IP Traceback

KRnet 2004

23th June 2004

Hyung-Woo Lee

Dept. of Software, Hanshin University, Korea

hwlee@hs.ac.kr

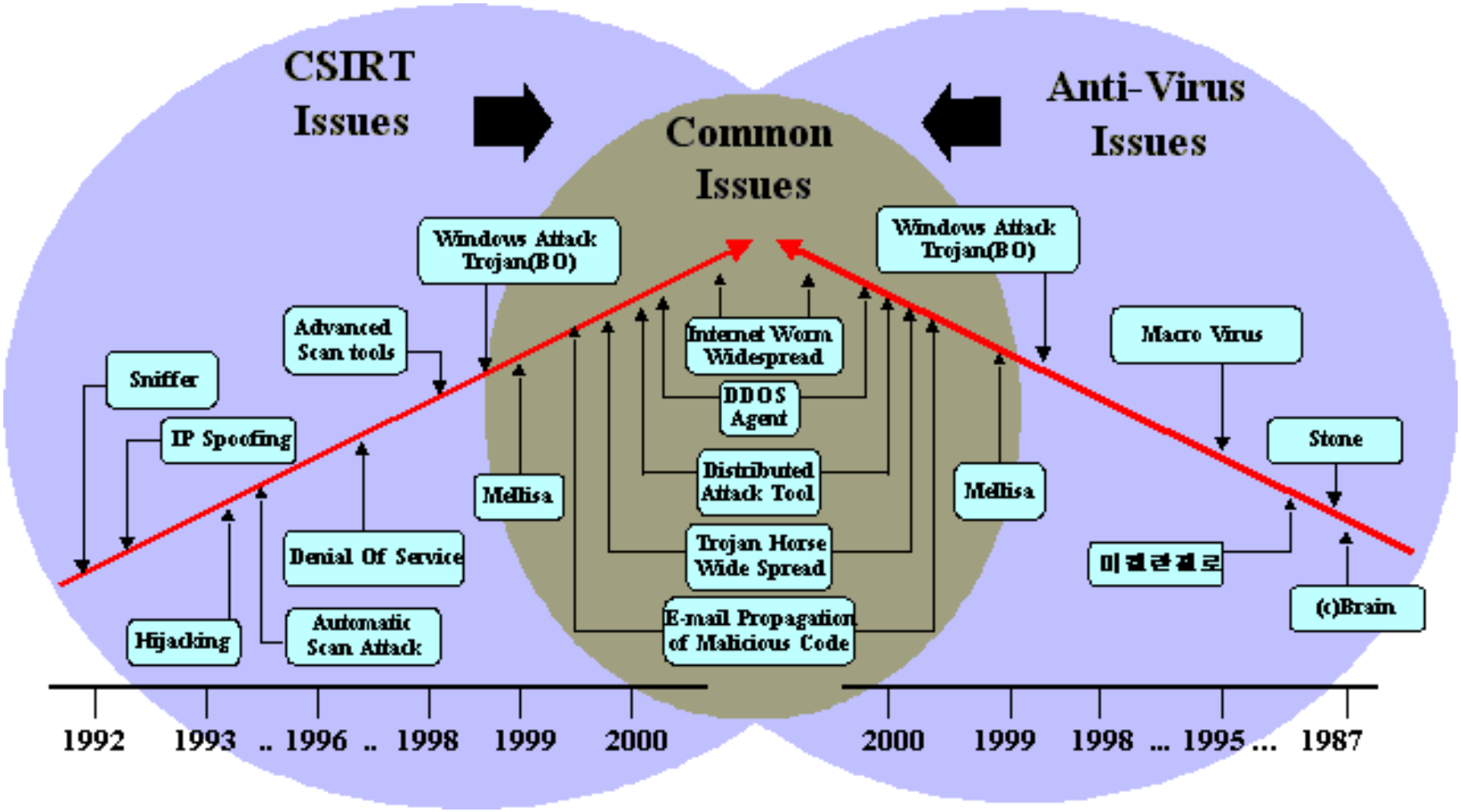
Contents

- Introduction : DDoS Attack
- Solution on DDoS Attack
  - Proactive/Reactive IP Traceback Technique
- Detailed IP Traceback Mechanism
  - Packet Marking
  - ICMP Traceback (iTrace)
  - Network based Mechanism
  - Advanced IP Traceback Scheme
- Simulation Results
- Applications and Conclusions

“Internet is Under DDoS Attack”

- Introduction -

DoS Attack



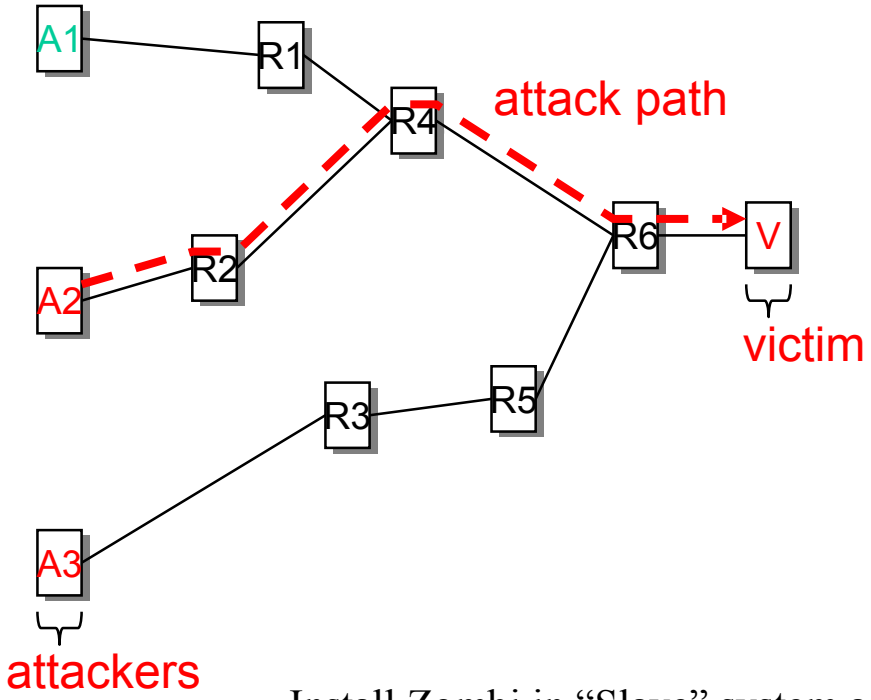
Attack Mechanisms are more complicated and combined with diverse intelligent scheme

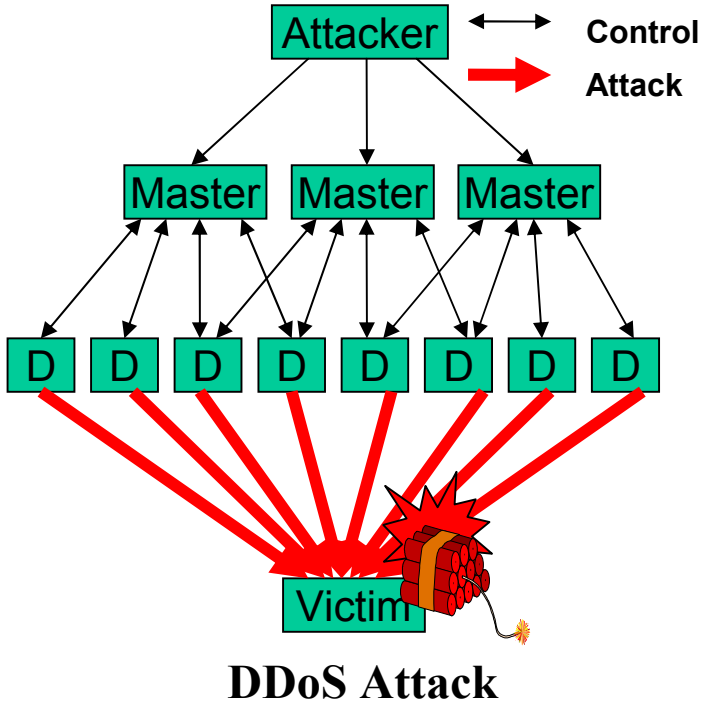
Type of DoS Attack

- **What is DoS Attack ?**
  - A malicious attack that "consumes resources of remote hosts or networks denying or degrading service to legitimate users"
- **Type of DoS Attack**
  - Bandwidth Consumption
  - Program Flaw Exploitation
  - Resource Starvation
  - Routing/DNS Attacks
  - SYN Floods
  - DDoS Attacks

DDoS Attack

Zombi based Attack





DDoS Attack

Install Zombi in “Slave” system and Attack by Distributed Multiple Connection

DDoS Attack

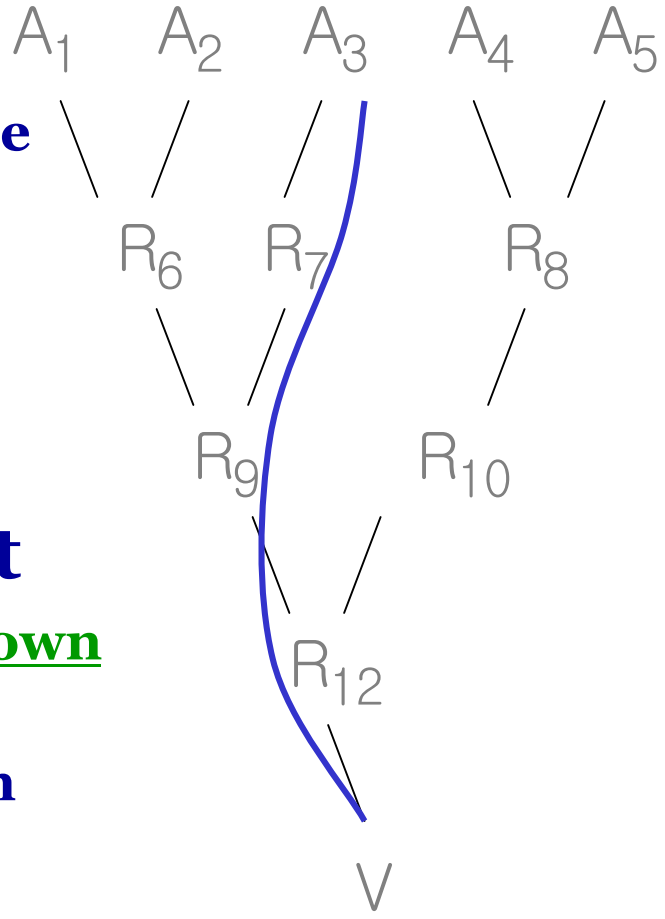
- **Easy to Attack**
  - **Denial of Service (DoS) attack**
    - remotely consume resource of server or network
    - Increase in number and frequency (Large volume of traffic)
    - simple to implement (such as.. Trinoo) (Easy…to attack)
- **Difficult to Trace**
  - **Indirection**
    - attacking packets sent from slave machines, which under the control of a remote master machine (Reflector based attack!)
  - **Spoof of IP source addresses**
    - Disguise their location using incorrect IP addresses, hence the true origin is lost (Spoofed address!)

