such as the too large space dimension of original data, serious related of variables, interference with unknown and low signal to noise ratio are removed, and the redundant information is abandoned. Then extract the major change information and statistical features from the new mapping space, which constitute the understanding of the original data with spatial characteristics.

Principal component analysis includes two functions of data reduction and data correlation extracted. The purpose of principal component analysis is by analyzing the reflected general information of original more observable data components to extract the small part of the data. And then, it takes advantage of the components of small part of the data to reflect the original data components contained more information to characterize the overall.

Overall, the principal component obtained through principal component analysis has the basic relationship between the original variables as the following aspects: (a) the main element retains most of the original variable information; (b) the main element The number is far less than the original number of variables; (c) each main element can be from the original linear combination of the variables; (d) there has no correlation between the main element, each containing information do not overlap. It is obvious that principal component analysis is not only a dimension reduction technique which can compress the number of indicators as possible, but also a comprehensive evaluation method.

The method of network traffic anomaly detection based on principal component analysis is an important branch of study in intrusion detection. It does not rely on mathematical models, can closely integrated with computer technology. The input of this method is based on sliding window of the source node of flow and the destination node (0D) matrix. It detects traffic anomalies through the determination of the PCA dimensionality reduction and the residual Q statistic threshold. Moreover, because of its high detection rate and resistance variants capabilities, it has increasingly widespread attention and application, as well as has important theoretical and practical value. Although PPCA algorithm presented in this paper is aimed for embedded system applications under the network environment, but it has some versatility. However, the algorithm has a good performance in certain premise, but it not yet fully consider the dynamic nature, which is the next step of research content.

References

[1] P Anyutin. Diffraction of plane and cylindrical waves by a cylindrical metamaterial shell with a negative refractive index. *Journal of Communications Technology and Electronics*. 2013; 58(2): 101-109.

[2] LIU Luo, GUO Li-Hong, XIAO Hui, Et al. Software Reliability Growth Model Based on Dynamic Fuzzy Neural Network with Parameters Dynamic Adjustment. *Computer Science*. 2013; 40(2): 186-190.

[3] Dongkyun Kim, Gicheol Wang, Gi-Sung Yoo, Seung-Hae Kim, Ok-Hwan Byeon. Media-Specific Network Service Environment on Federated Autonomous Distributed Networks. *IJACT*. 2013; 5(1): 659-667.

[4] BA Belyaev, AA Leksikov, AM Serzhantov, VV Tyurnev, Ya F Bal'va, An A Leksikov. Bandpass filter with an ultra-wide stopband designed on miniaturized coaxial resonators. *Journal of Communications Technology and Electronics*. 2013; 58 (2): 110-117.

[5] GUO Wei. Structural Optimization Algorithm for RBF Neural Network Based on Mutual Information. *Computer Science*. 2013; 40(6): 252-255, 271.

[6] Rongtao Ding. The Resource Scheduling Strategy for Occupation Ideal Network Games Based on Improved Hybrid Mutation Particle Swarm Algorithm. *JDCTA*. 2013; 7(2): 117-123.

[7] RB Vaganov, IP Korshunov, E N. Korshunova, A. D. Oleinikov. Experimental study of the field structure of the surface electromagnetic wave in an anisotropically conducting tape. *Journal of Communications Technology and Electronics*. 2013; 58(2): 118-123.

[8] Zhu Zhen. A Support Vector Machine Algorithm Based on Pretreatment of Neural Network Ensemble. *Bulletin of Science and Technology*. 2013; 29(4): 26-30.

[9] Anindita Kundu, Prasun Chowdhury, Iti Saha Misra, Salil K. Sanyal. QoS Aware Integrated Call Admission and Cognitive Channel Allocation Scheme for A Macro-Femto BWA Network. *RNIS*.2013; 11(47): 47-59.
[10] E. V. Sukhonin. On the issue of combined active-passive radio sounding of precipitation on radio-occultation paths. *Journal of Communications Technology and Electronics*. 2013; 58(2): 124-127.
[11] Hongyi Zhang, Zhidong Shen, Changsheng Zhang. A Non-Dominated Sorting Genetic Algorithm for the QoS Based Routing and Wavelength Allocation Problem. *JCIT.* 2013; 8(3): 560-567.
[12] Congcong Xiong, Long Feng, Lixian Chen. A New Task Scheduling Algorithm Based on Improved Genetic Algorithm in Cloud Computing Environment. *AISS*. 2013; 5(3): 32-38.
[13] JIANG Yun, CHEN Na, MING Li-te, et al. Bagging-based probability Neural Network Ensemble Classification Algorithm. *Computer Science*. 2013; 40(5): 242-246.