

2-7 The Mathematics Models and an Actual Proof Experiment for IP Traceback System

SUZUKI Ayako, OHMORI Keisuke, MATSUSHIMA Ryu, KAWABATA Mariko, OHMURO Manabu, KAI Toshifumi, and NISHIYAMA Shigeru

IP traceback is a technique that searches DDoS attackers. There are many kinds of IP traceback methods. The performance of IP traceback system can mainly evaluate using a race time and the error rate of the trace result. In this paper, we propose mathematical models of typical IP traceback methods, which are ICMP, IPPM, HASH, and an UDP and AS traceback method newly proposed. And, we estimate the time required to trace. And, we analyze reliability features of these. False positive rate are evaluation parameters of the reliability. And, we analyze mathematical models. Then we compare the predicted value with the measured values using the actual large network for verification.

Keywords

IP traceback, Inter AS(Autonomous System) traceback, An UDP method, Mathematical models, Analysis of FPR(False Positive Rate)

1 Introduction

R&D is currently underway on the use of IP traceback to track down the sources of DDoS (distributed denial of service) attacks. Major intra-AS IP traceback methods include the ICMP[1], IPPM[2], and HASH[3] methods. More recently, hybrid methods have emerged consisting of combinations of these existing methods (e.g., HASH + newly developed UDP)[4]-[6]. A method is also available to perform traceback across ASs through coordination of intra-AS traceback systems[7].

Performance of an IP traceback system can be evaluated mainly by its traceback time and the false detection rate of its traceback results. In false detection, a traceback system cannot track down the source of attacks (attackers) perfectly, for a variety of reasons. In this context a false positive rate (FPR) is used as an index of false detection. In this paper, we will refer to this as a “reliability index”. To ensure efficient operation of IP

traceback methods, it is necessary to understand traceback time and the reliability characteristics of the individual methods.

In this paper we will present mathematical models that express the traceback times of the ICMP, IPPM, HASH, UDP and inter-AS traceback methods. We will analyze the FPR characteristics of these methods in an anticipated environment of use. We will also conduct actual measurement on a large-scale verification network, and confirm the adequacy of these mathematical models through comparison with the measurement results. Section 2 will briefly describe the workings of intra-AS and inter-AS traceback and FPR. Section 3 will give definitions of mathematical models of individual methods. Section 4 will describe the verification environment used in actual measurement, comparison between predicted traceback time and actual measured values, and FPR analysis. Section 5 will summarize this research.

2 IP traceback

2.1 Functions of IP traceback

IP traceback methods are designed to track down the sources of attacks mainly within a single autonomous system (AS). In most cases, however, DDoS attack packets pass across several ASs to reach a victim. Therefore, in addition to performing traceback within each AS, it is necessary to execute traceback across ASs through coordination of the traceback systems used within these ASs[7]. In this paper, we refer to the former as “intra-AS traceback” and the latter as “inter-AS traceback”.

2.1.1 Intra-AS IP traceback

Major intra-AS IP traceback methods include the ICMP, IPPM, and HASH methods.

In the case of the ICMP and IPPM methods, routers generate traceback information on attack packets with a certain probability. Traceback paths to attackers are confirmed based on the generation of this information. One can therefore calculate the attacker-detection rate from the probability of generating traceback information on the edge of each attack route.

In the case of the HASH method, the agent at each router saves a HASH value for every packet that passes through the router. The manager figures out traceback paths by making queries as to whether attack packets have passed through each router. Therefore, traceback time depends on the number of queries by the manager.

In the case of the newly developed UDP method, the manager requests a nearby router to return information on the passage of attack packets, if any. The manager sends this request to one router after another.

2.1.2 Inter-AS traceback

Border and internal traceback methods are used to perform traceback across ASs that employ different intra-AS traceback methods. Border traceback only covers routers located on borders between ASs, while internal traceback covers all routers within each AS. An effective combination of these methods can enable high-speed traceback. Figure 1 shows an overview of border and internal traceback.

