Two-Level Detection Method of DDoS Attack Mimicking CDN Caches

Kazuya Taniguchi, Noriaki Kamiyama
Ritsumeikan University, Japan

Research Background (CDN Dissemination)

- CDN(Content Delivery Network):
  Distributed Network for Fast and Efficient Content Delivery Over the Internet

- CDN Market Share: Increasing Trend Annually
  - CDN Market Growth Forecast:
  2024: $19.96 Billion → 2029: $42.46 Billion

- Reasons for CDN Adoption:
  - Increased Demand for Online Content
  - Proliferation of Mobile Internet
  - Global Access Demands
  - Availability of CDN Security Features

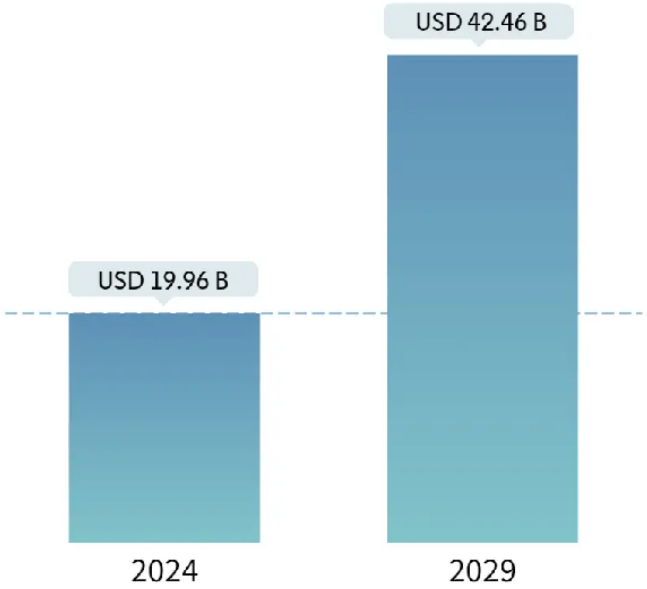


Figure: *Market Size and Market Share Analysis of Content Delivery Networks – Growth Trends and Growth Forecast (2024–2029) (Source: Mordor Intelligence)*

Research Background (Frequent DDoS Attacks)

- Increased frequency of DDoS attacks
  - Proliferation of attack methods
  - Vulnerability of IoT devices

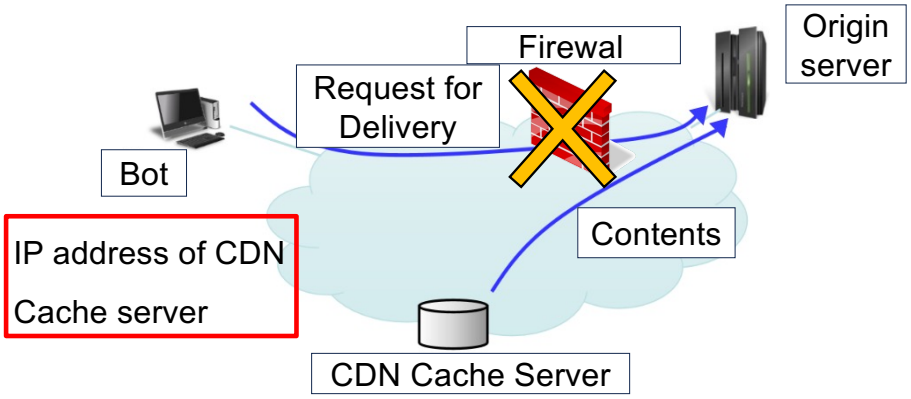
- Possible direct attack on OS (Origin Server)
  - Danger of an attack that cripples the OS by spoofing its IP address to launch a large-scale attack

Research Challenges

- Possibility of direct attack
  - The attacker identifies the IP address of the target server and sends packets directly to the identified IP address

  ⇒ DDoS attack is established
  - Packets arriving from other than CDN cache servers are blocked by firewalls
- Possibility that the attacker falsifies the IP address of the CDN cache server as the originating address

⇒ If DDoS packets are sent, they cannot be detected by the firewall



Utilization of DNS name resolution processing logs

- Detection Method
  - Normal requests via cache servers: Leave logs on the Domain Name System server
  - DDoS requests targeting origin servers directly: Do not leave DNS resolution logs

