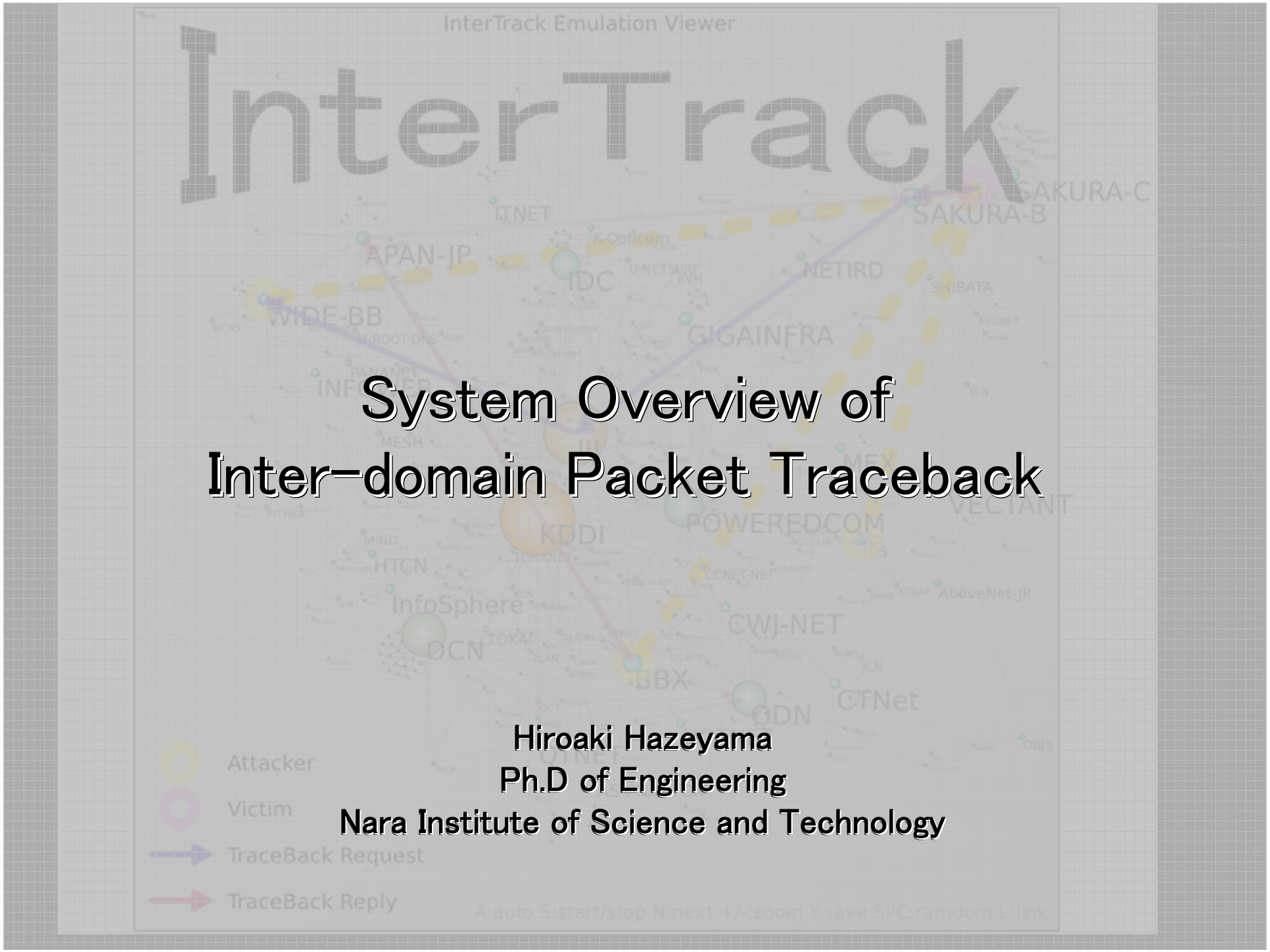


System Overview of Inter-domain Packet Traceback

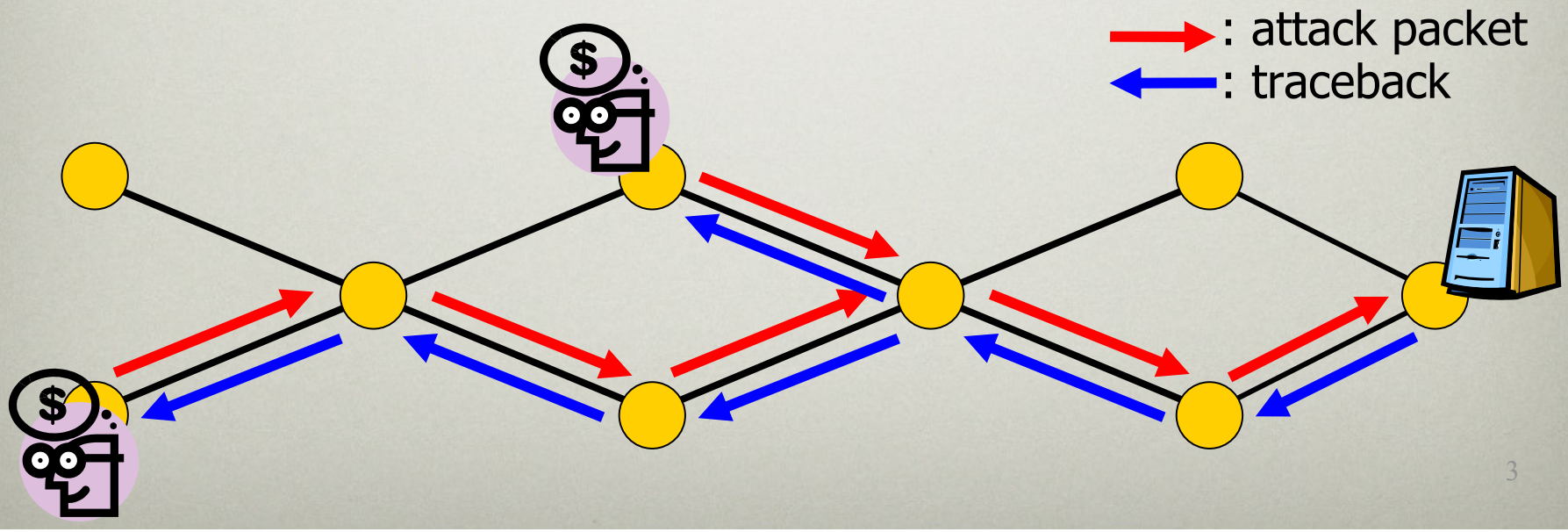
Hiroaki Hazeyama
Ph.D of Engineering
Nara Institute of Science and Technology

Outline

- Introduction
- System Overview
- Tests on StarBED
- Analysis of Tests
- Consideration

What is Packet Traceback ?

- Technique to track the true forwarding path of a packet
  - By querying packet capture agents
  - Even when the source IP address of the target packet is spoofed
- Packet Traceback is expected to track attack packets
  - DDoS attack, UDP exploit, spoofed DNS queries



System Overview

Operators

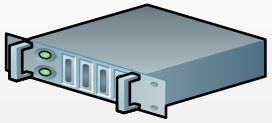
InterOp TTS
(Inter-Operator Trouble Ticket System)
(KDDI Lab)

Inter-AS

InterTrack
(Inter-domain Traceback Network)
(NAIST)

