2018 International Conference on Computational Science and Engineering (ICCSE 2018)

Research on Network Load Balancing Algorithm based on Resisting Route Spoofing

He Yan

Chongqing Medical and Pharmaceutical College, Chongqing, 400030, China

heyanjsj@126.com

Keywords: Route Spoofing; Network; Load; Equalization

Abstract: Traditional load balancing methods mostly use non-interference network, which cannot balance the load in the channel in the case of resisting routing spoofing. Based on this, this paper proposes the method of network load balancing, constructs IS-IS anti-spoofing protocol, uses complete topology structure to eliminate the effect of routing spoofing, and optimize heads IS-IS anti-spoofing protocol and limit the occurrence of routing spoofing through characters; complete the formation of network load balancing protocol to resist routing spoofing through the design of LSP load balancing protocol; use channel model to design the steps of network channel load balancing, calculate the optimal load diversion, and realize network load balancing. The experimental results show that the designed load balancing method can balance the network load under route deception.

1. Introduction

In order to achieve network load balancing, multi-server and multi-channel are usually used to respond to external requests in a symmetrical manner. Each channel and server has the same status. However, under the interference of routing deception, there will be a certain overload phenomenon, which results in the unbalanced responsibility of network load balancing method. In this paper, we propose a method of network load balancing. The IS-IS anti-spoofing protocol is constructed by using the complete topology structure. LSP load balancing protocol and IS-IS anti-spoofing protocol header are optimized to complete the construction of the anti-spoofing routing network load balancing protocol. By calculating the best load shunting and channel model, the network load balancing is realized. In order to ensure the validity of the design, a simulation experiment is carried out in the setting environment. The results show that the load balancing method designed can be balanced under routing deception.

2. Building a load balancing Protocol against routing spoofing network

2.1 Construction of IS-IS anti-spoofing protocol

IS-IS anti-spoofing protocol adopts a complete hierarchical topology structure, which divides the whole protocol into two levels: the head of IS-IS anti-spoofing protocol and the executive part of IS-IS anti-spoofing protocol to increase the anti-routing spoofing function. The head of IS-IS anti-deception protocol mainly aims at the protocol scope of link state and channel state. The executive part of IS-IS anti-deception protocol realizes network load balancing by executing the creeds in the protocol area. The implementation of packet message mechanism in the built IS-IS anti-spoofing protocol can guarantee the complete elimination of routing data spoofing and information spoofing in the protocol area.

IS-IS anti-deception protocol defines two kinds of LSP load balancing processes. The first one is the transmission protocol through the intermediate channel. The protocol times the maximum LSP time interval and redistributes all the carrying information in the protocol definition area. The carrying capacity of information in the time interval will be self-contained along the content of the protocol definition. The final result of equilibrium is the average [2] of information data. The second is to balance the protocol channel in the structure by the structure, and distribute the idle

DOI: 10.25236/iccse.18.070

channel and the main channel uniformly, so as to ensure that the balanced load changes regularly.

2.2 IS-IS anti-spoofing protocol header design

The head part of IS-IS anti-spoofing protocol decides whether IS-IS anti-spoofing protocol can be successfully implemented. The length of IS-IS anti-spoofing protocol head is defined as 8 bytes of PDU code, and the overlapping TLV field can effectively resist routing spoofing. Table 1 shows the general field definition of the IS-IS anti spoofing protocol header designed in this paper is as follows.

Table 1. Definition of header field for IS-IS anti spoofing protocol

IS-IS anti spoofing protocol identifier	
Length of IS-IS anti spoofing protocol identifier	
ID extension of Protocol	
Version of Protocol	
Reservations	Tyte of Protocol
Network address	

2.3 LSP load balancing protocol design

LSP load balancing protocol contains all the basic data in network load, including adjacent data, IP address in channel connection, OSI network information call code, channel address, etc. [3]. LSP load balancing protocol has two main functions, one is load information two is balanced load.

In the process of load information, LSP Load Balancing Protocol will distribute all the load of supporting paths, and distribute the information reasonably by the amount of load to ensure that the load capacity of the channel is within a certain control range. In the process of load balancing, each load channel is downloaded to avoid channel pause caused by information overload. In the process of allocation, the load defined by LSP load balancing protocol is the upper limit and the lower limit is zero. The LSP load balancing protocol designed in this paper redefines the contents as shown in Table 2.

Tab.2 LSP load balancing protocol redefines content

PDU Length		
Remaining Lifetime		
LSP ID		
equence Number		
Checksum		
P	ATT	Overload

3. Realization of Network Load Balancing

3.1 The steps to achieve network channel load balancing are as follows

The construction of channel model can facilitate the rapid implementation of load balancing steps. Considering the impact of channel path information transition, the channel model designed in this paper is constructed using user AP signal. The power of AP signal is as follows:

$$p = \alpha^2 A d^{-1} p_t \qquad (1)$$

In formula (1), p_t denotes the carrying power of AP signal channel, assuming that the transmitting power of AP signal power in this paper is constant and evenly distributed on the transmission channel of channel; α denotes the effective mean of carrying capacity, and each effective value satisfies the result of information random variable, so as to represent the capacity of channel load. Ad^{-1} denotes the loss of information transition in channel. The value of d is determined by carrier frequency and network channel constant. The data value is proportional to the information attenuation index. The channel gain results can be determined through the load mode of the mobile channel, and the channel gain data are:

$$g = \alpha^2 Ap \tag{2}$$

In formula (2): g represents channel gain data.

