Evaluating Routing Asymmetry by Passive Flow Measurements with Spark

Jun Liu* †, Chao Zheng*, Li Guo*, Xueli Liu*, Qiuwen Lu*
*Institute of Information Engineering, Chinese Academy of Sciences
†School of Cyber Security, University of Chinese Academy of Sciences
Beijing, China
{liujun9054, zhengchao, guoli, liuxueli, luqiuwen}@iie.ac.cn

***Abstract*—Routing asymmetry increases network efficiency, but also brings serious challenges to some use cases, such as policy enforcement, flow identification, malicious/anomaly detection, traffic shaping and limit etc. Routing asymmetry is an inevitable phenomenon. However, the question is that how is the specific asymmetric degree of network traffic. We classify and evaluate the conditions of network traffic actually routed asymmetry in the ISPs network that has a significant impact on the network security, measurement, model and management. For depicting asymmetric degree of the network packet in a flow and hosts behavior, we classify the routing asymmetry into flow asymmetry and IP asymmetry. In order to meet the high bandwidth, multiple observation points and passive measurement requirements, we build a scalable passive measurement system for online or offline evaluating routing asymmetry. The system adopts fast packet I/O technique to capture network traffic, and Spark to process the collected data. To prove its practicability, we deploy the system in a carrier grade network that has six data centers. We have found that 1) over 90% of TCP flows are asymmetric, and 2) over 70% of flows from full IP asymmetry that a same IP address traverse different links.**

Keywords-Routing Asymmetry; Passive Flow Measurements; DPDK; Spark; Flow Asymmetry; IP Asymmetry

I. INTRODUCTION

Routing asymmetry is widespread and pervasive throughout networks, and it is an inevitable phenomenon that each node independently offers multiple alternative router paths to the same destination. If packet streams between two endpoints follow the same physical links between intermediate nodes for both forward and reverse direction, they are symmetrically routed. Otherwise, the routing called asymmetric [1]. For example, routing asymmetry is that a path of forward direction from host A to host B is (R1, R2, R4), which is different from the path of reverse direction is (R4, R3, R1).

There are many reasons that lead to routing asymmetry. Long term asymmetric routers are mainly created due to routing police and traffic engineering [2]. Inter-domain router uses RIP or OSPF algorithms to calculate routing tables where the shortest path between a pair of hosts may not be unique. The Equal Cost Multi-Path routing results leads to randomly choose any of possible shortest paths. And the communications service providers (CSPs) need to improve the network performance, congestion management and the practice of load-balancing may cause each packet in a flow or different flow destined for the same endpoint take different physical links. Due to any one pair of neighboring AS have secret business relationships, the routing police of traffic engineering may cause packet in a provider's network but destined for other provider's and experience a longer path. In addition, malicious scanning, backscatter and misconfiguration routing could also result in routing asymmetry.

The assumption of routing symmetry is often embedded into traffic analysis and classification tools [1]. An in-depth study of routing asymmetry can undoubtedly enhance our understanding of the Internet and contribute to the network measurement, model and management. Models of Internet routing are critical for studies of Internet security, reliability and evolution [3]. ISPs often treat their connectivity and routing policies as trade secret [3]. Monitoring and quantifying routing asymmetry may improve routing model accuracy and potentially be an important indicator of the state of the Internet [4]. The dramatic fluctuation of routing asymmetry may suggest changes, misconfiguration or even error in the routing practices and reflect malicious events such as malicious scanning or DDOS maybe occurs in the network. Network traffic dynamic transfer in space and time, it is more difficult to associate two directions of a flow between any pairs of hosts in the Internet. There are some use cases such as accurate charging, policy-based measurements and congestion management that requires CSPs to propose effective solution to overcome the challenge. Routing asymmetry has been gradually studied, but there is still lack of systematic approach for classifying and evaluating the routing asymmetry except for computing Absolute Asymmetry and length-based Normalized Asymmetry [2] and estimating routing symmetry [1]. The goal of this paper is (1) classifying the routing asymmetry into flow asymmetry and IP asymmetry based on passive measurement, and (2) building a scalable passive measurement system for online or offline evaluating each type of the routing asymmetry, and (3) monitoring and quantifying a carrier grade network that has six data centers.

