Comprehensive prevention method of DDoS attack using Reconfigurable Communication Processor

Naoto Sumita, Masaki Murakami, Satoru Okamoto, and Naoaki Yamanaka

Graduate School of Science and Technology, Keio University, Kanagawa, Japan

NET-CENTRIC

Keio University
1858
CALAMVS GLADIO FORTIOR

Background(1/2)

- Increase in traffic
  - By 2022, it is expected to reach 396 exabytes, about 1.5 times more than in 2020.
- Increase in DDoS attacks
  - The number of attacks increases steadily every year.

[1] Cisco, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html.

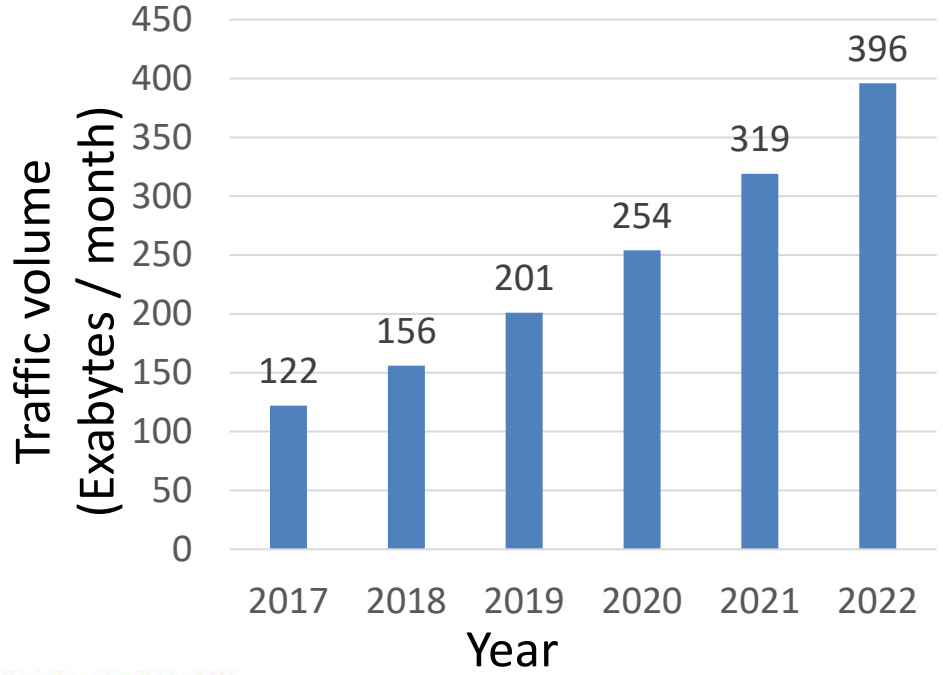


Fig.1 IP traffic forecast [1]

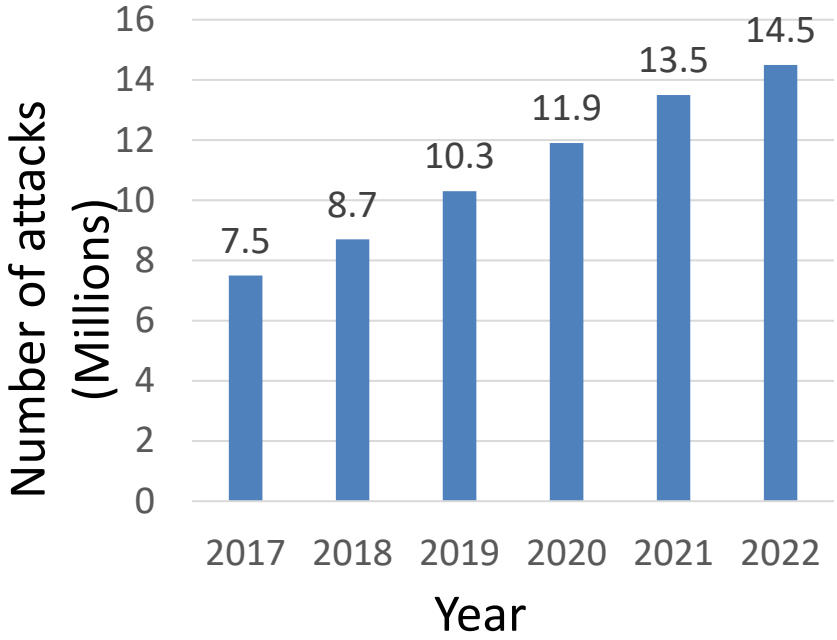


Fig.2 DDoS attacks forecast [1]

NET-CENTRIC

Keio University
1858
CALAMVS GLADIO FORTIOR

Background(2/2)

- As DDoS attacks become more sophisticated, detection requires more complex analysis.
- DDoS detection & prevention at the organization's gateway becomes inefficient when the attack traffic exceeds the link capacity.

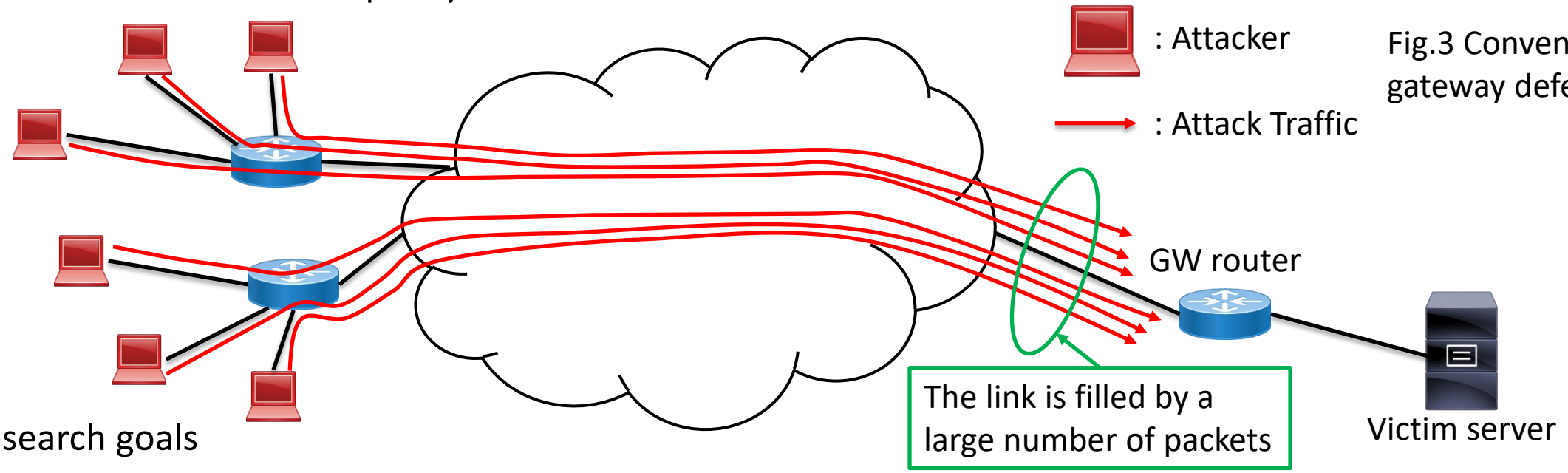


Fig.3 Conventional gateway defense

- Research goals
  - DDoS defense method for sophisticated attack patterns in core networks
  - Securing bandwidth to legitimate users by blocking the attack close to the attacker

Conventional work

- DDoS defense method at ISP[2]

[2] Z. Liu, Y. Cao, M. Zhu and W. Ge, "Umbrella: Enabling ISPs to Offer Readily Deployable and Privacy-Preserving DDoS Prevention Services," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1098-1108, April 2019, doi: 10.1109/TIFS.2018.2870828.

