How to Find the Research Issue
An Example Case: IP Trace Back

May 10 2005

Wen-Shyong Hsieh, PhD.
Professor, Vice President, STU
Professor, NSYSU

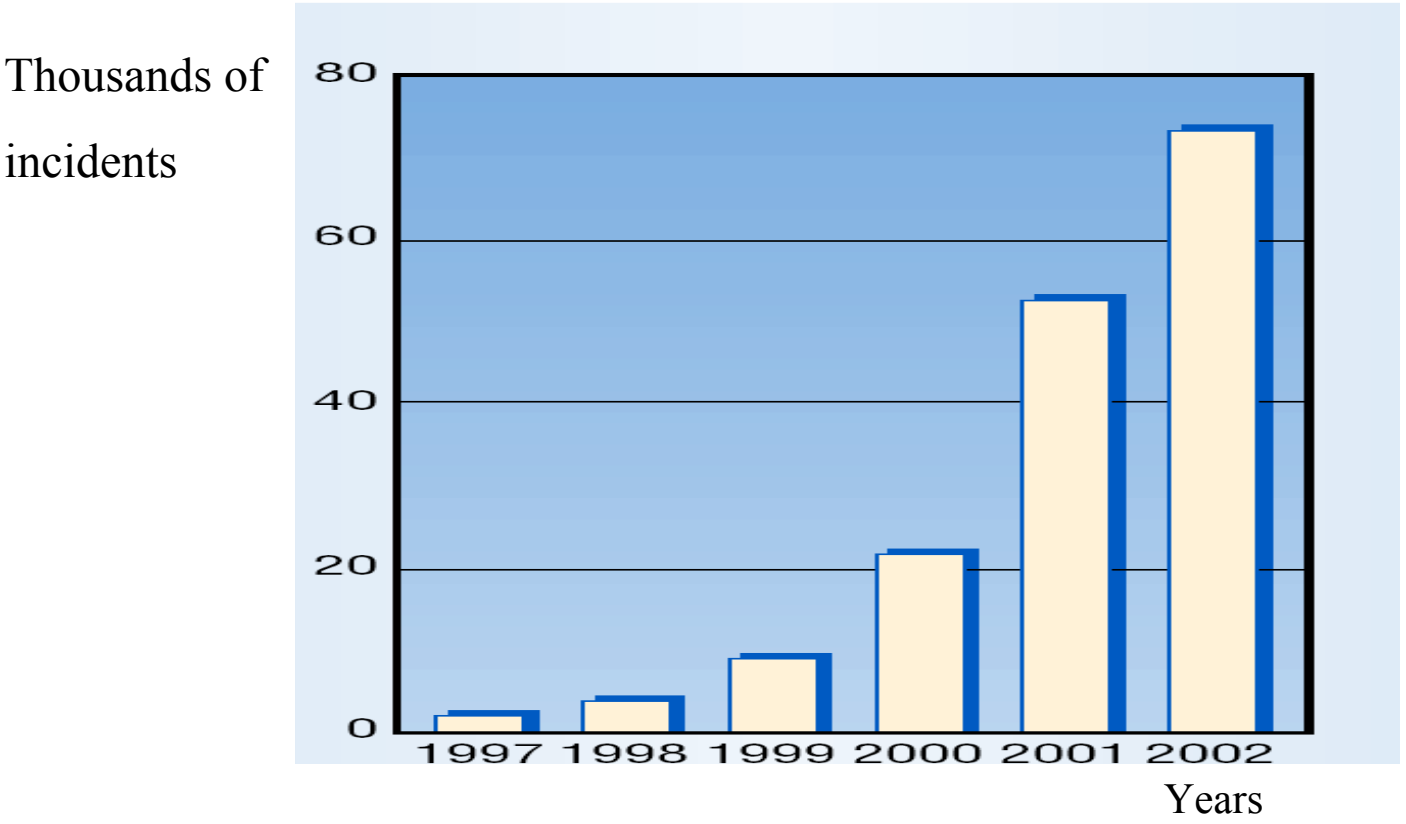
Outline

- Introduction
- IP Traceback

  Probabilistic Packet Marking (PPM)
  - *Improving Convergent Amount* (*Computational overhead*)
  - *Improving Incomplete Deployment Problem*
- Conclusion and Future Researches

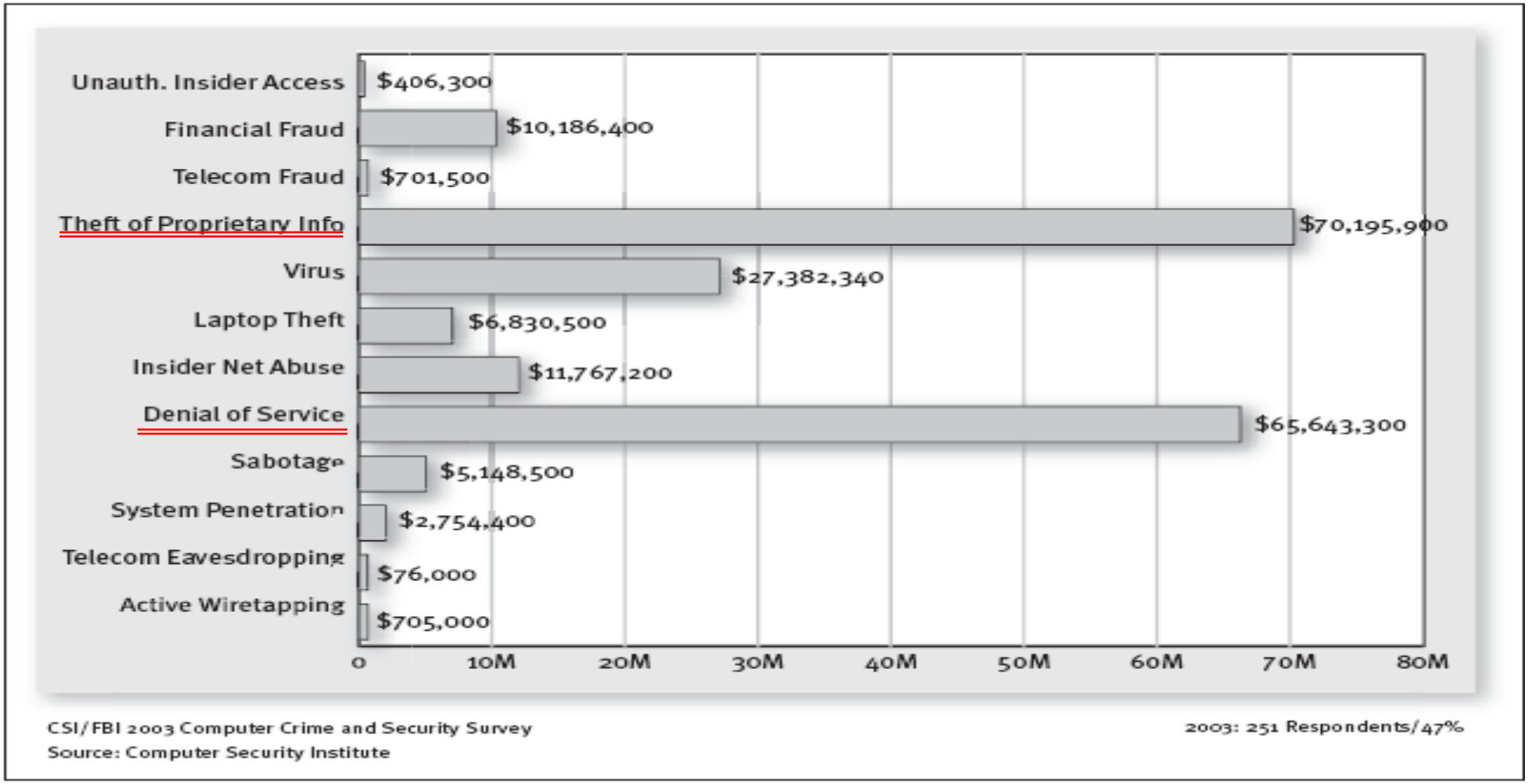
Introduction

- Network-security incidents reported to Carnegie Mellon University's CERT Coordination Center has increased steadily since 1997.



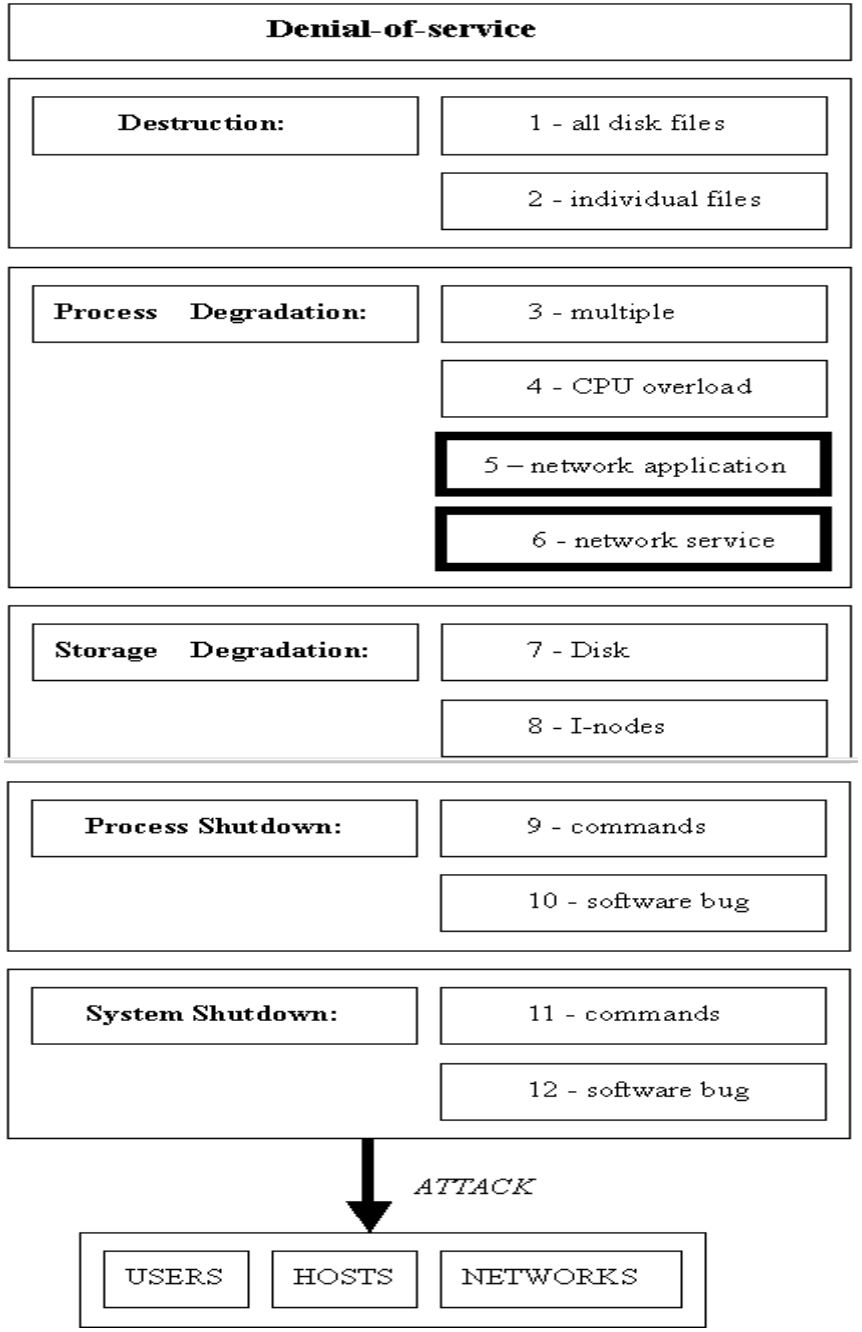
Linda Dailey Paulson, "Stopping Intruders Outside the Gates," IEEE Computer 35(11), pp. 20-22, 2002

Introduction



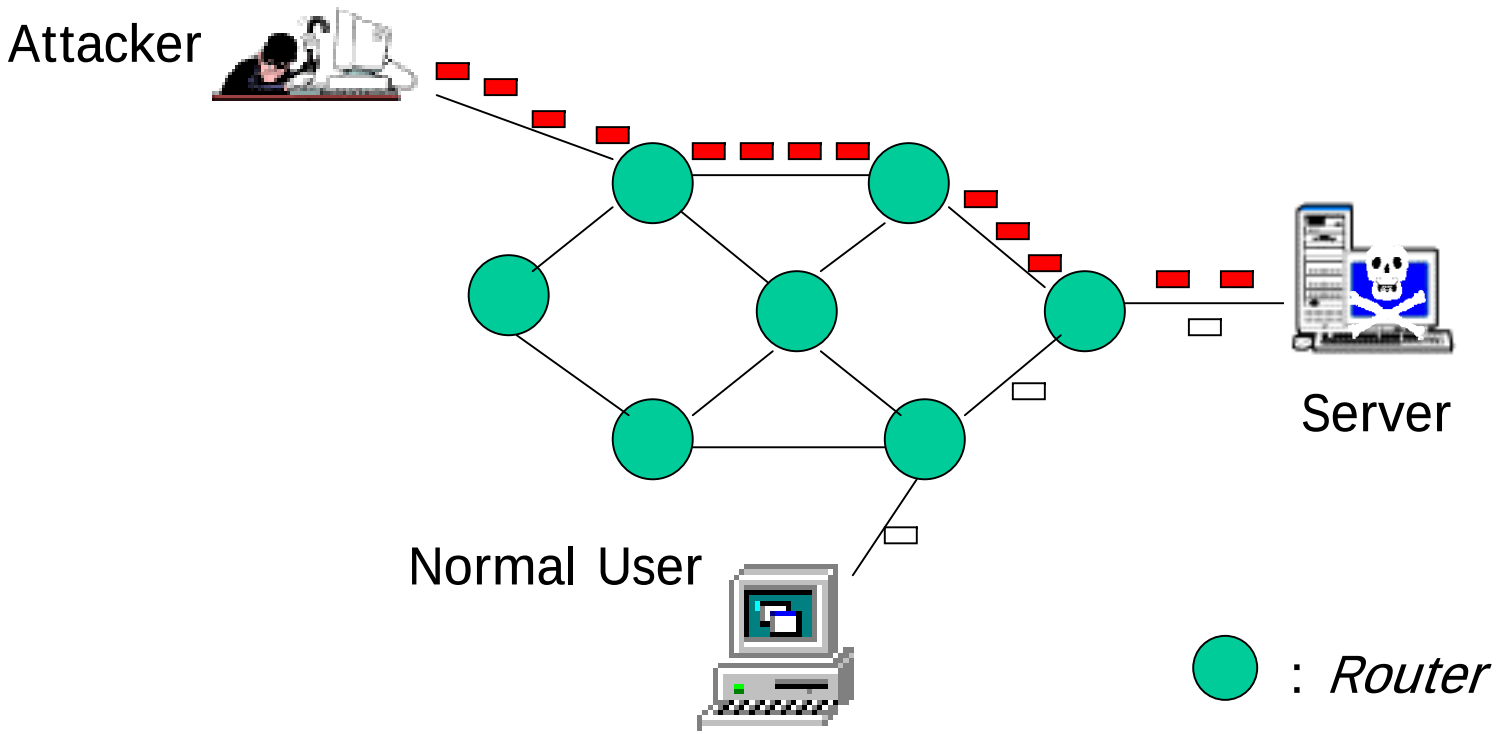
Computer Security Institute and Federal Bureau of Investigation, "2003 CSI/FBI computer crime and security survey," Computer Security Institute publication, 2003. [Online]. Available: http://www.security.fsu.edu/docs/FBI2003.pdf

A Comprehensive DoS Classification



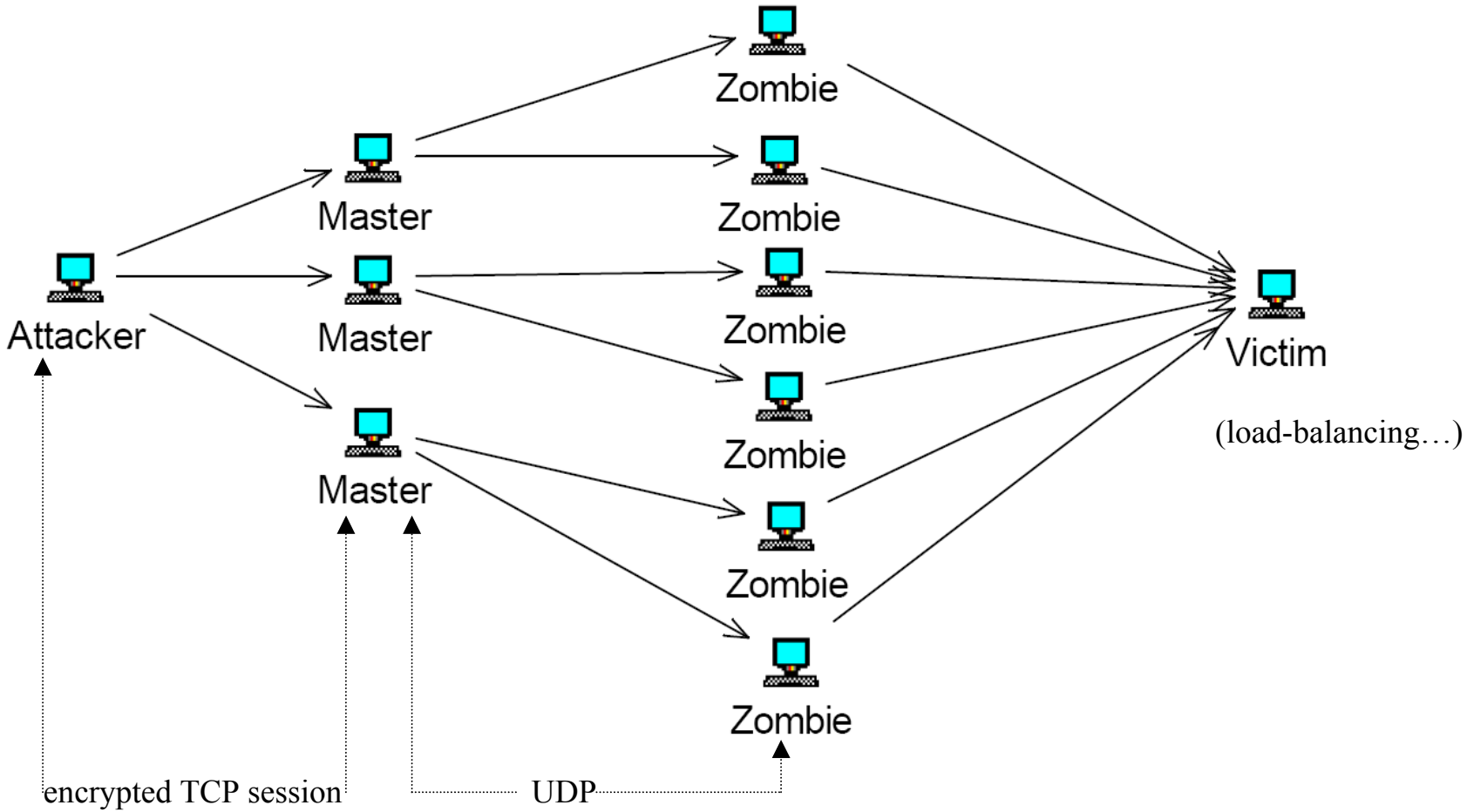
This dissertation mainly focuses on defeating network-based ***flooding-style*** DoS/DDoS attacks.

Introduction – Traditional DoS Attacks



Overwhelming stream of fake requests
consumes all resources on a server or network

Introduction – Distributed DoS Attacks



"Overview of scans and DDoS attacks," [Online]. Available: www.iwar.org.uk/comsec/resources/dos/ddos.pdf

Introduction – DoS/DDoS Defense Strategy

➢Three lines of defense:

- ***Attack prevention***
  - before the attack (Scan hosts; Monitor network traffic)
  - It's hard to know up-to-date attack models in advance.

- ***Attack detection and filtering***
  - during the attack (identify/detect and classify/filter attacks and attack packets)
  - *It is very hard to differentiate between normal traffic and attack traffic.*

  For example, rate-limiting schemes punish the good traffic as well as the bad traffic. (This is the fundamental problem of the Internet.)

- ***Attack source traceback***
  - during and after the attack

Introduction – DoS/DDoS Defense Schemes

passive V.S. active

(1)Most works in this area of dealing with DoS/DDoS attacks have focused on tolerating attacks by mitigating their effects on the victim.

(2)The other option is to trace attacks back toward their origin so as to

stop these annoying attacks thoroughly, and

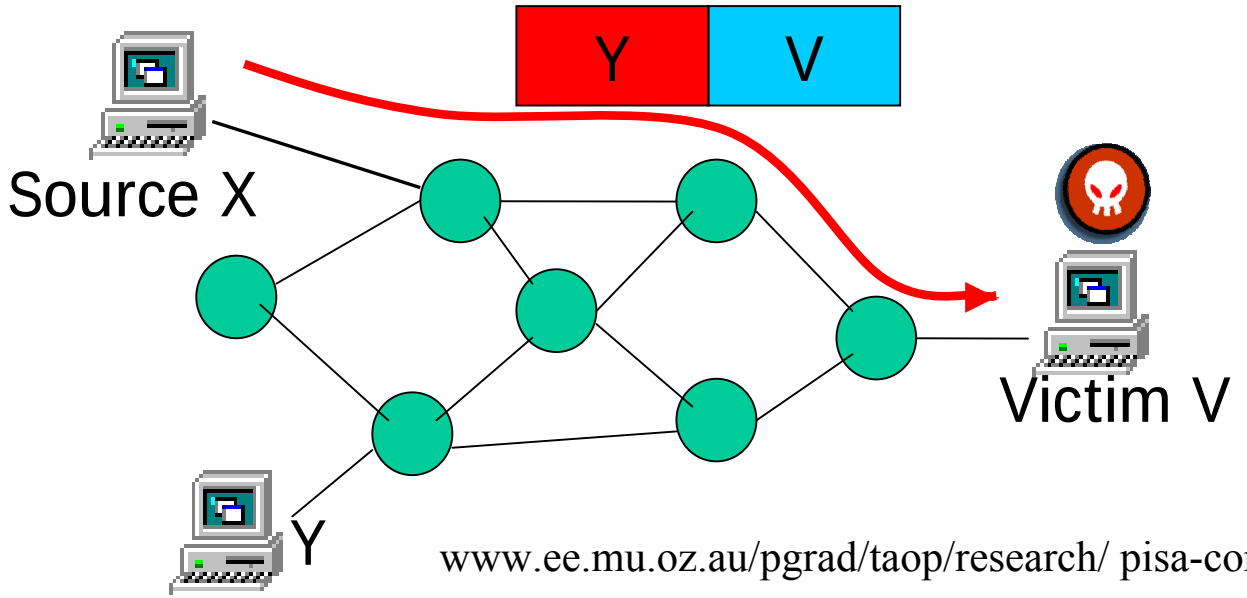
employ law-enforcement techniques against them.

