

Distributed Sampling Measurement Model in a Large-Scale High-Speed IP Networks^{*}

Gong Jian^{**}

Cheng Guang

(Department of Computer Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: The distributed passive measurement is an important technology for network behavior research. To achieve a consistent measurement, the same packets should be sampled at distributed measurement points. And in order to estimate the character of traffic statistics, the traffic sample should be random in statistics. A distributed sampling mask measurement model is introduced to tackle the difficulty of measuring the full trace of high-speed networks. The key point of the model is to choose some bits that are suitable to be sampling mask. In the paper, the bit entropy and bit flow entropy of IP packet headers in CERNET backbone are analyzed, and we find that the 16 bits of identification field in IP packet header are fit to the matching field of sampling mask. Measurement traffic also can be used to analyze the statistical character of measurement sample and the randomness of the model. At the same time the experiment results indicate that the model has a good sampling performance.

Key words: sampling measurement, bit entropy, matching field, identification field

At present there are mainly two kinds of measurement methods on network traffic, active measurements and passive measurements. Active measurements^[1] inject test traffic into network in order to measure network characteristics. But test traffic always generates additional load on network links and routers and may significantly influence the measurement results. In contrast to this, passive measurements rely on the traffic that already exists in the network. They provide a statement about the treatment of the current traffic at the observed network points. Since no test traffic is generated, passive measurements^[2] can only be applied in cases where the kind of traffic we are interested in is already presented in the network. Due to its high data volume and processing burden, it is very difficult to measure high-speed network traffic involved at the passive measurement points. In recent years there are some researches of distributed passive measurement architectures^[3-5].

In order to tackle the high-speed traffic in passive measurement, early in 1993, Claffy^[6] processed NSFNET measurement and firstly took statistic sampling technology to study classical event and time driven sampling methods to reduce the number of packets that would need to be received and processed by a network management node. J. Drobisz, et al^[7] believed that static traffic sampling method might produce inaccurate traffic static materials. In that paper, the static sampling method of Claffy was improved and a new self-adapted sampling method was

developed. RFC2330^[8] has analyzed the randomness of sampling measurement and suggests that Poisson sampling is fit to sample measure high-speed network traffic. These sampling models can only be used to single-point measurement architecture. In order to use sampling technology in distributed measurement architectures, some distributed sampling models are proposed. I. Cozzani^[5] proposes a sampling model that identifies a sampling event occurrence when particular function of the bit patterns in ATM cell's payload is met and the checksum data is used for the sampling selection plane. But according to that paper, the randomness of checksum data isn't very good, and the checksum fields will be changed when IP packet is transferred in network. So it is difficult to assure to sample the same IP packets at distributed measurement points. N. Duffield^[4] proposes to base the sampling decision on a deterministic hash function over the packet's invariant content. But it is difficult to assure the randomness of the hash function, and the model needs to have longer sampling time.

Two problems should be considered for distributed passive measurements on IP network traffic: high-speed traffic measurements and the consistency among different measurement points. Sampling technology is to decrease data amount used in measuring, storing and processing under the precision required. In order to coordinate the measurement results in distributed measurement environment, it is necessary to assure the same sampling results achieved at different measurement points. In this paper, a distributed sampling

mask measurement model is introduced which is based on the analysis for a great deal of measurement network traffic which comes from CERNET backbone. The distributed sampling model can not only embody the random character of sampling results but also realize the cooperation of data.

This paper is structured as follows. Bit entropy and the sampling mask measurement model are defined in section 1. Then, in section 2 we find that the identification field of IP header is an ideal matching bit flow. In section 3, we discuss the performance of the sampling model based on identification field. The paper is concluded in section 4.

1 Distributed Sampling Measurement Model

1.1 Definition

Entropy^[9], an important concept of information theory, is used in this paper to measure the random degree of bits in IP packet. Some important entropy concepts in sampling measurement model as the metric of traffic randomness are defined as follows.

Definition 1 Bit entropy that is the entropy value of a bit in IP packet header is defined as

$$H(b) = -(p_0 \log_2 p_0 + p_1 \log_2 p_1) \quad (1)$$

where b is 0 or 1 event of a bit; p_0 is the probability of 0 event, and p_1 is the probability of 1 event.

