Proceedings of the Asia-Pacific Advanced Network ***2012*** *v. 33, p. 65-75.*
http://dx.doi.org/10.7125/APAN.33.7
ISSN 2227-3026

Active and Passive Monitoring and Analysis of IP Option Header Transparency from Covert Channel Point of View

Katsuhiro Horiba [1,*], Yohei Kuga [1,*], Hiroaki Hazeyama [2] and Akira Kato [1]

1 KEIO University / 5322 Endo, Fujisawa, Kanagawa 252-0882, Japan
2 Nara Institute of Science and Technology / 8916-5, Takayama, Ikoma, Nara 630–0192, Japan

E-Mails: qoo@sfc.wide.ad.jp; sora@sfc.wide.ad.jp; hiroa-ha@is.naist.jp; kato@wide.ad.jp

* Author to whom correspondence should be addressed; Tel.: +81-466-49-3529; Fax: +81-466-49-1101

Abstract: In a context of network covert channels, unused header fields in communication protocols are vulnerable to embed secret data. An IP Option field in the IP header is considered as one of useful spaces for constructing the Internet-wide network covert channels. On the other hand, IP packets with IP Option have been said non-transparent on the global Internet. This paper investigates how an IP packet with IP option can be going through over the Internet by active and passive monitoring methods. At first, we investigated AS border traffic in an academic AS and a commercial IX. The result was that only four types of IP Options, Route Record (RR), Time Stamp (TS), No Operation (NOP) and End of Option List (EOOL), were observed. Then, we preliminary evaluated transparency of these four types IP Options over the global Internet by probing from ten Planetlab nodes on six countries against 5,000 randomly chosen destination IP addresses and 11,251 intermediate routers. Both destination addresses and intermediate routers were included in 1,132 intermediate ASes. As the active measurement result, 57% routers replied to IP packets with the RR Option, that is, the RR Option was transparent in 914 intermediate ASes on this experiment. On the other hand, 41% of intermediate routers replied probe packets with the TS option, that is, the TS Option was transparent in 811 intermediate ASes on this experiment.

Keywords: Network Covert Channel; Active and passive measurement; IP Option field

1. Introduction

Network monitoring and analyzing are important to know the behavior, trend or characteristics of the Internet. Network monitoring and analyzing also clarify security issues in the Internet today. Network covert channel is a hidden data communication that is unintended on the security policy of a network. Typical network covert channels, called storage channels, employ unused fields in communication protocols. IP is one of the most useful communication protocols in the Internet, because every Internet wide communication must use IP headers. In this paper, we focus on IP Option filed, the Option field in an IP header. IP Option field is used for many purposes such as measuring the Internet topology, achieving mobility, of course, constructing NCC. However, many reports have pointed that most ISPs have filtered or dropped such packets that have IP Option due to their security policy and / or the performance overhead of routers [8,9]. However, network policy in commercial ISPs can be changed. The assumption “IP Option is filtered or dropped” should investigate again from Network Covert Channel point of view. Therefore our objective is “how much transparent are IP packets with Option field in the current Internet?”.

To clarify reachability of IP packets with IP Option, we firstly developed a passive monitoring tool. We installed our passive monitor tool into AS borders of our academic AS (ASN 2500 WIDE) to check which type of IP Option had pass through on our AS borders. We also analyzed traffic datasets in commercial IX provided by CAIDA Project. The results were four types of IP Option (EOOL, NOP, TS and RR) were observed in our monitoring points, and 3 types of IP Option (EOOL, NOP and RR) were observed in CAIDA datasets.

On the other hand, we preliminary evaluated reachability of packets with IP Option by active measurements using Planetlab [10]. Our active measurement was rapid and lightweight active methodology that picked out the destination IP addresses from routable IP prefixes. In this active measurement, we focused only on clarifying major ASes behavior against IP Options. In result, many major ISPs still permitted the passage of packets with RR Option or TS Option.

