State Key Laboratory of Networking & Switching Technology

Beijing University of Posts & Telecommunications

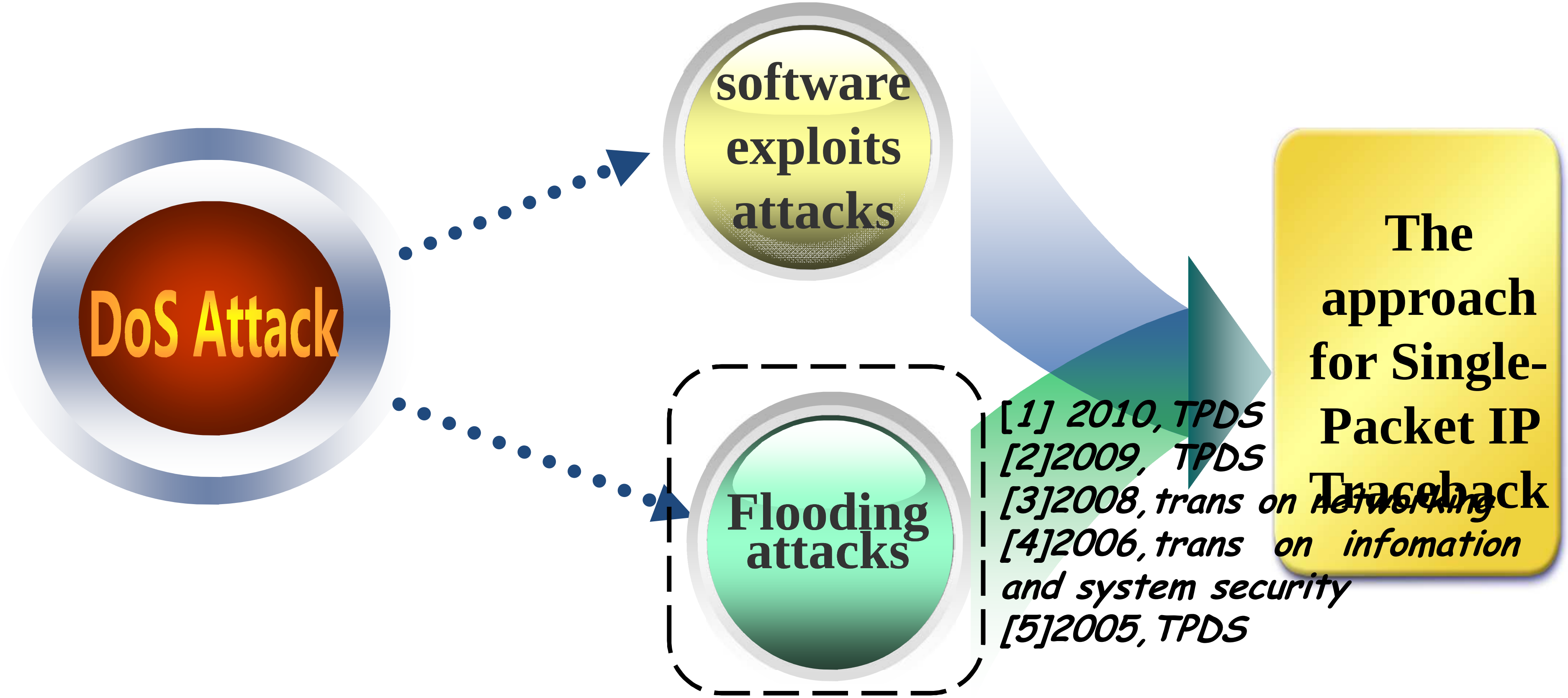
A Novel Approach for Single-Packet IP Traceback Based on Routing Path

Lu Ning
2012-2-13

Outline

- *Background*
- *Related Work and Motivation*
- *Approach Overview*
- *Performance Evaluation*
- Reference