  - When encountering congestion, a legitimate TCP sender tries to relieve the congestion by reducing its rate because its receiver cannot decode the data if some packets are lost. On the contrary, attackers focus on exhausting network resources.

    → Determine the bandwidth for the next time slot by considering the packet loss rate

  - Even if the attacker manages to control the packet loss rate well, if the set of legitimate user flows is N_L, the set of attacker flows is N_A, the maximum allowed packet loss rate is L_{th}, and the bandwidth is B, then the attacker can only allocate at most $\frac{(1+L_{th}) * N_A * B}{N_L + N_A}$.

    → This is because $\frac{N_A * B}{N_L + N_A}$ is given as an initial value and the bandwidth of the next time slot is reduced if the packet loss rate exceeds L_{th}.

This method works for TCP floods, but is insufficient for UDP and SYN floods.

Related works: Reconfigurable Communication Processer

- RCP consists of a Reconfigurable Processing Module (RPM), Reconfigurable Service Module (RSM), and Tbps class (electrical packet) switching module interconnecting them.

Features of RCP

- Edge node of optical core network
- It is possible to reconstruct functions provided by modules inside RCP according to user's request.

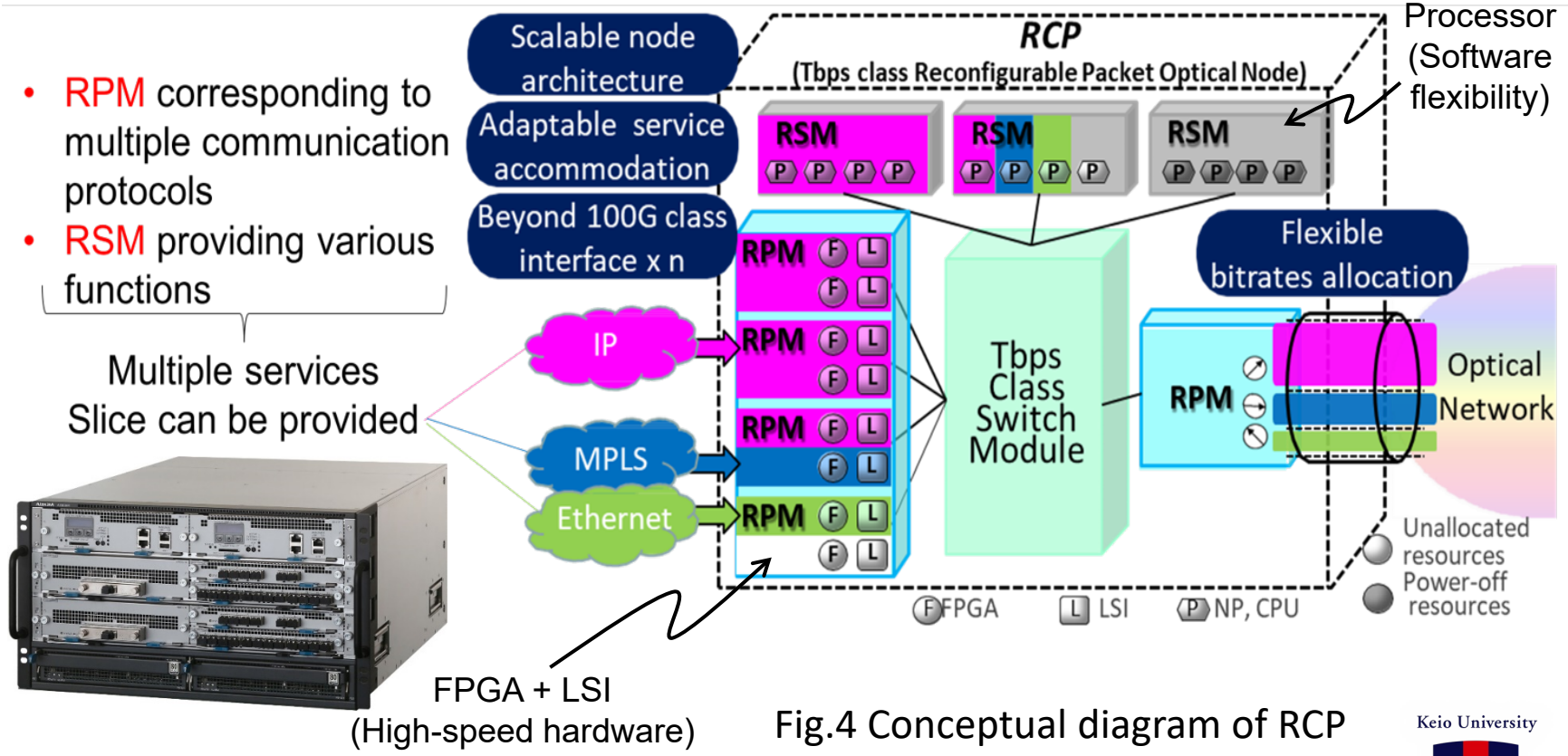


Fig.4 Conceptual diagram of RCP

Related works: Resource pool architecture

- Multiple RCPs can be used as a common resource pool by interconnecting high-speed optical networks.

