NCP 기반의 광대역 융합 망에서 DDoS 공격 대응 기법 설계

정회원 한 경 은*, 양 원 혁**, 유 경 민**, 학생회원 유 재 영**
종신회원 김 영 선*, 김 영 천**°

Design of Defence Mechanism against DDoS Attacks in NCP-based Broadband Convergence Networks

Kyeong-Eun Han*, Won-Hyuk Yang**, Kyung-Min Yoo** *Regular Members,*
Jae-Young Yoo** *Student member,* Young-Sun Kim*, Young-Chon Kim** *Lifelong Members*

요 약

본 논문에서는 DDoS (Distributed Denial of Service) 공격에 따른 비정상적인 트래픽의 범람(flood)을 방지하고 합법적인 트래픽 전송을 보장하기 위하여 NCP (Network Control Platform) 기반의 DDoS 공격 대응 기법을 제안한다. 또한 이를 위하여 NCP와 SR (Source Router), VR (Victim Router)의 기능 모듈을 정의하고 high-flow 감지를 위한 임계값 및 공격 패킷 폐기율 결정식을 제안한다. 제안한 기법에서 NCP는 SR과 VR로부터 수집된 high-flow정보와 큐 정보를 기반으로 DDoS 공격 여부를 판단하고 이에 따라 패킷 폐기율을 결정한다. SR과 VR은 NCP에 의하여 결정된 패킷 폐기율에 따라 해당 플로우에 속하는 패킷을 폐기시킨다. 성능 평가를 위하여 OPNET 환경에서 시뮬레이션을 수행하고 SR, VR의 큐 크기, 공격 트래픽의 전송량 관점에서 비교 분석한다.

Key Words : DDoS, Attack Detection, Rate Limiting, BcN

ABSTRACT

In this paper, we propose the NCP (Network Control Platform)-based defense mechanism against DDoS (Distributed Denial of Service) attacks in order to guarantee the transmission of normal traffic and prevent the flood of abnormal traffic. We also define defense modules, the threshold and packet drop-rate used for the response against DDoS attacks. NCP analyzes whether DDoS attacks are occurred or not based on the flow and queue information collected from SR (Source Router) and VR (Victim Router). Attack packets are dopped according to drop rate decided from NCP. The performance is simulated using OPNET and evaluated in terms of the queue size of both SR and VR, the transmitted volumes of legitimate and attack packets at SR.

Ⅰ. 서 론

최근 새로운 서비스에 대한 수요가 폭발적으로 증가함에 따라 망도 점차 다양하고 복잡한 형태로 발전하고 있다. 그러나 망을 보호하고 제어하는 기술은 상대적으로 미흡하여 시스템 보안에 취약한 실정이며, 이러한 시스템 취약성을 이용한 망 공격도 빈번하게 발생하고 있어 사회적, 경제적으로 큰

※ 본 연구는 교육과학기술부와 한국산업기술재단의 지역혁신인력양성사업과 한국연구재단의 지원(2009-0077301)을 받아 수행된 연구결과입니다.
* 한국전자통신연구원, ** 전북대학교 컴퓨터공학과 영상정보신기술연구소(yckim@jbnu.ac.kr), (° : 교신저자)
논문번호 : KICS2009-04-166, 접수일자 : 2009년 4월 17일, 최종논문접수일자 : 2009년 12월 28일

손실을 초래하고 있다. 특히 최근 증가하고 있는 DDoS (Distributed Denial of Service) 공격은 인터넷 서비스를 제공하는데 있어 가장 큰 위협 요소가 되고 있다. DDoS 공격은 인터넷을 통하여 분포하는 대규모의 호스트들이 서로 협력하여 비정상적인 패킷을 대량으로 발생시키는 형태이다. 이러한 공격 형태는 모든 사용 가능한 망 자원 또는 공격대상(victim/target)의 시스템 자원을 소비하여 합법적인 사용자들이 시스템이나 망에 접근하여 서비스를 이용하는 것을 방해한다. 따라서 합법적인 사용자들의 서비스 보장과 망의 효율적인 관리를 위하여 DDoS 공격에 대한 효과적이고 실제적인 방어 기법이 요구되고 있다 [1]-[4].

기존의 DDoS 공격 대응 기법은 크게 목적지 라우터(Victim Router: VR) 기반의 방어 기법과 근원지 라우터(Source Router: SR) 기반의 방어 기법으로 구분된다 [5]-[7]. VR 기반의 방어 기법은 목적지 망(victim network)이나 망 근처에 위치하여 공격 패킷을 감지하고 대응하는 방법으로 가장 정확한 공격 패킷 감지 능력을 제공할 수 있다. 이는 VR이 victim의 상태를 가장 정확하게 관찰하고 서비스 저하의 조짐을 감지하기 쉽기 때문이다. 그러나 이러한 방어 기법을 사용하는 경우 공격 패킷이 victim까지 전송되는 동안 망의 상당 대역을 소비하게 된다. 또한 상당량의 통합된 트래픽이 VR에 유입됨에 따라 공격 패킷 감지를 위하여 많은 자원이 할당되어야 한다는 문제점이 있다. SR 기반의 방어 기법은 공격 패킷이 위치한 근원지 망(source network) 또는 근처에 위치하여 공격 패킷을 감지하고 대응하는 기법이다. 이 기법에서는 자신의 망 영역에 속한 트래픽만을 처리하므로 적은 자원 할당으로 트래픽 특성의 분석이 용이하다는 이점이 있다. 또한 공격 트래픽이 망에 유입되어 망 자원을 소모하기 전에 이를 감지하여 폐기하므로 망 자원을 효율적으로 사용할 수 있다는 특성을 갖는다. 그러나 DDoS 공격이 대규모의 호스트들이 협력하는 형태임을 고려할 때, 이 기법은 victim으로 향하는 모든 트래픽을 감시하고 조절하기 어렵다는 문제점을 갖는다. 따라서 victim의 상태를 정확하게 파악하고 공격 트래픽에 대한 망 자원 소모를 최대한 감소시킴으로써 기존 기법의 문제점을 해결하고 DDoS 공격에 신속하고 효과적으로 대응할 수 있는 대응 기법이 필수적으로 요구된다.