Background



DoS Attack

software exploits attacks

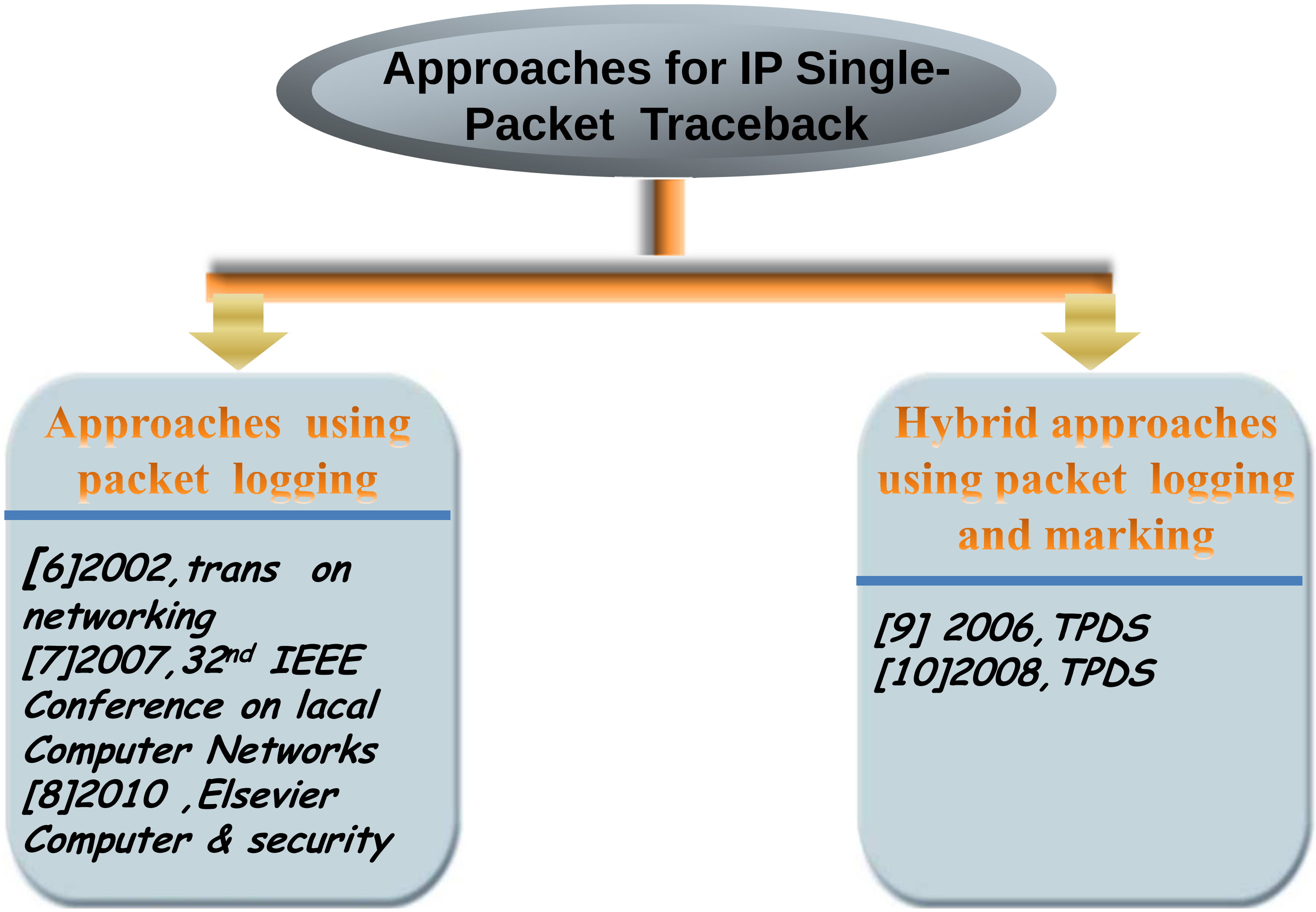
Flooding attacks

The approach for Single-Packet IP Traceback

[1] 2010, TPDS
[2]2009, TPDS
[3]2008, trans on networking
[4]2006, trans on infomation and system security
[5]2005, TPDS

