Outfitting an Inter-AS Topology to a Network Emulation TestBed for Realistic Performance Tests of DDoS Countermeasures

Hiroaki Hazeyama*, Mio Suzuki†, Shinsuke Miwa†, Daisuke Miyamoto*, and Youki Kadobayashi*
* Nara Institute of Science and Technology, Takayama 8916-5, Ikoma, Nara, Japan
Email: {hiroa-ha, daisu-mi, youki-k}@is.naist.jp
Phone: +81-743-72-5216 Fax: +81-743-72-5219
† National Institute of Information and Communications Technology, Nukuikita-machi 4-2-1, Koganei, Tokyo, Japan
Email: {mio, danna}@nict.go.jp
Phone: +81-42-327-6277 Fax: +81-42-327-6640

***Abstract*— One of the significant requirements for testing a software implementation of an inter-AS DDoS countermeasure is to measure the performance of the implementation in a large scale topology with typical DDoS tools and traffic. Ideally, an emulated inter-AS topology with same scale of the real Internet will provide similar characteristics of the real Internet if the same number of physical servers or facilities are used. However, the number of available physical nodes in a network emulation testbed are limited to tens or hundreds of physical servers. Boosting the number of nodes by virtual machines is not suitable to measure actual software performance.**

We take a filtering approach in order to pick up a subgraph from the whole inter-AS topology of the real Internet to fit the facilities of a network emulation testbed. Considering required characteristics for realistic evaluation results, we propose four filtering techniques. In this paper, we try to evaluate and discuss the pros and cons of our filtering approaches and the appropriateness of the emulated inter-AS topologies created by our filtering methods.

I. Introduction

To evaluate the scalability of a DDoS countermeasure, such an experimental environment is needed that is similar to the real Internet for as long as possible. Of course, it is difficult to construct an experimental network which has same size, same facilities, and / or same characteristics of the real Internet. Therefore, some emulation techniques should be taken to solve trade-offs among the scale of a test topology, the limitation of available resources, and the similarity to the real Internet.

In this paper, we tackle to create an emulated Internet for testing the scalability of a DDoS countermeasure. As a first step of this trial, we focus on testing "inter-Autonomous System(AS) Traceback" [1] for facilitating to construct an emulated Internet. A required topology for testing the traceback system is an emulated inter-AS topology, that is, an emulated IPv4 / IPv6 eBGP topology. We employ the topology to evaluate our implementation's performance, namely the message routing overhead, round trip time of a traceback message, or false positive / false negative rate of a traceback trial in inter-AS level. For constructing emulated Inter-AS topologies, we take a dataset of inter-AS topologies of the real Internet from a snapshot of IPv4 / IPv6 AS topology measurement dataset. Using these dataset we explore appropriate ways to map these inter-AS topologies onto a network emulation testbed(NET).

One of the significant requirements for testing an inter-AS packet traceback implementation is using physical servers to measure the performance of the implementation. However, the number of available physical nodes in a NET are limited to tens or hundreds of physical servers. Boosting the number of nodes by virtualization is not suitable to measure actual software performance. Imagine if several virtual machine(VM) instances run on one physical node, and one VM instance become heavily loaded. The physical node would also become heavily loaded and it would affect other VM instances which run on the physical node.

We take a outfitting approach in order to pick up a subgraph from the whole inter-AS topology to fit the facilities of a NET. According to the consideration about required characteristics for realistic evaluation results, we propose four inter-AS topology filtering techniques. In this paper, we try to evaluate and discuss the pros and cons of our filtering approaches and the appropriateness of the emulated topologies created by our filtering methods.

This paper is composed of following sections. Section II refers related work. In Section III, we explain our current emulating method for an inter-AS topology on NETs. We explore filtering rules against a whole inter-AS topology of the real Internet in Section IV, and discuss the limitation of our approach in Section V. Finally, we conclude this paper in Section VI.

II. Related Work

A. Network Emulation Testbed

A NET is composed of several physical nodes and two Ethernet network, one is management network, the other is experimental network. Several large scale NETs has operated for researches, Netbed in emulab [2] and DETER [3], StarBED in NICT Hokuriku Research Center [4], ModelNet [5], PlanetLab and PlanetLab6 [6], etc.

