Probabilistic Packet Marking as a Defense for DDoS Attacks

Akira Kanaoka
University of Tsukuba
kanaoka@cs.tsukuba.ac.jp

筑波大学
University of Tsukuba

Denial of Service (DoS)

Type of DoS

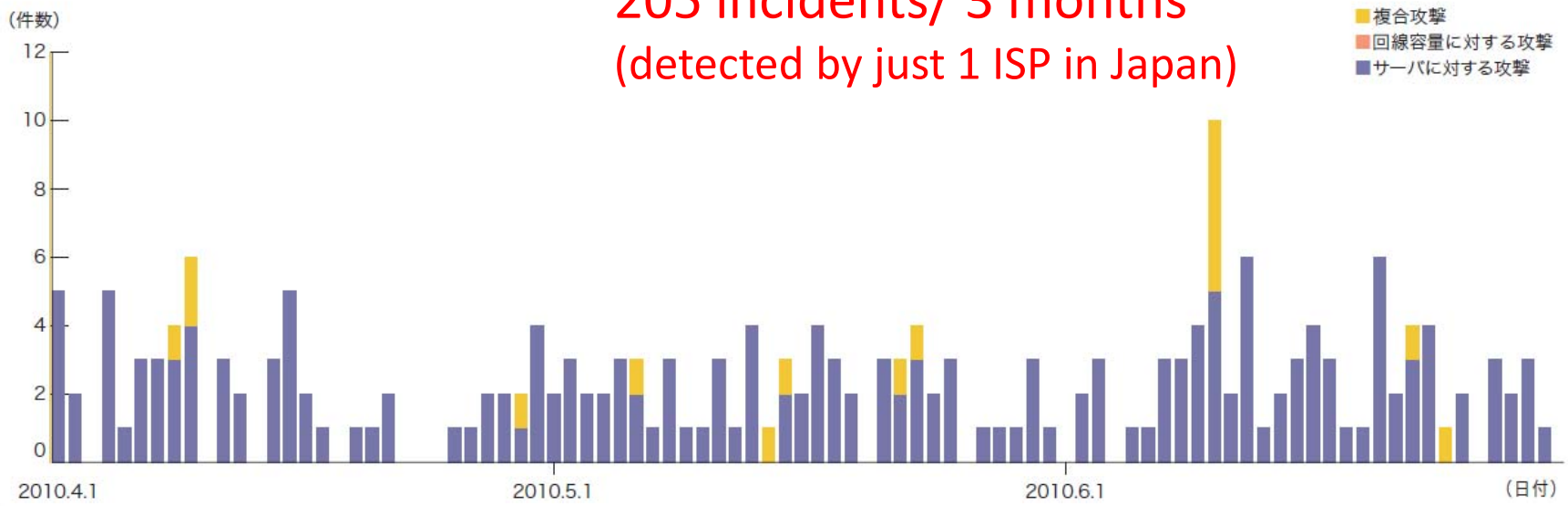
- "Ping of Death" type
- Flooding type

I call simply Flooding type DoS as "DoS"

DDoS incidents in Japan

"Internet Infrastructure Review vol.008", Internet Initiative Japan (IIJ)

205 incidents/ 3 months
(detected by just 1 ISP in Japan)



Taxonomy of DoS Attack Defense

Attack Prevention

- Stop attacks before they actually cause damage
- Ingress/Egress Filtering

Attack Detection

- Detect attacks when DoS attacks actually execute
- Pattern Matching, Anomaly Detection

Attack Source Identification

- Identify sources of attacks.
- IP traceback

Traceback

Logging	Record logs of packet at routers
ICMP	Submit ICMP packet including information for attack path re-building
Packet Marking	Add attack path information to each packet header

Attack Reaction

- Eliminate or mitigate of attack damage
- Congestion control

T. Peng, et. al., "Surven of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", ACM Computing Surveys, April 2007

Type of Traceback: Pros and Cons

Logging

- Storage device records packets information at each routers on attack paths
- Victim can obtain attack path info by matching information on each storage devices
- Drawback: Requiring recording equipment (large storage)

ICMP

- Routers submit ICMP packets including information for re-building attack paths
- Drawback: Additional traffic during DoS/DDoS attacks