Related work and Motivation

- Related work



Approaches for IP Single-Packet Traceback

Approaches using packet logging

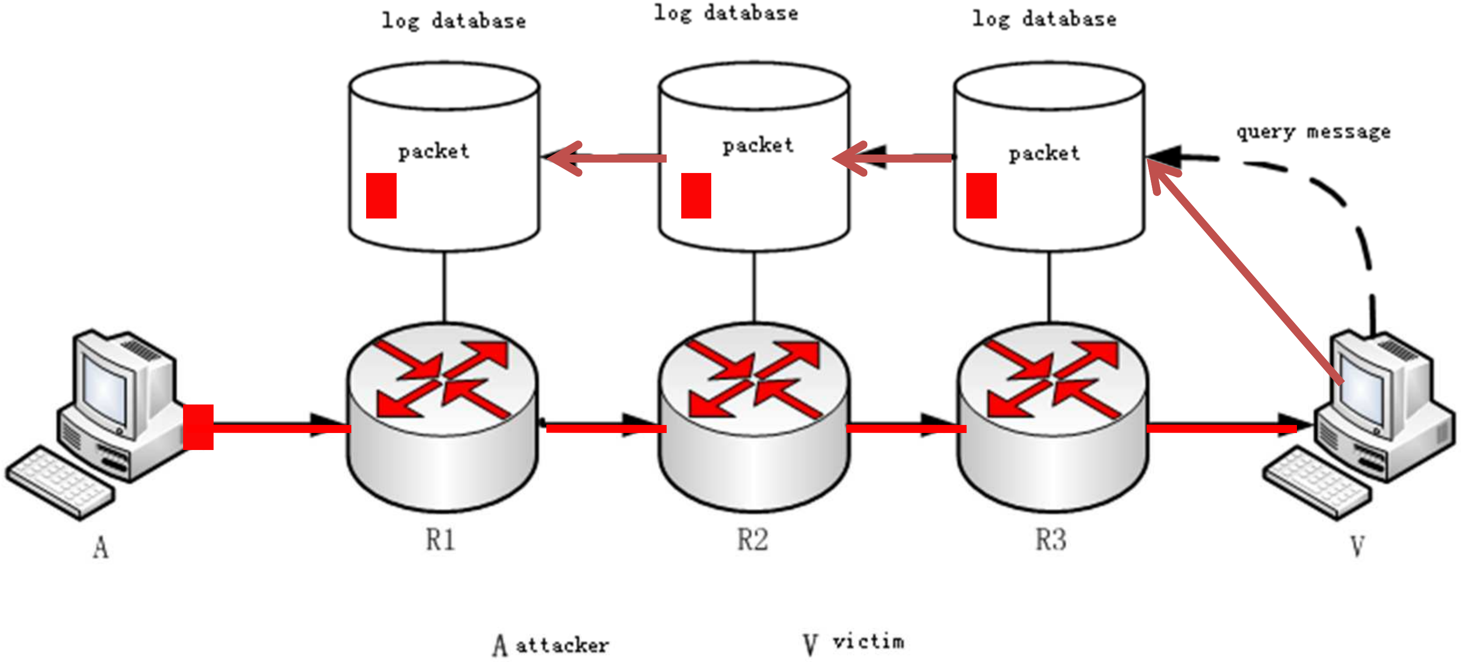
[6]2002,trans on networking
[7]2007,32nd IEEE Conference on lacal Computer Networks
[8]2010 ,Elsevier Computer & security

Hybrid approaches using packet logging and marking

[9] 2006,TPDS
[10]2008,TPDS

Related work and Motivation

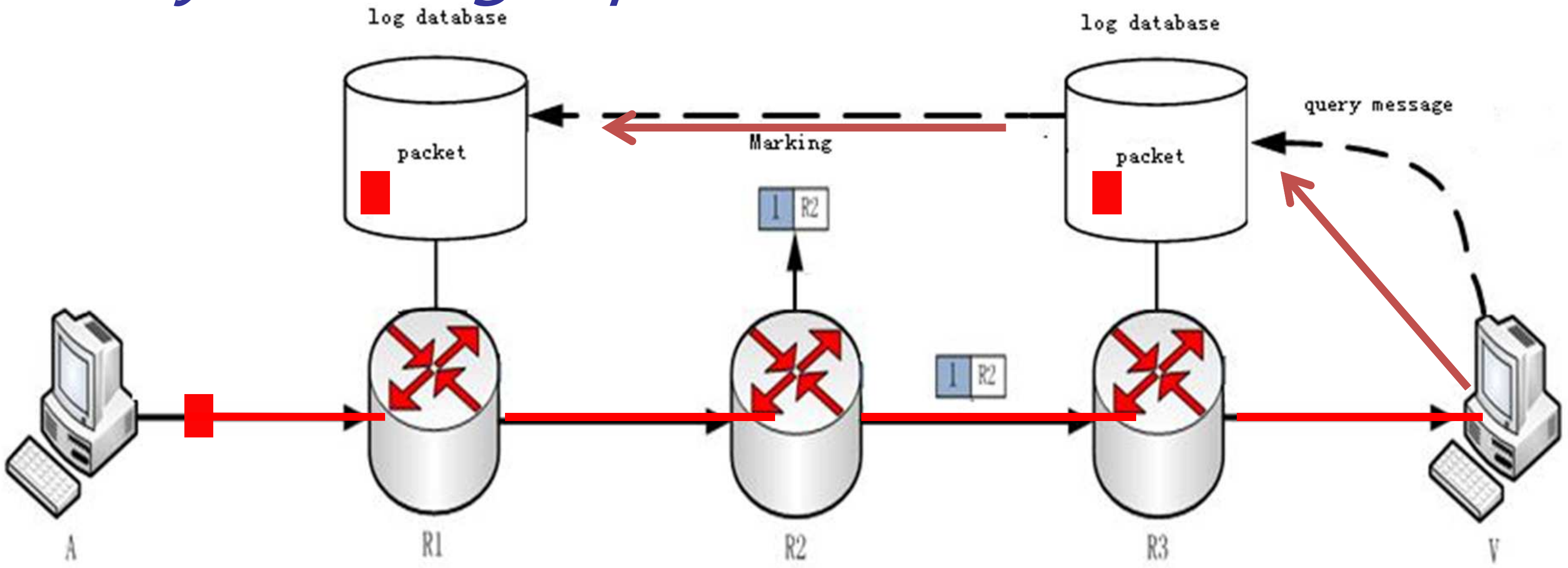
- *Log-based single-packet IP traceback*



Packets are logged by the routers on the path toward the destination. The network path is then derived based on the logged information. This approach is also known as SPIE.

