저사양 환경에서 eBPF/XDP 기술을 이용한 대용량 DDoS 공격 대응 방안

함준형*, 라민우*, 김도현*, 강성원*, 임정훈*, 최홍석*, 지도환*, 이민우**

*한국정보기술연구원 화이트햇스쿨 2기, **국립한국해양대학교

How to respond to high-capacity DDoS attacks using eBPF/XDP technology in low-spec environments

Junhyeong Ham*, Minwoo Ra*, Dohyun Kim*, Seongwon Kang*, Jeonghun Lim*, Hongseok Choi*, Dohwan Ji*, Minwoo Lee**

*KITRI, **Korea Maritime & Ocean University

요 약

본 연구는 저사양 환경에서 DDoS 공격에 효율적으로 대응할 수 있는 eBPF/XDP 기 반 기술을 제안한다. 기존 DPI와 DPDK 기술이 고사양 장비를 요구하는 반면, 제안된 방식은 커널 수준에서 패킷을 처리함으로써 저사양 시스템에서도 효과적인 대응이 가능 하다. 실험 결과, 싱글 코어 환경에서도 0.5Mpps의 트래픽을 처리할 수 있었으며, 기존 방식에 비해 최대 83.87%의 리소스 절감 효과를 확인하였다. 이 연구는 비용 효율적이면 서도 높은 성능을 제공하는 DDoS 대응 솔루션 개발에 기여할 것으로 기대된다.

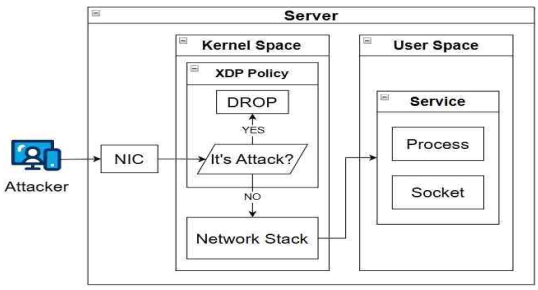
I. 서론

최근 DDoS(Distributed Denial of Service) 공격이 급증하고 있으며, 저렴한 비용으로 대규모 공격을 제공하는 DaaS(DDoS as a Service)의 확산으로 기업 서비스 운영에 심각한 위협이 되고 있다. 이러한 공격에 대응하기 위해 다양한 기술이 사용되고 있으나, 각각 한계점을 가지고 있다.

DDoS 공격 대응에 주로 사용되는 기술로는 DPI(Deep Packet Inspection)와 DPDK(Data Plane Development Kit)가 있다. DPI는 패킷의 헤더와 페이로드를 모두 검사하기 때문에 대용량 패킷을 분석하고 필터링하는 데 한계가 있다. DPDK는 네트워크 스택을 우회하여 사용자 공간에서 다중으로 패킷을 처리하기 때문에 고성능 하드웨어를 필요로 한다.

본 논문에서는 기존 처리 방법의 한계를 극복하기 위해 eBPF(extended Berkeley Packet Filter)와 XDP(eXpress Data Path) 기술의 활용 방안을 제안한다. eBPF/XDP는 커널 수준에서 동작하여 효율적인 패킷 처리가 가능하며, 저사양 환경에서도 높은 성능을 발휘할 수 있다.

실험을 통해 XDP의 패킷 처리 능력을 활용하여 실시간으로 위협을 탐지하고 차단할 수 있음을 보이고자 한다. 제안하는 방법을 통해 저사양 환경에서도 효과적인 DDoS 공격 대응이 가능함을 제시하며, 이는 비용 효율적이면서도 성능이 우수한 DDoS 대응 솔루션 개발에 기여할 것으로 기대된다.



[그림 1] XDP를 활용한 고성능 패킷 필터링

II. XDP 기반 DDoS 대응 방안 설계

2.1 eBPF/XDP의 특징과 장점

eBPF/XDP는 커널 수준에서 동작하며 네트워크 스택과 밀접하게 통합되어 높은 성능과 효율성을 제공한다. 특히 eBPF/XDP는 다음과 같은 장점이 있다.

첫째, 네트워크 스택의 보안 기술과 긴밀하게 통합되어 커널의 고유 보안 기능을 활용할 수 있다. 둘째, 기존 네트워크 설정이나 관리 도구의 수정 없이도 적용이 가능하다. 셋째, 그림 1에서처럼, 커널 내에서 공격 여부를 판단하고 이를 실시간으로 차단(XDP_DROP)하여 패킷 처리를 최적화할 수 있다. 넷째, 사용자 공간과 커널 간 오버헤드를 줄여 네트워크 성능을 향상시키며, 서비스 중단 없이 실시간으로 네트워크를 프로그래밍할 수 있는 유연성을 제공한다.

```
Algorithm 1 Packet Processing Algorithm
Require: Packet p
Ensure: XDP_ACTION
if CheckProtocol(p) && CheckBanned(p) then
  return XDP_DROP

if IsRateOverLimit(p) && IsDataOverLimit(p) then
  return XDP_DROP

return XDP_PASS
```

```
Functions
CheckProtocol (Packet p):
  return p is IP and not ICMP/UDP/TCP invalid

CheckBanned(Packet p):
  return p is not in the BannedIPs list

IsRateOverLimit(Packet p):
  return p (from the same IP) does not exceed the
  defined packets-per-second (PPS) limit.

IsDataOverLimit(Packet p):
  return p (from the same IP) does not exceed
  the defined Bytes-per-second (BPS) limit.
```

```
Persistence
PerIPStats:
  - type: BPF_MAP_TYPE_LRU_HASH
  - data:
    (IP_ADDRESS : struct {
        PacketReceived
        TotalData
        LastActiveTime
    })
BannedIPs:
  - type: BPF_MAP_TYPE_LRU_HASH
  - data: (IP_ADDRESS : Count)
```

[그림 2] XDP 의사 코드

마지막으로, 트래픽의 양에 따라 CPU 자원을 유동적으로 조정할 수 있다.