The network channel load balancing steps are as follows:

1) When network information needs load balancing, channel time and location are allocated by AP signal power.

2) When the amount of information is larger than the set amount of channel, the channel gain data is used to expand the channel to ensure the channel balance.

3) The execution time is separated by time interval to ensure that each item's time interval is within a pause time.

4) Calculate the best load diffluence

5) Achieve network information load balancing.

3.2 Calculate the best load diffluence

Setting R and W as the total bandwidth of the network channel and the downlink power of the load, the load ability per unit bandwidth on the network channel is:

$$f = R / W \tag{3}$$

In formula (4), f represents the load capacity.

The capacity of the channel is usually set according to the definition of the protocol. Under the same broadband condition, the maximum information transmission rate is used to distribute the load. According to Shannon's transmission theory, if the pilot load force is K and the variance of network noise is N, then the channel load shunting capacity is

$$C = \frac{1}{2}\log_2\left(f + \frac{p}{N}\right) \tag{4}$$

Under the conventional channel constraint, the definition of each group will be amplified according to the degree of protocol. The best load diffluence is to obtain the limit value after enlargement, and the optimal load flow is:

$$C_J = \frac{1}{2}\log_2\left(1 + \frac{pm}{N}\right) \tag{5}$$

In formula (5), C_J represents the optimal load flow; m indicates the limiting value of the amplification factor.

4. Experimental Results and Analysis

In order to ensure the accuracy of the network load balancing method designed in this paper, a simulation experiment is designed. In the course of the experiment, a network is taken as the experimental object, and interference is carried out through various routes. The frequency of information transmission in the network is observed, and the experiment is recorded by the third-party software. In order to ensure the effectiveness of the experiment, the traditional network load balancing method is compared with the network load balancing method designed in this paper, and the results are observed. The flow chart of this paper is shown in Figure 2.

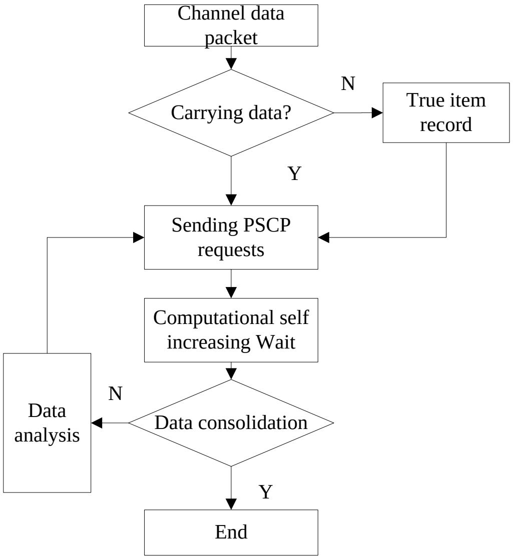

Fig. 2 test flow chart

4.1 Data preparation

In order to ensure the accuracy of the test process and set up the test data, the test object of this paper is the network. Because the results of network load balancing under different methods will change to some extent, it is necessary to ensure that the test environment parameters are consistent during the test process. The parameters are set as shown in Table 3.

Tab. 3 Experimental parameters

Parameter	value
Bandwidth	2.0GHz
Service generation interval	Poisson distribution
Traffic rate	50kb/s
BER parameters	10^{-3}
Channel noise power	-170dbm/Hz
Transmit power of access point	43dBm

4.2 comparison test results

This paper uses NS-2 platform to compare the performance of traditional load balancing algorithm and the anti-deception load balancing algorithm in the presence of interference network scenarios. The experimental results are shown in Figure 3.

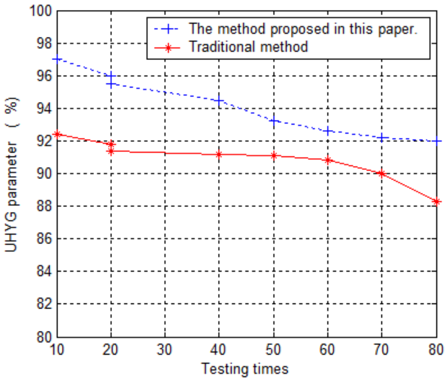

Fig.3 Comparison results of experiment

From Figure 3, we can see that the UHYG parameters of the network load balancing method designed in this paper are much higher than those of the traditional network load balancing method. The UHYG parameters can reflect the effect of load balancing, which shows that the network load balancing method designed in this paper has very high effectiveness.

5. Conclusion

A network load balancing method is designed in this paper. By constructing a load balancing protocol to resist routing spoofing, the network load balancing process can be realized by resisting the interference of routing spoofing. I hope that this research can enhance the effect of network load balancing.

References

[1] NI Xiao-jun, DUAN Yuan-xin, ZHANG Yun, et al. Research on Load Balancing Routing Strategy Based on Link Multi-index Evaluation System [J]. Computer Technology and Development, 2016, 26(6):46-50.

[2] DUAN Yuan-xin, NI Xiao-jun, ZHANG Yun. Investigation on Multi-index Comprehensive Evaluation for Load Balancing Algorithm [J]. Journal of Chinese Computer Systems, 2017, 38(2):209-212.

[3] ZHAO Hua-qiong, TANG Xue-wen. Evaluation model of network service performance based on fuzzy analytic hierarchy process [J]. Journal of Computer Applications, 2013,33(11):3035-3038.

[4] LIU Yong-bo, LIU Nai-an, LI Xiao-hui, et al.Load Balancing Routing Protocol Based on Traffic Prediction for Wireless Mesh Networks [J].Computer Science , 2017, 44(1):109-112.