A packet quantitative balance study on IP access network

Yan Yang, Wei Ding, Guang Cheng, Jian Gong

***Abstract*— Quantitative balance metrics of bidirectional packets for both TCP connection and IP access network are proposed in this paper. The former carries more semanteme and the latter is fit for application in high speed network. By the analysis of TCP protocol specification and the deduction of quantitative relation between the two, combined with the statistics in medicine, the model for the metric is established, in which two boundary lines are set as "red" and "yellow". This model provides a convenient and reltime method to evaluate the health of the network, which is helpful in the field of network management.**

***Index Terms*—access network, network management, packet balance metric**

I. INTRODUCTION

The rapid increase in scale has confronted the Internet with many challenges. Rapid traffic growth adds complexity to network management and puts new tasks for running the network. To resolve the problems efficiently so that the network can provide users with high quality services, a profound understanding of the network behavior and its characteristics is badly needed. Current research on Internet characteristics and user behavior is based on network measurement and traffic analysis, while the traffic analysis is performed on the basis of probability and statistics.

In Internet, TCP traffic is dominant in the whole network volume[1] and more than 90% of the Dos attacks use TCP[2], so its behavior predominates the network behavior, which makes it an important research issue in the study of network behavior. Therefore, network measurement should focus mainly on TCP traffic and in this paper, we mainly take TCP into consideration with regard to transport layer. Network measurement is based on network metrics so that the network users and ISPs can have a uniform understanding of the network performance. In RFC2330, metric is defined as "In the operational Internet, there are several quantities related to the performance and reliability of the Internet that we'd like to know the value of. When such a quantity is carefully specified, we term the quantity a metric.[7]" Network metrics can be differentiated as transport layer (especially for TCP) oriented and IP layer oriented. Most of the connection oriented metrics are stateful. It is difficult to calculate them on real time since maintaining the states of all the connections is required. However, TCP layer oriented metrics carry more semanteme and are easy for analysis and modeling. At the same time, IP layer oriented metrics are stateless and are easy to obtain on real time. They have few applications in network management and network security. However, its trait of realtime obtainment makes it a great advantage in occasions where real time is required.

The main contribution of this paper is to propose the connection oriented and access network oriented metrics and relate both. By developing the quantitative relation beween the two packet quantitative balance metrics, we convert the analysis of the former to the calculation of the latter. By referring to the methods used to establish boundary of medical metrics, we provide a method to identify the normal reference range for the latter metric to make it useful especially in occasions where real time is badly required. With this normal reference range, the quantitative balance metric of bidirectional packets which is access network oriented can help with the network management, user behavior analysis, overload balancing and the network QOS, as well as detecting the outburst traffic and abnormal traffic,so it is helpful in network management and network security.

The remainder of the paper is organized as follows. We summarize the related work in Section Ⅱ. Section Ⅲ introduces the data source used in this paper. Section Ⅳ gives the statistic and analysis of ratio of bidirectional packets in TCP connections. Section Ⅴ proposes some useful metrics for network management. Section Ⅵ illustrates the method to utilize the metric to evaluate the "health" of the network. Section Ⅶ describes the selection of time granularity for its application. Finally, conclusions are drawn in Section Ⅷ.

II. RELATED WORK

Currently, various metrics have been proposed for network management and inspection, but they are insufficient. Many mechanisms, especially in the field of network security to counter SYN flooding attacks, such as Syn cache [3], Syn cookies [4], SynDefender [5], Syn proxying [6] and so on, are

Manuscript received March 12, 2007. This work has been supported by the Key Project of Chinese Ministry of Education under Grant No. 105084, the National Grand Fundamental Research 973 program of China under Grant No. 2003cb314804, the Natural Science Fundamental of Jiangsu Province under Grant No. BK2006092, and the Excellent Youth Teacher of Southeast University Program under Grant No. 4009001018, and the Natural Science Fundamental of China under Grant No. 50609006.

All authors are with the Southeast University (e-mail: {yyang, wding, gcheng, jgong} @ njnet.edu.cn).

all stateful, that is, maintaining the states of all the TCP connections is needed, which largely degrades the end-to-end TCP performance and is inadequate for real time requirement.