- By verifying DNS resolution logs:
  - If logs exist: Process the request
  - If logs do not exist: Reject the request as a DDoS attack

⇒ Checking DNS logs for all requests increases load on OS

Research Purpose

- Differences in Request Patterns
  - Normal requests: Triggered during cache misses
  - DDoS attacks: Generate an overwhelming number of requests in short intervals

⇒Attacks are detected by setting a threshold for the arrival interval

Problems: Threshold-based detection identifies anomalies but may lead to false positives/negatives

- Using Z-Score
  - Real-time outlier detection with adaptive threshold adjustment

Two-step detection

- Detection of the attack method in question by checking the DNS name resolution logs

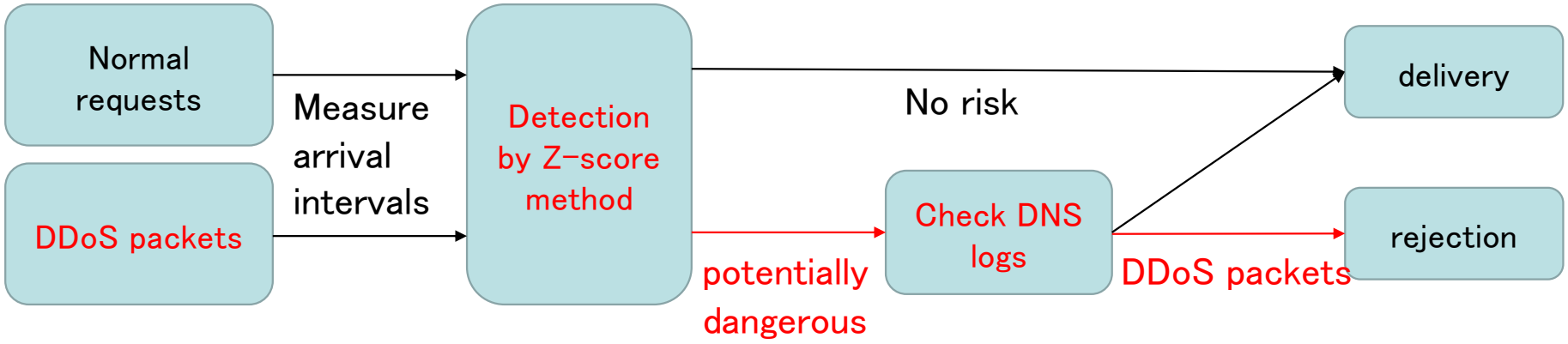
⇒ Concerns about processing load if all requests are checked

- Consider ways to reduce the load on the origin server

⇒ Implement two-step detection

  - Detect dangerous requests based on differences in request generation patterns from arrival intervals