본 논문에서는 대량의 비정상적인 트래픽의 범람(flood)을 방지하고 합법적인 트래픽 전송을 보장하기 위하여 NCP (Network Control Platform) 기반의 제어망에서 DDoS 공격에 효과적인 대응 기법을 제안한다. 제안한 기법에서 NCP는 SR과 VR로부터 수집된 플로우 및 큐 정보를 기반으로 망 상태 및 DDoS 공격 여부를 감지하고 공격 트래픽을 제어하는 기능을 수행한다. 또한 NCP는 플로우 정보와 함께 결정한 패킷 폐기율을 SR과 VR에게 전송함으로써 공격 패킷을 신속하게 차단하도록 한다. 이를 위하여 DDoS 공격 대응을 위한 각 기능 모듈을 정의하고 high-flow 감지를 위한 임계값 및 공격 패킷 폐기율을 결정한다. high-flow 감지를 위한 임계값 결정을 위하여 큐 크기, 링크 용량, 유입되는 플로우 수를 고려하며, NCP에서의 패킷 폐기율은 평균 지연시간, 큐점유율 및 증가율을 고려하여 결정한다.

기존 DDoS 공격 대응 기법들은 에지 라우터에서 이상 징후 감지, 공격 여부 판단, 공격 대응 등 모든 기능을 수행하도록 하고 있다. 이는 에지 라우터의 복잡성을 증가시키고 제한된 정보로 인하여 망 전체 상태의 정확한 판단 및 신속한 대응에 한계를 가져온다. 반면에 제안한 기법은 각 에지 라우터에서 이상 징후를 감지하고 NCP의 중앙집중제어를 통하여 전체 망 상태 및 공격 여부를 정확하게 판단하도록 한다. 따라서 에지 라우터의 복잡성을 줄이는 동시에 이상 징후 감지를 용이하게 하고 NCP의 분석 결과 및 대응 결정에 따라 DDoS 공격에 신속하고 정확하게 대응할 수 있다는 장점을 갖는다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 NCP 기반의 제어망 구조에 관하여 기술하고 3장에서는 제안한 DDoS 공격 대응 기법과 이를 위한 기능 구조를 정의한다. 또한 임계값 및 rate-limiting을 위한 패킷 폐기율 산출식을 결정한다. 4장에서는 제안한 기법의 성능 평가 수행을 위하여 망의 혼잡 및 공격 상황에서 트래픽 조절 능력, 임계값과 모니터링 주기에 따른 큐의 크기, 전송 대역 관점에서 성능을 평가한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. NCP 기반의 제어망 구조

DDoS 공격은 대량의 비정상적인 패킷을 발생시켜 망 또는 시스템의 모든 사용 가능한 자원을 고갈시키는 공격 방법으로서 크게 대역폭 소모 공격과 자원 소모 공격으로 분류할 수 있다. 대역폭 소모 공격은 ICMP (Internet Control Message Protocol)

또는 UDP (User Datagram Protocol) 플루딩(flooding)을 이용하는 플루딩 공격과 스머프(Smurf), 프래글(Fraggle) 공격과 같이 라우터의 브로드캐스트 IP를 이용하여 트래픽을 반사 또는 증폭시키는 증폭 공격이 있다. 반면에 자원 소모 공격은 시스템의 CPU 사용률, 메모리, 파일 시스템 등의 자원을 고갈시켜 공격 대상 시스템의 서비스를 불가능하게 만드는 공격으로서 TCP SYN 패킷을 이용한 플로우 공격과 유효하지 않은 형식의 기형 IP 패킷들을 전송하는 기형 패킷 공격이 있다 [5]-[9]. 이러한 DDoS 공격에 효과적으로 대응하기 위해서는 대량의 DDoS 공격 패킷들이 망에 유입되어 자원을 소모하는 것을 신속하게 차단하고, 공격으로 인한 망의 혼잡 상황에서 합법적인 패킷을 정확이 구별하고 이들 전송을 최대한 보장할 수 있어야한다.