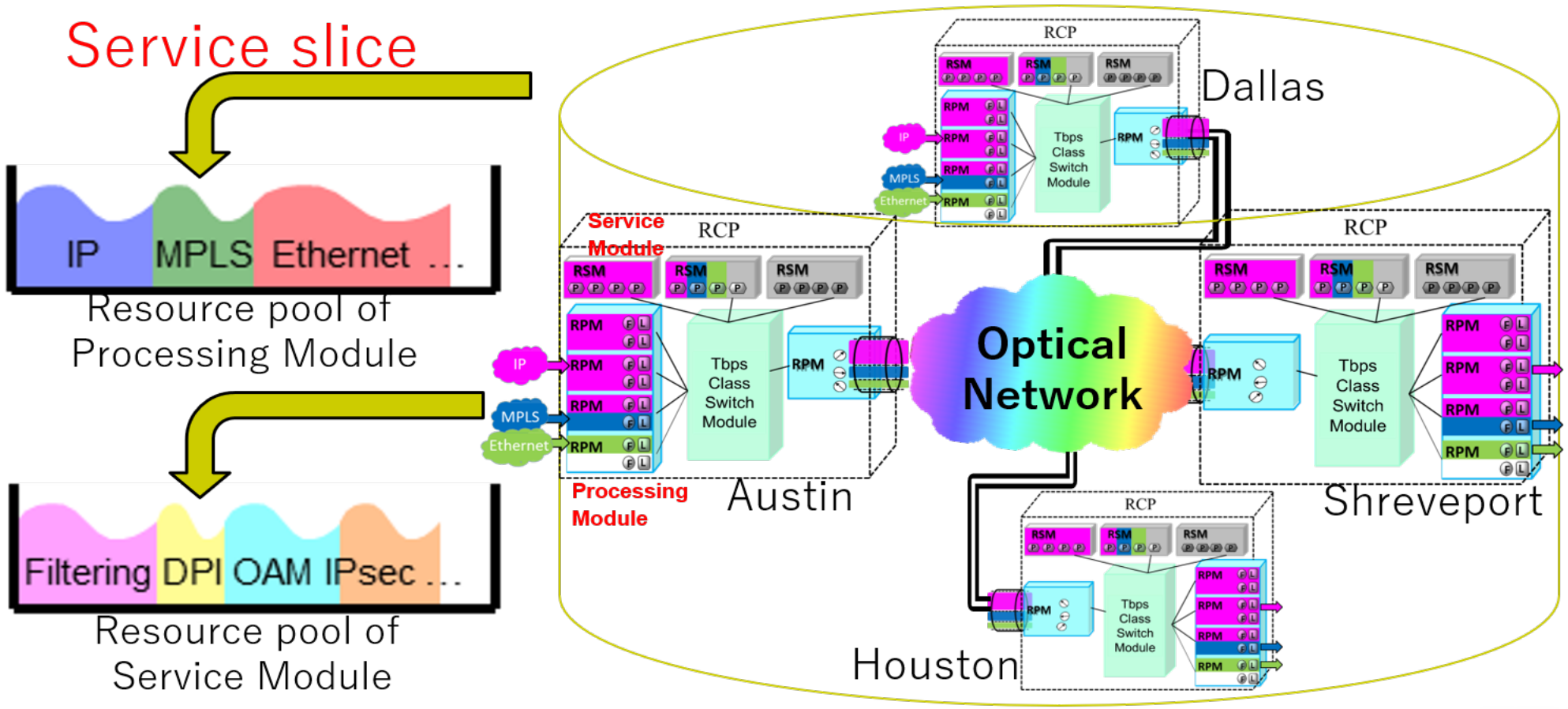


Fig.5 Conceptual diagram of Resource pool architecture

Resource pool architecture is realized by flexible reconfigurable nodes in the optical network. It accommodates flexible network services (service slices) and enables flexible network construction.

Related works: Bloom Filter

- Bloom Filter
  - Probabilistic data structure, saving storage and allowing fast retrieval.
  - Consists of an m-bit array of bits and k hash functions and the elements initially are all set to 0.
  - For each element to be added, use k hash functions to set the bits of the index of its hash value to 1.

- Counting Bloom Filter
  - Filter that evolved from the Bloom Filter.
  - The Bloom Filter is 0 or 1 as an array element, while the Counting Bloom Filter is a counter.
  - If an element is added to the filter, the counter is incremented.
  - Counting Bloom Filter can remove the element by decrementing the counter.

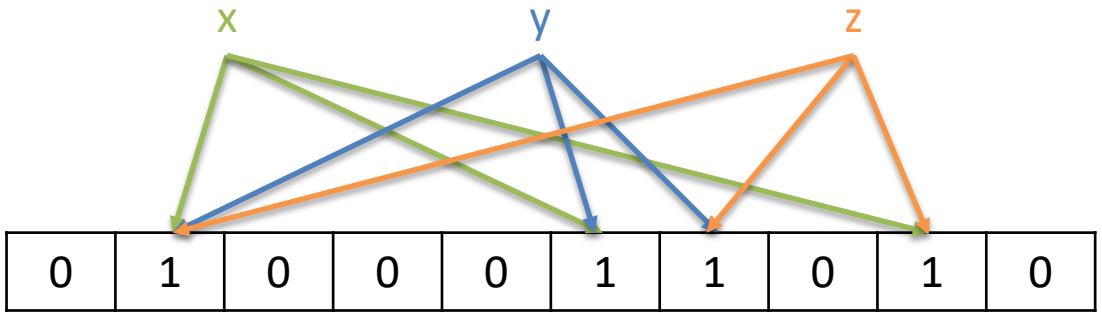


Fig.6 Bloom Filter

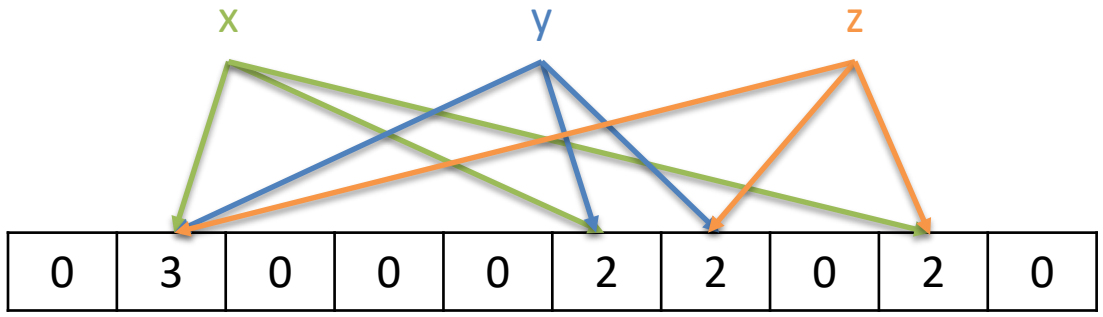


Fig.7 Counting Bloom Filter

Types of DDoS attacks

- The following five types of DDoS make up almost all of them.

Table.1 The main types of DDoS attacks

Type of DDoS attacks	Overview
SYN attack	Deplete the resources of the server by sending SYN packets
ICMP attack	Send a large number of ICMP packets
TCP attack	Send a large number of TCP packets
UDP attack	Send a large number of UDP packets
HTTP attack	Send a large number of HTTP request or Occupy TCP sessions for long periods of time

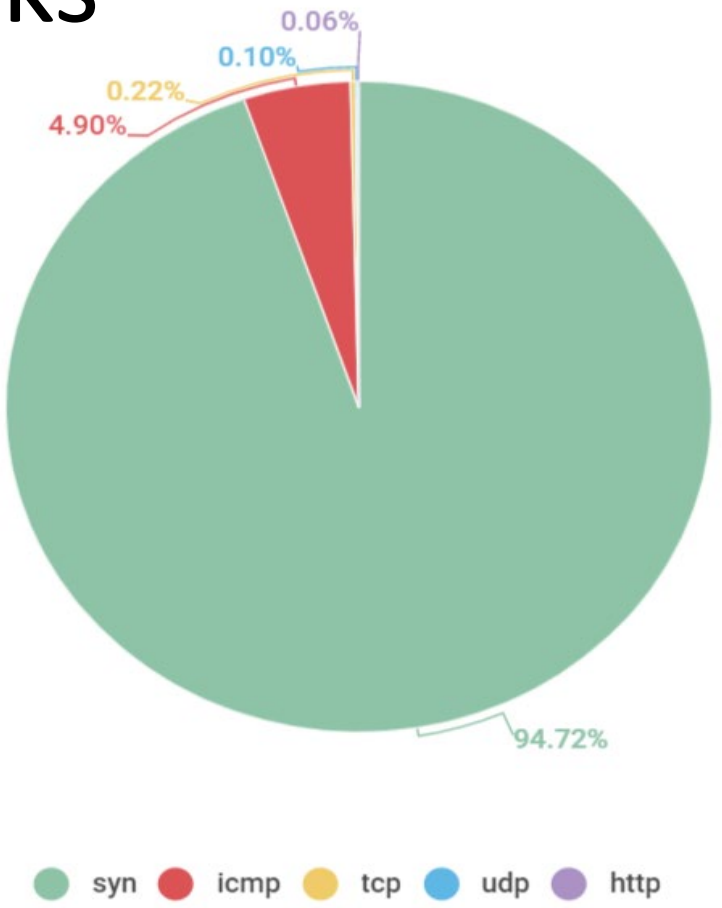


Fig.8 Types of DDoS in Q2 2020[3]

➢ DDoS attacks can be classified into three categories: SYN attacks, VOLUME attacks and SLOW attacks.

