Asymmetric Routing Detection Based on Normal TCP Streams

Yanjun Su
School of Computer Science and Engineering
Southeast University
Nanjing, China
Emai: yjsu@njnet.edu.cn

Wei Ding
School of Computer Science and Engineering
Southeast University
Nanjing, China
Email: wding@njnet.edu.cn

Lihua Miao
School of Computer Science and Engineering
Southeast University
Nanjing, China
Email: lhmiao@njnet.edu.cn

***Abstract*—The misconfiguration of border routers may cause asymmetric routing in enterprise networks or campus networks which connect to multiple ISPs. In this paper, an asymmetric routing detection method is proposed to solve this problem. The method checks the integrity and symmetry of TCP streams by setting test conditions, thus judging the existence of asymmetric routing in TCP connections. Our method is applied to IP Traces collected on the border of Jiangsu education and research network. The results show the existence of asymmetric routing. In particular, the method can accurately locate where the routing misconfiguration occurs.**

Keywords-TCP; the TCP stream; asymmetric routing

I. INTRODUCTION

Under the current architecture of the Internet, an enterprise network using access services of multiple ISPs needs to allocate the corresponding IP addresses in different ISP's access channel. The situation generally exists in the campus network of CERNET. In reality, this work is supported by border routers in most of the enterprise networks and the campus networks. So any configuration error of border routers may lead to the occurrence of asymmetric routing and it is difficult to be found. In general, asymmetric routing that is out of the design scope will cause a series of problems. By mathematical modeling and simulation approach, Wu Haitao [1] proved that asymmetrical path may result in a decrease of TCP throughput. The situation becomes more serious when there is a large difference between the bandwidth of two routes. In addition, asymmetric routing would cause large difference between hop counts in different directions and impact greatly on the performance of network transmission. Figure 1 shows the connections between *X*, *Y*, *ISP A* and *ISP B*. *X* is assumed to have an erroneous configuration in its border router, resulting in two asymmetric paths between *X* and *Y*. It can be seen from the figure that packets from *X* to *Y* need to pass through two ISP networks. This situation will cause an increase of network delay for clients. On the other hand, these packets will expand (line 2) additional bandwidth of backbone and have negative impact on network operators.

This paper proposes an asymmetric routing detection method to discover the asymmetric routing caused by erroneous configuration and solve the problem illustrated above, on the basis of analyzing the captured packets and the characteristics of TCP connections. The method checks the integrity and symmetry of TCP streams by matching one-way TCP flows and setting test conditions so as to get valid one-way TCP flows. Additionally, the positions of TCP endpoints are located through the IP ownership table, so we can even find out the organization which causes the asymmetric routing.

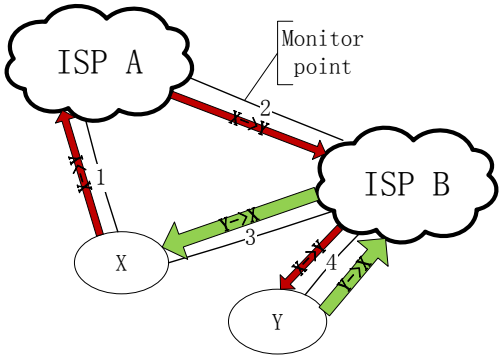

Figure 1. Asymmetric routing

II. THE CHARACTERISTIC OF TCP CONNECTION

TCP provides a connection-oriented, reliable byte stream service [2]. TCP is connection-oriented means that any two TCP applications (usually a client and a server) must establish a TCP connection before data exchange. Reliability is reflected in the ACK mechanism, timeout mechanism and retransmission mechanism. These interaction mechanisms provide a variety of important information for researchers. The following section will review the establishment and termination of a TCP connection.

The famous three-way handshake protocol is used to establish a TCP connection. As Figure 2 shows, the connection between *Sender A* and *Receiver B* needs a SYN packet, a SYN+ACK packet and an ACK packet to complete the connection establishment. The communication cannot begin data exchange until the completion of these handshakes. In general, the packets in the process of three-way handshake do not carry communication data, so their length is 40 bytes, including 20 bytes IP header and 20 bytes TCP header (without considering IP header options, and TCP header options).