A user in NET has to design his/her experimental layer 3 network topology. Then, the user generates actual network configuration files and injects them to NET nodes. To handle numerous physical or virtual nodes, various NET configuration tools have been researched and developed [3], [7]–[10].

In our emulation trials, we use two NETs. One is StarBED, which is a large scale centralized testbed composed of 3 master servers, 830 physical nodes for clients, 8 core layer 2/3 switches. The other is NET in our lab., named GARIT, a small centralized NET constructed by 1 master server, 40 Sunfire Blades for clients, 2 Ethernet switches for constructing a management network and an experimental network, and 13 Alaxala 3630 routers which can speak eBGP and generate sFlow packets. Using these two NETs, we explored filtering methods of AS topologies.

B. AS Relationship Dataset

We employ an AS Relationship Dataset(ASRD) to create large scale inter-AS topologies as like as Korkmaz et. al did [11]. We take two datasets for AS relationship. One is CAIDA Projects' IPv4 ASRD [12]. Supported by Route Views Project [13], CAIDA Project measured BGP4 full route information in several backbones and analyzed an inter-AS topology according to an inferring method mentioned in [14]. The other is IPv6 AS topology data measured by State Key Lab. [15].

An ASRD shows the state of each link between two active ASes. Variation of link state is determined by an algorithm described in [14]; *provider link*, *customer link*, *p2p link* and *siblings link*. Around 7th, Jan., 2008, there were 26,961 IPv4 ASes announced by 2 byte AS Number (ASN), and 583 IPv6 ASes existed. These link information were announced by BGP or BGP+.

C. Approaches On Creating Realistic Experimental Networks

Several researches have explored appropriate realistic topologies to evaluate DDoS countermeasures.

Gong et. al [16] simulated their inter-AS packet traceback with 3 large scale inter-AS topologies to evaluate deployment scenarios of their inter-AS packet traceback protocol. Their first topology was a 8998-node subgraph of an inter-AS topology generated from 3 weeks of CAIDA's data collected from 1 to 23 June, 2004 [12]. They also considered a randomly generated an inter-AS topology with 10,000 nodes created by BRITE (2006) [17] using the Barabasi and Albert (BA) model in generating their second topology. They mentioned that both of their inter-AS graphs obey commonly observed power-law degree characteristics of the Internet. Gong's third topology was a 30×30 mesh which were intended to investigate the impact of long paths on the traceback performance.

Zhang et.al. tried to outfit a subgraph of the real Internet onto 72 nodes of DETER testbed [18] to evaluate multi-origin AS (MOAS) attacks. They chose ASes according to tier-level mentioned in [19]. There were three Tier-1 ASes, four Tier-2 ASes and seven Tier-3 ASes. Each Tier-1 AS had three fully connected zebra routers. The three Tier-1 ASes were full meshed. In 4 Tier-2 ASes, two of them multi-home to two Tier-1 ASes, the others only connect to one Tier-1 AS. Tier-3 ASes emulate stub ASes. Carl et.al also tried to construct a subgraph of an inter-AS topology in the DETER testbed [9] to evaluate MOAS attacks. They outfitted 50 ASes subgraph of 22086 measured ASes by Route Views in April 1, 2006. Chertov et al. developed useful topology generation tools [20] for their experiments on DETER. Their tools can construct Inter-AS and Intra-AS topology based on real topology data obtained by their tools and Route Views project. Their tools can pick up a set of ASes from the dataset, or can perform breadth-first traversal of the topology graph from a specified AS number.

