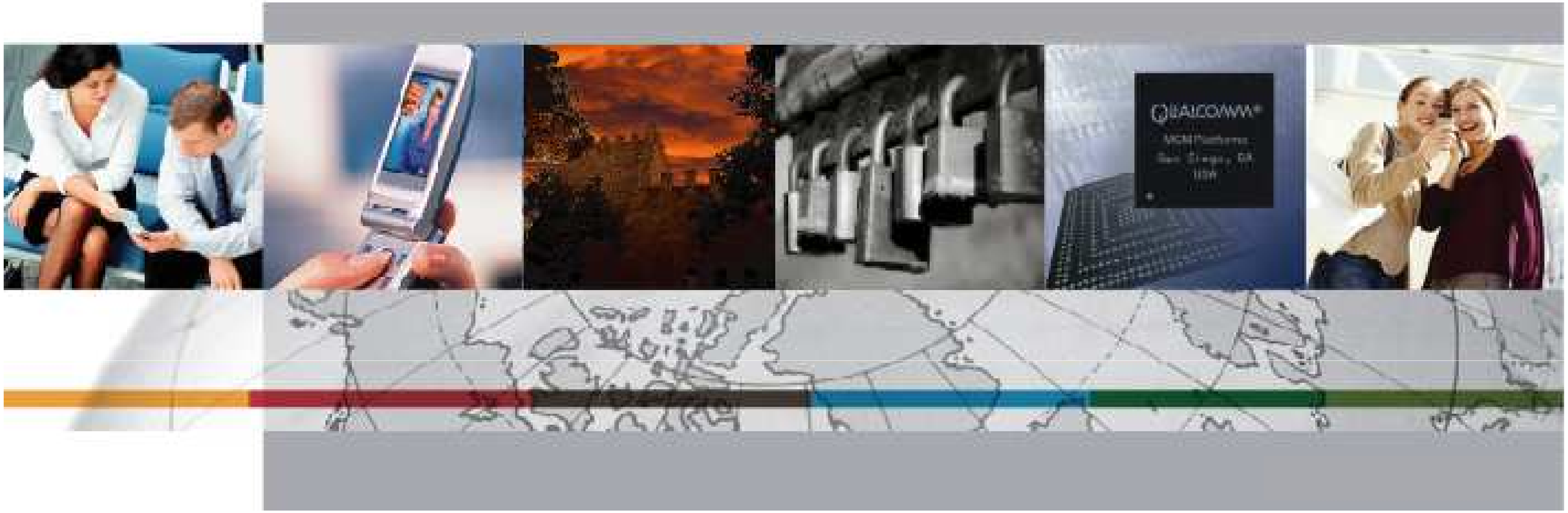
PRODUCT SECURITY INITIATIVE
QUALCOMM



DDoS Attack Traceback and Beyond

Yongjin Kim

Outline

- Existing DDoS attack traceback (or commonly called IP traceback) schemes*
  - Probabilistic packet marking
  - Logging-based scheme
  - ICMP-based scheme
- Tweaking of DDoS attack traceback as a powerful DDoS remedy
- Conclusion

*A. Belenky and Nirwan Ansari, "On IP Traceback", IEEE Communication Magazine

Introduction to DDoS attack traceback

- What DDoS attack traceback does mean?
  - Determine the approximate origin of attack traffic
- What DDoS attack traceback does not mean?
  - Identifying attackers themselves requires forensic means
- Why DDoS attack traceback is difficult
  - IP address can be easily spoofed. Morris wrote, “The weakness in the [Internet Protocol] is that the source host itself fills in the IP source host ID, and there is no provision in… TCP/IP to discover the true origin of a packet.”
  - Stateless nature of the Internet architecture