Intra-AS

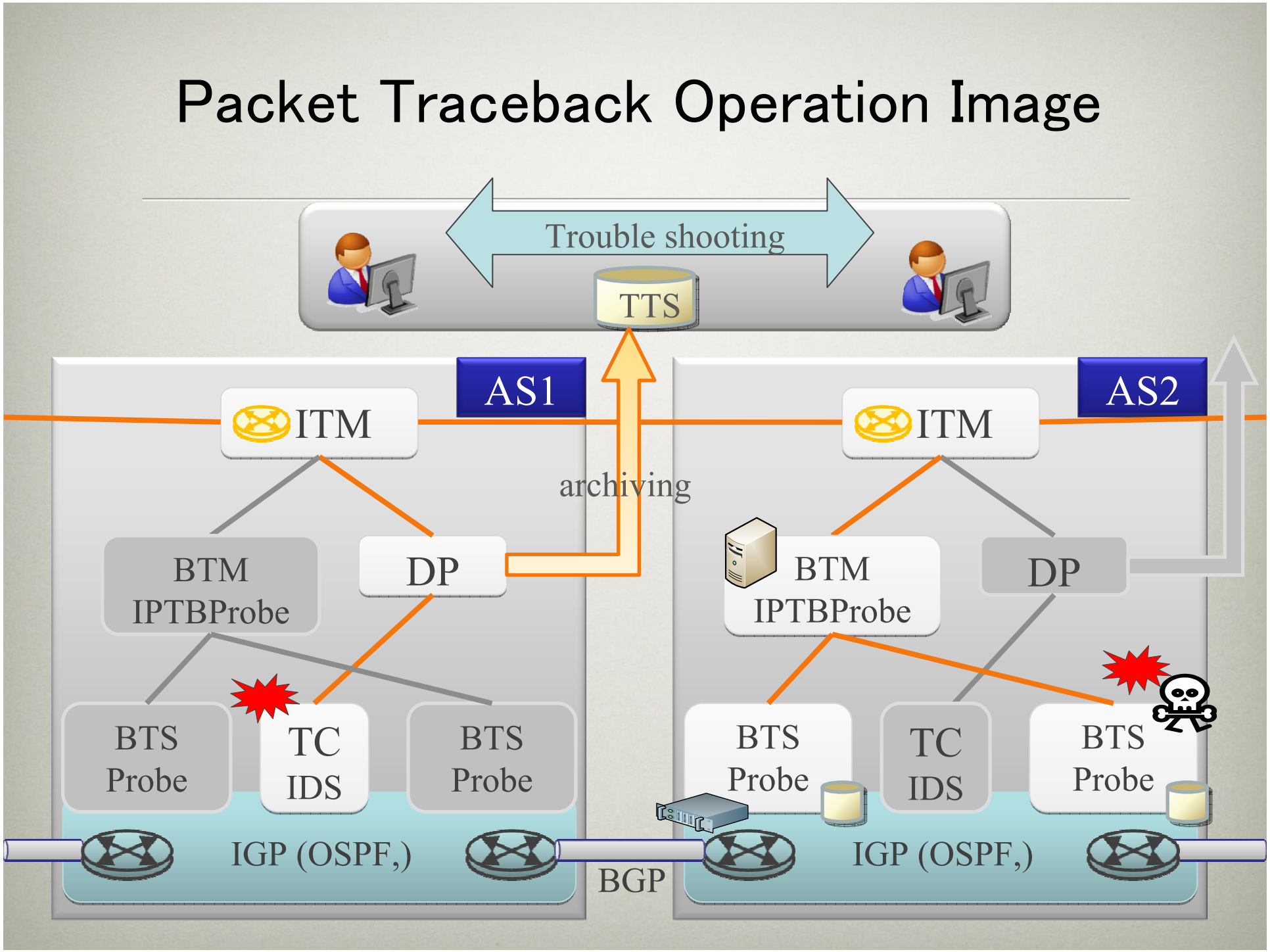
IP-TB
(IP Packet Traceback System)
(Matsushita Electric Works)



Layer 1 / 2

Packet Capture Probe（HW/SW）
(KDDI Lab)

