32 클라우드 컴퓨팅 공격 및 방어 플랫폼 개발

- YoYo Attack에 특화된 방어 플랫폼

소속 정보컴퓨터공학부 분과 C 팀명 DDALPI 참여학생 이강빈, 장진영, 강수민 지도교수 김태운

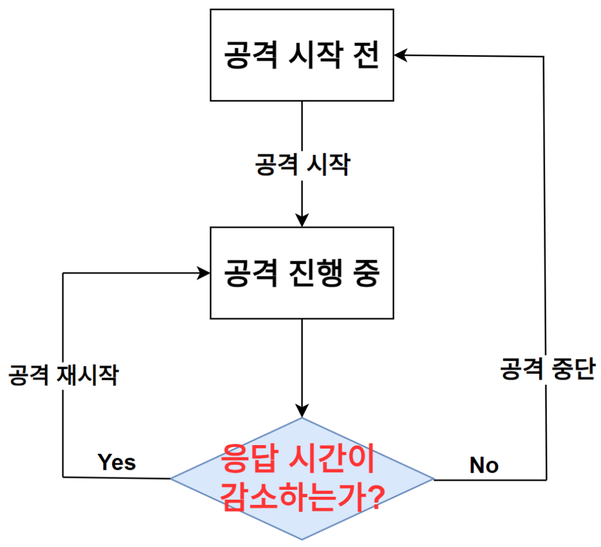
과제 목표

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**하고, 이의 효과성을 검증하기 위한 YoYo Attack **공격 알고리즘을 개발**한다.
- 공격 현황과 공격 대상 서비스의 상태를 시각적으로 보여주는 **대시보드를 개발**한다.
- 구현한 YoYo Attack 공격 및 방어 알고리즘을 검증할 수 있는 **실제 환경을 구축**한다.

과제 구성

공격자 중요 지표: 요청에 대한 **응답시간**



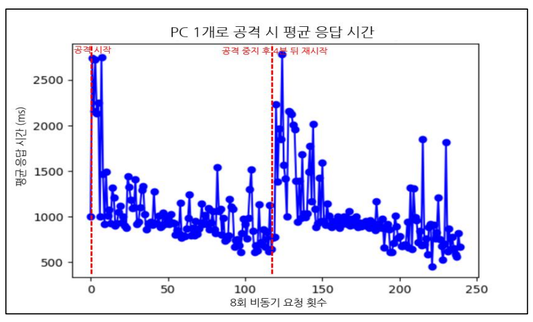
요청의 **응답시간**을 교란하자

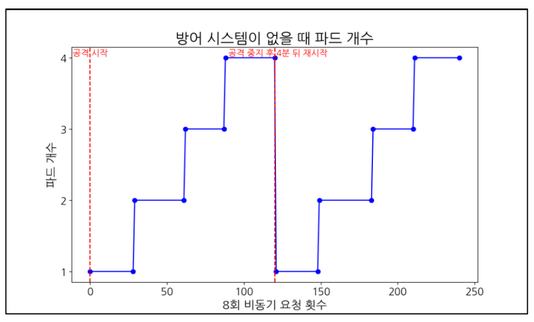
요청 횟수에 비례한 방어 매커니즘 적용

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**
OpenWRT를 이용한 중개방어	• IP의 요청 횟수에 비례하여 지연 시간 설정 • **라우터에서 지연 시간 만큼 응답을 지연**