PRODUCT SECURITY INITIATIVE
QUALCOMM

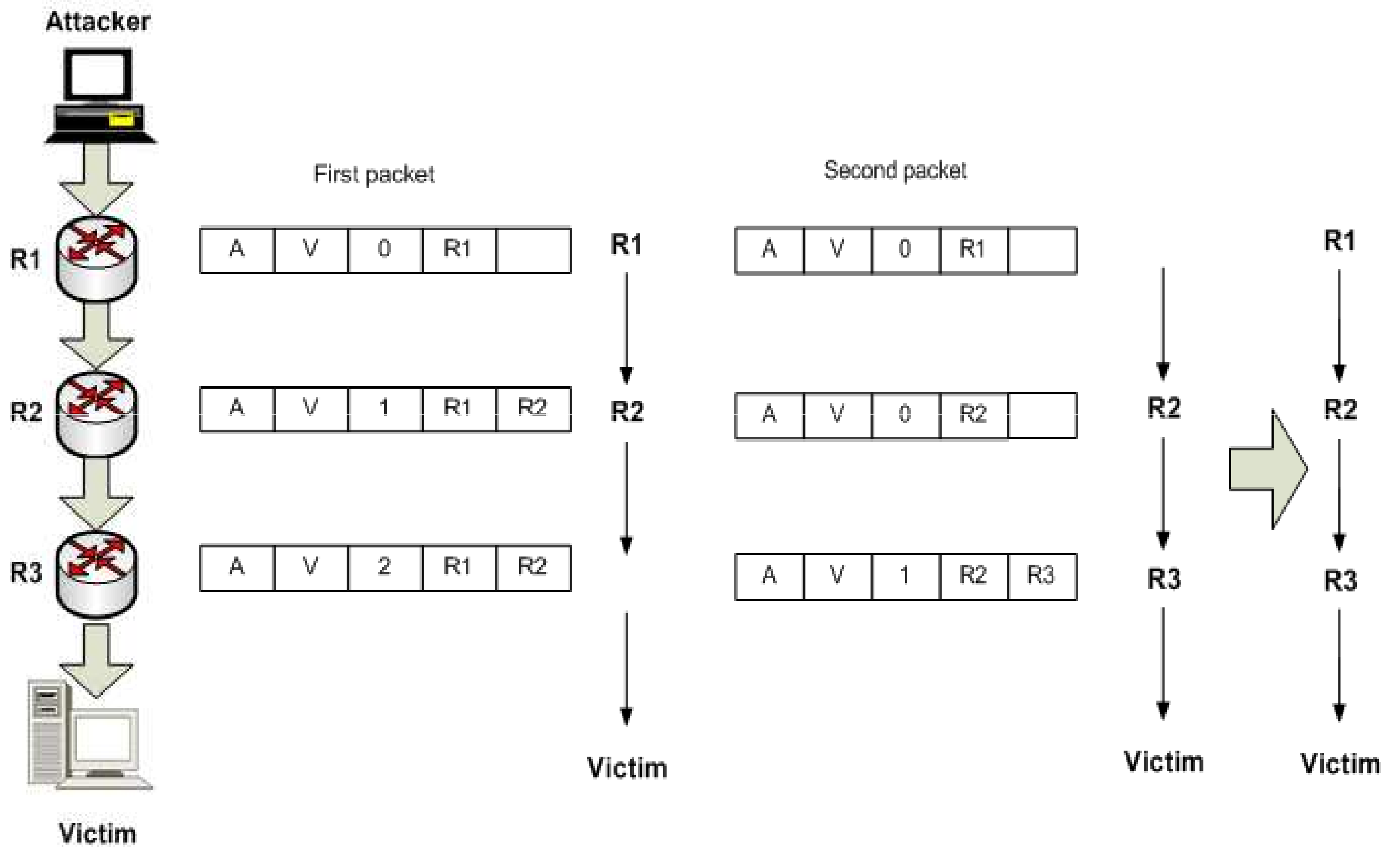
QUALCOMM CONFIDENTIAL AND PROPRIETARY

Existing DDoS Attack Traceback Schemes

Probabilistic Packet Marking

- Routers write their IP address in the IP packet header probabilistically
- Victim receives the marked packets and reconstructs the attacking path from them
- Use constant space in the packet header (e.g., IP identification field) to carry traceback-related information

