Distributed Sampling Measurement Model in a Large-Scale High-Speed IP Networks

Guang Cheng, Jian Gong (gcheng, jgong@njnet.edu.cn)
（Computer Department of Southeast University, NanJing 210096）

Abstract: The distributed passive measurement is an important technology for network behavior research. It is very difficult to measure the full trace of high-speed networks, so in the paper sampling technology is introduced into traffic measurement. Usually there are two main problems that should be solved in the distributed passive measurement. In order to corporate the distributed traffic information, the same packets should be sampled in distributed measurement points. Besides in order to estimate the character of traffic statistics, the traffic sample should be random in statistics. So a distributed sampling mask measurement model based on traffic statistics analysis is advanced and the key point of the model is to choose some bits that are suitable to sampling mask. In the paper, the bit entropy and bit flows 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 analysis the statistical character of measurement samples and the randomicity of the model. At the same time the experiment results indicate that the model has a good sampling performance.

Key Words: sampling measurement, sampling mask, bit entropy, matching field, identification field

1. Introduction

At present there are mainly two kinds of measurement methods [1-3] on network traffic, active measurements and passive measurements. Active measurements [4-10] inject test traffic into network in order to measure network characteristics. But test traffic always generates additional load on network links and routers and can 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 in observed network point. Since no test traffic is generated, passive measurements [11-15] can only be applied in cases where the kind of traffic we are interested in is already present in the network. But it is difficult to measure high-speed network traffic and involve the distributed passive measurements points. In recent years there are some researches of distributed passive measurement architectures [16-19].

In order to solve the high-speed traffic in passive measurement, early in 1993 Claffy had processed NSFNET measurement and firstly taken 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. Jack Drobisz etc believe static traffic sampling method maybe produce inaccurate traffic static materials. So considered the self-similar characters of network traffic, in that paper the static sampling method of Claffy is improved and a new self-adapted sampling method is developed. RFC2330 [22] has analyzed the randomicity of sampling measurement and suggests that Poisson sampling is fit to sample measure high-speed network traffic. These sampling models can only use to sample measure one-point measurement architecture. In order to use sampling technology in distributed measurement architectures, some

distributed sampling models are proposed. I. COZZANI [19] 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 sampling selection plane uses the checksum data. But according to that paper, the randomicity 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 in distributed measurement points. N. G. DUFFIELD [17] proposes to base the sampling decision on a deterministic hash function over the packet's invariant content. But it is difficult to assure the randomicity of the hash function, and the model needs have longer sampling time.

Distributed passive measurements on IP network traffic should solve two problems of both high-speed traffic measurements and the cooperation of measurement points. Sampling technology is to decrease data amount used in measuring, storing and processing under precision requiring. In order to cooperate the measurement results in distributed measurement points, it is necessary to assure same sampling results aiming at different measurement points. In the paper a kind of distributed sampling pattern matching with bit pattern through 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. We define bit entropy and the sampling mask measurement model in Section two. Then, in Section three we find that the identification field of IP header is an ideal matching bit flow. In Section four, we discuss the performance of the sampling model based on identification field. Finally, we conclude the paper.

2. Distributed Sampling Measurement Model

2.1 Definition

Entropy [26], an important concept of information theory, is to measure the random degree of various random experiments. In order to measure the random degree of bits in IP packet, we introduce the concept of entropy into the research of bit randomicity. Now we define some important entropy concepts in sampling measurement model as the metric of traffic randomicity.

Definition 1: Bit Entropy that is the entropy value of a bit in IP packet header is defined H(b).

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

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: Because the number of IP packets for statistical analysis are larger than 10,000,000, so given that p_0 and p_1 are continuous. So equation 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 equation 1 is replaced by $1-p_0$, then equation 1 is transformed into equation 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 $f'(p_0) = 0$

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

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 equation 2.

As follow proved that p_0= p_1=1/2 is the maximal value point. First we compute the two moment derivation function of equation 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 $p_0 \in (0, 1)$, $f''(p_0) > 0$, so p_0= p_1=1/2 is the extremum maximum point of equation f(p_0).