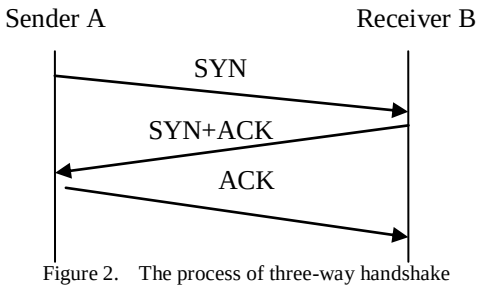

Figure 2. The process of three-way handshake

The establishment of a connection requires a three-way handshake, while the termination of a connection needs to go through a four-way handshake. As shown in Figure 3, when *Sender A* has completed its data exchange to *Receiver B*, a FIN packet is required to terminate the connection in this direction. After receiving the FIN packet, *Receiver B* should response by sending an ACK packet. The same process is also needed to terminate the connection on the other side. The four-way handshake which is incurred by the termination of a normal TCP connection is called orderly release. In some cases, TCP sends a RST packet instead of a FIN packet to release the connection. This process is called abnormal release, and the endpoint on the other side can terminate the connection directly and notify the application layer to reset without acknowledging the RST packet.

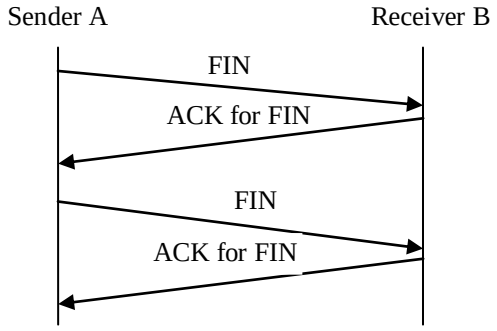

Figure 3. Normal termination of a TCP connection

From the analysis above, we can see that TCP has two important features, i.e. bidirectional feature and sequential feature. Bidirectional feature describes that TCP connection must have exchange packets in both directions. And sequential feature means that a TCP action must strictly obey the rules when establishing and terminating a connection. Our detection method is based on these two characteristics of a TCP connection.

III. PASSIVE MEASUREMENT DATA – IP TRACE

Network measurement can be classified as active measurement and passive measurement according to the measurement mode. In active measurement, the source node sends probe packets to the target link or the destination node and analyzes the network behavior through performance parameters returned from the network. Compared with the active measurement, passive measurement gets traffic from a specific node of the network rather than actively sending probe packets over the network. Passive measurement, which we use to detect the asymmetric routing, can obtain the overall status of the network and find out suspicious paths without increasing the burden of the network.

The passive measurement data referred in this paper are collected by East (North) Regional Network Center of CERNET with the purpose of supporting the collation and analysis of network data. The data are called IP TRACE and they were collected from the border channel of JSERNET (Jiangsu Education and Research Network). These data are stored in acquisition system [3] and classified into *in* direction and *out* direction. Packets in *in* direction are from out of JSERNET to JSERNET. The *out* stands for opposite packets.

IV. ASYMMETRIC ROUTIING DETECTION

A. Detection Principle

The detection method in this paper takes advantage of the features of TCP connections described above, which are called bidirectional feature and sequential feature. The bidirectional feature requires that packets must appear in both directions of TCP connection. So if packets of both directions are stored in IP TRACE, it means that there is no asymmetric path in the TCP connection. However, only one-way TCP flows stored in IP TRACE may prove that the data in the other direction does not go through the collection point and thus an asymmetric path exists. On the other hand, a normal TCP connection must be sequential which requires TCP connection to strictly obey the process of establishment and termination. So only when the specific packets such as a SYN packet are found in a one-way flow can it be a valid TCP flow. Therefore, only the one-way TCP flows which are sequential can be used to prove the existence of asymmetric routing.

B. Flow Record Generation Algorithm for IP TRACE

The detection principle described above is on the basis of flows. Since Claffy et al. proposed the concept of IP flow, network measurement methods in flow level have been intensively studied. The so-called IP flow is a collection of data packets that satisfy flow specification and timeout constraints [4] [5]. The flow-based approach is chosen for our detection method. Therefore, we must firstly apply grouping policy on the IP TRACE.

1) Packets in the same flow must have same source IP, destination IP, source port, destination port and protocol type;

2) When one of the following conditions satisfied, the data flow has to be terminated.

a) There is no new packet arrives in the last 16 seconds [6];

b) Packets with the FIN or RST flag arrive (only for TCP packets).