Probabilistic Packet Marking (PPM)

- Routers mark own information to packets probabilistically
- Drawback: Requireing lots of packets to re-build attack paths

Challenge

Re-building attack paths in smaller amount of packets

Probabilistic Packet Marking (PPM) Method <Savage's method>

Basic Strategy

Purpose:
"Identify paths (IP addresses and order of relaying routers) to attackers"

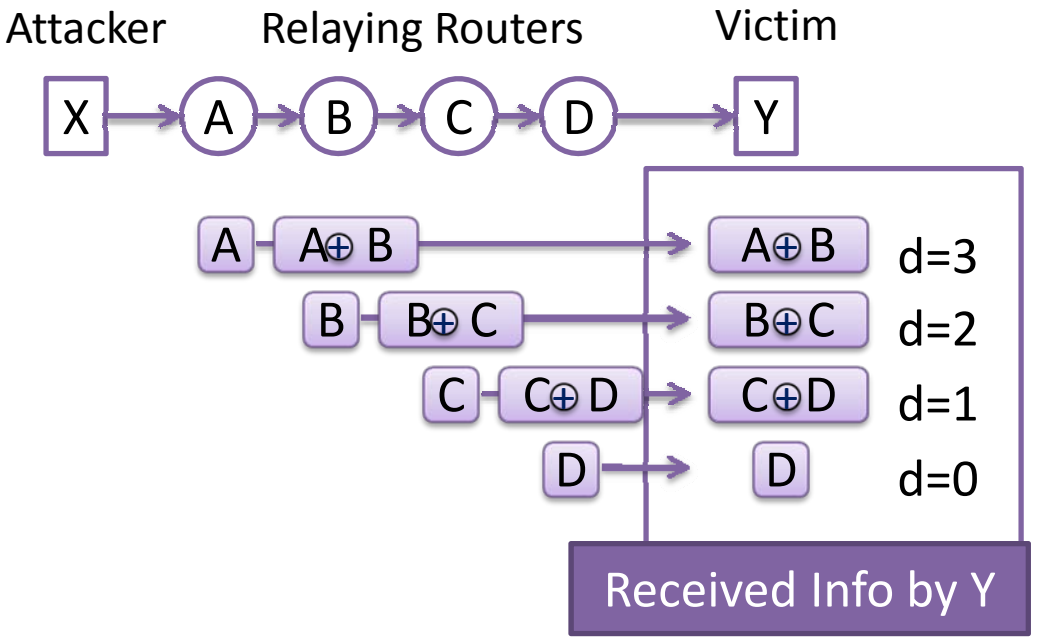
on probability p

- Write own IP info
- Set distance info to 0

on probability 1-p

- if distance info is 0
  XOR own IP info and current IP info
- increment distance info