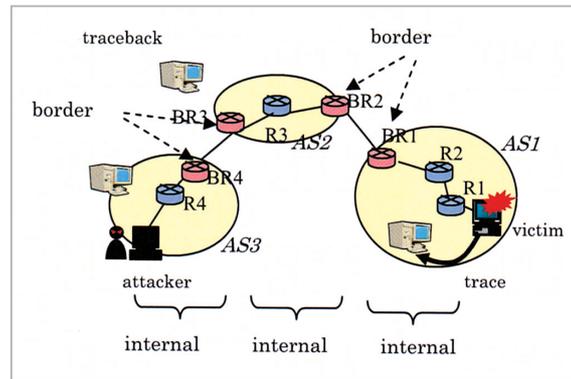


Fig. 1 Overview of border and internal traceback

2.2 Definition of reliability index, FPR

Expression (1) defines FPR. “Number of detected attackers” is the total number of nodes detected as attackers at a given time. This includes some falsely identified nodes. To use FPR in prediction, both the denominator and numerator of Expression (2) are assigned expectation values.

$$\text{FPR} = \frac{\text{Number of falsely detected attackers}}{\text{Number of detected attackers}} \quad (1)$$

$$\text{FPR} = \frac{\text{Expectation value of number of falsely detected attackers}}{\text{Expectation value of number of detected attackers}} \quad (2)$$

2.3 Factors of FPR

Table 1 shows anticipated factors of FPR during operation of the three traceback methods. There are four main factors of FPR. Other factors are related to errors in the IP traceback systems, but this paper does not address these.

Table 1 Factors of FPR

Cause	Description
Causes of false detection	a If traceback time is insufficient, a router on the attack route may be judged as the attacker.
	b If attack packets and normal packets are of the same type, normal users and attackers cannot be distinguished from each other, and therefore a normal user may be judged to be an attacker.
	c The IPPM and HASH methods use HASH values. If there is a conflict between HASH values, a terminal that did not actually make an attack may be judged to be an attacker.
	d The UDP method sets a TimeOut value for routers on the attack route. If the TimeOut value is exceeded before trace packets are generated, a router on the attack route may be judged to be an attacker.

3 Mathematical models

3.1 Intra-AS traceback systems

3.1.1 ICMP method

(1) Overview of evaluated system's processing procedure

We evaluated an iTrace system described in a different paper[1] as an ICMP method. In this system, each router monitors in-transit packets passing through each router and generates iTrace packets with a probability of 1/20,000. To prevent false detection, we set the threshold value to two; i.e., we stipulated that the collector must receive two iTrace packets from the same router before a traceback path to an edge can be confirmed.

(2) Detection rate of attackers

Calculate the probability "Pr(ei)" that a router will generate two iTrace packets for an edge "ei". When the probability of generation of iTrace packets is "p", and N (number) packets pass through that router, "Pr(ei)" can be calculated by Expression (3). In this case "(1-p)^N" is the probability of sending no iTrace packet, and "Np(1-p)^{N-1}" is the probability of sending one iTrace packet.

$$\text{Pr}(ei) = 1 - (Np(1 - p)^{N-1} + (1 - p)^N) \quad (3)$$

(3) FPR

In Table 1, "a" and "b" are possible factors of FPR within this system. In the case of a single attack route, the rate of false detection due to "a" can be calculated by subtracting the detection rate of the attacker from the detection rate of the victim's immediate router. In the case of multiple attackers, one can approximately calculate the false detection rate by subtracting the detection rate of the attackers from the detection rate of the router that is detected first.

For the number of falsely detected attackers due to "b", you can calculate an expectation value from the probability of generation of traceback information on normal packets to the edge.

3.1.2 IPPM method

(1) Overview of evaluated system's processing procedure

As an IPPM method, we evaluated an AMS-

II system described in a different paper[8]. In this system, each router samples in-transit packets with a probability of 1/20, and divides a 64-bit HASH value into eight fragments to be marked on eight packets.

To prevent false detection, we set the threshold value at 16; i.e., the collector needs to receive 16 marked packets from the same router before a traceback path to an edge can be confirmed.

(2) Detection rate of attackers

Suppose that "d" (number) routers are located linearly between the victim and an attacker. Calculate the probability "F_d" that a router marks a value on a packet and that other routers do not replace this value.