The rest of this paper is organized as follows: Section 2 briefly introduces background and related work about the topic of routing asymmetry. We depict our approach to classify the routing asymmetry and design the data structures of TCP streams in section 3. Then, we present a framework for online or offline evaluating each type of the routing

asymmetry in section 4. Measuring and analyzing each type of routing asymmetry in section 5. In section 6, we conclude our work and discuss possible future research directions.

II. BACKGROUND AND RELATED WORKS

In terms of measurement method, there are three ways of active probing, passive measurement and device data acquisition. The initial innovative study work in this area by Paxson [5] at 1996 who use traceroute to actively probe routing path and analysis the routing behavior between any pairs of hosts in the Internet and defines the problem of routing asymmetry. And then, other researchers gradually pay more attention to the problem of routing asymmetry. In National Laboratory of Applied Network Research (NLANR), Y. He [2][4] analysis data sets are collected by Active Measurement Project (AMP) and defines two types routing asymmetry of Absolute Asymmetry and length-based Normalized Asymmetry. John. W [1] uses passive measurement method to capture network data on a specific link and propose a Flow-Based Symmetry Estimator (FSE) to filter inherently asymmetry traffic such as UDP, ICMP and TCP background radiation and estimate routing symmetry in terms of three metrics type of flow, packets and bytes. Glatz, E [6] uses hardware-based NetFlow has been collected 7.41 petabytes unsampled flow records on regional academic backbone network since 2004 to 2011 and proposes a classification schema to shed light into the composition of one-way traffic, such as unreachable services, malicious scanning and backscatter etc. And Orsini, C [7] present an open-source software BGP Stream for the analysis of both historical and real-time BGP traffic data. Oztoprak, K [8] proposes the Hybrid Asymmetry Traffic Classifier (HATC) that combines the best aspects of state sharing and clustering to address all types of asymmetry traffic problem of DPI system.

There are several popular projects and traffic tools built to analysis routing properties. Traceroute, AMP monitor [4] and RETRO [2] can actively probe the network for collecting routing path information. But active probing can exhaust network resources and may cause negative impact on the state of Internet. BGP looking glasses can allow users to directly download the ASCII output of the current state of the router RIB [7]. RouteViews [9] that was created by University's Route Views Project obtains real-time information about the global routing system from perspectives of several different backbone and locations around the Internet.

Those works associated with routing behavior or routing asymmetry study. However, there is still lack of a systematic approach for classifying and evaluating the routing asymmetry.

III. ROUTING ASYMMETRY CLASSIFICATION AND METHODOLOGY

In this section, we firstly introduce the classification of routing asymmetry. Then, we discuss the new heuristic methodology of evaluating routing asymmetry used in our study. Finally, we explain why the flow data structures are designed and how routing asymmetry is classified.

A. *Routing asymmetry classification*

With the rapid development of the network and the explosive growth of Internet traffic, CSPs network becomes increasingly complex and the network characterized by more and more heterogeneous. Due to the practice of load balance or the business requirements, CSPs have made of various network policy strategy, which results in a variety of routing asymmetry phenomenon. As shown in Fig.1, there are two types of routing asymmetry—Flow asymmetry and IP asymmetry.

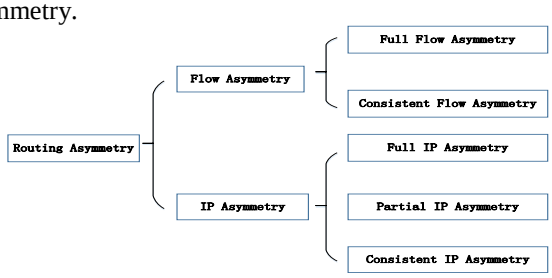


Fig.1 The Classification of routing asymmetry

1) *Flow asymmetry*

According to Sandvine [10], flow asymmetry mainly depicts asymmetric degree of the network packet in a flow. There are two types of flow full asymmetry and consistent partial flow asymmetry.

a) *Full flow asymmetry*: occurs when each packet in a flow may take any one of several links in either direction (i.e., upstream and downstream) [10], as shown in Fig.2 a);

b) *Consistent partial flow asymmetry*: all upstream packets are on one link and all downstream packets are on another link [10], as shown in Fig.2 b).

a) Full flow asymmetry b) Consistent partial flow asymmetry

Fig.2 The classification of flow asymmetry: round point represents hosts and unidirectional arrow represents one-way flow