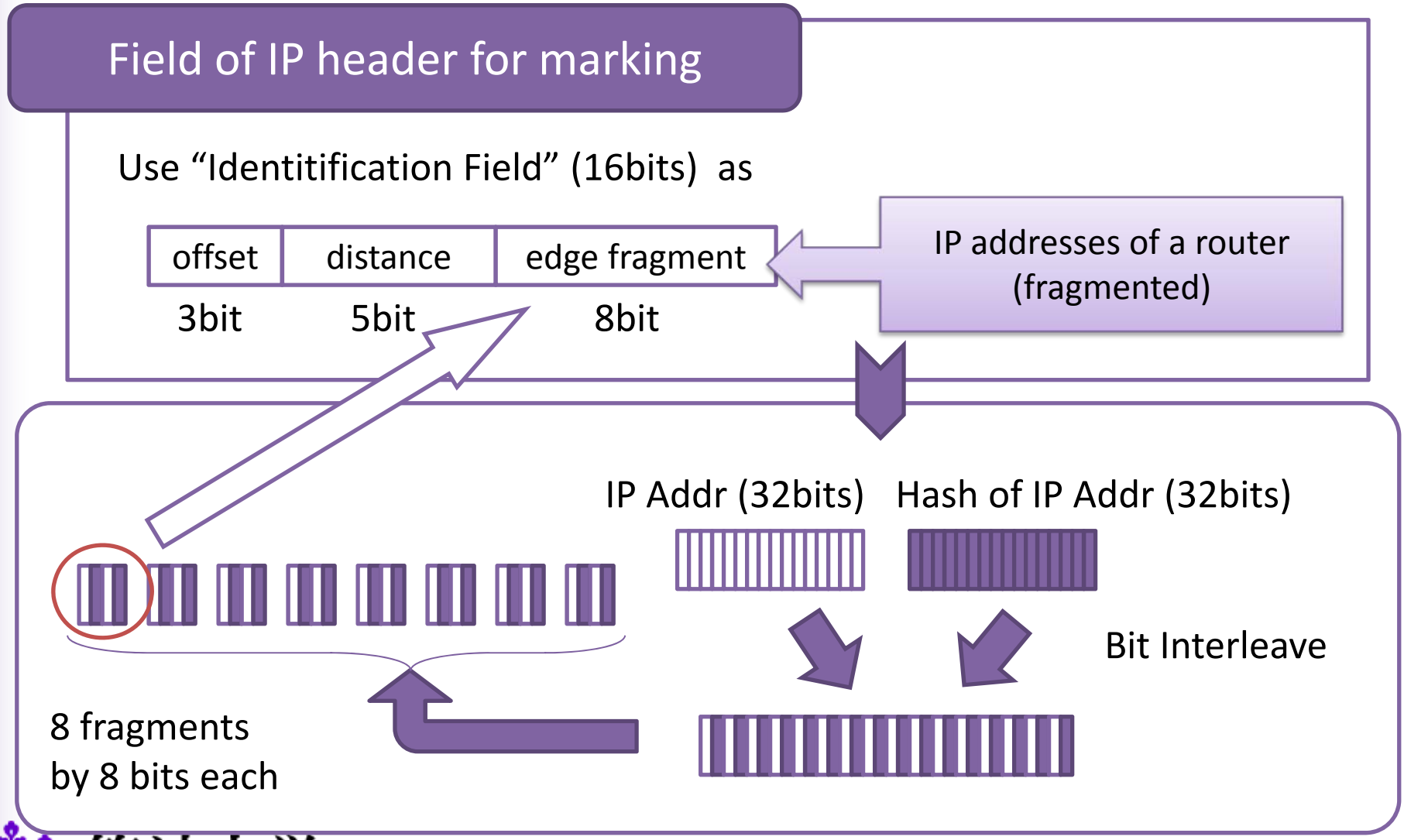
Example



Y can re-build IP addr info by XOR , step by step

Problem:
" Which part of packet should be used to mark IP addr info"

