RID Implementation Report

Toshifumi Kai (kai@trc.mew.co.jp), Akito Nagashima
(akito_nagashima@mewe1.mewnet.or.jp), Hiroshige Nakatani (nakatani@trc.mew.co.jp),
Naohiro Fukuda (fukuda@trc.mew.co.jp), Shimizu Hiroshi (shimizu@trc.mew.co.jp)
Matsushita Electric Works, Ltd.
Teruaki Takahashi (c300070@ns.kogakuin.ac.jp), Akira Hashiguchi (akira@cooweb.com),
Takayuki Suzuki (t-suzuki@pf6.so-net.ne.jp) Katsuji Tsukamoto (tsukamoto@tsukaken.jp)
Kogakuin University

Plan for Test by Mew

2004 Sep 27th – Oct 1st

→ Phase 1 (Finished) … RID system only

MEW's XML format is not same as RID format, No Encryption and Authentication

2004 Nov 1th – Dec 30th

→ Phase 2 (Planned and on Going) …RID with Traceback

MEW's XML format is not same as RID format, No Encryption and Authentication

2005 Jan 1th –

→ Phase 3 (Not Planned Yet) …RID with Traceback

Full Implemented system

MEW's Implementation Status

- Renaming Source Found to message result for not found case

  (-> history area)

  'Message Type 3 with NULL Attacker's IP' equal 'Not Found'
- Notification field for traceback system added for Source Found Message

  (-> free form text area)

  - It would be necessary for the following cases, if the initiator does not allow False Negative (FP) and use Hash traceback, however responder use ICMP trceaback then it may have False Positive (FP), and the traced result may be no meaning for initiator.
  - Hash traceback can trace in each packet but ICMP traceback traces DoS/DDoS packets. So, we added used-traceback-type in some field.
  - In the case of system down caused in responder's traceback system, it should be reported by the notification message.
- MEW's XML format is not equal for RID's XML format

  Implementation is not completed yet and modified for test purpose now.
- Encryption and authentication is not implemented yet.

  Implementation of SSL/XML encryption and authentication using CA remained
- Transport protocol is implemented with soap/http/tcp

  We used soap/http/tcp protocol for messaging

Simple Test

- We setup a very simple test case: star topology and straight chained topology with 7 PCs.
- 7 PCs as NMSes and without routers and traceback system between them
- We measured the response time until the source found (result) message will send to initiator
- NMS and the CPU time when the NMS handle the XML interpretation and SOAP
- communication. When it were straight topology, and if AS numbers were 7.

Test Results

- Straight Chained Topology:

  Response time for traceback was 1.6 sec, and Response time for handling SOAP/XML was 0.46 sec for 7 ASes.

- Star Topology:

  Response time for traceback was 0.6 sec, and Response time for handling SOAP/XML was 0.23 sec for 6 ASes.

- It will take about 0.1-0.22 sec per AS for handling traceback, 0.038-0.065 sec per AS for handling SOAP/XML, And total response time will be about 0.138-0.285 sec per AS.

  Note: We assume and feed the tracing time (delay) of inside AS defined as fixed value.

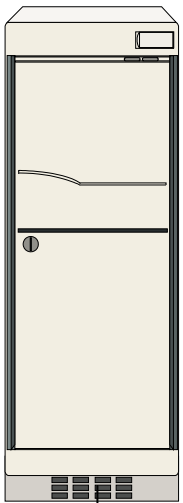
  First and Middle AS; 0.2sec

  Attacker's AS (Final AS); 0.4sec

  (We plan to test with the real tracing time in next month)