Basic idea



First packet

A	V	0	R1	
A	V	1	R1	R2
A	V	2	R1	R2

Second packet

A	V	0	R1	
A	V	0	R2	
A	V	1	R2	R3

Research issues

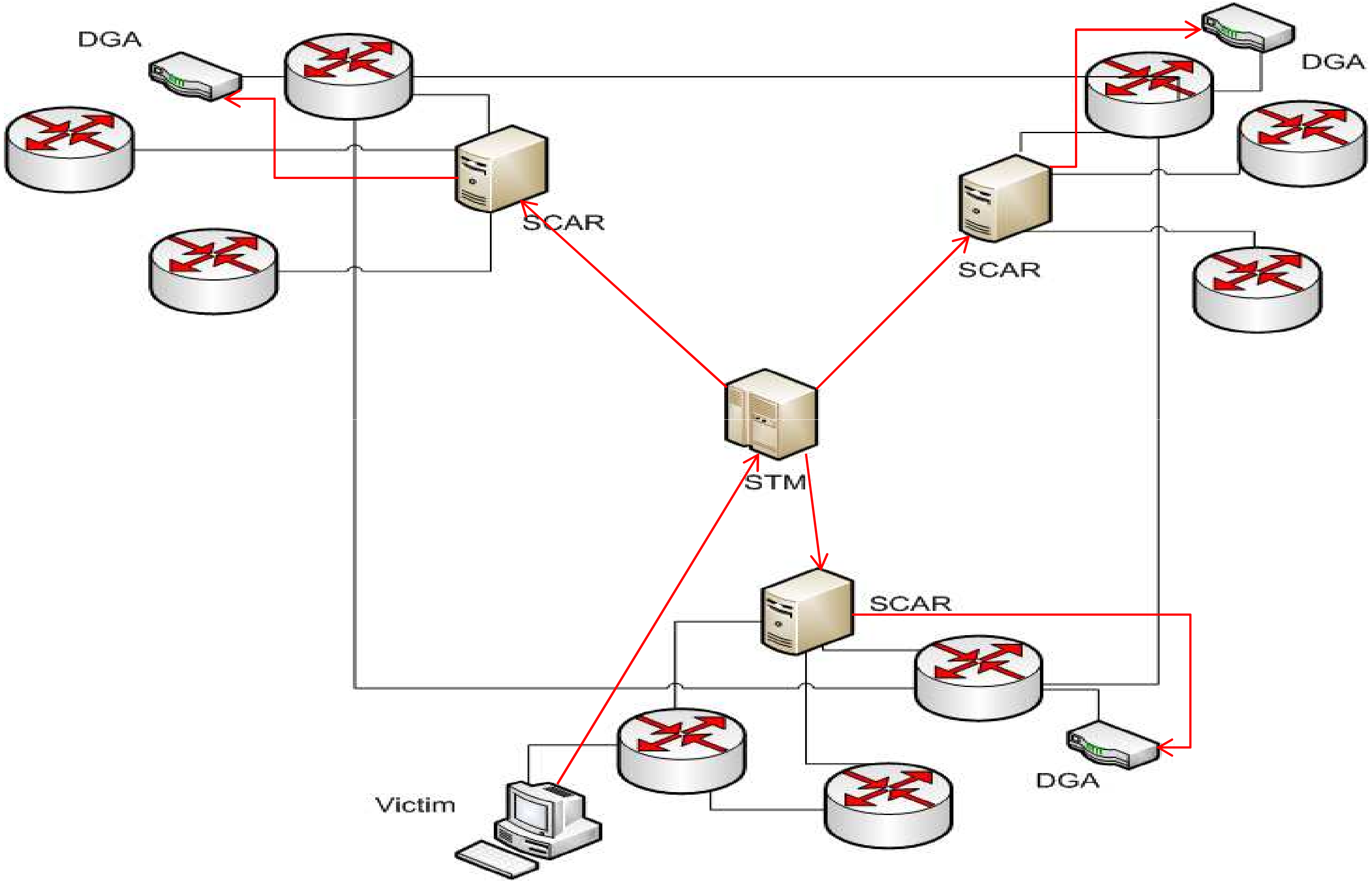
- Compressing traceback-related information to 16 bits of packet identification field
- Packet identification field is not usable under packet fragmentation or IPv6
- Traced packet authentication (MAC, time-released key chain, etc.)
- Partial deployment with legacy routers
- Time required for path reconstruction
- DDoS attack path reconstruction

Logging-based scheme

- Log packets at routers and use datamining techniques to find path
- An attack graph is constructed from a set of attack paths
- Three entities to achieve traceback
  - DGA (Data Generation Agent): Produces packet digests of each departing packet and stores them in a *digest table*
  - SCAR (SPIE[*] Collection and Reduction Agent): When attack is detected, SCAR produces attack graph for it’s region
  - STM (SPIE Traceback Manager): Interface to the intrusion detection system. Gathers complete attack graph

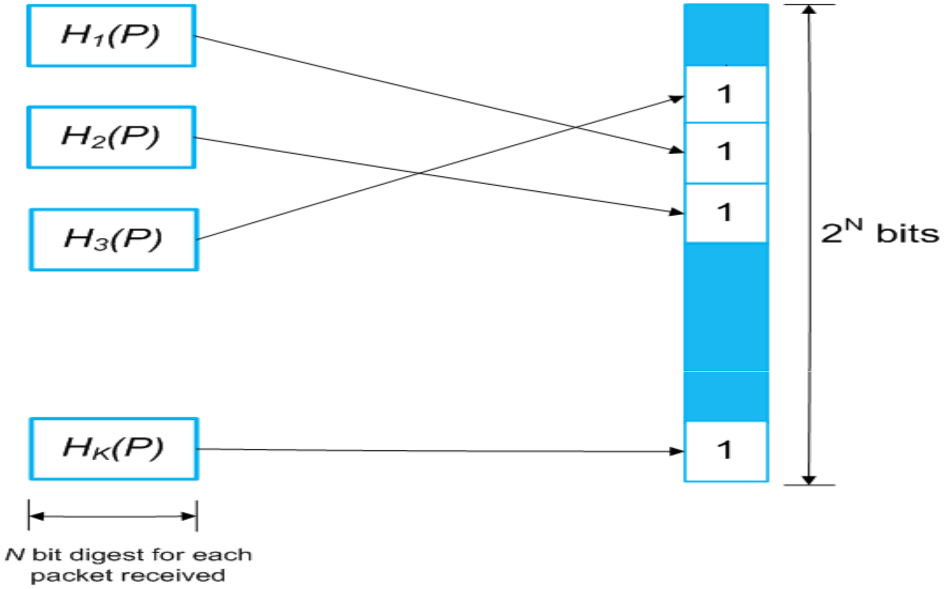
[*] SPIE: Source Path Isolation Engine

Basic idea



Research issues

- Privacy and storage size (Use hash and bloom filter)