About quantitative balance studies in network, there have been some findings. From the byte view(BPS) it is not symmetrical between the traffic that comes into and goes out of a network, however, it may be quite different from the packet view(PPS). [10] shows a macroscopical quantitative balance of TCP packets which are used to control TCP sessions, but the quantitative balance is aimed at TCP's control packets.

III. DATA SOURCE

The data for analysis comes from two traces, trace1 [8][9] was collected from the 100Mbps link of WIDE backbone across the Pacific Ocean in Janury 7th,2005. This 24-hour-long trace is mainly utilized to get the ratio of packets in both directions of TCP connection. Trace2 was collected by a platform for traffic measurement in high-speed network –WATCHER [11], which is run in the boundary of a provincial network of CERNET. Trace2 is collected in November 10th, 2005 and this 24-hour-long trace is mainly used for demonstrative analysis. It is collected using the method of passive measurement in the border router which connects the provincial network with the backbone. All the traffic that comes into and goes out of the provincial network passes through the boundary. The reason why we adopt this trace is that we can obtain all the constitution information of access networks.

IV. ANALYSIS OF RATIO OF BIDIRECTIONAL PACKETS IN TCP CONNECTIONS

A complete TCP connection includes three steps: connection establishment, data transmission and disconnection. The TCP connection establishment involves 3-way handshake, so the party which initiates the connection sends two packets and receives one packet; During the data transmission, since TCP uses Sliding Window Protocol to control traffic which enables the sender to send more than one packet before waiting for ACK, this mechanism indicates that there would be some relation between the number of packets sended and received; The disconnection involves a 4-way handshake and the sended and received number of packets for both parties are 2. It can be inferred from above that the number of packets in both directions has a proportional relationship. Denote the two parties in a TCP session X and Y , and the ratio of number of packets X and Y send $R_{X\to Y}$, if $R_{X\to Y}\in[a,b]$ when the error is %α, then call $R_{X\to Y}\in[a,b]$ satisfies with the error %α. When %α is small enough we can just regard $R_{X\to Y}\in[a,b]$ approximately satisfies.

Without loss of generality, we suppose the number of packets from X to Y is no less than that from Y to X in a complete TCP connection, then $R_{X\to Y}\in[1,\lambda_1]$ （$1<\lambda_1<\infty$） and $R_{Y\to X}\in[1/\lambda_1,1]$. Generally, no matter X or Y who sends more packets, it is always satisfied that the ratio of number of packets X and Y send :

$$R_{X\to Y}\in[1/\lambda_1,\lambda_1] \qquad (1)$$

To get the proportional relation between the number of packets in both directions of a TCP connection, we make a statistic of packets in trace1 in terms of TCP connection. In this experiment, we select 1000000 complete TCP connections from a successive time slot. Fig.1 gives the percentage of $R_{A\to B}$ in different ranges. So the number of TCP connections in range [1,2] is 951607, which makes up 95.2% of the total TCP connections, while the number of TCP connections in range [1,2.5] is 981435, which makes up 98.14% of the total

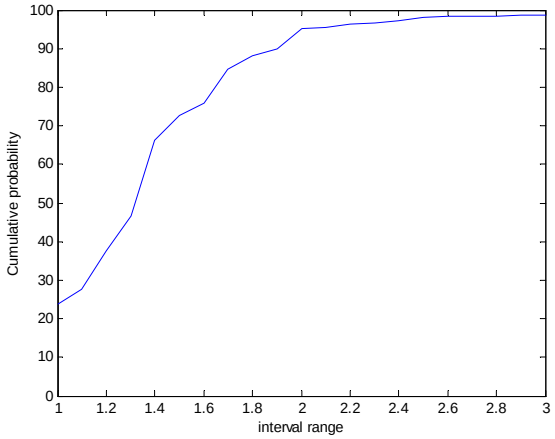

Fig. 1 Percentage of $R_{A\to B}$ in different ranges

TCP connections.