Related work and Motivation

- *hybrid single-packet IP traceback*

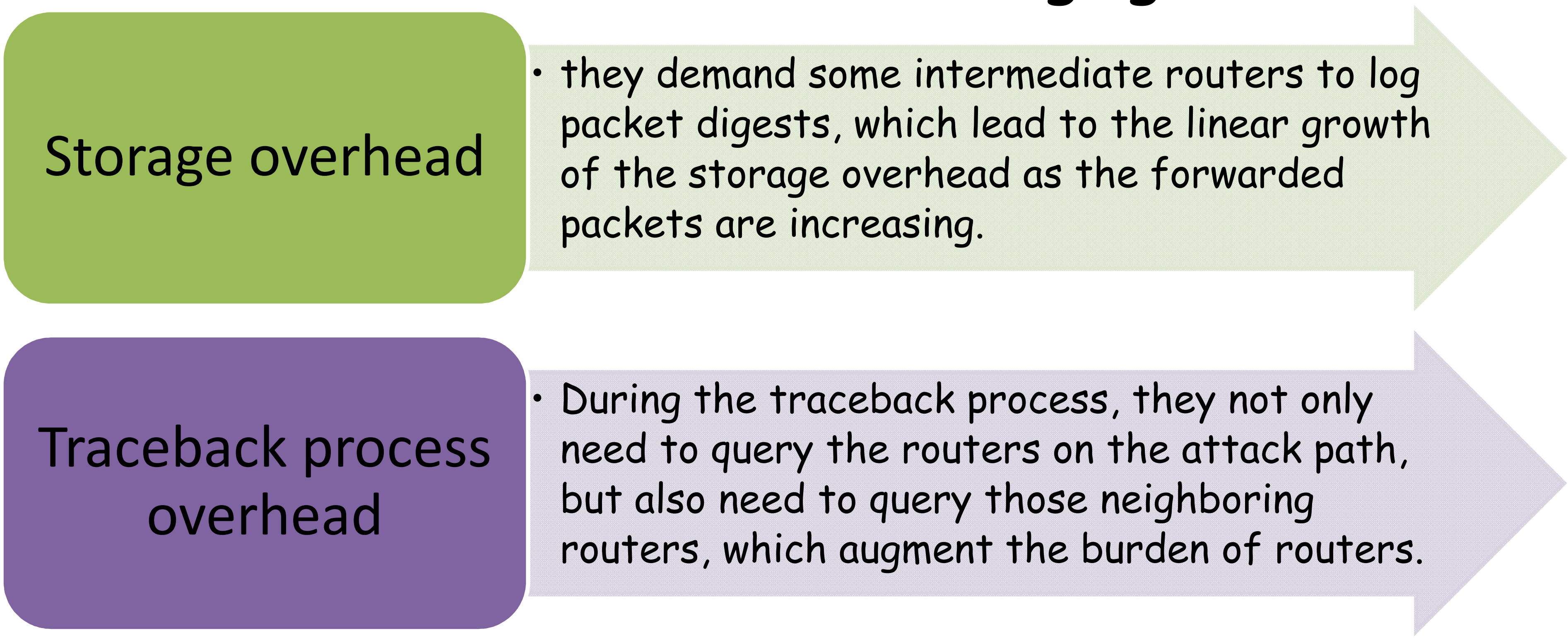


While a packet is traversing the network, the most recent routers write their identification information into a header filed of the packet, and the upstream routers log the packet digests. This approach is also known as hybrid single-packet IP traceback, referred as HIT.

Related work and Motivation

- *Problem Description*

The two approaches deployment at high-speed network has still been two challenging:



Storage overhead

- they demand some intermediate routers to log packet digests, which lead to the linear growth of the storage overhead as the forwarded packets are increasing.

Traceback process overhead

- During the traceback process, they not only need to query the routers on the attack path, but also need to query those neighboring routers, which augment the burden of routers.

Related work and Motivation

- *Motivation*

  » The heavy burden of the routers brought by these algorithms makes the ISP reluctant to deploy the traceability system on the internet. Thus, how to reduce the storage overhead and traceback process overhead, and give ISP incentives to deploy the traceability system