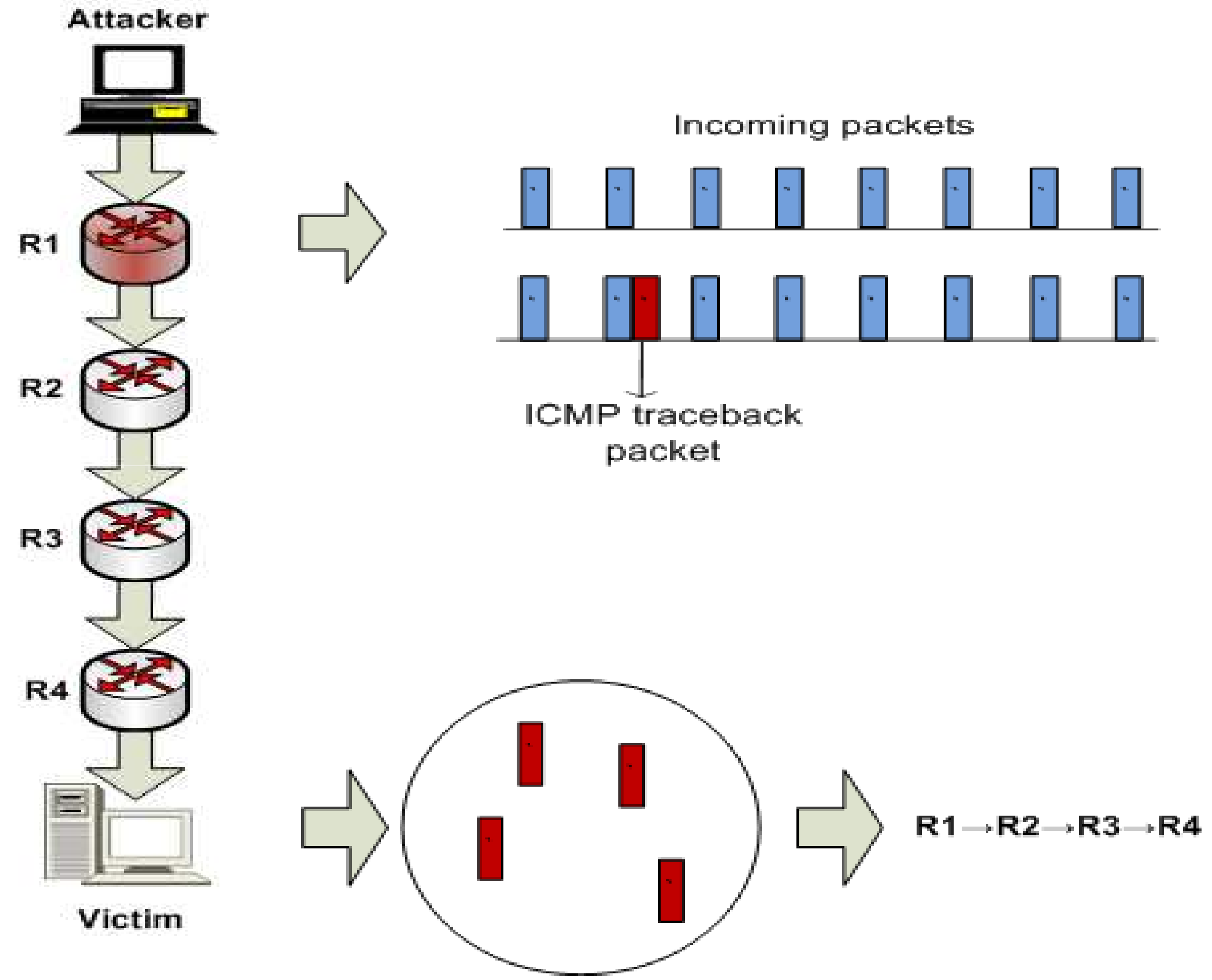


- Queries must be done very soon after the attack, unless the routers have some way of offloading historical data
- For packets transformed through tunnels, NATs,etc., keep TLT (Transform Lookup Table) to allow inversion

ICMP-based scheme

- ❑ Sample packet with low probability (1/20,000)
- ❑ Copy packet data and path information (i.e., next and previous hop information) into a ICMP packet
- ❑ TTL field is set to 255, and is then used to identify the actual path of the attack

Basic idea


Attacker
R1
R2
R3
R4
Victim
Incoming packets
ICMP traceback packet
R1→R2→R3→R4

Research issues

- Large number of packets are required for path reconstruction
- Key distribution to authenticate ICMP packets
- ICMP packets are differentiated and may be filtered or rate-limited
- Input debugging to generate ICMP packets is required

Existing schemes comparison

	Router overhead	Victim overhead	Protocol change	Bandwidth overhead	ISP overhead
Probabilistic Packet marking	**High**	**High**	**Required**	**N/A**	**N/A**
Logging	**Low**	**Low**	**N/A**	**Low**	**High**
ICMP-based	**High**	**High**	**Required**	**High**	**N/A**