Set λ_1=2, then (1) turns to be $R_{X\to Y}\in[1/2,2]$ with %α =4.8%; Set λ_1=2.5, then $R_{X\to Y}\in[0.4,2.5]$ with %α=1.8%. In the following sections, we regard 5% as an error that can be accepted or even ignored,so generally there is:

$$R_{X\to Y}\in[1/2,2] \qquad (2)$$

V. DEFINITIONS AND PROPERTIES OF THE QUANTITATIVE BALANCE METRICS OF PACKETS

Definition 1 Given a time slot t, denote the number of packets that the access network receives $\lambda_{in}(t)$ and the number of packets that the access network sends $\lambda_{out}(t)$, define the function $x(t)=\frac{\lambda_{in}(t)}{\lambda_{out}(t)}$ as the ratio of in-and-out packets of the access network during the time period t.

Definition 2 Denote the TCP connection beween the access network and the outside network li, the number of packets that the access network receives in this connection $\lambda_{in}(li)$ and the number of packets that the access network sends in this

connection $\lambda_{out}(li)$, define the function $R(li)=\frac{\lambda_{in}(li)}{\lambda_{out}(li)}$ as the ratio of in-and-out packets of connection li.

$x(t)$ can be easily obtained from SNMP of routers of access network on real time and $R(li)$, according to the above analysis, can not be easily obtained on real time since the acquisition of the value needs to process the packets to compose flows. However, in the following discussion, we will try to find the quantitative relation between the two metrics.

Definition 3 Given a time slot t, denote the number of packets that the access network receives $\lambda_{in}(t)$ and the number of packets that the access network sends $\lambda_{out}(t)$, define function $d(t)=\frac{\lambda_{in}(t)-\lambda_{out}(t)}{\lambda_{in}(t)+\lambda_{out}(t)}$ as the quantitative balance metric of bidirectional packets for access network during the time period t.

Obviously, $d(t)=\frac{x(t)-1}{x(t)+1}$.

Definition 4 Denote the TCP connection between the access network and the outside network li, the number of packets that the access network receives in this connection $\lambda_{in}(li)$ and the number of packets that the access network sends in this connection $\lambda_{out}(li)$, define function $D(li)=\frac{\lambda_{in}(li)-\lambda_{out}(li)}{\lambda_{in}(li)+\lambda_{out}(li)}$ as quantitive balance metric of bidirectional packets for connection li.

Theorem 1: Suppose $R_{X\to Y}$, the ratio of number of packets in two directions of a TCP connection, is within the range $[a,b]$. If t is large enough and only TCP volume is considered, then the range of $d(t)$ is $[\frac{a-1}{a+1},\frac{b-1}{b+1}]$.

Proof: The ratio of number of packets in two directions of a TCP connection has been analysised above. Suppose $R_{X\to Y}$ is within $[a,b]$, then for the TCP connection between the access network and the outside network li, there is: $a \le R(li) = \frac{\lambda_{in}(li)}{\lambda_{out}(li)} \le b \Rightarrow a\lambda_{out}(li) \le \lambda_{in}(li) \le b\lambda_{out}(li)$. $d(t)=\frac{x(t)-1}{x(t)+1}$ is the increasing function of $x(t)$; $x(t)>1 \Leftrightarrow d(t)>0$, $x(t)\le 1 \Leftrightarrow d(t)\le 0$.

In the case that only TCP volume is considered, all the traffic of the acccess network is made up of TCP connections. When t is large enough, all the connections can be regarded as complete. Suppose the number of connections during t is n, then $\lambda_{in}(t)=\sum_{i=1}^{n}\lambda_{in}(li)$, $\lambda_{out}(t)=\sum_{i=1}^{n}\lambda_{out}(li)$; $\because a\lambda_{out}(li)\le\lambda_{in}(li)\le b\lambda_{out}(li)$,

$\therefore \sum_{i=1}^{n}a\lambda_{out}(li)\le\sum_{i=1}^{n}\lambda_{in}(li)=\lambda_{in}(t)\le\sum_{i=1}^{n}b\lambda_{out}(li)$; $x(t)=\frac{\lambda_{in}(t)}{\lambda_{out}(t)}=\frac{\sum_{i=1}^{n}\lambda_{in}(li)}{\sum_{i=1}^{n}\lambda_{out}(li)}$, $\Rightarrow a\le x(t)\le b$; Since $d(t)=\frac{x(t)-1}{x(t)+1}$ is the increasing function of $x(t)$, the range of $d(t)$ is $[\frac{a-1}{a+1},\frac{b-1}{b+1}]$.