Probabilistic Packet Marking（PPM）Method <Savage's method>



Probabilistic Packet Marking (PPM) Method <Savage's method>

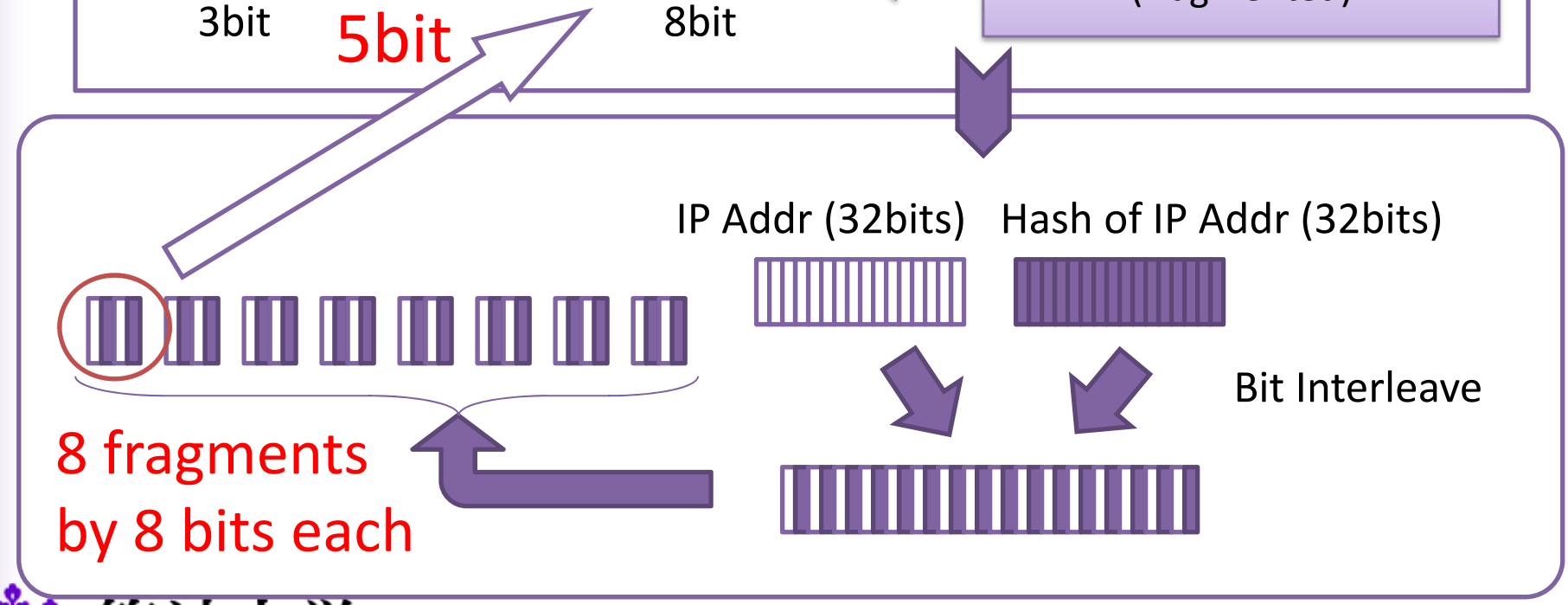
Is the length of distance appropriate?

Field of IP header for marking

Use "Identitification Field" (16bits) as

offset	distance	edge fragment
3bit	5bit	8bit

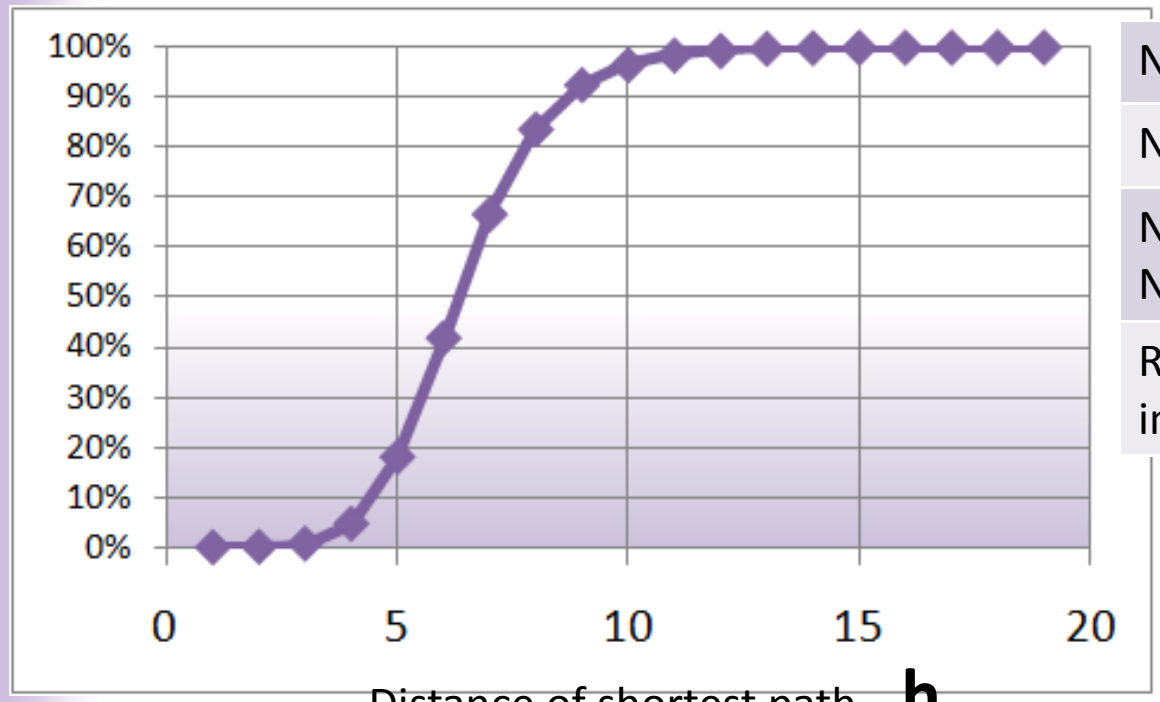
IP addresses of a router (fragmented)