그림 1은 NCP 기반의 제어망 구조를 나타낸다. 독립된 에지 라우터를 기반으로 수행되는 기존 DDoS 공격 대응 기법들[5]-[9]과 달리 NCP 기반의 제어망은 전체 망 상태를 파악하기 용이하며, 공격 여부 판단 및 정책 결정을 위한 통계 정보가 NCP에 집중되므로 에지 라우터의 단순한 구성이 가능하다는 특징을 갖는다. NCP 기반의 제어망은 중앙 제어 노드인 NCP, 코어에 위치한 라우터(R) 그리고 SR, VR과 같은 에지 라우터(3D-R)로 구성된다. NCP는 중앙집중형 제어기로서 망 토폴로지, 자원, 정책 결정 및 SLA (Service Level Agreement), 보안 등의 기능을 담당한다. 따라서 NCP는 DDoS 공격 대응을 위하여 에지라우터로부터 전송된 정보와 자신의 통계 자료를 기반으로 보안 정책을 결정한다. 이를 위하여 각 라우터와 독립된 제어 채널을 설정하고 주기적으로 연결 및 공격 관련 정보를 교환한다. 코어에 위치한 라우터는 DDoS 공격에 따른 혼잡 제어와 공격자(attacker) 추적을 위한 패킷 마킹(marking) 기능 등을 담당한다. 에지 라우터는 공격 감지(Detection), 공격 패킷 구별(Distinguish), 패킷 폐기(Discard) 등 DDoS 공격에 대한 위협 판단 기능을 담당한다. 에지 라우터는 플로우(flow)를 기반으로 트래픽을 감시하며 이상 징후가 발견되면 이에 따른 알람 메시지를 NCP에게 전송한다. NCP는 이상 플로우에 대한 통계 자료를 기반으로 공격 여부를 판단하고, 이에 따른 패킷 폐기율을 결정하여 에지 라우터에게 전송한다. 에지 라우터는 NCP의 정책에 따라 해당 플로우에 속하는 패킷을 폐기시킨다. 이때, 하나의 플로우는 소스 IP 주소, 목적지 IP 주소, 프로토콜 타입, 소스 포트 번호, 목적지 포트 번호가 동일한 패킷들의 집합으로 정의된다.

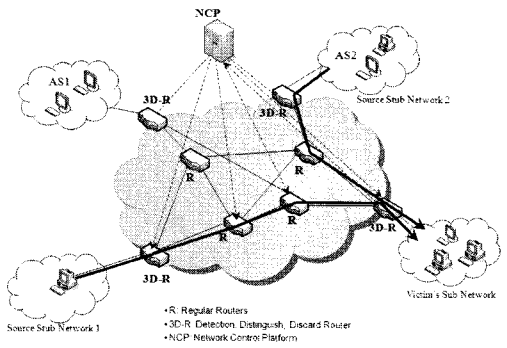


그림 1. NCP 기반의 제어망 구조
Fig. 1. Architecture of NCP-based control networks

Ⅲ. NCP기반의 제어망에서 DDoS 공격 대응 기법 설계

3.1 DDoS 공격 대응 시나리오

DDoS 공격 대응 기법은 공격에 따른 망의 혼잡 상황에서 합법적인 패킷들을 정확하게 인지하고 공격 패킷과 합법적인 패킷을 구분하여 목적지까지 안전하게 전송할 수 있어야 한다. 따라서 정확한 공격 감지, 공격에 따른 혼잡을 감소시키기 위한 효과적인 대응, 합법적인 트래픽의 정확한 구분 및 전송 보장이 필수적으로 요구된다. 본 논문에서 제안한 DDoS 공격 대응 기법을 위하여 NCP와 SR, VR이 담당하는 주요 기능은 다음과 같다.

- NCP: SR과 VR로부터 수집한 정보를 기반으로 트래픽을 분석하여 혼잡상황과 공격상황 판단, 합법적인 트래픽과 공격 트래픽의 구분, 망 상태에 따른 패킷 폐기율 결정을 수행한다.
- SR: high-flow 모니터링, high-flow 감지 시 VR의 평균 응답 시간 측정, NCP가 결정한 폐기율에 따라 SR에 유입되는 패킷을 폐기시키는 역할을 수행한다.
- VR: 주기적으로 VR의 큐 상태 수집 및 저장, NCP가 결정한 패킷 폐기율에 따른 플로우 기반 패킷 폐기, 큐 상태 정보를 NCP에게 전송하는 역할을 수행한다.

그림 2는 NCP 기반의 제어망에서 DDoS 공격이 발생하였을 때, 제안한 DDoS 공격 대응 기법을 기반으로 NCP, SR, VR이 수행하는 기능 및 정보 전