This paper is organized as follows. Section 2 describes what Network Covert Channel is, and how IP Option is useful for network covert channel. Section 3 and Section 4 show our passive and active measurement methods and analysis of them, respectively. Finally, we summarize and discuss result of transparency of IP Option from the view of network covert channel.

2. Network covert channel and IP Options

As firstly pointed out by Lampsson [6], a covert channel can occur when an attacker finds and exploits a shared resource that is not designed to be a communication mechanism. Covert channels in networks or on network protocols are generally called as “network covert channels”. In particularly, “storage channel” or “storage covert channel” is one of techniques to create network covert channel. A storage channel embeds secret data into packets [4]. Ahsan reported there were several fields in IP and TCP headers to be employed as storage channels [2].

In particular, IP Option is very curious field in IP header from the view of network covert channel. IP Option is basically optional, variable length, and defined various behaviors. For example, TS (Timestamp) or RR (Record Route) options are basically filled by intermediate routers. The length of IP Option field is limited to 36 bytes at maximum. If IP Option field has been already filled, intermediate routers just forward IP packets with IP Options to next hops as well as IP packets without IP Options. There is no technique to validate who modified the TS or RR field of an IP packet. That means IP Option is very useful to hide secret data. On the other hand, IP Option is employed to investigate the transition of the Internet topology [5]. Thus, IP Option is interested not only in the view of the Internet wide network covert channels, but also in the Internet measurement research.

However, most of IP Option has been insisted to be filtered in commercial ISPs, because some of IP Options behaviors are recognized as vulnerability of routing architecture or network covert channels [8,9]. From the view of network covert channels and of the Internet measurement researches, the transparency of IP Option must be examined. Therefore, we investigated transparency of the IP Option in the global Internet.

3. Passive monitoring

3.1. Monitoring Method

Basically, traffic analysis traces the traffic datasets which are captured in backbone networks and stored in storage. John et.al tried to capture traffic on a 10 Gbps link on the border of a regional ISP and analyzed the captured traffic to clarify malicious activities [3]. Generally, link-speed has been faster and faster and links has been aggregated to correspond the growth of the Internet traffic, capturing and storing network traffic on backbone networks become harder and harder. As a result of these things, full packet capturing has been difficult, storage space has also been lacking and this mechanism hasn't already been suitable to detect malicious packets in real-time. Thus, network operators should change methods to monitor and analyze backbone traffic according to their own purposes.

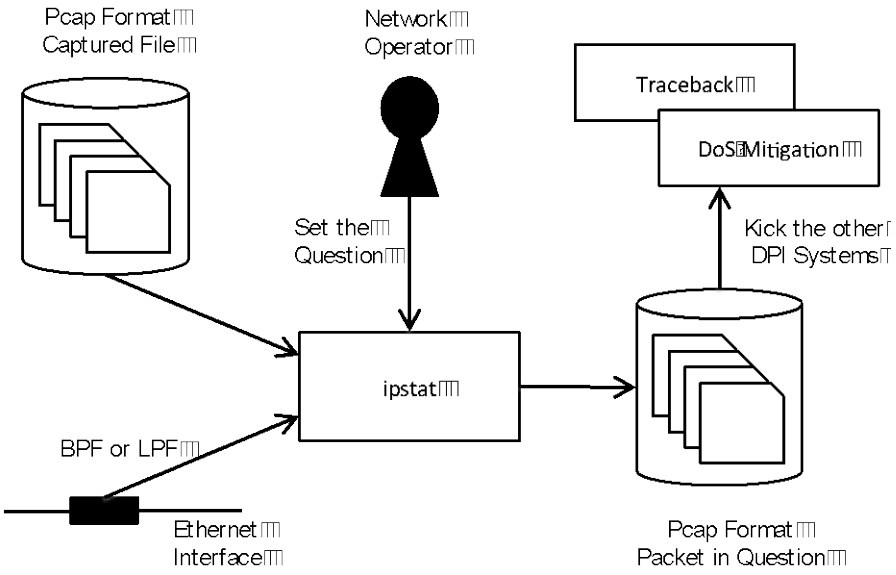

Figure 1. IPstat passive monitoring architecture.

