What's Going On in Chinese IPv6 World

Lei Gao[1], Jiahai Yang[2], Hui Zhang[2], Donghong Qin[1], Bin Zhang[1]
Tsinghua National Laboratory for Information Science and Technology
[1] Department of Computer Science and Technology, [2] Network Research Center
Tsinghua University, Beijing, P.R. China
gaolei04@gmail.com, {yang, hzhang} @cernet.edu.cn, qdh08@mails.tsinghua.edu.cn, zhang_bin163@163.com

Abstract—**With IPv4 addresses quickly dwindling, the Internet is forcing an evolution of itself. During the long term transition from IPv4 to IPv6, what's going on in IPv6 world becomes unknown for network operators and researchers. In this paper, we propose a heuristic algorithm to identify p2p traffic accurately and implement traffic classification based on Netflow v9 exports to illustrate what applications Chinese IPv6 users are really running. Additionally, we present a detailed study of p2p traffic over IPv6 and advice ISPs to localize p2p traffic at the AS level for future IPv6 traffic management and network resources planning, leaving modeling traffic behavior and deeper classification of IPv6 traffic as our future work.**

Keywords- IPv6; Netflow; peer-to-peer; traffic analysis

I. INTRODUCTION

The rapid growth of the Internet is forcing an evolution of itself, which is the transition of TCP/IP protocol suite from version 4 to its stable version 6. While evolving to IPv6, IPv4's dominating place has never been challenged by its successors. The majority of information transferred in the Internet is carried by IPv4 traffic and the routine life of our human beings totally depends on the underlying IPv4 networks. Nevertheless, with the rapid exhaustion of IPv4 addresses, IPv6 becomes an alternative for Internet applications. Especially since uTorrent (a popular BT client for windows) released its version 1.8 supporting IPv6 traffic in 2008, the proportion of IPv6 traffic in the entire Internet traffic has lasted a dramatic increase. And p2p becomes the killer application that drives the whole IP world to IPv6.

While IPv6 traffic makes up less than 1% of the total Internet traffic at present, p2p traffic has more than 60% proportion in the entire IPv6 traffic based on our observation, which is very similar to the situation in 2003 when p2p applications got really prevalent in IPv4 networks. P2P applications now drive more and more users with their traffic into IPv6 world, which is critical for the extensive transition from IPv4 to IPv6. But at the same time, there lies the challenge that p2p applications maybe purify the IPv6 traffic into their own traffic, create huge congestions and overwhelm the IPv6 network infrastructures. Compared with recent top IPv4 applications, IPv4's p2p applications are under effective control through traffic engineering and other management solutions. In order to give guidance to plan IPv6 network resources optimally and meet the increasing demand that traffic management is also required by future IPv6 networks, it's of vital importance to know what is going on in today's IPv6 world.

978-1-4673-0269-2/12/$31.00 ©2012 IEEE

Traditional traffic classification techniques are based on either payload or header information. Though deep packet inspection can provide enough information to identify most applications that the end users are running, DPI suffers from great measurement overhead and it fails to handle encrypted payload. On the contrary, flow based classification techniques focus on flow patterns or traffic behaviors to abstract application signatures using only header information, with less measurement overhead and a relative inaccuracy. Sen et al. [1] showed that DPI based classification of P2P traffic can gain benefits in the classification accuracy for most P2P protocols studied using the signatures of traffic at the application level. Techniques based on both port and DPI to identify network applications is presented in [13]. Paxson constructed empirical analytic models of wide-area TCP connections for application identification based on statistical traffic property in [14]. Later work on traffic identification often pay their attention to the usage of both supervised and unsupervised machine-learning techniques for automated classification. Nguyen and Armitage proposed supervised Naïve Bayes for traffic classification in [7]. Erman et al. [3] introduced clustering approach, an unsupervised ML algorithm, to identify traffic and showed that the performance of supervised ML algorithms would degrade if they were not trained properly. Furthermore, BLINC with its three-layer model gave a new way of traffic classification by focusing on the flow's host behavior at the transport layer [17].