CAVEAT: All the schemes require major infrastructure or protocol change

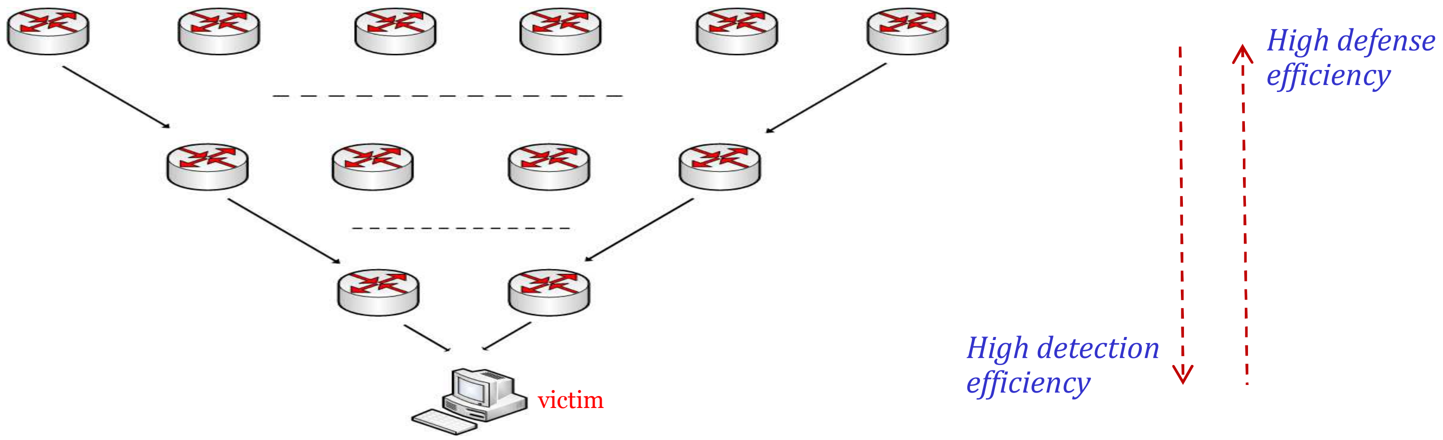
PRODUCT SECURITY INITIATIVE
QUALCOMM

QUALCOMM CONFIDENTIAL AND PROPRIETARY

Tweaking of DDoS Attack Traceback for DDoS Remedy

Dilemma in DDoS defense and detection

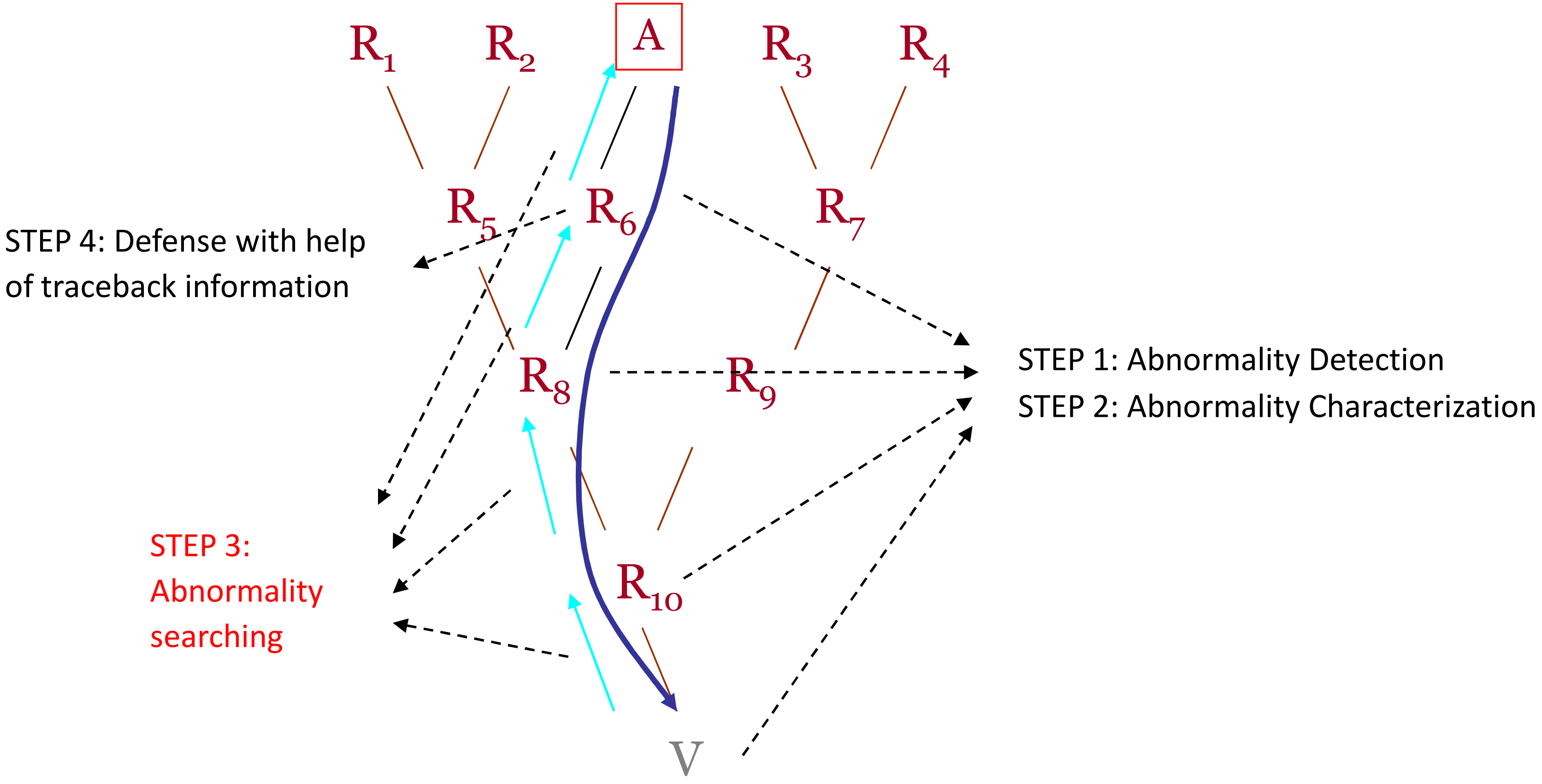
- Defense efficiency drops near victim
  - Defense at the victim is too late to handle large volume
  - Intermediate link is already exhausted
  - Hard to differentiate between legitimate and illegitimate traffic
- Detection efficiency drops near source
  - Not much clue to accurately detect far from victim
  - Misdetection is highly risky on legitimate traffic