According to the above analysis of formula (2) in section Ⅳ, we set a =1/2 and b =2, then $d(t)\in[-1/3,1/3]$ with the error 5%. Though UDP traffic accounts for a small part of the total network volumn , we can use a coefficient which is larger than 1 to reduce its influence. Since TCP traffic makes up 95% of the total traffic, we set this coefficient $1/0.95$ so that the range of $d(t)$ is enlarged to [-0.35，0.35].

The boundary line of range of $d(t)$ can be regraded as a cordon of the packet quantitative banlance of the network ("red cordon"). Inspecting the value of $d(t)$ can give us a perceptual understanding of the bidirectional packets of the access network. e.g, $d(t)$=0 means the number of packets that come into and go out of the access network is almost equivalent during this time period ; $d(t)\in(0,0.35]$ means the number of packets that come into is larger than that go out of the access network during this time period , and the closer it is to the upper bound of the range, the larger gap between the number of packets in the two directions; $d(t)\notin[-0.35,0.35]$, which indicates that $d(t)$ is out of the range, means something abnormal in the bidirectional packets of the access network during this period.

VI. THE METHOD TO EVALUATE THE HEALTH OF NETWORK BASED ON THE QUANTITATIVE BALANCE METRIC OF BIDIRECTIONAL PACKETS

A. The evaluation method

Whether the running state of the network is healthy can be reflected by a series of metrics, such as one-way delay, one-way packet loss and so on. While the definition of health in medicine is based on a series of metrics as well, such as blood pressure, blood sugar and so on, the method to evaluate the degree of health in medicine can give us some reference on that to evaluate the degree of health in network. In medical research, we usually gauge the metric of a group of homogeneous individuals in the case of unknown distribution to figure out the

normal reference range of this metric. In the case that the distribution of the quantitative balance metric of bidirectional packets is unknown, we can still figure out the normal reference range for this metric according to the medical statistics.

According to the medical method, most of the normal values measured should be within this normal reference range, where "most of" is regularly set 80%,90%,95% and 99%. A proper percentage is a key point to identify this normal reference range. In the case of unknown distribution, set the percentage index of α and β as the boundary line of the normal reference range. Using $d(t)$ to evaluate the quantitative balance of packets, there are （1+α%-β%）×100% networks whose metric $d(t)$ is out of the normal reference range. In medicine, α=2.5 and β=97.5 is generally adopted. Here we set α and β according to the network. We will give a normal reference range of "health" in terms of $d(t)$ based on trace2 and regard this normal reference range as another cordon of this metric("yellow cordon").

B. *Data analysis*

We take the 8-hour-long data(12:00~20:00) of trace2 and carry on analysis on the time granularity of 4 hours to satisfy the condition of "a time slot large enough". Withhold the individuals of the sample whose observation value is within the range $[-0.35,0.35]$ and then grouping and count the frequency of the individual observation values d (Set the groups 14 and group gap 0.05). The frequency distribution is shown in Fig.2.

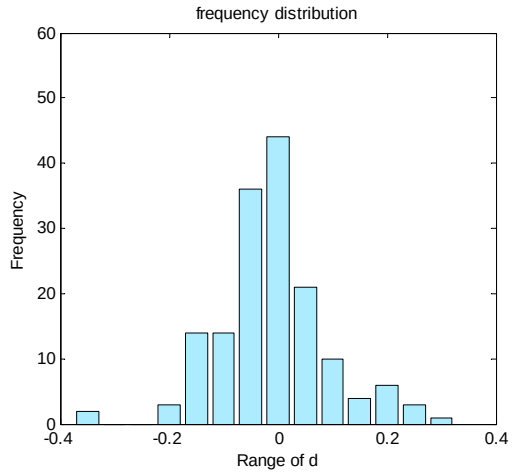

Fig.2 The frequency distribution of metric d

It can be figured out that the mean value of the metric $\overline{\eta}$ =0.014 and the standard deviation S =0.061. It can be seen that the distribution is almost symmetrical with a dense frequency in the central part and a gradually sparse frequency toward the two end sides (Regular check has been made and normal distribution is not testified).