According to such operational view, we designed and implemented IPstat passive monitoring architecture. Figure 1 shows the architecture of IPstat. Input of IPstat is pcap format files or packets through BPF interface of BSD or LPF interface of Linux. Basically, IPstat counts statistics of monitored packets. In addition to this, IPstat equips filter rules to highlight irregular packet header field, for example, TOS, ID or Option field isn't 0 in an IP packet. If a monitored packet is filtered as an irregular packet, IPstat stores the whole irregular packet into a Pcap format file. Also, a network operator can add other filter rules to capture his/her interested packets. Stored packets can be exported to other systems such as IP Traceback or DDoS Mitigation system.

This mechanism doesn't require huge size of memory, because most of regular packets are processed one by one and aren't stored into the storage. The concern is only PPS performance, but current NIC and general-purpose CPU have enough to monitor packets on a Gigabit Ethernet by IPStat with wire late.

3.2. Collection of Dataset

WIDE Project has been operated as AS (Autonomous System) number 2500. We installed optical taps on the two AS Border Routers' interfaces and monitored them by IPstat. One of two

AS borders connects to a Transit-AS (named Link-T) through a Gigabit Ethernet link, we call this link as Link-T. The other connects to an IX, named DIX-IE (Distributed IX in EDO), through a 10 Gigabit Ethernet link. We call the link to DIX-IE as Link-I. The data collections on LINK-T and LINK-I have been performed since November 2011. During this period, we separately monitored and captured packets with IP option on both directions on each link. We also use CAIDA's Anonymized 2012 Internet Traces Dataset [1], named CAIDA-Dataset in this paper. CAIDA-Dataset contains anonymized passive traffic traces from CAIDA's equinix-chicago and equinix-sanjose monitors on high-speed Internet backbone links since 2008. To compare our AS border links and CAIDA-Datasets, we chose data from LINK-I and Link-T at 19th January 2012, and from CAIDA at 17th January 2011 and19th January 2012. However, CAIDA provided shorter time traffic data than ours. We picked up 1 minute data from these lists on each identical time.

3.3. Analysis of Passive Monitoring

Figure 2 shows the number of monitored packets with IP Option on the direction from AS2914 to AS2500 in Link-T, and figure 3 shows that on the direction from DIX-IE to AS2500 in Link-I. According to figure 2 and 3, only four types (EOOL, NOP, RR, ES) of IP Option monitored on the incoming direction to AS2500 in both Link-T and Link-I. From these results, we can predict commercial ISP filtered most of IP Options except for NOP, EOOL, TS and RR.

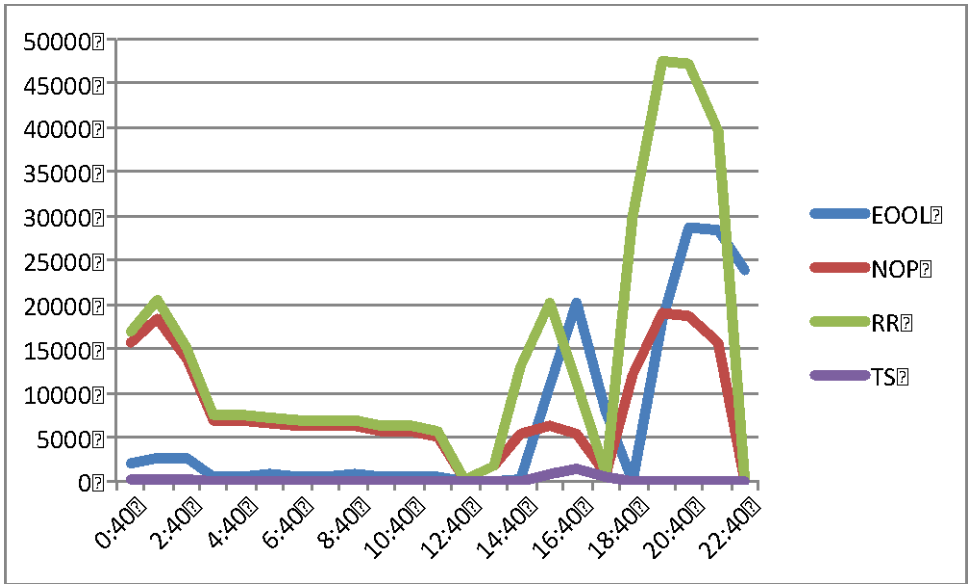

Figure 2. IP Option from AS 2914 to AS 2500.