Tweaking of DDoS attack traceback

- DDoS attack traceback is a key to resolve the dilemma :
  - Can take countermeasure near attack origin
  - Can increase detection efficiency near attack origin. I.e., reduce legitimate packet filtering
- However, we need to tweak DDoS attack traceback to make it practical and useful
  - Make traceback simple
  - Use existing infrastructure for traceback
  - Add minimal overhead between ISP’s
  - Add defense with traceback information

Tweaked traceback



STEP 4: Defense with help of traceback information

STEP 1: Abnormality Detection

STEP 2: Abnormality Characterization

STEP 3: Abnormality searching

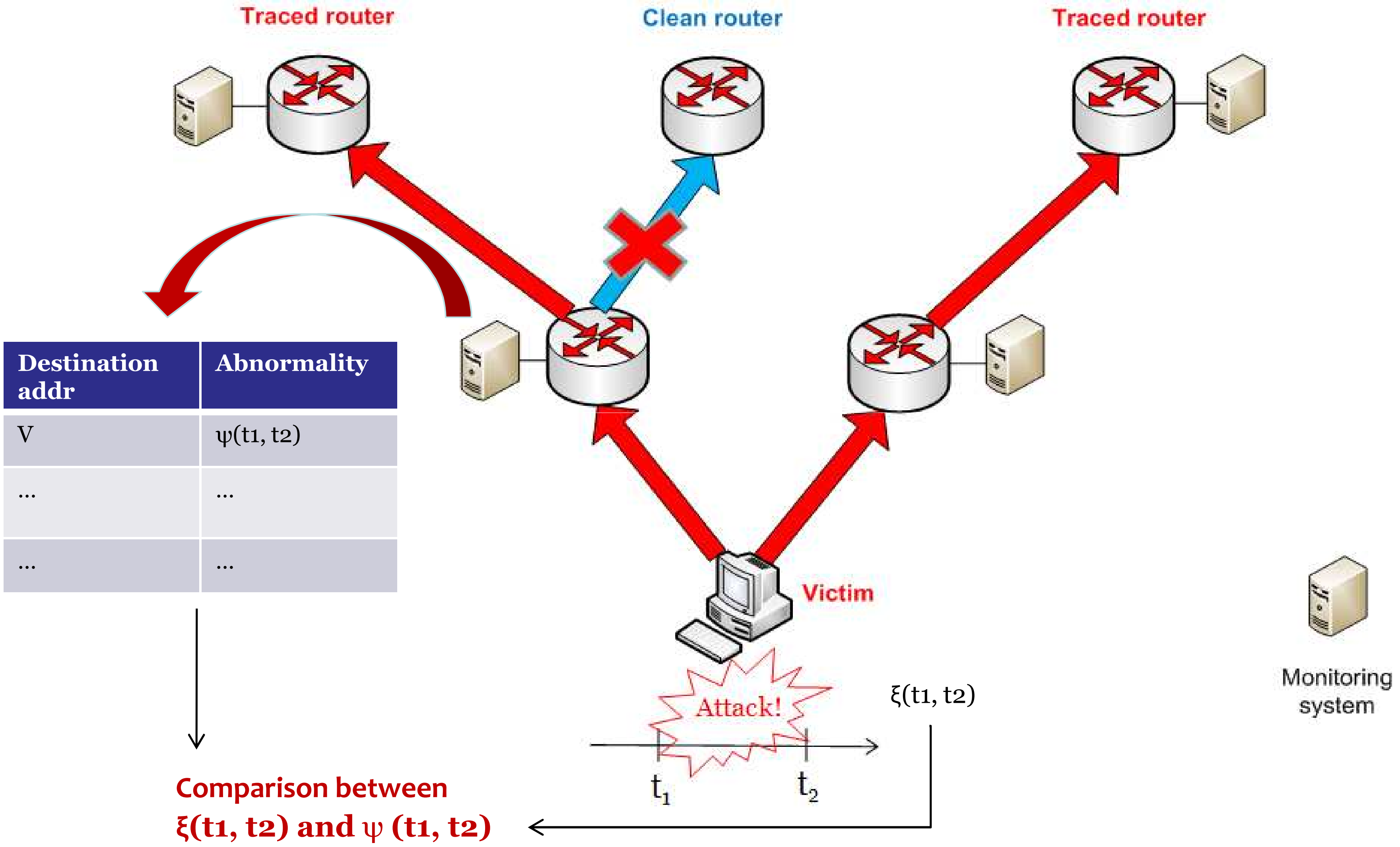
Utilize already available engines for step 1, 2, 4