III. Specifications of current emulated environment

The main purpose of our emulation trial is creating an scalable test environment for such binary codes that forward messages over inter-AS level. As a first step, we define the emulation specifications with consideration to the basic requirements for an inter-AS message forwarding environment and the cost on development. The current specifications are as follows;

1) *Use no virtual node*
   To avoid overheads, we decide not to use virtual nodes.
2) *Allocate one AS to one physical node*
   Because of the limitation of available resources and of scoping into inter-AS level performance test, we run only 1 eBGP software router for each AS.
3) *Construct eBGP topology with zebra/quagga daemon and bgpd daemon*
   In this experiment, we use zebra/quagga for routing daemons.
4) *Use 2 byte ASN for eBGP peering*
   Although 4 byte ASN is announced gradually, the number of announced 4 byte ASN is small. To avoid troubles caused by 4 byte ASN, we use only 2 byte ASN topology.
5) *Assign private addresses for each peering link and each local subnet*
   Ideally, allocated global addresses should be used to construct an emulated inter-AS topology, however, such emulated inter-AS topology environment must be isolated from the real Internet completely, not to cause routing accidents. Current StarBED facilities doesn't provide such isolated environment, therefore, we use private address space to construct emulated eBGP network.
6) *Use IP alias for BGP peering in a same layer 2 network*
   Because of limited number of 802.1Q TAG VLAN, we cannot allocate different VLAN number to each eBGP peering link. Due to this reason, we consider such eBGP peering environment that there are large scale Layer 2 Internet eXchange point (L2IX) and any eBGP router connect to this L2IX with only one interface. Using IP alias, we can assign different IP address to each subnet for eBGP peering.

Algorithm 1 Top-Ranking Filtering

```
procedure Top-Ranking Filtering
load AS_RELATIONSHIP_DATABASE into ASN_LIST
calculate ASRANK_SCORE from ASN_LIST
sort ASN_LIST order by ASRANK_SCORE
for all asn from ASN_LIST do
    select NEIGHBOR_ASN_LIST from ASN_LIST by asn
    sort NEIGHTBOR_ASN_LIST order by ASRANK_SCORE
    for all neighbor_asn from NEIGHBOR_ASN_LIST do
        select direction from AS_LIST by pairs(asn, neighbor_asn)
        output asn, neighbor_asn, direction
        increment number_of_output_asn
        if number_of_output_asn > THRESHOLD then
            break
        end if
    end for
end for
```

7) *No routing costs*
   The scope of this paper is outfitting subgraphs from the real Internet's inter-AS topology, therefore, we don't set routing cost in any eBGP daemons.
8) *Use no DNS servers in experiments*
   The DNS topology is quite different from the inter-AS topology. Emulating DNS topology is also different function from emulating inter-AS topology. Due to the out of scope in this paper, we don't use name resolution by DNS.

These specifications are chosen to create a primitive emulated inter-AS topology. An emulated inter-AS topology along with these specification lacks several functions of the real Internet. For example, our specifications cannot emulate inter-AS private peering and/or network bandwidth that CAIDA did not observe or did not publish. It is beyond the scope of our traceback experiment. However, these factors are important for emulating realistic Internet, so we would like to use them in our future work.

IV. Exploring Filtering Rules

Because of the limitation of available physical resources on a NET, we have to outfit the whole inter-AS topology to generate subgraphs according to the number of available resources. In this section, we try to explore several filtering rules to create a subgraph of an inter-AS topology. As a result of our exploitation, we develop four filtering rules, *Top-Ranking Filtering (TRF)*, *Root-AS Neighbors Filtering (RANF)*, *Region-Based Filtering (RBF)* , and *List-Based Filtering (LBF)*.

We implement our four filtering rules as several scripts written in Ruby or Perl. These scripts are available in AnyBed [10]. In the following sections, we explain each filtering rule.

A. Top-Ranking Filtering Rule

Our first filtering rule is Top-Ranking Filtering (TRF). This filtering rule is very simple filtering approach. CAIDA Project provides AS Rank based on ASRD and IP allocation data. As shown in Algorithm 1, TRF simply picks *N* ASes from Rank 1 AS.

When we tried this simple filtering method, some problem occurred, which we call "Isolated Island Problem". Isolated Island Problem is that a subgraph of an inter-AS Topology, which is composed of selected Top N ASes, included an AS that has no neighbor in the subgraph, or a subgraph is separated into several pieces. Because of the complexity on the peering by policy, several Top rank ASes don't peer due to the competitor. Two competitors are connected by one middle rank AS which will not be included top N ASes.