Basic Assumption

- **DDoS Attack Assumption**
  - Attacker may generate any packet
  - Multiple attackers may conspire
  - Attackers may be aware they are being traced
  - Packets may be lost or reordered
- **IP Traceback Assumption**
  - Attackers send numerous packets
  - Route between attacker and victim is fairly stable
  - Routers have limited CPU and memory
  - Routers are not widely compromised

Traceback Problems

- **Many packets**
  - DDoS involves many packets on same path
- **Goal**
  - Given set of packets
  - Determine path !
- **Store one link in each packet**
  - Each router probabilistically stores own address
  - Fixed space regardless of path length



Solutions

- **Defeating DDoS Attack**
  - **Passive Solutions :**
    - Such as vaccines, and IDS/IPS etc., Firewall…
  - **Active Solutions :**
    - such as tracing back the (not spoofed real) origin of attacks.
- **Active Solutions can be divided into two mechanisms**
  - **Proactive traceback (Under DDoS Attack)**
    - PPM, ICMP traceback, etc.
  - **Reactive traceback (After DDoS Attack)**
    - Overlay, Hash based traceback, etc

Solutions (Cont'd)

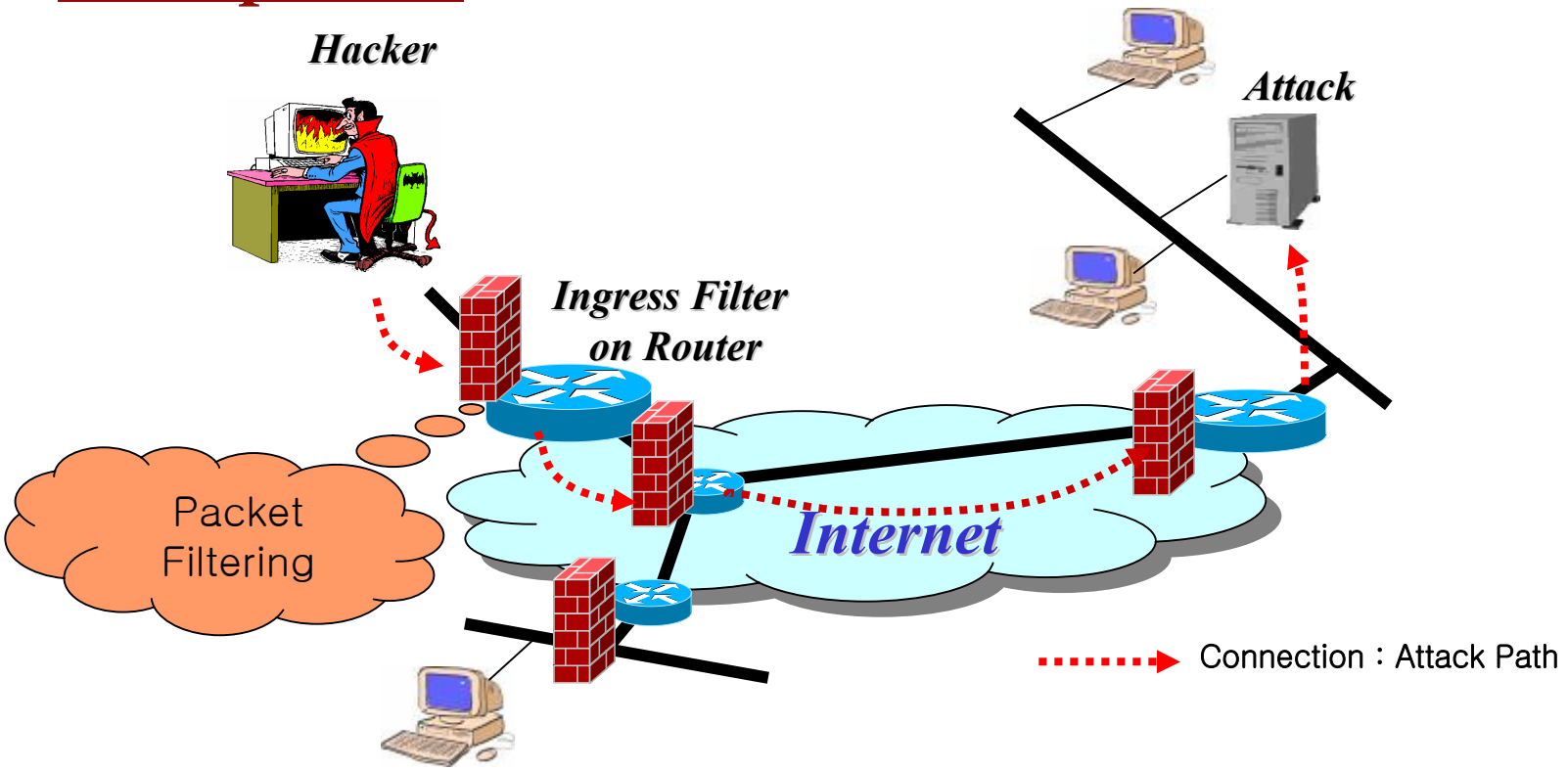
- **DDoS Counter Measure Solutions**
  - **Passive Solutions : Manual methods using current IP routing**
    - Ingress filtering
    - Link testing
      - input debugging/controlled flooding
    - Logging and etc.
  - **Active Solutions : Modify existing module or mechanism**
    - IP Traceback
      - ICMP Traceback(iTrace)/Probabilistic Packet Marking /Advanced PPM
    - Network based Solution
      - Overlay Network
      - Hash based IP Traceback(SPIE system)
      - IPSec based IP Traceback

“IP Traceback Mechanism”

- Passive Solutions -

Ingress Filtering

- **Ingress Filtering**
  - **Block packets with invalid source addresses**



Ingress Filtering

- **Ingress Filtering**
  - Defined in RFC 2267
  - Block packets with invalid source addresses
  - Edge Routers drop and log packets with invalid Source IPs or those coming from outside the network
  - Border Routers should not be allowed to transmit broadcast packets (MAC address FF:FF:FF:FF:FF:FF) to other routers by default (Blocking broadcast packets)
- **Pros**
  - Moderate management/network overhead (performance)
- **Cons**
  - require widespread deployment (modify existing router)
  - hard to do in backbone/transit network

Link Testing / Input Debugging

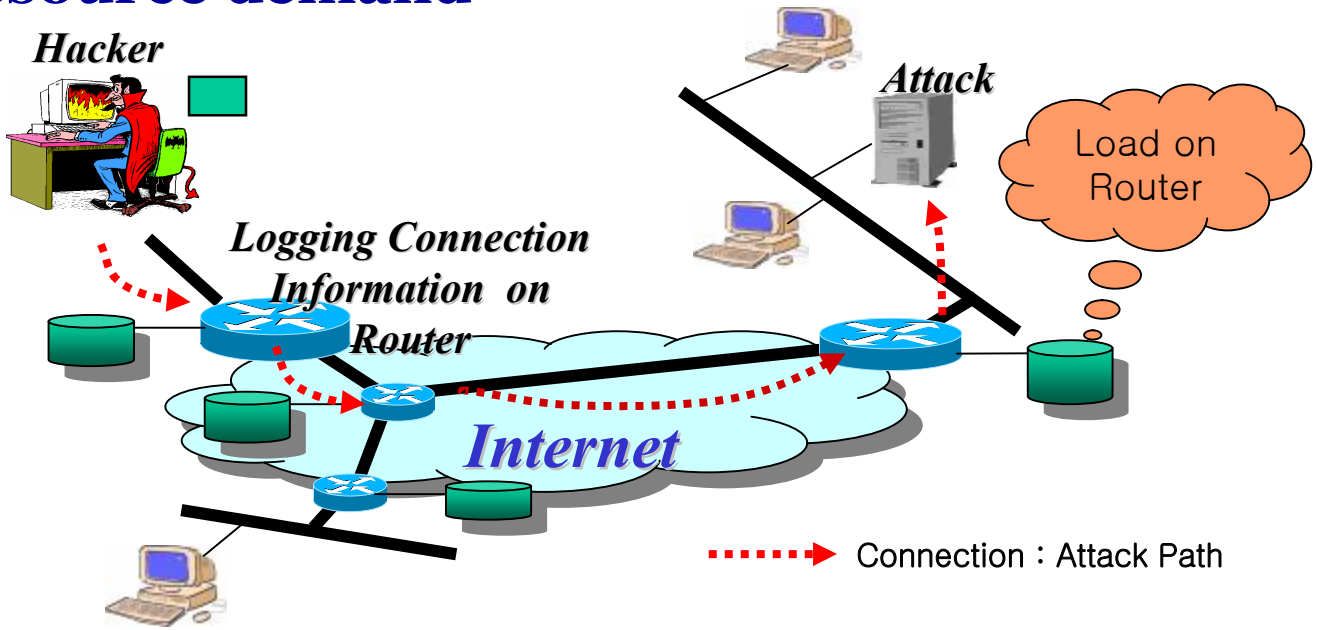
- **Link Testing**
  - **Basic Assumption**
    - Assume attack remains active until trace complete
  - **Start from victim and test upstream links (manual trace)**
    - Recursively repeat until source is located (similar with trace route)
- **Input Debugging**
  - **Victim recognize *attack signature (attack pattern)***
  - **Install filter on upstream router (similar with ing-Filter)**
  - **Pros**
    - May use software to help coordinate (Software based approach)
  - **Cons**
    - Require cooperation between ISPs
    - Considerable management overhead (Performance degradation)

Controlled Flooding

- **Flooding link with large bursts of traffic during attack**
- **Observe attacking packet rate change to determine the source**
  - Network Administrators send UDP chargen floods upstream (small scale DoS attack). If a router is perturbed then it is probably being used in the attack. Repeat upstream.
  - **Ethical issue – If the trace causes more damage than the attack, should it be used?**
- **Pros**
  - **Ingenious**
- **Cons**
  - **Itself a denial of service - possible worse**

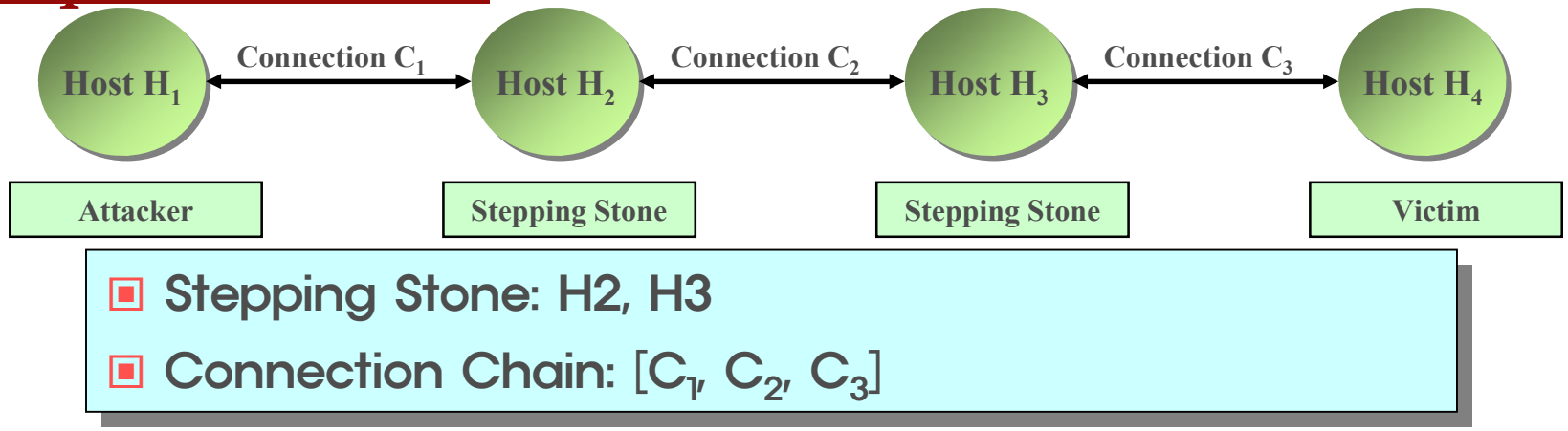
Logging

- Key routers logging packets
  - Data mining to analysis
- Cons
  - High resource demand