In the case of unknown distribution, we set α=2.5 and β=97.5, which is commonly used in medicine, to get the normal reference range of d as $[-0.189,0.236]$. Therefore, we define the range $[-0.189,0.236]$ as "green" mean it is totally "healthy", $[-0.35,-0.189]$ together with $[0.236,0.35]$ as the "yellow" range to mean it needs watchfulness and that less than -0.35 or greater than 0.35 as the "red" range to mean something unusual.

In real circumstance, the following issues should be considered as well: ①For a certain access network, when d is within some range steadily, it is an indication of its network constitution. The value of d reflects to some degree the relation between the servers and the users inside the network, which is a relatively stable factor. ② For some access networks, the priority of the incoming and outgoing traffic may be different. When the traffic reaches its peak and some packets have to be discarded because of the restriction of bandwidth, buffer and processor capability, we can selectively discard packets with low priority in some direction according to the balance degree that d represents and the service level agreement as well. ③When d shows a large fluctuation. One possibility is burstiness of traffic which indicates that appropriate active queue management methods are needed; The other possibility is security attack which indicates that effective security detection module is needed.

VII. ANALYSIS OF TIME GRANULARITY

All the above analysis is based on the condition that the time granularity is large enough while the time granularity of 4 hours is unacceptable for the utility of the metric. In this section, we take an access network for example to analyze this problem based on statistics. This method is referred to [12], in which draw the widely accepted conclusion that the timeout of TCP flow can be set 64s.

Fig.3 shows the number of in-and-out packets of the network at the time granularity of 300s during 00：00~09：00. From the 9-hour-long traffic we can see that though the number of incoming and outgoing packets varies greatly in different time period, the number of packets sended is quite close to that received.

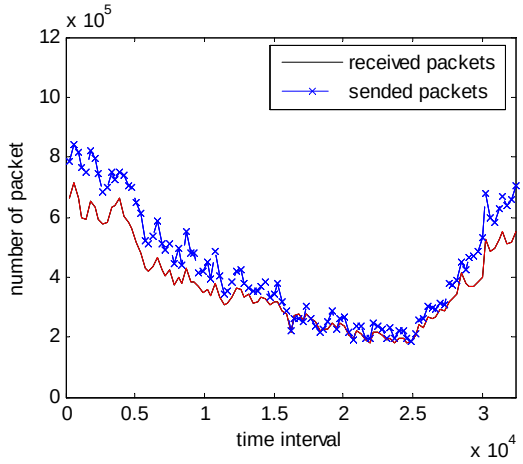

Fig.3 The number of in-and-out packets of the network in the time bin of 300s during 00:00~09:00

Fig.4 and Fig.5 show the value of metric at the time granularity of 600s and 300s respectively during 00：00~09：00. We can see that the trend of the two metric lines is almost homogeneous which indicates that there is no essencial