To figure out the applications that IPv6 users are running, we propose a heuristic algorithm to identify p2p traffic accurately and implement this algorithm in our infrastructure named FlowInfra which is designed for network-wide flow level measurement. We enable Netflow v9 export in the Juniper T640 router which lies in the exit of CERNET2 and several border routers which are in charge of routing packets between each campus network and the backbone network of CERNET2. NetFlow v9 supports IPv6 flow sampling, generation, and export, which enables direct flow level measurement of IPv6 traffic with a relatively small overhead. In this work, we collect Netflow v9 records exported from three routers and store Netflow v9 records into binary flow records *every 5 minutes*, router THU and router BUPT, which are both NE40e of HUAWEI. And we perform traffic classification based on these flow records which are generated from two distinct 10Gbps links.

The rest of the paper is organized as follows. In Section II we discuss about our heuristic algorithm for traffic classification based on Netflow v9 records. Section III presents the results of our algorithm and gives a detailed overview of

IPv6 traffic. Finally we conclude our work and summarize our future work in section IV.

II. ALGORITHM OVERVIEW

In its infant age, p2p applications in IPv6 networks don't need any approaches to get rid of the control of traffic management, because there is none of this kind of network management. As a result, p2p applications often use fixed data port, with their randomization of data ports disabled. Our observation also confirms that users of p2p applications tend to keep the default configurations including the default data port to run their p2p clients in CERNET2 and the majority of p2p traffic are generated between these famous fixed ports and random ports, with totally less than 2% p2p traffic between random ports.

We notice that IPv4 traffic will be accounted and billed in Chinese campus networks while IPv6 resources are free to use. Consequently, two big BT sites in CERNET2, ByrBT maintained by BUPT and EduBT maintained by NEU, customize their special versions of uTorrent clients with the support for IPv4 traffic disabled. To support pure IPv6 traffic and diminish the IPv4 traffic cost, ByrBT's customized uTorrent version uses uTorrent release 2.0 and port 18600 by default, while EduBT uses uTorrent release 1.8.5 and port 16703 by default.

In our heuristic algorithm, the criteria for classifying a particular pair of IP address and port number as p2p traffic is based on the following steps.

1) If a source or destination port in a flow is on the default data ports 16703 and 18600 we mentioned above,we straightly classify this flow as p2p traffic, and both the source and destination entities are considered as peers;

2) Flows using a source port or destination port number below 1024 are classified as non-p2p traffic, because most of p2p applications randomize their data ports in the non-assigned port ranges listed by IANA and ports below 1024 are often used by well-known non-p2p applications ;

3) Flows contains source or destination entities marked as peers, are classified as p2p traffic. And their counterpart entities are considered as p2p participants.

In the implementation of these heuristics, we use the hash function *hashlittle* in BOB hash functions with the 18-byte key generated from the 5-tuple of each flow record to compute its hashkey [13]. Our entire classification process for the identification of p2p traffic is outlined as follows:

1) initialize the seed set with an empty set (done for just once);

2) search one piece of flow record;

3) if a source or destination port in a flow is on the default data ports 16703 and 18600, this flow is classified as p2p traffic and added into this flow record's result set;

---if the source port is on the default port and the destination port is not, the hashkey of the destination pair of IP address and port will be added into both the seed set and result set;

---vice versa;

4) search this flow record again;

5) if a source or destination hashkey in a flow is in the seed set, this flow is classified as p2p traffic and added into the result set;

---if the source hashkey is in the seed set and the destination hashkey is not, the hashkey of the destination pair of IP address and port will be added into both the seed set and result set;

---vice versa;

6) continue step 4 and 5 until no more hashkey is added into the seed set or some threshold is reached (usually the 0.01% of the total flow number in each flow record).

We search the same binary flow record several times (mostly less than 5 times) and some p2p participants are detected. As another flow record is chosen as inputs and this process goes, the seed set is continually growing. Additionally, we introduce a replacing mechanism to avoid an amount of hash conflicts. Once a peer participant in the seed set isn't detected for continuous 288 flow records for one day (one flow record per 5 minutes), it will be removed from the seed set. In our algorithm, there is only one seed set for the identification and each flow record has its own result set where its p2p entities are stored.