이러한 특징으로 인해 eBPF/XDP는 CPU 코어 5개를 기준으로, 최대 100Mpps 속도로 패킷을 처리할 수 있어, 저비용/고가용성의 DDoS 방어 체계를 운영할 수 있다.

2.2 DDoS 공격 대응 방안 구현

본 연구에서는 eBPF/XDP를 이용하여 DDoS 공격 유형에 맞는 방어 코드를 구현하였다. 주요 특징은 다음과 같다. 첫째, 전송된 패킷은 eBPF Map에 저장되어 효율적으로 관리할 수 있다. 둘째, 과도한 패킷 전송 속도 기준을 20pps로 설정하고, 이를 초과하는 트래픽은 비정상 행위로 간주한다. 셋째, 비정상적인 패킷은 XDP_DROP행위를 통해 커널 자원의 사용을 최소화한다.

그림 2에서는 XDP 기반의 패킷 처리 알고리즘을 보여준다. 이 알고리즘은 먼저 패킷의 유효성을 검사하고(CheckProtocol), 비정상적인 트래픽을 감지하여(IsAbuseTraffic), 필요한 경우 XDP_DROP을 실행한다. 또한, Persistence기능을 통해 IP 주소 및 트래픽 패턴을 BPF Map에 저장하여 지속적인 관리가 가능하다.

이와 같이 설계된 eBPF/XDP 기반 DDoS 대응 시스템은 DDoS 공격을 효과적으로 처리할 뿐만 아니라, 전체 네트워크 성능을 최적화할 수 있는 유연한 솔루션을 제공한다. 또한, DDoS 공격의 복잡성과 규모가 증가하는 상황에서도 네트워크를 안정적으로 보호할 수 있는 방안을 제시한다.

[표 1] Resource utilization comparison

Sortation	Resource Utilization (%)			
	1 Core	2 Core	4 Core	8 Core
nDPI	84%	77.32%	43.5%	18.6%
DPDK	Unable	62.7%	35.64%	12.26%
eBPF/XDP	36.1%	22.1%	11.8%	3%

또한, DDoS 공격의 복잡성과 규모가 증가하는 상황에서도 효과적으로 대응할 수 있는 솔루션을 제공한다.

III. 성능 평가 및 분석

기존의 nDPI와 DPDK 기술과 제안된 eBPF/XDP 방식을 비교하여 성능을 테스트하였다. 테스트는 1 Core부터 8 Core까지의 저사양 환경에서 0.5Mpps의 UDP Flooding 공격을 기준으로 진행되었으며, hping3 도구를 사용하였다.

표 1에서 알 수 있듯이, 2 Core부터 eBPF/XDP는 nDPI와 DPDK에 비해 확연한 차이를 보였다. eBPF/XDP는 2 Core에서 71.42%, 4 Core에서 72.87%, 8 Core에서 83.87% 감소한 리소스 사용률을 기록하였다. 이는 eBPF/XDP가 저사양 환경에서도 적은 리소스로 동일한 트래픽을 처리할 수 있음을 나타낸다.

3.1 사례 연구 및 비교 분석

본 연구의 성능 평가 결과는 실제 사례와 비교를 통해 실무적인 적용 가능성을 논의할 수 있다. Cloudflare의 L4Drop 시스템은 XDP와 eBPF를 사용하여 네트워크 인터페이스 수준에서 초당 수백만 개의 패킷을 효율적으로 필터링하는 DDoS 완화 솔루션을 구현한 사례이다. 이 사례는 본 연구와 유사하게 저비용의 리소스 사용으로 고성능의 패킷 처리가 가능함을 보여준다.

IV. 결론

본 논문에서는 커널 수준에서 대규모 DDoS 공격을 효율적으로 처리하기 위한 eBPF/XDP 방식을 제안하였으며, 이를 통해 기존 사용자 공간에서 처리되던 방식보다 적은 리소스로 패킷 처리가 가능함을 확인하였다. Cloudflare 사례를 통해 실무적으로 적용할 수 있는 가능성도 시사하였다.

향후 연구에서는 자원 효율성을 더욱 극대화하여 제한된 시스템 자원에서도 안정적이고 지속적인 DDoS 방어를 구현할 수 있는 방안을 모색할 계획이다.

[참고문헌]

[1] M. Abranches et al., "LinuxFP: Transparently Accelerating Linux Networking," IEEE ICDCS, pp. 543-554, 2024.

[2] R. T. El-Maghraby et al., "A survey on deep packet inspection," Proc. ICCES, pp. 188-197, 2017.

[3] M. Wu, Q. Chen, and J. Wang, "Toward low CPU usage and efficient DPDK communication in a cluster," J. Supercomput., vol. 78, no. 2, pp. 1852 - 1884, 2022.

[4] J. H. Han et al., "The eXpress Data Path: Fast Programmable Packet Processing in the OS Kernel," Proc. CoNEXT, pp. 54-66, 2018.