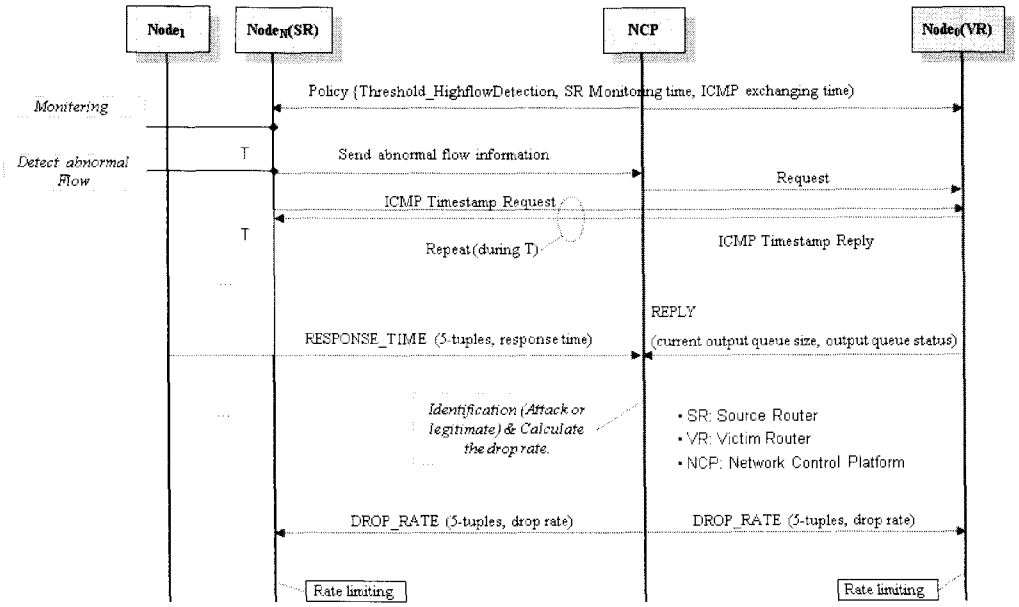


그림 2. NCP 기반의 제어 망에서 DDoS 공격 대응 기법의 절차
Fig. 2. Procedure of NCP-based defense mechanism against DDoS attack

송을 흐름도로 나타낸 것이다.

Step-1. NCP는 모든 노드에게 임계값 정보를 전송한다.

Step-2. SR은 특정 주기(Tm)를 기반으로 각 플로우 도착율 측정 및 모니터링을 수행한다.

Step-3. SR이 high-flow를 감지하면 해당 플로우 정보를 NCP에게 전송하고 ICMP 타임스탬프 요청 패킷(REQUEST)을 VR에게 전송한다. VR은 이에 대한 응답 패킷(REPLY)을 전송한다. SR은 주기 T 동안 평균응답시간을 측정한다.

Step-4. NCP는 VR로부터 큐 정보를 수집하기 위 하여 REQUEST 패킷을 전송한다.

Step-5. 일정시간(T) 후에 NCP는 SR과 VR로부터 수집한 평균응답시간과 큐 정보를 기반으로 DDoS 공격 여부를 판단하고 이에 따른 패킷 폐기율을 결정한다.

Step-6. NCP는 결정된 패킷 폐기율과 해당 플로우 정보를 SR과 VR에게 전송한다.

Step-7. SR과 VR은 결정된 패킷 폐기율에 따라 해당 플로우의 패킷을 폐기한다.

NCP는 망의 안정화를 위하여 DDoS 공격 뿐만 아니라 망의 혼잡 상황에 대해서도 신속하고 적절한 대응을 수행해야 한다. 제안한 구조에서 SR로부터 high-flow 상태를 보고 받은 NCP는 DDoS 공격 여부를 판단하기 위하여 SR과 VR간 평균 응답시간과 VR의 큐 정보를 이용한다. 해당 플로우에 대한 패킷을 모두 폐기시키는 DDoS 공격 상황과는 달리, 혼잡 상황인 경우 NCP는 망이 해당 플로우를 수용할 수 있는 범위 내에서 패킷 폐기율을 조절한다. 또한 해당 플로우 정보를 SR과 VR에게 동시에 전송함으로써 망의 혼잡 요인을 신속하게 제거한다. 제안한 기법에서는 임계값을 기반으로 DDoS 공격에 대한 판단과 대응을 수행하므로 적절한 임계값을 결정하는 것이 매우 중요하다. 임계값이 작으면 합법적인 패킷을 공격 패킷으로 인식할 확률이 높아지고, 임계값이 큰 경우 공격 플로우 검별 능력이 떨어져 공격 패킷을 인지하지 못할 수 있다. 이러한 임계값은 망구조, 트래픽 패턴 그리고 DDoS에 대한 대응 수준에 따라 다르게 적용될 수 있다.

3.2 기능 모듈 설계

3.2.1 SR 기능 모듈

NCP 기반의 제어망에서 SR은 크게 두 가지의 기능을 수행한다. 먼저, 임계값을 기반으로 모니터링 정보를 수집하여 NCP에게 전송한다. SR은 일정 주기 동안 유입되는 플로우를 모니터링하며 전송량 임계값을 초과하는 high-flow가 탐지되면 이를 NCP에게 알리고 특정 시간 동안 ICMP 패킷을 이용하

여 VR 평균 응답시간 측정한다. 측정된 결과 값은 NCP에게 전송된다. 두 번째는 NCP로부터 수신한 폐기율과 플로우 정보를 기반으로 공격 플로우와 혼잡 유발 플로우에 대한 트래픽제어를 수행하는 것이다.

그림 3은 high-flow 감지를 위한 SR의 기능 구조를 나타낸다. 'Packet Header Statistic' 모듈은 송·수신되는 패킷의 헤더 정보를 추출한다. 'Monitoring' 모듈은 공격 플로우 패턴 및 플로우 전송량의 모니터링을 수행하며 'Normal Flow Statistics Storage'에 저장된다. 'Alert' 모듈은 모니터링 모듈에서 수집된 통계정보와 임계값을 기반으로 의심 트래픽에 관한 정보를 NCP에게 알리는 기능을 수행한다. 또한 의심 트래픽의 VR에 대하여 평균 응답시간을 측정한다. 'Communication' 모듈은 NCP, VR과의 송수신을 담당한다. 마지막으로 'Response' 모듈은 NCP의 대응 정보를 기반으로 플로우에 해당하는 rate limiting, 패킷 필터링, 패킷 폐기 등의 기능을 수행한다.