Small World Property for Internet Routers

Topology of Internet Routers

Investigation by CAIDA (2003)
Small World Property (shorter path between nodes in spite of number of nodes)



Num. of Nodes	192244
Num. of Links	609066
Num. of Investigated Node Pair	1959065064
Ratio of investigated pairs	10.6%

h<=9 : 92.49%

h<=15 : 99.964%

Kanaoka's method

- Features
  - Appropriate distance field length
    - using "99.964% routers in 15 hops"
  - Reducing fragments by adjusting hash length
  - Hop count matching as an operation technique

- Evaluation of proposed method
  - Advantages of required packets for path re-building
- PPM load evaluation by implementing PPM

Kanaoka's method

Distance field

5bit to 4bit

offset	distance	edge fragment
3bit	5bit	8bit
3bit	**4**bit	**9**bit

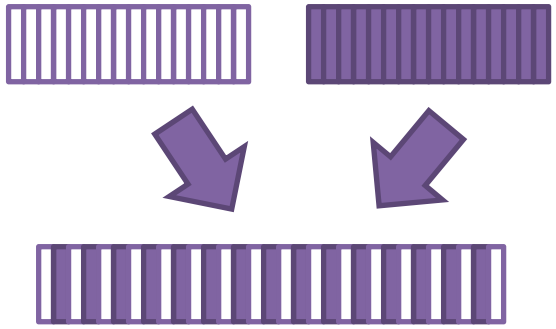
fragmented data length goes to 9bits

Size of hash

32bits to 31 bits

7 fragments by 9 bits each

IP Addr (32bits) Hash of IP Addr (**31**bits)

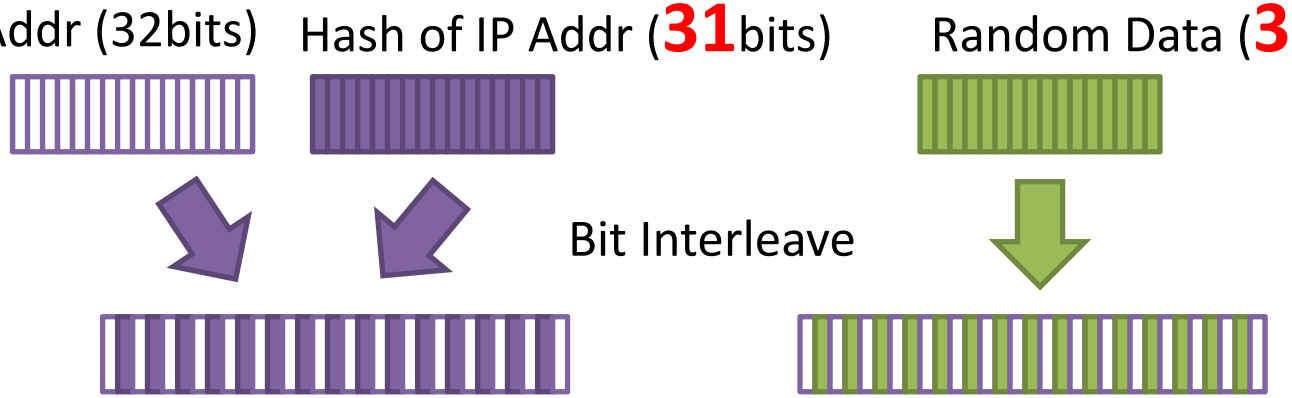


Bit Interleave

Kanaoka's method

If distance>15

Prepare another data for interlieve



in probability 1-p

- if distance value is 15
  set distance value to 0
  mark own IP info (**randomly chosen from 2 interleaved data**)

Hop Count Matching

Tolerance to Hash Collision

Hash value size in Savage's method **: 32 bits**

Hash value size in Kanaoka's method**: 31 bits**

Worse hash collision rate causes path re-building error.