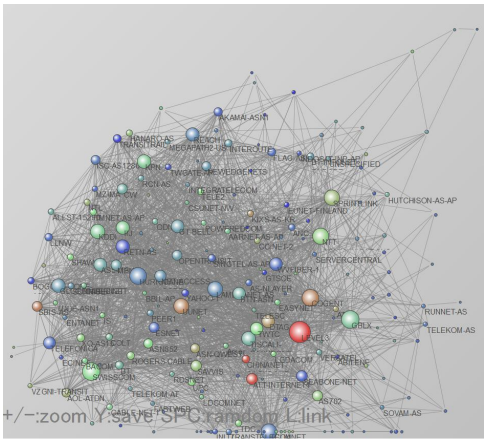

Fig. 1. Top 200 ASes in 7th Jan., 2008

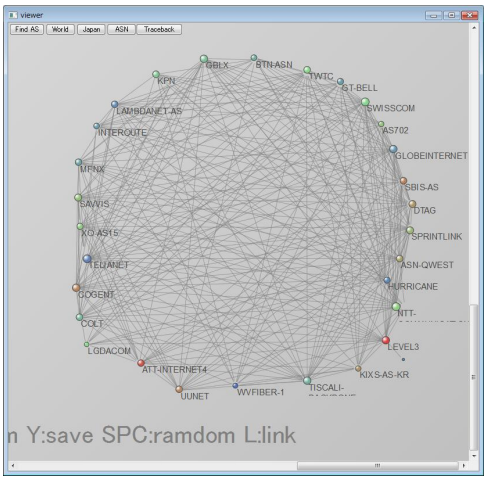

Fig. 2. Top 30 ASes in 7th Jan., 2008

Moreover, when only tens ASes will be selected by TRF, the generated inter-AS topology will include only tier-1 or tier-2 ASes and the inter-AS topology becomes a full-meshed inter-AS topology. Such small inter-AS topology by TRF shown in Fig.2 may not be suitable if an experimenter wants an inter-AS topology which includes all tier-level ASes.

B. Root-AS Neighbors Filtering Rule

The second filtering approach is Root-AS Neighbors Filtering (RANF) which picks up M hop neighbor ASes from a base point which is a user-specified AS. The pseudo-code of RANF can be described as Algorithm 2. Figure 3 shows a subgraph of the IPv4 inter-AS topology in 7th Jan., 2008 CAIDA IPv4 relationship, which includes the Root AS (AS 2500, WIDE backbone) and AS 2500's 1 AS hop neighbors. RANF can generate subgraphs both in a view of tier-1 AS and a view of a leaf AS.

Algorithm 2 Root-AS Neighbors Filtering

```
procedure Root AS Neighbor Filtering
load AS_RELATIONSHIP_DATABASE into ASN_LIST
input ROOT_AS
input HOP_THRESHOLD
TARGET_ASN_LIST ← ROOT_AS
for all i such that 0 ≤ i ≤ HOP_THRESHOLD do
    for all asn from TARGET_ASN_LIST do
        select NEIGHBOR_ASN_LIST from ASN_LIST by asn
        for all neighbor_asn from NEIGHBOR_ASN_LIST do
            select direction from AS_LIST by pairs(asn, neighbor_asn)
            output asn, neighbor_asn, direction
        end for
        TARGET_ASN_LIST ← NEIGHBOR_ASN_LIST
    end for
    increment i
end for
```