Theorem 1 (the maximal bit entropy theorem): If both p_0 and p_1 have the same probability, $p_0 = p_1 = 1/2$, then the bit entropy value is maximal. So the maximal bit entropy value is $H_{\max}(b) = 1$.

Prove Suppose that p_0 and p_1 are continuous because the number of IP packets used for statistical analysis are larger than 10 000 000, Eq. (1) is also considered a two dimension continuous function. $p_0 \in (0, 1)$, $p_0 + p_1 = 1$, $p_1 = 1 - p_0$, if p_1 of Eq. (1) is replaced by $1 - p_0$, then Eq. (1) is transformed into Eq. (2).

$$f(p_0) = -[p_0 \log_2 p_0 + (1 - p_0) \log_2 (1 - p_0)] \quad (2)$$

In order to obtain the maximal value of function $f(p_0)$, we compute the derivation function of equation $f(p_0)$ and assure $f'(p_0) = 0$.

$$f'(p_0) = \log_2 p_0 + \frac{p_0}{\ln 2} \cdot \frac{1}{p_0} - \log_2 (1 - p_0) - \frac{1 - p_0}{\ln 2} \cdot \frac{1}{1 - p_0} = 0 \quad (3)$$

So $p_0 = 1 - p_0$, $p_1 = p_0 = 1/2$, $f'(p_0) = 0$. $p_0 = p_1 = 1/2$ is the extremum point of Eq. (2).

Now we prove that $p_0 = p_1 = 1/2$ is the maximal value point. First we compute the two moment

derivation function of $f(p_0)$, $f''(p_0) = \frac{1}{\ln 2} \cdot \frac{1}{p_0} + \frac{1}{\ln 2} \cdot \frac{1}{1 - p_0}$. Due to $p_0 \in (0, 1)$, $f''(p_0) > 0$, $p_0 = p_1 = 1/2$ is the extremum maximum point of $f(p_0)$.

Considering both $p_0 = 0$ or $p_0 = 1$ are either an improbable event or a certain decided event, so the bit has not any information. Since $\lim_{\epsilon \rightarrow 0} \log \epsilon \rightarrow 0$ can be proved easily, $0 \times \log_2 0 = 0$, then $f(0) = 0 \times \log_2 0 + 1 \times \log_2 1 = 0$. $f(1) = f(0) = 0$. According to the above discussion, $p_0 = p_1 = 1/2$ is the maximal value point of $f(p_0)$ and the maximum of bit entropy $H_{\max}(b) = 1$.

Definition 2 The information efficiency E of bit entropy that is the ratio between $H(b)$ and $H_{\max}(b)$ is the metric of bit randomness.

Due to $H_{\max}(b) = 1$, $E = H(b)/H_{\max}(b) = H(b)$, $0 \leq E \leq 1$. If E approaches 1, then the randomness of the bit is large. And if E approaches 0, then the information of the bit is certain and bit entropy is small.

Definition 3 The bit redundant degree $R = 1 - E = 1 - H(b)/H_{\max}(b) = 1 - H(b)$. E is the random metric of bit, $(1 - E)$ is the certain degree of bit information.

1.2 Sampling measurement model

The sampling measurement on high-speed IP traffic is aimed at selecting partly traffic to estimate the total traffic information. The sampling theory is based on randomness. The more random the sample is, the more precise the general information is estimated. In the paper, according to the random character of packets in high-speed network, two ways to reflecting the sampling measurement are discussed and advanced.