Stepping Stone Tracking

- **Stepping Stone** – one link in a connection chain
  - If ON/OFF timing between 2 hosts is similar, it is probably a stepping stone
    - **Check clear text packets to see if the text from one host is transmitted to another**
- **Problem** – too much legitimate traffic, not an adequate solution

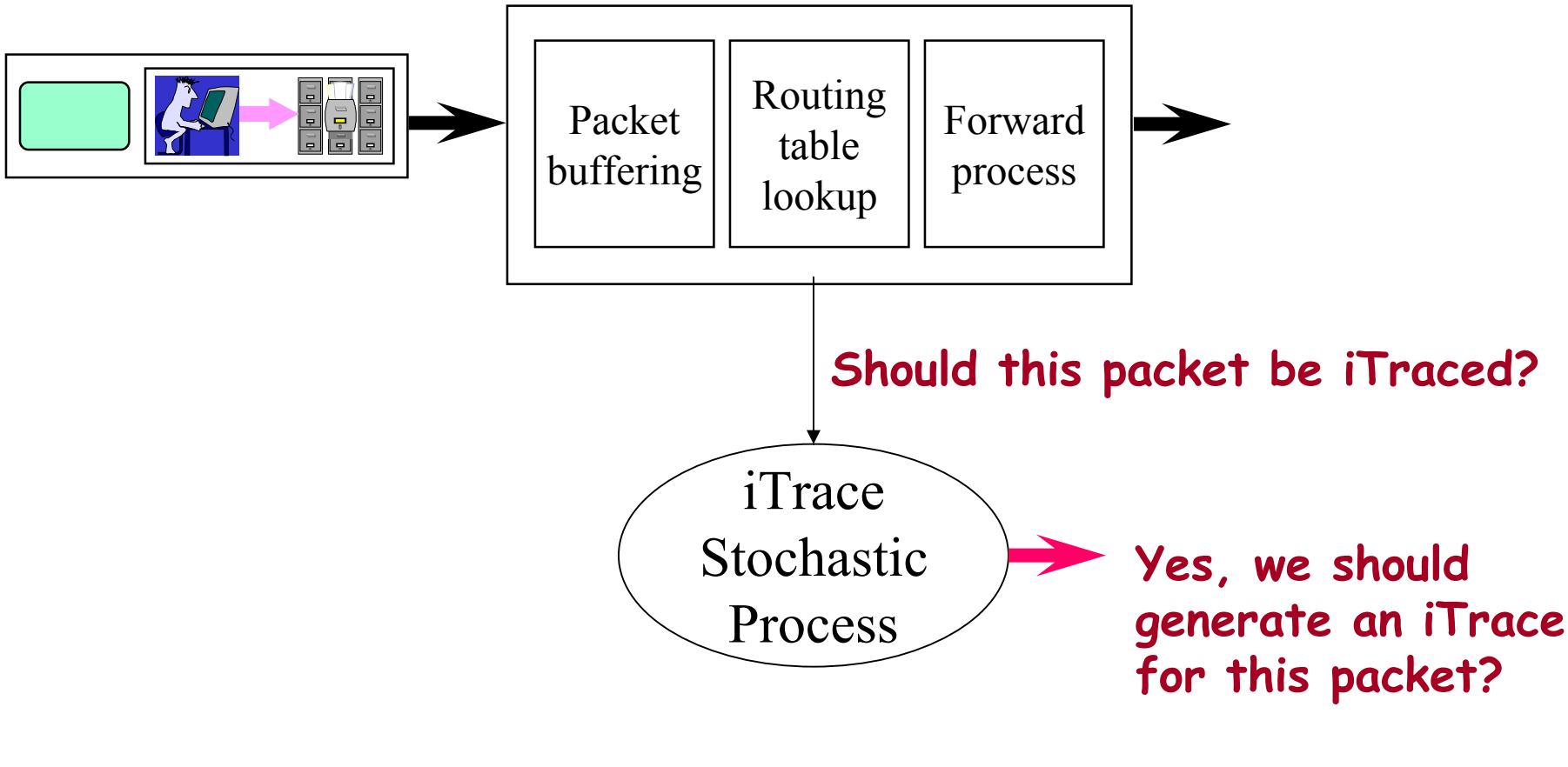


“IP Traceback Mechanism”

- Active Solutions -

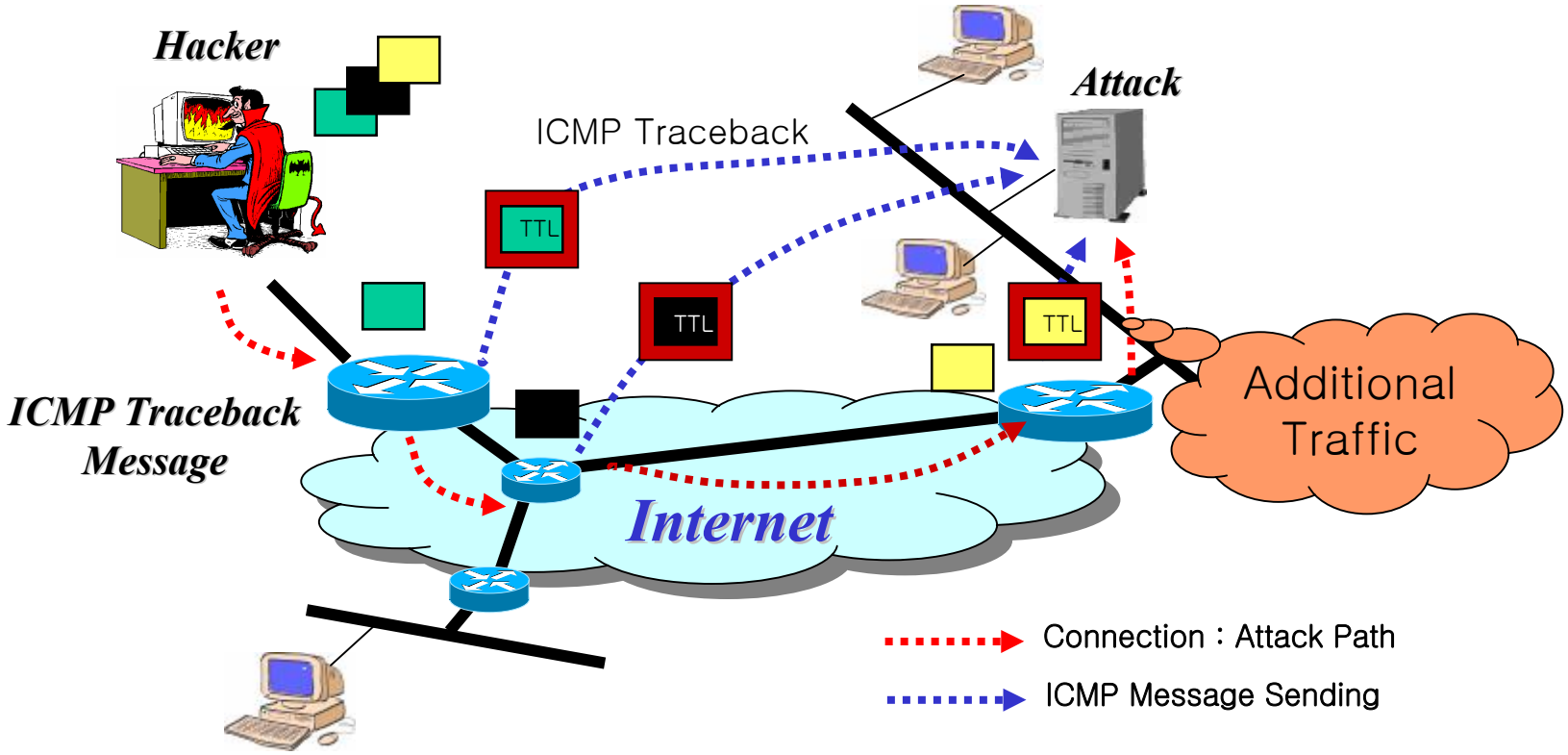
ICMP Traceback (iTrace)

- **ICMP packet to destination(victim) address**



ICMP Traceback (iTrace)

- ICMP packet to destination(victim) address



ICMP Traceback (iTrace)

- **ICMP Traceback**
  - Sample packets with low probability (Sampling)
  - Copy data and path information in a new ICMP packet
  - Routers send out ICMP traceback information (interface name, Time stamp) probabilistically (1/1000 – 1/20000) to the victim site
  - Public key system used to authenticate packets
    - TTL set to 255 to show distance
- **Pros**
  - Simple to reconstruct path information with small iTrace
- **Cons**
  - ICMP may be filtered and ICMP packet is also additional DDoS Traffic

Packet Marking (Cont'd)