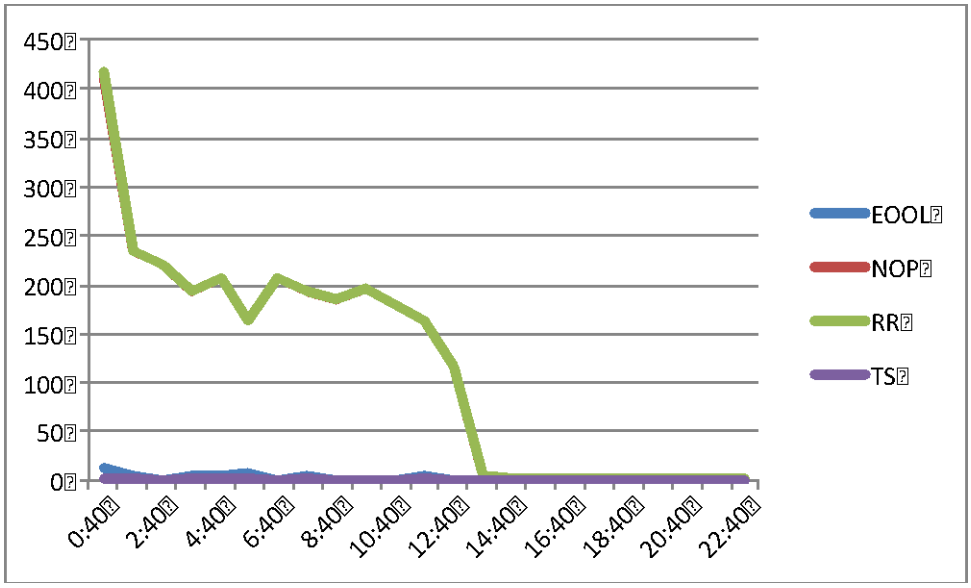

Figure 3. IP Option from DIX-IE to AS 2500.

Probe packets by iPlane project team [7] were the majority of monitored packets with TS and RR options, which were employed to investigate Layer-3 go and return paths.

Figure 4 shows statistics of monitored the direction from AS2500 to AS2914 in Link-T from 1st November 2011.There were 19 types of IP Option which included some undefined Option values. According to the result of deep packet inspection, the source address of undefined IP options is only one host. The host was a manufactured router, and the type of all packets with irregular IP options from the host was ICMP echo reply. Destination IP addresses of these packets were irregular or unallocated addresses like 0.0.178.203. In any cases, IP Option that was coming from other ASes were only four types which we explained above.