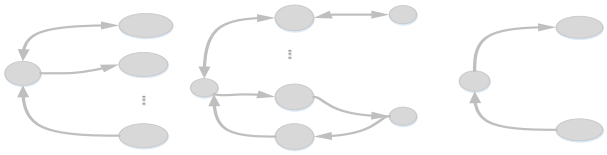
2) *IP asymmetry*

According to Sandvine [10], IP asymmetry mainly depicts asymmetric degree of host pair behavior, remote host behavior or local host behavior. There are three types of Full IP asymmetry, Partial IP asymmetry and Consistent IP asymmetry.

a) *Full IP asymmetry*: occurs when all flows from a given subscriber IP may be on different links [10], as shown in Fig.3 a);

b) *Partial IP asymmetry*: occurs when flows between the subscriber IP and a given endpoint are on the same link, but flows to a different Internet endpoint IP are on a different link [10], as shown in Fig.3 b);

c) *Consistent IP asymmetry*: occurs when all upstream traffic from an IP traverses one links, and all downstream traffic to an IP traverses another links [10], as shown in Fig.3 c).



a) Full IP asymmetry b) Partial IP asymmetry c) Consistent IP asymmetry

Fig.3 The classification of IP asymmetry: round point represents hosts, oval point represents passive observation point, bidirectional arrow represents two-way flow, unidirectional arrow represents one-way flow

B. Methodology

To the best of our knowledge, routing decision occurs for each packet dependence on destination IP address. Each packet in a flow should be destined for the same endpoint to follow same physical links in theory. Otherwise, routing between two endpoints is asymmetric. Our study methodology is passively evaluating each packet in a flow whether traverses the observed intermediate node or not. TCP is a connection-oriented, reliable transmission protocol. If not all packets in a flow traverse the passive observation point, the TCP flow between two endpoints is flow asymmetry.

Suppose the path between end hosts A and B is a sequence of network element equipment. The path of i-th packet traverses a sequence of m routers from hosts A to B:

$$F_{AB}^{(i)} = (H_A, f_1^i, f_2^i, \cdots, f_o^i, \cdots, f_m^i, H_B) \qquad (1)$$

and the reverse direction path of j-th packet traverses a sequence of n routers from host B to A:

$$R_{BA}^{(j)} = (H_B, r_1^j, r_2^j, \cdots, r_o^j, \cdots, r_m^j, H_A) \qquad (2)$$

Where , $f_k$and r_t represent the forwarding nodes, such as router. Specially, suppose that f_o and r_o are our passive observation points.

According to above the definition of routing symmetry, if all packets of the forward direction and the reverse direction in a flow has a same router path, and the forward sequence of F_{AB} and the reverses sequence of R_{BA} is equal in reverse order, the flow is routing symmetry. If $f_o$and r_o is not the same observation point, the TCP stream can be seen as an asymmetric flow. The logical measurement topology shown in Fig.4 (R2 and R3 are our passive observation point). For example, all packets router path of host A to host B is (HostA, R1, …, R2, …, R4, HostB) and all packets router path of host B to host A is (HostB, R4, …, R3, …, R1, HostA), the TCP stream is routing asymmetry. Moreover, if the passive measurement point not observes all packets of a flow, the TCP flow is also routing asymmetry because of not all packets in a flow take same physical links. Based on the methodology of flow asymmetry, we additional analyze the conditions of client IP, server IP and a pair of IP address appeared in different physical links to measure asymmetric degree of host pair behavior, remote host behavior or local host behavior. In summary, our method is presented in table 1.