Packet Traceback Operation Image



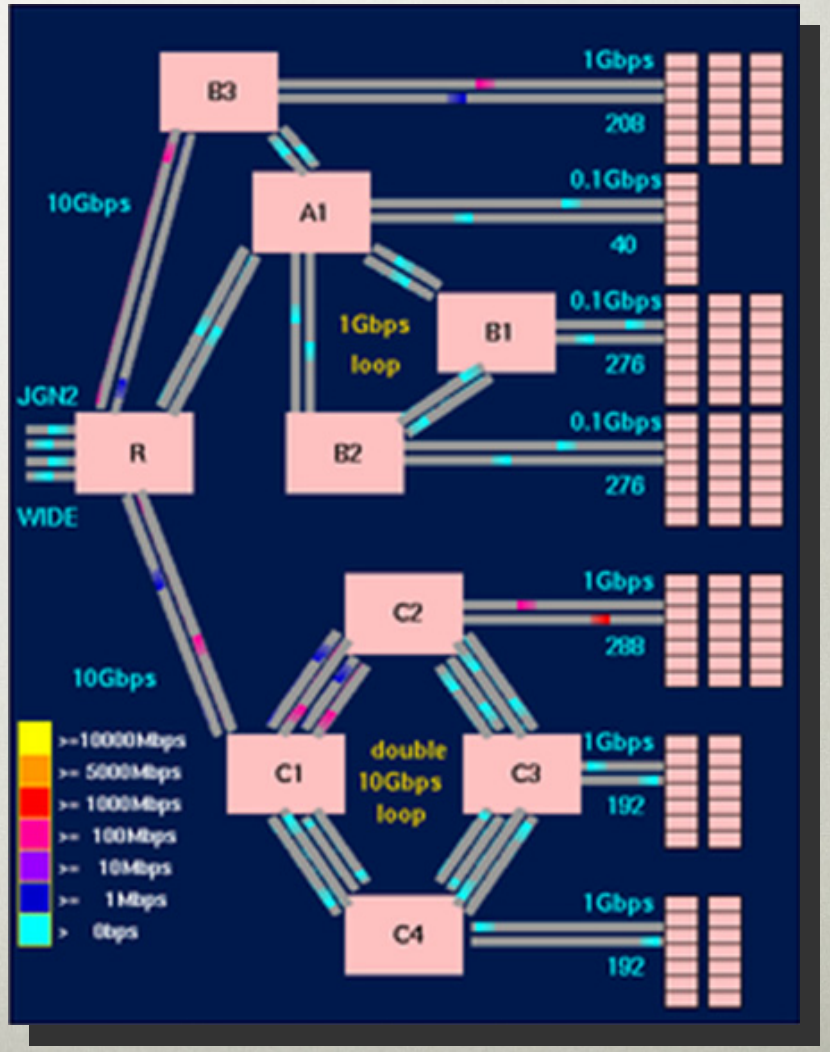
Emulation Tests toward Field Tests

- To reduce risks on field tests, we measured the bellow items in Emulation Tests
  - Specifications of each component
  - Interoperability among each component
  - Scalability of the whole system
  - Estimated Traceability along with Deployment Scenarios