IP traceback、 stepping stone traceback、layer-2 traceback (A Layer-2 Extension to Hash-based IP Traceback;IEICE)

S. Savage, D. Wetherall, A. R. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," SIGCOMM, 295-306, 2000

IP Traceback – Inherent Problems

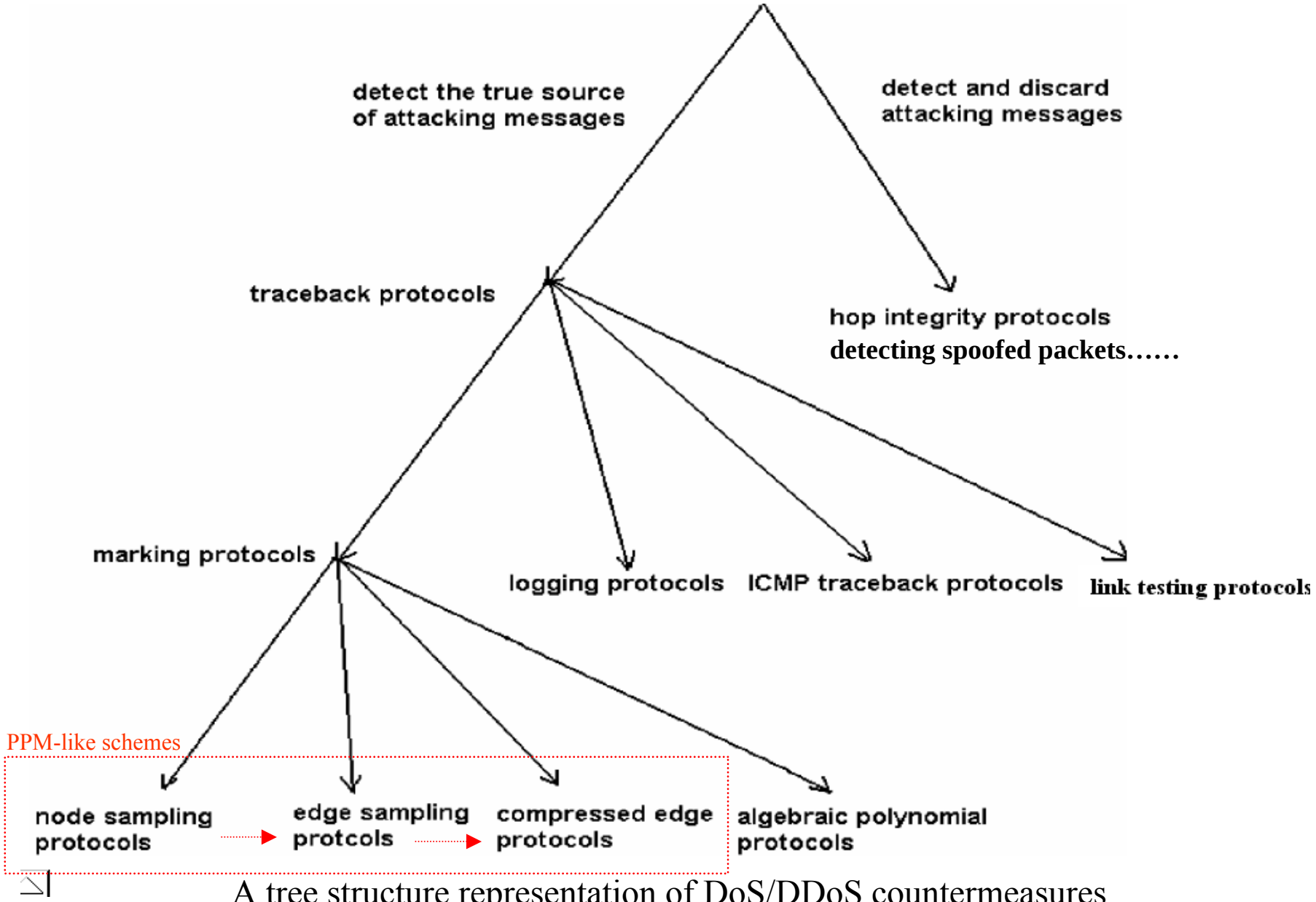
(1) Weakness of TCP/IP protocol



www.ee.mu.oz.au/pgrad/taop/research/ pisa-conference.ppt

(2) The Stateless nature of IP routing

Routers normally *know only the next hop* for forwarding a packet, rather than the complete end-to-end route taken by each packet.



A tree structure representation of DoS/DDoS countermeasures

Chun He, "Formal specifications of traceback marking protocols," An Honors Thesis, The University of Texas at Austin Department of Computer Sciences Austin, Texas, May 2002.

Probabilistic Packet Marking (PPM)

- Despite lots of proposed IP traceback approaches, PPM, still, is more feasible :

  (1) It is simple to incrementally implement,

  (2) doesn't need any additional bandwidth or storage, and

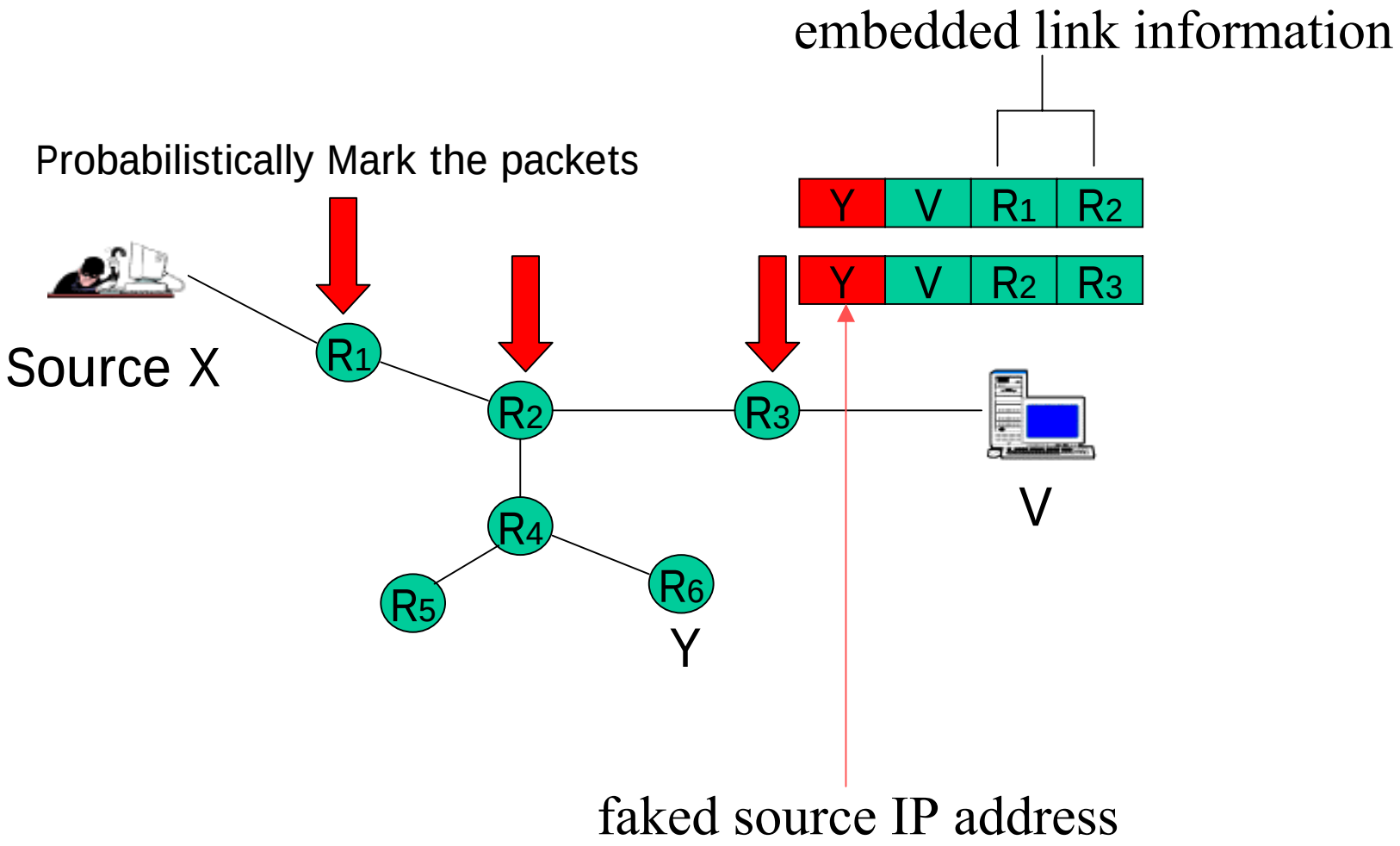
  (3) can be performed "post mortem".

- This dissertation designs an optimal IP traceback mechanism against DoS/DDoS attacks through improving the original PPM.

PPM – Assumptions

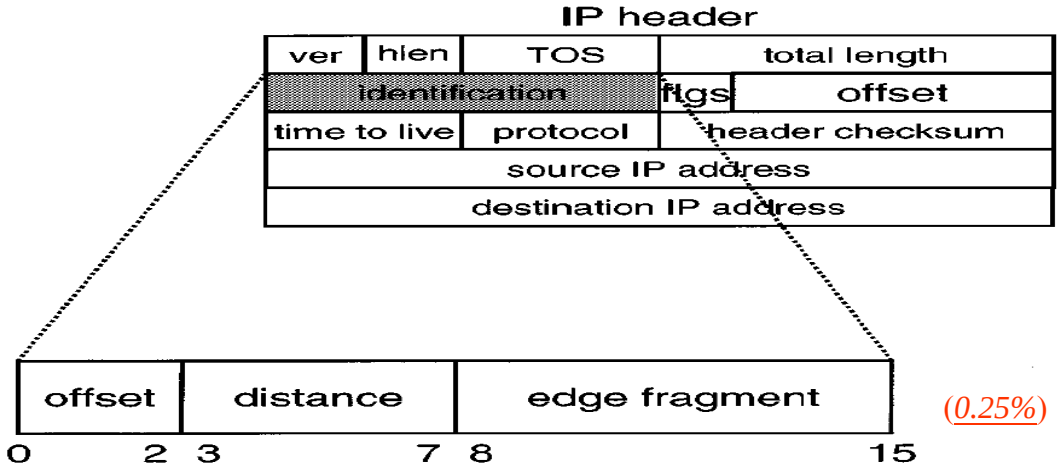
- ***Capability of Attackers*:**
  - Any attackers can generate any kind of IP datagram.
  - Multiple attackers may work cooperatively to conduct DDoS.
  - Attackers can assume the all the traffic are monitored by ISP and other authorities.
- ***Characteristics of Attacks*:**
  - Generating large number of packets for some long duration (e.g. 30 minutes)
    ("ping-of-death[CERT Advisory CA-96.26]" ➔This assumption may not hold.)
  - ***Attack path is hardly changed*** (stable)
- ***Assumptions on Routers*:**
  - Capacity of CPU processing and memory are limited
  - ***Router is not threatened by intrusion and other unauthorized access***
  - ***Router never generates any kind of forged data***
- ***Any packets may be discarded and reordered***

PPM – Overview

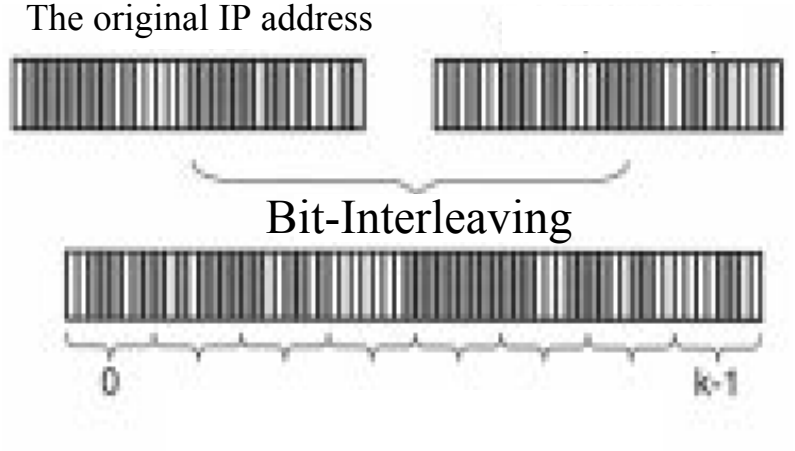


www.ee.mu.oz.au/pgrad/taop/research/ pisa-conference.ppt

PPM – CEFS



(0.25%)



Send *k* fragments into network.

(Address, verifier) pair similarity.

Address	Verifier
0x00a18**4**e0	0xd0246**7**1c
0x00a18**a**e0	0xd0246**5**1c

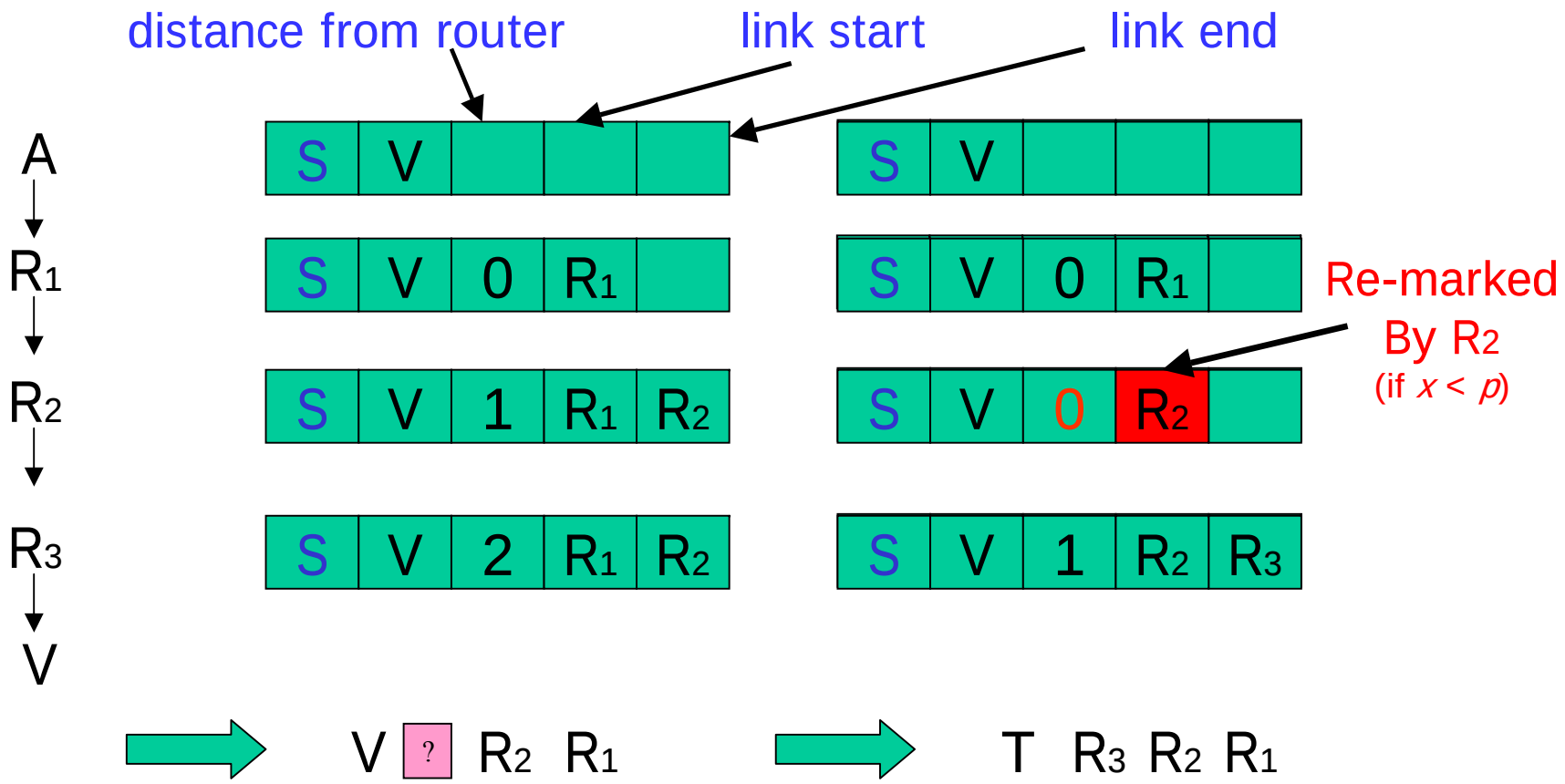
Messages sent out.

Format: (distance, offset i, address$_i$, verifier$_i$)

$(x, 7, 0, \mathrm{d})$
$(x, 6, 0, 0)$
$(x, 5, \mathrm{a}, 2)$
$(x, 4, 1, 4)$
$(x, 3, 8, 6)$
$\mathbf{(x, 2, 4, 7)}$ $\mathbf{(x, 2, a, 5)}$
$(x, 1, \mathrm{e}, 1)$
$(x, 0, 0, \mathrm{c})$

S. Savage, D. Wetherall, A. R. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," SIGCOMM, 295-306, 2000

PPM – Overview



PPM – Challenges

- ✓ (1) The convergent amount of marked attack packets
- ✓ (2) The computational overhead for reconstructing the attack path

  (3) The robust against the false positive/negative
- ✓ (4) The incrementally deployment

PPM – Improving Convergent Amount

- If each router has a disjoint equal marking probability p, the probability of receiving a marked packet from a router d hops away from the victim is $p(1-p)^{d-1}$.

  Problem: $p \geq p(1-p)^1 \geq p(1-p)^2 \geq \ldots \geq p(1-p)^{d-1}$

- Choices between different p values:

  marked-free packets or attacker's spoofed packets

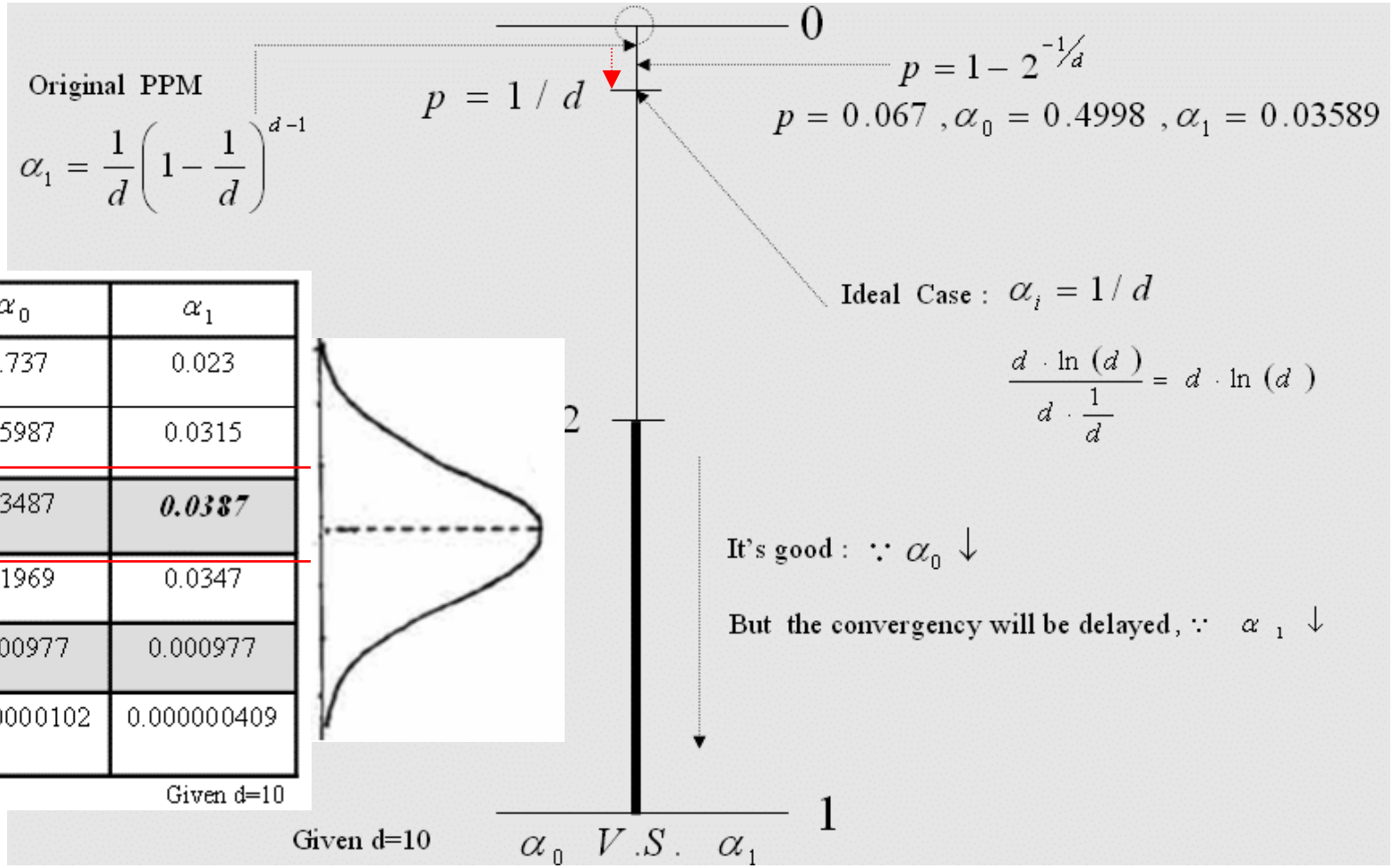
  The marking probability should be greater than 1/2 for completely eliminating attacker's spoofed packets to avoid $(1-p)^d \geq p(1-p)^{d-1}$, however, this will delay the convergency. (因此,原則上marked-free packets會有很多)

  Considering that the attacker's spoofed packets are in the absolute majority, $p \leq 1 - 2^{-1/d}$ holds, since $(1-p)^d \geq \sum_{i=1}^{d} p(1-p)^{i-1}$.

  Worst of all, $p(1-p)^{d-1} \leq 1 - 2^{-1/d}$, if $p \leq 1/d$.

PPM -- Improving Convergent Amount

a Dilemma of choosing p



p	α_0	α_1
0.03	0.737	0.023
0.05	0.5987	0.0315
0.1	0.3487	***0.0387***
0.15	0.1969	0.0347
0.5	0.000977	0.000977
0.8	0.000000102	0.000000409

Given d=10

PPM – Improving Convergent Amount

- PPM conservatively assumes that marked packets from all of d routers have the same likelihood as the furthest router.
- As the coupon collector problem, the expected trial number of getting one of each of d equiprobable marked packets is $d(ln(d)+\gamma)$.

$$1+\frac{d}{d-1}+\frac{d}{d-2}+\cdots+d=d\cdot H_d\approx d(\ln d+\gamma)$$

(γ presents Euler's constant) ($\gamma \doteqdot 0.58$)

(Bernoulli's binomial distribution)

	success	failure
X	1	0
P	p	$1-p$

- Therefore, the number of packets required for reconstructing a path of d routers has the following bounded expectation:

$$\mathrm{E}(X)\approx d(\ln(d)+\gamma)\cdot\frac{1}{dp(1-p)^{d-1}}=\frac{\ln(d)+\gamma}{p(1-p)^{d-1}}$$

PPM – Improving Convergent Amount

(1)*Worst Case* : (with a fixed probability)

$$E(x) < \frac{d \cdot (\ln(d) + \gamma)}{d \cdot p(1-p)^{d-1}} = \frac{(\ln(d) + \gamma)}{p(1-p)^{d-1}}$$

By differentiating $E(x)$, the optimal p is $1/d$.

