A Comparative Evaluation of Traceability in CJK Internet

Daisuke Miyamoto, Hiroaki Hazeyama, and Youki Kadobayashi

[1] National Institute of Information and Communications Technology
Traceable Network Group
4-2-2 Nukui-Kitamachi, Koganei, Tokyo 184-8795, JAPAN
daisu-mi@nict.go.jp
[2] Nara Institute of Science and Technology
Graduate School of Information Science
Internet Engineering Laboratory
8916-5 Takayama, Ikoma, Nara 630-0192, JAPAN
hiroa-ha@is.naist.jp
[3] Nara Institute of Science and Technology
Graduate School of Information Science
Internet Engineering Laboratory
8916-5 Takayama, Ikoma, Nara 630-0192, JAPAN
youki-k@is.naist.jp

Abstract. In this paper, we evaluate the traceability in IP traceback systems(IP-TBSs) by deployment simulation. In general, the traceability of attack sources or attack paths is expected to improve with the number of autonomous systems(ASes) participate in such systems. However, since there are various types of AS, such as core AS and leaf AS, the traceability would be would be affected by the types of network topology and/or the deployment scenario. Herein, we employ 3 types of emulated Internet topologies that resemble the inter-AS topology in China, Japan, and South Korea. We use 4 types of deployment scenarios to estimate the traceability of attack sources and attack paths. On the basis of the obtained results, we discuss the deployment scenario in each network region and demonstrate our scenario used in the field test conducted in the fiscal year 2009.

1 Introduction

Denial of Service(DoS) attacks exhaust the resources of a remote host or network that are otherwise accessible to legitimate users. According to a report published by Arbor Networks [1], the attack size in 2008 was 40 Gigabits, which was considerably greater than that in 2001(0.4Gigabits). Flood-based attacks were the most predominant among all attack vectors. In these cases, the attackers often used the source IP address spoofing technique. Therefore, it was difficult to identify the actual source of the attack packets using traditional countermeasures.

IP traceback aims to locate attack sources, regardless of the spoofed source IP addresses. Several IP traceback methods [2–4] have been proposed; especially Source Path Isolation Engine(SPIE) [4] is a feasible solution for tracing

individual attack packets. However, SPIE requires large-scale deployments for enhancing traceability. Traceability would decrease to a minimum if there were only a few routers to support SPIE.

Several researchers have proposed the use of AS-level deployment to facilitate global deployment of IP traceback systems(IP-TBSs). In this case, it is necessary to deploy an IP-TBS into each AS instead of implementing the SPIE in each router. Since the IP-TBS monitors the traffic between the AS border routers and exchanges information for tracing the issued packets, the traceback client can identify the source AS of the issued packet.

However, the traceability can be easily affected by the types of network topology and/or the deployment scenario. Gong et al. simulated traceability by using 3 types of artifactual network topologies [5], but their deployment scenario was the random placement; they selected ASes in a random manner. Castelucio et al. mentioned that IP-TBS should be deployed along with intent [6]. In their proposed "strategic placement", IP-TBSs were deployed in order of BGP neighbors. Hazeyama et al. proposed to emulate the Internet topology [7], that resembles the current Internet topology observed by CAIDA [8]. Hazeyama et al. also introduced 4 types of deployment scenario and estimated the traceability in the case of Japanese network topology [9].

Herein, we evaluated the traceability in China, Japan, and South Korea Internet using AS-level deployment. In our simulation, we created 3 types of emulated network topologies that resemble China, Japan, and South Korea, respectively. We also prepare 4 types of deployment scenario, namely, deployment in core ASes, deployment in leaf ASes, deployment in middle-class ASes, and deployment in a random manner.

The simulation results show that the traceability in the case of deployment into core AS outperforms that in the other 3 scenarios, regardless of the type of network topology. When the number of AS deploying the IP-TBS is 15, the pair of packet traceability and path traceability is (86.3%, 69.0%) in the Japanese network topology, (74.8%, 74.9%) in the Chinese network topology, and (92.6%, 93.4%) in the South Korean network topology. We observe that deployment for middle-classes is the second highest in almost of all cases, however, the pair of traceability is (18.5%, 11.6%) in the Japanese network topology, (27.3%, 22.9%) in the Chinese network topology, and (4.5%, 5.0%) in the South Korean network topology.

Our results also reveal the characteristics of the network topologies studied herein. In the Chinese network topology, middle-class and/or leaf AS are often interconnected. In contrast, many ASes in the South Korean network topology have established BGP peers with a few core AS. The characteristics of the Japanese network topology is a combination of those of the Chinese and South Korean network topologies. On the basis of these observations, we discuss the most suitable deployment scenario in each network region by using our FY 2009 field test scenario as the reference.

The rest of this paper is organized as follows: In Section 2, we present our related work, and we describe our simulation parameters, and we show our results

in Section 3. We discussed the applicability of deployment scenario in other network regions, in Section 4. Finally, we summarize our contributions in Section 5.