SR로 유입되는 플로우들의 모니터링을 위해서는 이상 트래픽임을 결정하기 위한 임계값(Th_{hf})과 모니터링 주기(T_m)가 필요하다. 임계값은 망 또는 트래픽을 처리하는 에지 라우터의 수용 능력과 밀접한 관련이 있다. 따라서 에지 라우터의 트래픽 처리 능력과 유입되는 트래픽양이 임계값 결정을 위한 중요 파라미터가 된다. 본 논문에서는 임계값(Th_{hf}) 결정을 위하여 안정화 상태의 SR 큐 크기($Q_{sr}\times\alpha$), 제공되는 링크 용량(C_l) 및 플로우의 수(N_f)를 고려한다. 여기서, Q_{sr}과 α 는 각각 SR 큐의 크기와 안정화 상태일 때의 최대 큐 임계값을 나타낸다. 예를 들어, 어떤 망에서 SR 큐가 70%를 초과하여 사용될 때 혼잡 제어를 요구한다면 $\alpha=0.7$로 정의할

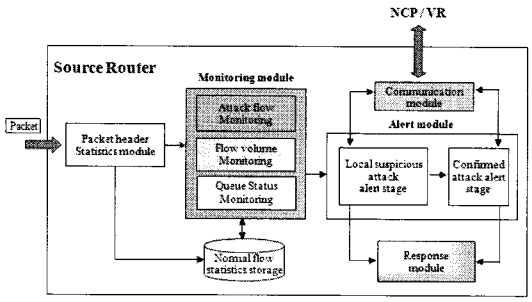


그림 3. DDoS 공격 대응을 위한 SR의 기능 구조
Fig. 3. Architecture of SR function module for response against DDoS attack

수 있다. SR의 안정화 상태 큐 크기는 제공되는 망의 구조와 트래픽 패턴 등 망의 특성에 따라 다르게 반영된다. 임계값 Th_{hf}를 구하는 식은 다음과 같다.

$$Th_{hf}=\frac{(Q_{sr}\times\alpha)+C_l}{N_f} \quad (1)$$

식 (1)을 기반으로 SR은 주기 T_m동안 플로우 i (F_i)의 유입된 데이터양을 측정하고, F_i의 유입량이 Th_{hf}를 초과하면 해당 플로우를 high-flow로 감지한다 ($1\le i\le N_f$).

high-flow 감지 슈도 코드

```
If (F_i × T_m) ≥ Th_hf Then
    Alarm ← High-flow detected
    Suspicious attack ← F_i
Else
    High-flow Not detected
    Normal flow ← F_i
End If
```

3.2.2 VR 기능 모듈

VR은 공격을 받는 라우터로서 방어적인 입장의 기능을 취하게 된다. 먼저 SR에 의해 VR로 향하는 high-flow가 감지되면 SR은 VR에게 ICMP REQUEST 메시지를 전송하고, NCP는 VR에게 큐 정보를 요청한다. VR은 이러한 요청에 응답하는 기능 뿐만 아니라 큐의 상태를 모니터링 하여 NCP에게 경고 메시지를 전송하는 기능도 수행한다. VR로부터 경고 메시지를 받은 NCP는 패킷 폐기율을 SR에 전송함으로써 VR로 유입되는 트래픽양을 조절한다. 또한 VR은 NCP로부터 수신한 패킷 폐기율과 플로우 정보를 기반으로 해당 플로우에 속하는 패킷을 우선적으로 폐기시킨다.

그림 4는 이를 수행하기 위한 VR의 기능 구조를 나타낸다. 'Monitoring' 모듈은 큐 점유율과 증가율에 대한 모니터링을 수행하며 'Alert' 모듈은 큐의 이상 징후를 NCP에게 알리는 기능을 수행한다. 'Response' 모듈에서는 'Alert' 모듈에서 수신한 정보를 기반으로 Rate-limiting, 패킷 필터링 및 패킷 폐기 기능을 수행한다. 마지막으로 'Communication'

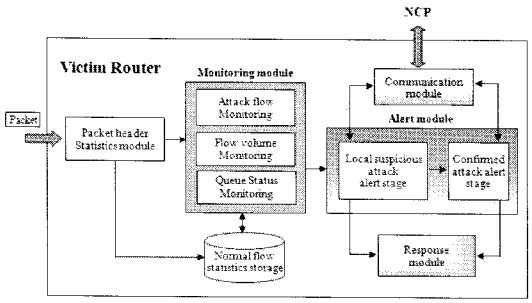


그림 4. DDoS 공격 대응을 위한 VR의 기능 구조
Fig. 4. Architecture of VR function module for response against DDoS attack

모듈은 NCP, SR과의 송수신을 담당한다.