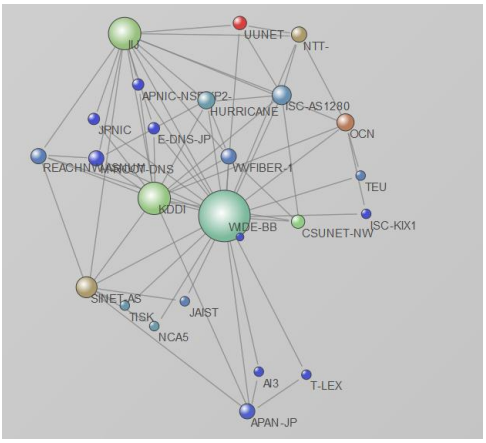

Fig. 3. One-hop neighbor ASes from AS 2500

One of significant problems on RANF is "Overflow Problem", that is, RANF will select much more number of ASes than the number of available physical resources, even if a specified hop number is few. Table I shows the number of N AS hop neighbors from each AS on 7th Jan. 2008 CAIDA's ASRD. For the number of 2 AS hop neighbors in 7th Jan. 2008 CAIDA's ASRD, the average was about 1012 ASes and the median was 249. The rank 1 AS on 7th Jan. 2008 CAIDA's ASRD had 16093 ASes in 2 AS hops away. Due to this characteristic of the real Internet, RANF easily overflows the number of available physical nodes on a NET.

C. Region-Based Filtering Rule

Our third filtering rule is Region-Based Filtering (RBF). The ASN allocation is managed by IANA and each regional Network Information Centers (NICs), such as ARIN in continent level, and JPNIC in country level. According to ASN registration information on a NIC, RBF selects ASes from ASRD only if an AS registered its ASN in the NIC. Because of locality on each region, RBF can pick up both core ASes and leaf ASes. An inter-AS topology filtered by RBF is useful to evaluate a deployment scenario of an inter-AS DDoS countermeasure as a regional service. Figure 4 shows the inter-AS topology in 7th Jan. 2008 filtered by RBF along with JPNIC's ASN registration information, which is composed of 448 JP domain ASes.

RBF has both "Isolated Island Problem" and "Overflow Problem". Isolated island problem on RBF is that some leaf

TABLE I

NUMBER OF NEIGHBOR ASES IN M HOP LENGTH IN 7TH JAN. 2008

hop	Ave.	Med.	Max.	Min.	Var.
1hop	4	2	2632	1	1117.018781
2hop	1012	249	16093	1	1997463.541
3hop	8242	8669	19138	1	31408380.44
4hop	12083	12408	19293	13	17390663.62
5hop	4703	3003	18879	48	18787808.11
6hop	826	194	18460	0	3133877.343
7hop	79	10	15284	0	194370.5825
8hop	5	0	4157	0	5324.307586
9hop	0.2	0	322	0	26.45993019
10hop	0.003	0	8	0	0.024914061

Algorithm 3 Region-Based Filtering

```
procedure Region-Based Filtering
load AS_RELATIONSHIP_DATABASE into ASN_LIST
load REGIONAL_AS_RELATIONSHIP_DATABASE into REGION_LIST
input IS_REGIONONLY_ENABLE
for all pairs(asn, neighbor_asn, direction) from ASN_LIST do
    if IS_REGIONONLY_ENABLE == TRUE then
        if REGION_LIST(asn) == EXIST AND REGOIN_LIST(neighbor_asn) == EXIST then
            output asn, neighbor_asn, direction
        end if
    else
        if REGION_LIST(asn) == EXIST OR REGION_LIST(neighbor_asn) == EXIST then
            output asn, neighbor_asn, direction
        end if
    end if
end for
```

AS(es) will be isolated from other ASes in a same region by RBF. The two ASes, which are placed in the left upper side on Fig. 4, are isolated from other JP domain ASes. The isolated island problem makes it difficult to identify troubles in setting eBGP configurations and / or running an experiment. This problem occurs when an AS is connected to another AS on the same region through other region AS(es). Most isolated island problems can be easily avoided by including 1 AS hop other region neighbor ASes in RBF, because most ASes connect to a tier 1 or tier 2 AS as an upstream neighbor. Algorithm 3 shows the pseudo-code of RBF with padding 1 hop neighbors in other regions. Figure 5 represents JP domain ASes and 1 AS hop other region ASes, which was used to evaluate our inter-AS packet traceback [1]. All 669 ASes in Fig. 5 have routes among each other.

The overflow problem in RBF will occur if RBF filters ASRD according to a continent level ASN registration information. The number of allocated ASN of RIPE was 11770 in 7th Jan. 2008. The overflow will occur even when an experimenter uses a large scale NET such as StarBED [4] if the experimenter tries to map a continent level inter-AS topology by RBF.