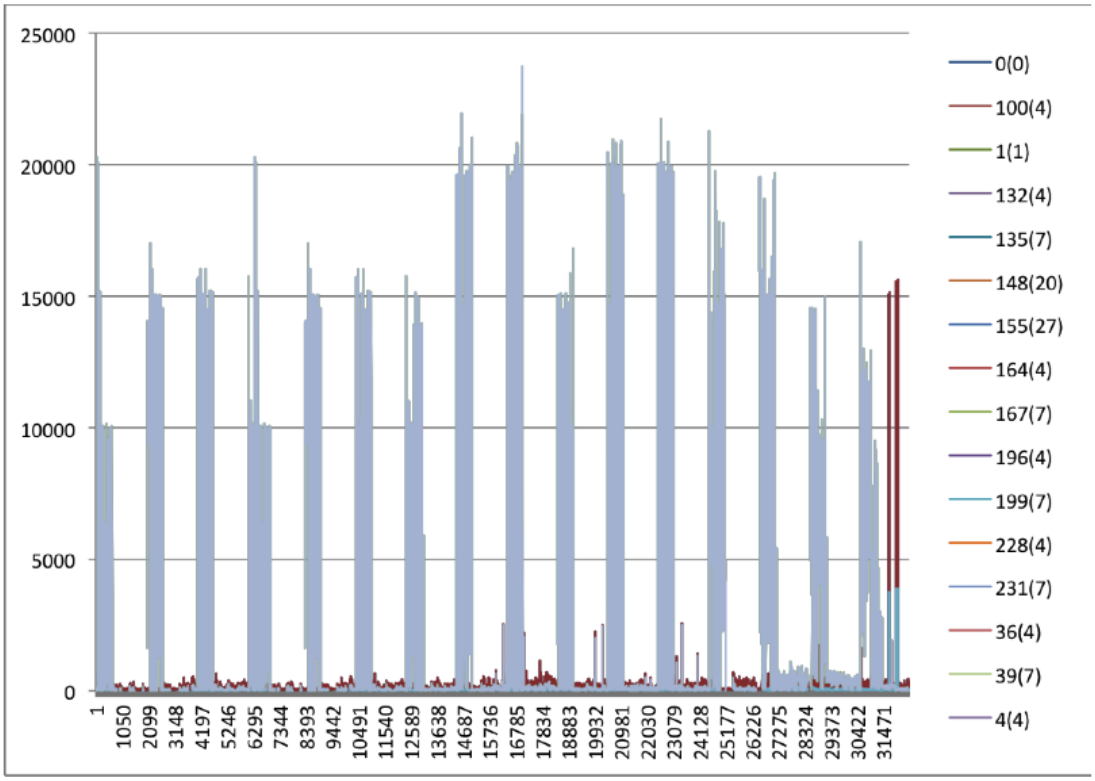

Figure 4. IP Option from AS 2500 to AS 2914.

Table 1 shows the statistic result of IP Option on CAIDA-Dataset. In CAIDA-Dataset, we couldn't find packets with TS Option. Most packets with RR option in CAIDA-Dataset had been filled by intermediate routers before these packets reached to the monitoring points of CAIDA. This result indicates that packets with RR option would be transparent.

Most of packets with TS Option monitored in WIDE were sent by iPlane project that we mentioned above. Probing packets by iPlane may be sent based on their schedule or algorithms, therefore, iPlane's packets might not be included in the time frame of CAIDA-Dataset. Thus, we should check much more samples to find out packets with TS Option.

Table 1. Statistics of CAIDA Anonymized Traffic

#. Option by Place and Time	17th Jan. 11 SanJose	17th Jan. 11 Chicago	17th Jan. 2012 San Jose
EOOL	12	17	10
NOP	10	9	12
RR	11	13	15
TS	0	0	0
Total Packets	15,285,909	5,355,928	30,801,712

4. Active Measurement

Our next goal is to check the reachability of packets with TS or RR option through major ISPs. In this section, we explain our active measurement method and results of our active measurement.

4.1. Methods

The Internet topology is always changing, and it's difficult to measure the properties on the Internet scale. Sometime, a macroscopic measurement is looked like DDoS (Distributed Denial of Service) attack, so we must take care of the network loads caused by our active measurement.

Figure 5 shows our methodology for checking the reachability of IP Option, and describe detail of individual method in following sections.

1. Generate a list of ping-able IP addresses from BGP full route datasets.
2. Select random IP addresses from the list, and check whether each selected random IP addresses replies ICMP echo. If a selected random IP address returns ICMP echo reply, set the selected random IP address as a target of our active measurement.
3. Execute traceroute toward selected random IP addresses in process 2, and send packets with IP Option to each hop' IP address on the route.
4. Refer the ASN of each hop's IP address from an active BGP table.