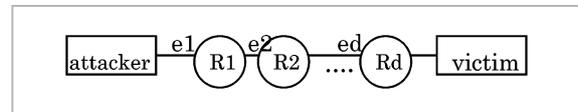


Fig.2 Route map used for calculation by mathematical models of IPPM method

In Fig.2, the probability that a router "R1" marks a value on a packet passing through an edge "e1" and other routers do not mark a value (replace the above value) is "p(1 - p)^{d-1}". This value is randomly selected from eight fragments of a HASH value. Therefore, the probability of generation of marked packets is "p/8", and the probability "F_d" can be calculated by Expression (4).

$$F_d = p(1 - p)^{d-1}/8 \quad (4)$$

Expression (5) defines the probability "Pr(ei)" that the collector receives two or more marked packets passing through an edge "ei". Expression (7) can be used to define Expression (5). Here, "N" is the number of attacker's packets, "N*F_d(1 - F_d)^{N-1}" is the probability of receiving one marked packet, and "(1 - F_d)^N" is the probability of receiving no packet. The calculation result is raised to the eighth power because the packets must contain the whole HASH value in order for the traceback path to be identified.

$$\text{Pr}(ei) = (1 - (N * F_d(1 - F_d)^{N-1} + (1 - F_d)^N))^8 \quad (5)$$

(3) FPR

In Table 1, “a” and “b” are possible factors of FPR by this system. The rate of false detection due to “a” or “b” can be calculated in the same manner as in the ICMP method.

3.1.3 HASH method

(1) Overview of evaluated system’s processing procedure

As a HASH method, we evaluated an SPIE system described in a different paper[3]. In this system, the agent at each router saves a HASH value for every packet that passes through the router. The manager performs traceback by performing queries as to whether attack packets have passed through each router. We used a system that generates 14-bit HASH values.

(2) Detection rate of attackers

Expression (6) defines attacker detection time “T”, where “n” is the total number of queries from the manager to the agent at each router. We obtained an approximate expression by regression analysis.

$$T = 0.004n + 1.2841 \quad (6)$$

(3) FPR

In Table 1, “c” is a possible factors of FPR by the system, but we did not include this item in our evaluation.

3.1.4 UDP method

(1) Overview of evaluated system’s processing procedure

As a UDP method, we evaluated a uTrace system described in a different paper[6]. In this system, the manager provides the victim terminal’s immediate router with information on intended packets (created in part from data on attacks detected by IDS). If traffic matches this information, the router will send a UDP packet to the manager. This packet includes, among other data, information on which router is to be monitored next. Based on UDP packets sent from the series of routers, the manager identifies the attack route and tracks down attackers. The information on intended packets includes protocol types, port numbers, and packet destinations.

To prevent false detection, we set the

threshold value to “2” in this test; i.e., the manager needs to receive two trace packets that include edge information on the end node before a traceback path can be confirmed.

(2) Attacker detection time

Expression (7) defines attacker detection time “T”, where “d” is the number of routers on the attack route and “A” is the attack speed [packets/sec].

$$T = \sum_i^{hop-1} \frac{1}{A_i} + \frac{2}{A_e} \quad (7)$$

(3) FPR

In Table 1, “a”, “b”, and “e” are possible factors of FPR by this system. We studied “b” using the configuration shown in Fig. 7. Before the victim’s immediate router “R1” is detected, FPR is 0. When “R1” is detected, the FPR value will change to 1 and will remain at that value until the attacker’s immediate router “R10” sends two trace packets. When the attacker is detected, FPR will become 0. Then, after detection of “R11”, FPR will continue to hover around 0.5 and will not stabilize at a smaller value. In Figure 4, merging of traffic flows occurs, and detection time is shorter at confluences (R1 to R6). Expression (7) can be used to calculate attacker detection time at confluences.

Table 2 shows mathematical models that express the traceback times of intra-AS traceback methods.

3.2 Inter-AS traceback systems

In most cases, DDoS attack packets pass across several ASs to reach a victim. Therefore, it is necessary to track down attackers through coordination among the ISPs that manage the individual ASs. Border and internal traceback methods are used to facilitate traceback across ASs. Border traceback only covers routers located on the border between ASs, while internal traceback covers all routers within each AS. High-speed traceback is enabled through the effective combination of these methods.