According to the grouping policy, packets that meet the conditions form a set, and all sets will be stored on hard disks in the format of flow records for follow-up study. Because our study is only for TCP packets, the protocol type of selected packets is 6. The format of flow record is shown in Figure 4. TCP flow record is a fixed data structure with the length of 35 bytes, including *Start Time*, *End Time*, *Source Address*, *Destination Address*, *Source Port*, *Destination Port*, *Total Bytes*, *Total Packets* and *TCP_flags*. *TCP_flags* indicates the result of cumulative OR of all TCP flags in this flow.

Timestamp(Start Time) (8 octets)	
Timestamp(End Time)(8 octets)	
Source Address (4 octets)	
Destination Address (4 octets)	
Source Port(2 octets)	Destination Port(2 octets)
Total Bytes(4 octets)	
Total Packets(2 octets)	Tcp_flags(1 octets)

Figure 4. The format of flow record

C. The Testing Conditions

Based on TCP connections' characteristics and flow records, the following two testing conditions are proposed for any flow record γ. Flow records that meet the following two conditions can be used to detect asymmetric routing.

1) During detection time, there is no flow record in the opposite direction of record γ.

2) The packet number of record γ must be no less than 4 and both of the SYN flag and the ACK flag are set, one of the FIN flag and the RST flag must be set; or the packet number is no less than 3, both of the SYN flag and the ACK flag are set and the average length of packets is more than 100 bytes.

A normal TCP connection has packets in both directions which is required by the bidirectional feature of TCP connection. But TCP connections filtered by the first condition are only unilateral data flows. These one-way flows are filtered by combining two-ways flows. If two flow records have same four-tuples but opposite directions, they will be marked as two-ways flows. The TCP flows which do not have any packet in the opposite direction during detection time will be marked as one-way TCP flows.

The purpose of setting the second condition is to filter out abnormal one-way TCP flows. Statistical analysis of IP TRACE points out that abnormal one-way TCP flows are mainly caused by network attacks such as SYN flood. If these attacks are intercepted by firewalls, unpaired one-way flows will be generated. Therefore, the second condition takes advantage of sequential feature to weed out abnormal one-way TCP flows. There are two cases under the second condition. If SYN flag is set, it means that the TCP connection has experienced three-way handshake. If FIN or RST flag is set, it means that the TCP connection used a FIN or RST packet to terminate the connection. In order to strengthen the condition, the maximum number of packets required for the establishing and terminating of the connection is set to 4. TCP connections in the second case also need to experience three-way handshake. The timeout period of grouping policy is set to a fixed 16s, which may lead a large flow to be split and FIN or RST packet is not recorded in this flow. The first case can't occur when it happens. So the average length of packets is added to check the effectiveness of TCP flows. If the average length is not less than 100 bytes, it shows that there are data packets apart from the symbolic packets. The existence of TCP packets with payload shows the TCP connection may be produced by an actual transmission instead of network attacks or abnormal behavior. The limit of the number of packets is obtained by summing up the maximum number of packets for establishing a connection and the minimum number of data packet with payload, which is not less than 3.

V. Experiment of Asymmetric Routing Detection

A. Data Sets

The collection point of IP TRACE is set up in the boundary channel of JSERNET, so IP TRACE contains interactive packets between all users in JSERNET and users out of JSERNET. However, the data selected in our study are only related to three schools in JSERNET, which are recorded as *A*, *B*, and *C*. The connection between each school and the *collection point* are shown in Figure 5. The gathering time of the experiment data sets is 00:00-23:59 in July 15, 2011.Table 1 describes some basic information of the three data sets, in which *Bytes* represents total bytes of TCP packets, *TCP/ALL Ratio* represents the proportion of TCP bytes in total bytes and *Flows* refers to the number of TCP flows in the data set.

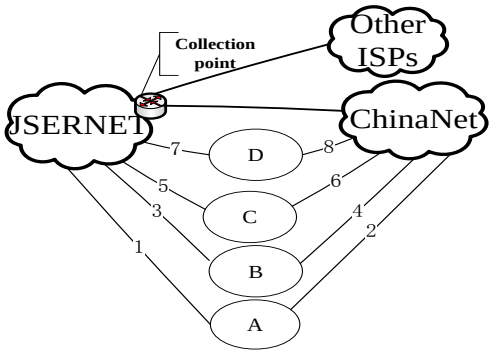

Figure 5. Network structure

TABLE I. Basic Informatin of Data Sets

No.	Direction	Bytes	TCP/ALL Ratio	Flows	Unmatched Flows	Result
A	in	49.6G	64.0%	14.2M	1.7M	38
	out	21.9G	10.0%	15.0M	0.3M	3
B	in	193.8G	73.2%	13.4M	2.9M	161
	out	106.2G	58.7%	10.3M	1.0M	12
C	in	335.3G	69.2%	15.7M	5.0M	670
	out	249.5G	15.2%	20.2M	1.0M	8,210