- **Marking Procedure**
  - by routers
  - add information to packets
- **Path Reconstruction Procedure**
  - by victim
  - use information in marked packets
- **Convergence Time**
  - # of packets to reconstruct the attack path

$$E(X) < \frac{\ln(d)}{p(1-p)^{d-1}}$$

where p is marking probability, d is length of path

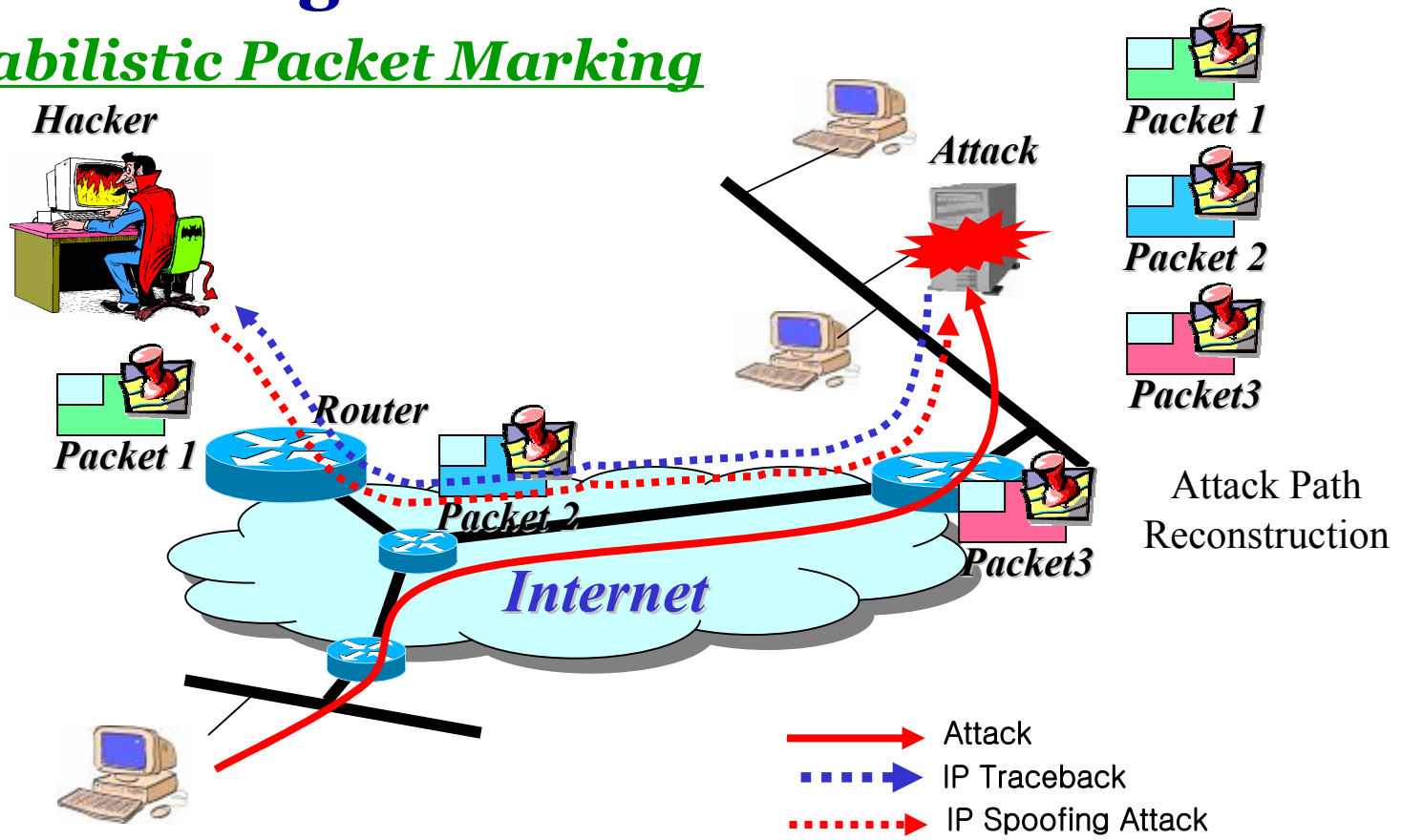
Packet Marking (Cont'd)

- **Probabilistic Packet Marking(PPM)**
  - Probabilistically inscribe local path information on IP header field (marking at IP header field)
  - Use constant space in the packet header
  - Reconstruct the attack path with high probability
- **Detailed Mechanism**
  - Node Appending (Simple but …)
  - Node Sampling (Gattering router's address)
  - Edge Sampling (Gathering packet transmission path)
  - Fragment Marking Scheme (Using multiple packet)
  - Advanced Marking Scheme (Providing enhanced security)

Packet Marking (Cont'd)

❑ Packet Marking at Router

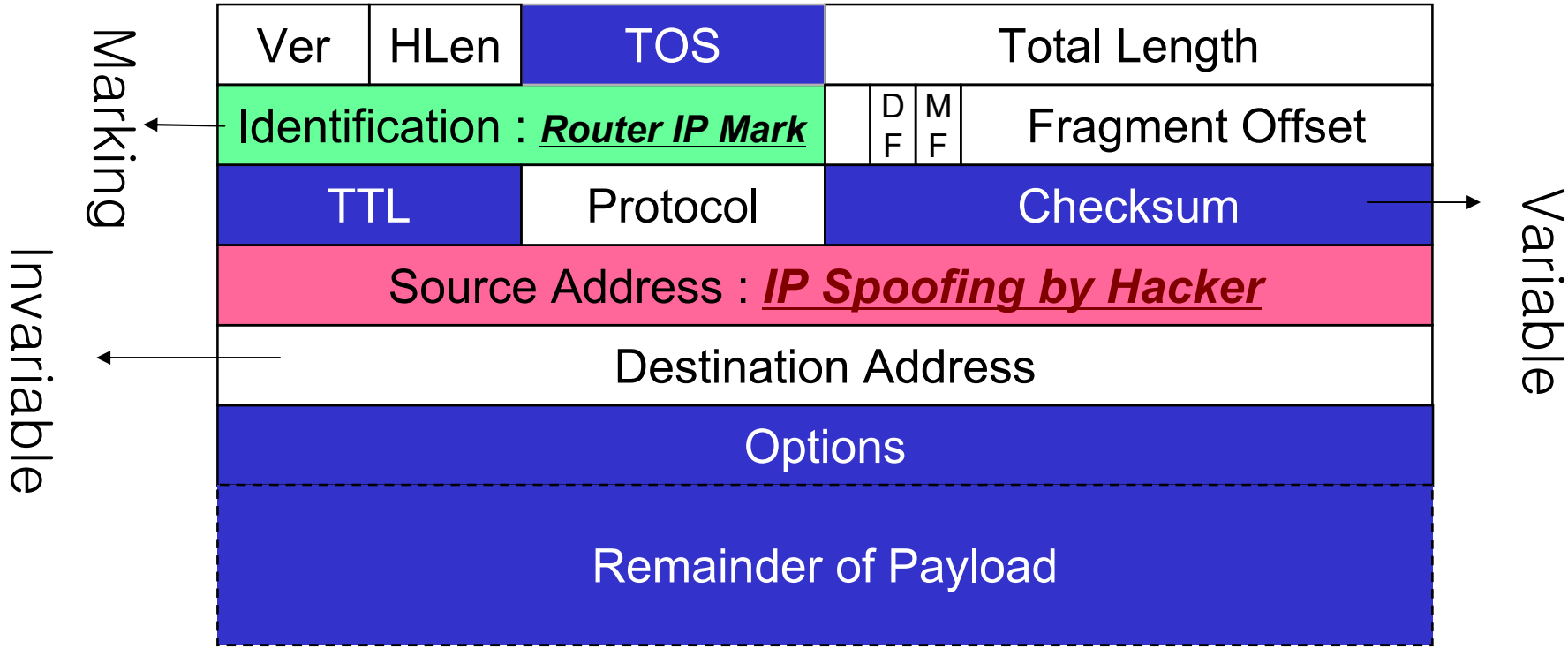
❖ *Probabilistic Packet Marking*



Packet Marking (Cont'd)

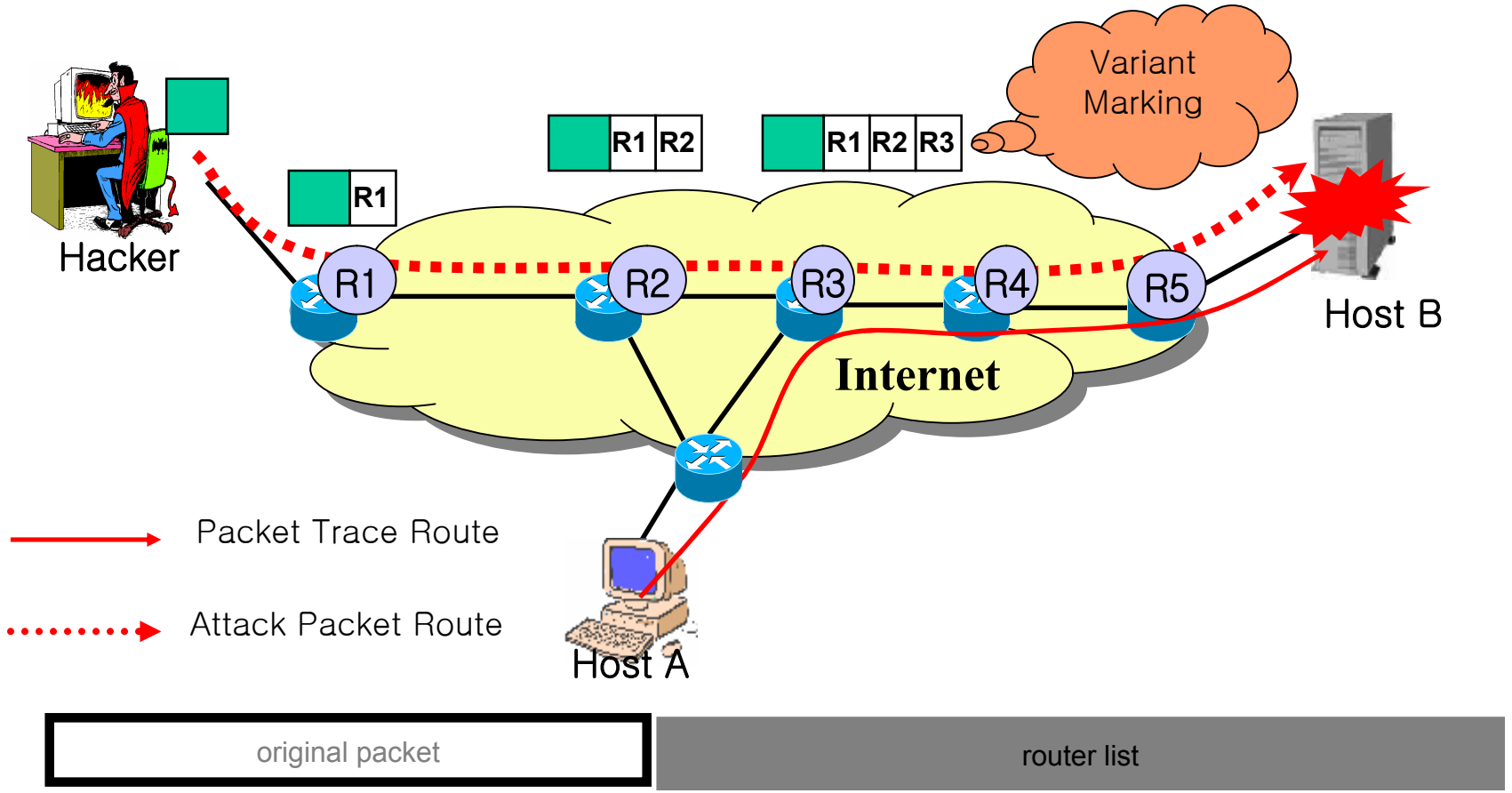
❑ Packet Marking at Router

❖ *Marking Router's IP Address in IP Packet Header*



Packet Marking (Cont'd)