2 Related Work

2.1 Traceback Methods

Many researchers in the past have focused on IP traceback, the method used for which can be categorized into 3 types: ICMP traceback, probabilistic packet marking(PPM), and hash-based traceback.

ICMP traceback was proposed by Bellovin et al. [2], and was discussed in the IETF working group *itrace*. In this method, an iTrace router probabilistically samples an incoming packet with a very low probability (e.g., 1 out of 20,000) and generates an ICMP traceback message containing its own IP address as well as the IP address of the previous and next hop routers. Finally the router forwards the message either to the source or to the destination address. The disadvantage of ICMP traceback is that it requires a large number of attacker packets because of the lower probability of generation of ICMP traceback messages. In addition, the ICMP traceback may amplify the attack traffic, and/or the spoofed ICMP traceback messages can be easily transmitted by the attackers to disturb a traceback process. Hence, the ICMP traceback method has not been deployed yet.

In PPM [3], a router samples packets with quite low probability, and marks packets with its identification information as they pass through that router. The marking value overwrites a rarely used field in the IP header, usually IP identification field. By comparing with ICMP traceback, PPM has an advantage of that PPM does not amplify the attack traffic. PPM approach needs multiple packets due to the probabilistic nature, but FIT, proposed by Yarr et al. [10], requires tens of packets to identify an attack path with high probability. Moreover, there are several researches [11–14] that contributed to improve the scalability and efficiency of PPM. However, PPM has a critical problem in its approach. Since PPM-based method repurposes IP identification field, it damages existing service traffic that relies on IP identification field, e.g., IPsec VPN and video streaming [15].

Snoeren et al. [4] proposed Source Path Isolation Engine(SPIE), a hash-based IP traceback architecture wherein every router calculates a hash of an incoming packet and records the hash as a footprint of that the packet is transferred by the router. When a node is suffered from DoS attacks, the node (victim node) also calculates a hash from the attack packet, composes a traceback query including the hash, and sends the query toward the previous hop router. In comparison among ICMP traceback and PPM, SPIE has several advantages of that (i) it can determine the attack path with single packet, (ii) it can trace without interfering with the current version of IP protocols. Especially, Gong et al. mentioned [16] that SPIE can appeal to ISPs. In SPIE, the traceback process is requested by end hosts and accomplished by ISPs who can offer IP traceback as

a revenue-generating service. Although tracing individual packet requires prohibitive amounts of memory, SPIE attempt to reduce the memory requirement through the uses of Bloom filters [17]. There are also several researches [18, 19] that contributed to improve the scalability and efficiency of SPIE.

2.2 Deployment Scenario

Because of the increase in the number of large scale DoS attacks, deployment of IP-TBSs into a single AS is ineffective for blocking these attacks. Ideally, IP-TBSs should be deployed into many ASes, but this process is time-consuming.

Gong et al. introduced the AS-level partial deployment scenario in [5]. They also simulated the traceback success rate and the average number of queries issued by SPIE traceback manager(STM). According to their simulation result, the attackers could not be detected unless at least 40% of ASes deployed IP traceback. They also found that around 70% deployment made 50% chance of detecting an attacker. Within their simulation, they used 3 types of network topologies. The first one was a network topology modified from ANSNET [20], the second one is a network topology generated by INET [21], the third one is 30×30 mesh topology. For each topology, they randomly chosen 10%, 20% ... 100% ASes in the topology to set them to support SPIE, respectively. Notice that Gong et al. assumed all SPIE-deployed ASes exchange SPIE deployment information with each other; SPIE-deployed ASes advertise their support for SPIE in a BGP attribute in the network route advertisement. Hence, each AS is able to know which ASes deploy SPIE, how many hops (in AS-level) they are far away, and their respective STMs.

The results obtained by Castelucio et al. [6], the deployment scenario should be along with intent. They introduced strategic placement, where highly connected ASes have a traceback system deployed first. They used 2 types of topologies generated by Nem [22] with Barabasi-Albert Model [23] and NS-2 [24] patched by BGP++ [25] simulation module. Their results showed that 75% of deployed ASes were necessary for discovering 100% of AS-level reverse paths in the case of strategic placement. On the other hand, to achieve the same results using random placement, a traceback systems should be deployed in almost 100% of the ASes.

Hazeyama et al. also evaluated traceability when InterTrack deploys in AS-level [9]. Aside from Gongs' simulation, they assumed that the traceback query was transferred along with BGP topology; no ITM deployed information were exchanged and each ITM did not know which ASes deploy ITM. Within their simulation, they prepared 1 network topology which were designed to emulate Internet topology in Japan. On designing deployment scenarios, they defined "AS rank points" which can be calculated from CAIDA datasets [26], and introduced 4 types of scenarios based on AS rank points as follows. The first one was the deployment in the decreasing order of AS rank points, the second one was the deployment in the increasing order of AS rank points. The third was also the deployment in the increasing order of AS rank points, except for leaf ASes, which were customers of the other ASes and had no peer or provider links. The

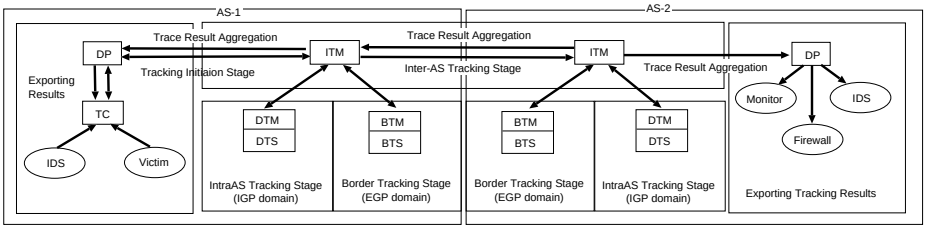


Fig. 1. Procedures of an attack tracking on InterTrack

fourth scenario was deployment in the decreasing order of AS rank points among academic network and/or campus networks in Japan. Finally, they estimated the traceability for deployment in each of the above scenarios. According to Hazeyama's simulation results, traceability will be over 70% if top 5 ASes in Japan deploy IP traceback in their networks. In addition, we will explain the emulated Internet topology in Section 3.2.

However, some issued were left unaddressed in the previous studies. In Gongs' scenario, there were 3 types of network topologies but only 1 type of deployment scenario. Castelucio only used artifactual topologies. Conversely, Hazeyama et al. introduced 4 types of deployment scenario but only 1 type of network topology. The network topology and deployment scenario are closely related traceability. In this paper, we prepare 3 types of network topologies and 4 types of deployment scenarios, and show the simulation results in 12 ($= 3 \times 4$) of the cases.

2.3 InterTrack

In order to facilitate meaningful discussions on the traceback process, we summarize the features of our traceback architecture, InterTrack [27]. InterTrack is designed for AS-level deployment and is mainly used to reconstruct the reverse AS path (the true attack path at the AS hop level) and to detect the source ASes of an attack, if possible. Further, InterTrack can be used to establish interconnections among IP TBSs, detection systems, and prevention systems within an AS.

The architecture of InterTrack resembles the Internet routing architecture, because the latter is designed along with the boundaries among operation domains having different operational policies. In a traceback trial, network operators cannot investigate other network domains; the same restriction is also observed in the BGP/OSPF routing operation. Therefore, the network operators attempt to detect upstream neighbor AS for further tracking.

In the InterTrack architecture, each AS has a set of InterTrack components. This set includes Inter-domain Tracking Manager (ITM), Border Tracking Manager (BTM), Domain Traceback Manager (DTM), Decision Point (DP), and Traceback Client (TC). Fig. 1 shows the overview of InterTrack architecture. A phased-tracking approach is applied on inter-domain traceback trials through InterTrack. InterTrack separates a traceback trial in four stages along with network

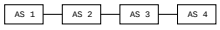


Fig. 2. Topology (A)

Fig. 3. Topology (B)

boundaries; *the tracking initiation stage*, *the border tracking stage*, *the intra-AS tracking stage* and *the inter-AS tracking stage*. After accepting a traceback request on the tracking initiation stage, each AS preliminarily investigates its own status against the mounted attack on the border tracking stage. On the border tracking stage, an AS judges by InterTrack whether or not the AS is suffered from an attack, whether or not the AS is forwarding malicious attack packets, or whether or not the AS is suspected of having attacker nodes on the inside. Triggered by the investigated AS status, InterTrack runs the inter-AS tracking stage and the intra-AS tracking stage in parallel. Detailed behavior of each component were described in [28].

3 Simulation of Traceback Deployment

Deployment of the IP-TBS should be considered along with the type of network topology. Let us assume that network has a star topology and that the IP-TBS is deployed in the central node. In this case, all ASes and AS links can be traced. The Internet topology is more complicated than other artefactual topology models.

In this section, we evaluate the traceability by deployment simulation. First, we explain the two classes of traceability used in our simulation. We then introduce 3 types of outfitted Internet topologies, i.e., emulated inter-AS topologies in China, Japan, and South Korea. We also introduce 4 types of deployment scenarios and show the simulation results.

3.1 Metrics

In this paper, we employ traceability as a performance metric. There are two principal classes of traceability: *packet traceability* and *path traceability*. Traceability in the first class is that the system can specify the AS number where the issued IP packet is generated. The second class, path traceability, is that the system can designate the datalink of the AS border.

To calculate the traceability, we refer to the deployment case of previous study [9]. In [9], the traceability had been defined in Equation 1, where N_S denotes the number of strict ASes, N_L denotes the number of loose ASes, and N denotes the amount number of ASes in the network topology. A strict AS is an AS where an IP-TBS is deployed.

$$T_{packet} = (N_S + N_L)/N \tag{1}$$

Algorithm 1 Region Based Filtering

```
1: procedure Region Based Filtering
2: load AS_RELATIONSHIP_DATABASE into ASN_LIST
3: load REGIONAL_AS_RELATIONSHIP_DATABASE into REGION_LIST
4: input IS_REGIONONLY_ENABLE
5: for all pairs(asn, neighbor_asn, direction) from ASN_LIST do
6:    if IS_REGIONONLY_ENABLE == TRUE then
7:       if REGION_LIST(asn) == EXIST AND REGOIN_LIST(neighbor_asn) == EXIST then
8:          output asn, neighbor_asn, direction
9:       end if
10:   else
11:      if REGION_LIST(asn) == EXIST OR REGION_LIST(neighbor_asn) == EXIST then
12:         output asn, neighbor_asn, direction
13:      end if
14:   end if
15: end for
```

A loose AS is an AS where the IP-TBS is not deployed, however, the neighboring AS of a loose AS is a strict AS. Because of border tracking in InterTrack, as explained in Section 2.3, Hazeyama et al. recognized that a loose AS can be traced within the InterTrack architecture.

Further, the path traceability in Equation 2, where L_S denotes the number of strict AS links, L_L denotes the number of loose AS links, and L denotes the amount number of AS links in the network topology.

$$T_{path} = (L_S + L_L)/L \tag{2}$$

In a strict AS link, both peered ASes deploy the IP-TBS. In a loose AS link, on the other hand, an AS that deploy an IP-TBS is interconnected to another AS that does not deploy an IP-TBS.

For better clarify, we use with several network topologies as shown in Fig. 2 for our explanation. Imagine if AS 1 deployed IP-TBS. The number of strict ASes is 1 (AS1) and that of loose ASes is also 1 (AS2). Due to the amount number of ASes in Fig. 2 is 4, hence $T_{packet} = 50\%$. The number of strict ASes link is 0 and the number of loose ASes is 1 (AS1-AS2), the amount number of AS links is 3, thus $T_{path} = 33\%$. There are also 4 AS in the network as shown in Fig. 3, but traceability is different in the case of Fig. 2; $T_{packet} = 75\%$ and $T_{path} = 40\%$ in the case of deployment IP-TBS in AS 1.

3.2 Network Topology

We employ the emulated network topologies for several regions. Basically, every traceback method can be used to construct attack paths. Hence, with the use of such traceback methods, communication privacy may be affected. Because of the large number of legal interpretations of privacy, deployment across border society governed by law may not be easy. As the first step in deployment simulation, we selected the emulated topologies of China, Japan, and South Korea.

We have developed several techniques, including Internet emulation [7], to construct the emulated topologies. Basically, Internet emulation involves outfit-

Table 1. The numbers of Deployment Target and Traceback Target

	Japan	China	South Korea
Deployment Target (Number of ASes)	500	196	640
Traceback Target (Number of ASes)	768	308	755
Traceback Target (Number of AS links)	1589	529	1375

ting an Inter-AS topology to a network emulation testbed for carrying out a realistic performance test; however the Region Based Filtering(RBF) algorithm for Internet emulation is more useful for our simulation.

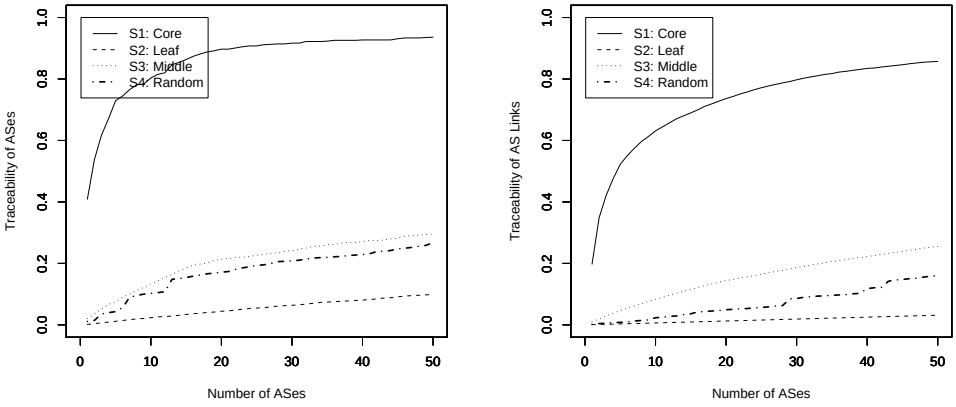
RBF algorithms can be summarized in Algorithm 1. The AS number(ASN) allocation is managed by IANA and each regional Network Information Centers (NICs), such as ARIN in continent level, and JPNIC in country level. According to ASN registration information on a NIC, RBF selects ASes from AS Relationship Dataset(ASRD), which is distributed by CAIDA project [26], only if an AS is registered its ASN in the NIC. Because of locality on each region, RBF can pick up both core ASes and leaf ASes.

In our simulation, we employ the snapshot version of ASRD published on November 22, 2008. The dataset can be summarized as shown in Table 1. Because there are loose ASes located outer region, the number of deployment target AS and traceback target AS are different. Notice that CAIDA extensively surveys AS relationships; however, some types of BGP peering styles such as private peering hinder the creation of a perfect ASRD.

3.3 Simulation Scenario

We consider 4 types of deployment scenario as follows.

- S1: Deployment in order of core ASes
  In the ideal scenario, IP-TBSs are deployed into the core ASes. Since the core ASes are interconnected to many BGP neighbors, the traceback system can handle many ASes and AS links. Hence, traceability is expected to be high even if the number of deployed traceback system is low.
  Although various criteria need to be satisfied for for identifying the network core [9, 29], we used the number of BGP peers as a metric. In this scenario, the traceback system is deployed to ASes in the decreasing order of the number of established BGP peers.
- S2: Deployment in order of leaf ASes
  In this scenario, IP-TBSs are deployed to ASes in the increasing order of the number of established BGP peers. Since the IP-TBSs will trace fewer ASes and AS links in this case, traceability will be low. However, an attacker nodes often exist in the leaf ASes. The major ISPs (core ASes) are prone to DoS attacks. Hence, it is reasonable to assume that these types of AS installed defense schemes against DoS Attacks, such as Ingress Filtering [30].



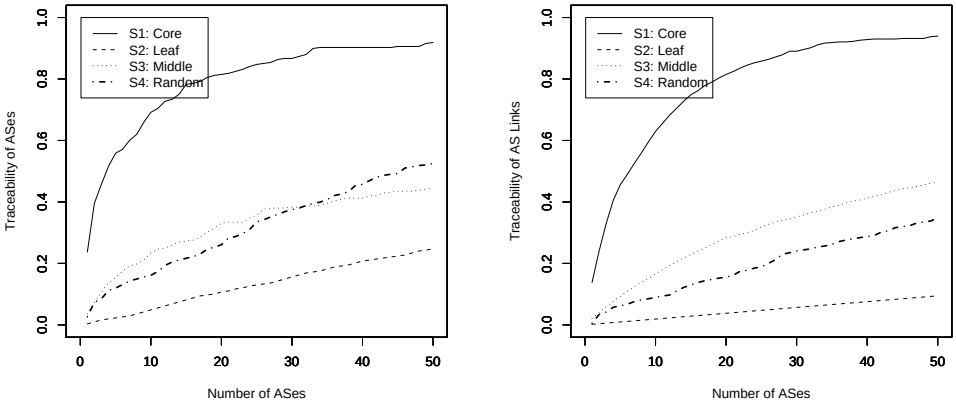
(a) Packet traceability in Japan (b) Path traceability in Japan

Fig. 4. Traceability in the case of Japan

– S3: Deployment in middle-class ASes
We assumed that the traceability observed with deployment into the core AS to be comparable to that reported by Hazeyama [9]. However, deployment in the core AS might be difficult due to the number of AS border routers. Unless hash-based IP-TBSs are used to network traffic among the AS border routers, the cost involved for deployment into core ASes would be high.
In this scenario, IP-TBSs are deployed to ASes in the decreasing order of the number of established BGP peers, except for core ASes. We assumed that the number of core AS will be estimated by the power-law, referring to the Barabasi-Albert Model [23]. For example, the number of ASes in Japan was 500 according to CAIDA ASRD published on November 22, 2008. The number of core AS is roughly 22 ($\fallingdotseq \sqrt{500}$), and hence, we measure the traceability by deploying IP-TBSs to the remaining ASes.
– S4: Deployment in a random manner
Similarly to the simulation performed by Gong et al. [5], IP-TBSs are deployed in a random manner in this scenario. To eliminate bias, we repeated trial experiments 10 times and calculated the average of the traceability values obtained for 1 AS, 2 ASes ... 50 ASes.

3.4 Simulation Result

First, we calculated the packet traceability for the Japanese network topology and summarized in Fig. 4(a), where x axis denoted the number of ASes which



(a) Packet traceability in China

(b) Path traceability in China

Fig. 5. Traceability in the case of China

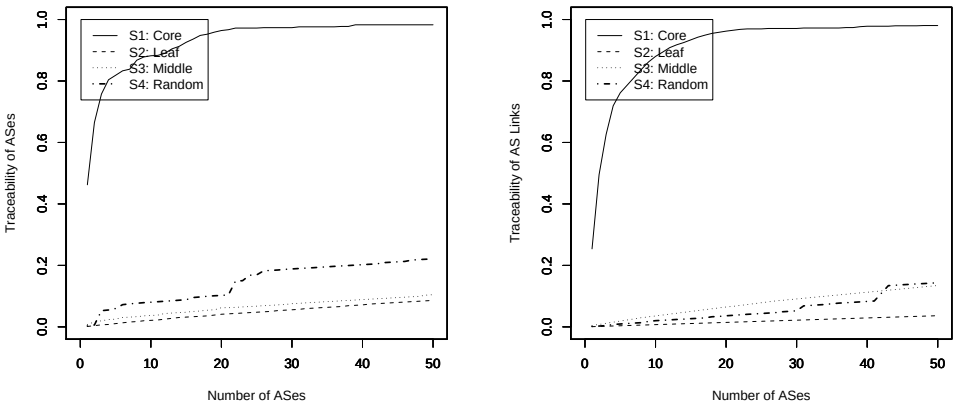
deployed IP-TBS, y axis denoted the packet traceability(T_{packet}). If IP-TBS were deployed in 15 AS, the highest T_{packet} was observed in the case of S1(86.3%), followed by S3(18.5%), S4(15.4%), and S2(3.4%). We also calculated path traceability as shown in Fig. 4(b), where x axis denoted the number of ASes which deployed IP-TBS, y axis denoted the packet traceability(T_{path}). Given the number of deployed ASes(N) = 15, the highest T_{path} was 69.0% in the case of S1, followed by S3(11.6%), S4 (3.6%), and S2(0.9%).

We then measured the traceability in the case of the Chinese network topology and the results were shown in Fig. 5(a) and Fig. 5(b). Given $N = 15$, we observed that the highest T_{packet} was in the case of S1(74.8%), followed by S3(27.3%), S4(21.7%), and S2(8.1%). The highest T_{path} was 74.9% in the case of S1, followed by S3 (22.9%), S4(13.0%), and S2(2.8%).

Finally, we simulated the case of the South Korean network topology and the results were shown in Fig .6(a) and Fig. 6(b). The results indicated that S1 could performed better than others. Given $N = 15$, the highest T_{packet} was 92.6% in the case of S1, followed by S4(8.8%), S3(4.5%), and S2(3.1%). The highest T_{path} was 93.4% in the case of S1, followed by S3(5.0%), S4(2.7%), and S2(1.1%).

In all cases, the highest T_{packet} and the highest T_{path} were observed in the case of S1. Notably, in the South Korean network topology, traceability in the case of S1 outperformed that in the other cases. We assumed that many ASes in the South Korea network topology were interconnected to a few core ASes.

However, the efficiency of deployment in the core AS was not significantly high in the Chinese network topology. The pair of traceability (T_{packet}, T_{path})



(a) Packet traceability in South Korea (b) Path traceability in South Korea

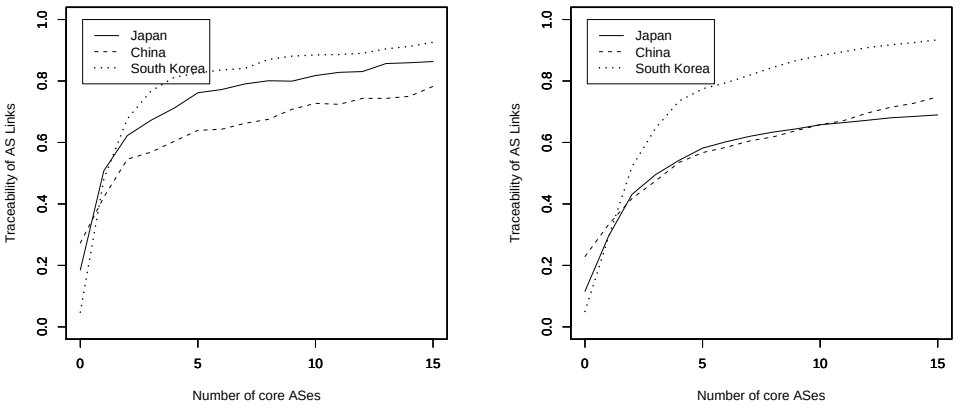
Fig. 6. Traceability in the case of South Korea

was (27.3%, 22.9%) in the case of S3, higher than that in the other network topologies. We considered there are 2 reason. The one is the number of deployment target. As shown in Table 1, the number of deployment target was 196 in China. The other one is the geographical restrictions in China; we considered that the core ASes were distributed due to the large space of China. We, therefore, assumed middle-class and/or leaf ASes have established BGP peers each other.

We found that the South Korean network topology was of the "concentrated" type while the Chinese network topology was of the "distributed" type. The characteristics of the Japanese network topology were found to be intermediate between South Korean and Chinese network topologies. However the path traceability in the Japanese network topology was not very high. As shown in Table. 1, the number of AS links in the Japanese network topology(1589) was higher than that in the South Korean network topology(1378); however, the number of deployment target in the Japanese network topology(500) was lower than in the South Korean network topology(640). We assumed that middle-class and/or leaf ASes have established BGP peers with both core ASes and other ASes.

4 Discussion

Currently, our research group is conducting field tests on IP-TBSs with 15 commercial ISPs in Japan. Deployment into core ASes, though the ideal scenario, would be difficult to create, as mentioned in Section 3.3. For practical purpose,



(a) Packet traceability within practical deployment

(b) Path traceability within practical deployment

Fig. 7. Traceability in the case of practical deployment

several core ASes and the remaining middle-class ASes are selected as deployment targets.

In order to verify whether the aforementioned practical scenario will be useful in the case of China and/or South Korea, we selected the deployment targets in the following manner. First, we selected n core ASes with S1. Then, we chose $(15 - n)$ middle-class ASes with S3. Finally, we calculated the traceability by using given set of ASes. We repeated the trial experiments by incrementing n and summarized the results in Figure 7(a) and 7(b), in respectively.

If the packet traceability is increased beyond 75%, the number of core ASes should be 3 in the South Korean network topology, 5 in the Japanese network topology, and 14 in the Chinese network topology. To achieve path traceability was higher than 75%, there might be 5 core ASes in the South Korean network topology; in the both cases of the Japanese and Chinese network topology, the path traceability could not higher than 75% when the number of deployment target was 15 ASes. Given path traceability $\geqq$ 60%, the number of core ASes should be 3 in the South Korean network topology, 6 in the Japanese network topology, and 13 in the Chinese network topology.

Moreover, our results indicated that the deployment scenario should be considered along with each region. The consideration is important for obtaining desired the traceability, but investigation of this aspect is beyond the scope of this paper.

5 Conclusion

In this paper, we simulated the traceability by using our strategy for deployment of IP traceback system(IP-TBS) into AS. We considered InterTrack and its algorithm for our study, and used two types of traceabilities - packet traceability and path traceability - as performance metrics in our simulation.

Generally, traceability was affected by the types of network topology and the deployment scenario. We constructed 3 types of network topologies. For practical simulations, we used emulated Chinese, Japanese and South Korean network topologies. We also introduced 4 types of deployment scenario, namely, deployment in core ASes, deployment in leaf ASes, deployment in middle-class ASes, and deployment in a random manner.

Our simulation results showed that the traceability obtained for deployment into core ASes outperformed that obtained for the other scenarios, regardless of the type of our network topology used. When the number of ASes that deployed IP-TBS was 15, the pair of packet traceability and path traceability was (86.3%, 69.0%) in the case of Japan, (74.8%, 74.9%) in the case of China, and (92.6%, 93.4%) in the case of South Korea. Deployment for middle-classes was the second highest in almost of all cases, however, the pair of traceability was (18.5%, 11.6%) in the case of Japan, (27.3%, 22.9%) in the case of China, and (4.5%, 5.0%) in the case of South Korea.

The results also revealed the characteristics of 3 network topologies. In the Chinese network topology, middle-class ASes and/or leaf ASes were interconnected. Conversely, tin the South Korean network topology, many ASes established BGP peers with a few core ASes. By comparing these two regions, Japanese network topology was intermediate between South Korea and China.

From these findings, we verified if the deployment scenario used in our field test in the fiscal year 2009 could be used in other regions. Deployment into core AS, though an ideal scenario, would be difficult to create. In the practical scenario, several core ASes and the remaining middle-class ASes were selected as deployment targets. If the packet traceability is increased beyond 75%, the number of core ASes should be 3 in the South Korean network topology, 5 in the Japanese network topology, and 14 in the Chinese network topology. It also required 3 ASes in the South Korean network topology, 6 ASes in the Japanese network topology, 13 ASes in the Chinese network topology for achieving 60% of path traceability. The results indicated that deployment scenario should be considered along with each region.

In our future study, we plan to estimate the traceability when IP-TBSs deployed in China, Japan, and South Korea are interconnected. Although there are several legal interpretations of privacy in communication, the IP-TBSs should be capable of exchanging traceback queries; this is because DoS attacks often originate regardless of the regions. We will also perform simulation studies using emulated network topologies derived from other network regions.

References

1. McPherson, D., Labovitz, C., Hollyman, M., Nazario, J., Malan, G.R.: World-Wide Infrastructure Security Report Volume IV. Technical report, Arbor Networks (2008)
2. Bellovin, S., Leech, M., Taylor, T.: ICMP Traceback Message (2003) IETF, Internet Draft, draft-ietf-itrace-04.txt.
3. Savage, S., Wetherall, D., Karlin, A.R., Anderson, T.E.: Practical network support for IP traceback. In: Proceedings of the ACM SIGCOMM 2000 Conference on Applications, Technologies, Architectures, and Protocols for computer communications. (2000) 295–306
4. Snoeren, A.C., Partridge, C., Sanches, L.A., Jones, C.E., Tchakountio, F., Kent, S.T., Stayer, W.T.: Hash-based IP traceback. In: Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for computer communications. (2001) 3–14
5. Gong, C., Le, T., Korkmaz, T., Sarac, K.: Single Packet IP Traceback in AS-level Partial Deployment Scenario. In: Proceedings of IEEE Global Telecommunications Conference. (2005)
6. Castelucio, A.O., Salles, R.M., Ziviani, A.: Evaluating the partial deployment of an AS-level IP traceback system. In: Proceedings of the 2008 ACM symposium on Applied computing. (2008) 2069–2073
7. Hazeyama, H., Suzuki, M., Miwa, S., Miyamoto, D., Kadobayashi, Y.: Outfitting an Inter-AS Topology to A Network Emulation TestBed for Realistic Performance Tests of DDoS Countermeasures. In: Proceedings of Workshop on Cyber Security and Test. (2008)
8. CAIDA: cooperative association for internet data analysis: The CAIDA Web Site. (Available at: http://www.caida.org/)
9. Hazeyama, H., Wakasa, K., Kadobayashi, Y.: A consideration on deployment scenarios on a filed test of IP traceback in Japan. In: Proceeding of IEICE technical report. Internet Architecture. (2008) 25–30 (in Japanese).
10. Yaar, A., Perrig, A., Song, D.X.: FIT: fast Internet traceback. In: Proceedings of the 24th Annual IEEE Conference on Compuer Communications. (2005) 1395–1406
11. Doeppner, T.W., Klein, P.N., Koyfman, A.: Using router stamping to identify the source of IP packets. In: Proceedings of ACM Conference on Computer and Communication Security. (2000) 184–189
12. Song, D.X., Perrig, A.: Advanced and Authenticated Marking Schemes for IP Traceback. In: Proceedings of the 20th Annual IEEE Conference on Compuer Communications. (2001) 878–886
13. Dean, D., Franklin, M.K., Stubblefield, A.: An algebraic approach to IP traceback. ACM Transactions on Information and System Security **5** (2002) 119–137
14. Goodrich, M.T.: Probabilistic packet marking for large-scale IP traceback. IEEE/ACM Transactions on Networking **16** (2008) 15–24
15. Shannon, C., Moore, D., Claffy, K.C.: Beyond Folklore: Observations on fragmented Traffic. IEEE/ACM Transactions on Networking **10** (2002) 709–720
16. Gong, C., Saraç, K.: A More Practical Approach for Single-Packet IP Traceback Using packet Logigng and Marking. IEEE Transactions on Parallel and Distributed Systems **19** (2008) 1310–1324
17. Bloom, B.H.: Space/time trade-offs in hash coding with allowable errors. Communications of the ACM **13**(7) (1970) 422–426

18. Lee, T.H., Wu, Z.K., Huang, T.Y.W.: Scalable Packet Digesting Schemes for IP Traceback. In: Proceedings of the 2004 IEEE International Conference on Communications. Volume 2. (2004) 1008–1013
19. Li, J., Sung, M., Xu, J.J., Li, L.E.: Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Theoretical Foundation. In: Proceedings of the 25th IEEE Symposium on Security and Privacy. (2004) 115–129
20. Comer, D.E., Stevens, D.L.: Internetworking With TCP/IP Vol. I. third edn. Prentice Hall, Englewood Cliffs, NJ (1991)
21. Winick, J., Jin, C., Chen, Q., Jamin, S.: Inet Topology Generator. (Available at: http://topology.eecs.umich.edu/inet/)
22. Magoni, D.: network manipulator(nem). (Available at: http://www.labri.fr/perso/magoni/nem/)
23. Barabási, A.L., Albert, R.: Emergence of Scaling in Random Networks. Science **286** (1999) 509–512
24. ns 2: The Network Simulator. (Available at: http://www.isi.edu/nsnam/ns/)
25. Dimitropoulos, X., Riley, G.: BGP++. (Available at: http://www.ece.gatech.edu/research/labs/MANIACS/BGP++/)
26. CAIDA: cooperative association for internet data analysis: The CAIDA AS Relationships Dataset. (Available at: http://www.caida.org/data/active/as-relationships/)
27. Hazeyama, H., Kadobayashi, Y., Miyamoto, D., Oe, M.: An Autonomous Architecture for Inter-Domain Traceback across the Borders of Network Operation. In: Proceedings of the 11th IEEE Symposium on Computers and Communications. (2006)
28. Hazeyama, H., Kadobayashi, Y., Oe, M., Kaizeki, R.: InterTrack: A federation of IP traceback systems across borders of network operation domains. In: Proceedings of Annual Computer Security Applications Conference, Technology Blitz Session. (2005)
29. Dimitropoulos, X.A., Krioukov, D.V., Fomenkov, M., Huffaker, B., Hyun, Y., Claffy, K.C., Riley, G.F.: AS Relationships: Inference and Validation. ACM SIGCOMM Computer Communication Review (CCR) **37**(1) (2007) 29–40
30. Greene, B.R., Morrow, C., Gemberling, B.W.: Tutorial: ISP Security - Real World Techniques II. (Available at: http://www.nanog.org/meetings/nanog23/)