Now we discuss about p_0=0 or p_0=1. p_0=0 or p_0=1 that is an improbable event or a certain event is a decided event, so the bit has not any information. In theory, $\lim_{\varepsilon \to 0} \varepsilon \log \varepsilon \to 0$ can be proved easily, so $0 \times \log_2 0 = 0$, then $f(0) = 0 \times \log_2 0 + 1 \times \log_2 1 = 0$. $f(1) = f(0) = 0$.

According to the above discuss, 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 randomicity. Due to H_{max}（b）=1, $E = H(b) / H_{\max}(b) = H(b)$, $0 \le E \le 1$. If E approaches 1, then the randomicity 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. E is the random metric of bit, (1-E) is the certain degree of bit information. So we define that the bit redundant degree R=1-E=1-H(b)/H_{max}(b)=1-H(b).

2.2. 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 randomicity. 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 kinds of ways 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. Such as Poisson random sampling randomly generates packets number or time, before a packet arrives, we have known whether the pack will be sampled. The kind of sampling method now mainly is used in passive measurements, such as RFC2330 etc. However the sampling method can only be used in a single-point measuring architecture. The other sampling measurement method that will be researched in the paper is based on the sampling event generated by sampling model is specific, yet the static attributes of sampling event are random statistically. After a packet arrives, according to its content, then 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 same sampling mask can satisfy to measure the same packets for different measuring points and also can realize the randomicity of measuring packet samples. I. COZZANI and N. G. DUFFIELD use the kind of

sampling technology.

In order to assure the cooperation of sampling measurement results in different measurement points of the distributed sampling measurement architecture, the same packet sample in different measuring points should be obtained. That is to say, to any packet through measurement domain, the packet should be captured by all measuring points or captured by no one point. Therefore in order to realize sampling measurement in this system, the second method is the only way. By using specific sampling function, the packet sampling process is to be done according to the content of packet.

Provided a reference mask that matches with part bits of packets, then the monitor will select the sampling packet, and if in all monitors a same reference mask is used, then the synchronized sampling measuring packets may be processed in distributed system. The matched mechanism is based on a bit mask and matching bits with random content. 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 as fig.1.

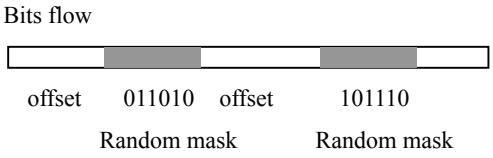


Fig.1 sampling model

3. The statistical analysis of IP header

3.1 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 1000Mbps 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. We found the entropy of identification field is very high and content of the identification field will not be changed during transportation.

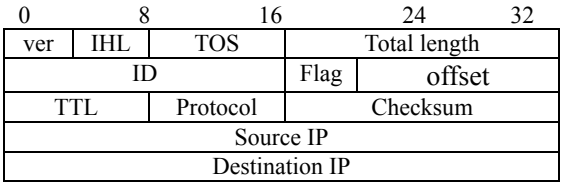
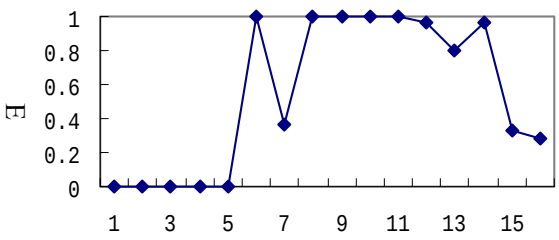


Fig2: the structure of IP header

Version field that has four bits contains the version protocol 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 separately 0.171, 0.193 and 0.004. 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 transport network routers, So TOS field isn't considered as the matching bit flow of sampling mask.

Fig 3: E of packet length field



Bit number of packet length field

The packet length field is mainly 40, 552, 576 and 1500 bits. The entropy efficiency E of packet length field is shown as Fig 3. The figure shows that E of the first byte is very low, and the E of the second byte is larger than 90%. But the packet length field can be

changed through network.