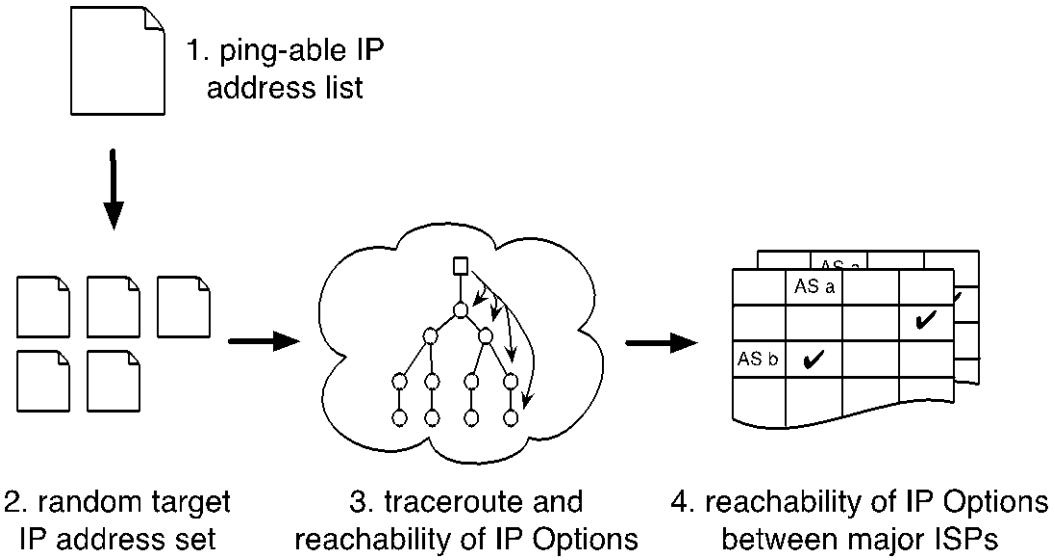

Figure 5. Our active measurement method.

4.2. Random target IP address set

Generally, discovering Internet topology uses ping and traceroute. These network dialogue tools need to set a destination IP address. We generated destination IP addresses on two steps. At first, we generated a list of existing IPv4 addresses as ping-able IP addresses from BGP datasets. We used BGP datasets to grasp routable IPv4 prefixes. We surveyed the existing routes using Routeviews [11] and RIPE's [12] full route BGP dataset.

Secondly, we generated random target IP address set from the ping-able IP address list to avoid generating a DDoS attack by our active measurement, and ensured equality of routes on the Internet. We expanded multiple routes shorter than /24 route. For example, a route with /16 prefix length will be expanded to 256 /24 routes. Note that, there is no difference in the all IP addresses in the minimal size of route.

These random IP addresses may yet fail to have reachability although the route is appeared on the Internet. Of course, unreachable routes and IP addresses are not necessary to investigate transparency and intermediate node's behavior of IP Option. Therefore, we examined such whether these random IP addresses return ICMP echo reply, and we extracted surely ping-able random IP addresses.

Along with these steps, we picked up 1,000 random targets IP addresses as a target IP address set in one trial. In this paper, we conducted 5 trials, that is, we used 5,000 random IP addresses to examine the reachability of IP Option on the Internet.

4.3. Discovering IP route and reachability of IP Options

We employed traceroute and scamper [10] tool to evaluate the reachability of IP Option. Traceroute is a network dialogue tool to discover the IP route toward a destination IP address. Scamper is a network dialogue tool that can conduct Internet measurement tasks to large numbers of IP addresses. Scamper can send an IP packet with RR Option and TS Option through traceroute like method. In this paper, we used ten Planetlab nodes on five countries; CN, JP, IT, UK and US.

4.4. Analysis of Active Monitoring

We tested the reachability of packets with RR or TS Option against 5,000 random target IP addresses by active measurement method mentioned above from ten Planetlab nodes. The measurement result included 11,251 intermediate routers' IP addresses in 1,332 ASes. Then, we focused on the transparency of these IP Options between major ISPs. We extracted major ISPs' AS numbers from the result of intermediate routers' IP addresses. Note that the major ISP in this paper means top 100 ASes of CAIDA's AS ranking [13] based on AS link out-degrees.