⇒ Introduce Z-score to change threshold dynamically

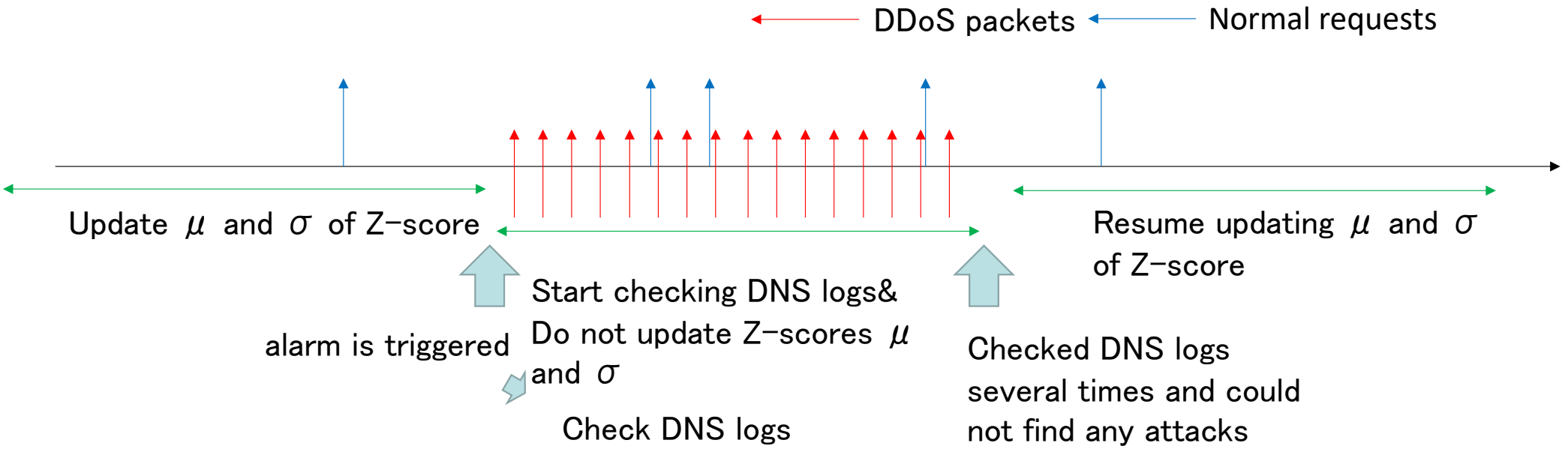


Z-Score-Based Detection Details

- Detection method with Z-score introduction
  - Utilize the inverse of the arrival interval as data

  ⇒ Detects that DDoS packets have occurred based on the difference in arrival intervals
  - Incorrect data during an attack is not reflected in the average

  ⇒ Detects different arrival interval patterns than when only normal requests are occurring



Computational Complexitly

- Time computation for DNS log search process
  - Assuming linear search
  - Worst-case time complexity is O(n) for n entries

- Time complexity of Z-score algorithm
  - $Z = (X - \mu) / \sigma$
    - (Z is the Z-score, X is the input value, μ (mu) is the mean, and σ (sigma) is the standard deviation)
  - Since it is a simple formula, the mean and standard deviation can be pre-computed to output results instantly

  ⇒ The time complexity of the Z-score algorithm is independent of the number of inputs
  - Time complexity is O(1)

⇒ Difference in computational complexity between Z-score method and DNS log search enables reduction of processing cost