NET-CENTRIC

[3] https://securelist.com/ddos-attacks-in-q2-2020/98077/

Keio University
1858
CALAMVS GLADIO FORTIOR

Proposed method: Detection method

- Detection method corresponding to SYN attacks, VOLUME attacks, SLOW attacks respectively

Table.2 Detection method

Type of DDoS attacks	Detection method
SYN attacks	Deplete the server‘s resources by sending SYN packets from a large number of spoofed IP addresses in order to prevent legitimate users from communicating. → Change point detection by entropy of the source IP address
VOLUME attacks	Overwhelm the network bandwidth by sending large numbers of packets to prevent legitimate users from communicating. →Detection by traffic amount change
SLOW attacks	Hold a TCP session for a long period of time with a small number of packets to prevent legitimate users from communicating. → Detection by packet continuous arrival time

Proposed method: Filtering method

- Blacklist by Counting Bloom Filter and random forest corresponding to SYN attacks, Volume attacks, Slow attacks respectively
  - ex) If detected by entropy of the source IP address, install Counting Bloom Filter with high threshold(Coarse filtering) and execute random forest for SYN attack.

    → Lower the Counting Bloom Filter threshold for the source IP address determined to be an attack by random forest(Fine-grained filtering).

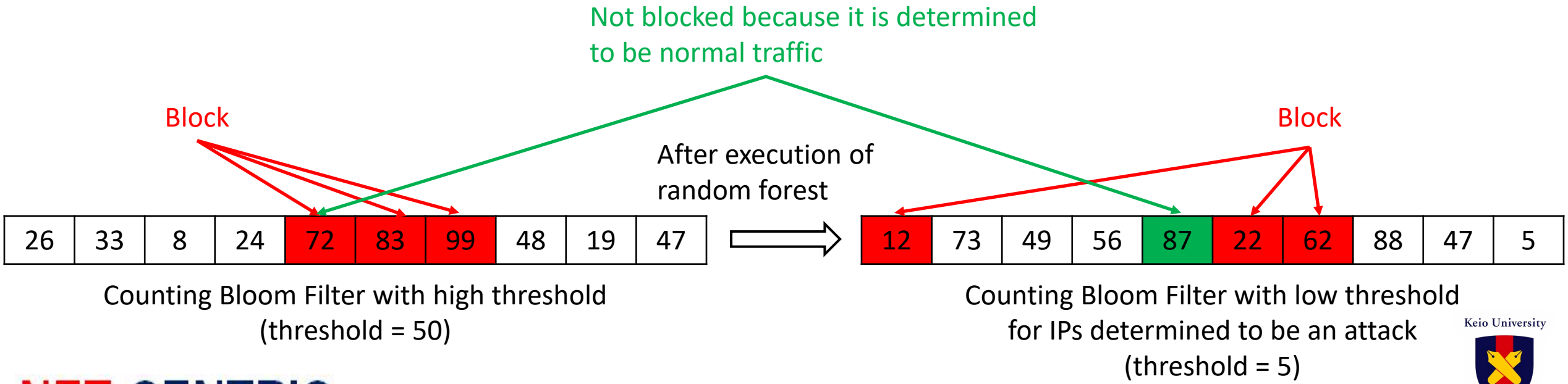


Fig.9 Coarse filtering and fine-grained filtering

Proposed method: Flowchart(1/5)

Sampling and copying the traffic

Run each detection program

After detection

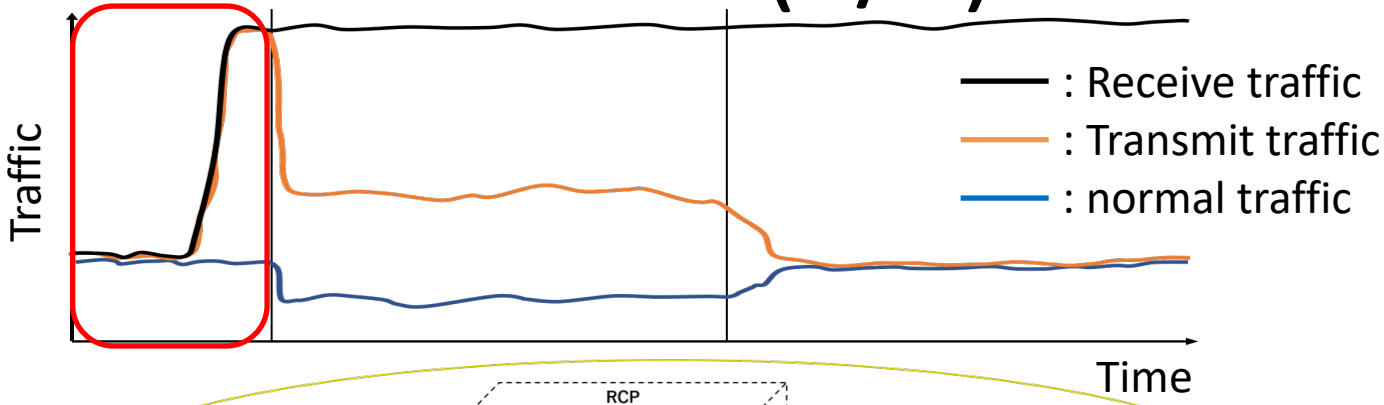
Build an RPM with a Counting Bloom Filter with a high threshold and set it to pass