It is possible to select and operate traceback methods independently on each AS. A

Method	Mathematical model
ICMP	$\Pr(e_i) = 1 - (Np(1-p)^{N-1} + (1-p)^N)$ $\Pr(\prod A_j) = \prod \Pr(e_i)$ <p>Where “p” is the probability of generation of iTrace packets at each edge, and “N” is the number of attack packets.</p> <p>Change the number of packets to determine a traceback time for which the probability becomes 95%.</p>
PPM	$F_d = p(1-p)^{d-1}/8$ $\Pr(e_i) = (1 - (N * F_d(1-F_d)^{N-1} + (1-F_d)^N))^8$ $\Pr(\prod A_j) = \prod \Pr(e_i)$ <p>Where “p” is the probability of generation of iTrace packets at each edge, “N” is the number of attack packets, and “d” is the hop count from the victim.</p> <p>Change the number of packets to determine a traceback time for which the probability becomes 95%.</p>
Hash	$T = 0.004n + 1.2841$ <p>Where “n” is the total number of queries from the manager to each router agent.</p> <p>Determine an approximate expression by regression analysis.</p>
UDP	$T = \sum_i^{hop-1} \frac{1}{A_i} + \frac{2}{A_e}$ <p>Where “Ai” is the average volume of attack packets at each edge, and “hop” is the largest hop count of any of the attack paths. “Ae” is the average volume of attack packets at the attack terminal. Determine this value from the traceback time of the attack path with the largest hop count.</p> <p>This model can be applied to b d t h h’</p>

combined system performs border traceback first, and then executes internal traceback to track down the attackers (e.g., AS1 border→AS2 border→AS3 border→AS3 internal). Border traceback time increases with an increase in the number of ASs involved while internal traceback time is determined by the number of ASs in which attackers are present.

When there are multiple attackers, these are traced back in parallel. In this case, traceback time “T” depends on the time required to trace a route with the maximum hop count within the AS. If UDP method is used in inter-

nal traceback, traceback time “T” can be calculated by Expression (8).

$$\begin{aligned}
T &= \text{MAX (Time required to finish internal traceback on ASn)} \\
&= \text{MAX (Border traceback time from start to ASn + internal traceback time on ASn)} \\
&= \frac{1}{A_j} + \sum_i^{hop-1} k \times \frac{1}{A_i} + \frac{2}{A_e} \tag{8}
\end{aligned}$$

Here, “Aj” is the average volume of attack packets at each edge of the border router, “Ai” is the average volume of attack packets at

each edge, “hop” is the number of routers on the attack route with the maximum hop count within that AS, and “Ae” is the average volume of attack packets at the attacker. If merging of attack routes occurs, this value is 2; if not, this value is 1.

4 Verification testing

4.1 Configuration of verification environment

(1) Objective of verification network

We established a verification network to assess the reliability characteristics of the above-mentioned traceback methods in a close approximation of an actual environment. We used only part of this verification environment in this test, but we also conducted verification testing on hop counts and the number of attackers using the entire environment.

(2) Specifications of verification network

Tables 3 and 4 show the specifications of the network and tools used for verification. We used virtual OS technology to create a large network with a small number of machines. Since all traceback systems under test supported Linux, we selected the Linux operating system and UML (User-Mode Linux) virtualization technique [9].

Table 3 Specifications of verification network

Features		Details
AS configuration		Single AS
Size of network	No. of servers	300 units
	No. of clients	180 units
	No. of PC routers	110 units
Topology		Tree, partial mesh (average number of branches: 2.3; average depth: 5; full mesh)
Largest hop count		10 (No change in NW configuration, ASs are serially connected)
Routing protocol		OSPFv3
Types of servers		NTP server, WWW server
OS		Linux Redhat7.3
Virtual network	Technology	User Mode Linux
	Terminals	Client/server terminals, some of the PC routers

Table 4 Verification tools

Verification tools	Configuration	Traffic type	Specifications
Attack-traffic generation tool	Manager Attack traffic pseudo-terminal	Synflood	<ul style="list-style-type: none"> Variable attack speed and time Spoofed source IP address Up to 25,000pps Up to 10pps (virtual)
Pseudo-traffic generation tool	Manager Normal traffic pseudo-terminal	HTTP request	<ul style="list-style-type: none"> Variable request speed Up to 25 requests/s

4.2 Verification results

4.2.1 Traceback time

(1) Intra-AS traceback

A) Verification procedure

Measure traceback time using different numbers of attackers.

B) Verification conditions

Vary the number of attackers: 1, 10, 20, 50, and 100. The speed of attacks is constant at the victim’s location. Table 5 shows measurement conditions, and Fig.3 shows a configuration of the verification network.