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. At the same time E of identification field is lager than 99% is shown as Fig. 4 and it can be shown the randomicity of identification field is very high and the 16 bits of identification fits the matching bits. The first bit of Flag field isn't used, the second bit DF with 88.7% and the third bit MF with 0.31% statistically. Fig 5 is the E of fragment field shows the fragment field doesn't fit the matching bits of sampling mask. TTL is decremented per hop. Protocol field is low bit entropy. It takes only several values, TCP(6) 93.04%, UDP(17) 6.37, and others 0.59%. The entropy efficiency E of destination IP is shown in Fig.6 and the source IP shows E of the last 16 bits of two IP bits are larger than 90%, so they can be considered as the matching bits.

Fig 4: E of identification field

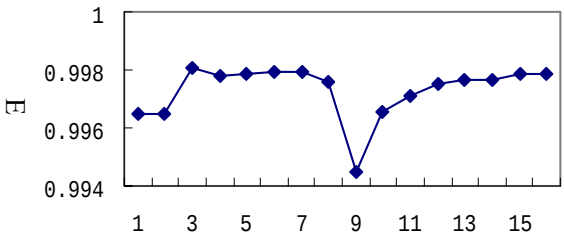


Fig5 E of offset field

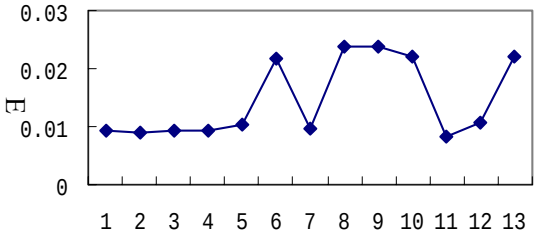
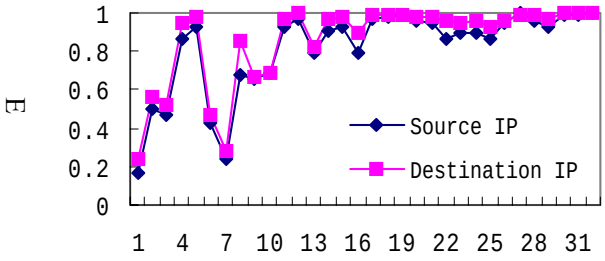


Fig6 E of IP field



According to the bit entropies of each field in IP packet header, we found that 16 bits of identification field, the later 16 bits of both source IP and destination IP all 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..

3.2 bit flow entropy analysis

According to the statistical analysis of bit entropy, the identification field, source IP and destination IP have high bit entropy and aren't changed in transit network. So we consider that the three bit flow can be used the matching bit flow. Now we analyze the correlation between different bits. Firstly, we give the definition of bit flow entropy and the maximal bit flow entropy theorem.

Definition 7: bit flow entropy is the entropy of bit flow. s bits have $n+1=2^s$ events, and their probability are respectively $p_0, p_1, \cdots, p_n$, so bit flow entropy H(s) is defined.

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

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

equation 5.

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

Prove: the same as theorem 1, we consider equation 3 also is a continuous function, and theorem 2 is an optimal problem. Namely, it is expressed as equation 6.

$$f(X) = -\sum_{i=0}^{n} p_i \log_2 p_i, \quad (X = (p_0, p_1, \cdots, p_n)^T \in D) \qquad (6)$$

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 $\left(X^* = (p_0^*, p_1^*, \cdots, p_n^*)^T\right)$ in D to obtain maxf(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 equation 6 is replaced with 1-S, and equation 7 is obtained.

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

if $X^* = (p_1^*, p_2^*, \cdots, p_n^*)^T$ is the extremum of f(X), then gets the gradient vector $\nabla f(X^*) = \left(\frac{\partial f}{\partial p_1^*}, \frac{\partial f}{\partial p_2^*}, \cdots, \frac{\partial f}{\partial p_n^*} \right)^T = \vec{0}$, and contains the condition, and equation 8 is obtained.

$$\begin{cases} \frac{\partial f}{\partial p_1^*} = \log_2 p_1^* - \log_2 \sum_{i=1}^{n} p_i^* = 0 \\ \frac{\partial f}{\partial p_2^*} = \log_2 p_2^* - \log_2 \sum_{i=1}^{n} p_i^* = 0 \\ \vdots \qquad\qquad \vdots \\ \frac{\partial f}{\partial p_n^*} = \log_2 p_n^* - \log_2 \sum_{i=1}^{n} p_i^* = 0 \\ \sum_{i=0}^{n} p_i^* = 1 \end{cases} \qquad (8)$$