B. Experimental Results and Analysis

Flows from these data sets (Table 1) indicate a relatively large difference between two directions traffic. The asymmetry of TCP transmission which is caused by some abnormal behavior or the defects of network link can be inferred from the difference. In accordance with the first test condition, in which the first step is matching TCP flows in both directions to filter out flows that cannot be matched during detection time (24 hours), the number of such flows is shown in the *Unmatched Flows*. From this column we can see that there are a large number of unmatched TCP flows. So the second condition is needed to exclude abnormal TCP flows. The *Result* field shows the number of unmatched flows still remains after applying the second condition. These flows are chosen to detect asymmetric

routing. Fortunately, the ratio between *Result* and *Flows* tells that the asymmetric routing in these schools is at a pretty low level.

In order to locate the link where the erroneous configuration happens, batch query system for IP address [7] was applied to get the location of the endpoint. We produced detailed result for each school and made a test report. Due to the limited paper length and the network privacy risk, this paper only listed the test result of school *A*, and the statistical analysis of IP attribution is shown in Table 2. Flows were also separated into two directions. In *out* direction, the source address of flows belong to school *A* and the destination address are out of JSERNET. The situation is opposite in *in* direction. The location of IP address(not belong to school *A*) was split into two categories, one for IP address in CERNET, and the other for IP address out of CERNET which called others. Because the collection point is on the border of JSERNET, the proportion of IP addresses belonging to Jiangsu province must be obtained. Data in Table 2 shows that most of asymmetric routing of *in* direction appears in JSERNET. This phenomenon was also found in the test results of school *B* and school *C* and most of the interactions were from the same school *D* (Figure 5). This result was fed back to the center of JSERNET, and they verified that the school *D* indeed had configuration error in its border router. The connections between school *D* and the other three schools are shown in Figure 6. As a matter of fact, school *D* send packets whose destination IP address belonged to JSERNET to the other ISP (line 8), which causes the traffic designated to JSERNET sent back from the ChinaNet interface, resulting in asymmetric routing. It can be seen that the proposed detection method for asymmetric routing has great guidance for network monitoring and management. It can be used not only to test the specific unit, but also to find asymmetric routing for other units through the integrate detection of various units.

TABLE II. THE TEST RESULT FOR SCHOOL *A*

Direction	CERNET	CERNET in Jiangsu	Others	Others in Jiangsu
in	98.3%	99.5%	1.7%	8.8%
out	100.0%	0.0%	0.0%	0.0%

VI. CONCLUSION

This paper proposed an asymmetric routing detection method to detect the asymmetric routing problem in enterprise networks connecting to multiple ISPs. The method uses two features of TCP connections, i.e. bidirectional feature and sequential feature. The method is applied in monitoring three schools in JSERNET. The information of asymmetric routing provided by the test results is accurate, proving the feasibility of this method. Meanwhile, the test report generated by this method can not only help enterprise network managers to identify problems early, but also provide information for network operators to improve their billing system.

REFERENCES

[1] WU Hai-tao, LONG Ke-ping, WU Jing, and CHENG Shi-duan, MA Jian, “Performance Analysis of TCP over Bandwidth Asymmetry Networks,” Journal of Beijing University of Posts and Telecommunications, vol. 23, pp. 30-33, Dec 2000.

[2] W. Richard Stevens, TCP/IP Illustrated Volume 1:The Protocols. New Jersey:Addison-Wesley, 1994.

[3] http://iptas.edu.cn.

[4] Claffy K.C, Braun H.W, and Pulyzos G.C, “A parameterizable methodology for internet traffic flow profiling,” IEEE Journal on Selected Areas in Communications, vol. 12, pp. 1481-1494, 1995.

[5] Ryu B, Cheney D, Braun H.W, “Internet Flow Characterization: Adaptive Timeout Strategy and Statistical Modeling,” Workshop on Passive and Active Measurement, pp. 94-105, 2000.

[6] WANG Yuan, DING Wei, GONG Jian, “Study on TCP F low Timeout, “ Journal of Xiamen University (Natural Science), vol. 46, pp. 192-193, Nov 2007.

[7] http://202.112.25.134/Search/multiRequest.php.