Adding step 3 is trivial

Tweak I: Detection-assisted traceback

- Monitoring sensor (e.g., traffic monitoring system) is readily available in most networks
- Use spatio-temporal relation of abnormality from monitoring sensor for traceback
- Abnormality can be as simple as abnormal traffic pattern destined to victim at given time slots
- Traceback can help distributed detection sensors to reduce false alarm

Cont’d



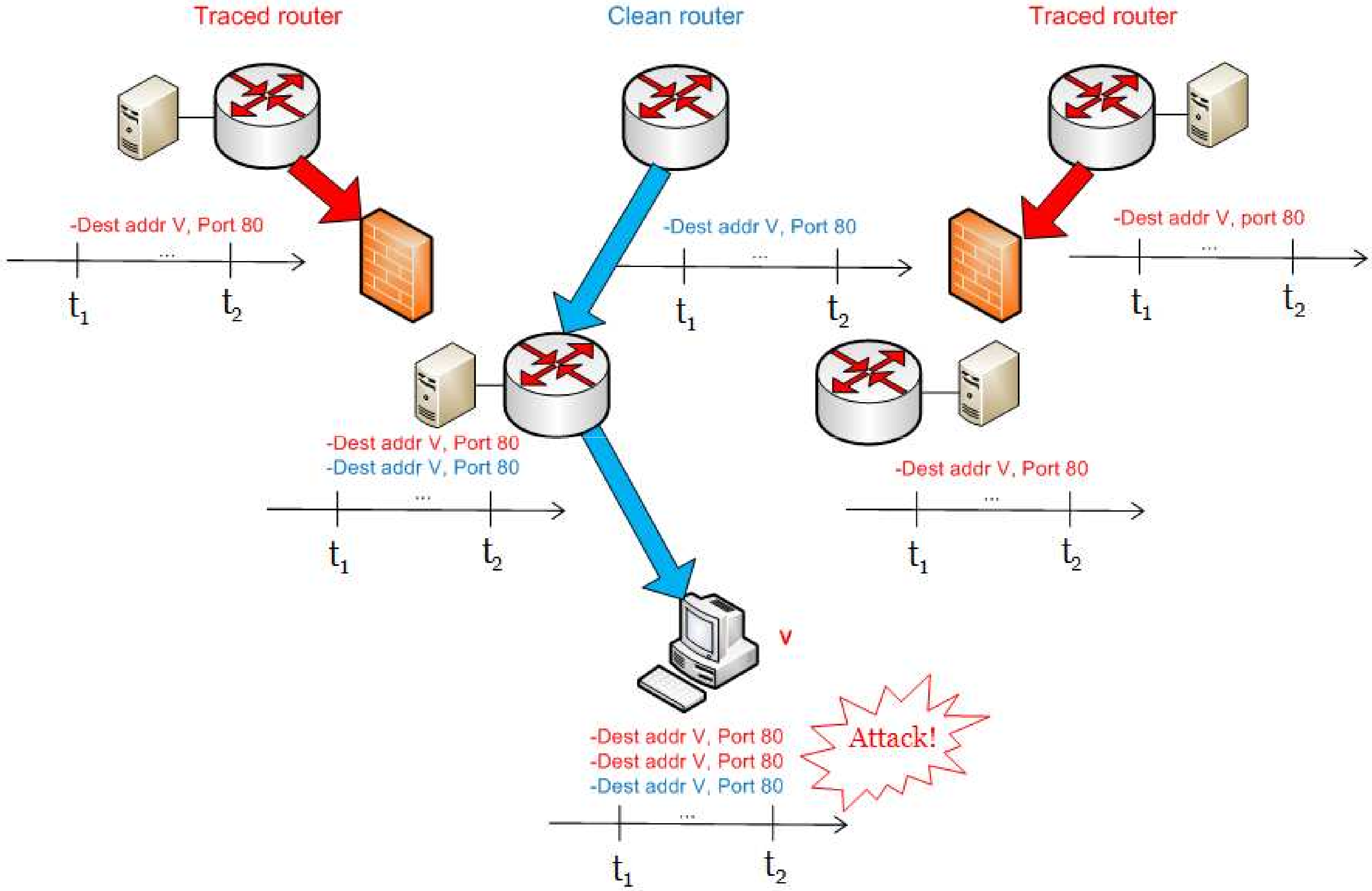
Destination addr	Abnormality
V	ψ(t1, t2)
…	…
…	…