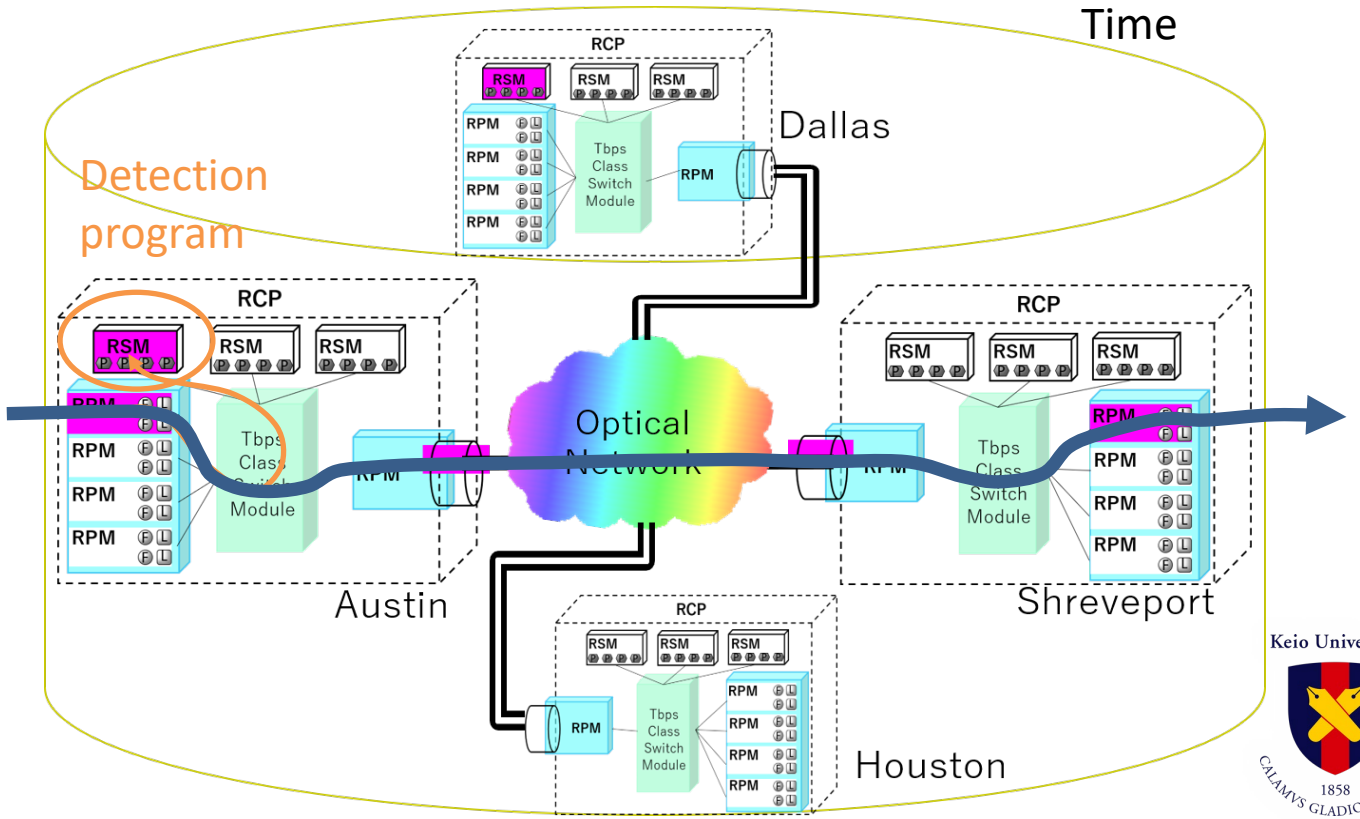
Build a tap device

Configure the path to a random forest program for detected attacks

Decreasing the Counting Bloom Filter threshold

Identify the IP address





NET-CENTRIC

Keio University
1858
CALAMVS GLADIO FORTIOR

Proposed method: Flowchart(2/5)

Sampling and copying the traffic

Run each detection program

After detection

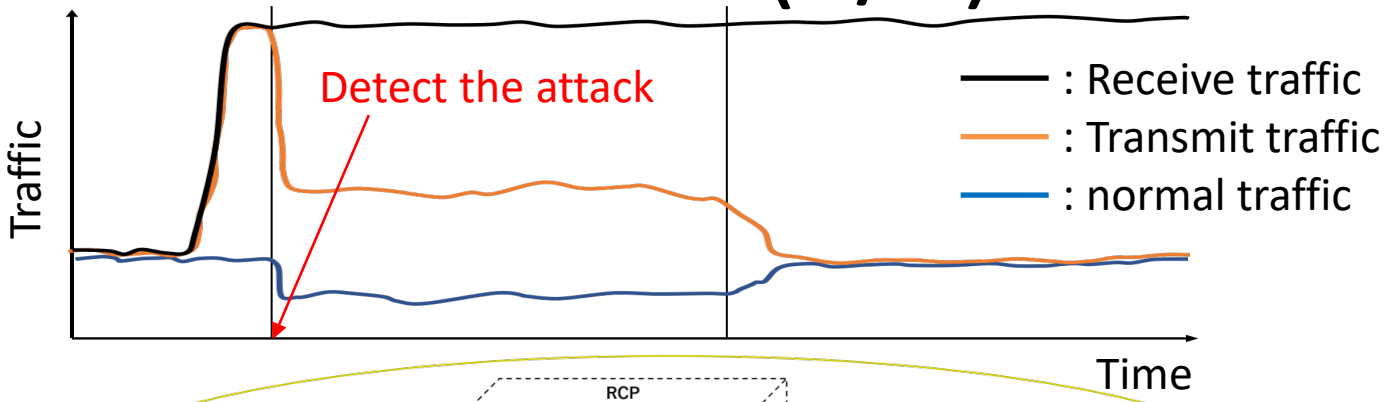
Build an RPM with a Counting Bloom Filter with a high threshold and set it to pass