III. OVERVIEW OF IPV6 TRAFFIC

The flow records exported from these three routers form the basis of the implementation of our heuristic algorithm. The dataset is consisted of flow records with their time span from 1st June to 30th July. We performed our analysis on flow records stored in every 22 o'clock sharp which was usually the peak time in the diurnal pattern curve. Flow records from THU cover pure IPv6 traffic between the backbone network of CERNET2 and the campus network of THU. And flow records from BUPT cover flows between the backbone network of CERNET2 and the campus network of BUPT. We show that p2p traffic keeps its dominating proportion in the traffic distribution of the exit of CERNET2 in Figure 1. Figure 2 shows that p2p traffic makes up more than 70% of the entire traffic, and IPTV traffic reaches up to 15%, leaving web traffic a small proportion next to 1%. As a data source of ByrBT and Bupt IPTV, the sum of p2p and IPTV traffic proportion in BUPT grows bigger than the sum in THU.

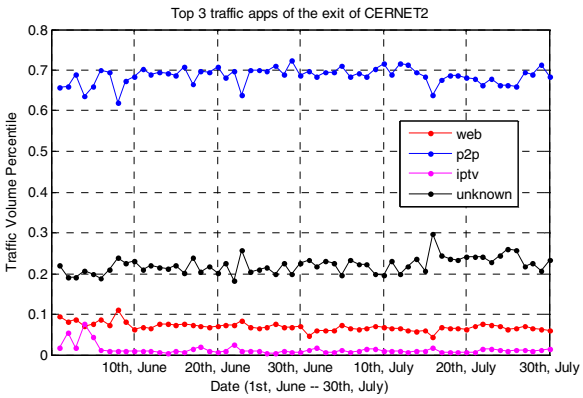

Figure 1. IPv6 traffic distribution from the exit of CERNET2

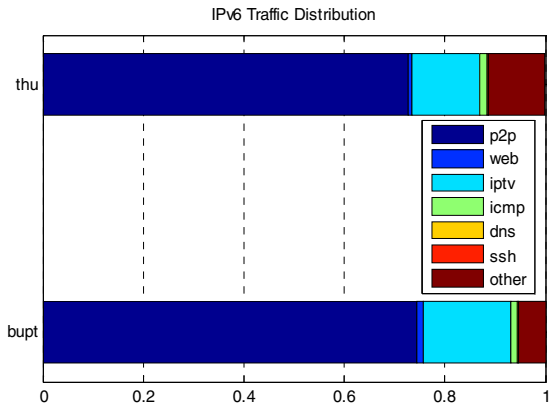

Figure 2. IPv6 traffic distribution from THU and BUPT

Compared with IPv4 traffic distribution, IPv6 world is filled with video streaming and there are little direct web users in IPv6 world, with the majority of web traffic coming from tunneling or other communication solutions between IPv4 and IPv6.

We perform a comparative study on p2p traffic and web traffic. Figure 3 shows that p2p traffic dominates the bandwidth of the link and also has a prominent diurnal pattern. The bandwidth of web traffic can be totally neglected compared to the bandwidth of p2p traffic. Furthermore, the average packet size of p2p traffic is stable at the size of 930 bytes while the average packet size of web traffic fluctuates notably over one-day period and is always below the size of 800 bytes.

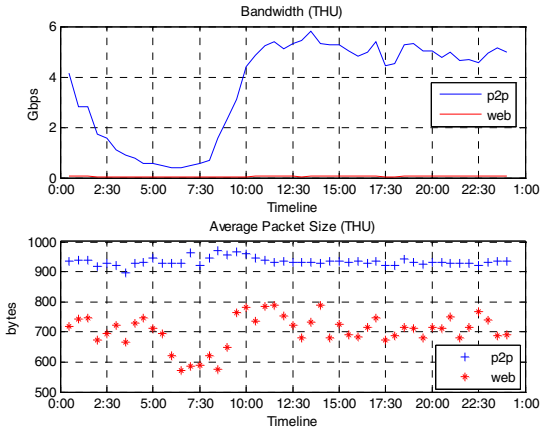

Figure 3. Difference between p2p and web traffic

To give guidance for future network management and traffic engineering, we compute the number of unique IP-port pairs participating in p2p overlay network at two different levels (prefixes and ASes) in each five-minute period across several weeks. From the distribution of AS and prefix entities, we can figure out whether p2p traffic localization would be an effective solution for future p2p traffic management and network resources planning.

Figure 4 shows that about half of p2p traffic providers and receivers are located in their local AS, which indicates that we can greatly reduce the transiting traffic between ASes through p2p traffic localization and other approaches of traffic engineering. AS rank14 is AS 24350 which is assigned to BUPT while AS rank 1 represents THU with AS number 24348. Notice that, the distribution has a heavy tail. To take p2p traffic across ASes under control, detailed IPv6 p2p traffic research and deep traffic engineering are getting increasing demand.