(2)*Best Case* : (Ideal Case)

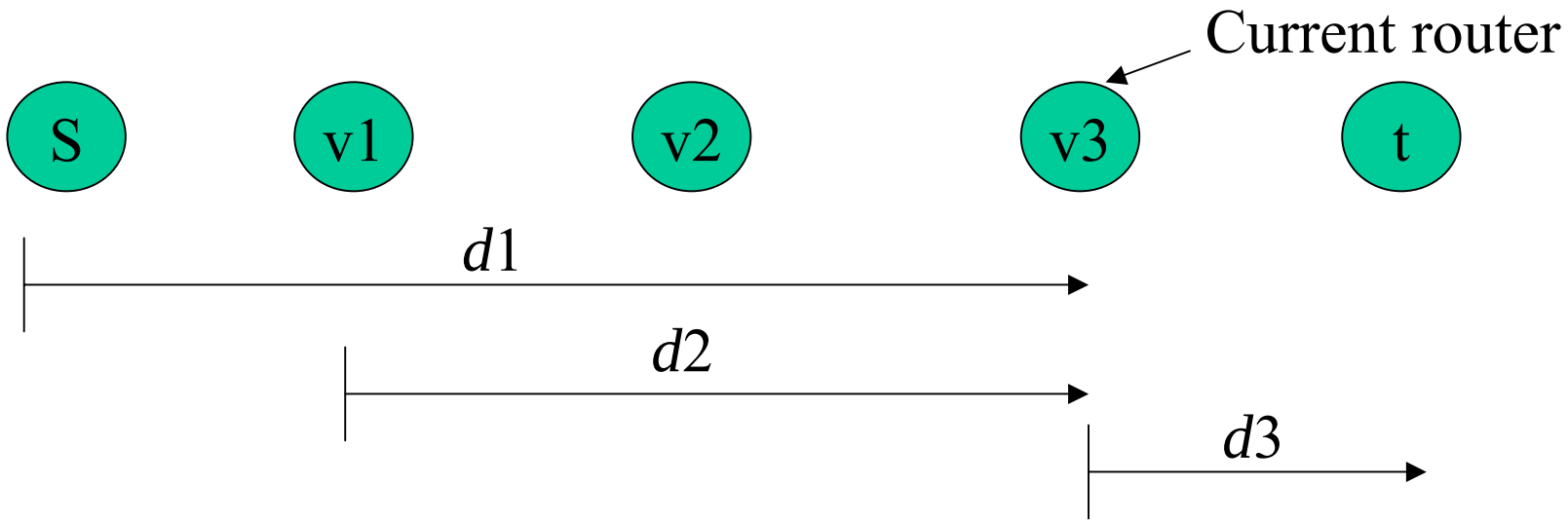
For the ideal case, if all marked packets marked by every router with marking probability p can be collected fully by the victim, $E(X)$ will be $d(ln(d)+\gamma)$ when $p=1/d$.

$$\frac{d \cdot (\ln(d) + \gamma)}{d \cdot p}$$

PPM – Improving Convergent Amount

Adjusted Probabilistic Packet Markingdaptive (APPM)

- T. Peng et al propose 3 different schemes for adjusting the marking probability based on the different distance measures *d*1, *d*2 and *d*3.



*d*1 :distance from attack source to current router

*d*2 :distance from last router to mark packet to current router

*d*3 :distance from current router to destination

T. Peng, C. Leckie, and K. Ramamohanarao, "Adjusted Probabilistic Packet Marking for IP Traceback," in Proc. Networking, May 2002

PPM – Improving Convergent Amount

Adjusted Probabilistic Packet Markingdaptive (APPM)

Scheme 1: $P_1(d_1) = 1 / d_1$

$1 \cdot (1 - 1/2) \cdot (1 - 1/3) = 1/3$

Add extra field in IP option field to record the distance *d1* ***:Ideal but need extra field; not practical***

Scheme 2 : $P_2(d_2) = \dfrac{1}{2(d_2 + 1)}$

Extract the distance information *d2* from the marking field: ***Need solve security problem***(to make sure the distance value in the marking field is trustable; not optimal)

Scheme 3 : $P_3(d_3) = \dfrac{1}{c + 1 - d_3}$

$1/c \le 1/d$

Find distance *d3* from the routing table : faked routing update info. (metric=1)

T. Peng, C. Leckie, and K. Ramamohanarao, "Adjusted Probabilistic Packet Marking for IP Traceback," in Proc. Networking, May 2002

PPM – Improving Convergent Amount

Proposed Ideas

- *Probabilistic packet marking with non-preemptive compensation* (PPM-NPC) (non-preemptive ; waiting the opportunity)

- *Compensated Probabilistic Packet Marking* (CPPM) (preemptive)

PPM – Improving Convergent Amount

Proposed PPM-NPC : Algorithm

PPM-NPC marking procedure at router R with marking probability p:

```
for each incoming packet w with a tuple (w.start, w.end, w.distance) in the IP Header
    get a random number x. x is in [0..1]
    let C be a compensation counter in this router
    if x < p then
      {
       if w.start <> 0 then
          {
            C= C + 1
          }
       if w is a marked-free packet then
          w.start = R,    w.distance = 0
    }
    else
     if w is a marked-free packet and C is not zero then
      {
       w.start = R,    w.distance = 0
       C= C - 1
      } /* end of " if x<p" */

    if ( w.disatnce = 0 and w.start <> R ) then
      w.end = R
    increment w.distance
```

PPM – Improving Convergent Amount

Proposed PPM-NPC : Properties-1

- We have proven that the volume of marked-free packets is always equal to or greater than the reduction of marking probability, so that the probability that a marked packet is received by the victim is equal to its marking probability p.

$p_{j,i} = p$ in all j and $i \geqq j$.

PPM – Improving Convergent Amount

Proposed PPM-NPC : *Properties-2*

- While d is 10 and p is 1/25 , the average counter size of each router is approximately 4.

If the total number of packets is M, each router's counter must handle $[M \cdot((2^5-1)-1) \cdot p^2]$ at most.

While the number of packets required for convergence in PPM-NPC is $[(d\cdot(ln(d)+\gamma))/(d\cdot p)]$, the necessary counter size of a linear topology is:

$$\left[\frac{\ln(d)+\gamma}{p}\right]\cdot\left(2^5-2\right)\cdot p^2=\left(2^5-2\right)\cdot p\cdot(\ln(d)+\gamma)$$

- Therefore, for a 2-byte integer variable, we can cope with (65536 / 4) different attack paths, especially in the distributed DoS attacks.

PPM – Improving Convergent Amount

Proposed PPM-NPC : Simulation

- The real-time NS-2 simulator is used to verify the proposed PPM-NPC scheme as well.
- The experimental linear topology consists of one attacker, one victim, and ten intermediate routers.
- Because 50% of DoS attacks have at least 1,000 packets per second and most attacks last at least 10 minutes, the attack traffic rate is 1000 User Datagram Protocol (UDP) packets per second.
- The marking probability is 0.1.
- After 15 simulation runs, the mean value is roughly 30, and the standard deviation is 7.8.
  Because the idea result is $(\ln(10)+0.58)/0.1 \fallingdotseq 29$, the simulation result also proves PPM-NPC can approach the optimal situation.

Moore, D. Voelker, G. and Savage, S., "Inferring Internet Denial of Service Activity," in Proc. USENIX Security Symposium, Washington D.C., August 2001

LBNL Network Research Group, UCB/LBNL/VINT Network Simulator - ns (version 2), DARPA: VINT project. [Online]. Available: http://www.isi.edu/nsnam/ns.

PPM – Improving Convergent Amount

Proposed CPPM

➢ *Drawbacks of Non-preemptive compensation*:

(1) If the attackers knew this scheme, they are easy to disable this scheme by simply generate each attack packet embedded with random ID value in advance.

(2) It can't prevent malicious packets from passing through.

➢ *Preemptive Compensation*

A CPPM-capable router will maintain a compensation table, formatting each entry *e* as (e.start, e.end, e.distance, e.counter), to record the information of marked packets, which are remarked by this router.

The reduced marking probability is compensated according to the compensation table, while each marked-free packet is received.

PPM – Improving Convergent Amount

Proposed CPPM : Algorithm

CPPM marking procedure at router R with the marking probability p:

for each incoming packet *w* with a tuple (*w.start*, *w.end*, *w.distance*) in the IP header
  get a random number *x*. *x* is in [0..1]
  let *T* be the compensation table in this router
  if *x* < *p* then {
    if *w.start* <> 0 then {
      for each entry *e* in *T*
        if (*w.start*, *w.end*, *w.distance*) == (*e.start*, *e.end*, *e.distance*) then
          increment *e.counter*
        else
          insert (*w.start*, *w.end*, *w.distance*, 1) into *T*
    }
    w.start = *R*, *w.distance* = 0
  } else {
    if *w* is a marked-free packet and *T* is not empty then {
      select a entry *e* by round robin from *T*
          (*w.start*, *w.end*, *w.distance*) = (*e.start*, *e.end*, *e.distance*)
          e.counter = *e.counter* – 1
          remove the entry while *e.counter* is zero }
    if *w.disatnce* = 0 then {write *R* into *w.end* }
    increment *w.distance*
  }

PPM – Improving Convergent Amount

Proposed CPPM

- We have proven that, with CPPM, the probability that each marked packet will arrive at the victim equals its original marking probability. Consequently, *CPPM efficiently achieves the optimal convergent situation as well*.

- The computational overhead will also be improved while the convergency is revised.

PPM – Improving Convergent Amount

Proposed CPPM: Simulation

- The same real-time NS-2 simulator is used to verify CPPM.
- The experimental linear topology comprises one attacker, one victim, and ten intermediate routers.
- The attack traffic rate is 1000 UDP attack packets per second. The marking probability is
- Following ten simulation runs, the mean value is roughly 30, and the standard deviation is 8.6.
  Because the idea result is $(\ln(10)+0.58)/0.1 \fallingdotseq 29$, the simulation results presented here also prove that CPPM can approach the optimal situation.

LBNL Network Research Group, UCB/LBNL/VINT Network Simulator - ns (version 2), DARPA: VINT project. [Online]. Available: http://www.isi.edu/nsnam/ns.

PPM – Improving Convergent Amount

Proposed CPPM : Pros & Cons

- *The advantages of CPPM are*:
  (1)This scheme can *disturb* marked packets with preemptively re-marking them.
  (2)CPPM can *avoid the disadvantage of PPM-NPC*, that is, an attacker can easily disable PPM-NPC through producing each attack packet embedded with random ID value in advance.

- *The disadvantages of CPPM are*:
  (1)This scheme needs *an additional storage space* as compared with PPM-NPC.
  (2)*CPPM can not prevent malicious packets from passing through as well*. Although CPPM can disturb marked packets, forged path messages kept in the compensation table may still have a chance to be compensated and then arrive at the victim. This is resulted from the fundamental PPM robustness problem. *(future work)*

PPM – Improving Incomplete Deployment Problem

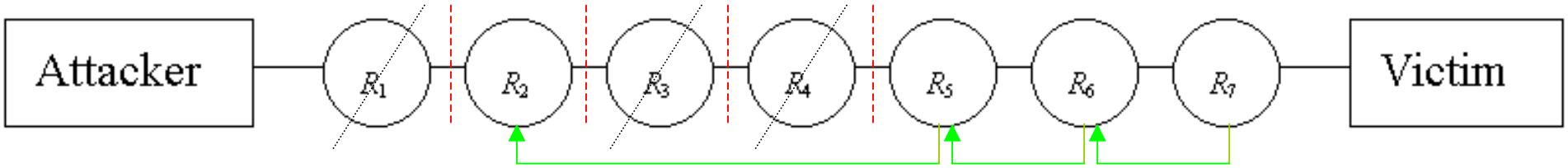
- One of the desired features of a traceback approach is incremental deployment into the current Internet structure, at low cost.

- In PPM, any reconstructed link is only composed of two neighboring PPM routers.

  - *It may imply that we need to implement the mechanism on every router, if we require the complete attack path for forensic evidences.*

  - *On the other hand, if more than one router along the attack path does not support PPM, this PPM mechanism may reconstruct unreliable paths.*

PPM – Improving Incomplete Deployment Problem



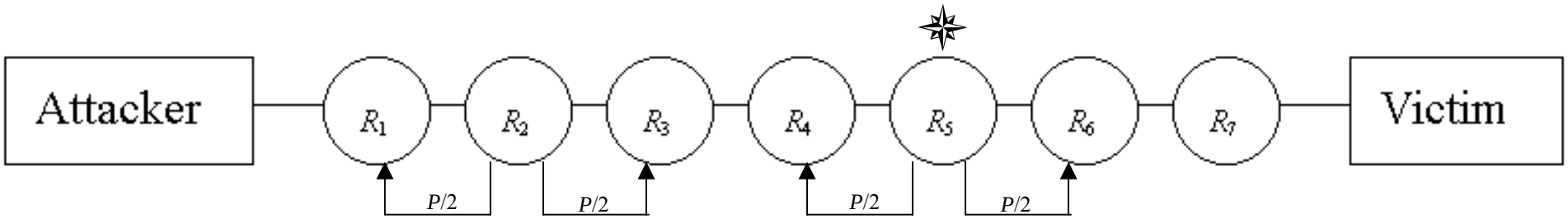
- If R_2, R_5, R_6, and R_7 is PPM routers, the link information, i.e. (R_1, R_2), (R_2, R_3), (R_3, R_4), and (R_4, R_5), will be apparently lost, and worst of all, one also can't precisely point out the leaf router R_1, which may be an attacker's compromised router.

- Accordingly, an improved PPM approach, which is based on PPM-NPC, for IP traceback to advance the accuracy of a reconstructed path in an incomplete PPM deployment environment is proposed. Moreover, this improvement may also be used with a view to reducing the deployment overhead without requiring the participation of all routers on the attack path.

PPM – Improving Incomplete Deployment Problem

The proposed Idea

➢ *Remedial PPM-NPC* (RPPM-NPC)



$(R_3,R_4,1)$ ➔ $(R_3,R_4,2)$+R_4 does not work if R_5 doesn't receive $(R_4,R_5,1)$ yet.

$(R_4,R_5,1)$ ➔ R_4 works

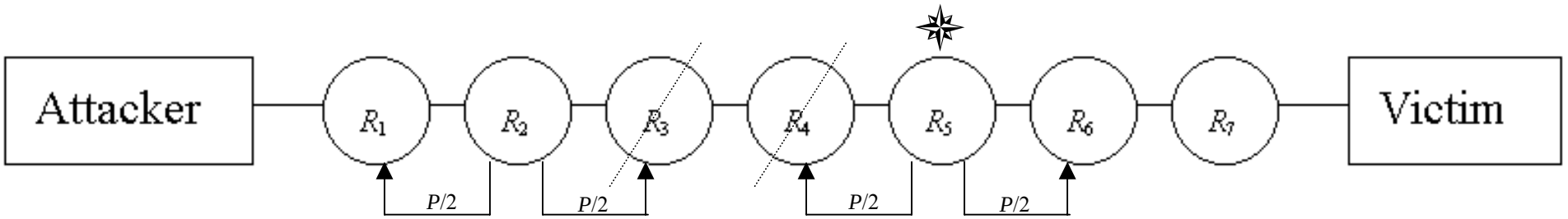
$(R_3,R_4,1)$+ R_4 works ➔ $(R_3,R_4,2)$

$(R_2,R_3,1)$+ R_4 does not work ➔ $(R_2,R_3,3)$

PPM – Improving Incomplete Deployment Problem

Proposed Idea

- *Remedial PPM-NPC* (RPPM-NPC)



$(R_3,R_4,1)+(R_4,R_5,1)$ R_4 is neither a RPPM-NPC-capable router nor an individual transparent router.

$(R_1,R_2,1)$ → (R_1,R_2)

$(R_2,R_3,1)$ → (R_2,R_3)

$(R_1,R_2,1) \rightarrow (R_1,R_2,4)$

$(R_2,R_3,1) \rightarrow (R_2,R_3,3)+(R_3,R_4,2)$

R_3: the first transparent router

RPPM-NPC marking procedure at R_i with marking probability p :

for each incoming packet with marked message, $M(m.start, m.end, m.distance)$

```
if (R_i is the attached router of the source node of this incoming packet)
   { R_i marks the incoming packet with W(0, 0, 0)} /* R_i is a leaf router*/
get x at random from [0..1]
if (0 ≦ x < p/2) { R_i makes a backward-link message W(R_i-1, R_i, 1)}
else
   if (p/2 ≦ x < p) { R_i makes a forward-link message W(R_i, R_i+1, 1)}
   else { R_i makes W with null value}
if ( W(w.start, w.end, w.distance) is equal to one of (r.start, r.end, r.distance)
     in R ) {increase this r.counter by 1}
else { if (W is not null) {insert (w.start, w.end, w.distance, 1) into R}

 if (m.distance <> 0) /* the incoming packet is not marked-free */
  {if (m.distance <> 1) { increase m.distance by 1}
   else{ /* m.distance =1 */
    if (m.end = R_i) { I_R_i-1 = 1}  /* R_i-1 is a RPPM-NPC-capable router */
    else { if (m.end = R_i-1) {
              if (I_R_i-1 = 1) { w.distance =2}
              else { /* R_i-1 may be an individual transparent router*/
                     I_R_i-1 = 2, w.distance =2} }
         else{ /* m.end <> R_i and m.end <> R_i-1, but m.distance=1 */
           if (I_R_i-1 = 2) { w.distance =3} /* It's the link (R_i-3, R_i-2).*/
           else {
            if ((m.start, m.end) is not any one of (c.start, c.end) in C)
                 { insert (m.start, m.end) to C }
            /*Find the backward link of the previous closed RPPM-NPC router.*/
            if (m.end is equal to one of c.start in C) { w.distance =4}
            else{
            /* Find the first one among consecutive transparent routers.*/
               if (m.start is equal to one of c.end in C) {
                  w.distance =3
                  if ((m.end, R_i-1, 2) is one of (r.start, r.end, r.distance)
                       in R) { r.counter = r.counter +1}
                  else{ insert (m.end, R_i-1, 2, 1) into R }}}}}}}
 else{ /*w.distance =0, that is the incoming packet is marked-free */
  if ( R is not empty) {
       pick up any one (r.start, r.end, r.distance, r.counter) of R
       mark the incoming packet with (r.start, r.end, r.distance)
       r.counter = r.counter −1
      if (r.counter =0) {remove this corresponding tuple from R}
  }
} /* end of main-program */
```

Proposed RPPM-NPC

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC

- RPPM-NPC can correct and recover

143

144

  any discontinuous individual transparent router and

  any segment of consecutive double transparent routers.

  In the future, we will try to extend the remedial capacity, and devise an optimal solution to recover all transparent routers in a segment.

- If the attacker makes many faked marked packets and the leaf router is a RPPM-NPC-capable router, the problem can also be corrected by clearing each faked packet's mark field.

- *If the leaf router is a compromised router, RPPM-NPC can help the victim reconstruct a correct path, including the concealed leaf router.*

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC* : *The Consideration to Reducing Deployment Cost

- Let's consider a attack path R_1, R_2,…, R_{15}. If R_2, R_5, R_8, R_{11}, and R_{14} are RPPM-NPC routers in this path, this scheme can still reconstruct the complete path, and the ratio of the saved deployment cost will be 2/3.

- As a result, RPPM-NPC may also be used to *really achieve the "incremental deployment"* and reduce the deployment overhead without requiring the participation of all routers on the attack path.

- From another view, a few routers with RPPM-NPC, which located in some distance from each other, can do the same work as a large number of PPM-capable routers in a row.

Conclusion

- In consideration of the difficulty in defeating DoS/DDoS attacks, the research in this dissertation *focuses mainly on designing an optimal IP traceback mechanism against DoS/DDoS attacks* for tracing back to the origins of DoD/DDoS attacks, so as to stop these annoying attacks thoroughly, and employ law-enforcement techniques against them.

- A better IP traceback scheme, the probabilistic packet marking (PPM) , has been discussed. In this dissertation, an outstanding improvement regarding some PPM criteria: *the convergency*, *the computational overhead*, and *the incomplete PPM deployment problem*, has been achieved.

Future Research

I. ***Distributed Attacks*** -- ***DDoS***

For moderate distributed attacks, it has serious limitations due to ***the difficulty in correctly grouping fragments together***.

II. ***Advanced Attack Origin Detection***

Attackers can hide their true identities by *"laundering" attacks through third parties*,either indirectly (e.g., smurf attacks or DNS reflectors) or directly via compromised *"stepping stone"* machines or IP-in-IP tunnels. *One interesting possibility enabled by the packet marking approach is to extend traceback across "laundering points."*

Future Research

III. PPM cannot handle ***reflective DDoS*** attack very well.

IV. IP traceback is just a small research area in the network security. Therefore, it is also necessary for further promoting the traceback ability by combining other network security mechanisms, such as security auditing system, IDS, system access control and user authentication mechanism, to implement a more complete, integrated security architecture.

E.g.

CPPM or PPM-NPC can also combine the Moving Firewall concept, proposed by NTT (Nippon Telegraph and Telephone Corporation), or the congestion-control based Pushback method mentioned above for alleviating the attack effect at the same time while tracebacking the attacker.

M. Falk and J. Bengtsson, " Distributed denial of service: Countermeasures from a system's perspective," TDDC03 – Information Security Report, May 2003. [Online]. Available: http://www.ida.liu.se/~TDDC03/old/projects/grp_7.pdf

Future Research

V. ***Reducing the number of duplicate Traceback messages***

- Some ICMP traceback schemes, such as iCaddie and PICA , are proposed to reduce the number of ICMP messages produced for avoiding generating duplicate messages to the victim.
- The same improvement should be also achieved in PPM, *such that each PPM-capable router does not aimlessly mark packets, and will intelligently decides when to mark or re-mark a packet according to these passing marked packets*, which are resulted from the upstream routers.

[81] B.T. Wang and H. Schulzrinne, "A denial-of-service-resistant IP traceback approach," 3rd New York Metro Area Networking Workshop (NYMAN), Polytechnic University, Sept. 2003. [Online]. Available: http://www.nyman-workshop.org/2003/papers/ A Denial-of-Service-Resistant IP Traceback Approach_paper.pdf

[82] F.H. Hsu and T.C. Chiueh, "A path information caching and aggregation approach to traffic source identification," Proc. 23rd IEEE Intl. Conf. Distributed Computing Systems (ICDCS), May 2003.

Future Research

VI. ***Weak Assumptions***

PPM assumes each router along the attack paths is not compromised, thus it is not robust against a compromised routers.

VII. ***Improving PPM Robustness***

VIII. ***Improving PPM Computation overhead***

The End

Future Research
Improving PPM Robustness

- two terms: (defined by Song and Perrig)
  - *false positive*:
    A path that does not take part in an attack but it is reconstructed by a traceback mechanism.
  - *false negative*:
    A path that takes part in an attack but it is not reconstructed.
- The traceback approach is robust if it gives a *relatively low rate of false positives and false negatives*, and if *the rate does not grow rapidly with increased number of attackers*.

Dawn X. Song and Adrian Perrig, ”Advanced and authenticated marking schemes for IP traceback,” in Proceedings IEEE INFOCOM, 2001.

Future Research
Improving PPM Robustness

- In terms of robustness, the PPM-like approaches are insufficiently robust. The Savage algorithm gives a very high rate of false positives.

- Such behavior is explained, again, by a constraint *to break the router's IP address into eight pieces (k=8)*, rising the probability of the accidentally incorrect reconstructed paths at the victim side.

$$k \uparrow \Rightarrow computational \quad overhead \uparrow$$
$$\Rightarrow per-packet \quad space \quad overhead \downarrow$$
$$\Rightarrow robustness \downarrow$$

- In fact, no PPM approach is "collision-resistant" in the sense that ambiguous representation of the same edge increases the rate of false positives during the reconstruction procedure.

Vadim Kuznetsov, Andrei Simkin, and Helena Sandstrom. "An evaluation of different ip traceback approaches". In Proc. 4th International Conference on Information and Communications Security, December 9-12, 2002.