과제 결과

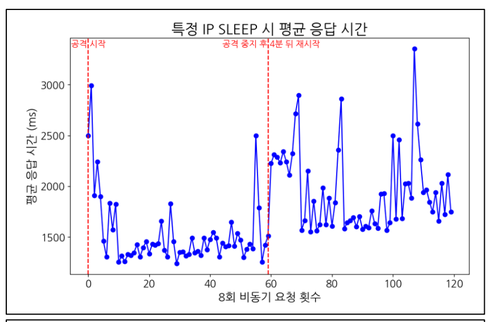
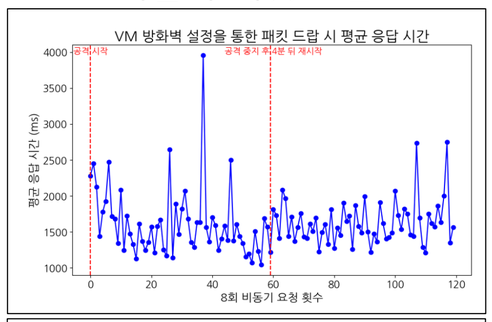
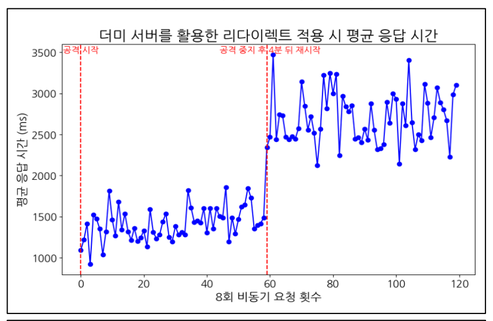
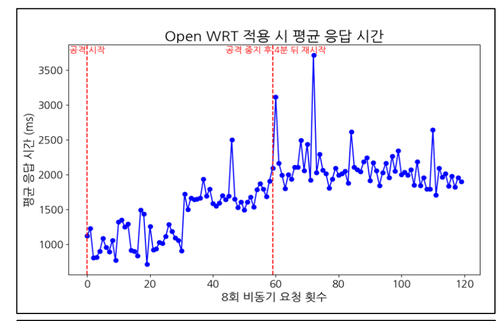
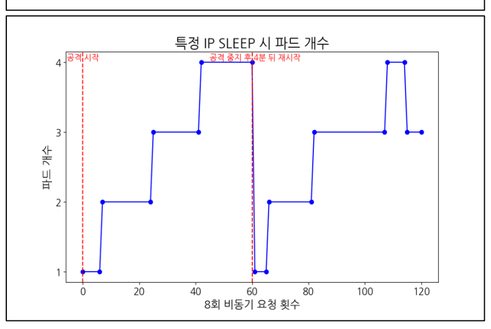
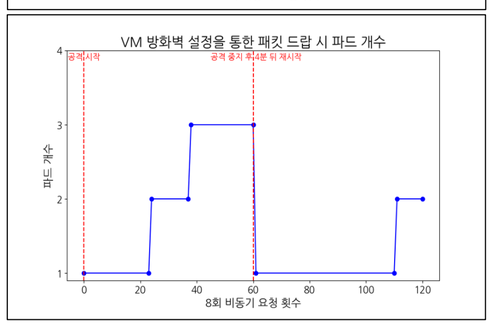
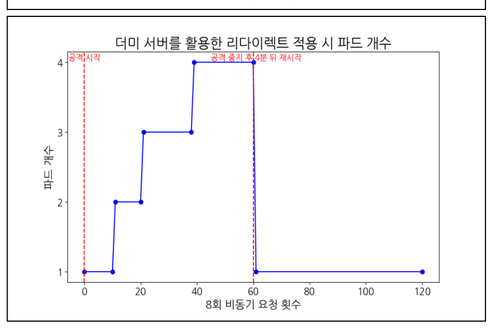
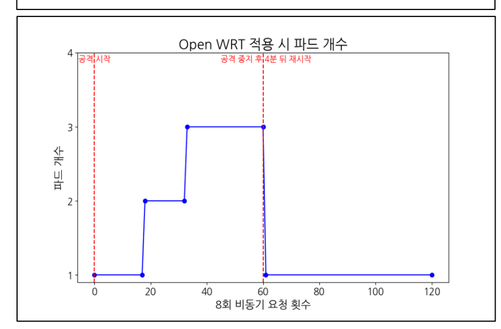
방어 시스템이 없을 때 공격 결과





- 응답 시간 경향성이 뚜렷하게 우하향을 보임
- Pod가 최대 개수까지 증가하여 **경제적 손실 발생**

방어 시스템 적용

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

결론

- 응답 시간의 우하향 경향성이 사라짐 → **응답시간 교란 성공**
- Pod 개수가 최대까지 증가하지 않음 → **경제적 손실 감소**