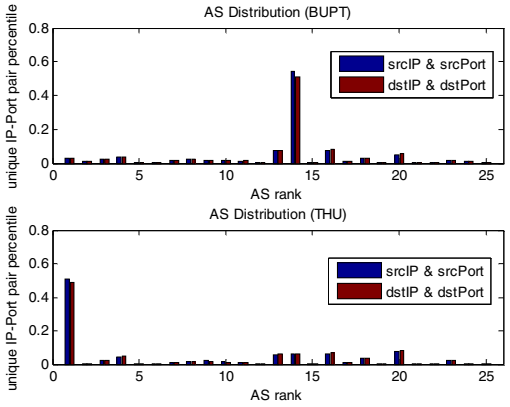

Figure 4. Distribtution of AS entities

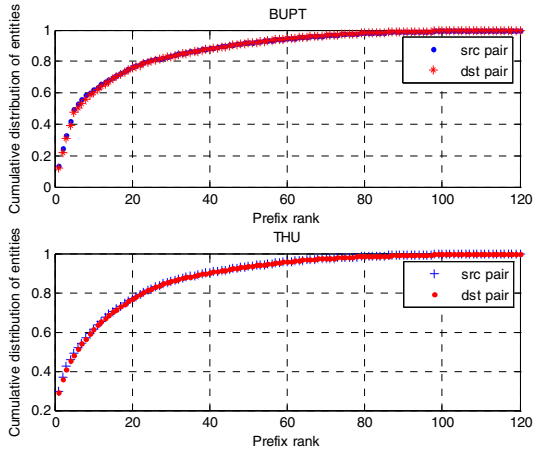

Figure 5. Distribution of prefix entities

The ranked cumulative distribution of prefix entities is shown in Figure 5. We find that unique IP-port pairs in p2p traffic from BUPT falls into 150 prefixes and those from THU falls into 149 prefixes. In the prefix level, top 20 prefixes dominate approximately 80% of unique IP-port pairs and the downstream entities (destination IP-port pairs) has a similar distribution with the upstream ones (source IP-port pairs). Above all, the distribution also has a long tail and traffic management at the prefix level requires more fine-grained planning.

We define a measurement metric called balance to describe the upstream and downstream behaviors of unique ports. The bytes from a source port to a destination port are considered as

an income belonging to the source port. Meantime, the bytes are accounted as expenditure in the account of the destination port. Also the port degree is defined as the number of its distinct counterpart port. The social behaviors of different applications are reflected in the differences of the degree and the remaining balance of the account of ports.

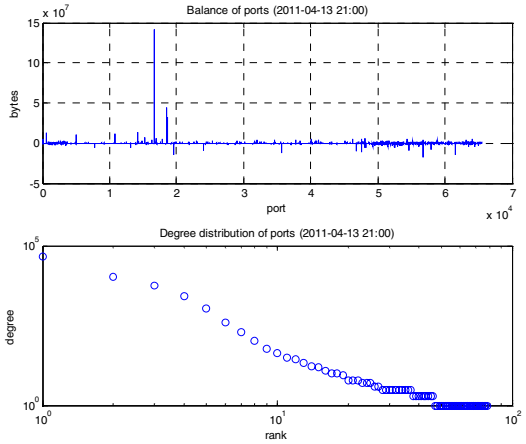

Figure 6. Balance and degree distribution of ports

The balance and degree distribution of different ports are shown in Figure 6. The overall degree distribution of ports is approximately following power-law. Further modeling of these traffic behaviors and detailed classification of IPv6 traffic are left as our future work.

IV. CONCLUSION

In order to understand what's going on in Chinese IPv6 world during the transition from IPv4 to IPv6, give guidance to plan IPv6 network resources optimally and meet the increasing demand that traffic management is required by future IPv6 networks, we propose a heuristic algorithm to identify p2p traffic and implement traffic classification to illustrate what applications Chinese IPv6 users are running. Compared to IPv4 traffic distribution, a conclusion can be drawn that the transition from IPv4 to IPv6 is still in the beginning of its long term evolution and network management solutions in IPv6 are quite immature. What's more, we perform a deep analysis of IPv6's p2p traffic and advice ISPs to localize p2p traffic in each AS and get prepared for future IPv6 traffic management. Additionally, we leave modeling traffic behavior and detailed classification of IPv6 traffic as our future work.