A kind of sampling method is that the sampling event is generated by sampling model randomly, but the sampling event is specific itself. For example, Poisson random sampling randomly generates packet number or time. Before a packet arrives, we have known whether the packet will be sampled. This kind of sampling method now is mainly used in passive measurements, such as mentioned in RFC2330. However this sampling method can only be used in a single-point measuring architecture. The other sampling measurement method that has been studied in this paper is based on the sampling event generated by specific sampling model, yet the static attributes of sampling event are random statistically. After a packet arrives, according to its content, we can know whether the packet is sampled. For example we can define a specific mask and compare the mask with some bits of

the arrived packet, and the bits of the packet are random statistically. The shared sampling mask can not only assure that the same packets will be measured at different measuring points, but also realize the randomness of measuring packet samples. Both the offset of the matching bits and the length of bit mask may decide the precision and reliability of measurement architecture. A sampling mask measurement is shown in Fig.1. The measuring points are distributed near network backbone routes, and the simplest measuring architecture is composed of two measuring points and one routing. Then we can measure the end-to-end network performance between the two measuring points with the sampling measuring architecture.

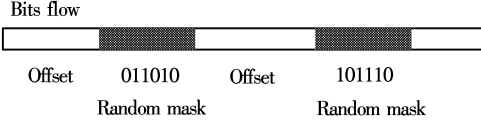


Fig.1 Sampling model

2 Statistical Analysis of IP Header

2.1 Bit entropy analysis of IP header

In the paper, we develop a measurement system for measuring the traffic in CERNET backbone link that is based on 1 Gbit/s network card, PIII 1G CPU, and Red Hat Linux6.2 operation system. We have measured about 10 000 000 packets from the measurement point and analyzed these IP packet headers statistically with 20 bytes and 160 bits. The structure of IP header is shown in Fig.2. We find the entropy of identification field is very high and its content will not be changed during transportation.

Version field contains the protocol version of packet. However all measured packets are IPv4, so information efficiency of its bit entropy is $E = 0$, and bit redundant $R = 1$. The IHL of all measured packet is 5. So IHL field also expresses a certain value. In TOS field only 0.021% packets are expressed from the 1th to the 3th bits. 2.55% packets with the 4th bit, 2.98% packets with the 5th bit, 0.03% packets with the 6th bit. The bit entropy from the 4th to the 6th bit is 0.171, 0.193 and 0.004, respectively. The last two bits aren't defined. These data indicate that the bit entropy of TOS field is very low, and some bits can be changed when packets go through network routers, so TOS field isn't considered as the matching bit flow of sampling mask.

The packet length is mainly 40, 552, 576 and 1 500 bits. The entropy efficiency E of packet length field is shown in Fig.3. The figure shows that E of the first byte is very low, and the E of the second byte is

0		8		16		24		32	
Ver	IHL	TOS		Total length					
ID				Flag	Offset				
TTL		Protocol		Checksum					
Source IP									
Destination IP									

Fig.2 Structure of IP header

larger than 90%. But the packet length field can be changed through network.

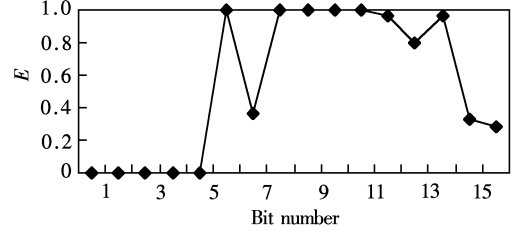


Fig.3 E of packet length field

The identification field usually is the most entropy field of the IP packet header. Therefore it is suitable for the matching with bits of the sampling mask. As shown in Fig.4, the E of identification field is larger than 99%. It can also be shown that the randomness of identification field is very high, and the 16 bits of identification field fits the matching bits. The first bit of

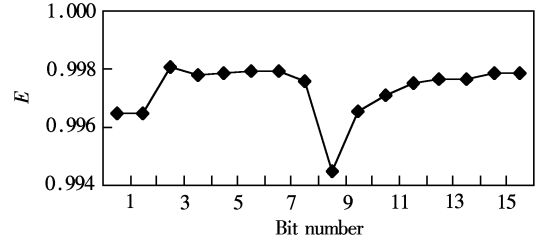


Fig.4 E of identification field

Flag field isn't used, the second bit DF with 88.7% and the third bit MF with 0.31% statistically. Fig.5 shows the E of fragment field. Obviously it doesn't fit