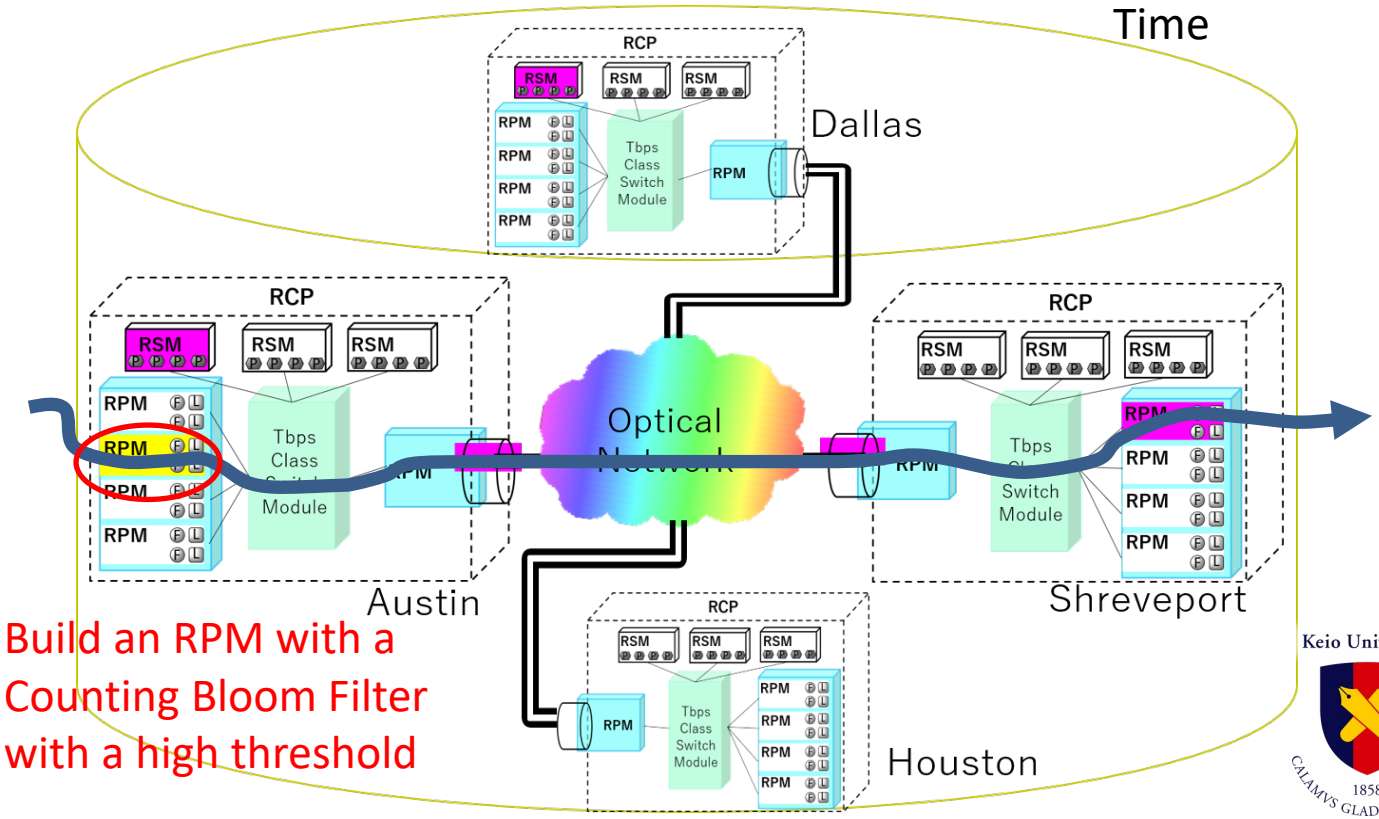
Build a tap device

Configure the path to a random forest program for detected attacks

Decreasing the Counting Bloom Filter threshold

Identify the IP address

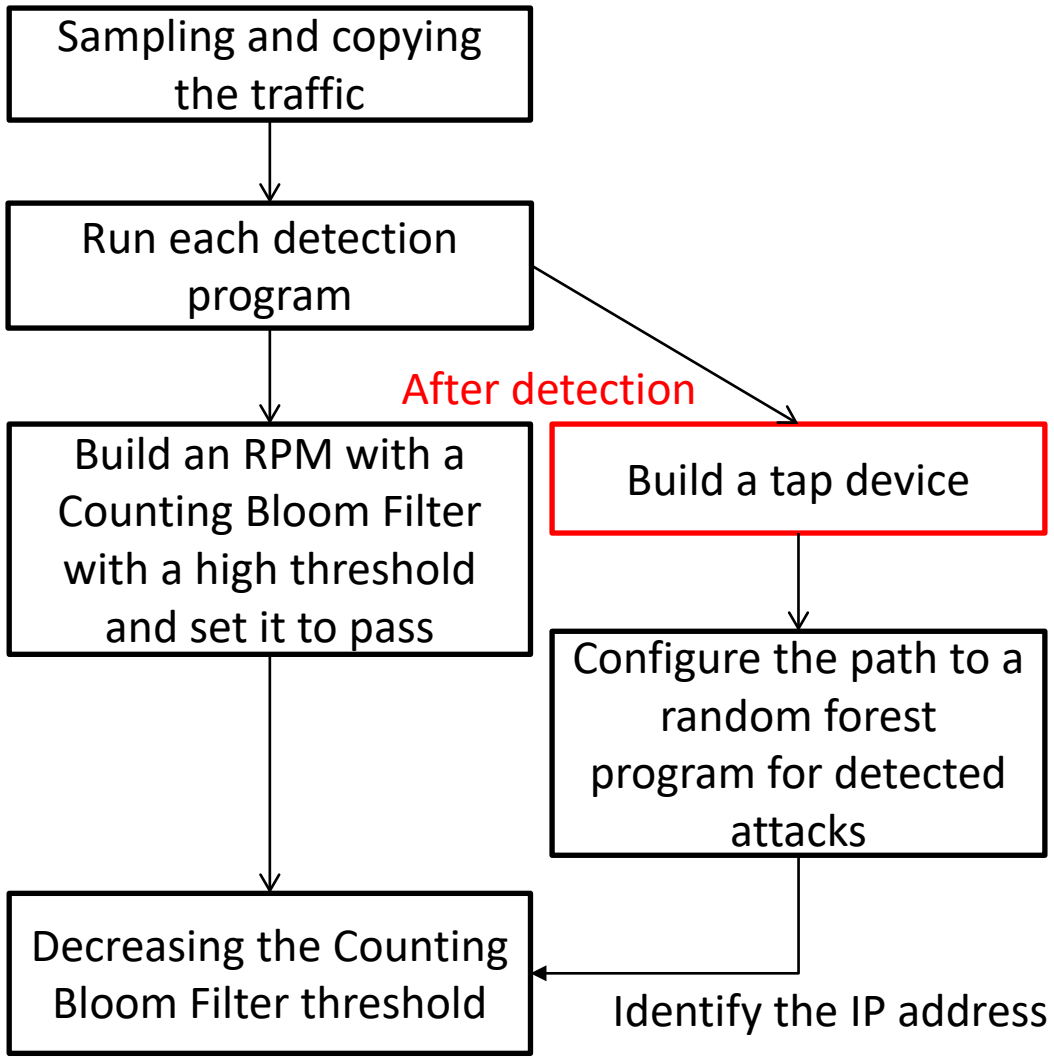


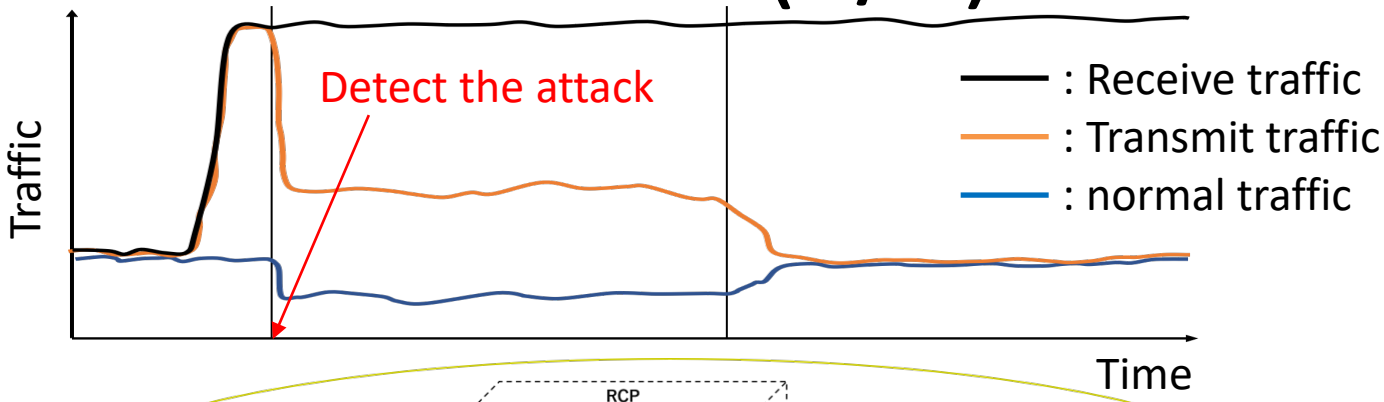


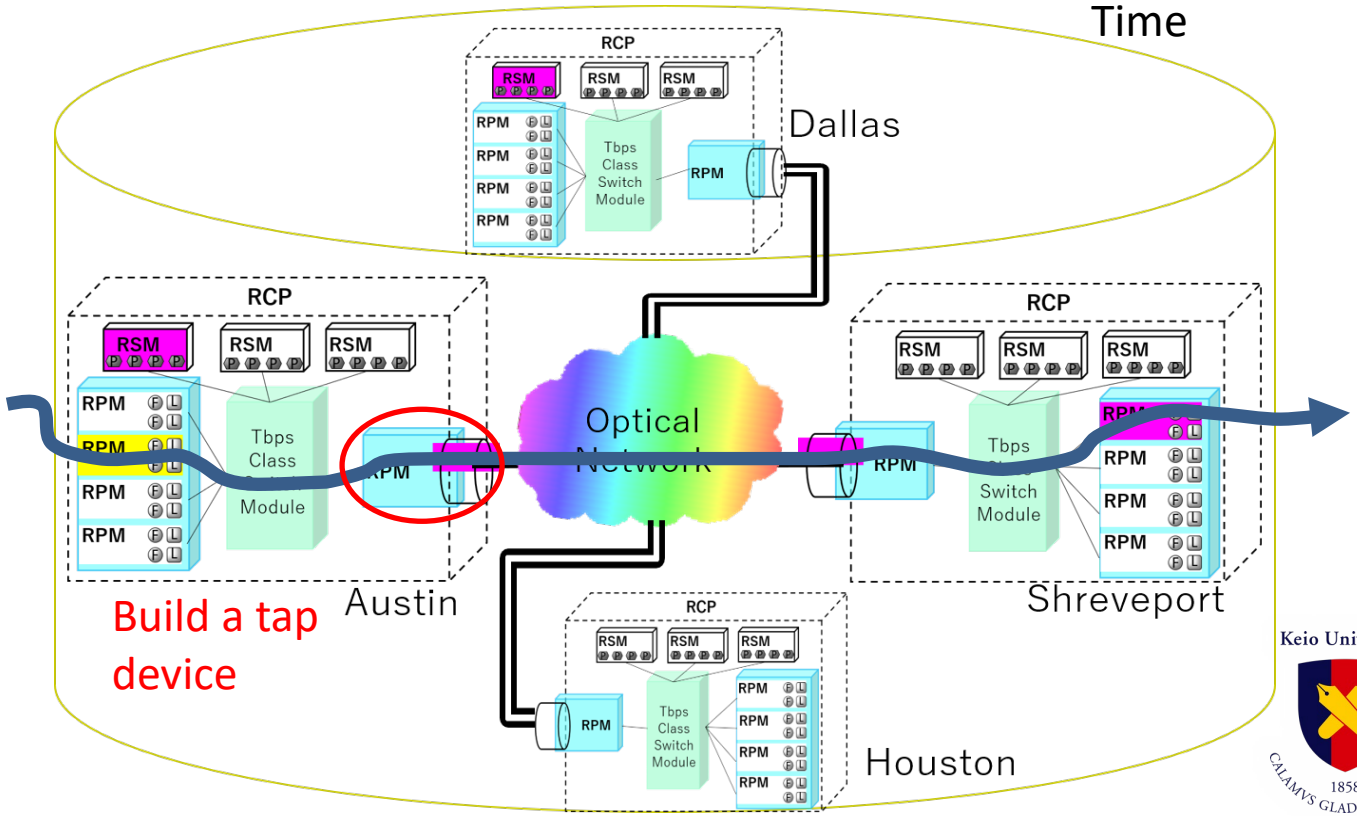
NET-CENTRIC

Keio University
1858
CALAMVS GLADIO FORTIOR

Proposed method: Flowchart(3/5)







NET-CENTRIC

Keio University
1858
CALAMVS GLADIO FORTIOR

Proposed method: Flowchart(4/5)