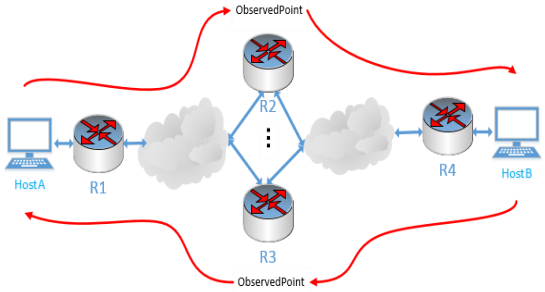


Fig.4 Overview of asymmetric traffic

TABLE I. CLASSIFICATION OF ASYMMETRIC TRAFFIC

Router Asymmetry	***Classify***	***ISN_C2S***	***tuple4***	***TCP_Handshake_Integrity***	***Flow_Type***	***Observer_Point_Num***	***Inconsistent TTL***	***LostPkt***
Flow asymmetry	Full flow asymmetry	√	√	×			√	√
		√	√	√			×	√
		√	√	√			√	×
	Consistent partial flow asymmetry	√	√	√	One-way Flow	=2	√	√
IP asymmetry	Full ip asymmetry		IP	×			√	√
			IP	√			×	√
			IP	√			√	×
			IP	√	Two-way Flow	>1	√	√
			IP	√	One-way Flow	>2	√	√
	Partial ip asymmetry		IP-pair	√	Two-way Flow	=1	√	√
			IP-pair	√	One-way Flow	=2	√	√
	Consistent ip asymmetry		IP	√	One-way Flow	=2	√	√

C. Flow Data Structures

UDP traffic is inherently asymmetrical traffic. Moreover, TCP traffic is a larger composition of Internet traffic. We should pay more attention to analyzing TCP traffic and detecting TCP behaviors. According to RFC 5470 [11], a flow defined by the 5-tuple of source and destination IP address and port number and transport layer protocol number. Due to the protocol of NAT and cloud computing technology is widely used in network, there is a phenomenon that port reuses and IP reuses in real network. For TCP stream, 5-tuples {src_ip, src_port, dst_ip, dst_port, proto_id} is not the unique properties for defining a flow. So, we redefine a TCP flow by 6-tuple {init_seq_c2s, src_ip, src_port, dst_ip, dst_port, protocol_id}. For the purpose of measurement, we design the flow data structures shown in table 2:

TABLE II. TCP STREAMS DATA STRUCTURES

Field	Type	Remark
Observer_point	String	Passively observation point information
Observer_point_num	Number	the value of observer_point_num is depict how many a flow or a IP show up in passively observation point
ISN_C2s	Number	The init sequence number of SYN packet of client-to-server
Tuple4	String	Client_ip, client_port, server_ip, server_port
C2s_pkt	Number	The number of client-to-server packet
S2c_pkt	Number	The number of server-to-client packet
C2s_bytes	Number	The bytes of client-to-server packet
S2c_bytes	Number	The bytes of server-to-client packet
TCP_Handshake_Integrity	Number	Packets of TCP connection whether be observed completely or not
Flow_Type	Number	Type of one-way or two-way flow, such as c2s, s2c and csc
Inconsistent TTL	Number	equal cost multi-path routing lead to packets in a flow have different TTL
LostPkt	Number	all packets in a flow whether traverse the passive observation point or not

c2s :client-to-server one-way flow s2c :server-to-client one-way flow
csc : two-way flow

IV. TRAFFIC MEASUREMENT AND ANALYSIS SYSTEM WITH SPARK

A. Measurement scenario

As shown in Fig.5, there are 39 measurement nodes of 6 data centers and more than 3Gbps of bandwidth per node. Many passive measurement nodes generate large data volumes. One key difficulty is a demand for efficient technology for processing large-scale dynamic data stream in real time. DPDK is a high performance packet I/O framework [12]. Apache Spark is designed for real time analysis of high velocity live data streams [13]. In order to meet the high bandwidth and multiple observation points measurement requirements, we designed and implemented the scalable passive network traffic measurement and analysis system, as shown in Fig.6.

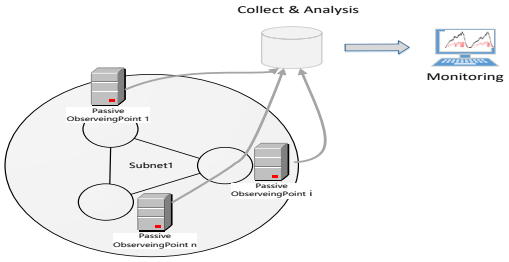


Fig.5 Overview of Traffic Measurement System deployment in ISPs network

B. Traffic Measurement ansd Analysis Framework

As shown in Fig.6, our system consists of four modules. Packet Processing Module is a DPDK-based high-performance packet processing system, which has four functions that are packet capture, flow sampling, flow information extraction and flow information in JSON format sent to Kafka. Kafka is a scale-out and high throughput distributed streaming platform [14]. Big-Data Analysis Module is a Spark-based memory computing system. And Data-Visualization Module is used for visualizing the analyzed results into a chart in real time.