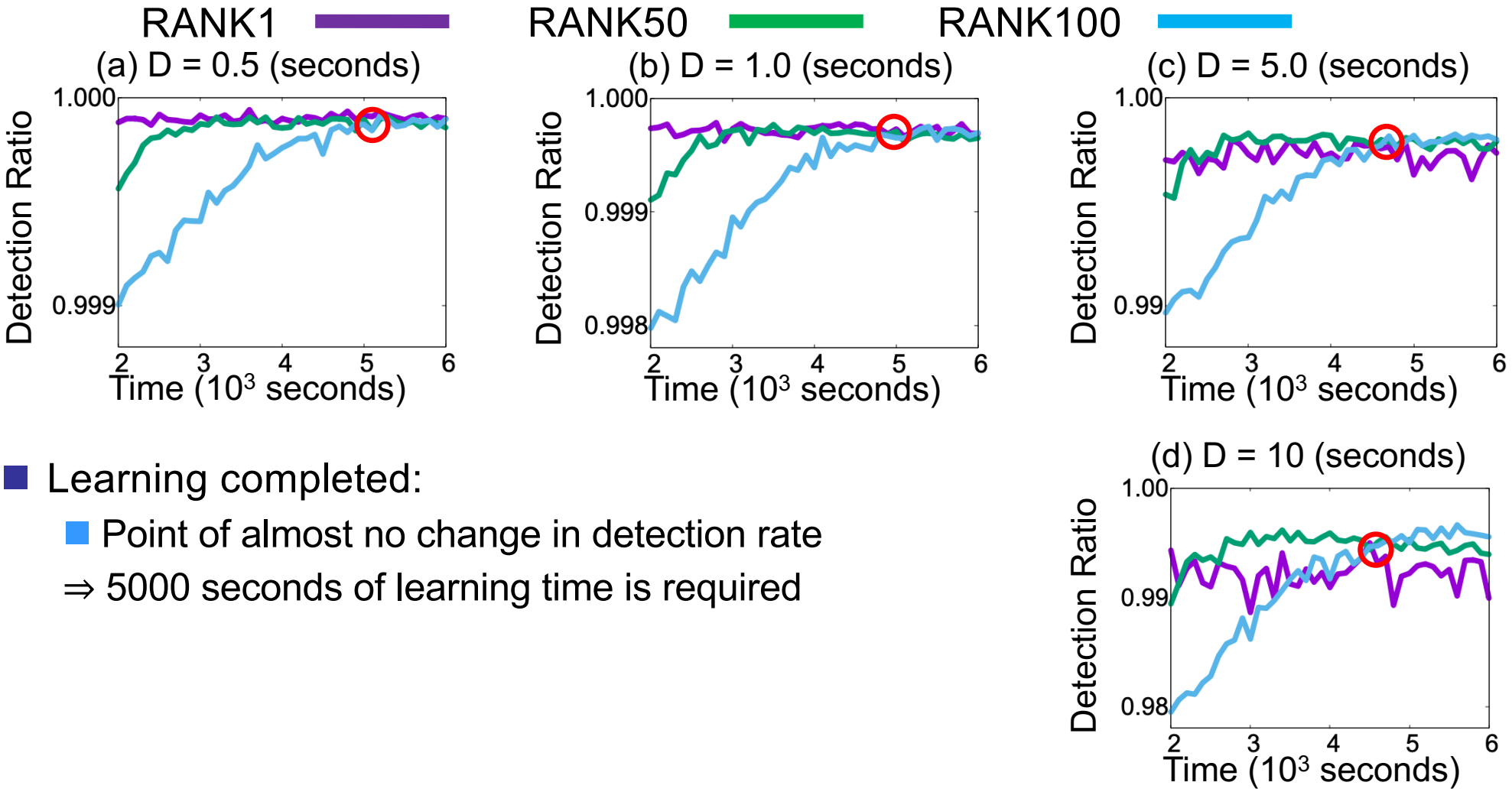
Simulation conditions

- Parameters for Z-score: lag (L): 10, threshold (η): 4.0, impact (α): 0.5
- Content Request Simulator Settings

Item	Set value
Simulation Time	10000 seconds
Content Type	100 pieces
Cache capacity	10 pieces
Average number of request occurrences	1 time
Period of attack	3000 seconds after 5000 seconds have elapsed

- Evaluation Item
  - Learning Time of proposed method
  - Performance Ratings based on Popularity
  - Performance evaluation based on attack frequency

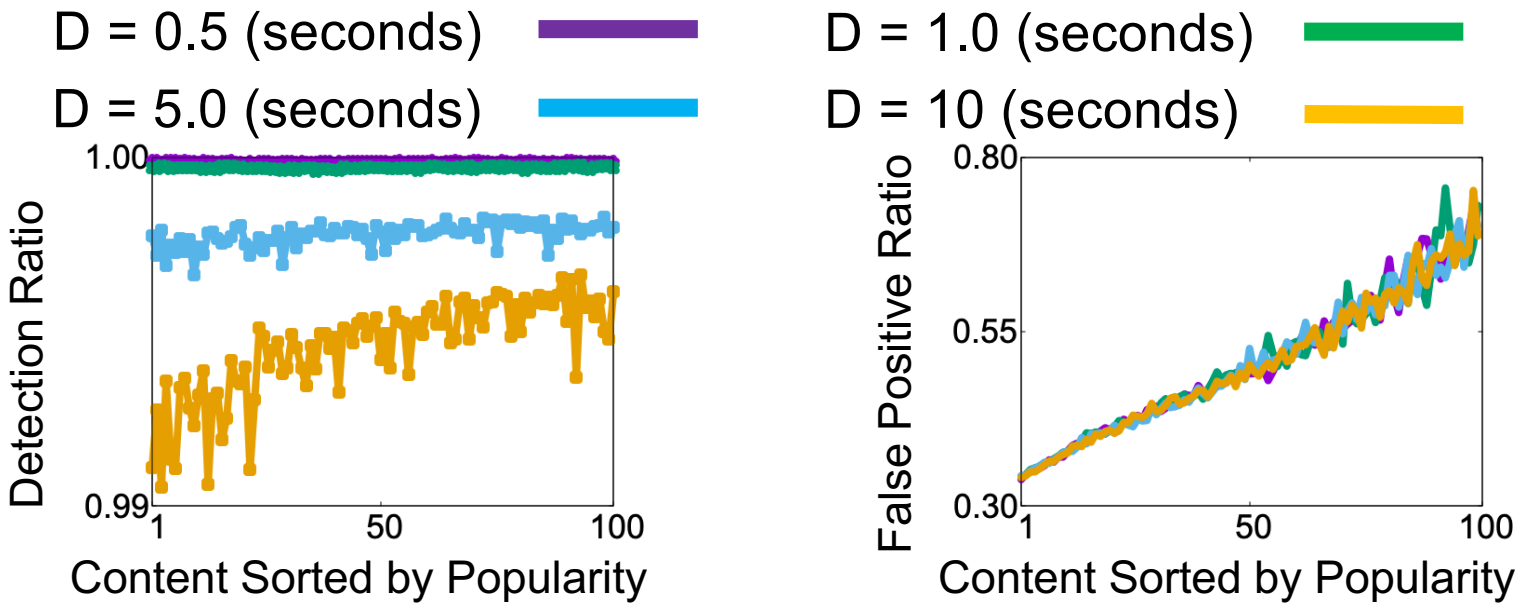
Learning Time of Proposed Method



- Learning completed:
  - Point of almost no change in detection rate

  ⇒ 5000 seconds of learning time is required

Performance Ratings based on Popularity



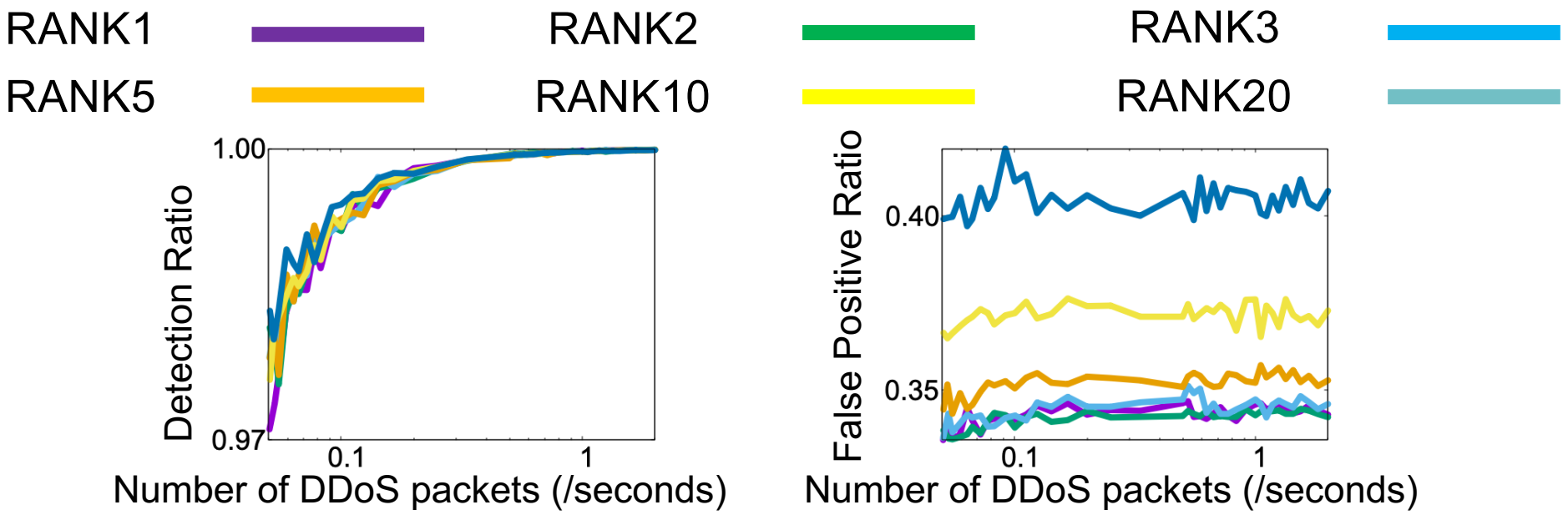
- Since we focus on the arrival interval, we assume that highly popular content is more difficult to detect

⇒ High detection rate of 99% or higher regardless of popularity

- False positive rate: 30-80%

⇒ Effective for highly popular content with a relatively high number of requests and high risk

Performance Evaluation based on Attack Frequency



- Detection rate: Higher arrival rate of DDoS packets facilitates detection

⇒ Detection rate increases as detection rate increases, and detection rate is almost 100%

- False positive rate: independent of DDoS arrival rate

conclusion

- In this study, a two-stage detection approach using the Zscore method was used to detect possible attacks that cannot be detected by firewalls

⇒ the load on the OS was significantly reduced

- Future Works
  - we are considering implementing a method to narrow down dangerous CDN cache servers by focusing on the type of source IP address

  ⇒ By doing so, it is not necessary to apply the proposed method to all of the large number of CDN cache servers, and we believe that further cost reduction will be possible