Approach Overview

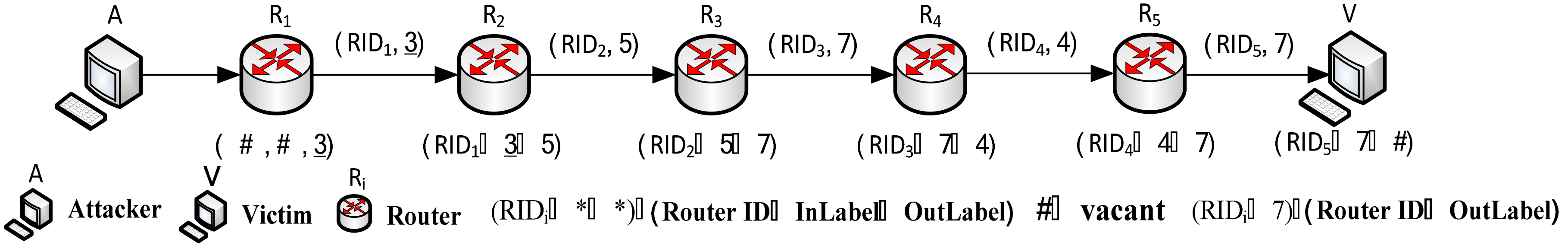
- **Basic theory**
  - Attack packets with different source addresses may possess the same routing.[13]
  - The end-to-end routings will not change frequently. [14]

Approach Overview

- **Main idea**
  - Introduce the relevant theories of LSP in MPLS and set up a traceback path in IP , which is reverse to the routing path and named as traceback path, referred as TP.

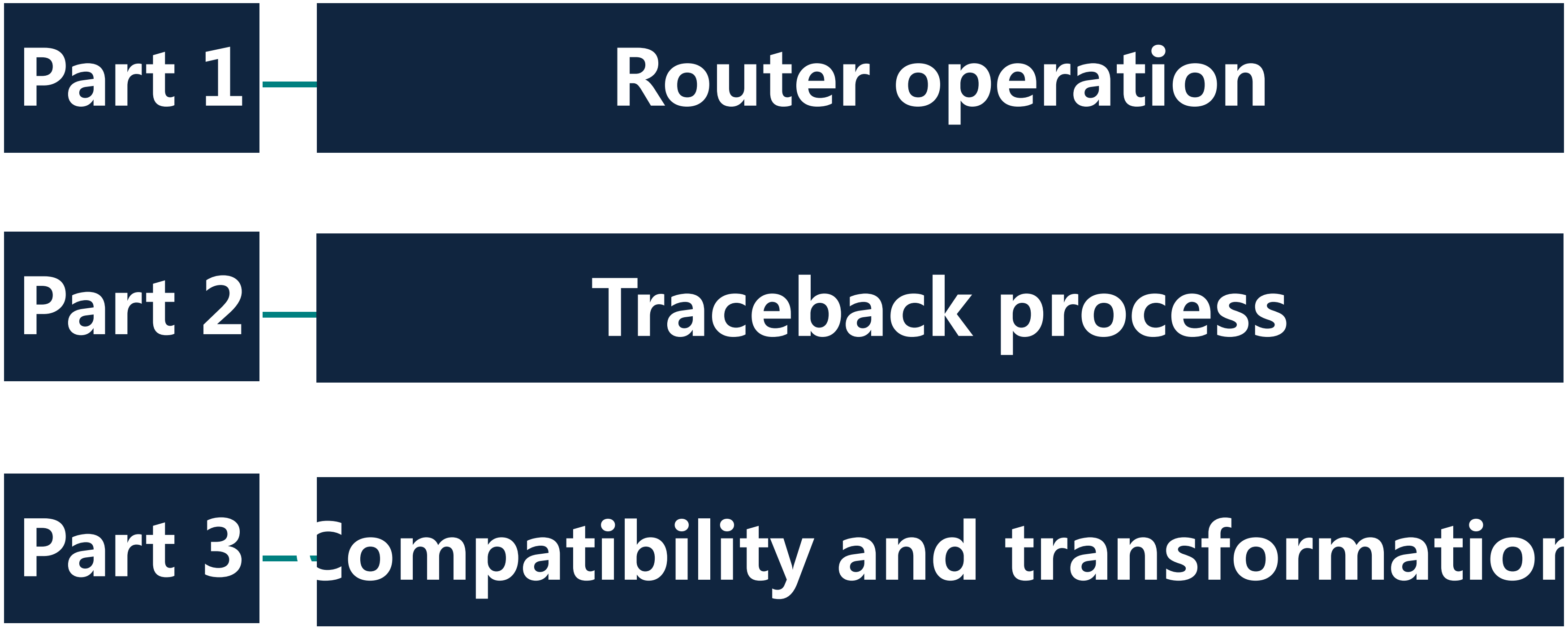
Approach Overview

Model



Routers will assign a sole label$_{out}$ to each label switching path that passes it. When IP package is transmitted in the LSP, routers will write the label$_{out}$ corresponding to that package in the package as a label message.

Approach Overview



Part 1

Router operation

Part 2

Traceback process

Part 3

Compatibility and transformation

Approach Overview part 1

- **Router operation**
  - We can set up label switching path by making use of the transmission of IP package among routers which could transmit label information.

  - IP package could be transmitted by the routers on certain built label switching path which is composed of the label switching items.