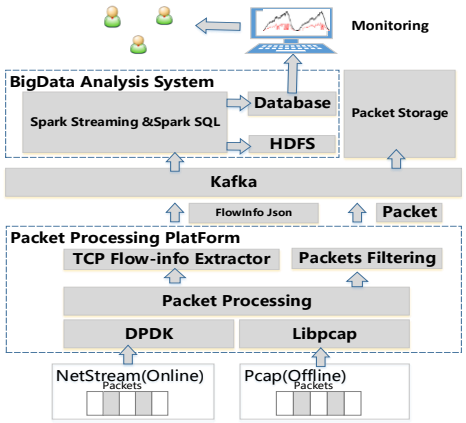


Fig.6 Compositions of The Traffic Measurement and Analysis System

1) TCP Traffic Sampling

Flows provide an aggregated view of network traffic by grouping streams of packets [15]. Multiple passive observation points can generate a large amount of traffic data. To effectively reduce the network traffic data, keep the characteristics of the network traffic data information and maintain data consistency on multiple nodes, we propose a proper flow sampling algorithm that sample client IP or server IP of new 6-tuple {init_seq_c2s, client_ip, client_port, server_ip, server_port, protocol_id}. For example, as shown in Fig.4, if the upstream of a flow that passes the router R2 has been sampled, the downstream must be sampled at router R4 for keeping data consistency.

2) Flow Information Extractor

Before performing traffic analysis in spark, we need to extract TCP stream information such as table 2. To gather all network packets of a flow with a set of common properties by using traffic processing technology, we defined a large flow

table and used multi-thread technology to process traffic. If the captured packet is SYN or SYN+ACK packet and the packet is sampled successfully, we will build a record in the flow table and assign a thread to process subsequent network packets belong to the flow. When captured a RESET or FIN packet or timeout signal of the flow record in the flow table, we transfer the flow information in JSON format to Kafka and remove the corresponding record in the flow table. The process is presented in Fig.7.

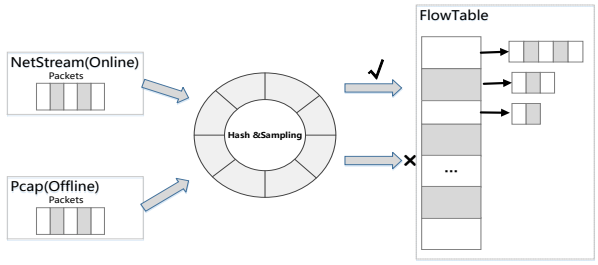


Fig.7 Overview of Flow Information Extractor

3)Spark Big-data Analysis System

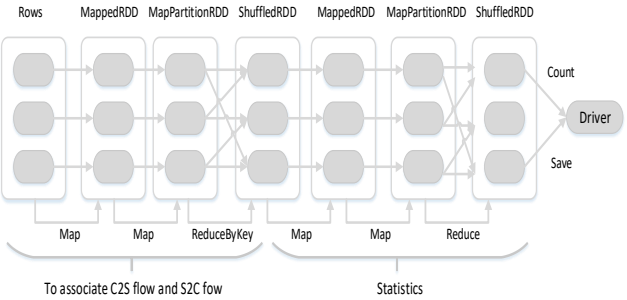


Fig.8 Logical Process of Spark Analysis Procedure

As shown in Fig.8, we use Spark Streaming technology, Spark SQL technology and other complex analysis algorithm to analyze the data that ingested from Kafka based on windowed computations mechanism. There is a key challenge is accurate asymmetry traffic correlation. For conveniently matching C2S unidirectional flow and S2C unidirectional flow, we are treat 6-tuple {init_seq_c2s, src_ip, src_port, dst_ip, dst_port, protocol_id} as new 6-tuple {init_seq_c2s, client_ip, client_port, server_ip, server_port, protocol_id} by the port number comparison. And then saving the analyzed results in HDFS or database.

V. REAL DATA STUDY

We deploy our Packet Processing Platform in 6 data centers of ISPs network for capturing sampled TCP stream in real time and will generate 400,000 TCP connection's metadata per second. Spark analysis procedure runs on a spark cluster of 23 servers sand occupies 23 cores in total and 2GB memory per node. And we promise not to abuse the privacy of network traffic.