❑ IP Traceback : Node Appending

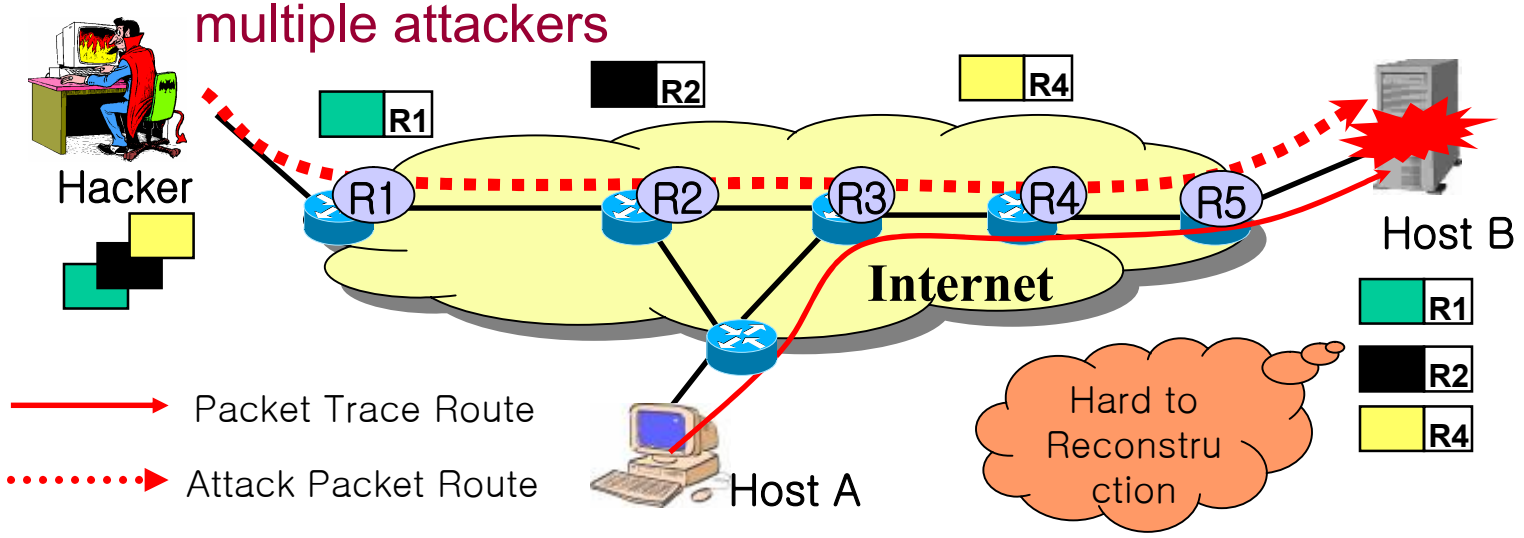


Packet Marking (Cont'd)

- **IP Traceback : Node Appending**
  - **Append address of each node to the end of the packet**
  - **Complete, ordered list of routers attack path**
  - **Disadvantages :** High router overhead/No space in the packet
- **Pros**
  - **complete, ordered attack path**
  - **converge quickly (single packet)**
- **Cons**
  - **infeasibly high router overhead (routing performance)**
  - **attacks can create false path information**

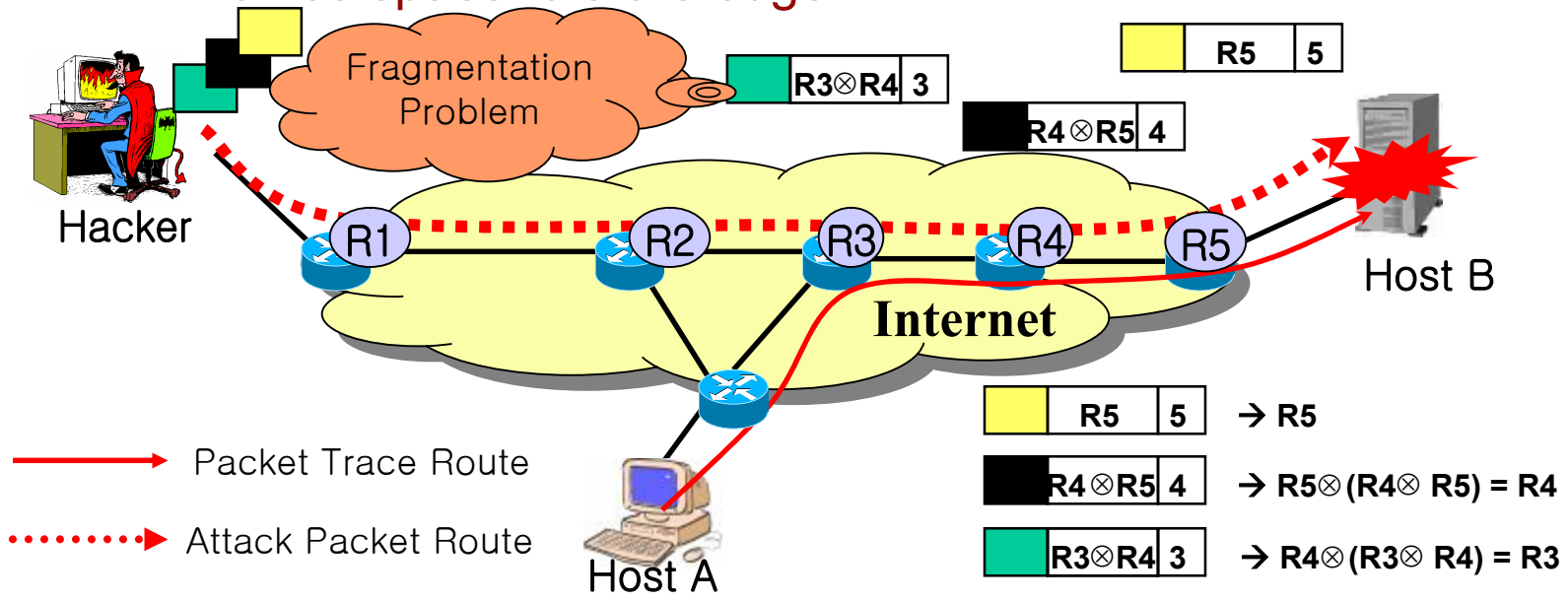
Packet Marking (Cont'd)

- **IP Traceback : Node Sampling**
  - **Reserve node file in packet header**
  - **Router write address in node field with probability *p***
  - **Reconstruct path using relative # of node samples**
    - Disadvantage : Slow convergence, Not robust in the case of multiple attackers



Packet Marking (Cont'd)

- **IP Traceback : Edge Sampling**
  - **Edge represent routers at each end of the link**
  - **Store edges instead of nodes**
    - start and end addresses of edge routers with distance
  - **XOR edge endpoints**
    - → halves space to store edge



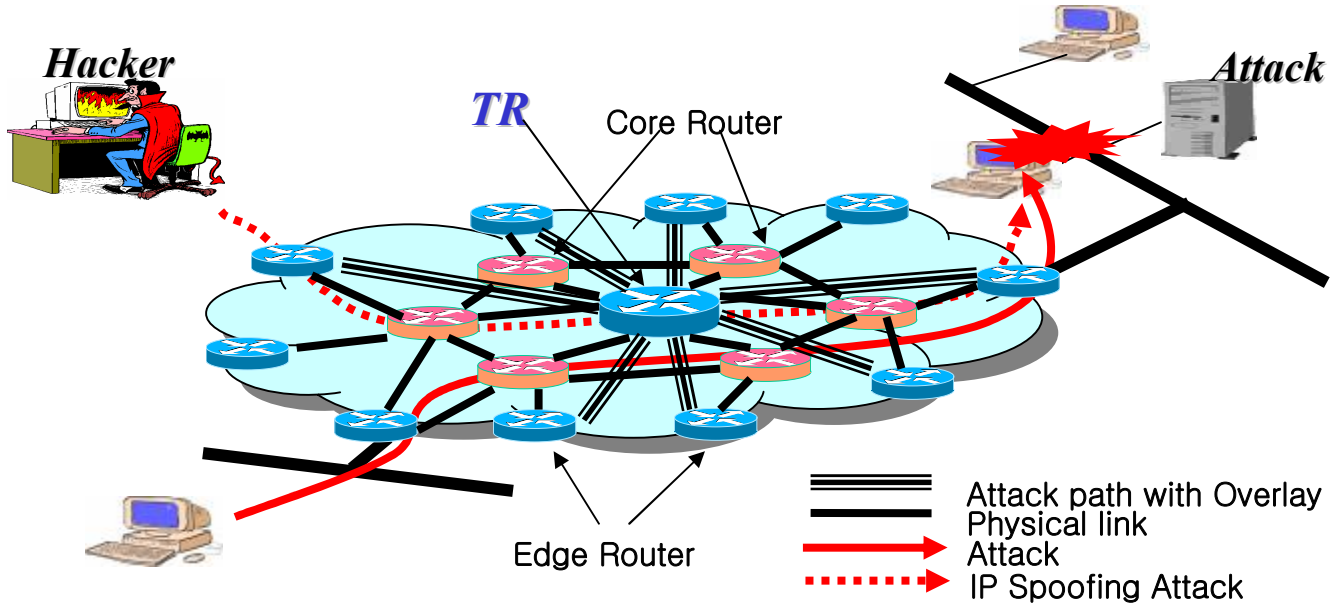
Packet Marking & Path Reconstruction

- **Packet Marking Algorithm**
  - A router writes its own address in the *start* field, and 0 into the distance field
  - Distance field is zero means the packet is already marked
    - router writes its own address in the end address field and increase the distance field by 1
- **Path Reconstruction Algorithm**
  - Consider *G* is a graph with root *v*
  - Insert tuples (start, end, distance) into *G*
  - Remove any edge (*x*, *y*, *d*) with *d* != distance from *x* to *v* in *G*
  - Extract path from *G*.