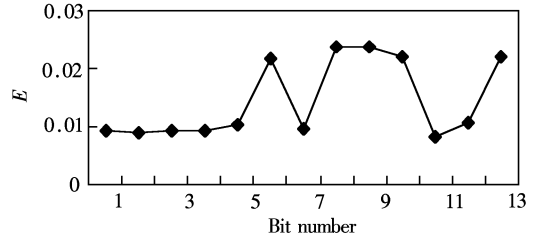
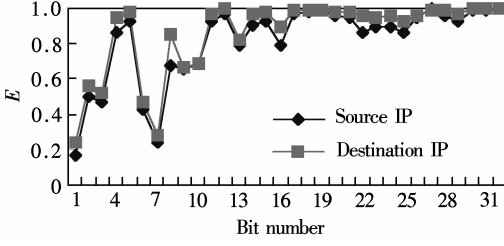


Fig.5 E of offset field

the matching bits of sampling mask. TTL is decremented per hop. Protocol field^[10] has low bit entropy, which takes only several values, TCP(6) 93.04%, UDP(17) 6.37%, and others 0.59%. The entropy efficiency E of destination IP and the source IP is shown in Fig.6 which indicates that the E of the last 16 bits of two IP address fields are larger than 90%, so they can be considered as the matching bit.

Fig. 6 E of IP field

According to the bit entropies of each field in IP packet header, we find that the 16 bits of identification field, the later 16 bits of both source IP and destination IP address possess unchanging character with high efficiency of bit entropy information during transportation. So in the paper the above three bit flows are chosen as the matching bits and the relation among 16 bits of 3 bit flows will be analyzed as the following.

2.2 Bit flow entropy analysis

Firstly, we give the definition of bit flow entropy and the maximal bit flow entropy theorem.

Definition 4 Bit flow entropy is the entropy of bit flow. s bits have $n + 1 = 2^s$ events, and their probability are respectively p_0, p_1, \dots, p_n , so bit flow entropy $H(s)$ is defined.

$$H(s) = - \sum_{i=0}^{2^s-1} p_i \log_2 p_i \quad (4)$$

Theorem 2 (the maximal bit flow entropy theorem): If the 2^s events of s bit have the same probability, that is to say, $p_0 = p_1 = \dots = p_n = 1/2^s$, its bit flow entropy is maximal, and its value is

$$H_{\max}(s) = - \sum_{i=0}^{2^s-1} \frac{1}{2^s} \log_2 \frac{1}{2^s} = s \quad (5)$$

Prove The same as theorem 1, we consider Eq. (4) also is a continuous function, and theorem 2 is an optimal problem. Namely, it is expressed as

$$f(X) = - \sum_{i=0}^n p_i \log_2 p_i \quad (6)$$

$$X = (p_0, p_1, \dots, p_n)^T \in D$$

under conditions $\sum_{i=0}^n p_i = 1, p_i \in (0, 1), n = 2^s - 1$, to look for a maximal value.

So we need to find out a set of parameters value $X^* = (p_0^*, p_1^*, \dots, p_n^*)^T$ in D to obtain $\max f(X) = f(X^*)$. First we transfer the limited problem into an unlimited problem. The limited condition is transferred into $p_0 = 1 - \sum_{i=1}^n p_i = 1 - S, S = \sum_{i=1}^n p_i$, and p_0 of Eq. (6) is replaced with $1 - S$, and Eq. (7) is obtained.

$$f(X) = - \sum_{i=1}^n p_i \log_2 p_i -$$

$$(1 - \sum_{i=1}^n p_i) \log_2 (1 - \sum_{i=1}^n p_i) \quad (7)$$

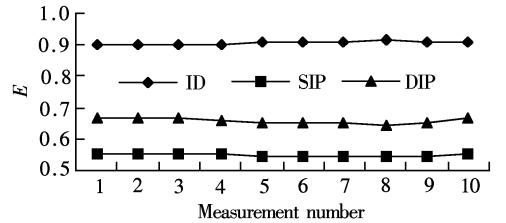
If $X^* = (p_1^*, p_2^*, \dots, p_n^*)^T$ is the extremum of $f(X)$, then we can get the gradient vector $\nabla f(X^*) = (\frac{\partial f}{\partial p_1^*}, \frac{\partial f}{\partial p_2^*}, \dots, \frac{\partial f}{\partial p_n^*})^T = \vec{0}$, and the gradient vector contains the condition, and Eq. (8) is obtained.