GOSSIB(Group Of Strongly SImilar Birthdays)

Partial-*birthday attack*

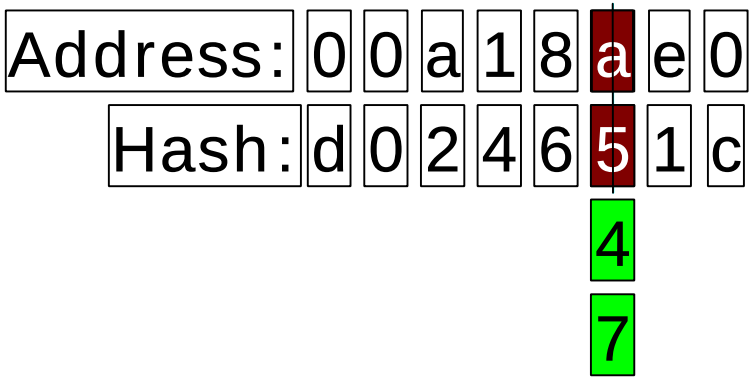
Single-chunk replacement allowed

as long as hash still matches

Result

8 fragments for single (true) edge

9 fragments for **two fake** edges(more efficient)



(Address, verifier) pair similarity.

Address	Verifier
0x00a18**4**e0	0xd0246**7**1c
0x00a18**a**e0	0xd0246**5**1c

Messages sent out.

Format: (distance, offset i, address$_i$, verifier$_i$)

$(x, 7, 0, \mathrm{d})$
$(x, 6, 0, 0)$
$(x, 5, \mathrm{a}, 2)$
$(x, 4, 1, 4)$
$(x, 3, 8, 6)$
$\mathbf{(}x\mathbf{, 2, 4, 7)}$ $\mathbf{(}x\mathbf{, 2, a, 5)}$
$(x, 1, \mathrm{e}, 1)$
$(x, 0, 0, \mathrm{c})$

(robustness)

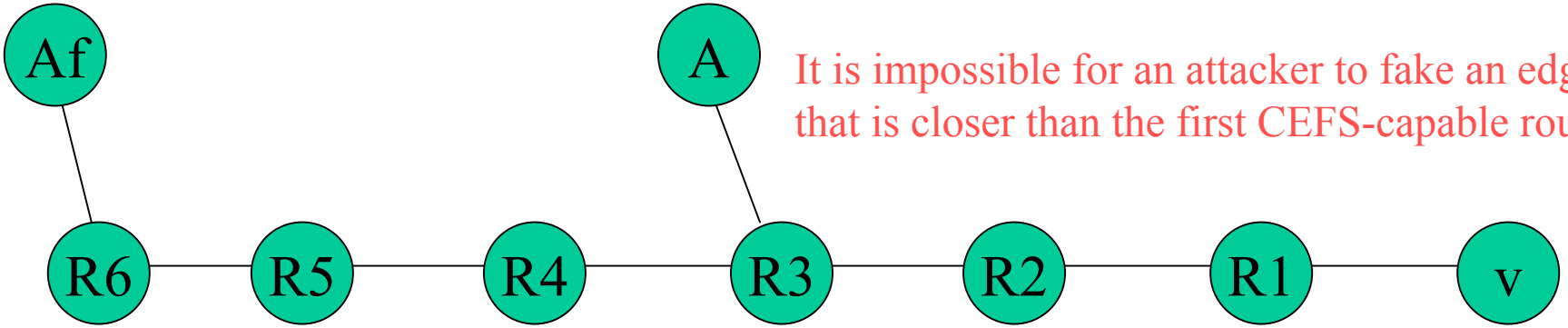
M. Waldvogel, "GOSSIB vs. IP Traceback Rumors," 18th Annual Computer Security Applications Conf. (ACSAC 2002), pp. 5-13, Las Vegas, Nevada, USA, December 2002.

Future Research
Improving PPM Robustness

- As attackers at distance d have the distance field of any packet incremented by d, only $t=2^{11}(31-d)$ distinct IP IDs may arrive at the destination.
  At a marking rate of p, an attacker needs to send out only $t/(1-p)^d$ packets to get t packets through to the victim.

M. Waldvogel, "GOSSIB vs. IP Traceback Rumors," 18th Annual Computer Security Applications Conf. (ACSAC 2002), pp. 5-13, Las Vegas, Nevada, USA, December 2002.

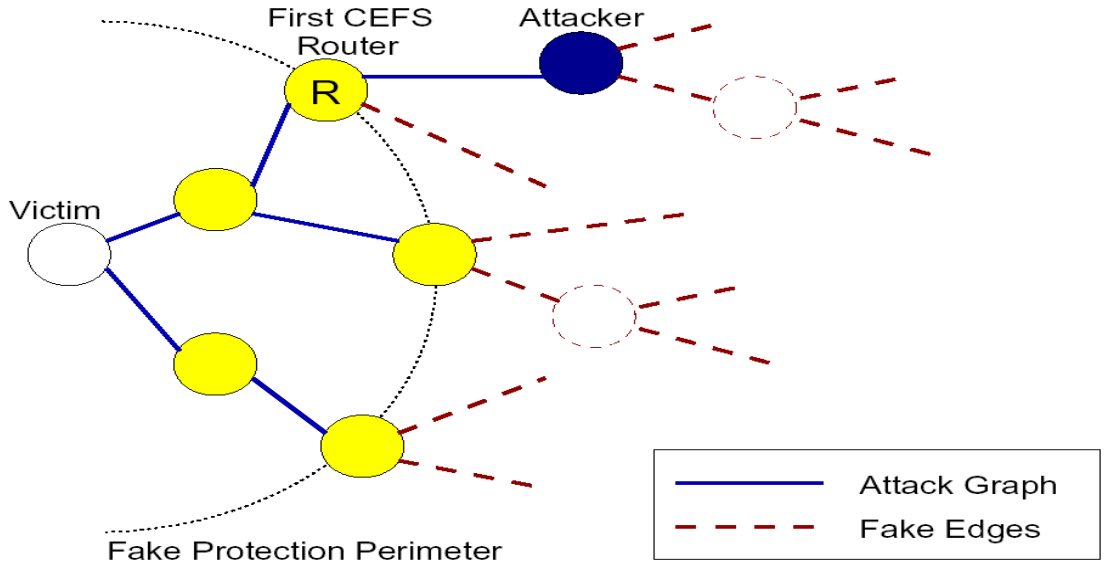
Effect of Spoofing the Marking Field



It is impossible for an attacker to fake an edge that is closer than the first CEFS-capable router *R*.

(Fake sub-path:R4 to R6 , true path: R1 to R3).

A: Real Attacker
Af: Spoofed Attacker
R1-R6: Routers
V: Victim



www.ee.mu.oz.au/pgrad/taop/conversiontalk.ppt
(Control High-bandwidth Traffic Aggregate)

M. Waldvogel, "GOSSIB vs. IP Traceback Rumors," 18th Annual Computer Security Applications Conf. (ACSAC 2002), pp. 5-13, Las Vegas, Nevada, USA, December 2002.

Future Research
Improving PPM Robustness

- Song et al. uses the hash function to produce authenticated marking (HMAC), but this scheme is infeasible in that it assumes that a victim has a map of upstream routers to all attackers.

- Although PKI requirement prevents attackers from generating false traceback messages, but it is unlikely that every routers will implement certificate-based scheme. (overhead and delay)

- Consequently, some researches regarding this unsolved problem will be conducted in the future.

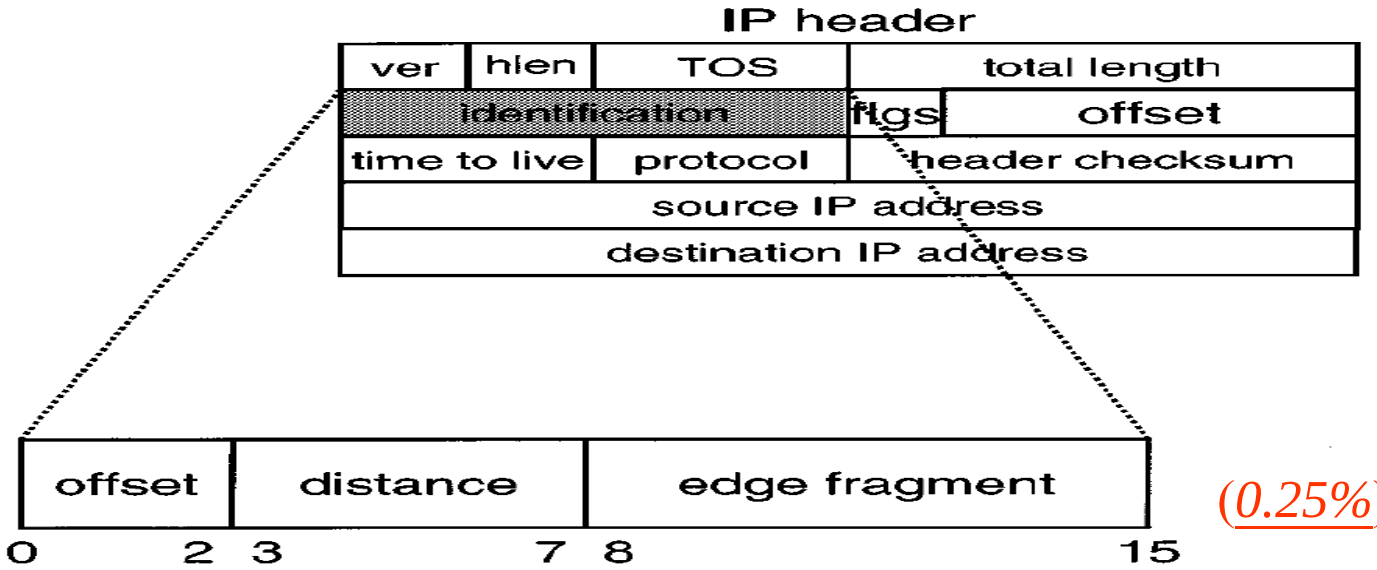
Vadim Kuznetsov, Andrei Simkin, and Helena Sandstrom. "An evaluation of different ip traceback approaches". In Proc. 4th International Conference on Information and Communications Security, December 9-12, 2002.

Future Research
Improving PPM Computation overhead

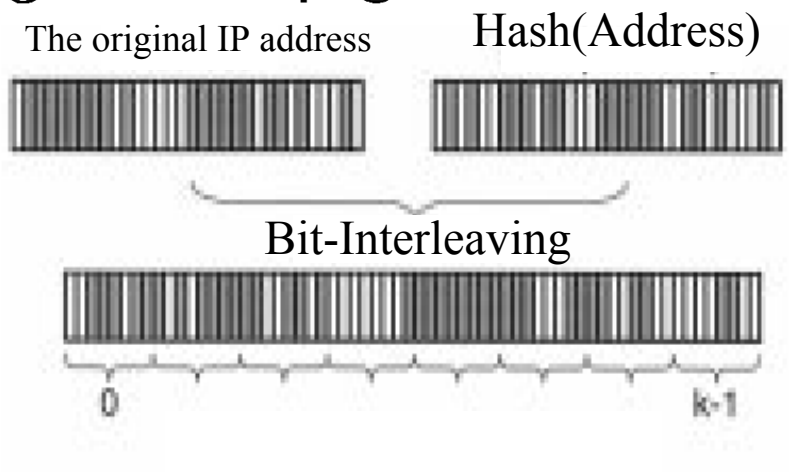
- The estimated time, required for processing collected information to be able to reconstruct the path back to the attackers, is desirable to be minimized for *achieving a fast response to an attack, and diminishing the damage*.

- PPM suffers from enormous computation overhead in case of a large scale DDoS. The path reconstruction of all attacking sources can take hours or days.

PPM – CEFS



(*0.25%*)



Send *k* fragments into network.

S. Savage, D. Wetherall, A. R. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," SIGCOMM, 295-306, 2000

PPM – Reconstruction at the victim

Select all fragments with *distance=0*

Pick any set of 8 fragments with distinct fragment ID

Verify reconstructed previous hop address with hash

Add to list of routers at distance=0, if match

Repeat until all combinations checked

For all i ∈ [1..max], select fragments with distance=i

Pick any set of 8 fragments with distinct fragment ID

Try for all prev ∈ (set of routers at *distance = i* – 1)

next = curr.address ⊕ prev

Add to list of routers at distance = i and to graph,

if hash(next) ⊕ hash(prev) = curr.hash

Repeat until all combinations checked

E.g.

M. Waldvogel, "GOSSIB vs. IP Traceback Rumors," 18th Annual Computer Security Applications Conf. (ACSAC 2002), pp. 5-13, Las Vegas, Nevada, USA, December 2002.

Future Research
Improving PPM Computation overhead

- The large overhead is explained by the constraint to break the IP address of a router into *eight pieces* to fit each piece into the fragmentation field in the IP header.

  (level-by-level uninformed search without using any special knowledge about the problem domain) (brute force)

- The goal is to design a fast, correct, efficient search or classification (clustering) algorithm. (It may be based on some authentication scheme)

Vadim Kuznetsov, Andrei Simkin, and Helena Sandstrom. "An evaluation of different ip traceback approaches". In Proc. 4th International Conference on Information and Communications Security, December 9-12, 2002.

Future Research
Improving PPM Computation overhead

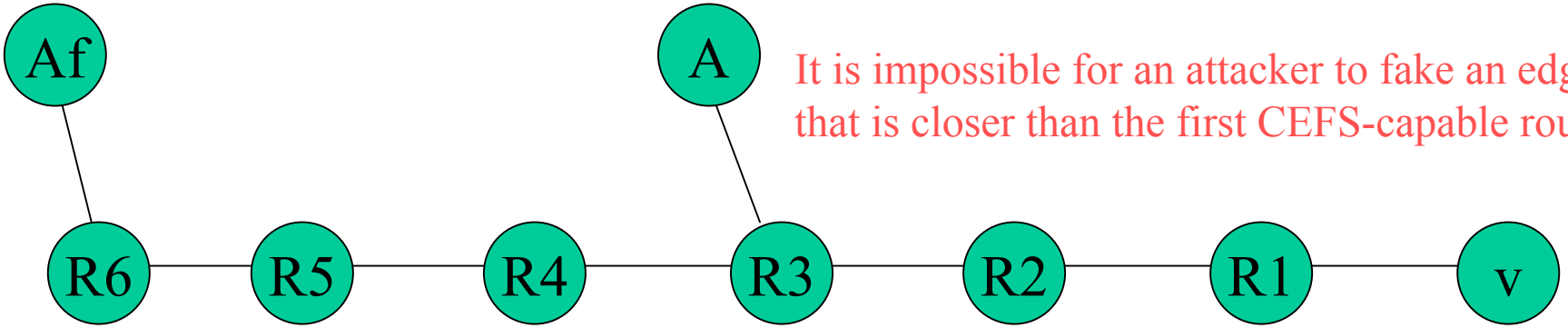
- The attacker may try to complicate the reconstruction time:

  Add any edge fragments to increase state space *(a alternative flooding attack)*

  Add fake edges to increase the work of reconstruction

M. Waldvogel, "GOSSIB vs. IP Traceback Rumors," 18th Annual Computer Security Applications Conf. (ACSAC 2002), pp. 5-13, Las Vegas, Nevada, USA, December 2002.

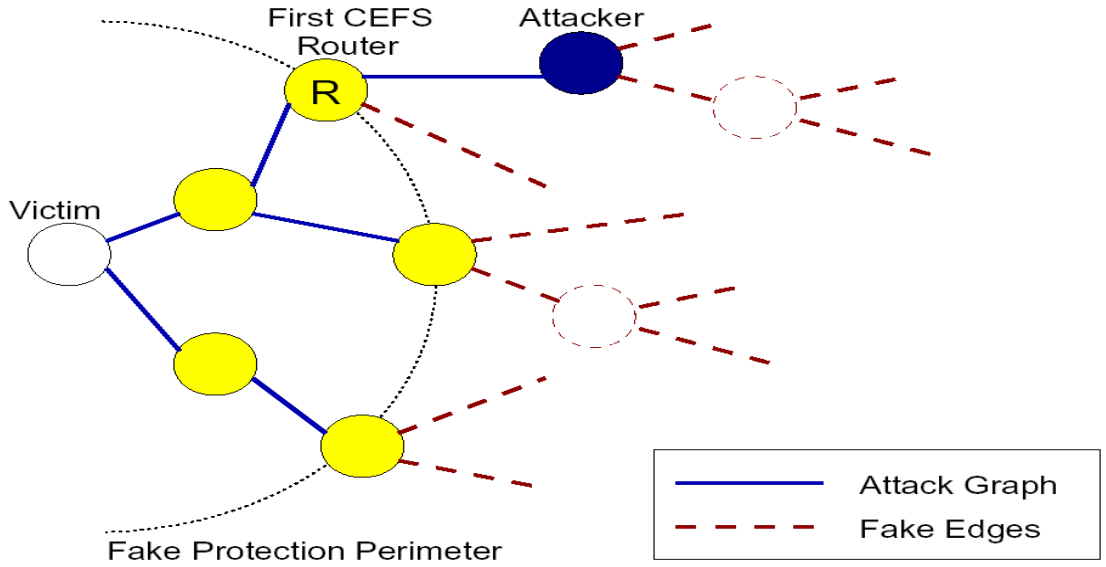
Effect of Spoofing the Marking Field



It is impossible for an attacker to fake an edge that is closer than the first CEFS-capable router *R*.

(Fake sub-path:R4 to R6 , true path: R1 to R3).

A: Real Attacker
Af: Spoofed Attacker
R1-R6: Routers
V: Victim



www.ee.mu.oz.au/pgrad/taop/conversiontalk.ppt
(Control High-bandwidth Traffic Aggregate)

M. Waldvogel, "GOSSIB vs. IP Traceback Rumors," 18th Annual Computer Security Applications Conf. (ACSAC 2002), pp. 5-13, Las Vegas, Nevada, USA, December 2002.

Future Research
Improving PPM Computation overhead

- As attackers at distance d have the distance field of any packet incremented by d, only $t=2^{11}(31-d)$ distinct IP IDs may arrive at the destination.
  At a marking rate of p, an attacker needs to send out only $t/(1-p)^d$ packets to get t packets through to the victim.

M. Waldvogel, "GOSSIB vs. IP Traceback Rumors," 18th Annual Computer Security Applications Conf. (ACSAC 2002), pp. 5-13, Las Vegas, Nevada, USA, December 2002.

GOSSIB(Group Of Strongly SImilar Birthdays)

Partial-*birthday attack*

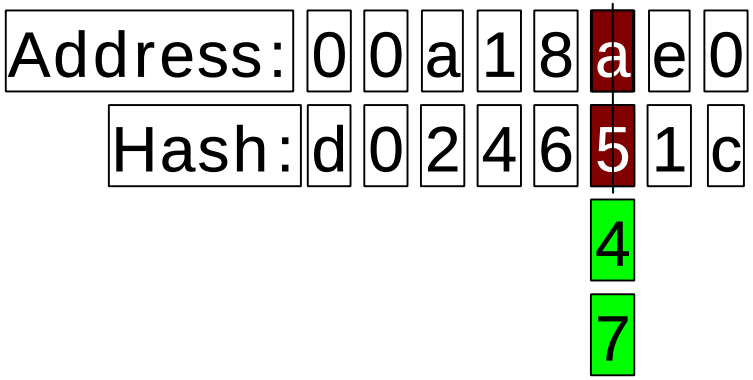
Single-chunk replacement allowed

as long as hash still matches

Result

8 fragments for single (true) edge

9 fragments for **two fake** edges(more efficient)



(Address, verifier) pair similarity.

Address	Verifier
0x00a18**4**e0	0xd0246**7**1c
0x00a18**a**e0	0xd0246**5**1c

Messages sent out.

Format: (distance, offset i, address$_i$, verifier$_i$)

$(x, 7, 0, \mathrm{d})$
$(x, 6, 0, 0)$
$(x, 5, \mathrm{a}, 2)$
$(x, 4, 1, 4)$
$(x, 3, 8, 6)$
$\mathbf{(}x\mathbf{, 2, 4, 7)}$ $\mathbf{(}x\mathbf{, 2, a, 5)}$
$(x, 1, \mathrm{e}, 1)$
$(x, 0, 0, \mathrm{c})$

(robustness)

M. Waldvogel, "GOSSIB vs. IP Traceback Rumors," 18th Annual Computer Security Applications Conf. (ACSAC 2002), pp. 5-13, Las Vegas, Nevada, USA, December 2002.

- Moore *et al.* shows that

  (1)There are an average of at least 4,000 denial-ofservice attacks/week

  (2)50% of attacks have an intensity of at least 1,000 packets/second

  (3)Most attacks last at least 10 minutes, 10% last more than an hour, and 2% last at least 5 hours (some even last days).

Moore, D. Voelker, G. and Savage, S., "Inferring Internet Denial of Service Activity," in Proc. USENIX Security Symposium, Washington D.C., August 2001

ICMP Traceback – ICMP Message Definition

Backward link -- information on the previous hop (in "forward order")

(1)the interface name of the generator
(2) the source and destination IP addresses of the two routers
(3)link-level association string

Forward link -- information on the next hop

Timestamp -- in NTP(Network Time Protocol) format

Traced packet -- as much of the traced packet as will fit.

IP Traceback – Relative Works

iCaddie: problem-1

- If there is not too much attack traffic going through an upstream router, e.g. DDoS attacks, or a upstream router can't picked up any attack packet with probability 1/20000 to generate a useful ICMP message, then the farther away from the victim are intermediate routers, the lesser useful ICMP messages do they generate to help the victim reconstruct the attack path *just according to the counter without the distinguishable capability*, such as utilizing the destination IP address.

IP Traceback – Relative Works

iCaddie: problem-2

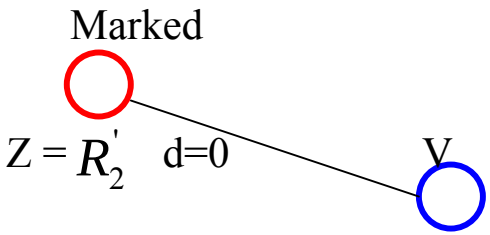
- If the attackers knew this scheme, it is easy to allow the attacker to bypass the scheme.

  If *before every normal attack packet an attacker periodically generates a faked Caddie message* with a TTL value equal to the path length between it and the victim such that faked messages will never arrive at the victim.

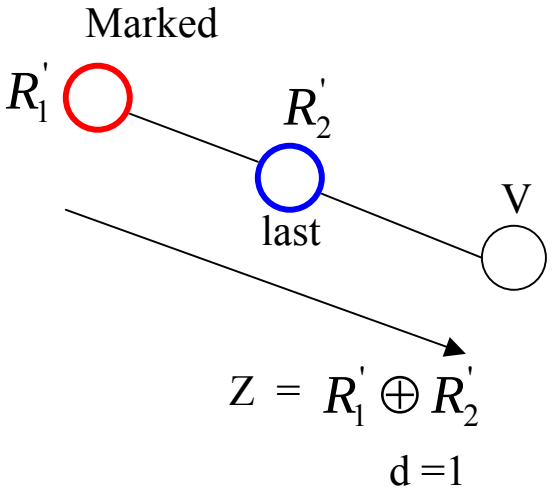
  However, when *an intermediate router resets it's counter because of the received faked path message*, it will stop the intermediate router to create any path message.

PPM -- Reconstruction at the victim

CEFS :




```
if d = 0 then
   if Hash(EvenBits(z))=OddBits(z) then
      insert edge (EvenBits(z),v,0) into G
      last := z
```




```
else
   z : =z ⊕ last
   if Hash(EvenBits(z))=OddBits(z) then
      insert edge (EvenBits(z), EvenBits(last),d) into G
      last := z
```

PPM -- Improving Convergent Amount

Proposed PPM-NPC : Proof

➢Prove $E_i \geqq (1 - i \cdot p)$.