Approach Overview part 1

- **Key technologies of Router operation**
  - Routing paths partition
  - Label assignation
  - Packet marking
  - Traceback Path Table

Approach Overview part 1

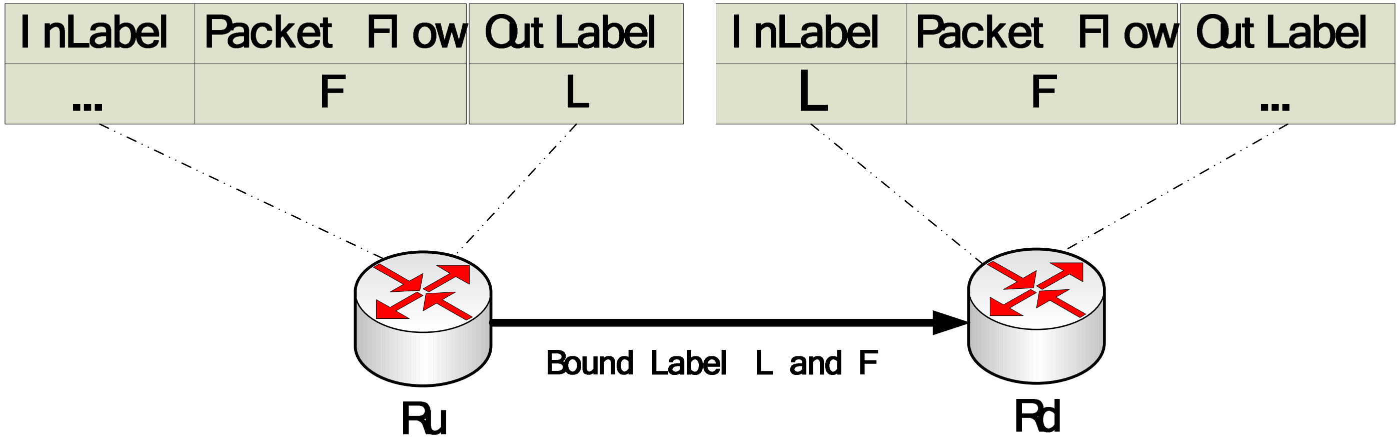
Routing paths patition

- Each router partitions the pass-by routing paths according to their different destinations.
- UDR: the routing paths with the same destinations.
- DDR: the routing paths with different destinations.

Approach Overview part 1

Label assignation

- For all the routing paths in a group of UDR, the router assigns distinct labels$_{out}$ to them so as to ensure the diversity that could distinguish them.
- For all the routing paths in the DDR, the router assigns labels$_{out}$ to them at random.



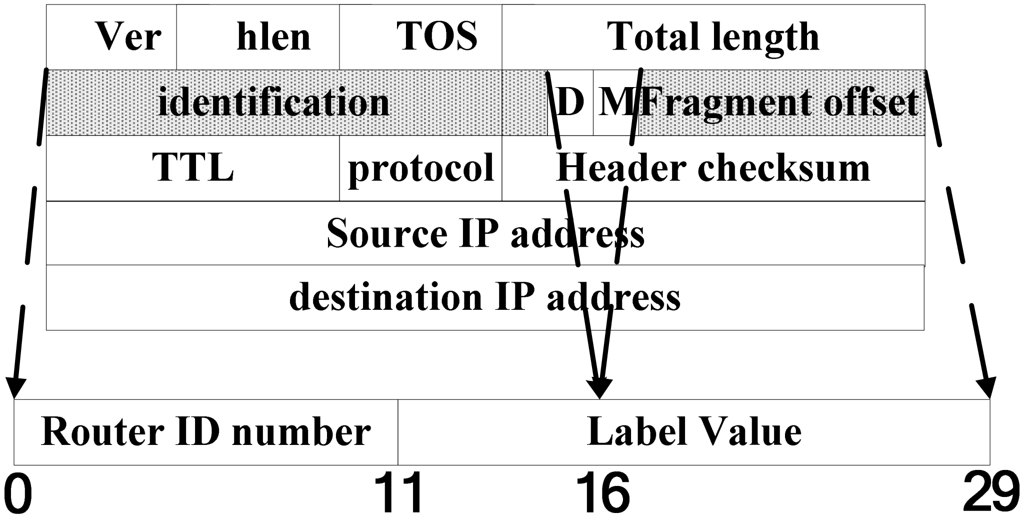
InLabel	Packet Flow	Out Label
...	F	L

InLabel	Packet Flow	Out Label
L	F	...