We ran Large Scale Emulation Tests on StarBED

StarBED

NICT Hokuriku Research Center
Large Scale Network Emulation / Simulation Testbed

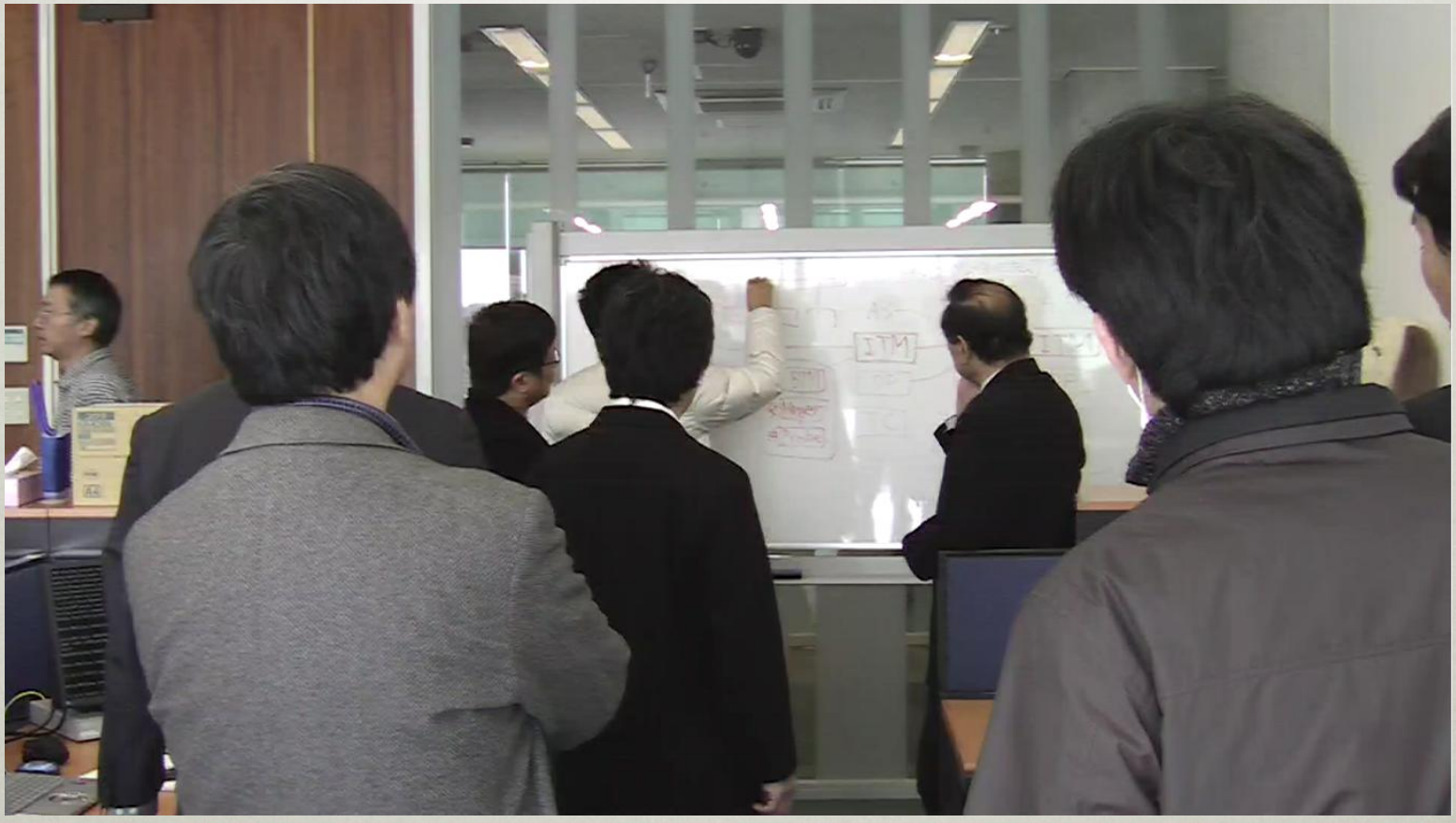


Test in Dec. 2007

Test in Dec. 2007

- Interoperability test
  - InterTrack <-> IP-TB manager <-> SW/HW probe
  - Checked Hash value format, Message format, Behaviors
  - Measured throughput on a minimum set
- Practice for Emulation Test in Jan. 2008
  - Create configuration templates, test scenarios and test tools
  - Be familiar with StarBED consoles