When $i = 1$, $E_1 = 1 - p$. When $i = 2$, $E_2 \geqq (1 - p)(1 - p) - p^2 = 1 - 2p$. Assume that $E_n \geqq (1 - n \cdot p)$ is true, while $i = n$.

$$E_{n+1} = \left[E_n \cdot (1 - p) - \left(\sum_{j=1}^{n} p_{j,n+1} \right) \cdot p \right] \geq E_n \cdot (1 - p) - n \cdot p^2 \geq$$

$$(1 - np)(1 - p) - np^2 = 1 - (n + 1)p$$

PPM -- Improving Convergent Amount

Proposed CPPM : Properties

- $C_i = (i\text{-}1)\, p^2$

  $C_{i+d,i} = p^2$ has been proven to be true for all $i \geqq 1$ and $d \geqq 1$.

$$C_i = \sum_{j=1}^{i-1} C_{i,j} = (i-1)p^2$$

- $p_{i+d,i} = p$

  The general form of $p_{i+d,i}$ can be displayed as follows:

$$p_{i+d,i} = p \cdot (1-p)^{d-1} + \sum_{j=1}^{d-1} C_{i+j,i} (1-p)^{d-j-1}$$

This equation has also been proven to be true for all $i \geqq 1$ and $d \geqq 1$.

PPM -- Improving Convergent Amount

Proposed CPPM : Properties

- $E_i = 1 - i \cdot p$

  The general form of E_i is as follows:

$$E_i = E_{i-1}(1-p) - C_i = 1 - i \cdot p$$

When $i = 1$, $E_1 = 1 - p$ is true. Moreover, when $i = 2$,
$E_2 = E_1 \cdot (1-p) - C_2 = (1-p) \cdot (1-p) - p^2 = 1 - 2p$ is true.
Assume that $i=n$, $E_n = 1 - np$ is true. When $i=n+1$,

$$E_{n+1} = E_n(1-p) - C_{n+1} = (1-np)(1-p) - np^2 = 1 - (n+1)p$$

is true also. Consequently, $E_i = 1 - i \cdot p$ is true for all $i \geqq 1$.

IP Traceback – Relative Works

ICMP Traceback (iTrace) : *Format*

Tag	Element Name
0x01	Backward Link
0x02	Forward Link
0x03	Interface Name
0x04	IPv4 Address Pair
0x05	IPv6 Address Pair
0x06	MAC Address Pair
0x07	***Operator-Defined Link Identifier***
0x08	Timestamp
0x09	Traced Packet Contents
0x0A	***Probability***
0x0B	RouterId
0x0C	HMAC Authentication Data
0x0D	Key Disclosure List
0x0E	Key Disclosure
0x0F	Public-Key Information

draft-ietf-itrace-01.txt

PPM – Improving Incomplete Deployment

Proposed RPPM-NPC* : *The Feasibility of Compensation

- Two important conditions must be discussed for the sake of ensuring that E_j will be large enough for the RPPM-NPC-capable router R_j, while the marking probability $p \leqq 1/j$.

- Assume that there are d routers along the attack path before the RPPM-NPC-capable router R_j, such that there are x RPPM-NPC-capable routers, y discontinuous individual transparent routers, and z segments of consecutive two or more transparent routers.

PPM – Improving Incomplete Deployment

Proposed RPPM-NPC : The Feasibility of Compensation

Condition (1): None of z segments is adjacent to R_j.

Because R_j is the j-th router, we can get $j-1 \geq x+y+2\cdot z$

$$E_j = 1-\sum_{i=1}^{j-1}\left(p_{ij}\right) \geq 1-\left(x\cdot p+\frac{p}{2}\cdot z\right)$$

where $p_{i,j}$ is the probability that a packet is marked by a RPPM-NPC-capable router R_i, and this marked packet will arrive at the successive router R_j, where j is greater than i.

PPM – Improving Incomplete Deployment

Proposed RPPM-NPC : The Feasibility of Compensation

$$E_{j+1} = E_j - (1 - E_j) \cdot p = E_j(1 + p) - p > E_j - p$$

$$\geq 1 - \left(x + \frac{z}{2} + 1 \right) p$$

Here, the $(1–E_j)\cdot p$ is the probability that a compensation will be performed for the non-preemptive scheme.

Because $j \geqq (x+y+2\cdot z+1) \geqq (x+z/2+1)$, so that

$$E_{j+1} \geq 1 - j \cdot p \geq 0$$

while $p \leqq 1/j$.

PPM – Improving Incomplete Deployment

Proposed RPPM-NPC : The Feasibility of Compensation

Condition (2): One segment of consecutive double transparent routers is adjacent to R_j.

$$E_j = 1 - \sum_{i=1}^{j-1}(p_{ij}) \geq 1 - \left(x \cdot p + \frac{p}{2}(z-1)\right)$$

$$E_{j+1} = E_j - (1 - E_j) \cdot p - \frac{p}{2} = E_j(1+p) - \frac{3}{2}p$$

$$\geq E_j - \frac{3}{2} \cdot p \geq 1 - \left(x + \frac{(z-1)}{2} + \frac{3}{2}\right)p$$

Because $j \geqq (x+z/2+1)$, so that

$$E_{j+1} \geq 1 - \left(x + \frac{z}{2} + 1\right)p \geq 1 - j \cdot p \geq 0$$

while $p \leqq 1/j$.

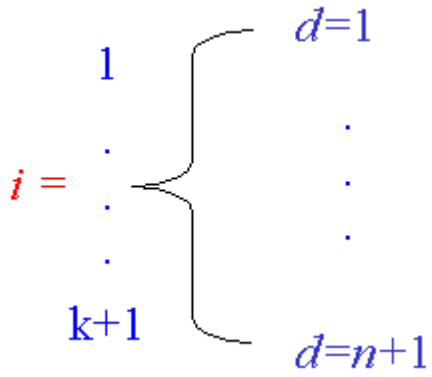
PPM -- Improving Convergent Amount

Proposed CPPM : Proof-1

- $C_{i+d,i} = p^2$

proof:

For $i = 1$, we prove $C_{1+d,1} = p^2$ is true.



When $d=1$, $C_{2,1} = p \cdot p = p^2$.

When $d=2$, $C_{3,1} = p \cdot (1-p) \cdot p + C_{2,1} \cdot p = p^2$.

In general form for $d=n$,

$$C_{1+n,1} = p \cdot (1-p)^{n-1} \cdot p + \sum_{j=1}^{n-1} C_{1+j,1} (1-p)^{n-j-1} \cdot p$$

The first term in this equation is the probability that a packet marked by R_1 and is passed by $R_2 \ldots R_n$, then is remarked at R_{n+1}. The second term represents the summed probability that a packet is marked in R_1, remarked and compensated in R_{j+1}, then passed by $R_{j+2} \ldots R_n$, and remarked in R_{n+1}, where j is a value from 1 to n-1.

PPM -- Improving Convergent Amount

Proposed CPPM : Proof-2

Assume that $C_{1+n,1} = p^2$ is true. When $d=n+1$,

$$C_{2+n,1} = p\cdot(1-p)^n \cdot p + \left[\sum_{j=1}^{n-1} C_{1+j,1}(1-p)^{n-j}\cdot p + C_{1+n,1}\cdot p\right]$$

$$= (1-p)\cdot C_{1+n,1} + p^2 \cdot p = p^2$$

is true also. Thus, $C_{1+d,1} = p^2$ is true for all $d \geqq 1$ and $i=1$.

PPM -- Improving Convergent Amount

Proposed CPPM : Proof-3

Assume that $C_{k+d,k} = p^2$ is true for all $d \geq 1$, and $i=k$.

When $i=k+1$ and $d=1$, $C_{k+1+1,k+1} = p \cdot p$ is true.

Assume that $C_{k+1+n,k+1} = p^2$ is true for $i=k+1$ and $d=n$,

$$C_{k+1+n,k+1} = p \cdot (1-p)^{n-1} \cdot p + \sum_{j=1}^{n-1} C_{k+1+j,k+1} (1-p)^{n-j-1} \cdot p$$

PPM -- Improving Convergent Amount

Proposed CPPM : Proof-4

When $d=n+1$,

$$C_{k+1+n+1,k+1} = p\cdot(1-p)^n\cdot p + \sum_{j=1}^{n} C_{k+1+j,k+1}(1-p)^{n-j}\cdot p$$

$$= (1-p)C_{k+1+n,k+1} + C_{k+1+n,k+1}\cdot p = p^2$$

Now $C_{i+d,i} = p^2$ is proven to be true for all $i \geqq 1$ and $d \geqq 1$.

IP Traceback – Relative Works

ICMP Traceback (iTrace) : *Authentication*

- The ideal form of authentication would be a digital signature or HMAC. (The basic problem: PKI infrastructure for all routers)

- link-level association string: (A simple method)

  It is a black box that is only known to and used by both adjacent routers to tie together ICMP traceback messages emitted by them.

  E.g. On LANs, it is constructed by concatenating the source and destination MAC addresses of the pair of machines.

  If there are no such addresses (say, for a point-to-point link), a suitable string must be provisioned in both routers, to be used as the Operator-Defined Link Identifier.

draft-bellovin-itrace-00.txt

IP Traceback – Relative Works

ICMP Traceback (iTrace) : *Authentication*

➢ ***Recipients should use the TTL field differences in conjunction with the link fields to verify the chain.***

- The initial TTL field must be set to 255.

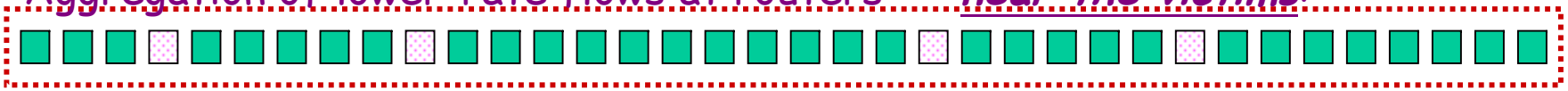
  If the Traceback packet follows the same path as the data packets, this provides an unambiguous indication of the distance from this router to the destination.

- By comparing the distances, a chain can be constructed and partially verified even without examining the authentication fields.

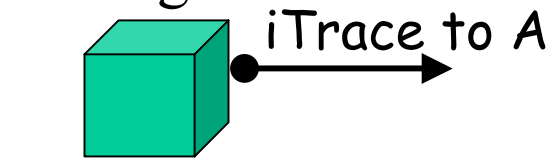
A high-rate attack flow from the attack source:

A low-rate attack flow from the attack source:

Aggregation of lower-rate flows at routers ***near the victims***:



- Assuming destination A is under attack:



S2A:	**100%**
S2B:	0%
S2C:	0%
S2D:	0%

Ideal traffic distribution

S2A:	**25%**
S2B:	25%
S2C:	25%
S2D:	25%

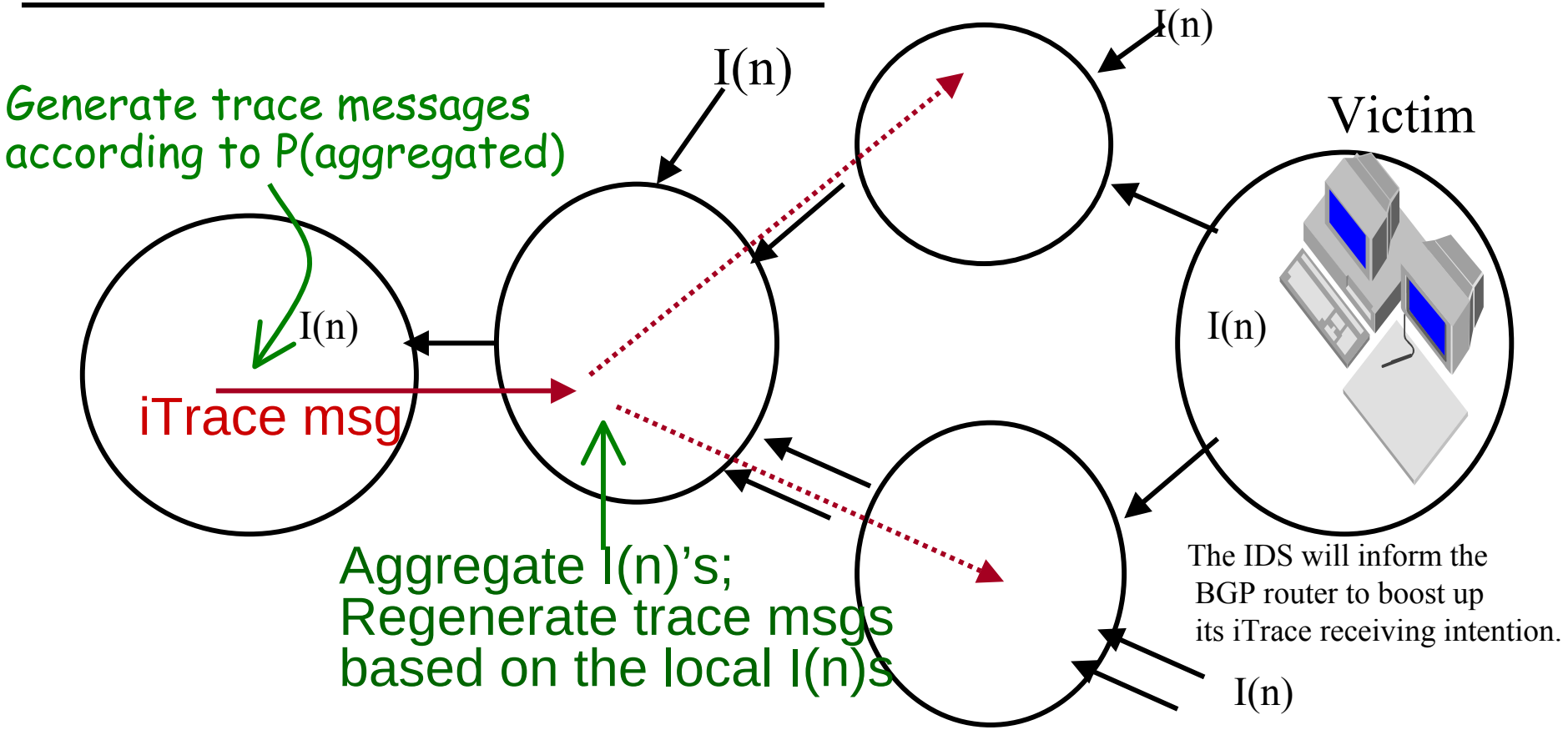
Actual traffic distribution

B,C, and D receive statistically the same amount of iTrace messages even if they are not under attack

IP Traceback – Relative Works

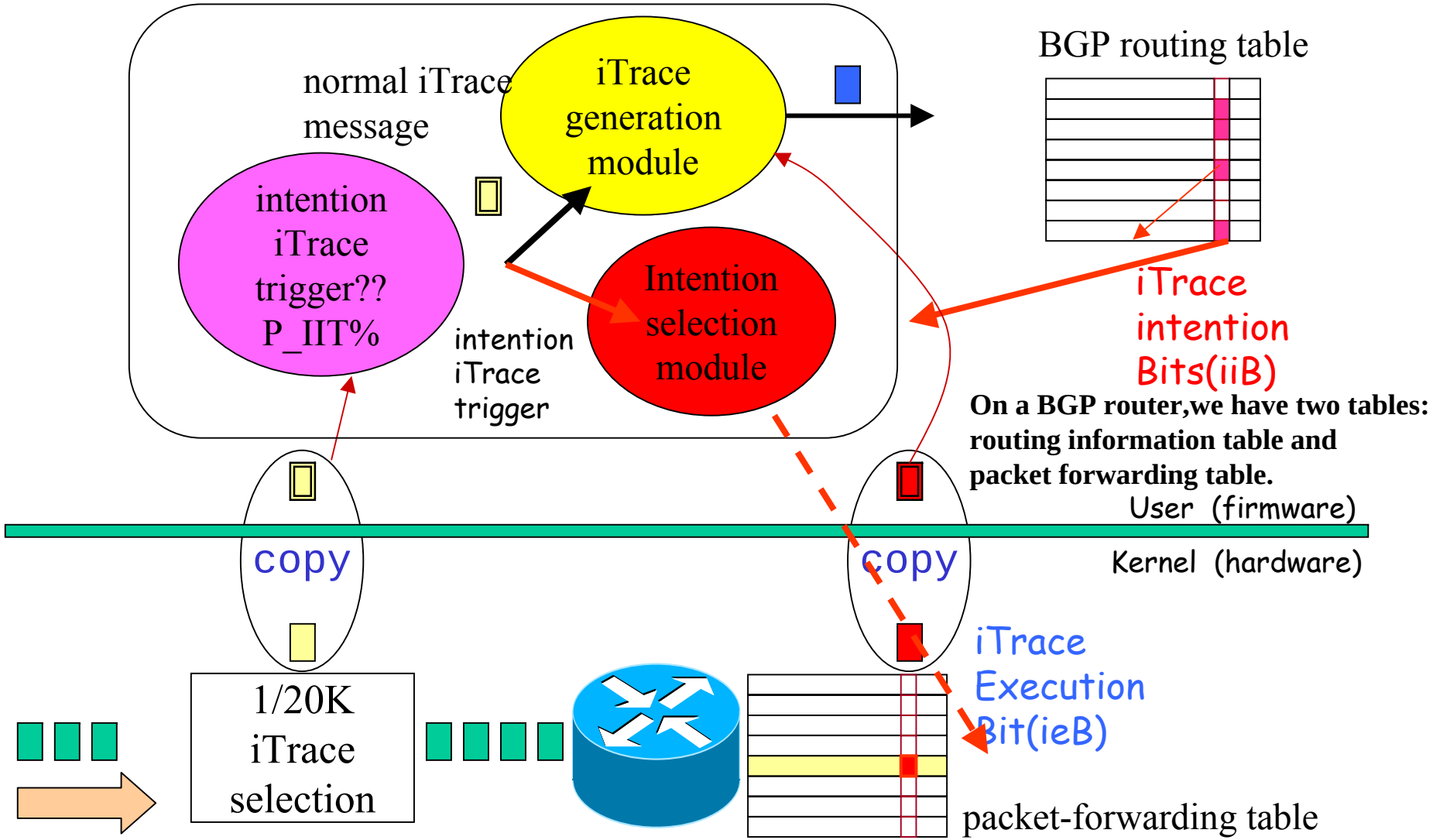
Intention–Driven ICMP Traceback

To distribute Intention



IP Traceback – Relative Works

Intention–Driven ICMP Traceback : *Architecture*



(draft-wu-itrace-intention-01.txt)

IP Traceback – Relative Works

Intention–Driven ICMP Traceback **:** ***Architecture***

- Every time, when a packet is selected, through the standard iTrace scheme (1/20,000 probability), ***another random coin will be flipped***, ***controlled by P_IIT***, to determine whether this iTrace message should be sent "as it is" or we should invoke the "intention" iTrace mechanism.

- For example, if P_IIT is 0.5, then 50% used to handle the "original“ iTrace scheme, while the rest will be used for only those who really want to receive iTrace messages.
  1/20,000 ➔ 1/40,000

IP Traceback – Relative Works

PICA & Caddie

- PICA uses a path message cache indexed by the destination IP address of the path message to implement downstream path messages suppression.

  Before a router generates a path message, it checks its path message cache first, *the path message is generated and sent out if and only if the path message cache does not contain any message* dispatched to the same destination host.
  If a path message cannot be created and sent out successfully because it hits the path message cache, the hit entry is deleted. (given a second chance)

F.H. Hsu and T.C. Chiueh, "A path information cashing and aggregation approach to traffic source identification," Proc. 23rd IEEE Intl. Conf. Distributed Computing Systems (ICDCS), May 2003.

- *In order to reduce the number of redundant Caddie messages*,
  Each input port of a router maintains a simple Caddie timer/counter, which indicates how long this port has not received any Caddie message, regardless of its source or destination. If the amount exceeds a specified threshold, the router will start to act as a Caddie initiator.

  A router should not generate any Caddie message unless it has not received any Caddie message from its upstream routers for a certain amount of time. (problem)

B.T. Wang and H. Schulzrinne, "A denial-of-service-resistant IP traceback approach," 3rd New York Metro Area Networking Workshop (NYMAN), Polytechnic University, Sept. 2003. [Online]. Available: http://www.nyman-workshop.org/2003/papers/ A Denial-of-Service-Resistant IP Traceback Approach_paper.pdf

PPM -- Improving Convergent Amount

Proposed CPPM : Properties

For $i=1$, $p_{1+d,1} = p \cdot (1-p)^{d-1} + \sum_{j=1}^{d-1} C_{1+j,1}(1-p)^{d-j-1}$

When $d=1$, $p_{2,1} = p$. When $d=2$, $p_{3,1} = p(1-p) + C_{2,1} = p$.
Assume that $d=n$ is true for $i=1$,

$$P_{1+n,1} = p \cdot (1-p)^{n-1} + \sum_{j=1}^{n-1} C_{1+j,1}(1-p)^{n-j-1} = p$$

When $d=n+1$,

$$P_{1+n+1,1} = p \cdot (1-p)^{n} + \left[\sum_{j=1}^{n-1} C_{1+j,1}(1-p)^{n-j} + C_{1+n,1} \right]$$

$$= (1-p)\, p_{1+n,1} + C_{1+n,1} = p$$

is true. Similar to property $C_{i+d,i} = p^2$, it is easy to prove that $p_{i+d,i} = p$ is true for all $i \geq 1$ and $d \geq 1$.

Hop Integrity Protocols

- A computer network is said to provide hop integrity iff when any router *p* in the network receives a message *m* supposedly from an adjacent router *q*, then *p* can check that *m* was indeed sent by *q*, was modified after it was sent, and was not a replay of an old message sent from *q* to *p*.

secret exchange protocol
weak integrity protocol
strong integrity protocol
(密碼學的角度)

M.G. Gouda, E.N. Elnozahy, C.T. Huang, and T.M. McGuire, "Hop Integrity in computer Networks," IEEE Trans. Networking, Vol.10, No.3, June 2002.

Detecting Spoofed Packets-1

- It's beneficial to know if network traffic has spoofed source addresses. This knowledge can be particularly useful as an adjunct *to reduce false positive from defense mechanisms*, e.g. IDS.
- Active Methods

  Active methods either make queries to determine the true source of the packet (reactive), or affect protocol specific commands for the sender to act upon (proactive).

  Active methods require a response from the claimed source. Only if the spoofed host is active (i.e. connected to the network and receiving and processing packets) can it be probed.

  A host that is heavy firewalled and cannot respond to probes is effectively inactive. Because *inactive hosts are commonly used as source addresses in spoofed packets*, if these packets are seen in an attack, it is likely they are spoofed. When hosts will not respond to any probes, passive methods will be required for corroboration.

S.J. Templeton and K.E. Levitt, "Detecting spoofed packets," Proc. 3rd IEEE DARPA Information Survivability Conference and Exposition (DISCEX), Washington, D.C., April 2003.

Detecting Spoofed Packets-1

- Active Methods: *Direct TTL probes*.

  By *sending a packet to the claimed host that will cause a reply* we can check to see if the TTL in the reply is the same as the packet being checked. *If they are of the same protocol, they generally have the same TTL*. Because different protocols use different initial TTLs, when the probe packet is of a different protocol, we must infer the actual hop count.

- Only a few initial TTL values are commonly used.

  For TCP/UDP, 64 and 128 are most commonly seen.
  ICMP commonly uses 128 and 255 as the initial value.