Reference

Spec for NMS

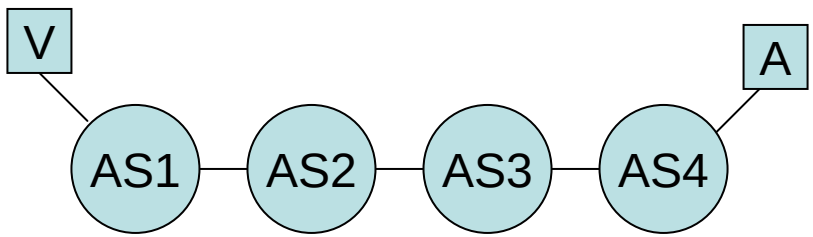
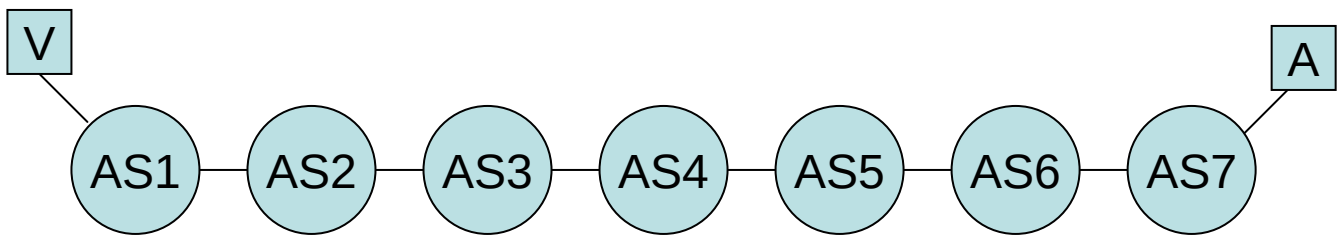


NMS(RID)
(Inter-AS traceback Software)

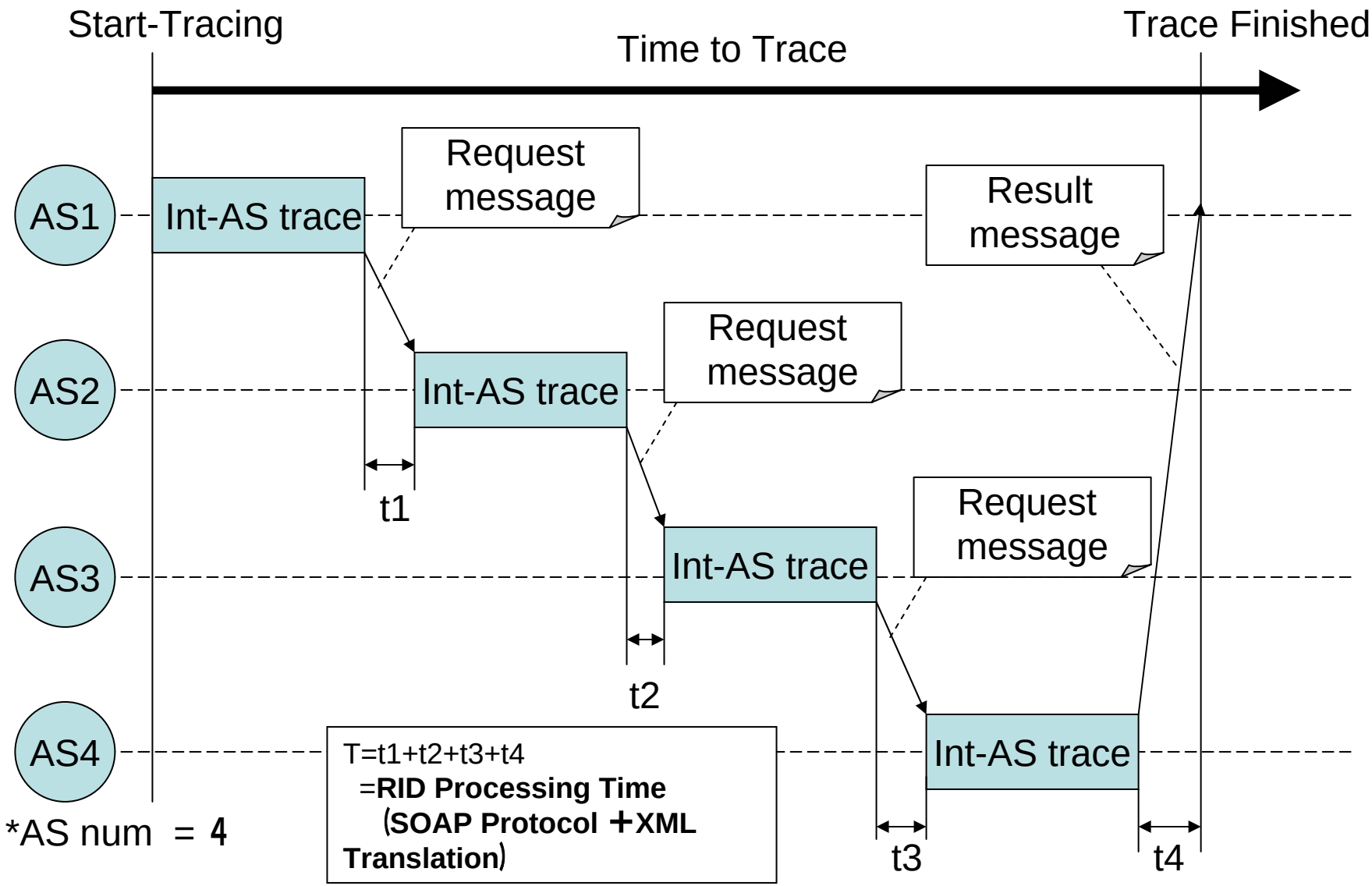
- CPU：
  - Pentium４ 3.0GHz
- Memory：
  - 512MBytes
- Network:
  - Fast Ether (100Base-T)