Overlay Network

❑ Overlay Network : Center Track

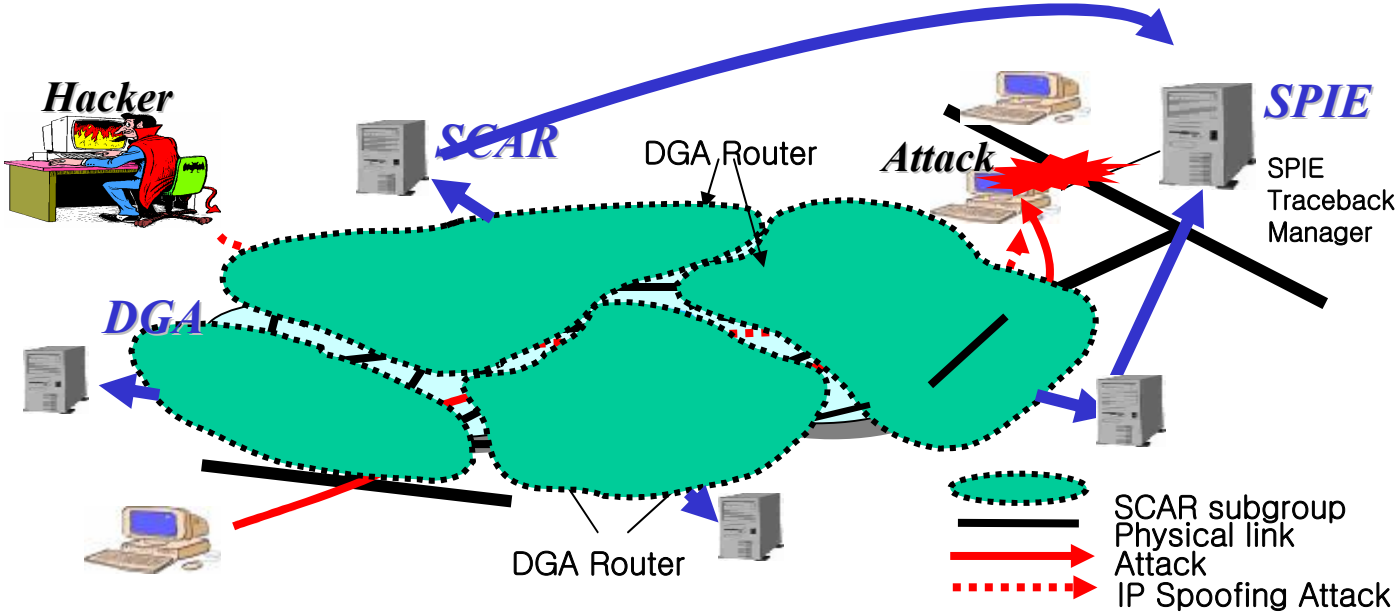
- ❖ Edge routers are connected to a special overlay network composed of **tracing routers via IP Tunnels**
- ❖ In case of attack, **the packets are forwarded to the tracking routers** which follow the stream back to the source of the attack



Hash based IP Traceback

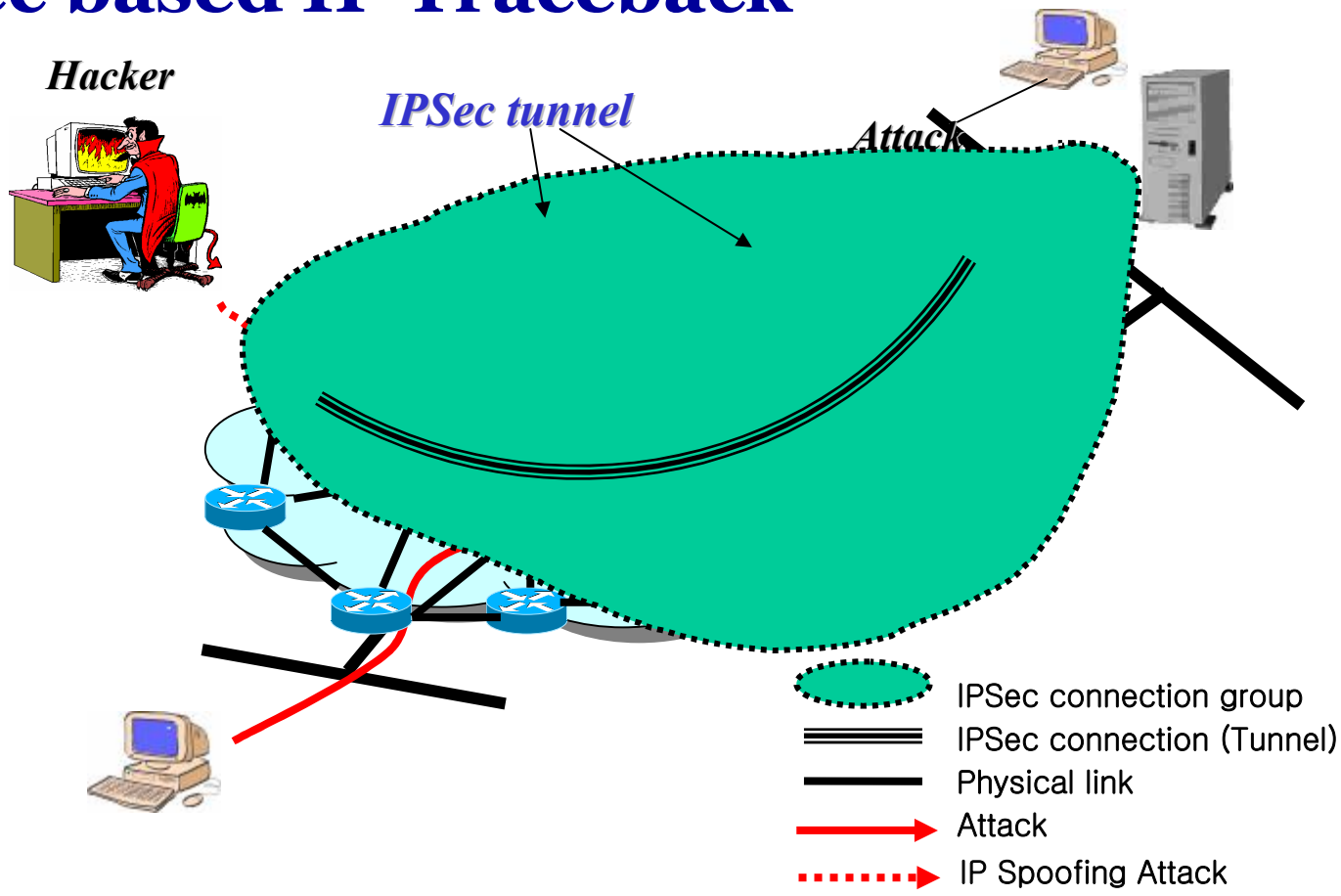
Hash based IP Traceback

- **SPIEs (Source Path Isolation Engines)** are installed in routers, or connected to them
  - **SPIEs generate packet digests from 28 non changing bits in the packet (20 from the header, 8 from the payload).**
  - **The digest is stored in router memory or external storage**



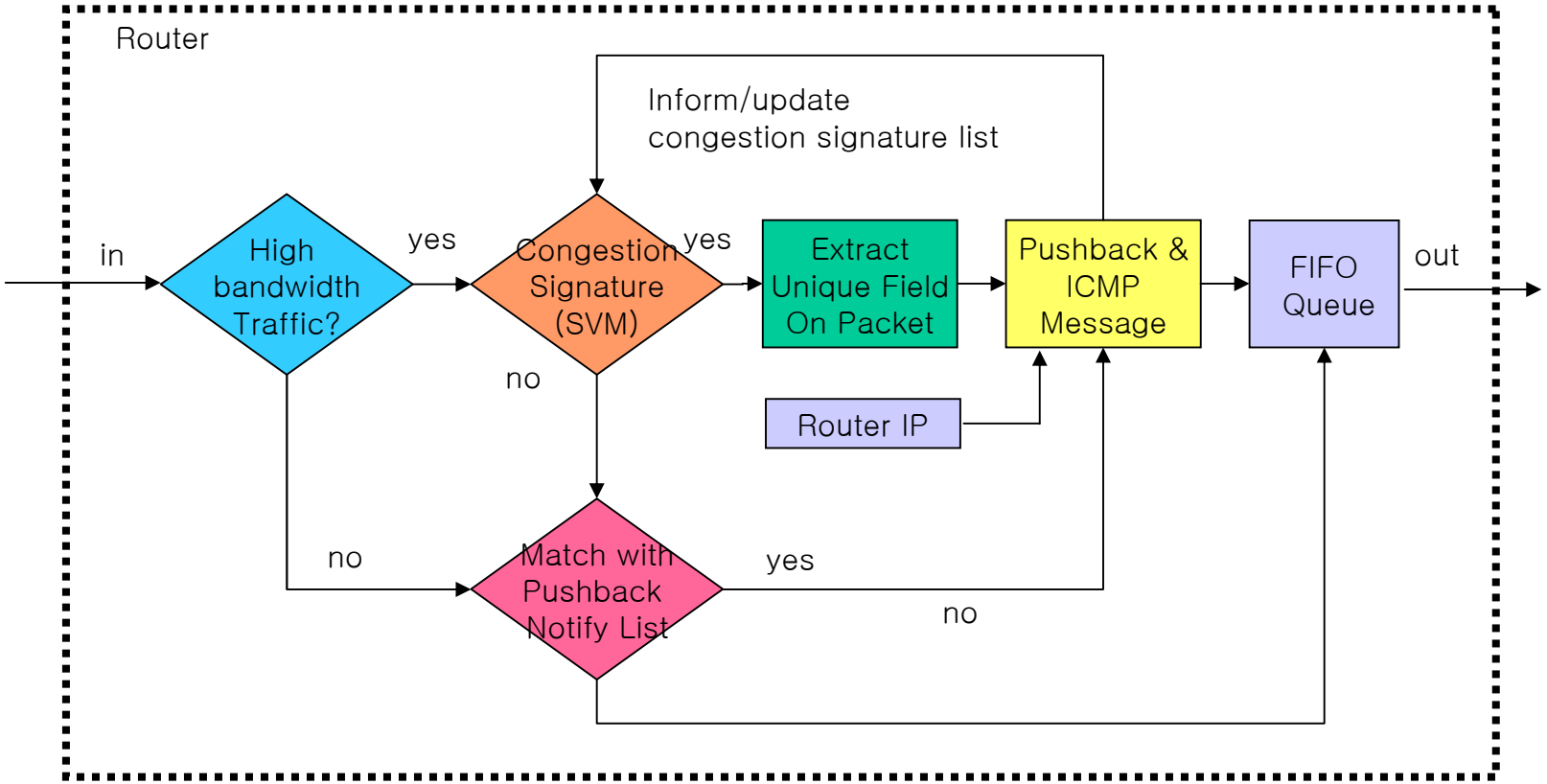
IPSec based IP Traceback

❑ IPSec based IP Traceback



Advanced Mechanism

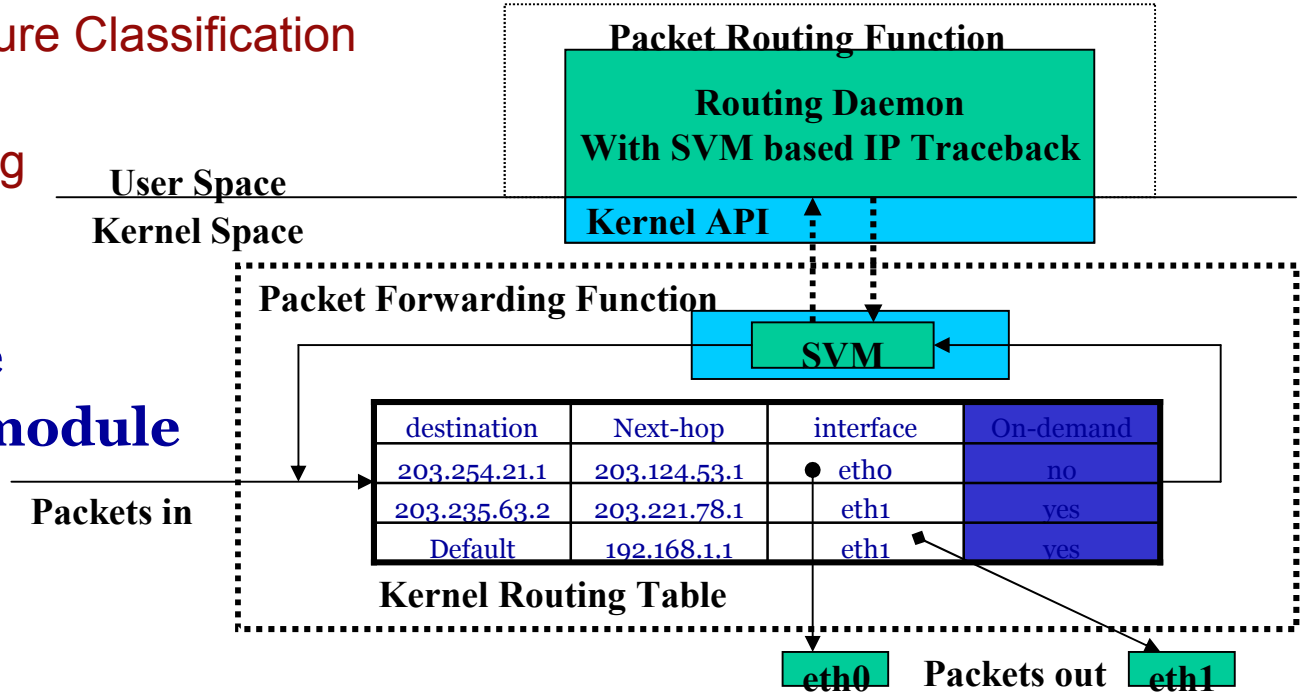
❑ SVM based IP Traceback Mechanism



Pushback Mechanism with SVM

- **Support Vector Machine based IP Traceback**
  - **Inputs are converted into a high dimensional feature spaces, which enable to separate non-linear separable spaces into a proper classes.**
    - Packet Signature Classification with SVM
    - Packet Marking & Traceback