  By subtracting the observed TTL from the supposed initial value we can estimate the number of hops.

S.J. Templeton and K.E. Levitt, "Detecting spoofed packets," Proc. 3rd IEEE DARPA Information Survivability Conference and Exposition (DISCEX), Washington, D.C., April 2003.

Detecting Spoofed Packets-1

- For example, for an ICMP packet with an observed TTL of 241, we get 255-241 or 14 as the estimated number of hops.

- If we are checking a TCP packet with an observed TTL of 50, we get 128-50=78 and 64-50=14. Because 14 is the expected value, we can assume the packet was not spoofed.

S.J. Templeton and K.E. Levitt, "Detecting spoofed packets," Proc. 3rd IEEE DARPA Information Survivability Conference and Exposition (DISCEX), Washington, D.C., April 2003.

Detecting Spoofed Packets-1

- Passive Methods

  Passive methods involve observing packet data that would be anomalous in legitimate packets.

  As for observed data, they will have a *predictable value*, not relative to some prior packet, we can learn what values are to be expected and consider packets with unexpected values suspicious.

  Because TTL values are a function of a host's OS, the packet's protocol, and the network topology, all which are reasonably static, TTLs can be used as a basis for passive detection.

S.J. Templeton and K.E. Levitt, "Detecting spoofed packets," Proc. 3rd IEEE DARPA Information Survivability Conference and Exposition (DISCEX), Washington, D.C., April 2003.

Detecting Spoofed Packets-1

- Passive Methods: Passive TTL Methods.

TTL values are an indication of how many network hops exist between a packet's source and destination. By recording, over a period of time, the TTL values of distinct source IP address/protocols , we can learn which values are expected from particular hosts.

We believe that these are reliable, *predictable values of a given IP address/protocol*. This will give us a reasonable basis for identifying suspicious packets from previously observed hosts.

S.J. Templeton and K.E. Levitt, "Detecting spoofed packets," Proc. 3rd IEEE DARPA Information Survivability Conference and Exposition (DISCEX), Washington, D.C., April 2003.

How to distribute Intention?

- BGP Extension
  - For every BGP route update (advertises the reachability of some network address) , we include I(n) as a new community attribute:
    - 0x[iTrace-Intention]:0x[0-1]
  - These I(n) values will be forwarded or even aggregated by the routers *who understand this new community attribute*.
    - aggregation: I(new) = max {I(n)}
  - Rate-Limiting on Intention Update:
    - should not be more frequent than Keep-Alive messages.
    - should not trigger any major route computation.

How to distribute Intention?

- The BGP community string, an existing BGP attribute, is a 32 bit unsigned integer. We would like to use two of the available values,one for the positive intention to receive iTrace messages, and the other for negative. For instance, 0x78B0 for not wanting any iTrace,while 0x78B1 for the positive intention of iTrace. In other words,0x78B1 means 1 for iiB.

Advantages of using BGP

- Because of BGP route aggregation, our proposal will not increase the number of entries in the routing or forwarding tables.

- We believe that our design is practical as it doesn't require changes to all the routers. And, even for the new routers, the change is fairly small as we do not introduce a new BGP attribute, but two new values for an existing BGP attribute.

  (others traditional routers will still pass the intention bits around,)

- Since the rate of our updates can be limited by the BGP keepALive interval, our design will not introduce extra BGPa traffic, while the intention bit value can be distributed through the whole Internet. Currently, it will take a few seconds (up to maybe 10~15 seconds) for BGP to propagate to the whole Internet.

•A. Mankin, D. Massey, C.-L. Wu, S. F. Wu and L. Zhang,"On design and evaluation of `intention-driven' ICMP traceback",
in Proc. IEEE Int. Conf. Computer Communications and Networks , Oct. 2001, pp. 159-165.
•draft-wu-itrace-intention-01.txt

Disadvantages of using BGP

- The propagation of the “intention” value through BGP updates may be quite slow, delaying the invocation of the intention driven mechanism.

- It may cause instability in the routing mechanism due to frequent updates in the routing table.

Modified iTrace

- Significant overhead caused by necessity to implement the iTrace mechanism on ***every router***. (Disadvantages of iTrace)

- Requiring a modification in the mechanism itself in order to add such a desirable characteristics as "incremental deployment" and reduce the overhead by implementing the iTrace mechanism only an a small amount of the routers. (aiming at reducing the deployment overhead)

- K. Vadim *et al.* suggest to select packets with a relatively low probability from the queue in a router and if the selected packet is an iTrace message then mark it by adding some additional information to the body of the message.

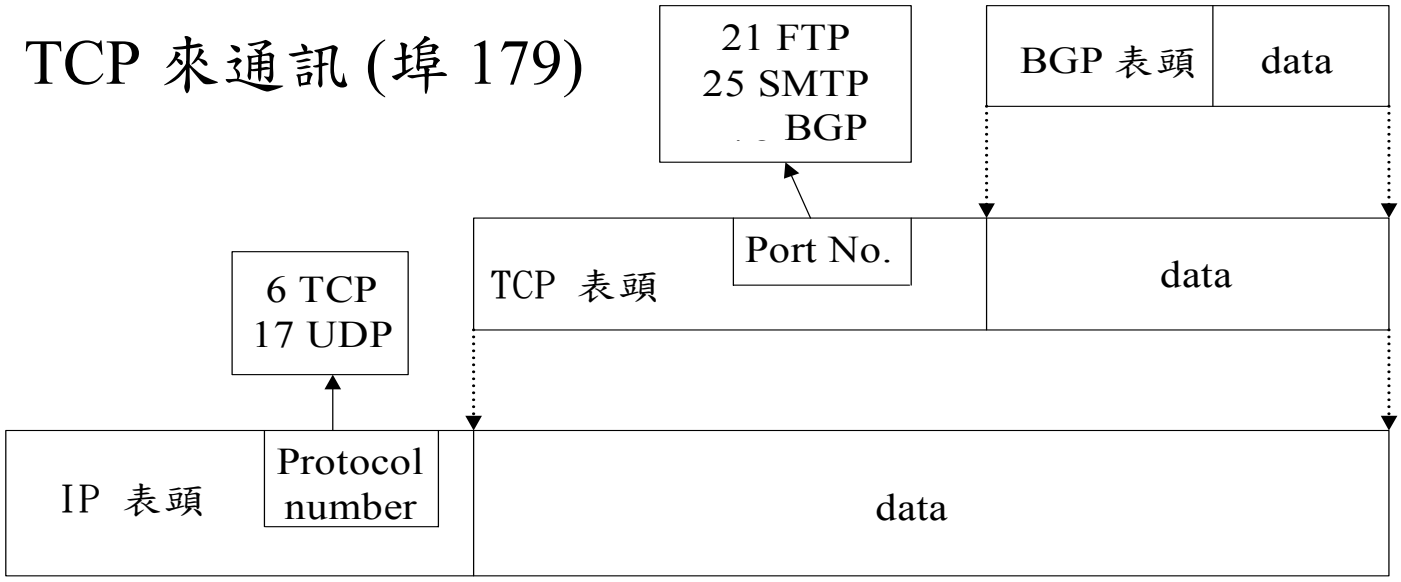
Modified iTrace

- The router that implements iTrace should not only generate iTrace messages but also examine the randomly chosen packets and, if the examined packet is an iTrace message from another router, add its own IP address to a special field of the iTrace message.

- The reconstruction procedure at the victim side will use this information to fill in the "gaps" between the routers which do not implement the iTrace mechanism.

  nodes ==> edges (chain)

- **外部閘道協定** (Exterior Gateway Protocol、EGP)
  - 在兩個自治系統間傳送繞路資訊的協定。
  - **Border Gateway Protocol** Version 4 (**BGP-4**)
    - 當一對自治系統同意交換繞路資訊時，雙方需標示為 BGP 路由器。
    - 這兩個路由器可稱為
      - **邊界閘道器** (border gateway)
      - 或**閘道路由器** (border router)
      - 或 **BGP 對等** (peer)
  - BGP 使用 TCP 來通訊 (埠 179)



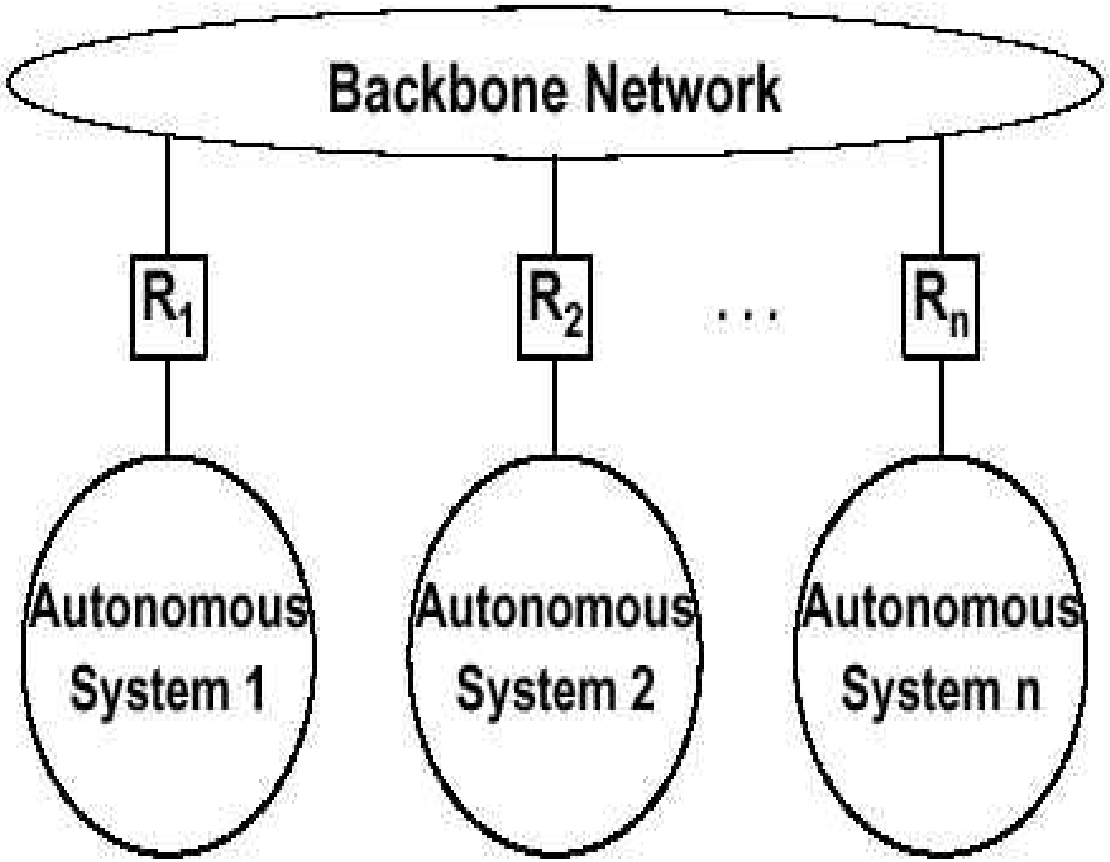


Figure 15.3 Architecture of an internet with autonomous systems at backbone sites. Each autonomous system consists of multiple networks and routers under a single administrative authority.

從接收端觀點的資訊

- R_2 執行 BGP
- R_2 必須報告到 Net 1 到 Net 4 的可達性：
  - 到 經

到	經
Net 1	R_1
Net 2	R_2
Net 3	R_3
Net 4	R_3

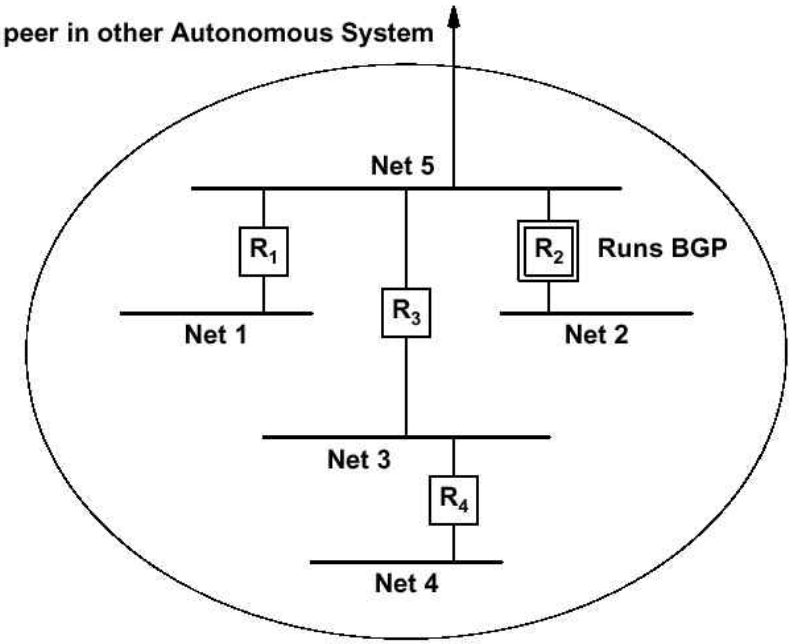


Figure 15.12 Example of an autonomous system. Router R_2 runs BGP and reports information from the outsider's perspective, not from its own routing table.

- 每一個自治系統必須向其它核心路由器傳播資訊。
- 每一個自治系統由中央管理機構指定一個自治系統號碼
- 每一個自治系統可以自由的選擇內部繞送架構和演算法。

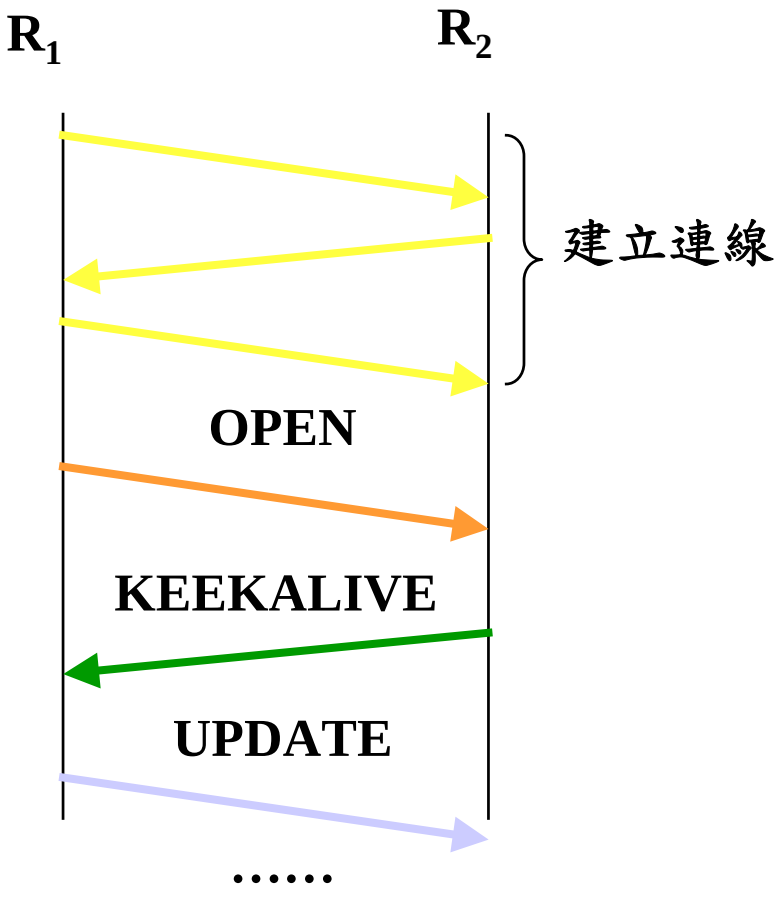
- 四個基本訊息型態

Type Code	Message Type	Description
1	OPEN	Initialize communication
2	UPDATE	Advertise or withdraw routes
3	NOTIFICATION	Response to an incorrect message
4	KEEPALIVE	Actively test peer connectivity

Figure 15.5 The four basic message types in BGP-4.

BGP 功能與訊息型態

- 運作
  - 建立一個 TCP 連線
  - 協商握手 (Negotiation Handshake)
    - ***OPEN*** 訊息
      - 宣告 AS 編號與其他的操作參數
    - ***KEEKALIVE*** 訊息
  - 傳送路由資訊
    - ***UPDATE*** 訊息
  - 錯誤通告
    - ***NOTIFICATION*** 訊息



- 兩個 BGP 對等建立一 TCP 連線後，雙方開始傳送 *OPEN* 訊息，開啟 BGP 連線，宣告其自治系統號碼，並建立其操作參數。

- 另一端對等若接收開啟 BGP 連線則回應一 *KEEPALIVE* 訊息，做為 OPEN 的確認。

- 另一端對等若拒絕開啟 BGP 連線則回應一 *NOTIFICATION* 訊息。

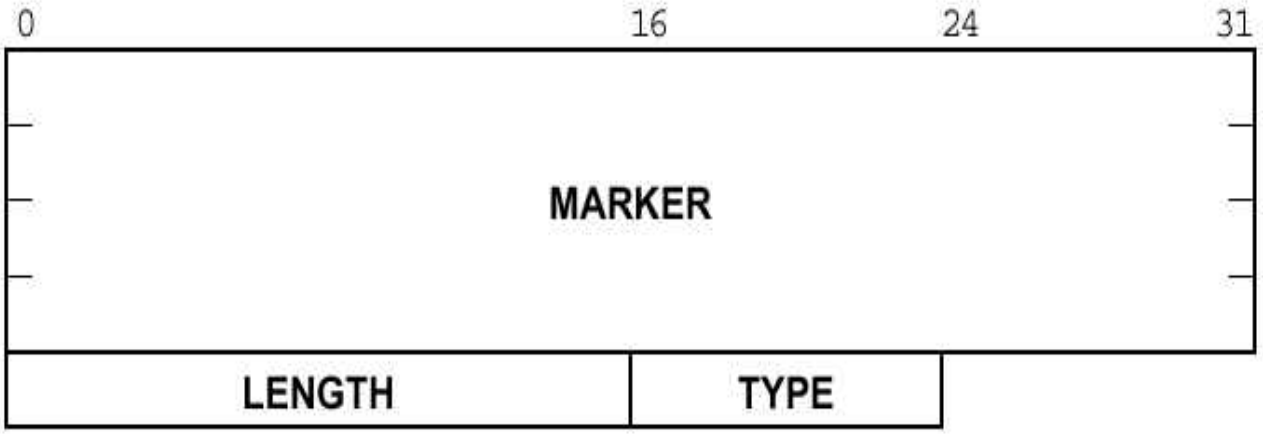


Figure 15.6 The format of the header that precedes every BGP message.

- 在每個 BGP 訊息之前的固定標頭
  - MARKER (標記)[16]
    - 雙方同意一個用來標記訊息開頭的值 (同步)。
  - LENGTH (長度)[2]
    - 訊息總長度
    - 最小值 = 19
      最大值 = 4096
  - TYPE (型態)[1]
    - 圖 15.5

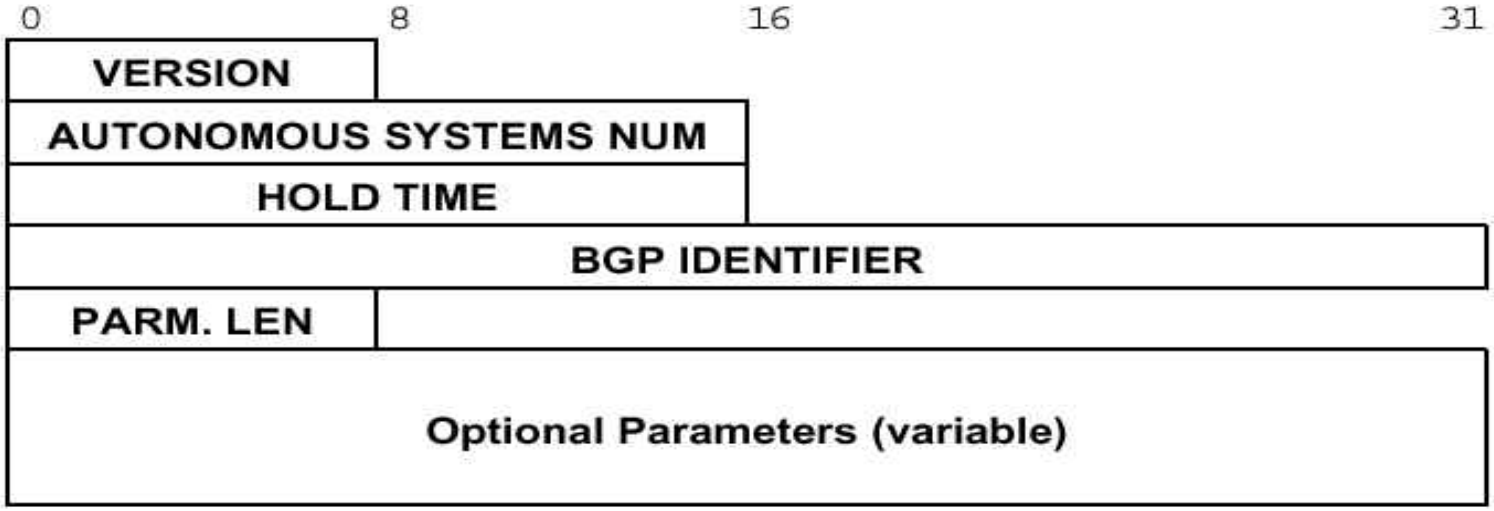
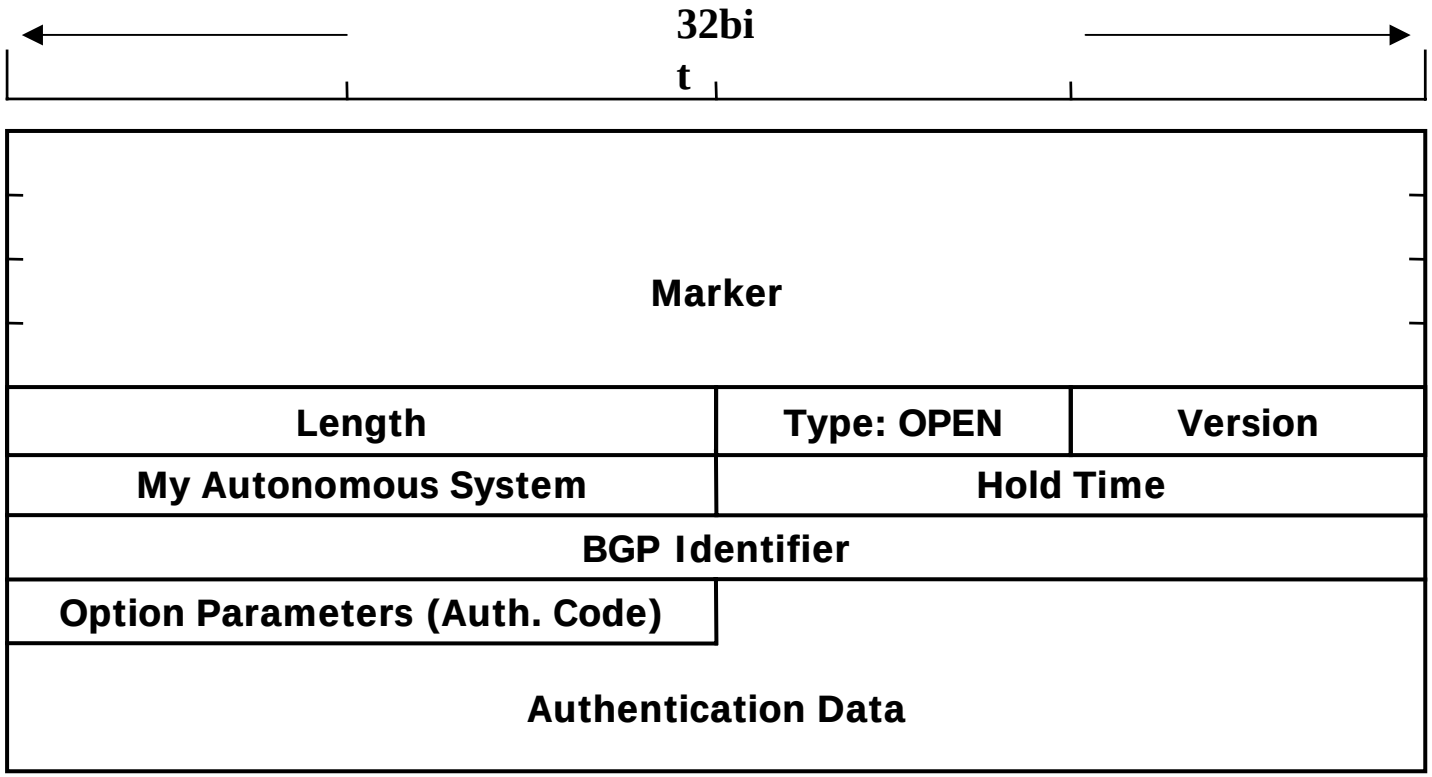


Figure 15.7 The format of the BGP OPEN message that is sent at startup. These octets follow the standard message header.