Comparison between
ξ(t1, t2) and ψ (t1, t2)

Tweak II: Traceback-assisted defense

- Traceback allows attack source identification
- Defense can be taken near attack sources after traceback
  - Intermediate link is not exhausted
  - Attack traffic is filtered out in distributed source networks
- Traceback can help reduce negative impact on legitimate traffic
  - Packets are filtered only when those are from traced routers

Cont'd



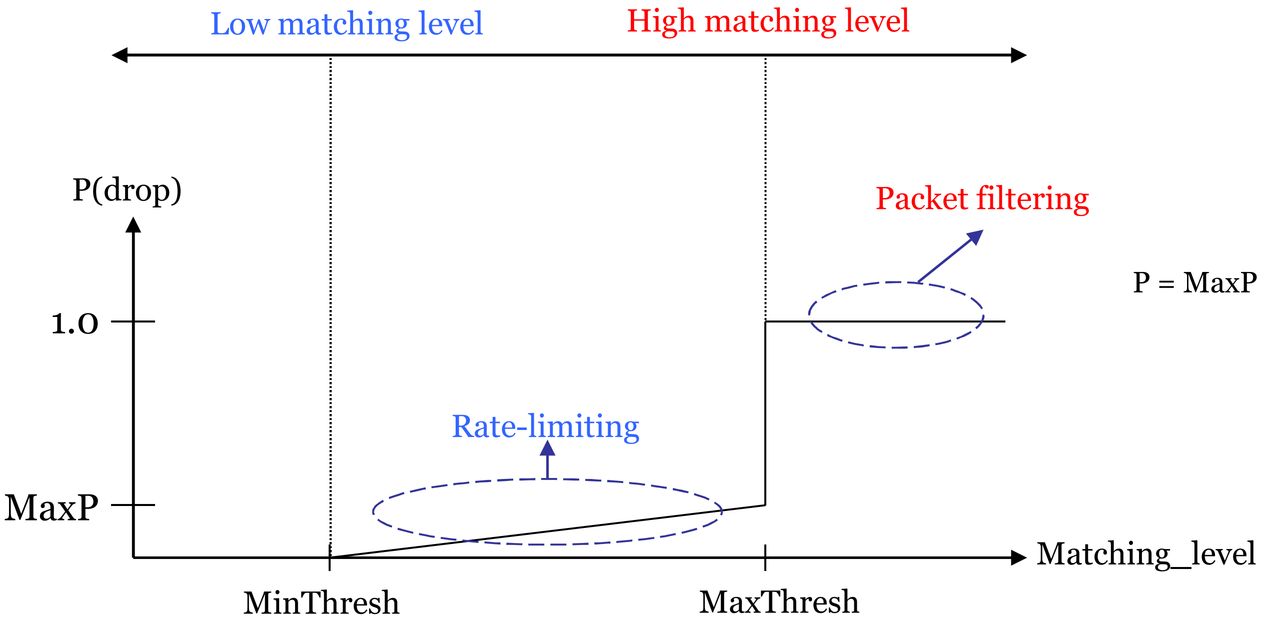
Traced router
Clean router
Traced router
-Dest addr V, Port 80
t_1
...
t_2
-Dest addr V, Port 80
t_1
...
t_2
-Dest addr V, port 80
t_1
...
t_2
-Dest addr V, Port 80
-Dest addr V, Port 80
t_1
...
t_2
-Dest addr V, Port 80
t_1
...
t_2
V
-Dest addr V, Port 80
-Dest addr V, Port 80
-Dest addr V, Port 80
Attack!
t_1
...
t_2

Tweak III: Traceback-assisted countermeasure

- Packet filtering
  - Attack packets are filtered out and dropped at the ingress point
  - How to distinguish between good packets and bad packet?
- Rate-limiting
  - Allows a relay node to control the transmission rate of specific traffic flows
  - Rate-limiting mechanisms are deployed when attack detection has a high false positive or cannot precisely characterize
  - How much rate-limiting we need to apply?
- Traceback can convey clue for better countermeasure

Cont’d

- Apply countermeasure based on abnormality matching level between victim and source networks
- Apply packet filtering in good matching. Otherwise apply rate limiting. By doing so, we can reduce negative impact on legitimate traffic and increase attack packet filtering



$$P = \text{MaxP} \bullet \frac{\text{Matching\_level - MinThresh}}{\text{MaxThresh - MinTresh}}$$

Conclusion

Conclusion

- DDoS attack traceback provides key information for effective DDoS remedy
  - Can take defense near attack origin
  - Can reduce legitimate packet filtering by misdetection
  - Can take effective countermeasure
- Make traceback simple and plug it into existing DDoS detection and defense mechanism
- Inter-ISP cooperation is minimal but worth doing since it can resolve half-baked detection and defense problem