Hop Count Matching

Check hop count for re-built IP by using "Tracepath" commands, and compare to "distance" value.

Evaluation of each PPM methods

Expectation of required packets

Expectation for each distance

$$E_d[n, p] = \frac{n\ln(n) + \gamma n + 1/2}{p(1-p)^{d-1}}$$

n : number of fragments
d : distance

Expectation as a whole

$$E[n, p] = \sum_{d=1}^{\infty} f_d E_d[n, p]$$

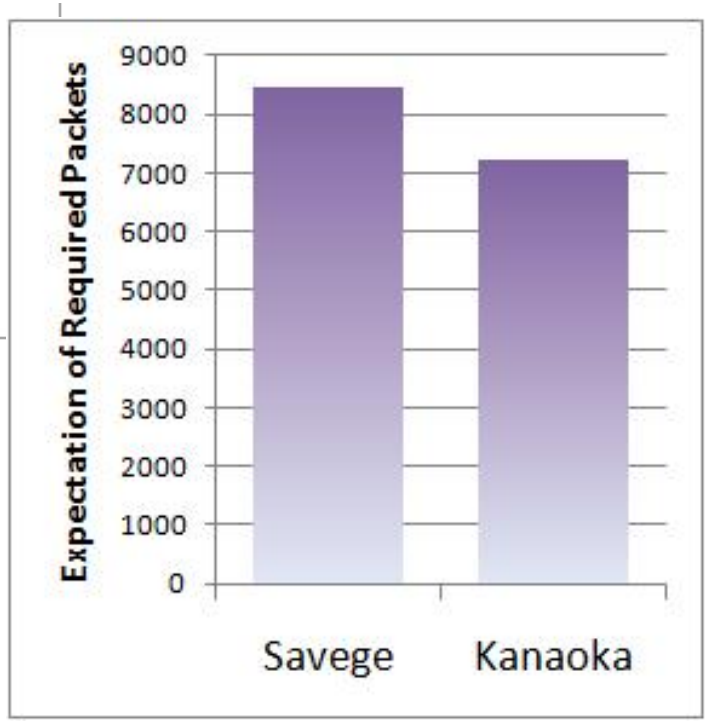
New evaluation method

f_d : path length frequency obtained by CAIDA data

Evaluation result

$E_d[n,0.04]$

	Comparison to Savage's method
Kanaoka	0.8517



$E[n,0.04]$

PPM load experimentation

Load of packet marking

If a load of packet marking is high for routers,
it will be disadvantages of PPM

We can mitigate a load by smaller marking probability.
But it makes large amount of packets for path re-buidling

Load on non-marking

PPM also make packet marking in probabiliity **1-p**,
as well as in probability **p**

Probability **1-p**

- if distance info is 0
  XOR own IP info and
  current IP info
- increment distance info

Routers rewrite packets

PPM load experimentation

Linux Implementation

Modify linux kernel and add PPM function

CPU	Intel Pentium Dual CPU E2180 2.00GHz
RAM	2GB
NIC	BCM95754 10/100/1000BaseT Ethernet Realtek R8169 Gigabit Ethernet
Kernel	2.6.18
Distribution	Cent OS 5.3

Prepared Kernels

Three types of kernels

- **ID only**
  : write constant info to Ident field
- **PPM (4%)**
  : 4% packets are marked
- **PPM (50%)**
  : 50% packets are marked

Result

Type of Kernel	Throughput (MB/s)	CPU load (%)
Defaults	39.61	12.76
ID only	40.27	12.82
PPM(4 %)	39.15	12.65
PPM (50%)	38.06	12.95

There is no meaningful difference !