$$\left. \begin{aligned} \frac{\partial f}{\partial p_1^*} &= \log_2 p_1^* - \log_2 \sum_{i=1}^n p_i^* = 0 \\ \frac{\partial f}{\partial p_2^*} &= \log_2 p_2^* - \log_2 \sum_{i=1}^n p_i^* = 0 \\ &\vdots \\ \frac{\partial f}{\partial p_n^*} &= \log_2 p_n^* - \log_2 \sum_{i=1}^n p_i^* = 0 \\ \sum_{i=0}^n p_i^* &= 1 \end{aligned} \right\} \quad (8)$$

If $p_0^* = p_1^* = \dots = p_n^* = \frac{1}{n+1} = \frac{1}{2^s}$, then the same as theorem 1, we can prove that X^* is maximal point. So the prove is finished.

Definition 5 The information efficiency E of bit flow is the ratio between $H(s)$ and $H_{\max}(s)$ and the metric of bit flow randomness, $E = H(s)/H_{\max}(s) = H(s)/s$.

The IP traffic of CERNET backbone is measured 10 times at different time, each time with 1 000 000 packets. The information efficiency of the three bit entropy mentioned above is compared and the results are shown in Fig. 7. For the identification field, the minimal information efficiency E of 16 bits is 0.901, with the maximum $E = 0.915$ and wave range 0.014, the later 16 bits of source IP with the minimal $E = 0.648$, the maximum $E = 0.668$ and wave range 0.020, the later 16 bits of destination IP with the minimal $E = 0.544$ and the maximum $E = 0.556$ and wave range 0.012. Considering the stability character, 16 bits in identification field are chosen as random sampling matching bits.

Fig. 7 Comparison of E

3 Performance Analysis of Sampling Measurement Model

According to above analysis, we choose from 0th bit to 16th bits of the identification field as sampling

matching bits, so the ratio of sampling can be from 1 to 2^{16} , the maximal sampling ratio can be 65 535. Now a common PC can deal with 10 Mbit/s traffic easily, so theoretically speaking, this model can sample 640 Gbit/s traffic. The sampling measurement is mainly bit operation which can easily be carried out through hardware, so this sampling measurement can be implemented in network card.

3.1 Randomicity analysis of the sampling model

The offset of the sampling model based on identification field, that is a fix value, is defined as the start position from the header of identification field, and the maximal mask length is 16 bits. Fig.8 is the bits E statistics analysis of 10 000 000 packets from CERNET backbone. In Fig.8, the minimal bits entropy is larger than 0.90, so the identification field is very random and its autocorrelation is very small.

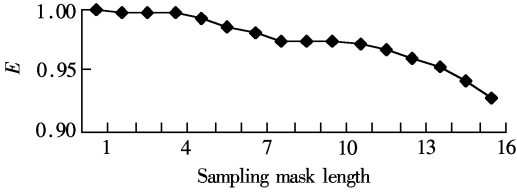


Fig.8 Comparison of the bits E

The relation between sampling mask length and sampling ratio is shown in Fig.9. If the sampling mask length is n bits, then the theory sampling ratio $1/2^n$, and have 2^n masks corresponding to sampling ratios. The maximal ratio, minimal ratio, median ratio, 95% ratio, and 5% ratio are listed respectively. Except the maximal ratio, the other sampling ratios draw near because the full 0 bits of identification field is higher than other bits. So we don't choose the full 0 bits as the sampling mask. Through Fig.9 it can be proved that the identification field owns a good randomicity and it fits to matching bits.