- Transport Protocol:
  - TCP + HTTP + Open SOAP
- Inter-AS Traceback Protocol:
  - RID-mew (modified RID + XML)

Chained AS Topology

AS Num	Topology
1	
4	
7	

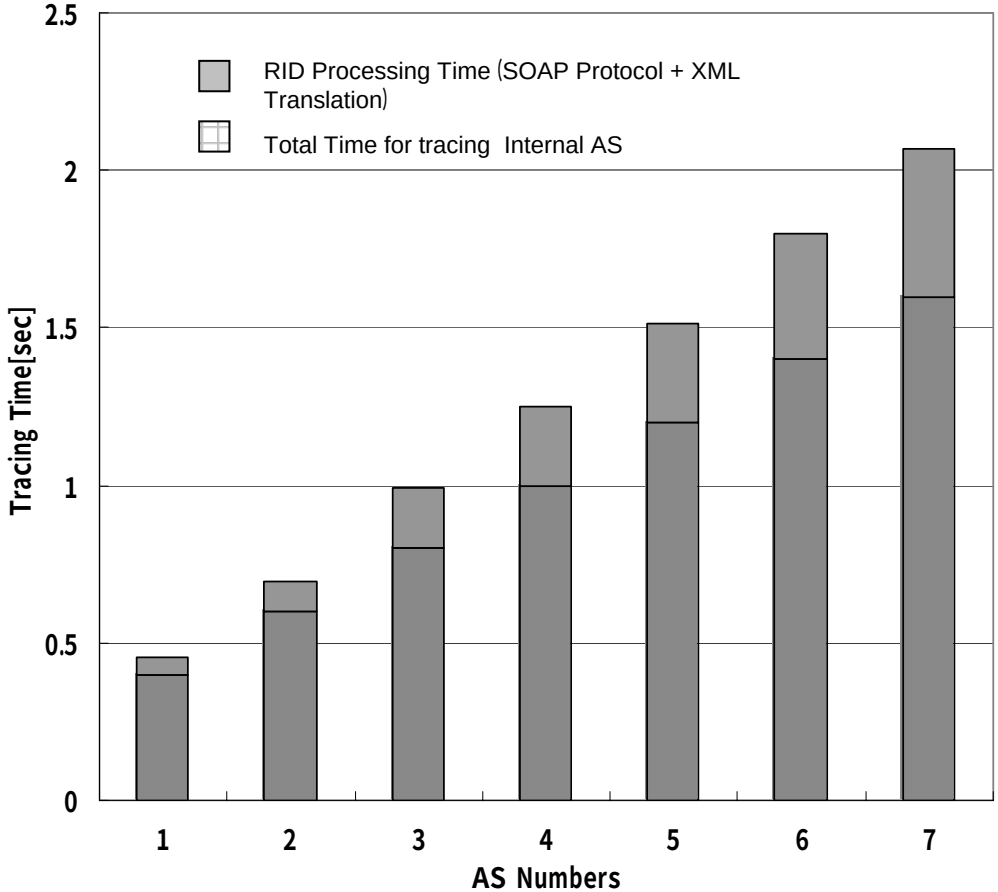
Timeline for Chained Trace



Chained Results

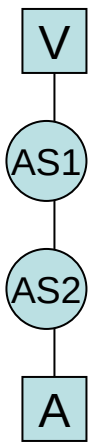
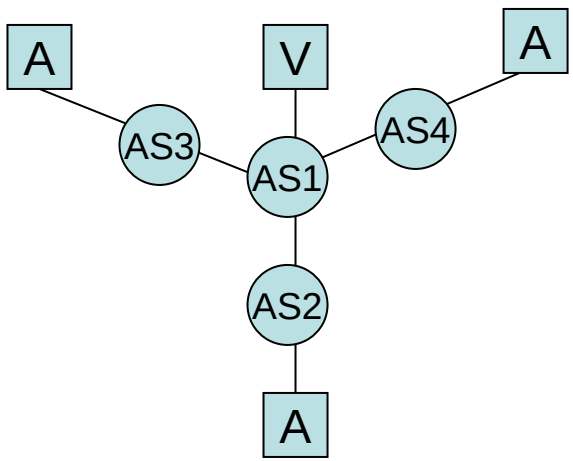
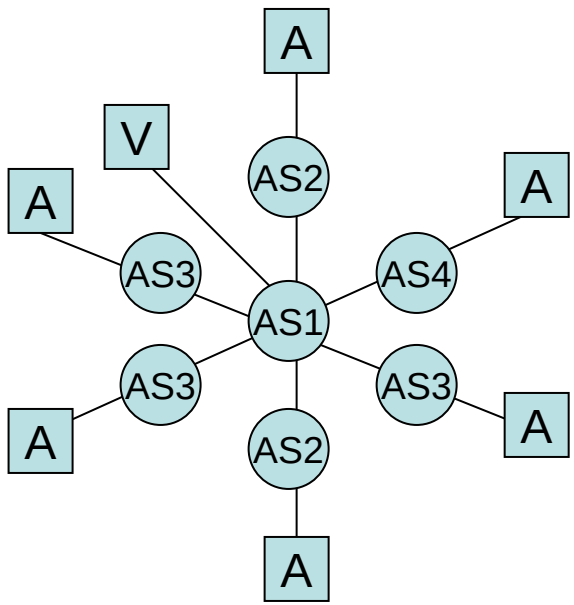
AS num	Tracing Time for Total int-AS	RID Processing Time (SOAP Protocol + XML Translation)
1	0.4	0.053916
2	0.6	0.096066
3	0.8	0.189532
4	1.0	0.252760
5	1.2	0.315661
6	1.4	0.401333
7	1.6	0.466741

[sec]