Sampling and copying the traffic

Run each detection program

After detection

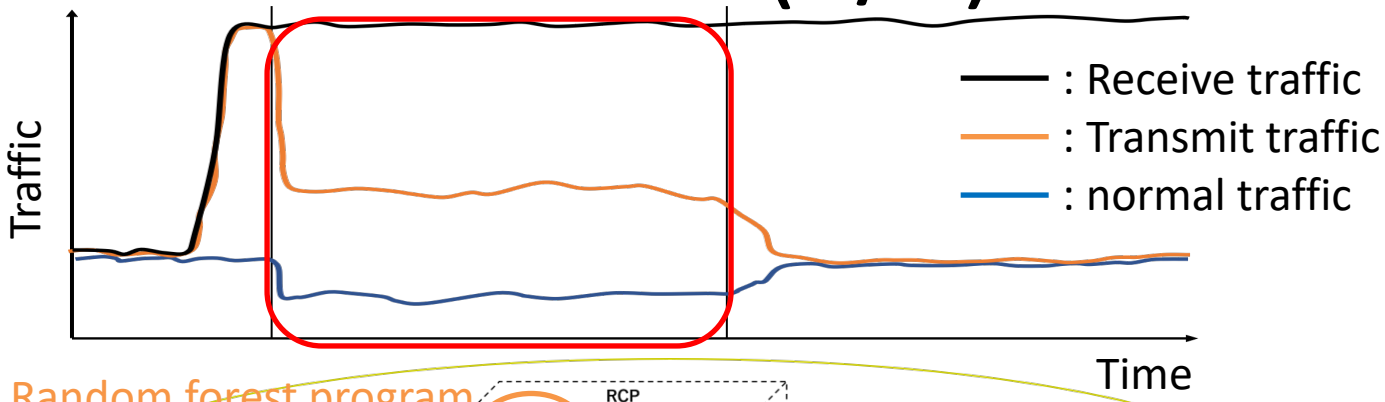
Build an RPM with a Counting Bloom Filter with a high threshold and set it to pass

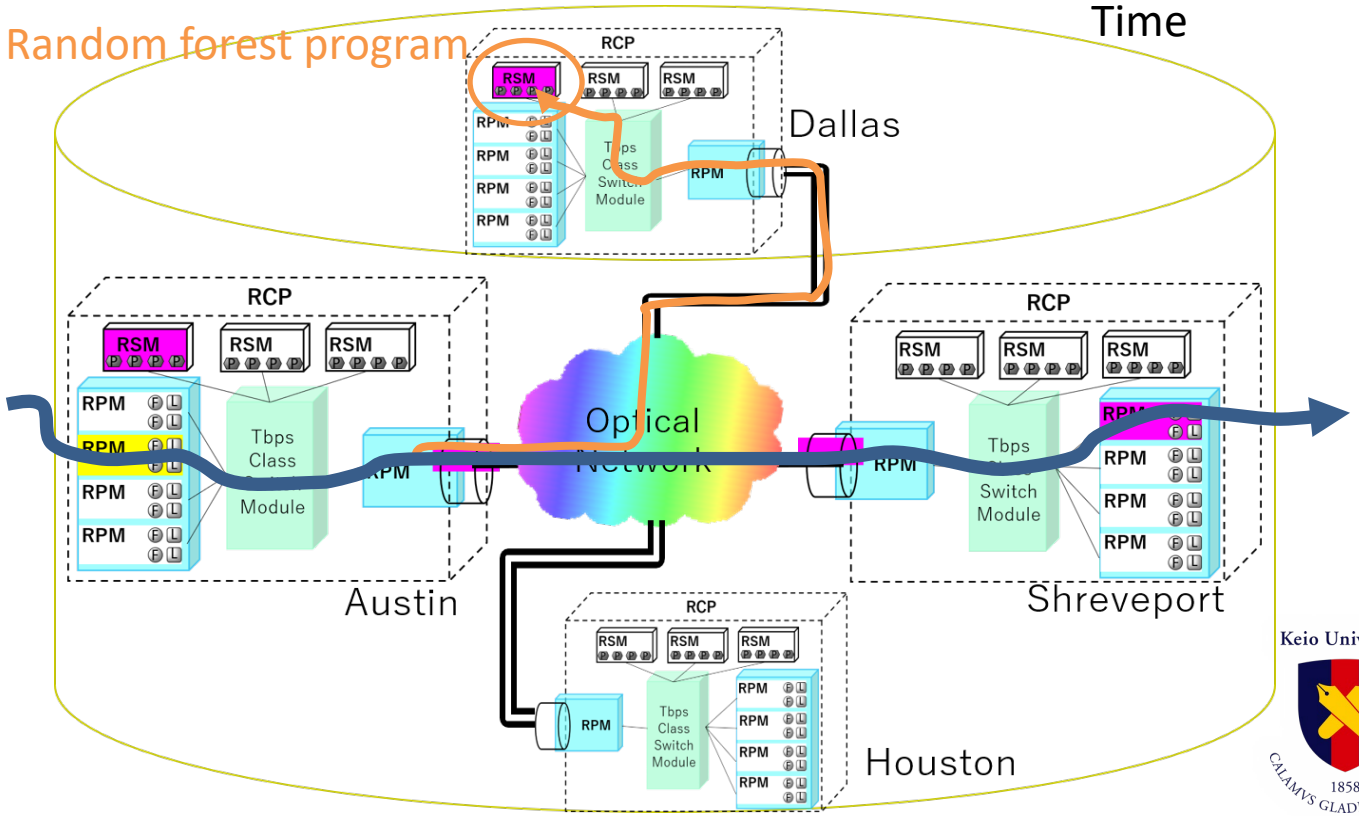
Build a tap device

Configure the path to a random forest program for detected attacks

Decreasing the Counting Bloom Filter threshold

Identify the IP address





NET-CENTRIC

Keio University
1858
CALAMVS GLADIO FORTIOR

Proposed method: Flowchart(5/5)