RR option passed through 57% of measured intermediate routers, that is, RR option was transparent over 914 ASes. Focusing on major ISPs, 63 major ISPs forwarded packets with RR option. On the other hand, packets with TS option were forwarded by 41% of measured intermediate routers, that is, TS option was transparent over 811 ASes. Among major ISPs, 67 major ISPs passed through TS option. We couldn't observe any special filter policy that changed filter rules according to the incoming AS of a packet. Finally, we focus top 10 ISPs in CAIDA AS rank. Only one ISP of top 10 ISPs dropped packets with RR option or TS option.

5. Summary

We investigated transparency of IP Option to clarify vulnerability of network covert channel using IP Option field. According our analysis of passive monitoring on our AS borders and CAIDA anonymized traffic dataset, most IP Options were likely filtered in commercial ASes, except for EOOL, NOP, RR and TS options.

We built a stationary measurement to check reachability of TS / RR Options among major ASes. In result, some major ASes filtered any IP Options, however, many major ASes didn't drop TS and RR Options. Along with these measurement results, storage covert channel using TS or RR option is useful in the current Internet, especially when a packet can go across major ISPs.

In our future work, we will check the time series result focusing major ISPs, and we will evaluate IPv6 cases with measuring extend IP header behaviors.

Acknowledgements

This document is supported by a commissioned research named "Research and Development on Evaluating Security of Communication Protocols and its Implementations" (2011) of National Institute of Information and Communications Technology (NICT), Japan. Also, CAIDA's Internet Traces is provided by the National Science Foundation, the US Department of Homeland Security, and CAIDA members.

References

1. kc claffy, D. Andersen and P. Hick,; The CAIDA Anonymized 2012 Internet Traces - <dates used>, http://www.caida.org/data/passive/passive_2012_dataset.xml
2. K. Ahsan.; Covert channel analysis and data hiding in TCP/IP. Master Thesis for Graduate Department of Electrical and Computer Engineering University of Toronto, 2002.
3. W. John and S. Tafvelin.; Analysis of Internet Backbone Traffic and Header Anomalies observed. In Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement 2007, San Diego, California, USA, October 24-26, 2007. ACM, 2007.
4. T. Handel and M. Sandford. Hiding data in the OSI network model. LNCS Information Hiding 1174:23–38. 1996.
5. E. Katz-Bassett, H. V. Madhyastha, V. K. Adhikari, C. Scott, J. Sherry, P. Van Wesep, T. Anderson, and A. Krishnamurthy.; Reverse traceroute. In Proceedings of the 7th USENIX conference on Networked systems design and implementation, NSDI'10, pages 15–15, April 2010.
6. B. W. Lampson.; A note on the confinement problem. Communication of the ACM, 16(10):613–615, October 1973.
7. H. V. Madhyastha, E. Katz-Bassett, T. Anderson, A. Krishnamurthy, and A. Venkataramani.; iPlane Nano: path prediction for peer-to-peer applications. In Proceedings of the 6th USENIX symposium on Networked systems design and implementation, NSDI'09, pages 137–152, April 2009.
8. Cisco Systems, Inc.; ACL Support for Filtering IP Options, http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtipofil.html
9. F. Gont, R. Atkinson and C. Pignataro.; Recommendations on filtering of IPv4 packets containing IPv4 options. IETF OPSEC (Operational Security Capabilities for IP network Infrastructure) Working Group draft (BCP), March, 2012, http://tools.ietf.org/html/draft-gont-opsec-ip-options-filtering-04
10. Planetlab,http://www.planet-lab.org/
11. M. Luckie.; Scamper, http://www.wand.net.nz/scamper
12. Routeviews, http://www.routeviews.org/
13. RIPE NCC, http://www.ripe.net/
14. CAIDA AS Ranking, http://as-rank.caida.org/