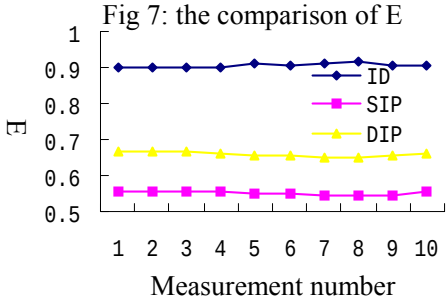
If $p_0^* = p_1^* = \cdots = p_n^* = \frac{1}{n+1} = \frac{1}{2^s}$, the same as theorem 1, we can prove that X^* is maximal point. So the prove is finished.

Definition 8, the information efficiency E of bit flow, is the ratio between H(s) and $H_{max}(s)$ and the metric of bit flow randomicity, $E = H(s) / H_{\max}(s) = H(s) / s$.

In different time, IP traffic of CERNET backbone is measured 10 times, each time with

1,000,000 packets. The information efficiency of the three bit entropy mentioned above is compared and the results are shown as 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. According to the stability character we could take part bits as the sampling matching bits to reflect random character. In the paper part of 16 bits in identification field are chosen as random sampling matching bits.

Fig 7: the comparison of E



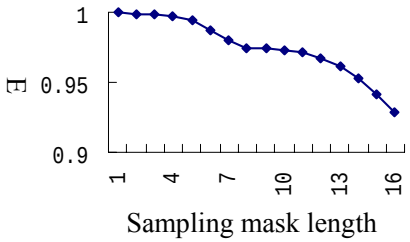
4. Performance Analysis of Sampling Measurement Model

According to above analysis, we can choose 16 bits of the identification field as sampling matching bits. The matching bits can choose from 0^{th} bit to 16^{th} bits, so the ratio of sampling can be from 1 to 2^{16}, the maximal sampling ratio can realize 65536. Now a common PC can deal with and store 10Mbps traffic, so it can sample 640Gbps traffic in theory. Of course, its condition is that the PC can measure the traffic. The sampling measurement model is mainly bit operation, and bit operation can easily be carried out through hardware, so we can carry out the sampling measurement in network card. Below we will analyze the randomicity of the model and the statistical character of traffic samples.

4.1 the randomicity analysis of the sampling model

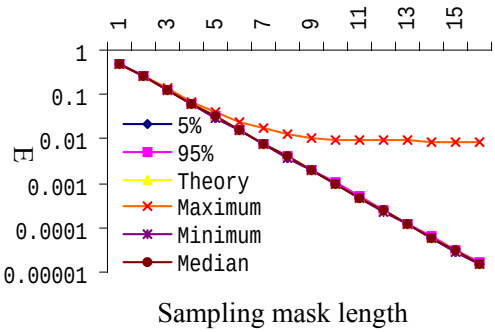
The offset of the sampling model based on identification field that is a fix value, is defined as the position of the header of identification field, and the maximal mask length is 16 bits. Now we analyze the bits E from 1^{th} to 16^{th} bits. Fig 8 is bits E statistics analysis of 10,000,000 packets. In fig 8, the minimal bits entropy is larger than 0.9, so the identification field is very random and its autocorrelation is very small.

Fig 8: the comparison of the bits E



In the paper the relation between sampling mask length and sampling ratio is shown as 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 ratio of maximal ratio, minimal ratio, median ratio, 95% ratio, and 5% ratio is listed separately. Except the maximal ratio, the others sampling ratios draw near because the full 0 bits of identification field is higher than others bits. So we don't choose the full 0 bits as the

Fig 9: the relation between sampling ratio and mask length



sampling mask. Through fig.9 it can be proved that the identification field owns a good randomicity and it fits to matching bits.

4.2 the 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 (α =0.05 or 0.01), independence hypothesis H_0:$F(x)=F_0(x)$ is tested by χ^2 distribution.

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

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

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 α =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 1^{th} to 16^{th} bits of identification field in turn. In the test, there are 10,000,000 packets, and the sampling mask of sampling model is respectively 1, 10, 101, 0110, 10111, 101011, 1010111, 10100100, 110011101, 1010111000, 11110000111, 000011110000, 1010101010101, 10000001110010, 011000101110000, 0010101011101101.