D. List-Based Filtering Rule

Our fourth filtering rule is List-Based Filtering (LBF). LBF is similar to RBF. The difference between LBF and RBF is that LBF doesn't assume that listed ASes are in same region. Algorithm 4 is the pseudo-code of LBF. Along with a given ASes list, LBF searches the shortest paths among each listed AS till a specified threshold of AS hop length, and picks searched AS paths from ASRD. LBF is useful to construct an inter-AS topology which contains specific ASes,

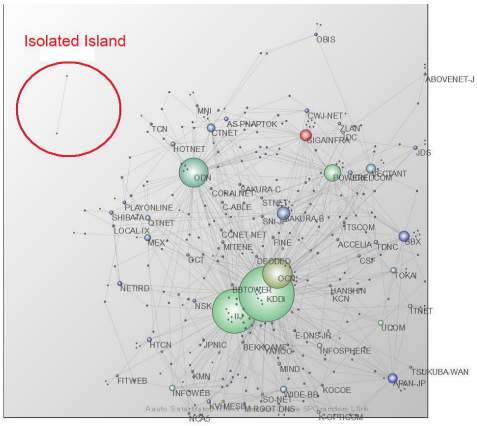

Fig. 4. JP domain ASes in 7th Jan., 2008

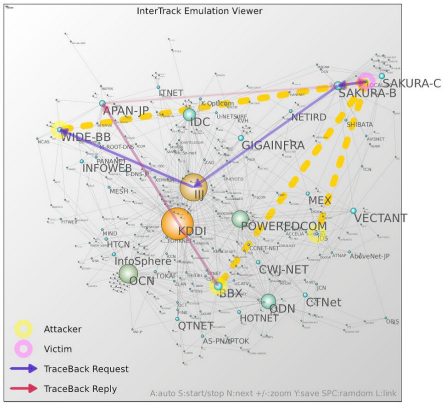

Fig. 5. JP domain ASes and one AS-hop neighbors in 7th Jan., 2008

for example, an inter-AS topology to evaluate countermeasures against DDoS attack to root DNS servers. Figure 6 shows LBF filtered inter-AS topology with a list which contains 14 ASes for 13 root DNS servers. Each yellow circle in Fig. 6 is the AS which propagates routes to each root DNS server.

Due to the characteristics of the route searching algorithm in LBF, an isolated island problem never occurs in LBF. The overflow problem will occur when the number of listed AS is over or close to the number of available physical nodes. The overflow problem also occurs if listed ASes are far from to each other. For example, an inter-AS topology by LBF with 9 listed ASes, namely AS27086, AS31009, AS12803, AS28924, AS8536, AS31002, AS42192, AS30790, AS42292, becomes almost same size as the original ASRD, because AS 27086 is located 10 AS-hop away from other 8 ASes.

E. Comparison Among Filtering Rules

Here, we try to compare pros and cons of each filtering rules with Zhang's Tier Level Filtering (TLF) approach. Table II shows a comparison among each filter rules. Comparing with TLF, our four filtering rules are semi-automated filtering algorithm. Although they have such semi-automatic characteristic, our filtering algorithms have the isolated island problem

Algorithm 4 List-Based Filtering

```
1: procedure List-Based Filtering
2: load AS_RELATIONSHIP_DATABASE into ASN_LIST
3: input SELECTED_ASN_LIST
4: input HOP_THRESHOLD
5: for all asn from SELECTED_ASN_LIST do
6:     NEIGHBOR_ASN_LIST ← remove(asn) from SELECTED_ASN_LIST
7:     for all neighbor_asn from NEIGHBOR_ASN_LIST do
8:         for all i such that 0 ≤ i ≤ HOP_THRESHOLD do
9:             NHOP_LIST ← N_HOP_NEIBHOR(asn, i)
10:            for all pairs(nhop_id, nhop_asn) from NHOP_LIST do
11:                if nhop_asn == neighbor_asn then
12:                    call Print AS Path(asn,neighbor_asn,nhop_id)
13:                    break
14:                end if
15:            end for
16:            break
17:        end for
18:    end for
19: end for
```