VR은 큐 상태를 모니터링하고 큐 점유율(R^q)과 증가율(S) 정보를 주기적으로 업데이트시킨다. 이때, 큐 점유율은 큐 크기에 대한 현재 큐 길이를 나타내고, 큐 증가율은 큐 길이의 증가정도로 과거와 현재의 증가율 정보가 반영된다. 큐 점유율과 증가율은 다음과 같이 구할 수 있다 (식 2). 여기서, L_{cq}는 현재 사용되는 큐 크기, L_q는 전체 큐 크기를 나타낸다.

$$R^q = \frac{L_{cq}}{L_q},\quad S = \left| \frac{L_q(t+T) - L_q(t)}{L_q(t)} \right| \qquad (2)$$

3.2.3 NCP 기능 모듈

NCP는 전체 망의 상황을 분석하고 제어하는 기능을 수행한다. 따라서 NCP는 DDoS 공격에 대응하기 위하여 SR과 VR로부터 필요한 정보를 수집하고, 이를 기반으로 패킷 폐기율을 결정하여 각 에지 라우터에게 전송한다. 이를 통하여 NCP는 공격 상황 및 혼잡 상황을 신속하게 제어한다. 그림 5는 NCP의 제어 기능 구조를 나타낸다. 'Alert classifier' 모듈은 SR에서 수신된 경고 메시지를 분류하고 보관하는 역할을 수행한다. 'Network status analyzer' 모듈은 공격으로 의심되는 플로우에 대한 정보를 분석하여 망의 이상 유무를 판단하는 기능을 수행한다. 이러한 플로우 정보 분석은 'Alert classifier' 모듈에서 분류된 경고 메시지를 기반으로 수행되며 분석 결과는 추후에 활용하기 위하여 저장소에 보관된다. 'Response' 모듈은 공격 플로우에 대한 망 제어를 위하여 수집한 정보를 기반으로 패킷 폐기율을 결정하는 역할을 담당한다. 마지막으로 'Communication'

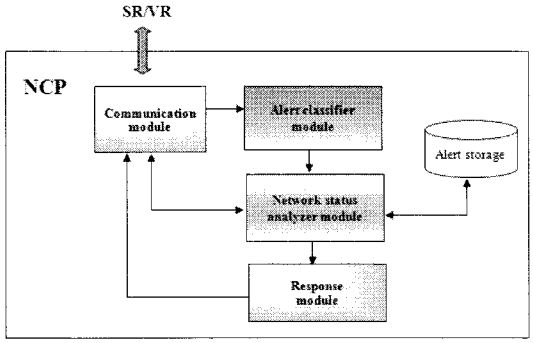


그림 5. NCP 제어 기능 구조
Fig 5. Architecture of NCP function module

모듈은 SR, VR과의 송수신 기능을 담당한다.

NCP는 DDoS 공격 여부를 판단하고 패킷 폐기율을 결정하기 위하여 큐 점유율과 증가율, SR과 VR사이의 평균 지연 시간을 고려한다. DDoS 공격은 짧은 시간에 대량의 공격 패킷을 전송함으로써 공격 대상 망을 마비시키는 특성을 가지므로 VR의 큐 정보와 SR, VR간 평균 지연은 NCP가 DDoS 공격 여부를 판단할 수 있는 척도가 될 수 있다.

- 응답시간: SR로부터 수집되는 정보, DDoS 공격은 필연적으로 과부하를 발생시키기 때문에 정상 상태일 때 보다 훨씬 긴 응답시간을 갖는다.
- 큐 정보: VR로부터 수집되는 정보, VR의 큐 점유율이 높고 큐에 입력되는 속도가 급격하게 증가하는 경우 DDoS 공격을 의심할 수 있다.

제안한 기법에서 NCP는 해당 VR의 큐점유율(R^q)이 최대 큐 임계값($Q_{\max}$)보다 큰 경우, 의심 트래픽으로 간주하고 큐 증가율(S)을 기반으로 공격 및 혼잡여부를 판단한다. 이를 위하여 두 개의 임계값(β,γ)이 사용되며 두 임계값은 DDoS 공격 패턴의 분석 결과를 기반으로 결정될 수 있다. DDoS 공격으로 판별된 경우 NCP는 해당 플로우의 폐기율을 1로 설정한다. 반면 혼잡 상황으로 판별되는 경우, 현재 VR의 큐 상태, 평균 응답 시간, 목표 큐 점유율(Q_{target})을 고려하여 패킷 폐기율(R_{drop})을 결정한다. 다음은 NCP에서 패킷 폐기율을 결정하는 방법을 보여준다. 이때 C_{rsp}는 측정된 평균 응답시간, Th_{rsp}는 응답시간의 임계값을 나타낸다.

NCP에서의 패킷 폐기율 결정 방법

If $Q_{\max} < R^q \leq 1$ then check the occupancy rate of queue.