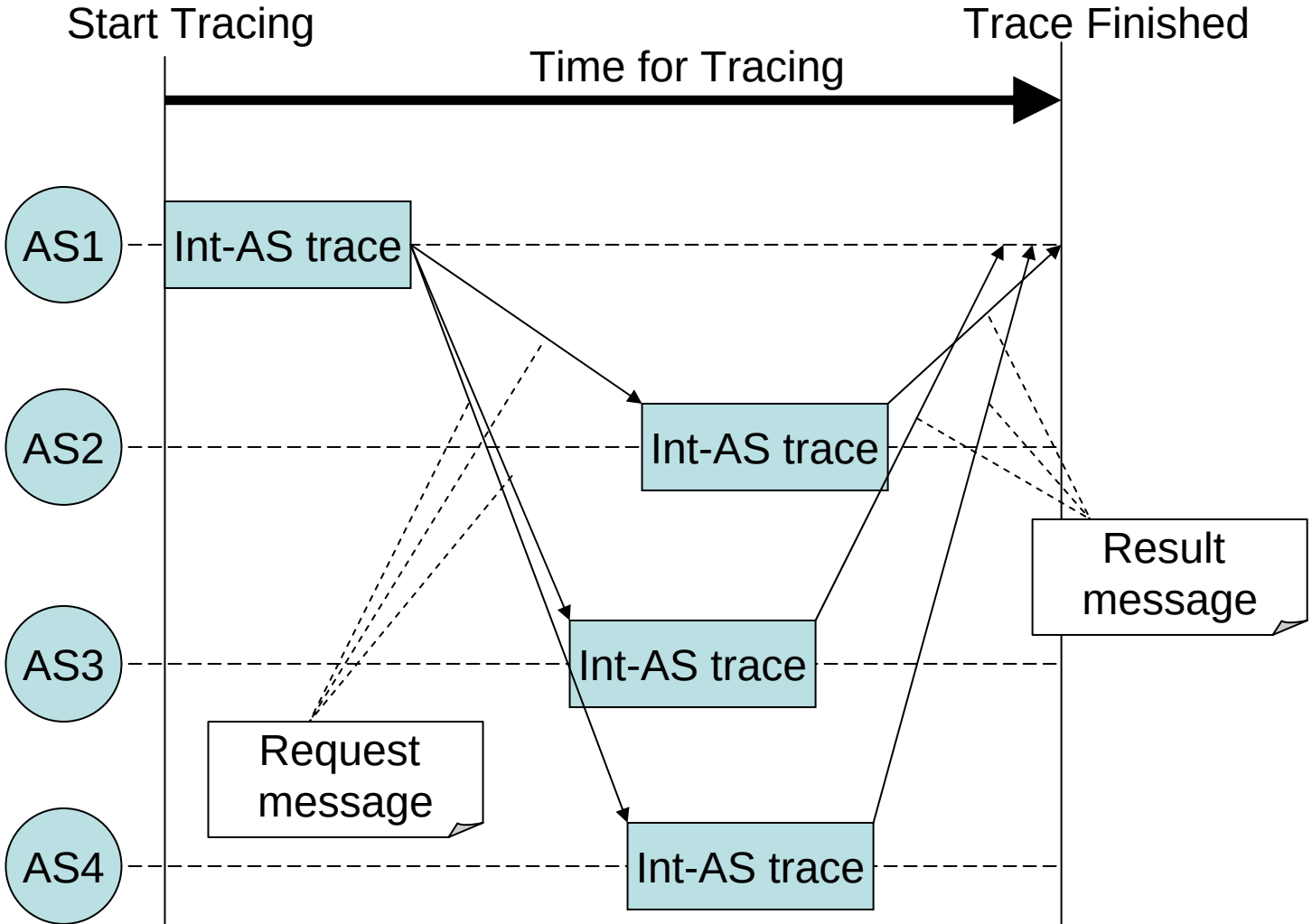
*We assume that the tracing time of inside AS defined as fixed value
(first and middle AS;0.2sec, Attacker's AS; 0.4sec)