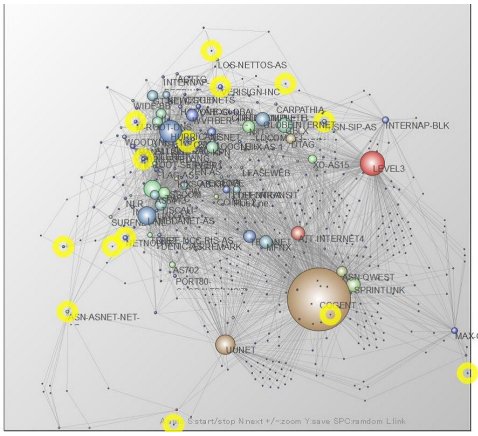

Fig. 6. A subgraph which interconnects 14 ASes for root DNS servers

and the overflow problem.

However, our semi-automatic filtering algorithms will expedite editing well-considered ASN list for TLF. Of course, each filtering rule can be combined to generate small scale inter-AS topology for a small scale NET such as GARIT in our lab.. Figure 7 shows a small subgraph for evaluating inter-AS packet traceback implementations in GARIT.

V. Discussion

A. Model of An Autonomous System toward More Realistic Experiments

The model of AS on our emulated inter-AS network was simplified as consisting of a single AS border router and some network links to other ASes. This simplification would make it difficult to emulate ASes connected by multiple links via multiple border routers such as MOAS experiments [9]. Multiple border routers on a single AS have to be emulated when a target experiment would require high fidelity emulation of network links, because they are popular for redundantly connecting to other ASes. Furthermore, the routing policy of each border router on the emulated inter-AS network might not be accurately emulated, because a route filter on each bgpd.conf.

We think that the original Route Views dataset and the Routing Assets Database (RADb) [21] could help us to infer relationships of border routers and their policies.

TABLE II

PROS AND CONS OF EACH FILTERING RULE

	TRF	RANF	RBF	LBF	TLF
Tier Level	top	all	all	all	all
View	tier-1	various	a region	various	various
Isolated Island	occurs	never	occurs	never	never
OverFlow	never	easily occurs	occurs	occurs	rarely occurs
topology	mesh	various	various	various	various
Required Info.	# of ASes	root ASN hop length	ASN list	ASN list	ASN list
operation	auto	semi-auto	semi-auto	semi-auto	manual

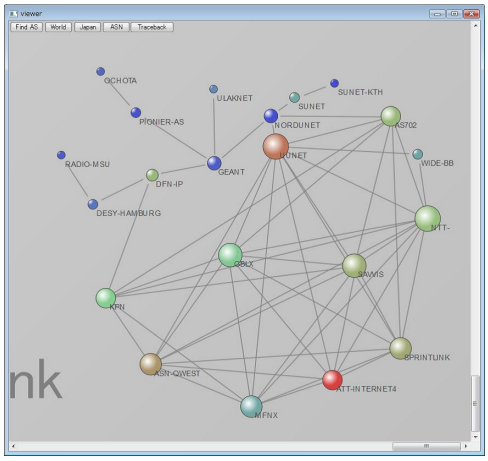

Fig. 7. A small subgraph filtered by combined rules

B. Emulating Intra-AS topology

Our assumption that assigning 1 node for 1 AS would omit the various behavior which comes from intra-AS networks. We are aware that major reminder part of our Internet emulation is the intra-AS network emulation. The intra-AS network emulation would require many observations of the real intra-AS networks such as Rocketfuel [22] to emulate intra-AS network as the real one, because intra-AS networks have their respective topologies and various constructions.

C. Fidelity of Emulation

Fidelity of Emulation is an important issue in constructing more realistic experimental environments. We expect that behavior of a software router are different from behavior of actual router instruments. If higher fidelity were required, higher fidelity of router implementation would have to be provided by employing hardware routes in spite of software routing daemons, or by using a virtualization / emulation technology such as CISCO 7200 Simulator [23].