Approach Overview part 1

- **Packet marking**

[10][11][12]



Ver hlen TOS Total length

identification D M Fragment offset

TTL protocol Header checksum

Source IP address

destination IP address

Router ID number Label Value

0 11 16 29

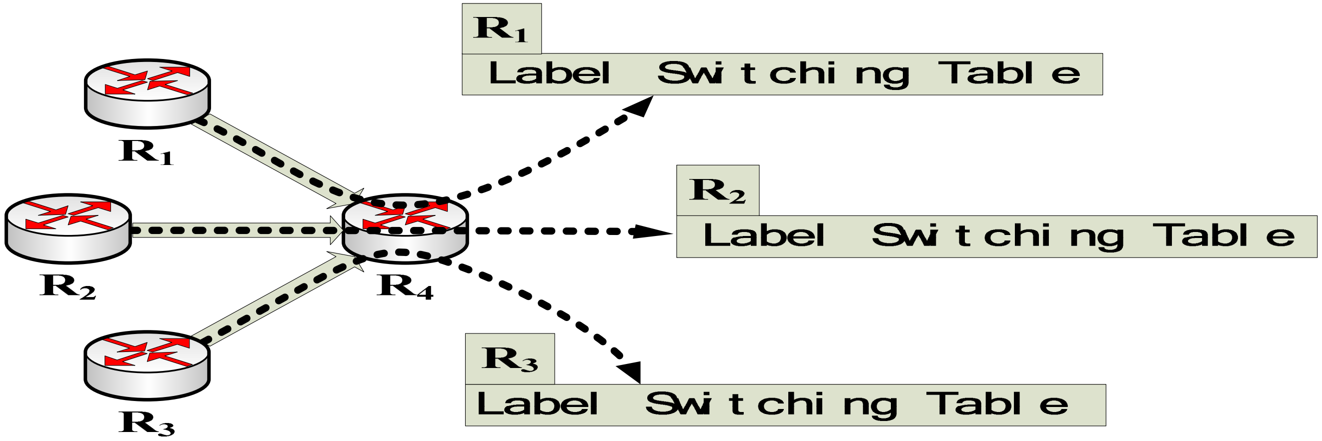
In order to fit the router ID number and label into one packet, we use 16-bit identification field and 13-bit fragment offset field in the IP header, which referred as marking field.

Approach Overview part 1

- **Traceback Path Table**

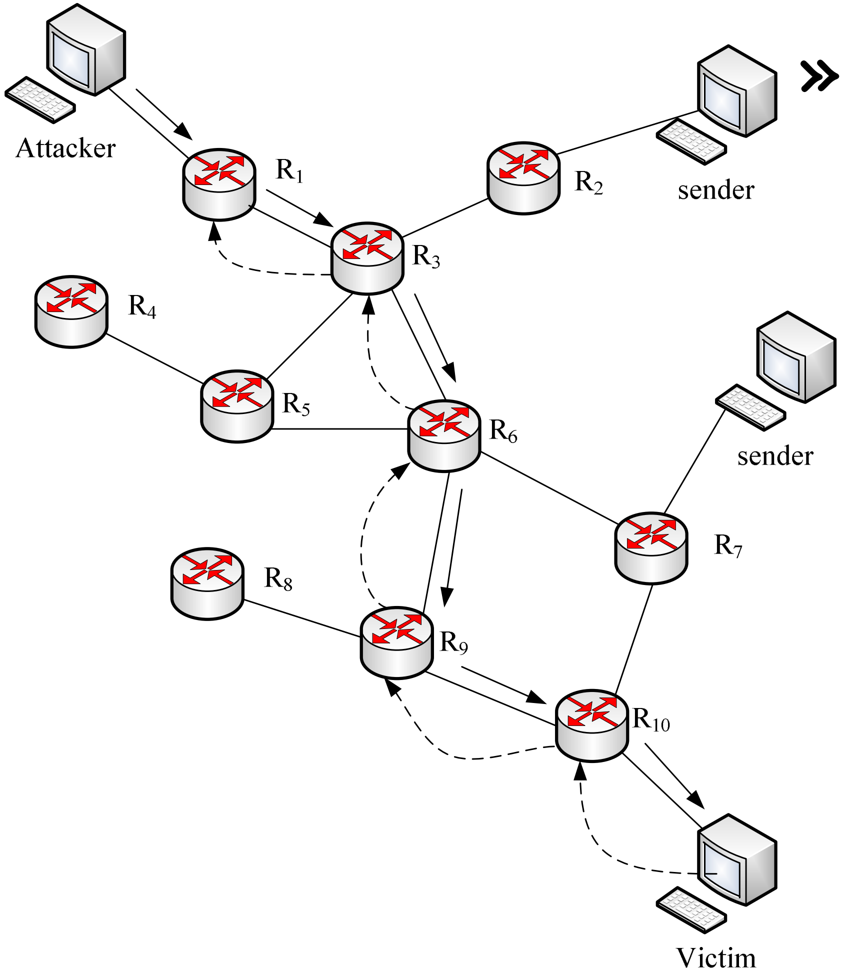
» Be composed of several Traceback Path Blocks.

» In order to accelerate the processing speed of routers , each router can simultaneously maintain several traceback path tables which are related to one or more destination IP addresses.


R₁
Label Swi t chi ng Tabl e
R₁
R₂
Label Swi t chi ng Tabl e
R₂
R₄
R₃
Label Swi t chi ng Tabl e
R₃

Approach Overview part 2

- Traceback process



» Given victim V , packet P and the time of attack T , traceback server can pinpoint the last-hop router based on the location of V and the router ID number carried by P. Then we can revert to the complete attacking path.