In the experiment, the prefix of source IP is tested with $I=2^5$. Due to the packet length between 40 bytes and 1500 bytes, a bin per 30 bytes, so 49 bins are built. There are mainly three kinds of protocols TCP, UDP, and others, so 3 bins are set. Consider the number of protocol

Fig 10: hypothesis distribution of protocol

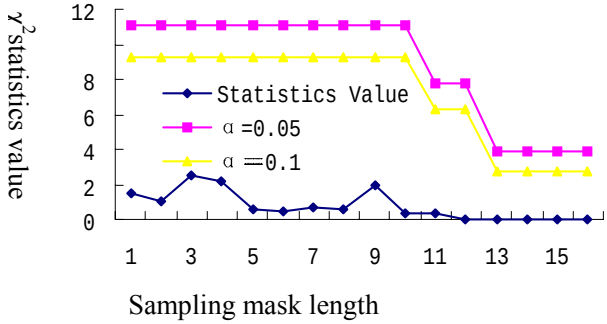


Fig 11: hypothesis distribution of packet length

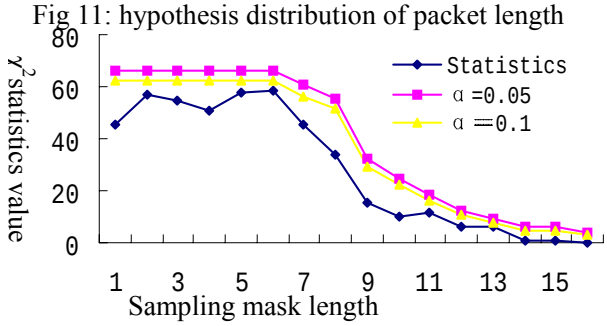
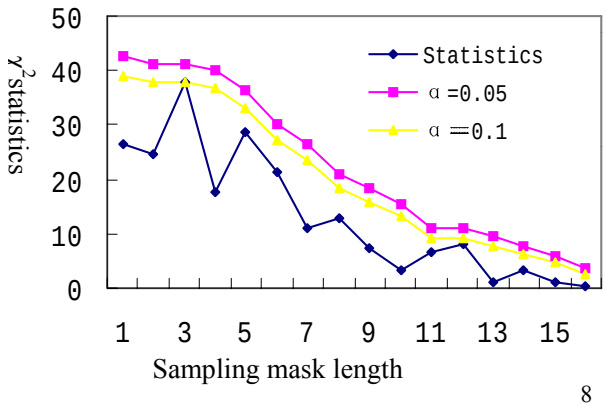


Fig 12: hypothesis distribution of IP Address prefix



bins is very little, unsampled bins also are considered. So the number of protocol bins is six, 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 hypothesizes show separately fig 10 hypothesis distribution of protocol, fig 11 hypothesis distribution of packet length, and fig 12 hypothesis distribution of source IP prefix. From these figure, For a given confidence level α (α =0.05 or 0.01), $\chi^2<\chi^2_\alpha$, so we accept the hypothesis H_0, and believe the same statistics distribution between the sample traffic and the full traffic.

5 Conclusions

The distributed passive measuring on network performance is a research focus all over the world. However it is difficult to find a general traffic measuring method. Owing to sampling measuring method as a good way to solve the problem and so as to ensure traffic information cooperation and make the randomicity of measurement samples at the same time, a new bit mask sampling model is advanced in the paper which can be used in distributed passive measuring environment.

In the paper, information theory is applied into analyzing the bit entropy of IP header of measurement traffic in CERNET backbone network. Through analysis we find the identification field is suitable to sampling matching bits and there are four main reasons for selecting the identification fields as sampling matching bits. Firstly during transportation the identification field content will not be changed. Secondly its bit entropies and bits entropies is much higher than fields of all other IP header and their information efficiencies are more than 99% and the information efficiency of 16 bits entropy also can reach 90%. Thirdly because of identification field with a random sign, so it does not contain correlative information with packet content such as packet length and IP address etc. So once we use other fields with packet statistical attribute, random attribute of the field will not be assured. Finally the 16 bits is enough to satisfy the developing requirement of future network bandwidth, so we will control sampling measurement only through bit mask. So in this way not only network burden can be decreased and sampling configure can be simplied in some degree.