We can combine ACC/Pushback module With SVM for IP Traceback

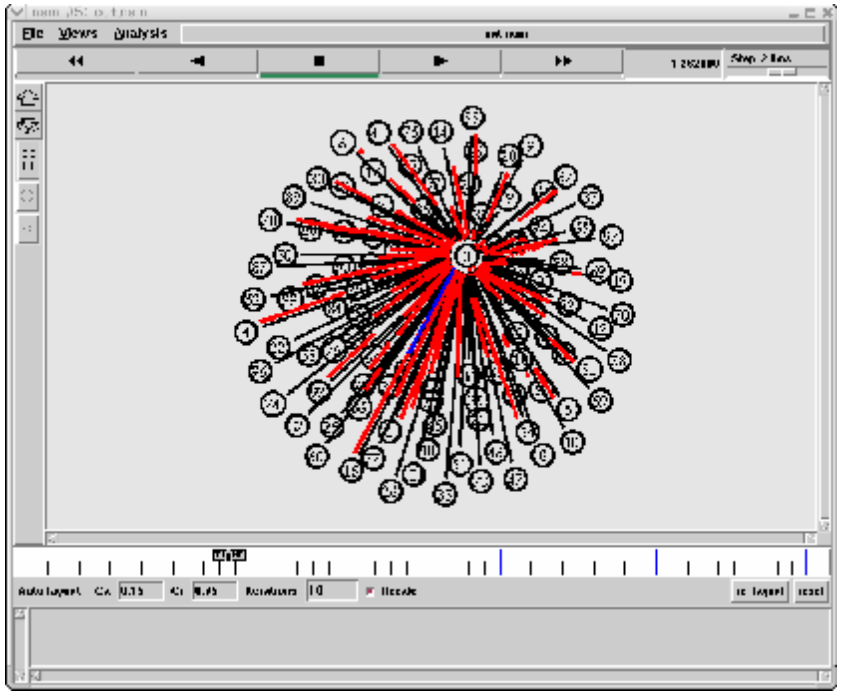


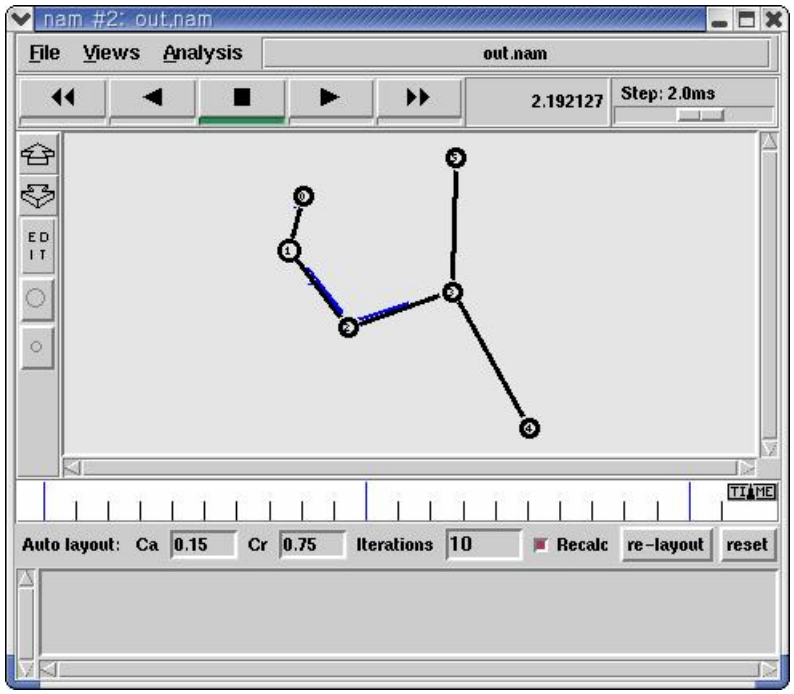
“Simulation and Applications”

- Simulation and Future Works-

Simulation

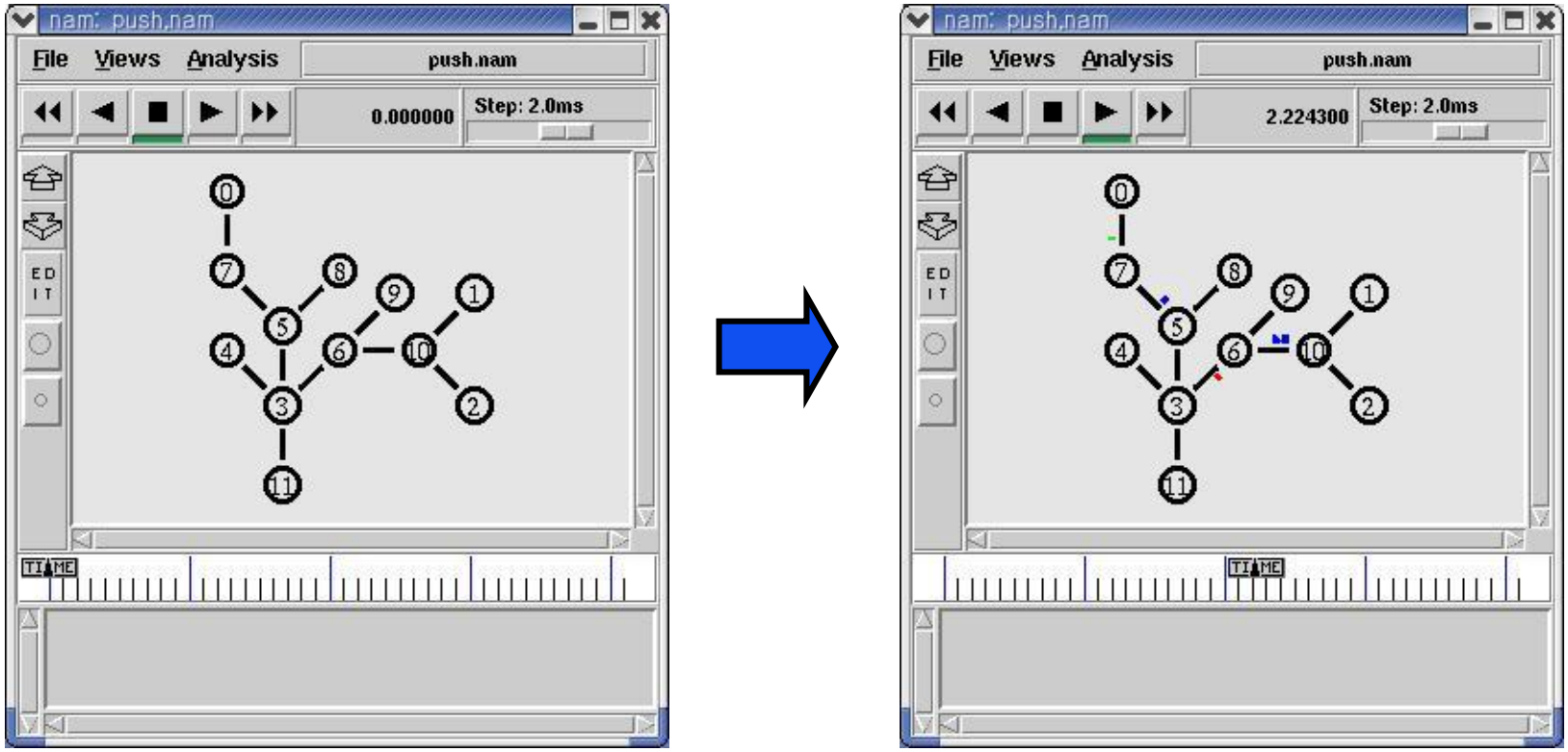
- **Simulate on ns-2 in Linux 9.0**
  - **Ns-2 2.26 / gTraceback module**





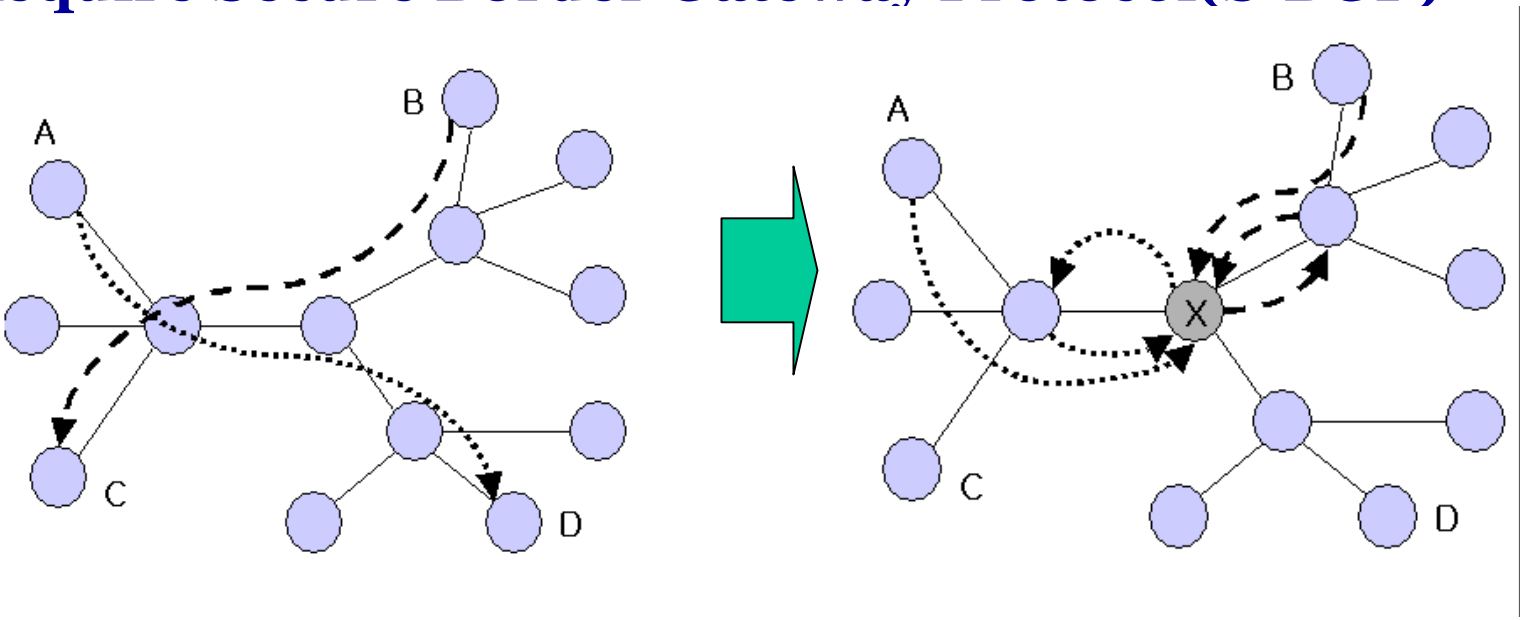
Simulation

- **Simulate on ns-2 in Linux 9.0**
  - **Ns-2 2.26 / gTraceback module**



Secure Router with IP Traceback

- **Router based Inter-networking**
  - **Routing table modification (attack)**
  - **Require Secure Border Gateway Protocol(S-BGP)**