Star AS Topology

Num of Neighbor AS	1	3	6
Topology			

A: Attacker
V: Victim

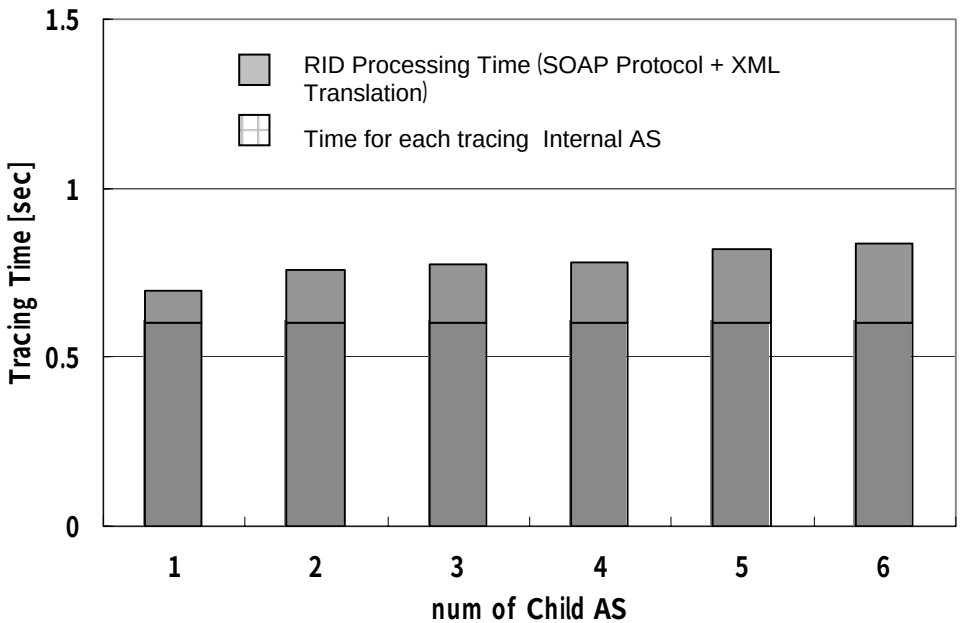
Timeline for Star Topology



※num of neighbor AS was 3

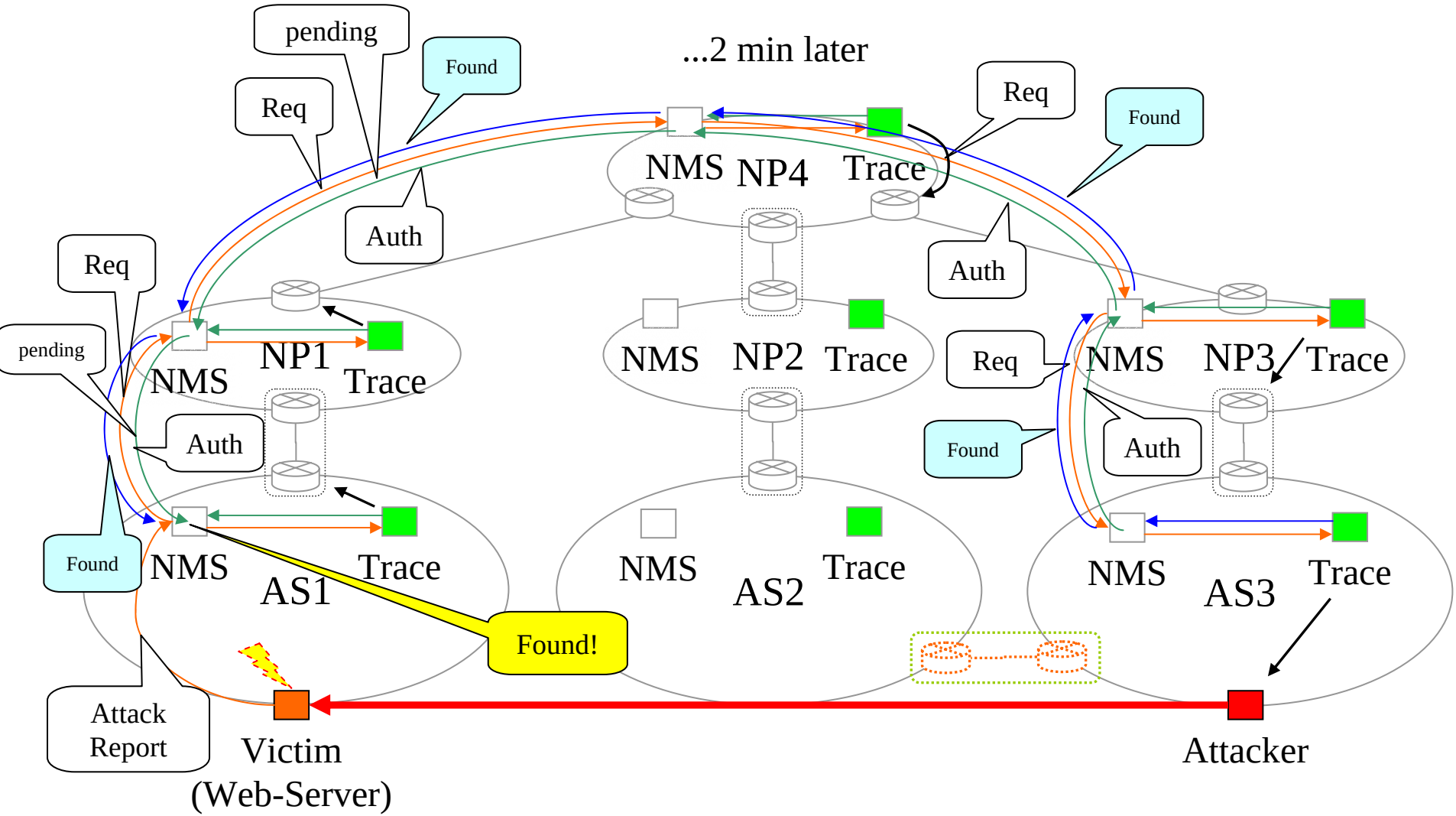
Star Results

Num of neighbor AS	Tracing Time for each Int-AS	RID Processing Time (SOAP Protocol + XML Translation)
1	0.6	0.096066
2	0.6	0.157692
3	0.6	0.177469
4	0.6	0.180390
5	0.6	0.219429
6	0.6	0.237459