- Initial exchange

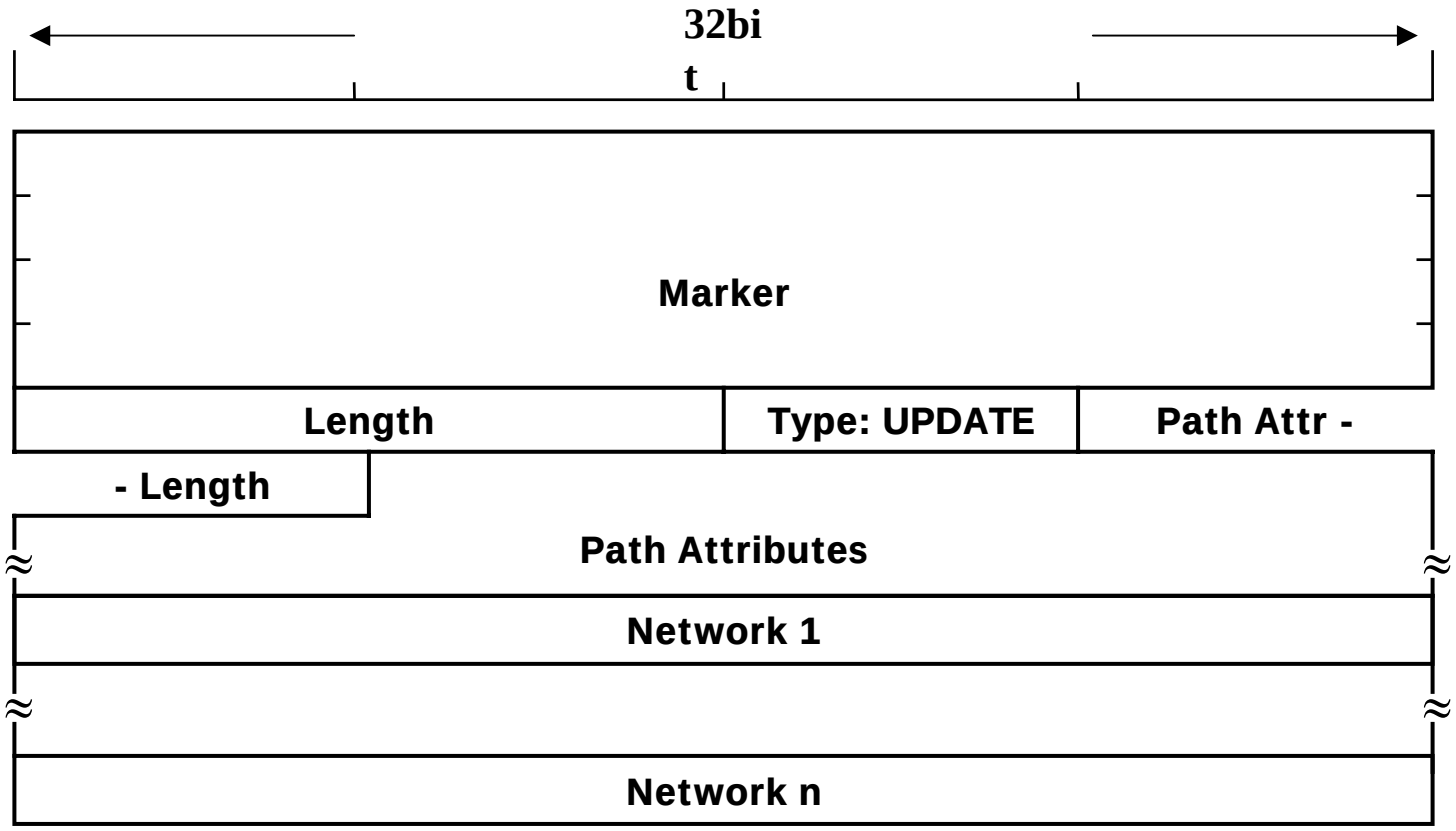


BGP UPDATE 訊息

- BGP 對等建立 TCP 連線、傳送 OPEN 訊息後，使用 UPDATE 訊息：
  - 告知 (advertise)目的地可抵達性
  - 或撤回 (withdraw)先前目的地可抵達性。
- 路由器只在路徑改變時，才傳送更新訊息。

BGP UPDATE 訊息

- Transfer routing information



BGP UPDATE 訊息

- 每個 UPDATE 訊息分為兩部份：
  (1) 第一部份列出要被取消的目的地
  (2) 第二部份列出要被告知的目的地
- WITHDRAWN LEN (取消長度)[2]
  – 取消目的地欄位的大小 (位元組)
- Withdrawn Destinations (取消目的地)

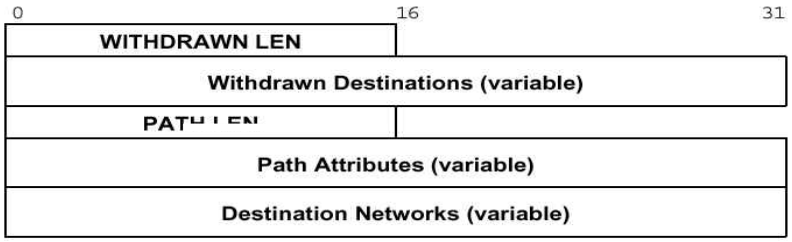


Figure 15.8 BGP UPDATE message format in which variable size areas of the message may be omitted. These octets follow the standard message header.

BGP UPDATE 訊息

- PATH LEN (路徑長度)[2]
  - 路徑屬性欄位的大小 (位元組)
- Path Attributes (路徑屬性)
- Destination Networks (路徑網路)

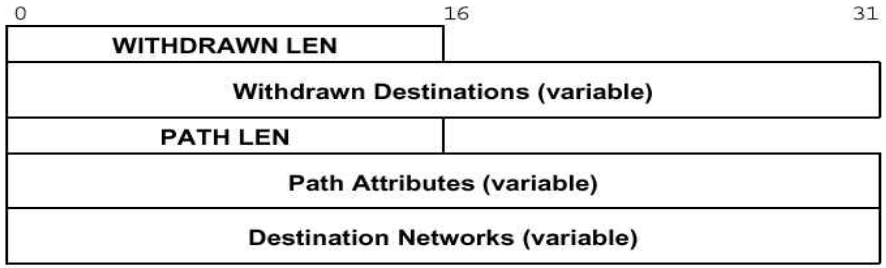


Figure 15.8 BGP UPDATE message format in which variable size areas of the message may be omitted. These octets follow the standard message header.

壓縮的遮罩-位址對

- *取消位址與目的位址*欄都包含一 IP 網路位址串列
- 為容納無類別 (Classless，例如 CIDR)，BGP 傳送 IP 位址時也必須傳送遮罩 (mask)
  - LEN (長度)[1]
    - 遮罩位元的長度 (例如 /25)
    - 0：預設路由
  - IP Address (IP 位址)[1~4]
    - 只包含被遮罩涵蓋的位元組
    - 例如 /23 傳 3 個位元組
    - 例如 /24 傳 3 個位元組
    - 例如 /25 傳 4 個位元組
    - …

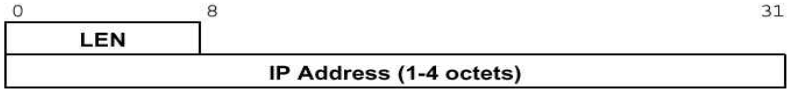


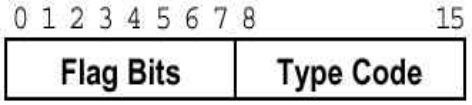
Figure 15.9 The compressed format BGP uses to store a destination address and the associated mask.

BGP 路徑屬性

- 額外資訊是包含在更新 (*UPDATE*) 訊息的路徑屬性 (*Path Attribute*) 欄位。 (Community Attribute)
  - 到目的地的下一跳躍點
  - 到目的地間路徑上的各個自治系統序列
  - 路徑資訊由其他自治系統學習而得或由發送端的自治系統學習而得。
- 路徑資訊很重要：
  - 接收端可以檢查繞路迴圈 (routing loop)。
  - 接收端實現政策限制 (policy constrains)。
  - 接收端知道來源的所有路由，可決定接受或拒絕所接收的訊息。
- 路徑屬性欄位包含三項：
  - (type, length, value)

BGP 路徑屬性

- 2-位元組 型態 (Type) 欄位
  - 旗標 (Flag) 位元
    OTPE0000
    - O (Optional、可有可無)
      - 1: 屬性是選擇性的
      - 0: 屬性是必要的
    - T (Transitive、可變的)
      - 1: 屬性是可變的
      - 0: 屬性是不可變的
    - P (Partial、部份的)
      - 1: 屬性是部份資訊
      - 0: 屬性是完整資訊
    - E (Extend、擴充的)
      - 0: 屬性的長度欄為 1 個位元組
      - 1: 屬性的長度欄為 2 個位元組



Flag Bits	Description
0	0 for required attribute, 1 if optional
1	1 for transitive, 0 for nontransitive
2	0 for complete, 1 for partial
3	0 if length field is one octet; 1 if two
5-7	unused (must be zero)

Figure 15.10 Bits of the 2-octet type field that appears before each BGP attribute path item and the meaning of each.

BGP 路徑屬性

- 2-位元組 型態 (Type) 欄位
  - 型態碼 (Type Code) 位元
    - 1: ORIGIN (發源)
    - 2: AS_PATH (自治系統路徑)
    - 3: NEXT_HOP (下一跳躍)
    - 4: MULTI_EXIT_DISC (多重 AS 離開點)
    - 5: LOCAL_PREF (本地喜好設定)
    - 6: ATOMIC_AGGREGATE (已聚集的路由器)
    - 7: AGGREGATOR (已聚集的路由器 ID)

Type Code	Meaning
1	Specify origin of the path information
2	List of autonomous systems on path to destination
3	Next hop to use for destination
4	Discriminator used for multiple AS exit points
5	Preference used within an autonomous system
6	Indication that routes have been aggregated
7	ID of autonomous system that aggregated routes

Figure 15.11 The BGP attribute type codes and the meaning of each.

BGP KEEPALIVE 訊息

- 兩 BGP 對等定期交換*保持連線* (KEEPALIVE) 訊息，以測試網路連接性並確定兩對等持續運作。

- *保持連線* 訊息只有標準訊息標頭而無額外資料，因此該訊息長度為 19 位元組 (最小 BGP 訊息長度)。

- BGP 將測試連接性與繞路更新的功能分開，讓 BGP 可以常常傳送小的保持連線訊息，而可達性改變時才傳送較大的更新資訊。

Detecting Spoofed Packets-2

hop-count inspection & filtering

- C.Jine *et al.* present a novel *filtering technique* that is immediately deployable to validate the source IP address of each packet via hop-count inspection and weed out spoofed IP packets.

- This hop-count information can be inferred from the Time-to-Live (TTL) value in the IP header. *Using a mapping between IP addresses and their hop-counts to an Internet server*, the server can distinguish spoofed IP packets from legitimate ones.

- The final TTL value when a packet reaches its destination is the initial TTL subtracted by the number of intermediate hops, however, the challenge in hop-count computation is that a destination only sees the final TTL value.

Cheng Jin, Haining Wang, and Kang G. Shin, "Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic", Proc. 10th ACM Conf. .Computer and Communications Security (CCS), Washington, DC, October 2003.

Detecting Spoofed Packets-2

hop-count inspection & filtering

- C.Jine *et al.* show that most modern OSs use only a few selected initial TTL values, 30, 32, 60, 64, 128, and 255.

- Moreover, *most of these initial TTL values are far apart*, except between 30 and 32, 60 and 64, and between 32 and 60.

- Since Internet traces have shown that
  few Internet hosts are apart by more than 30 hops,
  one can determine the initial TTL value of a packet by selecting the smallest initial value in the set that is larger than its final TTL.

Cheng Jin, Haining Wang, and Kang G. Shin, "Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic", Proc. 10th ACM Conf. .Computer and Communications Security (CCS), Washington, DC, October 2003.

Detecting Spoofed Packets-2

hop-count inspection & filtering

- For example, if the final TTL value is 112, the initial TTL value is 128, the smaller of the two possible initial values, 128 and 255.

- To resolve ambiguities in the cases of {30, 32}, {60, 64}, and {32, 60}, a hop-count value for each of the possible initial TTL values will be computed, and the packet will be accepted if there is a match with one of the possible hop-counts.

Cheng Jin, Haining Wang, and Kang G. Shin, "Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic", Proc. 10th ACM Conf. .Computer and Communications Security (CCS), Washington, DC, October 2003.

Detecting Spoofed Packets-2

hop-count inspection & filtering

```
for each packet:
    extract the final TTL T_f and the IP address S;
    infer the initial TTL T_i;
    compute the hop-count H_c = T_i − T_f;
    index S to get the stored hop-count H_s;
    if   (H_c ≠ H_s)
            the packet is spoofed;
    else
            the packet is legitimate;
```

- The algorithm extracts the source IP address and the final TTL value from each IP packet.
- The source IP address serves as the index into the table to retrieve the correct hop-count for this IP address. If the computed hop-count matches the stored hop-count, the packet has been "authenticated;" otherwise, the packet is likely spoofed.

Cheng Jin, Haining Wang, and Kang G. Shin, "Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic", Proc. 10th ACM Conf. .Computer and Communications Security (CCS), Washington, DC, October 2003.

An Algebraic Approach to IP Traceback

D. Dean, M. Franklin, and A. Stubblefield, "An Algebraic Approach to iP Traceback," in Proc. of the Network and Dsitributed System Security Symposium (NDSS), pp. 3-12, February 2001.
http://www.isoc.org/isoc/conferences/ndss/01/2001/papers/dean01.pdf

ACM Transaction on Information and system Security,May 2002

The basic idea

- Let $A_1, A_2, \ldots, A_n$ be the 32-bit IP addresses of the routers on path P. We associate a packet id with the j-th packet.

$$((((0 \cdot w) + A_1)w + A_2)w + A_3)w + A_4 = A_1 w^3 + A_2 w^2 + A_3 w + A_4.$$

- As long as all of the x_i's are distinct, the matrix is a Vandermonde matrix (and thus has full rank) and is solvable in field operations.

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{pmatrix} = \begin{pmatrix} FullPath_{n,1} \\ FullPath_{n,2} \\ \vdots \\ FullPath_{n,3} \end{pmatrix}$$

IP Traceback – Relative Works

Logging

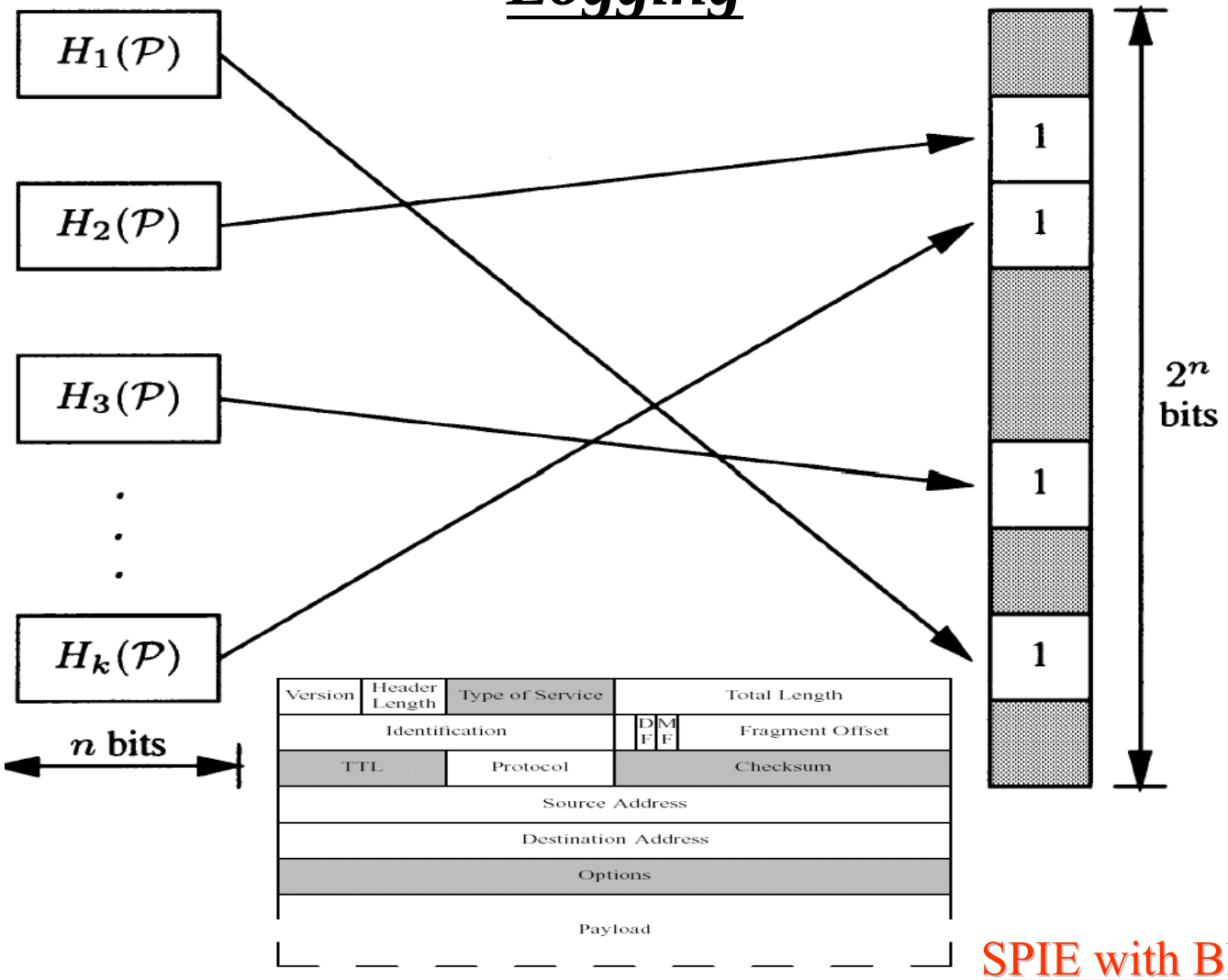


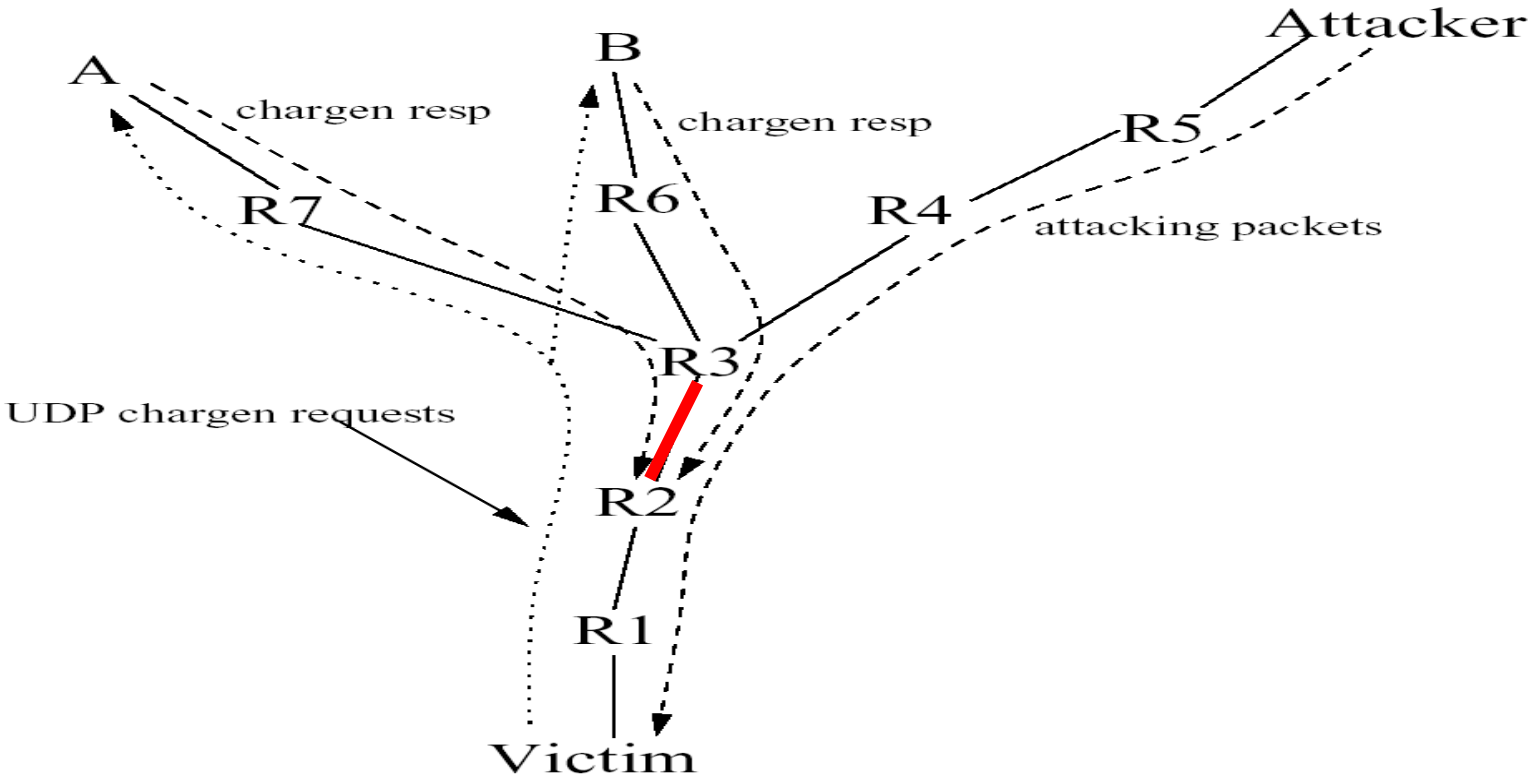
Figure 2: The fields of an IP packet. Fields in gray are masked out before digesting, including the Type of Service, Time to Live (TTL), IP checksum, and IP options fields.

SPIE with Bloom Filters

A.C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer," Single-Packet IP Traceback," IEEE/ACM Transactions on Networking (ToN), Volume 10, Number 6, December 2002.