VI. CONCLUSION

It is difficult to map subgraphs of the real Internet onto a network emulation testbed to evaluate DDoS attack and / or DDoS countermeasures. In this paper, we proposed four filtering rules to pick up subgraphs of the inter-AS Topology of the real Internet for mapping subgraphs onto network emulation testbeds according to typical situation of DDoS attacks and deployment situations of a DDoS countermeasure. Although the limitation of our emulation approach and of our filtering rules exist, our filtering rules will help experimenters to construct semi-realistic inter-AS topologies to evaluate their inter-AS level DDoS countermeasures.

ACKNOWLEDGMENTS

This work was a part of ”Research and Development on Traceback Technologies in the Internet” sponsored by the National Institute of Information and Communications Technology(NICT).

REFERENCES

[1] H. Hazeyama et.al., “An Autonomous Architecture for Inter-Domain Traceback across the Borders of Network Operation,” in *Proceedings of ISCC ’06*, June 2006, pp. 378–385.
[2] “Netbed built with emulab,” http://www.emulab.net/.
[3] T. Benzel et.al., “Design, Deployment, and Use of the DETER Testbed,” in *Proceedings of DETER community workshop 2007*, Aug. 2007.
[4] StarBED Project, http://www.starbet.net/.
[5] A. Vahdat et.al., “Scalability and Accuracy in a Large-Scale Network Emulator.” in *Proceedings of OSDI 2002*, Dec. 2002.
[6] “PlanetLab - An open platform for developing, deploying, and accessing planetary-scale services,” http://www.planet-lab.org/.
[7] T. Miyachi et.al., “StarBED and SpringOS: Large-scale General Purpose Network Testbed and Supporting Softwared,” in *Proceedings of Valuetools 2006*, Oct. 2006.
[8] M. Hibler et.al., “Fast, Scalable Disk Imaging with Frisbee,” in *Proceedings of USENIX Annual Technical Conference*, June 2003.
[9] G. Carl et.al., “Preliminary BGP Multiple-Origin Autonomous Systems (MOAS) Experiments on the DETER Testbed,” in *Proceedings of DETER community workshop 2006*, June. 2006.
[10] M. Suzuki, “AnyBed,” http://sourceforge.net/projects/anybed/.
[11] T. Korkmaz et.al., “Single packet IP traceback in AS-level partial deployment scenario,” *International Journal of Security and Networks (IJSN)*, vol. 2, no. 1, pp. 95–108, 2007.
[12] CAIDA: cooperative association for internet data analysis, “The CAIDA AS Relationships Dataset,” http://www.caida.org/data/active/as-relationships/.
[13] University of Oregon Route Views Project, “Route Views Project Page,” http://www.routeviews.org/.
[14] X. Dimitropoulos et.al., “AS Relationships: Inference and Validation,” *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 37, no. 1, pp. 29–40, 2007.
[15] IPv6 Team Of State Key Laboratory of Software Development Environment,BeiHang University, “IPv6 Backbone Network Topology (A Map of Ipv6 Internet),” http://ipv6.nlsde.buaa.edu.cn/index.htm.
[16] C. Gong et.al., “Single Packet IP Traceback in AS-level Partial Deployment Scenario,” in *Proceedings of IEEE GLOBECOM 2005*, Nov. 2005.
[17] A. Medina et.al., “BRITE: An Approach to Universal Topology Generation,” in *Proceedings of MASCOTS’01*, Aug. 2001.
[18] K. Zhang et.al., “Performing BGP Experiments on a Semi-realistic Internet Testbed Environment,” in *Proceedings of the 2007 Workshop on Experimental Computer Science*, 2007.
[19] L. Subramanian et.al., “Listen and Whisper: Security mechanisms for BGP,” in *Proceeding of NSDI ’04*, Mar. 2004.
[20] R. Cherto et.al., “Topology Generation, Instrumentation, and Experimental Control Tools for Emulation Testbeds,” in *Proceedings of DETER community workshop 2006*, June. 2006.
[21] Merit Network Inc., “RADb Routing Assets Database.” [Online]. Available: ”http://www.radb.net/”
[22] Rocketfuel, “An ISP Topology Mapping Engine,” http://www.cs.washington.edu/research/networking/rocketfuel/.
[23] C. Fillot, “Cisco 7200 Simulator,” http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator.