응답 시간 기반의 EDoS 공격 대응 기법

YoYo Attack에 특화된 방어 플랫폼

저자 **이강빈, 장진영, 강수민, 김태운** 소속 **부산대학교 정보컴퓨터공학부**

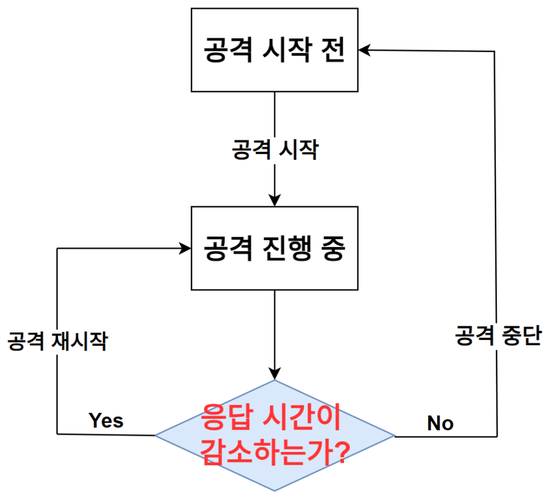
연구 배경 및 목표

기존 DDoS의 방어법은 대규모 트래픽 공격을 막는 데 초점을 두고 있어, 클라우드 시스템을 대상으로 지속적인 트래픽을 발생해 경제적 손실을 유도하는 EDoS를 방어하기에는 적절하지 않다. 우리는 EDoS 중 하나인 **YoYo Attack**에 대해 연구한다.

- YoYo Attack에 대응하기 위한 **방어 매커니즘을 개발**한다.
- 개발한 YoYo Attack 방어 매커니즘을 검증할 수 있는 **실험 환경을 구축**한다.

연구 방법

공격자 중요 지표: 요청에 대한 **응답시간**



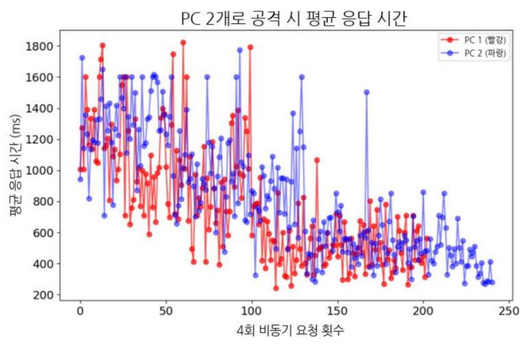
요청의 **응답시간**을 교란하자

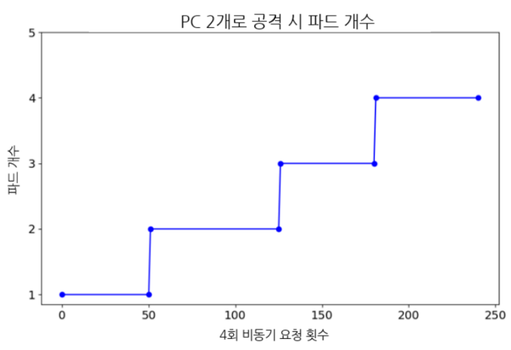
요청 횟수에 비례한 방어 매커니즘 적용

매커니즘 이름	매커니즘 설명
특정 IP SLEEP	• IP의 요청 횟수에 비례하여 Thread Sleep Time을 설정 • 해당 시간 만큼 **Thread Sleep을 적용**
VM 방화벽 이용 확률적 패킷 드랍	• IP의 요청 횟수에 비례하는 확률 설정 • 확률에 따라 해당 **IP의 패킷 드랍을 적용**
더미 서버 기반의 확률적 리다이렉트	• IP의 요청 횟수에 비례하는 확률 설정 • 확률에 따라 **응답을 지연하는 더미 서버로 리다이렉트**