IP Traceback – Relative Works

Link Testing– Controlled Flooding

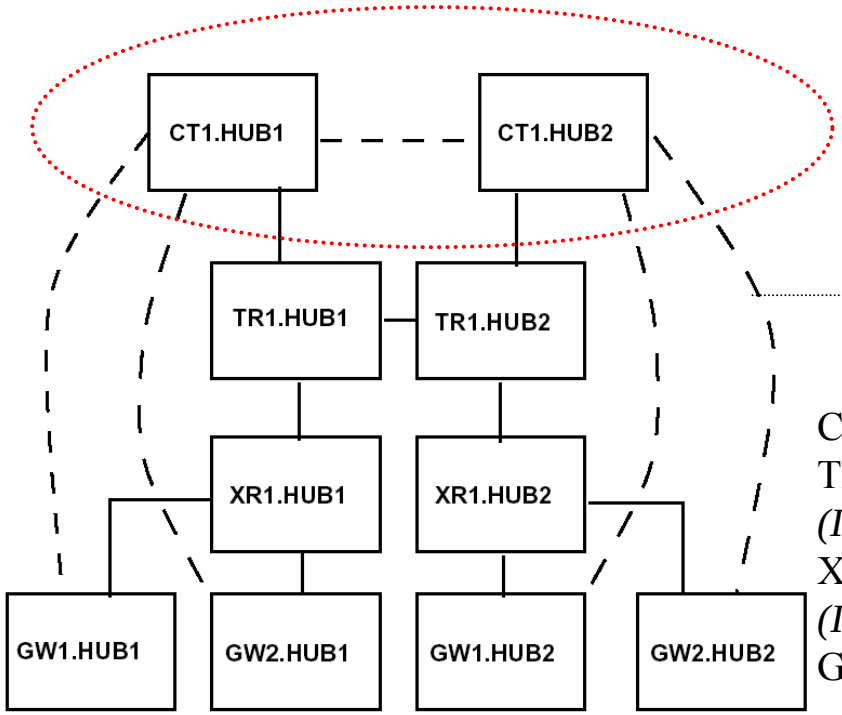


Example of traceback step. Packets are sent to A and B, spoofed from R2, in order to initiate packet flows towards the victim. This causes increases congestion along the R3-R2 link, which, if sufficient, will induce packet loss.

H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source." Usenix LISA (New Orleans) Conf., pp.313-322, 2000.

IP Traceback – Relative Works

Input Debugging--CenterTrack



AS : BGP

(The physical connection between tracking routers)

IP Tunnels

CT:CenterTrack Routers
TR:Transit Routers
(It represent the top level in the transit router hierarchy.)
XR:Transit Routers
(It represent the bottom level in the transit router hierarchy.)
GW:Edge Routers

The CenterTrack approach use the edge routers to select interesting datagram and forward them to special tracking routers that examine the datagrams coming from various connections.

Stone, R., "CenterTrack: An IP overlay network for tracking DoS floods," Proc. 9th USENIX Security Symp., Denver, CO, Aug. 2000.

IP Traceback – Relative Works

ICMP Traceback (iTrace)

- The principle idea in this scheme is *for every router to sample*, with low probability (e.g.,1/20000), *one of the packets* it is forwarding and *copy the contents into a special ICMP Traceback message* including information about the adjacent routers along the path to the destination.The victim host can then use these messages to reconstruct a path back to the attacker.

- ICMP traceback message =

  (Backward link, forward link, time stamp, traced packet , Authentication)

draft-bellovin-itrace-00.txt

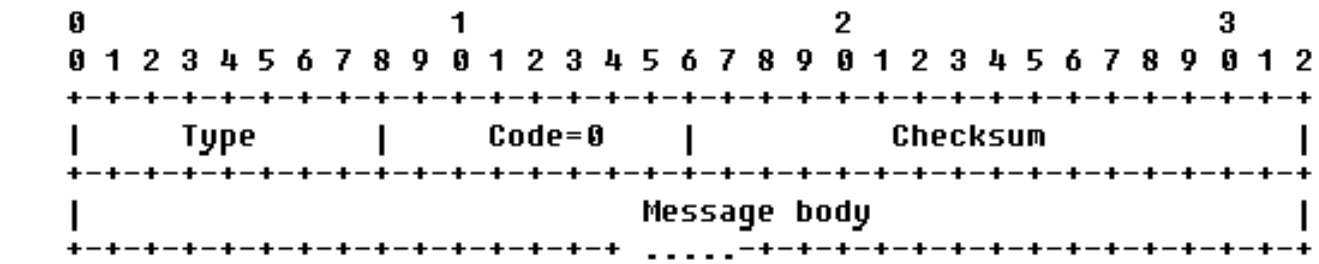
IP Traceback – Relative Works

ICMP Traceback (iTrace) : *Format*

- ICMP TYPE of TRACEBACK will be assigned by IANA. (Internet Assigned Numbers Authority)

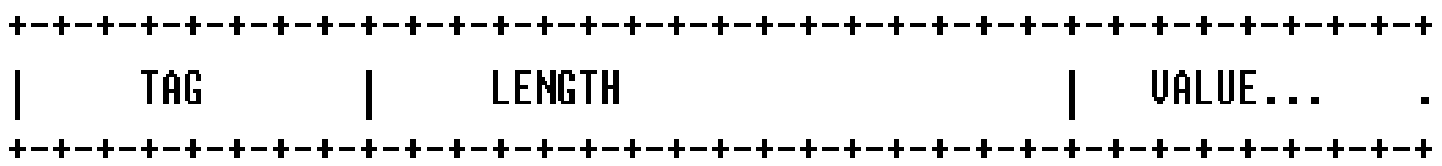
  The CODE field must always be set to 0 (no code), and must be ignored by the receiver.

Traceback Message



- The body of any ICMP TRACEBACK message consists of a series of individual elements that are self-identifying, using a TAG-LENGTH-VALUE scheme as follows:

巢狀式套疊

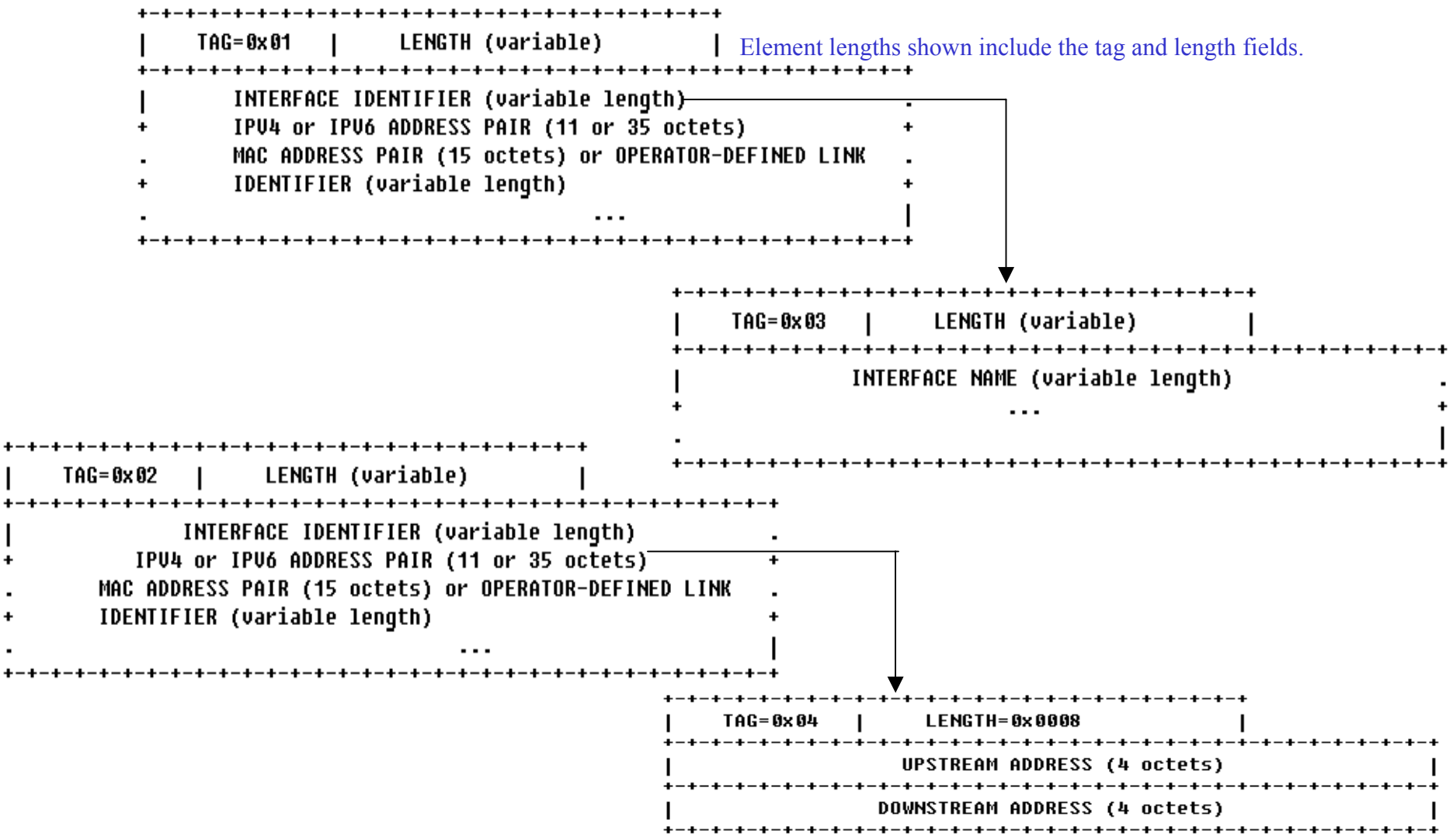


(a single octet)

draft-ietf-itrace-01.txt

IP Traceback – Relative Works

ICMP Traceback (iTrace) : *Format*



Element lengths shown include the tag and length fields.

draft-ietf-itrace-01.txt

IP Traceback – Relative Works

Other ICMP Traceback Schemes

- *Intention–driven ICMP traceback*
- *ICMP traceback messages suppression schemes*
- *“Incremental deployment" improvement*

IP Traceback – Relative Works

ICMP Traceback (iTrace) : *disadvantages-1*

(1) ICMP traffic is increasingly differentiated and may itself *be filtered in a network under attack*.

(ICMP message filter is normally enabled at firewalls.)

(2) Generate overhead traffic

(3) Reconstruction of attack path takes longer duration such as 30 min, because the probability is 1/20000 for avoiding traffic overhead.

(4) It requires a key distribution infrastructure to deal with the problem of attackers sending false ICMP traceback messages. (It's not realistic.)

IP Traceback – Relative Works

ICMP Traceback (iTrace) : *disadvantages-2*

(5) Although intention-driven iTrace mechanism resolves the statistic problem in iTrace , intention-driven iTrace causes some extra overhead by aimlessly broadcasting BGP updates to all routers in the whole Internet .

(6) In practice, this related IETF drafts of iTrace have been expired and not been maintained since March 28, 2002.

(7) Again, it is quite clear that these schemes cannot cope with all conceivable DoS/DDoS attacks.

For example, an attack based on inducing innocent and uncorrupted machines to send traffic to the victim would be traceable only to these machines, and not to the real attackers.

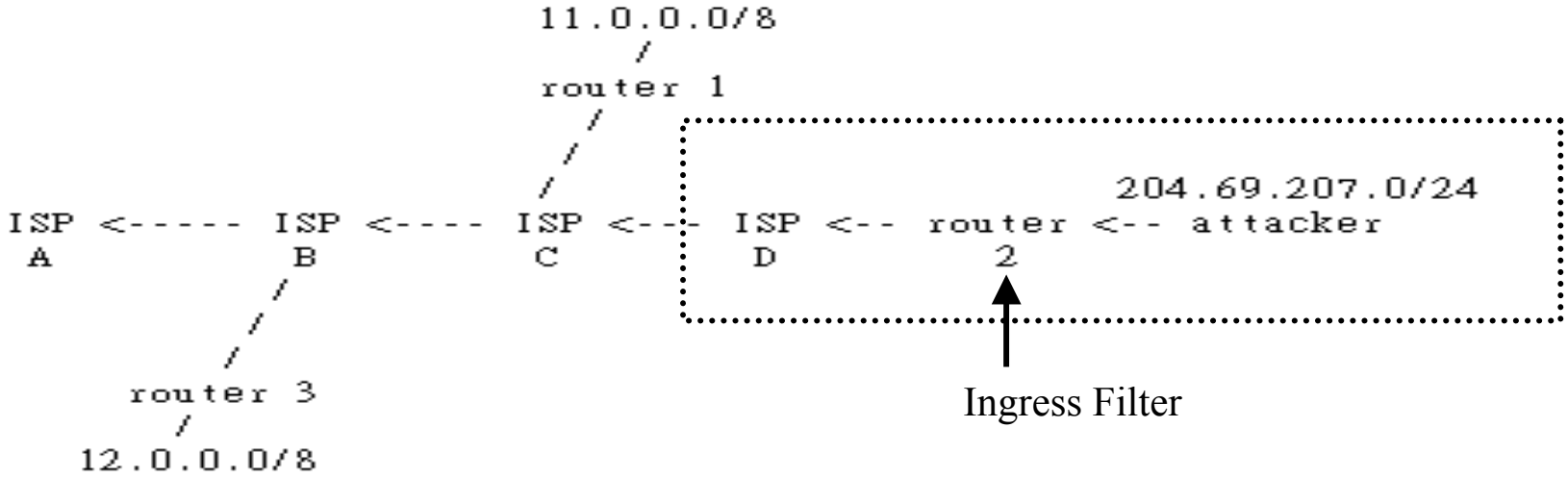
S. Felix Wu et al.,*Intention-Driven ICMP Trace-back*, Internet Draft: draft-wu-itrace-intention-00.txt,IETF

Allison Mankin et al.,*On Design and Evaluation of Intention-Driven ICMP Traceback*, Proc. of 10th IEEE International Conference on Computer Communications and Networks,Oct. 2001

IP Traceback -- Relative Works

Ingress Filtering

By restricting transit traffic which originates from a downstream network to known, and intentionally advertised, prefix(es), the problem of source address spoofing can be virtually eliminated in this attack scenario. [RFC2267;1998] [RFC2827;2000]



IF packet's source address from within 204.69.207.0/24
THEN forward as appropriate

IF packet's source address is anything else
THEN deny packet

PPM – Improving Convergent Amount

Proposed PPM-NPC : Parameters

(a) $p_{j,i}$ is the probability that a packet is marked by R_j, and this marked packet will arrive at the successive router R_i, where $i > j$.

(d) E_i is the probability that outgoing packets from R_i are marked-free.

PPM – Improving Convergent Amount

Proposed PPM-NPC : *Properties-1*

- $p_{j,i} \leqq p$

  As the non-preemptive nature of PPM-NPC, every packet marked by R_j will arrive at the successive routers (R_i) without being altered, so that $p_{j,i} \leqq p$ while $i > j$.

- $E_i \geqq (1 - i \cdot p)$, for all $i \geqq 1$

$$E_i = \left[E_{i-1} \cdot (1-p) - \left(\sum_{j=1}^{i-1} p_{j,i} \right) \cdot p \right] \geq E_{i-1} \cdot (1-p) - (i-1) \cdot p^2$$

- If the distance from the attacker to the victim is $max(i)$ hops, and we set p as $1/max(i)$, then we can get $E_i \geqq 0$ for all $i \geqq 1$.

  This result shows that the volume of marked-free packets is always equal to or greater than the reduction of marking probability, so that we can get $p_{j,i} = p$ in all j and $i \geqq j$.

PPM – Improving Convergent Amount

Proposed CPPM : Parameters

(a) $C_{i+d,i}$ denotes the probability that the packet marked by R_i may be remarked and then be compensated in R_{i+d}, where $d \geqq 1$.

For $i=k+1$ and $d=n$, $C_{k+1+n,k+1} = p \cdot (1-p)^{n-1} \cdot p + \sum_{j=1}^{n-1} C_{k+1+j,k+1}(1-p)^{n-j-1} \cdot p$

(b) C_i represents the probability needed for compensating in R_i.

(c) $p_{i+d,i}$ is the probability that a packet is marked by R_i, and this marked packet will arrive at R_{i+d}.

(d) E_i denotes the probability that the outgoing packets from R_i are marked-free.

PPM – Improving Convergent Amount

Proposed CPPM : Properties

The properties of CPPM are summarized below.

1) $C_i = (i-1)\cdot p^2$ reveals that CPPM in any router will remark and then compensate the packet marked in any previous router with p^2.

2) E_i, $1-i\cdot p$, is monotonously decreasing, and $E_i > E_j$ when $i<j$. If $p=1/(max(i))$, then E_i is always zero or greater for all $i \geqq 1$. This means that it is always possible to compensate the remarked packet in any router.

3) $p_{i+d,i} = p$ reveals that all packets marked in any router will arrive at all of the successive routers, including the victim, when $E_i \geqq 0$. The show on probability equals its marking probability.

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC : *Notation-1*

- $W(w.start, w.end, w.distance)$ denotes the marking message generated by R_i.
- $M(m.start, m.end, m.distance)$ denotes the marked message in a marked packet.
- $R(r.start, r.end, r.distance, r.counter)$, initialized to a null table, in R_i denotes the remedial table for

  remedying the incomplete path information because of consecutive transparent routers, or

  compensating the marking probability because of the non-preemptive marking resulted from PPM-NPC.

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC : Notation-2

- $C(c.start, c.end)$, initialized to a null table, in R_i denotes the check table in order for the remedial process.

- A global variable I_R_{i-1}, initialized to 0, in R_i is an indicator of the R_{i-1}'s status.

  If I_R_{i-1} is set to 1, it indicates R_{i-1} is a PPM-NPC-capable router.

  If I_R_{i-1} is set to 2, it indicates R_{i-1} is an individual transparent router.

- Here, E_i is the probability that incoming packets for R_i are market-free.

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC : Algorithm-1

- Once receiving an incoming packet, R_i with RPPM-NPC will create a

  forward link massage, if $0 \leqq x < p/2$,

  backward link massage, if $p/2 \leqq x < p$,

  or null value.

  Note: The total marking probability is still p.

- If the incoming packet is a marked packet and R_i does not generate a null value, R_i will put this generated link information into its remedial table R, waiting for being compensated to a next available marked-free packet. (*compensating the marking probability*)

- R_i will also modify the distance field of marked packets in some special cases, for correcting the order of links under reconstructing the attack path.

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC : Algorithm-2

- R_i increases the *m.distance* by 1 and forwards this marked packet, if *m.distance* is not equal to 1.

If m.distance is equal to 1: (1)—(4)

(1)If *m.end* = R_i, this implies that R_{i-1} is a RPPM-NPC-capable router. Therefore, R_i just forwards it, and sets I_R_{i-1} as 1.

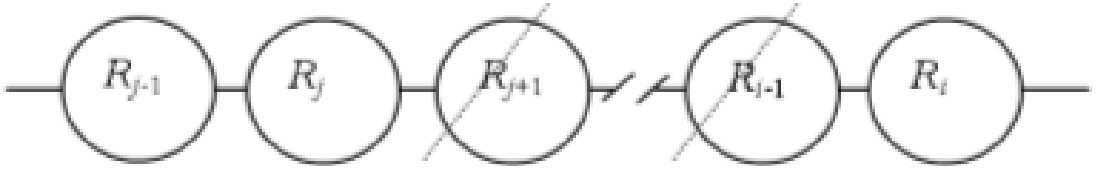
(2)If *m.end* = R_{i-1} and R_{i-1} is known as a RPPM-NPC-capable router, then *m.distance* will be assigned as 2.

Otherwise, if *m.end* = R_{i-1} and R_{i-1} may be an individual transparent router, then R_i sets I_R_{i-1} as 2, as well as *m.distance* will be assigned as 2 in order to make up the gap resulting from R_{i-1}. 2->(1)->1

(3)If *m.end* is not equal to R_{i-1} and R_i, as well as R_{i-1} is known as an individual transparent router, then *m.distance* will be modified as 3 to remedy the gap resulting from R_{i-1}. (R_{i-3}, R_{i-2})

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC : Algorithm-3



(4) If *m.end* is not equal to R_{i-1} and R_i, as well as R_{i-1} is neither a RPPM-NPC-capable router nor an individual transparent router. R_i will record (R_{j-1}, R_j) or (R_j, R_{j+1}), in its check table C(*c.start*, *c.end*).

- If *m.end* is equal to one of *c.start* in the check table C, the marked message may be the backward link produced by R_j. Thus, the *m.distance* will be modified as 4.
- If *m.start* is equal to one of *c.end* in C, the marked message may be the forward link produced by R_j. Thus, the *m.distance* will be modified as 3, and a special link (*m.end*, R_{i-1}, 2, 1) will be stored in a remedial table R, or *r.counter* is just increased by 1 in order to remedy the gap resulting from R_{j+1} to R_{i-1}.

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC : Algorithm-4

- Table *R* is utilized to record (*remedying the incomplete path information*)

  the first transparent router among these consecutive transparent routers as *r.start*, and

  the final transparent router, R_{i-1}, as r.*end*.

  r.distance is also set to 2, if the *m.end* of the incoming packet is not equal to R_i itself or any R_i's previous router, but *the distance field in this marked packet is 1*.

- If the received packet is marked-free, R_i will pick up one of (*r.start, r.end, r.distance, r.counter*) in *R*, and embed (*r.start, r.end, r.distance*) into this packet.

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC : The Feasibility of Compensation

- Property: $E_j+1 \geqq 0$, while $p \leqq 1/j$ for all j.

  This property means that the size of E_j is more than the need to make up the remedial and compensated marking.

- If the distance from the attacker to the victim is $\max(j)$ hops, and the marking probability p can be set as $1/\max(j)$, then we can get $E_{j+1} \geqq 0$ for all j.

PPM – Improving Incomplete Deployment Problem

Proposed RPPM-NPC : The Convergent Condition

- In these resolvable incomplete deployment cases, the marking probability of any remedied link will become $p/2$ at most, although each link can be shown on the victim.

- We will *conservatively* assume that the marking probability of each link is $p/2$.
  Hence, comparing with the scheme of PPM-NPC without remedial ability, the increased ratio of the convergent amount is:

$$\frac{\left\{\left[\ln(\#\text{ of total routers})+\gamma\right]\div\left(p/2\right)\right\}}{\left\{\left[\ln(\#\text{ of PPM - NPC routers})+\gamma\right]\div p\right\}}$$

References (iTrace)

- S. M. Bellovin,, "***ICMP traceback messages***,"IETF,Internet Draft, draft-bellovin-itrace-00.txt , March 2000.

- S. Felix Wu et al.,"***Intention-Driven ICMP Trace-back***", Internet Draft: draft-wu-itrace-intention-00.txt,IETF,Febuary 2001.

- S. Felix Wu et al.,"***Intention-Driven ICMP Trace-back***", Internet Draft: draft-wu-itrace-intention-01.txt,IETF,July 2001.

- S. M. Bellovin, M. Leech, and T. Taylor, "***ICMP traceback messages***,"IETF, Internet Draft, draft-ietf-itrace-01.txt, October 2001.

- A. Mankin, D. Massey, C.-L. Wu, S. F. Wu and L. Zhang,"***On design and evaluation of `intention-driven' ICMP traceback***", in Proc. IEEE Int. Conf. Computer Communications and Networks , Oct. 2001, pp. 159-165.

- Vadim K. et al,"***An evaluation of different IP traceback approaches***", 4th ICICS , December 2002