Test in Jan. 2008



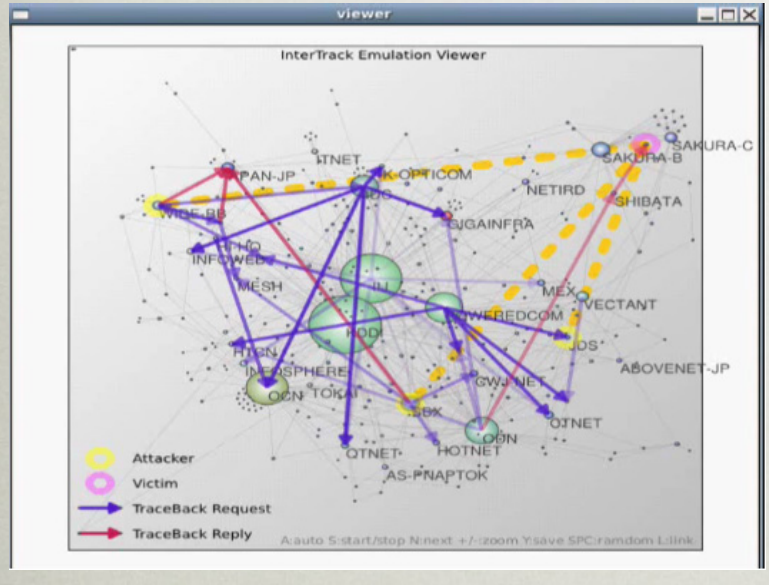
Tests in Jan. 2008

- Interoperability test
  - TTS <-> InterTrack <-> IP-TB manager <-> SW probe
- Verification test of the whole system
  - In a minimum set
- Scalability test of the whole system
  - In an Emulated 200 AS topology in JP-Domain
- Audit by a Lawyer and T-ISAC Traceback WG

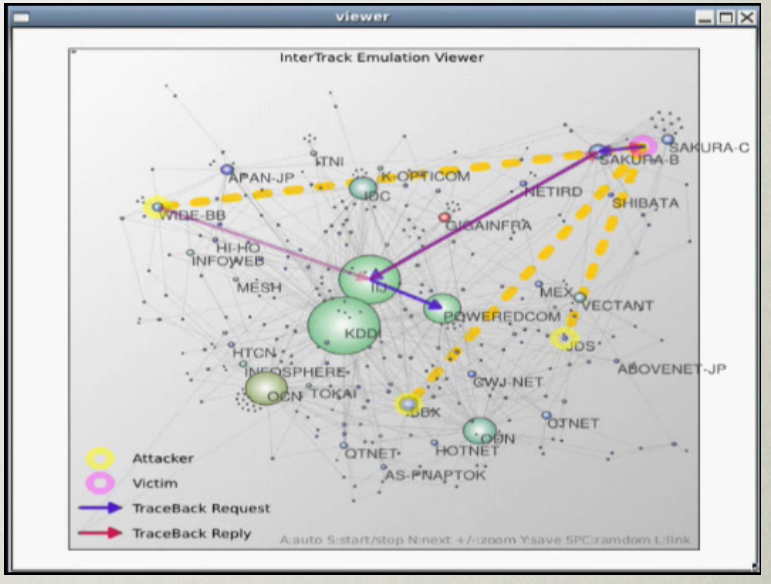
Procedure of Emulation Tests

1. Configure PXE Boot and OS image
2. Setting a basic L2/L3 network
3. Creating an Emulated eBGP topology
4. Generating configuration files from the eBGP topology
5. Booting each software
6. Running experiments