C) Results

Figure 4 shows the measurement results. As can be seen from the figure, the actual

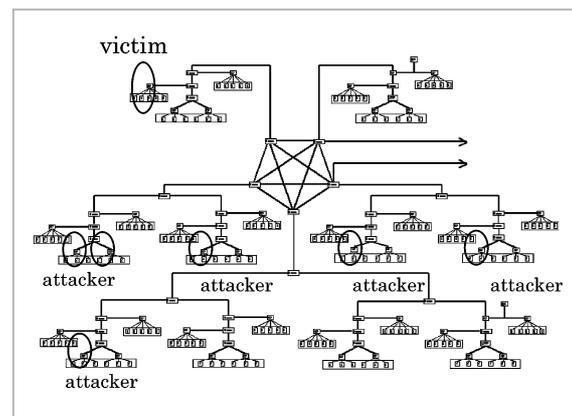


Fig.3 Configuration of verification network for intra-AS traceback

Table 5 Verification conditions for intra-AS traceback

Method	No. of attackers	No. of attackers × Vol. of attack	No. of attempts
ICMP	1,10,20,50,100	25000pps	10
PPM	Same as above	1000pps	60
Hash	1,10,20,50,100	50pps	5
UDP	10,20,50,100	100pps	60

measured values are almost the same as the predicted values, and the newly developed UDP method is faster than the other methods. When performing traceback against 100 terminals, the ICMP method exceeded the measurement time limit (10 minutes); the measured value is thus not shown in the figure.

(2) Inter-AS traceback

A) Verification procedure

Measure traceback time using different numbers of ASs, attackers, and different topologies.

B) Verification conditions

The speed of attacks per attacker is constant at 10 pps. Figure 5 shows the measurement conditions and network configuration.

C) Results

Figure 6 shows the verification results. As can be seen from the figure, the actual measured values are almost the same as the predicted values, and traceback time is determined by the maximum hop count between the victim and attackers; it is not dependent on the topology or the number of attacks.

4.2.2 False detection rate

A) Verification objective

Suspects detected by IP traceback are not always attackers. This is because attack pack-

ets and normal packets may be of the same type; if this is the case it becomes impossible to distinguish between them after a certain period of time.

We studied the possibility of identifying attackers according to volumes of attack and normal packets.

B) Verification conditions

To check FPR, change the proportion of attack packets and normal packets: from 50/50 to 10/90. Compare the IPPM and UDP methods. Measure FPR using the configuration shown in Fig.7. Table 6 shows the measurement conditions.

C) Results

Figure 8 shows the measurement results. As can be seen from the figure, while UDP can identify suspects quickly, it is difficult for UDP to distinguish between attackers and normal users based on the flow or ratio of attack packets. On the other hand, while IPPM is slower than UDP, it can effectively improve FPR based on the flow or ratio of attack packets.

In order for UDP to reduce FPR and improve accuracy in the detection of attackers, it is necessary to set a threshold value greater than 2. It seems possible for IPPM to reduce FPR by gauging the attack time in the event of