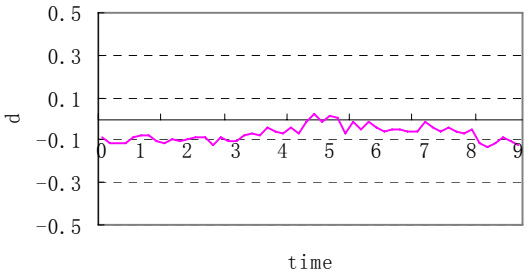

Fig.4 Values of $d(t)$ in the time bin of 600 seconds

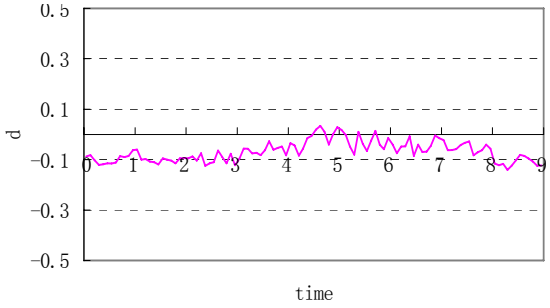

Fig. 5 Values of $d(t)$ in the time bin of 300 seconds

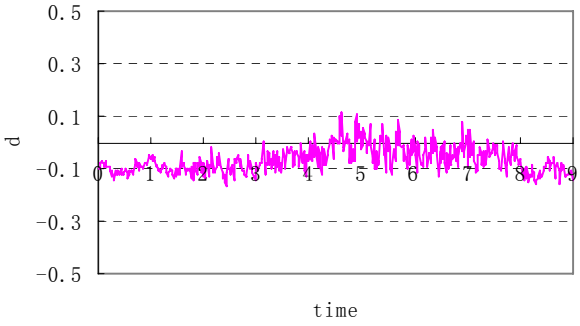

Fig.6 Values of $d(t)$ in the time bin of 60 second

difference between the selection of the two time granularities. When the time granularity is set 60s, there shows remarkable differences in some points. Therefore, we believe that the time granularity of 300s is appropriate.

VIII. RESEARCH CONCLUSION

To define reasonable and effective metrics is the demand of Internet measurement standardization, which is fundamental to the research of network behavior. The difficulty lies in two aspects: One is the acquirement of metrics(including two phases of parameter acquirement and calculation) and the other is to identify the boundary line of normal range. This paper begins with the quantitative balance metric of bidirectional packets and studies the issues in detail. We give the definition of metrics $d(t)$ and $D(li)$ from the perspective of accesss network and TCP connection respectively. According to Internet running rules, the cost of calculating IP layer oriented metrics is small since it can be obtained directly from router or channel data collection. However, the cost of calculating TCP layer oriented metrics is much larger since maintaining the flow information is needed though they carry more semanteme and are easy for analysis. So the acquirement of $d(t)$ is much easier than $D(li)$. Here we analysed the range of $D(li)$ based on the characteristics of TCP connection and discussed the method of mapping it to IP layer oriented metric $d(t)$. We also give the range $[-0.35,0.35]$ for $d(t)$ on the ground of real trace and statistical results and improved it by referring to medical statistics to get a more accurate range $[-0.189,0.236]$, through which we got the “red cordon” and “yellow cordon” for the health range of the metric thus made it a practical utility.

The significance of research in this paper lies in the method to obtain the bondrary line of the metric rather than the bondrary itself. On one hand, the boundary line, especially the “yellow cordon” can be adjusted according to the running state of the network; On the other hand, we hope that this kind of method can be applied in similar reseach for metrics, which is also a key point for our further research.

REFERENCES

[1] Marina Fomenkov, Ken Keys, David Moore, KC Claffy. “Longitudinal study of Internet traffic in 1998-2003.” In *Winter International Symposium on Information and Communication Technologies (WISICT)*, Cancun, 2004

[2] D. Moore,G.. Voelker and S. Savage, “Inferring Internet Denial of Service Activity”, *Proceedings of USENIX Security Symposium’ 2001*, August 2001.

[3] J. Lemon, “Resisting SYN Flooding Dos Attacks with a SYN Cache”, *Proceedings of USENIX BSDCon’2002*, Februrary, 2002.

[4] D. J. Bernstein and Eric Schenk, “Linux Kernel SYN Cookies Firewall Project”, http://www.bronzesoft.org/projects/scfw.

[5] Check Point Software Technologies Ltd. SynDefender: http://www.checkpoint.com/products/firewall-1.

[6] Netscreen 100 Firewall Appliance, http://www.netscreen.com/.

[7] V. Paxson. Framework for IP Performance Metrics, May 1998. Internet RFC 2330.

[8] WIDE MAWI WorkingGroup, “MAWI Working Group Traffic Archive”, http://tracer.csl.sony.co.jp/mawi/samplepoint-B/20050107/

[9] ftp://tracer.csl.sony.co.jp/pub/mawi/tools/tcpd-tools.tar.gz

[10] Gong Jian, Peng Yanbing, et al.. Macroscopical Quantitative Balance of TCP Packets. *Chinese Journal of Computers*, 2006, 29(9), 1561~1571

[11] Cheng Guang, Ding Wei, Gong Jian.General Platform for Traffic Measurement in High-speed Network-WATCHER. In *Proceedings of CSIT*, 2004, 122~128

[12] CLAFFY K C. *Internet Traffic Characterization*:[Ph D dissertation]. San Diego : University of California, 1994.