PPM load experimentation 2

Linux Implementation

Modify linux kernel and
add PPM function

CPU	Intel Core2Duo E8400 (3.0GHz)
RAM	2GB
NIC	Marvell Yukon 88E8057 Intel PRO/1000 PT Desktop Adapter
Kernel	2.6.18
Distribution	Cent OS 5.3 (kernel 2.6.18)

Prepared Kernels

Three types of kernels

- **ID only**
  : write constant info to Ident field
- **PPM (4%)**
  : 4% packets are marked
- **PPM (50%)**
  : 50% packets are marked

Result

Type of Kernel	Throughput (MB/s)	CPU load (%)
Defaults	109.66	2.94
ID only	109.82	2.83
PPM(4 %)	109.21	2.96
PPM (50%)	109.88	3.07

There is no meaningful difference !

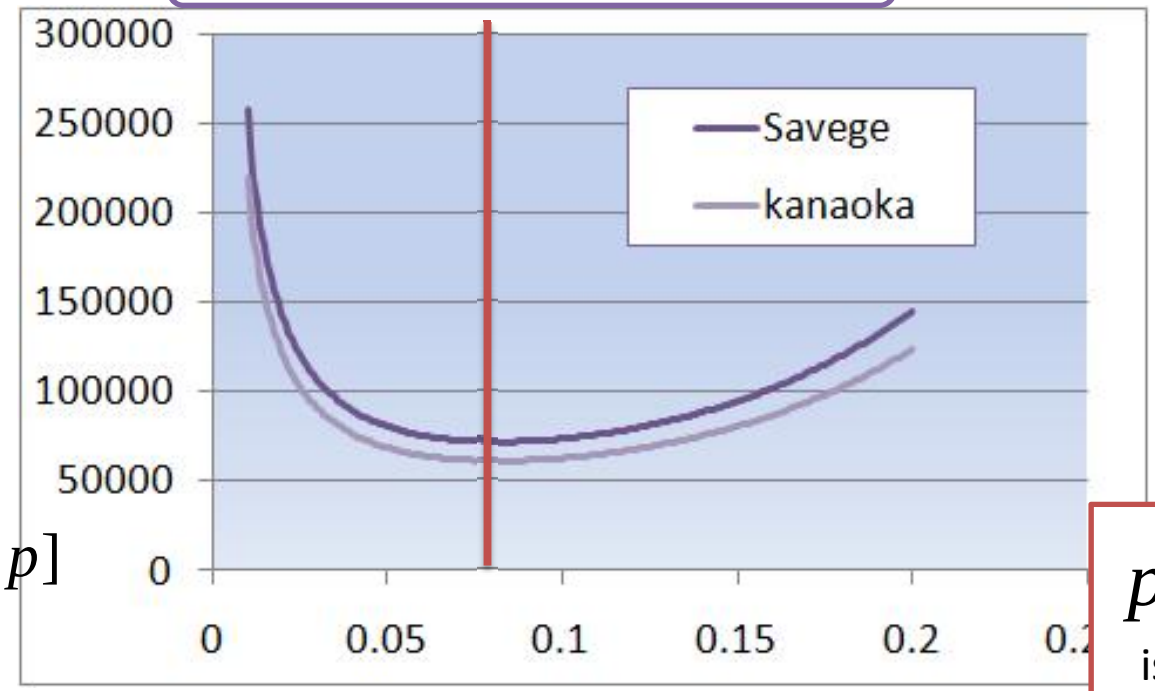
Optimum Marking Probability

to obtain **Optimum probability** for PPM, we need

Required number of packets
without distance consideration

Load of PPM for routers

Both are cleared by our research



$p = 0.082$
is optimum marking probability

Consideration of law

Telecommunications Business Act

"Secrecy of Communication"

Secrecy of communication shall not be violated.

→ All telecommunications carrier must follow the law.

Can we use any IP traceback methods ?

Recent Discussion

- Traceback without agreement of the organization concerned, may violates "Secrecy of Communication."
- If Traceback can be thought as reasonable ISP business, Traceback will be allowed.
- Is Traceback reasonable for ISP business?

→ Yes, by its purpose, necessity and appropriateness

Conclusion

- Traceback techniques
  - Probabilistic Packet Marking (PPM)
- PPM outline
  - Savege's method
  - Kanaoka's method
- PPM load experimentation
  - No meaningful difference between PPM router and default router
- Optimum Marking Probability
  - p=0.084
- Consideration of Low
  - "Secrecy of Communication"

- Contact:
  - kanaoka@cs.tsukuba.ac.jp