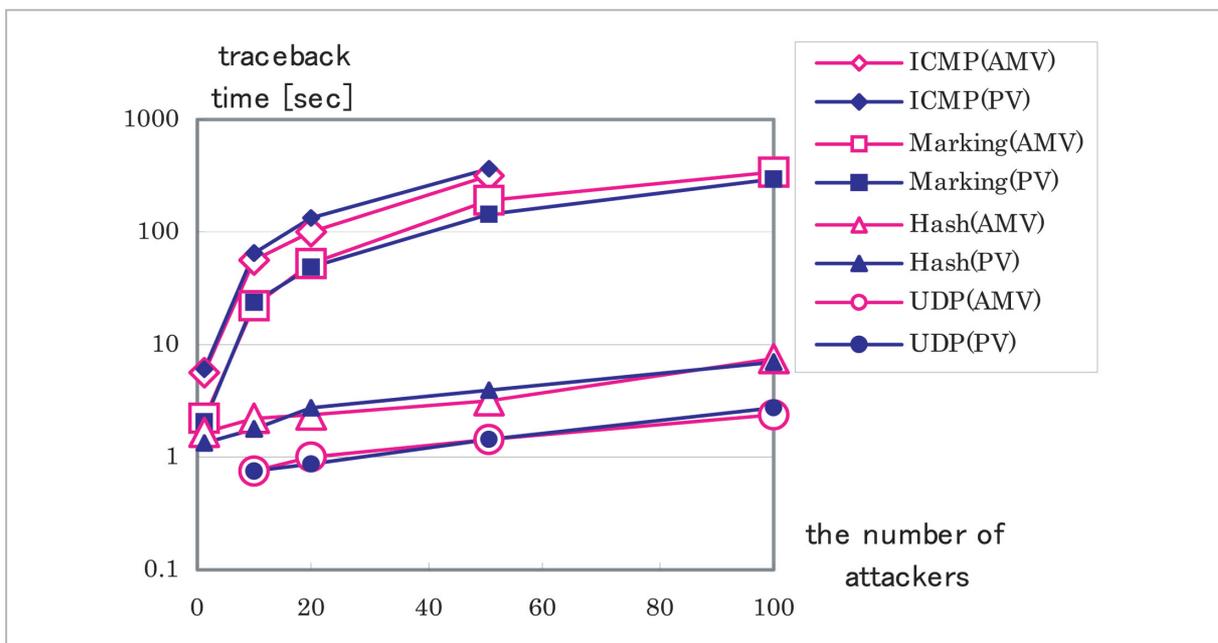


Fig.4 Traceback time of intra-AS traceback methods

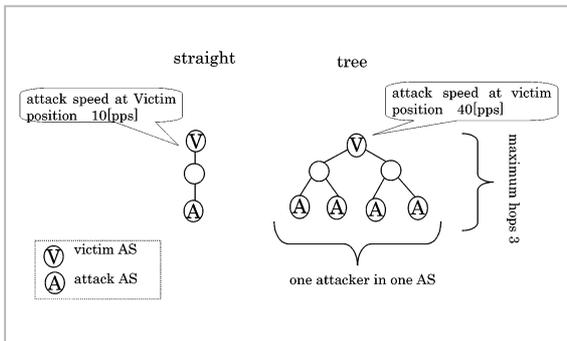


Fig.5 Verification conditions and configuration of verification network for inter-AS traceback

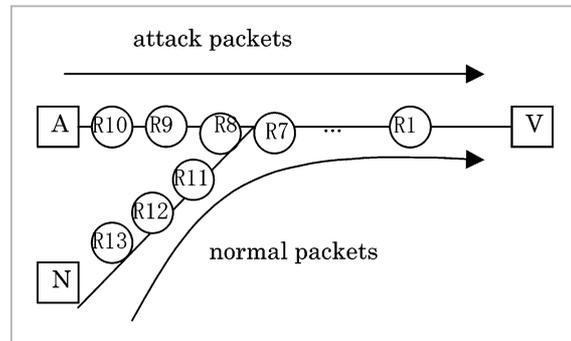


Fig.7 Configuration of verification network for mixed (attack and normal) traffic

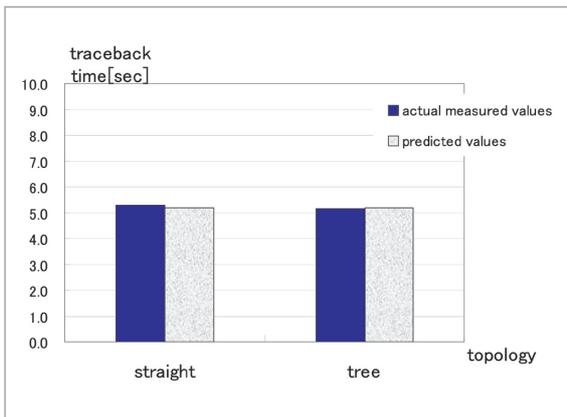


Fig.6 Traceback time of inter-AS traceback

Table 6 Verification conditions for mixed (attack and normal) traffic

		IPPM	UDP
Probability of generation of traceback information		1/20	—
Ratio of normal packets 50%	Vol. of attack packets	25pps	25pps
	Vol. of normal packets	25(3)pps	25(3)pps
Ratio of normal packets 90%	Vol. of attack packets	5pps	5pps
	Vol. of normal packets	45(9)pps	45(9)pps

The number of SYN packets included in normal packets is parenthesized.

fairly high-speed DDoS attacks.

D) Proposals related to operation

Based on the FPR verification results of traceback systems we suggest the following three approaches:

- Measure Synflood attacks in real time in order to distinguish between normal data and attack flows.
- When an attack is detected by the above procedure, use a traceback system to generate a suspect list.
- Generate a suspect list periodically (e.g., every second at the time of attacks) and judge frequently listed nodes as highly suspicious.