Approach Overview part 3

Compatibility and transformation

In order to achieve the backward compatibility and trace packets undergoing transformation, our approach improves the following steps:

If the packet P is an IP fragment and not transformed at the current router

- The router store the digest of P

If the packet P is an IP fragment and transformed at the current router

- The router record the transformation information and store the digest of P

If the packet P is a nonfragmented and transformed at the current router

- The router computes the digest of P with the same packet prefix, then records the transformation information.

Performance evaluation

- **Storage Overhead**

Packet Type	Percentage
1.IP fragments	α
2.IP fragment and transformed packets at the current router	$\alpha\beta$
3.IP fragment or transformed packets at the current router （include 2 above）	$\alpha+\beta-\alpha\beta$
4.non-fragment packets and not transformed at the current router	$1-(\alpha+\beta-\alpha\beta)$

Consider all packets forwarded by a router R. Assume that the percentage of IP fragment is α, and the percentage of P packets undergoing transformation at the router is β. Then, the percentage of different types of IP packets in all packets forwarded by a router can be expressed as this table.

Performance evaluation

- ## Storage Overhead

We assume that the number of IP packets that arrive at the router R per unit time is n, and the number of routing paths, on which the packets traverse, is S. Let STP_x, STP_y and STP_z denote the number of items logged at the router in our approach, HIT and SPIE.

$$STP_x = S + n \times \left(\alpha + \beta - \alpha\beta\right) \qquad STP_y \approx 0.5 \times n$$

$$STP_Z = n$$

Measurement studies have shown that α≤0.25%, β≤3% [11][12], so

$$STP_X \leq STP_y < STP_Z$$

Performance evaluation

- **Traceback process overhead**

Suppose an attack path has n hops and each router on the attack path has m neighboring routers on the average. Let NRx、NRy and NRz denote the number of routers queried during the traceback process in our approach, HIT and SPIE.

$$NR_x = n - 1 \qquad NR_Z = (m-1) \times n$$

$$NR_y = (m-1) \times 1/2 \times \mathrm{n}$$

Measurement studies show that m in the AS-Level internet topology is about 6.3 [13], so

$$NR_X \le NR_y < \mathrm{NR}_Z$$

Reference

[1]S.Yu, W.zhou, and R.Doss, “Traceback of DDoS Attacks using Entropy Variations,” IEEE Transactions on Parallel and Distributed Systems,2010.

[2] Y.Xiang, W.zhou, and M.Guo, “Flexible Deterministic Packet Marking:An IP Traceback System to Find the Real Source of Attacks , ” IEEE Transactions on Parallel and Distributed Systems,2009.

[3]M.T.Goodrich, “Probabilisitic Packet Marking for Large-Scale IP Traceback, ” IEEE/ACM Transactions on Networking, 2008.

[4]D.Dean, M.Franlin, and A.Stubblefield, “An Algebraic Approach to IP Traceback,” ACM Transactions on Information and System Security,2006.

[5]T.K.T.Law, J.C.S.Lui, and D.K.Y.Yau, “You Can Run, But You Can’t Hide: An Effective statistical Methodology to Traceback DDoS Attackers, ”IEEE Transactions on Parallel and Distributed Systems,2005.

[6]A.Snoeren, C.Partridge and L.Sanchea, “Single-Packet IP Trace-back,” IEEE/ACM Trans.Networking, 2002.

[7]R.P.Laufer,R.B.Velloso and D.O.cunha, “Towards Stateless Single-Packet IP Traceback,” 32nd IEEE Conference on Local Computer Network,2007.

[8]E.Hilgenstieler, E.P.Duarte and G.Mansfield-Keeni, “Extensions to the source path isolation engine for precise and efficient log-based IP traceback,” ELSEVIER Computers & Security,2010.

Reference

[9]B.Al-Duwairi, and M.Govindarasu, “Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback,” IEEE Transactions on Parallel and Distributed Systems,2006.

[10]C.Gong, and K.Sarac, “A More Practical Approach for Single-Packet IP Traceback Using Packet Logging and Marking, ” IEEE Transactions on Parallel and Distributed Systems,2008.

[11]M. Muthuprasanna and G. Manimaran, “Space-time encoding scheme for DDoS attack traceback,” ***in Proc. of IEEE GLOBECOM, November 2005.***

[12] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Network support for IP traceback,” ***IEEE/ACM Transaction on Networking, Vol.9, No.3, 2001, pp.226-337.***

[13]V.Paxson, “Measurements and Analysis of End-to-End internet Dynamics,”PhD thesis, U.C. Berkeley,1997.

[14]V.Paxson, “End-to-End routing behavior in the internet ,”ACM SIGCOMM Computer Communication Review,1996.

Thank you!