ACKNOWLEDGMENT

This work is supported by the National Basic Research Program of China under Grant No. 2009CB320505, the National Science and Technology Supporting Plan of China under Grant No. 2008BAH37B05, and the National High-Tech Research and Development Plan of China under Grant No. 2008AA01A303 and 2009AA01Z251.

REFERENCES

[1] S. Sen, O. Spatscheck, and D. Wang, "Accurate, scalable in network identification of P2P traffic using application signatures," in *WWW2004*, New York, NY, USA, May 2004.

[2] C. Estan, K. Keys, D. Moore, and G. Varghese. Building a Better NetFlow. In Proc. of SIGCOMM'04, Portland, Oregon, USA, Aug. 2004.

[3] J. Erman, M. Arlitt, and A. Mahanti, "Traffic classification using clustering algorithms," in MineNet '06: Proc. 2006 SIGCOMM workshop *on Mining network data*. New York, NY, USA: ACM Press, 2006, pp. 281–286.

[4] P. Barford, J. Kline, D. Plonka, and A. Ron. A Signal Analysis of Network Traffic Anomalies. In Proc. ACM SIGCOMM IMW'02, pages 71–82, Marseille, France, Nov. 2002.

[5] N. Duffield. Sampling for Passive Internet Measurement: A Review. Statistical Science, 19(3):472–498, 2004.

[6] A. Lakhina, M. Crovella, and C. Diot. Mining Anomalies Using Traffic Feature Distributions. In Proc. ACM SIGCOMM '05, Philadelphia, PA, USA, Aug. 2005.

[7] T. Nguyen and G. Armitage, "Training on multiple sub-flows to optimise the use of Machine Learning classifiers in real-world IP networks," in Proc. IEEE 31st Conference on Local Computer Networks, Tampa, Florida, USA, November 2006.

[8] C. Estan and G. Varghese, "New directions in traffic measurement and accounting," presented at the ACM SIGCOMM, Pittsburgh, PA, Aug. 2002.

[9] Cisco NetFlow. http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

[10] BOB hashing function: http://burtleburtle.net/bob/hash/doobs.html.

[11] B. Claise: Cisco Systems NetFlow Services Export Version 9, RFC3954, October 2004.

[12] B. Claise: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information, RFC5101, January 2008.

[13] A. Moore and K. Papagiannaki, "Toward the accurate identification of network applications," in Proc. Passive and Active Measurement the Internet (SAINTW'04), Tokyo, Japan, January 26-30, 2004, pp 91-98.

[14] V. Paxson, "Empirically derived analytic models of wide-area TCP connections," *IEEE/ACM Trans. Networking*, vol. 2, no. 4, pp. 316–336, 1994..

[15] P. Maymounkov, D. Mazières: *Kademlia: A Peer-to-Peer Information System Based on the XOR Metric*, IPTPS 2002, March 2002, Cambridge, MA, USA.

[16] NFDump Project: http://nfdump.sourceforge.net/.

[17] T. Karagiannis, K. Papagiannaki, and M. Faloutsos, "BLINC: Multilevel Traffic Classification in the Dark," in *SIGCOMM'05*, Philadelphia, USA, August 21-26, 2005.

[18] A. Moore and D. Zuev, "Internet Traffic Classification Using Bayesian Analysis Techniques," in *SIGMETRICS'05*, Banff, Canada, June 6-10, 2005.

[19] J. Erman, A. Mahanti, and M. Arlitt, "Internet traffic identification using machine learning techniques," in *Proc. of 49th IEEE Global* Telecommunications Conference (GLOBECOM 2006), San Francisco, USA, December 2006.

[20] N. Williams, S. Zander, and G. Armitage, "A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification," Special Interest Group on Data Communication (SIGCOMM) Computer Communication Review, vol. 36, no. 5, pp. 5–16, 2006.

[21] M. Halkidi, Y. Batistakis, and M. Vazirgiannis, "Cluster validity methods: part I," *SIGMOD Rec.*, vol. 31, no. 2, pp. 40–45, 2002.

[22] R. Xu and D. Wunsch, "Survey of clustering algorithms," *IEEE Trans. Neural Networks*, no. Vol.16, Issue 3, pp. 645– 678, May 2005.