Snapshots of Emulation Tests

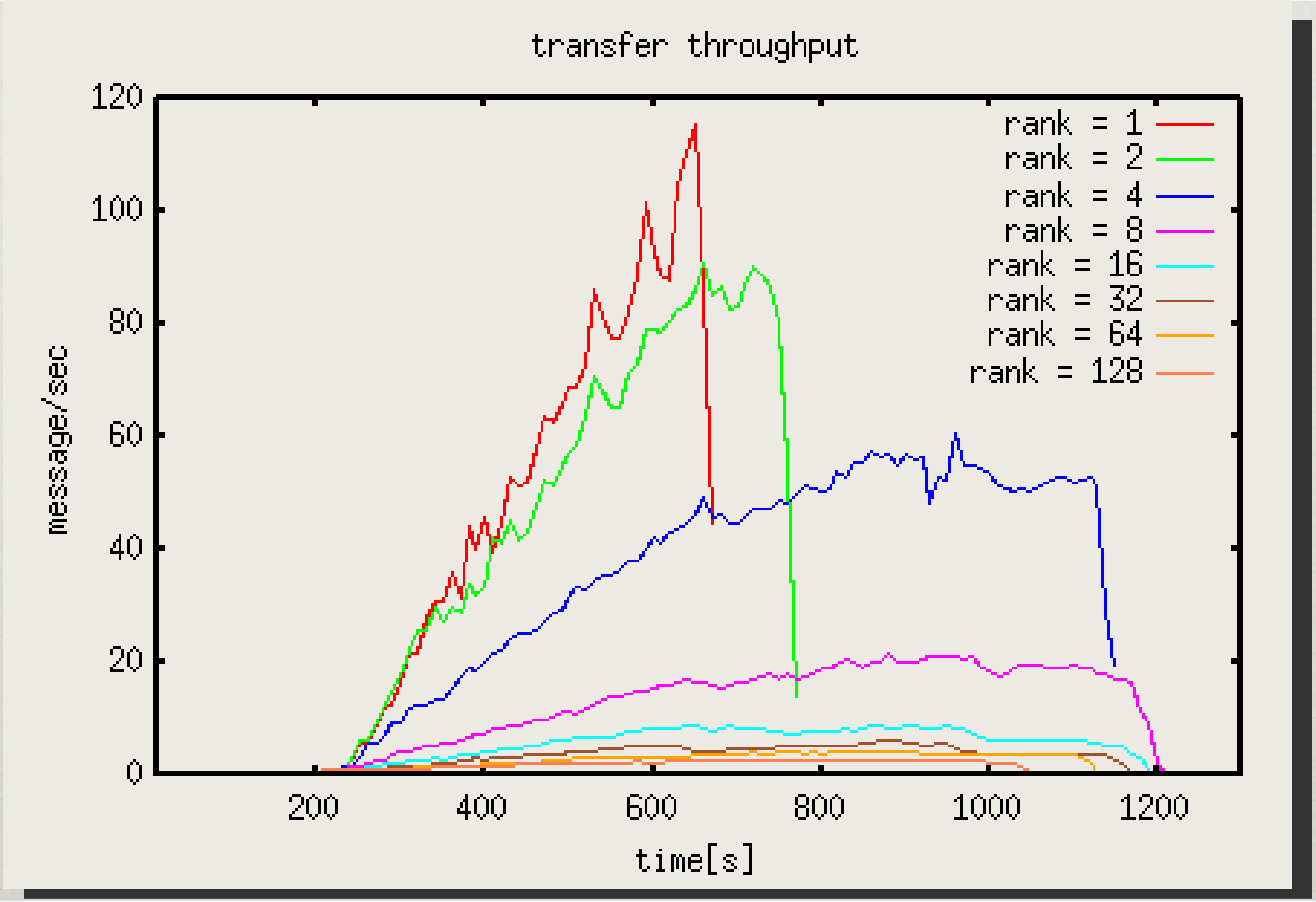


Flood Mode
message forwarding
(worst case analysis)



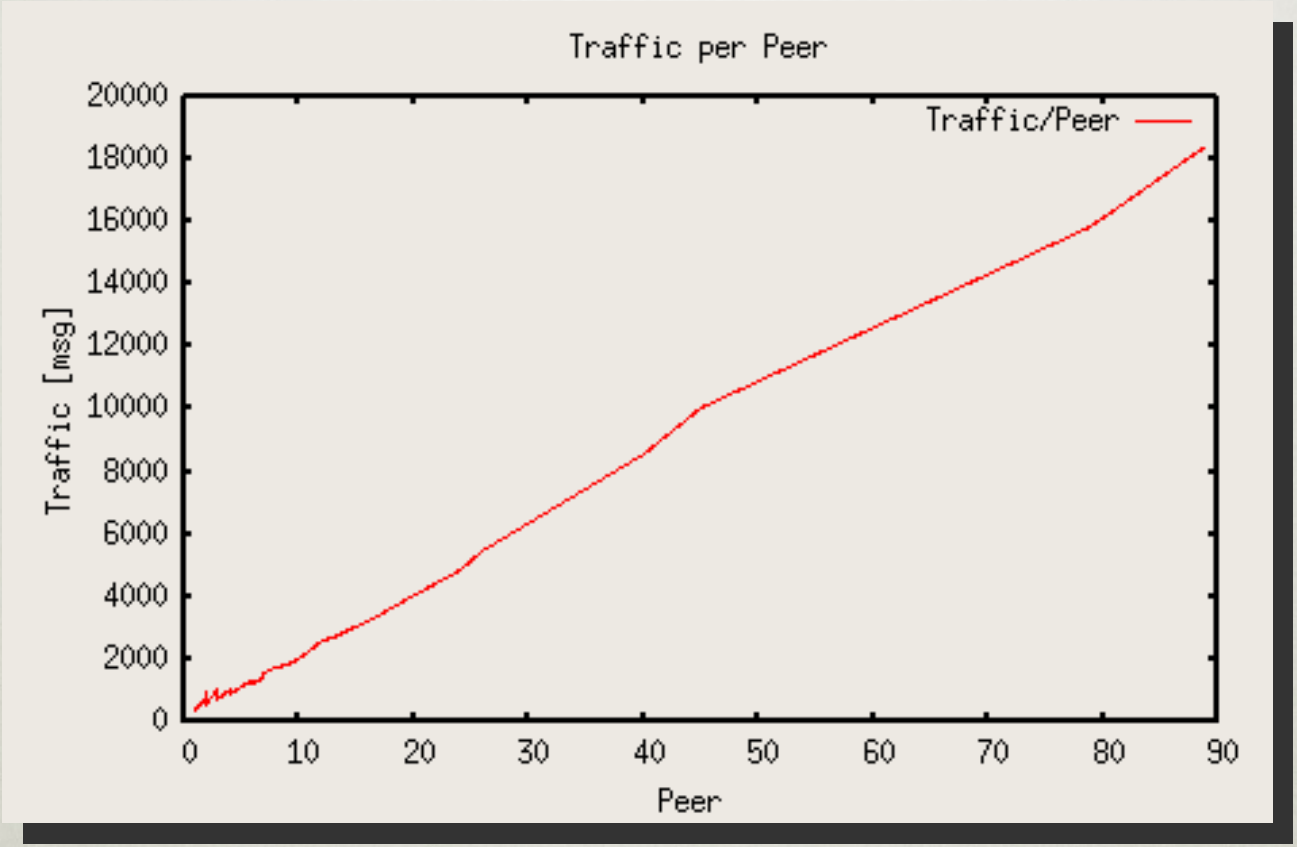
Strict Mode
message forwarding
(best case analysis)

Throughput Analysis (in worst case)



At Rank 1 AS (89 eBGP neighbors)
1.0GHz (Pentium3) / Mem 256M→120[msg/s]

Ratio of # of Peers and # of messages (in worst case)



According to # of peers,
ITM can apply a rate limit filter

Benefits from Tests in StarBED

- Verified behaviors of the whole system
- Measured the basic specifications
- Revealed several problems and research / development topics about scalability issues
- Improved the whole system as soon as we found problems
  - Because all researchers and developers were gathered in StarBED

More and More Emulation Tests

- Experiments with More reality while running Filed Tests
  - Considering delay and bandwidth
  - More detail emulations with Intra-AS topologies
  - Emulation Test in All JP-domain AS topology
  - Test Various Scenarios
  - Feedback from / to actual filed tests

Next is the details of our field test plan
by Mr. Wakasa of T-ISAC-J