5 Conclusions

In this study, we put forward mathematical models that express traceback time of intra-AS traceback methods such as ICMP, IPPM,

HASH, and UDP, as well as inter-AS traceback. Based on these models, we then predicted traceback time in the event of multiple attackers. We also conducted actual measurement of traceback time and compared the measurement results with our predictions. By testing intra-AS traceback, we verified that the actual measured values are almost the same as the predicted values, and that the newly developed UDP method is faster than the other methods. By testing inter-AS traceback, we verified that the actual measured values are almost the same as the predicted values, and that traceback time is determined by the maximum hop count between the victim and attackers and is not dependent on topology or number of attacks.

Moreover, we analyzed “FPR” reliability characteristics in a mixed (attack and normal) traffic environment, comparing the UDP and IPPM methods. The results indicate that it is

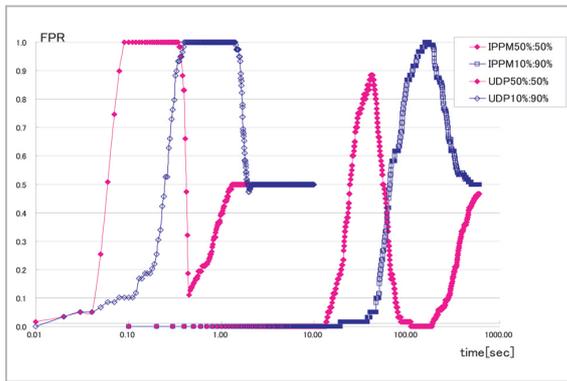


Fig.8 Change in FPR

necessary to set a threshold value greater than 2 in order for the UDP method to reduce FPR and improve accuracy in the detection of attackers, and that it seems possible for IPPM to reduce FPR by gauging the attack time in

the event of fairly high-speed DDoS attacks.

We verified that it is possible to predict traceback time of traceback methods using the mathematical models we put forward in this paper, and we used reliability indexes, FPRs, to analyze the reliability characteristics of these methods.

Acknowledgements

This research was carried out based on the “Research and Development on Security of Large-Scale Networks” project commissioned by the National Institute of Information and Communications Technology. We would like to express our gratitude to NICT for its guidance and support.

References

- 1 StevenM. Bellovin, “ICMPTracebackMessage”, InternetDraft: draft-vellovin-itrace-00.txt, submitted Mar. 2000.
- 2 S. Savage et al., “Practical Network Support for IP Traceback”, Proc. of the ACM SIGCOMM conference, Aug. 2000, Stockholm, Sweden.
- 3 Alex C. Snoeren et al., “Hash-Based IP Traceback”, Proc. of the ACM SIGCOMM 2001 Conf., Sandiego, CA, Oct. 2001.
- 4 Naohiro Fukuda et al., “Research and Development for Traceback System in Large-Scale Networks”, IEICE2004 General Conference, Mar. 2004.
- 5 Toshifumi Kai et al., “Efficient Traceback Method for Detecting DDoS”, Internet conference2004 collected papers, pp111-118, Oct. 2004.
- 6 Toshifumi Kai et al., “Inter AS Traceback Method for Detecting DDoS Attacks”, IPSJ CSEC Group, 2004.
- 7 Toshifumi Kai et al., “Efficient Traceback Method for Detecting DDoS Attacks”, IPSJ CSEC Group, 2004.
- 8 D.Song et al., “Advanced and Authenticated Marking Schemes for IP Trace back” Proc. IEEE INFOCOM, Apr. 2001.
- 9 <http://user-node-linux.sourceforge.net>

SUZUKI Ayako

*Core Network Business Headquarters,
NTT Advanced Technology Corp.
Networks Security*

OHMORI Keisuke

*Core Network Business Headquarters,
NTT Advanced Technology Corp.
Networks Security*

MATSUSHIMA Ryu

*Core Network Business Headquarters,
NTT Advanced Technology Corp.
Networks Security*

KAWABATA Mariko

*Core Network Business Headquarters,
NTT Advanced Technology Corp.
Networks Security*

OHMURO Manabu

*Core Network Business Headquarters,
NTT Advanced Technology Corp.
Networks Security*

KAI Toshifumi

*Advanced Technologies Development
Laboratory, Matsusita Electric Works,
Ltd.
Networks Security*

NISHIYAMA Shigeru

*Senior Engineer, Core Network Business
Headquarters, NTT Advanced
Technology Corp.
Networks Security*