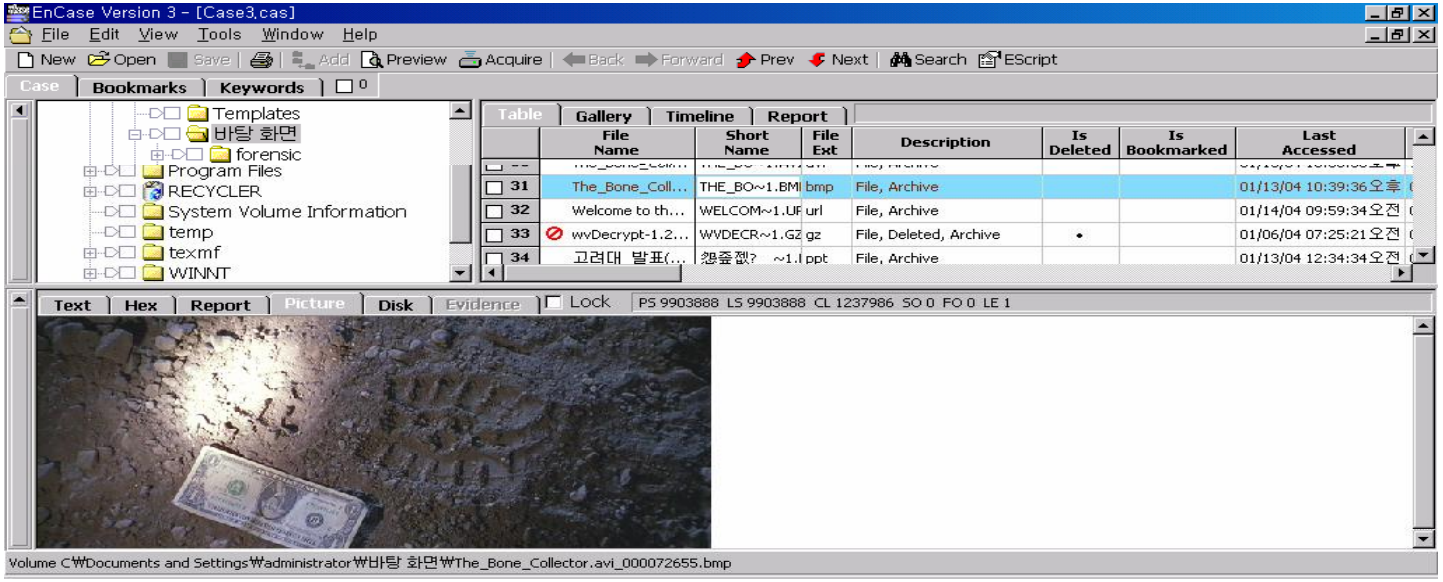
  - **IP Traceback Embedded Router ?**

Computer Forensic with IP Traceback

❑ Chain of Custody

❖ Digital Transaction and its real IP

- ➢ Require IP Traceback system

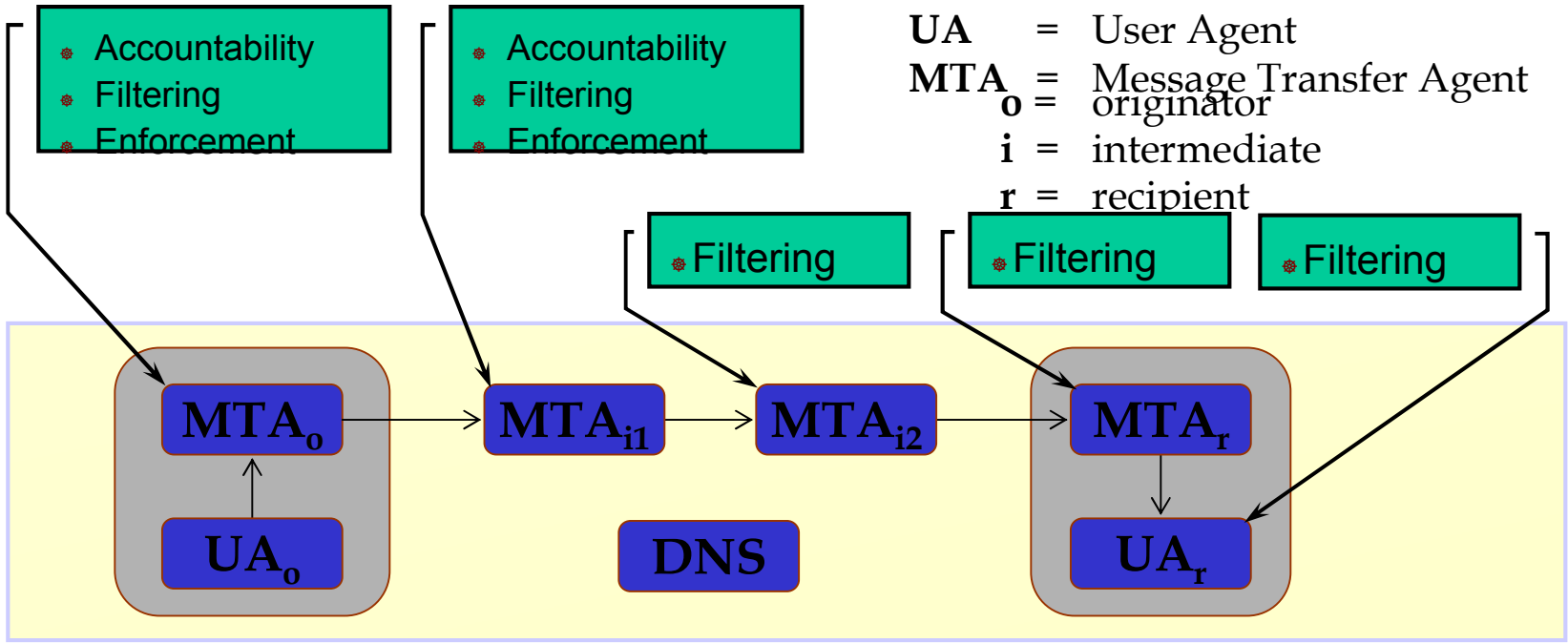


❖ IP Traceback Embedded System ?

SPAM Protection with IP Traceback

SPAM mail Protection

- SMTP based SPAM Protection
- Require Control Mechanism : Real IP and Real Sender



- SPAM Black IP Traceback on SMPT Protocol ?

Conclusion

- Review DDoS Attack
- Providing a Solution on DDoS Attack
  - Proactive/Reactive IP Traceback Technique
- Review on Detailed IP Traceback Mechanism
  - Packet Marking / ICMP Traceback (iTrace) / Network based Mechanism / Advanced IP Traceback Scheme
- Simulation Results with Applications
  - Ns-2 based simulation and Applications
- Future Works
  - Require more research on the IP Traceback for providing enhanced performance, safety and function.
  - Research on the Advanced Application on IP Traceback

References

1. **Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, Network Support for IP Traceback, IEEE/ACM Transactions on Networking, 9(3):226-237, June 2001. (***)**
2. **Savage, Wetherall, Karlin, Practical Network Support for IP Traceback, Proceedings of the 2000 ACM SIGCOMM Conference, August 2000. (***)**
3. **Alex C. Snoeren (MIT), Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, W. Timothy Strayer (BBN Technologies), Hash-Based IP Traceback (Best Student Paper) 2001 SIGCOMM (**)**
4. **Dawn Song, Peridg, Advanced and Authenticatd Marking Schemes for IP Traceback IEEE Infocom 2001 (***)**
5. **Dean, Franklin, An Algebraic Approach to IP Traceback, Network and Distributed System Security Symposium, 2001 (*)**
6. **K. G. Anagnostakis, S. Ioannidis, S. Miltchev, J. Ioannidis, M. Greenwald, J. M. Smith, Efficient Packet Monitoring for Network Management, Proceedings of IFIP/IEEE Network Operations and Management Symposium (NOMS) 2002 (*)**
7. **K. Park and H. Lee. On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack, *Proc. IEEE INFOCOM '01*, 2001. (**)**
8. **Micah Adler, Tradeoffs in Probabilistic Packet Marking for IP Traceback, Proceedings of 34th ACM Symposium on Theory of Computing (STOC) 2002. (*)**
9. **Hal Burch, W Cheswick, "Tracing Anonymous Packets to Their Approximate Source", Proceedings of 2000 Systems Administration Conference (*)**
10. **Jun Li (UCLA), Jelena Mirkovic, Mengqiu Wang, Peter Reiher, Lixia Zhang, *SAVE: Source Address Validity Enforcement Protocol*, Infocom 2002 (*)**
11. **Brian Carrier (Purdue University), Clay Shields (Georgetown University), A Recursive Session Token Protocol for use in Computer Forensics and TCP Traceback, Infocom 2002**
12. **Tom Dunigan, "Backtracking Spoofed Packets", ORNL/TM-2001/114, October, 2000, (ps, 120KB)**
13. **Robert Stone, UUNET Technologies, Inc., CenterTrack: An IP Overlay Network for Tracking DoS Floods, in Proceedings of 9th USENIX Security Symposium, Denver, CO, Aug. 2000.**
14. **K. Park and H. Lee. A proactive approach to distributed DoS attack prevention using route-based packet filtering. Technical Report CSD-TR-00-017, Purdue University, Dept. of Computer Sciences, December, 2000.**

“Thanks”

- Q & A –

Hyung-Woo Lee
Dept. of Software, Hanshin Univ.
Korea
hwlee@hs.ac.kr