연구 결과

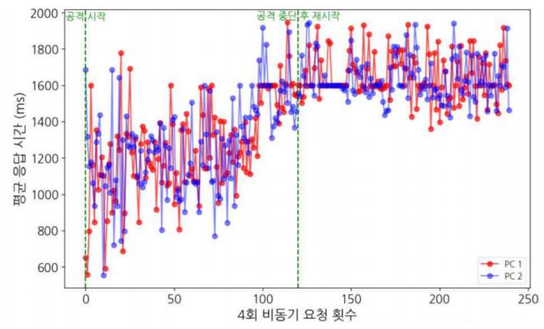
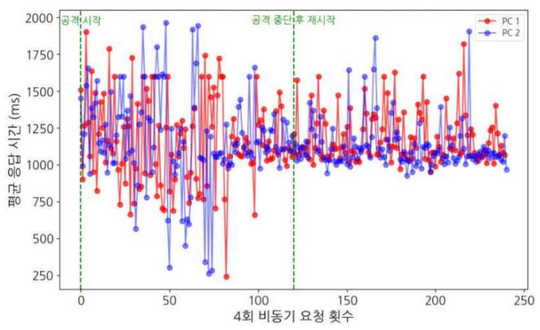
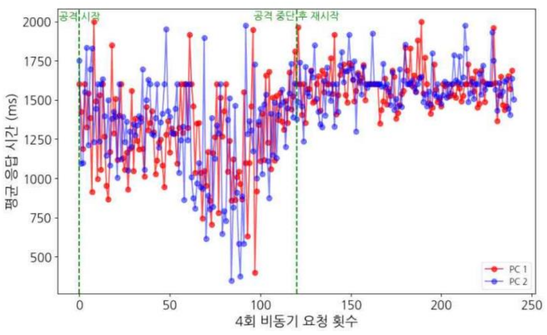
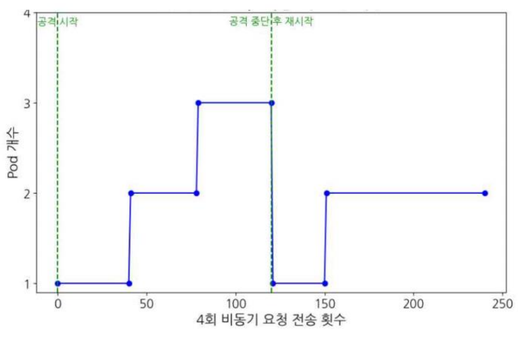
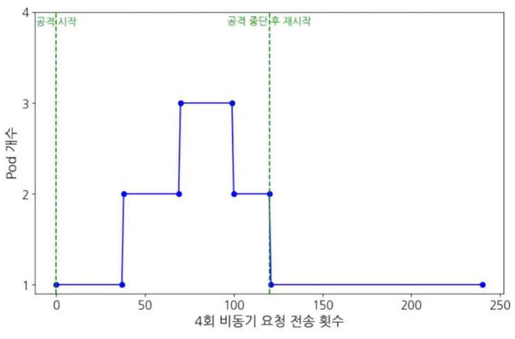
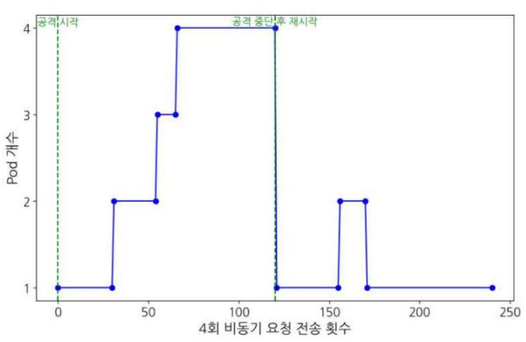
방어 매커니즘이 없을 때 공격 결과





- 응답 시간 경향성이 뚜렷하게 우하향을 보인다.
- Pod가 최대 개수까지 증가하여 **경제적 손실 발생**한다.
- 공격자는 해당 패턴의 공격을 반복한다.

방어 시스템 적용

	특정 IP SLEEP 방어법	VM 방화벽 이용 확률적 패킷 드랍	★ 더미 서버 기반의 확률적 리다이렉트
응답시간			
파드개수			

연구 결론

본 연구에서 개발한 방어 매커니즘을 실험 환경에서 검증한 결과, 다음과 같은 결론을 얻었다.

1. 방어 매커니즘은 공격자의 응답 시간을 교란하여 우하향 경향성을 없애고, 이를 통해 **공격을 중단하도록 유도**한다.
2. 방어 매커니즘을 적용함으로써 서버 부하를 줄이고 Pod 개수를 낮은 수준으로 유지하여 **경제적 손실을 감소**시킨다.

본 연구에서 개발한 방어 매커니즘을 통해 클라우드 환경에서의 자원 남용을 방지하고, 서버의 안정적인 운영을 도모할 수 있을 것으로 기대된다.