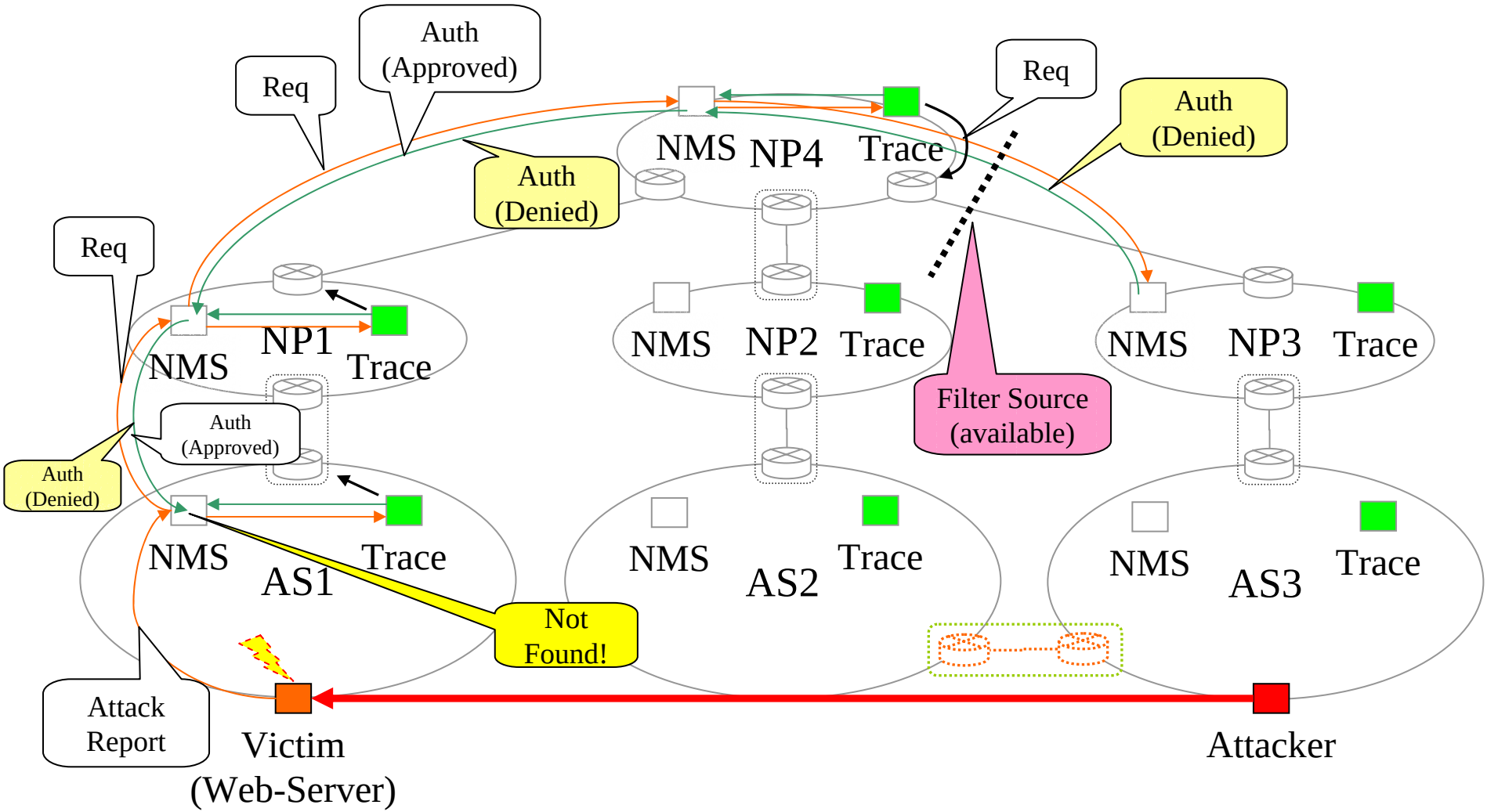


*We assume that the tracing time of inside AS defined as fixed value
(first and middle AS;0.2sec, Attacker's AS; 0.4sec)