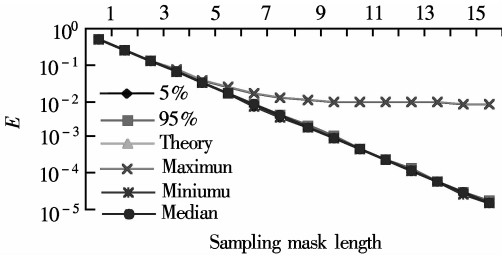


Fig.9 Relation between sampling ratio and mask length

3.2 Statistics character of traffic sample

We will use χ^2 distribution to perform tests of the independence hypothesis of the packet length, source IP, and protocol from the samples and the full traffic. Supposed that the statistical distribution of the full traffic is $F_0(x)$, and the sample statistics is $F(x)$.

For a given confidence level α ($\alpha = 0.05$ or 0.01), independence hypothesis $H_0: F(x) = F_0(x)$ is tested by χ^2 distribution^[11]. Consider the given character of the set of packets (protocol, packet length, and source IP), we divide the range value of the full traffic into the number I of bins, with n_i packets falling in bin i ,

the number of full packets are $n = \sum_{i=1}^I n_i$. If there are m_i packets in bins i , then the number of sampling packets are $m = \sum_{i=1}^I m_i$. So there are $u_i = n_i - m_i$ packets unsampled in bins i . The χ^2 distribution statistics is

$$\chi^2 = \sum_{i=0}^{I-1} \frac{(m_i - n_i p)^2}{n_i p} \sim \chi^2(I-1) \quad (10)$$

where p is the sampling ratio, $n_i p = n_i \times m/n$ is the number of sample packets in theory.

For a given confidence level $\alpha = 0.05$ or 0.01 , if $\chi^2 < \chi^2_\alpha$, we accept the hypothesis. χ^2_α is the α th quantile of χ^2 distribution with $I-1$ degrees of freedom. The statistical attributes of the prefix of source IP, packet length, and protocol are tested with matching bits from 1th to 16th bits of identification field in turn. In the test, there are 10 000 000 packets, and the sampling mask of sampling model is 1, 10, 101, 0110, 10111, 101011, 1010111, 10100100, 110011101, 1010111000, 11110000111, 000011110000, 1010101010101, 10000001110010, 011000101110000, 0010101011101101, respectively.

In the experiment, the prefix of source IP is tested with $I = 2^5$. Due to the packet length between 40 bytes and 1 500 bytes, a bin per 30 bytes, so 49 bins are built. The protocols are classified as TCP, UDP, and others, so 3 bins are set. Since the number of protocol bins is very little, unsampled bins are also considered. So the number of protocol bins is 6, TCP bin (m_0), UDP bin (m_1), others bin (m_2), u_0 , u_1 , and u_2 . In order to reduce the estimated error, if the theory sampling number in i bin is less than 5, then different bins will be united. The results of test hypotheses are shown separately as hypothesis distribution of protocol in Fig.10, hypothesis distribution of packet length in Fig.11, and hypothesis distribution of source IP prefix in Fig.12. From these figures, for a given confidence level α ($\alpha = 0.05$ or 0.01), $\chi^2 < \chi^2_\alpha$, we accept the hypothesis H_0 , and believe the same statistics distribution between the sample traffic and the full traffic.

4 Conclusion

In the paper, information theory is applied to analyze the bit entropy of IP header measured from