If $\gamma < S$ then $R_{drop} = 1$;

ElseIf $\beta \leq S < \gamma$ then

$$R_{drop} = (R^q - target) + (\frac{S}{\gamma} \times \frac{C_{rsp} - Th_{rsp}}{C_{rsp} + Th_{rsp}});$$

ElseIf

Ⅳ. 성능 평가 및 분석

성능 평가를 위하여 OPNET 시뮬레이터를 기반으로 시뮬레이션을 수행하였으며 제안한 임계값과 패킷 폐기율을 기반으로 임계값 변화에 따른 망의 성능을 분석한다. 이를 통하여 제안한 공격 대응 기법의 공격 감지 능력의 정확성, 공격에 대한 효과적인 대응, 합법적 트래픽의 구분 및 전송 보장 관점에서 비교 분석한다. 시뮬레이션을 위하여 망은 5개의 정상 노드와 1개의 공격 노드로 구성되며 각각 2.5Mbps, 3.0Mbps의 트래픽을 발생시킨다. 이때, 패킷은 평균 500byte 크기의 지수 분포를 따른다. high-flow 모니터링 및 ICMP 패킷 교환주기, VR의 응답시간 임계값은 각각 0.3sec, 0.5sec, 5ms로 설정한다. SR의 큐는 무한으로 설정하였고 VR의 큐 크기는 1Mbits로 설정한다. 패킷 폐기율에 사용되는 파라미터 β, γ, min, max는 각각 3.0, 5.0, 0.1, 0.8로 가정하였다. 표 1은 시뮬레이션 파라미터를 나타낸다.

표 1. 시뮬레이션 파라미터

파라미터	값
패킷 크기 (지수분포)	500 byte
링크용량	3.0 Mbps
노드 수 (normal: abnormal)	6 (5 : 1)
ICMP 패킷 교환 주기	0.5 sec
VR 응답시간 임계값	0.005 sec
정상 트래픽 양	2.5 Mbps
비정상 트래픽의 양	3.0 Mbps
비정상 플로우 발생 시간	3 sec
SR의 큐 크기	infinite
VR의 큐 크기	1 Mbps

그림 6은 DDoS 공격 시 SR과 VR의 큐 크기 변화를 보여준다. NCP가 없는 경우 대규모 트래픽을 발생시키는 DDoS 공격 특성으로 인하여 SR의 큐 크기가 급증한다. 이와 함께 VR 큐도 점차 증가하므로 4.8초 이후 VR에 도착한 패킷들은 모두 폐기된다. 반면 제안한 기법을 사용하는 경우, DDoS 공격 시 SR과 VR의 큐가 크게 증가하나 곧 안정화되는 것을 확인할 수 있다. 이는 NCP가 결정한 패킷 폐기율과 플로우 정보를 SR, VR에게 동시에 전송함으로써 현재 유입되는 공격 트래픽 뿐만 아니라 이미 망을 지나 VR로 유입되는 공격 트래픽까지 제거하기 때문이다. 따라서 VR 큐는 VR과

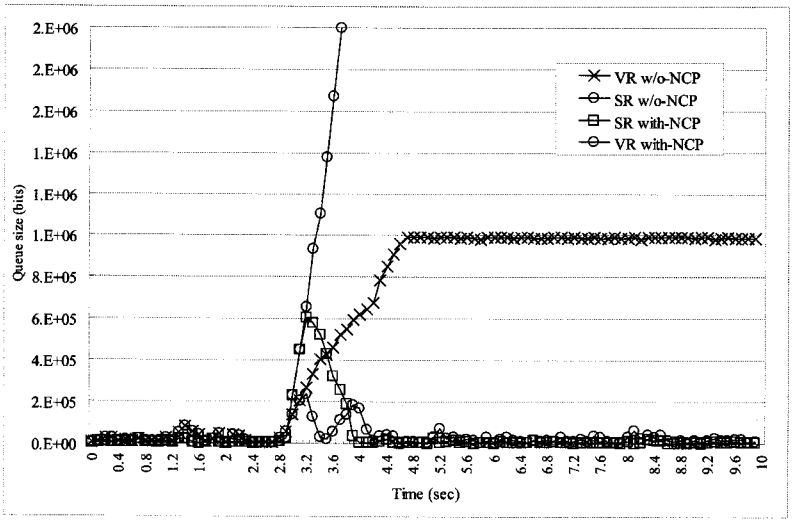


그림 6. DDoS 공격 상황에서 SR과 VR의 큐 크기
Fig. 6. Queue size of SR and VR under DDoS attack

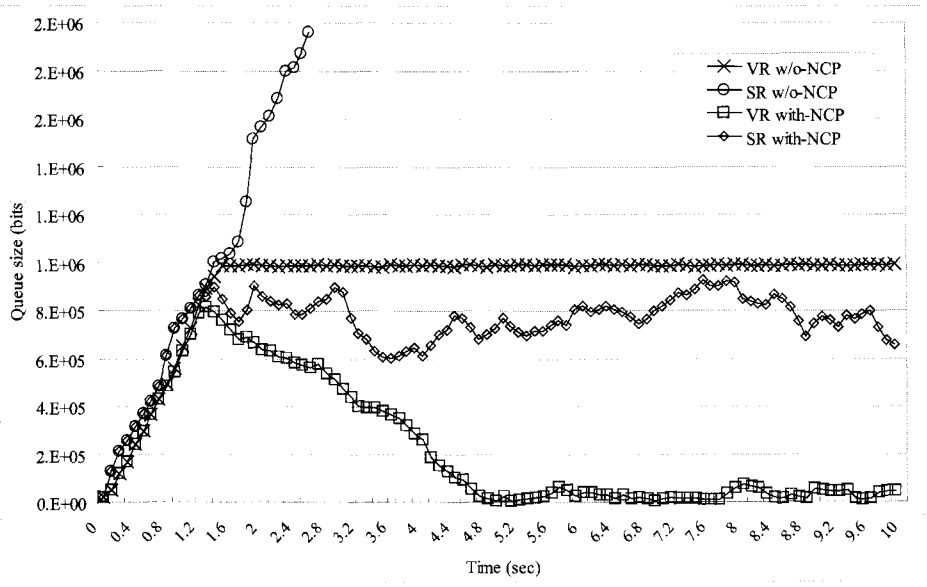


그림 7. 혼잡 상황에서 SR과 VR의 큐 크기
Fig. 7. Queue size of SR and VR under congestion

SR이 각각 공격 패킷을 폐기함에 따라 두 번에 걸쳐 감소하는 형태를 보인다.