Reference

[1] CAIDA Homepage, http://www.caida.org.

[2] CAIDA Tools site, http://www.caida.org/tools/.

[3] ISMA web page, http://www.caida.org/outreach/isma/.

[4] skitter Web Site, http://www.caida.org/tools/measurement/skitter/

[5] B. Huffaker, Marina Fomenkov, David Moore, Evi Nemeth, K. Claffy, Measurements of the Internet topology in Asia- pacific Region, 2000, http://www.caida.org/outreach/papers/asia_paper/

[6] Kc Claffy, Sean McCreary, Internet measurement and data analysis: passive and active measurement, ASA99 paper, http://www.caida.org/outreach/papers/Nae/4hansen.html

[7] L. Cottrell, "PingER Tools," http://www.slac.stanford.edu/xorg/icfa/ntf/tool.html, May 1998.

[8] I. D. Graham, S. F. Donnelly, S. Martin, J. Martens, and J. G. Cleary, "Nonintrusive and Accurate Measurement of Unidirectional Delay and Delay Variation on the Internet," Proc. INET '98, Jul. 1998.

[9] I. D. Graham, et al., Waikato Applied Network Dynamics (WAND) Project homepage,

http://atm.cs.waikato.ac.nz/wand/

[10] RIPE Network Coordination Centre, Test Traffic Project Homepage, http://www.ripe.net/test-traffic/index.html

[11] B. Huffaker, Marina Fomenkov, David Moore, Evi Nemeth, K. Claffy, Measurements of the Internet topology in Asia- pacific Region, 2000, http://www.caida.org/outreach/papers/asia_paper/

[12] CoralReef, http://www.caida.org/tools/measurement/coralreef/

[13] NLANR(MOAT)-PMA Passive Measurement and Analysis, http://moat.nlanr.net/PMA/

[14] NPACI's Network Weather Service, http://nws.cs.utk.edu/

[15] WAND (Waikato Applied Network Dynamics) Project, http://wand.cs.waikato.ac.nz/

[16] Tanja Zseby, Sebastian Zander, Georg Carle, Evaluation of Build Blocks for Passive One-way-delay Measurements, PAM2001

[17] Nick Duffield, Matthias Grossglauser, Trajectory Sampling for Direct Traffic Observation, Proceedings of ACM SIGCOMM 2000, Stockholm, Sweden, August 28 – September 1, 2000

[18] Ian D. Granham, Stephen F. Donnelly, Stele Martin, Jed Martens, John G. Cleary, Nonintrusive and Accurate Measurement of Unidirectional Delay and Delay Variation on the Internet, INET'98, Geneva, Switzerland, 21-24 July, 1998.

[19] Cozzani, I.; Giordano, S, A passive test and measurement system: traffic sampling for QoS evaluation, Global Telecommunications Conference, 1998. GLOBECOM 1998. The Bridge to Global Integration. IEEE , Page(s): 1236 –1241, Volume: 2 , 1998

[20] K. Claffy, G. Polyzos, H. Braun, Application of Sampling Methodologies to Network Traffic Characterization, May 1993, Proceedings of ACM SIGCOMM '93.

[21] Jack Drobisz, Kenneth J. Christensen, Adaptive Sampling Methods to Determine Network Traffic Statistics including the Hurst Parameter, 23rd. Annual Conference on Local Computer Networks, October 11-14, 1998.

[22] V. Paxson, G. Almes, J. Mahdavi, M. Mathis, Framework for IP Performance Metrics, IETF RFC 2330, 1998.

[23] J. Reynolds,J. Postel., Assigned Numbers, IETF RFC1700, October 1994.

[24] Tang Xiangneng, Dai Jianhua, Mathematics Statistics, Mechanism Technology Press pp：140－151, 1994.5, BeiJing (in Chinese)

[25] Jin Zhenyu, Information Theory, BeiJing University of Science and Technology Press, pp：11－47, 1991.12, BeiJing. (in Chinese)