Sampling and copying the traffic

Run each detection program

After detection

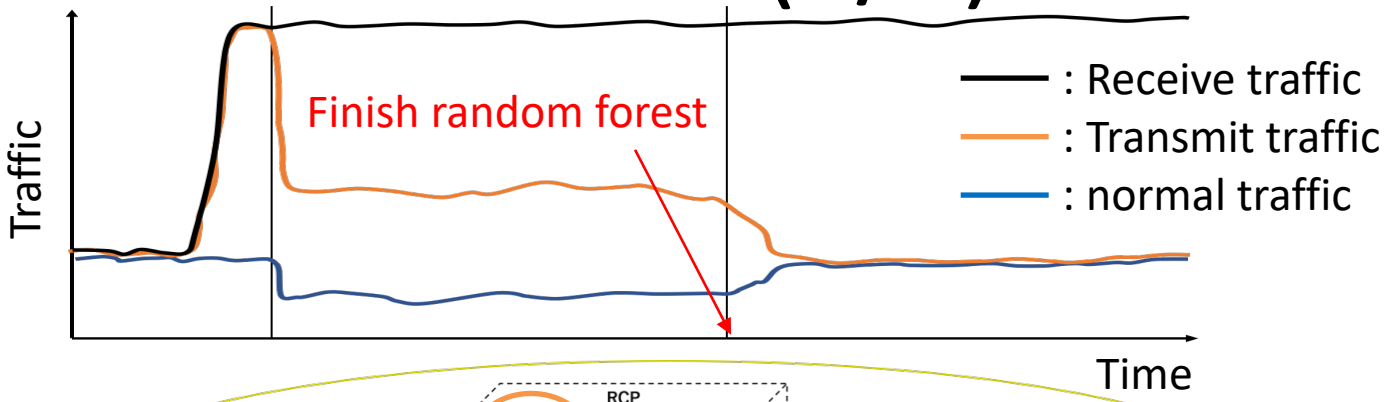
Build an RPM with a Counting Bloom Filter with a high threshold and set it to pass

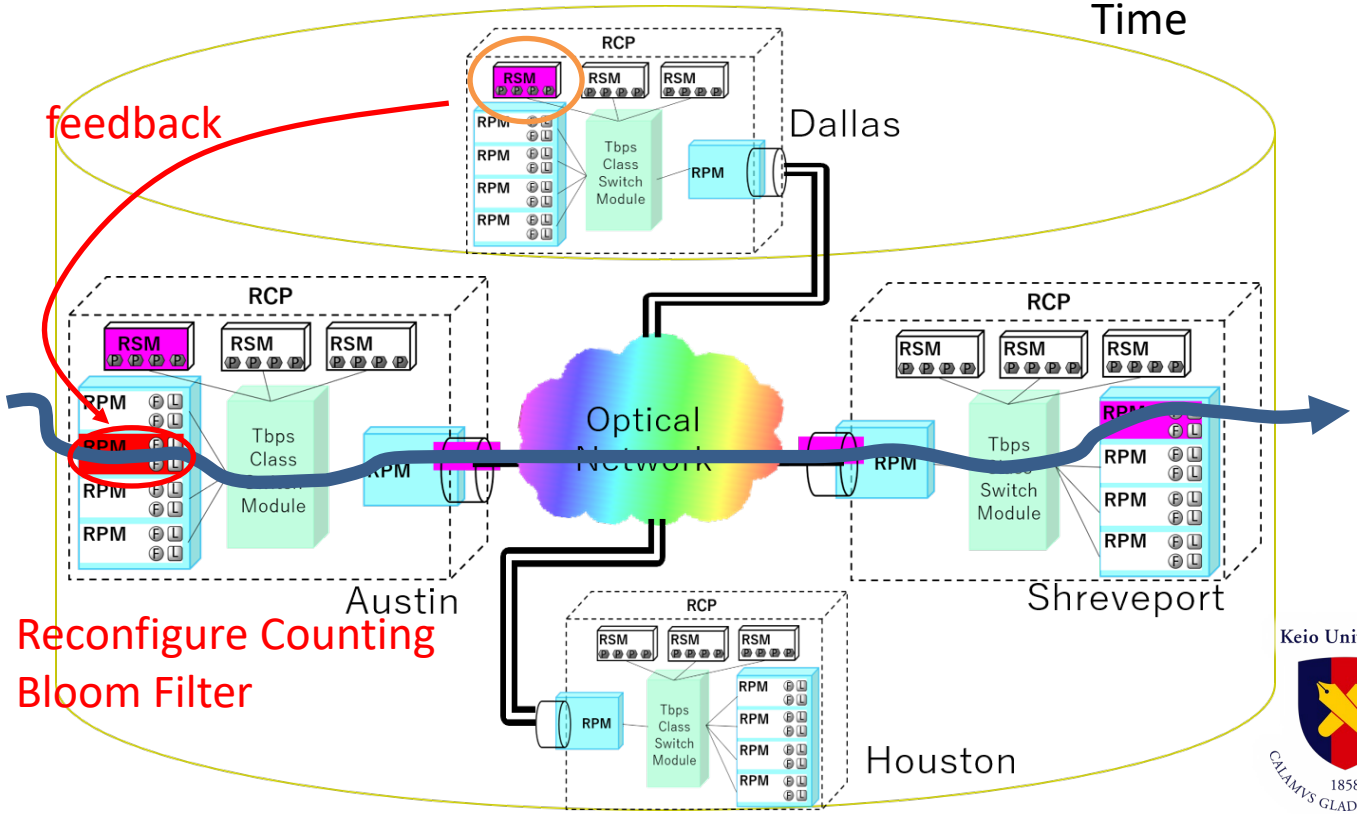
Build a tap device

Configure the path to a random forest program for detected attacks

Decreasing the Counting Bloom Filter threshold

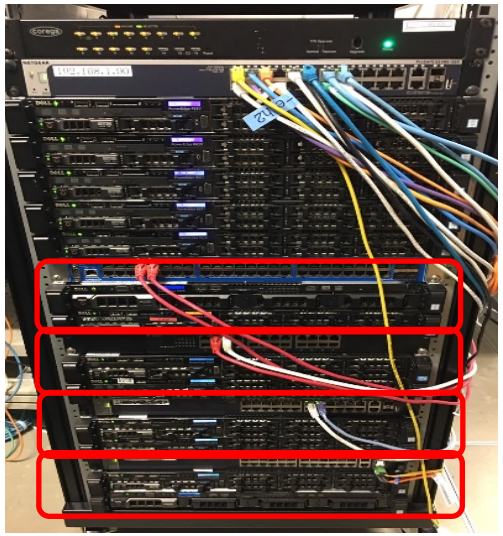
Identify the IP address





NET-CENTRIC

Keio University
1858
CALAMVS GLADIO FORTIOR



Experimental Environment

NET-CENTRIC

Keio University
1858
CALAMVS GLADIO FORTIOR

Conclusion

- DDoS attacks have been considered as a serious threat.
- Reconfigurable Communication Processor and resource pool architecture has been proposed.
- We proposed DDoS defense method with Counting Bloom Filter using Reconfigurable Communication Processor.
- We will evaluate the performance of proposed method in the near future.