RID-Anime (Tracing)

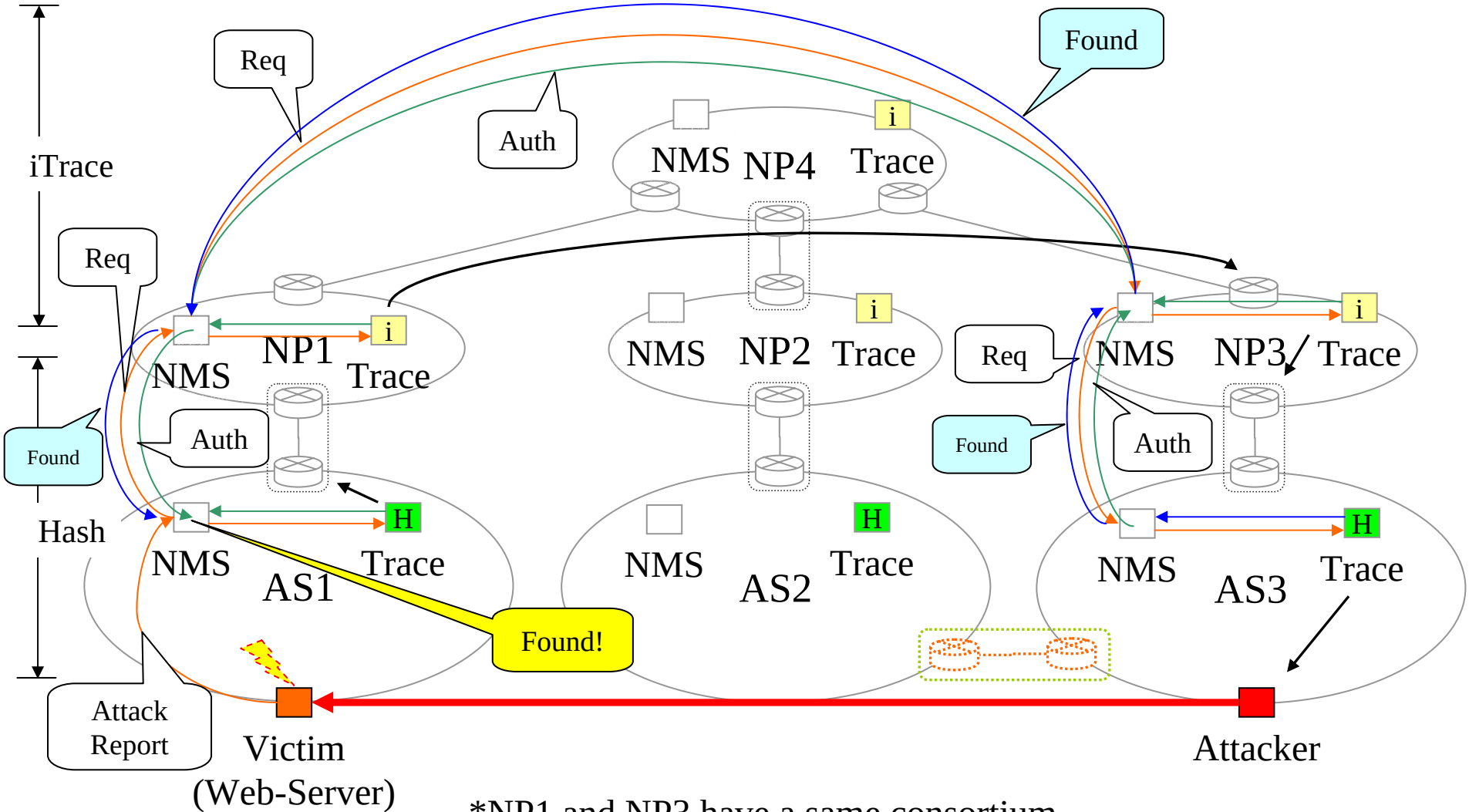


RID-Anime (Filtering)



RID-Anime

(Probabilistic Traceback)



*NP1 and NP3 have a same consortium

RID-Anime

(Multi-Traceback)