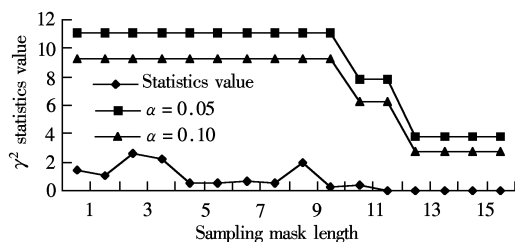


Fig. 10 Hypothesis distribution of protocol

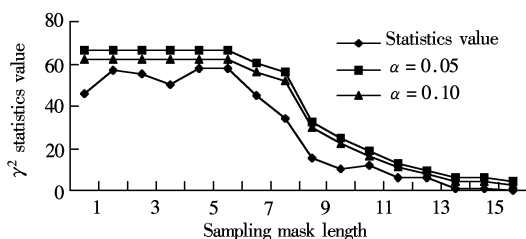


Fig. 11 Hypothesis distribution of packet length

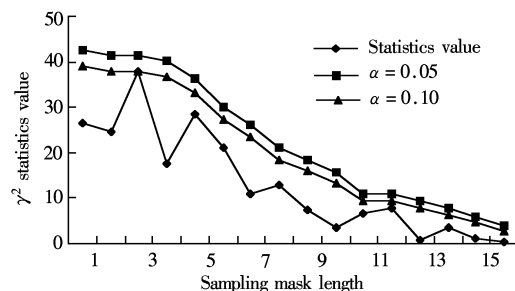


Fig. 12 Hypothesis distribution of IP address prefix

CERNET backbone network. Through analysis we find four reasons that the identification field is suitable to be sampling matching bits. Firstly during transportation the identification field content will not be changed. Secondly its bit entropies and bits entropies are much higher than all other fields in IP header. Their information efficiencies are more than 99% and the information efficiency of 16 bits entropy also can reach 90%. Thirdly, compared with other fields such as packet length and IP address etc. the content in identification field has better randomness, it does not

contain correlative information with packet content. Finally the 16 bits is enough to satisfy the developing requirement of future network bandwidth, we can use these bit masks only to control the sampling measurement. So in this way not only can network burden be decreased but also sampling configure can be simplified greatly.

References

- [1] Huffaker B, Fomenkov M, Moore D, et al. Measurements of the internet topology in Asia-Pacific region[EB/OL]. http://www.caida.org/outreach/papers/asia_paper/, 2000.
- [2] Graham I D, Donnelly S F, Martin S, et al. Nonintrusive and accurate measurement of unidirectional delay and delay variation on the internet[A]. In: *Proc. INET'98*[C]. July 1998.
- [3] Zseby T, Zander S, Carle G. Evaluation of build blocks for passive one-way-delay measurements, PAM2001, In Amsterdam USA, 2001. 10.
- [4] Duffield N, Grossglauser M. Trajectory sampling for direct traffic observation[A]. In: *Proceedings of ACM SIGCOMM 2000*[C]. Stockholm, Sweden, August 28 - September 1, 2000.
- [5] Cozzani I, Giordano S. A passive test and measurement system: traffic sampling for QoS evaluation[A]. In: *Proc. of IEEE Globecom'98 Sydney*[C]. Australia, November 1998.
- [6] Claffy K, Polyzos G, Braun H. Application of sampling methodologies to network traffic characterization[A]. In: *Proceedings of ACM SIGCOMM'93*[C]. May 1993.
- [7] Drobniz J, Christensen K J. Adaptive sampling methods to determine network traffic statistics including the hurst parameter[A]. *23rd Annual Conference on Local Computer Networks* [C]. October 11 - 14, 1998.
- [8] Paxson V, Almes G, Mahdavi J, Mathis M. Framework for IP performance metrics, IETF RFC 2330, 1998.
- [9] Jin Zhenyu. *Information theory*[M]. Beijing: Beijing University of Science and Technology Press, 1991. 11 - 47. (in Chinese)
- [10] Reynolds J, Postel J. Assigned numbers, IETF RFC1700, October 1994.
- [11] Tang Xiangneng, Dai Jianhua. *Mathematics Statistics* [M]. Beijing: Mechanism Technology Press, 1994. 140 - 151. (in Chinese)

大规模高速 IP 网络分布式抽样测量模型

龔 俭 程 光

(东南大学计算机科学与工程系, 南京 210096)

摘 要 分布式被动测量是研究网络行为的一个重要手段. 为了获得分布式协同处理流量信息, 要求分布的测量点能抽取同样报文; 为了能估计流量总体统计属性, 抽样样本需要具有统计随机性. 为此, 文章提出分布式掩码抽样测量模型处理高速网络流量, 其核心是确定合适的抽样掩码匹配位串. 对 CERNET 主干网络流量 IP 报头各字段的位熵和位流熵进行分析, 结果表明标识字段 16 比特适合于抽样掩码匹配字段. 使用测量数据分析基于标识字段抽样模型的随机性和抽样样本的统计属性, 实验进一步验证了所提出的模型具有良好的抽样性.

关键词 抽样测量, 位熵, 匹配字段, 标识字段

中图分类号 TP393.07