A. Anomalies/Noise data

In experiment, we find that there is a large amount of TCP traffic without data and account for more than 70% of client-to-server (C2S) traffic, as illustrated in Fig.9. It seems like a DDOS attack or malicious scanning have occurred in the network. Here we will temporarily treat one-way traffic without data as noise data. Subsequently, we analyze network traffic after excluding the noise data.

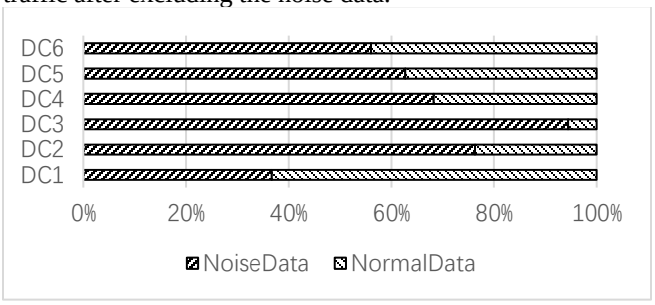


Fig.9 Noise Data Flow Ratio

B. One-way Flow and Asymmetric Routing

As shown in Fig.10, we have found that the one-way traffic accounts for more than 90%, the ratio of two directions is nearly same and the routing policy of data center 3 is different from others. It suggests that asymmetric routing is pervasive phenomenon throughout network. Meanwhile, we evaluate the asymmetric traffic in terms of flow asymmetry and IP asymmetry that shown in table 3.

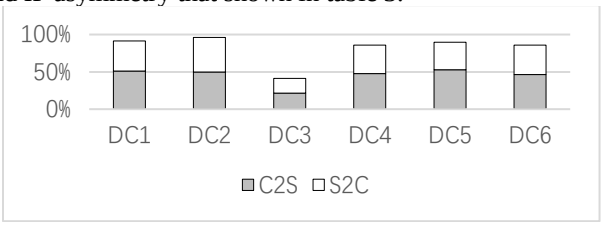


Fig.10 One-way Traffic Flow Ratio

TABLE III. THE MEASUREMENT RESULTS OF TWO TYPE OF ROUTING ASYMMETRY

	Flow asymmetry						**IP asymmetry**								
	Full flow asymmetry			***Consistent flow asymmetry***			***Full IP asymmetry***			***Partial IP asymmetry***			***Consistent IP asymmetry***		
	Flow (%)	**Packet (%)**	**Bytes (%)**	**Flow (%)**	**Packet (%)**	**Bytes (%)**	**Flow (%)**	**Packet (%)**	**Bytes (%)**	**Flow (%)**	**Packet (%)**	**Bytes (%)**	**Flow (%)**	**Packet (%)**	**Bytes (%)**
Time1	93.3	96.27	91.82	1.38	2.40	0.78	75.15	90.58	92.54	11.4	6.20	0.42	0.30	0.21	0.01
Time2	94.4	95.82	92.11	1.39	3.94	4.71	83.35	92.80	94.82	13.2	5.07	0.26	0.25	0.10	0.16
Time3	87.5	88.42	87.28	1.40	2.15	1.57	85.31	87.77	87.69	13.1	3.57	5.52	0.43	0.12	0.18
Time4	89.6	93.93	94.70	1.67	2.48	2.22	84.25	84.92	86.57	12.3	6.96	0.41	0.32	0.06	0.04
Time5	84.5	89.23	91.13	1.87	1.86	1.12	77.97	78.96	82.17	11.9	2.42	0.26	0.28	0.11	0.07
Time6	90.5	92.80	92.77	1.33	1.25	1.15	72.82	75.38	79.45	13.7	7.97	0.52	0.31	0.13	0.09
Time7	93.9	94.43	94.38	1.09	1.76	0.95	83.66	83.91	87.28	10.5	7.27	0.79	0.27	0.21	0.13

Firstly, we quantify routing asymmetry at flow level. flow asymmetry mainly depicts asymmetric degree of the network packet in a flow. We observe that over 90% of TCP flow is full flow asymmetry. As introduced in the previous section, we find that most of packets in a flow be routed by multiple physical links due to the equal cost multi-path routing. On this type of flow asymmetry can be explained by the load-balancing policy applied in the ISPs network. Network traffic dynamic transfer in space and time, it is very hard to associate upstream traffic and downstream traffic. There are about 1.3% of TCP flow that is a consistent flow asymmetry. However, we suspect that the percentage of consistent flow asymmetry will be higher if we can collect network traffic from more passive observation points

Secondly, we evaluate routing asymmetry at IP level. IP asymmetry mainly depicts asymmetric degree of host pair behavior, remote host behavior or local host behavior. Table 3 depicts that over 70% of TCP traffic is full IP asymmetry. It suggests that most of IP address appears on different links. Only about 11% of TCP traffic generated by pairs of IP address that appear on same physical links within the time window. However, the proportion of consistent IP asymmetry is much lower. Aiming at the phenomenon, our explanation is that most routing is done on a flow- or IP-Pair level in order to minimize jitter and out-of-order packets within sessions [1].

In a word, our measurement results fit our understanding of the inter-domain routing system, and we can also know the specific asymmetric degree of the network traffic, which can provide help for network security, model and management.

VI. CONCLUSION

In this paper, we propose a scalable passive traffic measurement system combines DPDK-based traffic processing technology and Spark-based streaming computing technology to overcome the difficulty of limited computing and storage resources for network traffic measurement and analysis. The system can help in monitoring the tendency and fluctuation of routing asymmetry with data visualization, which can provide useful help for network management and enhance the understanding of the inter-domain routing system. Through experiments conducted in a carrier grade network that has 6 data centers, we have found that over 90% of TCP flows are asymmetric and over 70% of flows from full IP asymmetry that a same IP address traverse different links.

In future work, we plan to use machine learning to further analyze network traffic based on this system. And we hope that the system designed and implemented practically by us can be useful for operators and researchers.

REFERENCES

[1] John, W., Dusi, M., & Claffy, K. (2010). Estimating routing symmetry on single links by passive flow measurements. IWCMC 2010 - Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, 473–478.

[2] He, Y., Faloutsos, M., Krishnamurthy, S., & Huffaker, B. (2005). On routing asymmetry in the internet. GLOBECOM - IEEE Global Telecommunications Conference, 2(858), 904–909.

[3] Anwar, R., Niaz, H., Choffnes, D., Cunha, Í, Gill, P., & Katz-Bassett, E. (2015). Investigating interdomain routing policies in the wild. ACM Internet Measurement Conference, IMC 2015, 2015–Octob, 71–77.

[4] Y. He, M. Faloutsos, and S. Krishnamurthy, "Quantifying Routing Asymmetry in the Internet at the AS Level," in IEEE GLOBECOM, 2004.

[5] V. Paxson. End to end behavior in the Internet. In Proceeding of the ACM SIGCOMM, Volume 26, number 4, page 25-38, August 1996.

[6] Glatz, E., & Dimitropoulos, X. (2012). Classifying internet one-way traffic. ACM SIGMETRICS Performance Evaluation Review, 40(1), 417.

[7] Orsini, C., King, A., Giordano, D., Giotsas, V., & Dainotti, A. (2016). BGPStream : A Software Framework for Live and Historical BGP Data Analysis. Proceedings of the 2016 ACM on Internet Measurement Conference (ACM IMC'16), 429–444. [12]E.

[8] Oztoprak, K., & Yazici, M. A. (2017). A hybrid asymmetric traffic classifier for deep packet observation systems with route asymmetry. 2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC 2016

[9] U. of Oregon. Route Views Project. http://www.routeviews.org/, 2015.

[10] R. Ghosh and G. Varghese, Symmetrical routes and reverse path congestion control. Technical Report TR-97-37, Department of Computer Science, Washington University, St. Louis, September 1997.

[11] Sadasivan, G., Brownlee, N., Claise, B., Quittek, J.: Architecture for IP Flow In- formation Export. RFC 5470 (Informational) (2009)

[12] DPDK, http://www.dpdk.org/

[13] Spark, http://spark.apache.org

[14] Kafka, http://kafka.apache.org/

[15] Gill, P., Schapira, M., & Goldberg, S. (2013). A survey of interdomain routing policies - Slides. ACM SIGCOMM Computer Communication Review, 44(1), 28–34.