그림 7은 혼잡 상황에서 SR과 VR의 큐 크기 변화를 나타낸다. NCP가 없는 경우 대규모 트래픽 발생으로 인하여 SR과 VR의 큐가 급증하며 1.6초 이후 VR로 유입되는 모든 패킷은 폐기된다. 반면에 제안한 기법을 사용하는 경우 SR과 VR은 NCP가 판별한 공격 플로우 정보와 결정한 패킷 폐기율 정보에 따라 해당 플로우에 대한 rate-limiting을 수행한다. 따라서 공격 패킷들의 폐기로 인하여 일정 시간 후 큐 크기는 감소한다. 이는 합법적인 패킷이 대량의 공격 패킷에 의해 큐에서 폐기되지 않고 안전하게 전송할 수 있도록 한다.

그림 8은 DDoS 공격 시 SR에서 전송된 트래픽

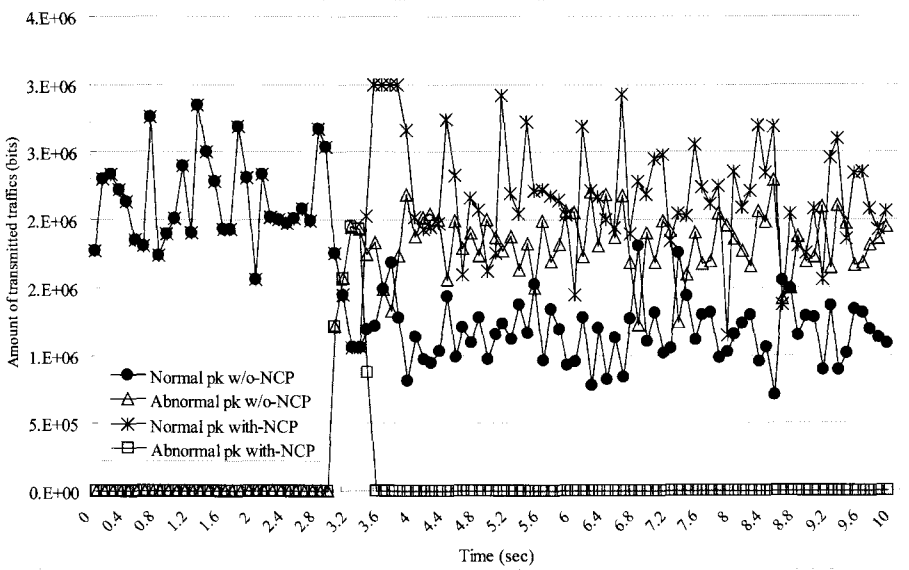


그림 8. 공격 상황 시 SR에서 전송되는 트래픽 양
Fig. 8. Transmitted traffic from SR under attack

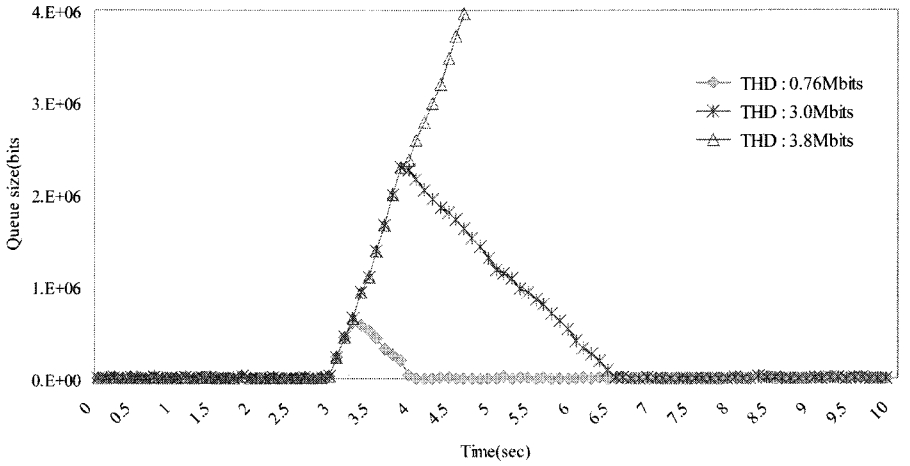


그림 9. SR의 큐 크기 (T_m = 1sec)
Fig. 9. Queue size of SR (T_m = 1sec)

양을 나타낸다. NCP가 없는 경우, 정상 상태에서는 합법적인 패킷들에 대한 전송이 보장되나 공격이 발생하여 트래픽이 크게 증가하면 대부분의 합법적인 패킷들이 폐기된다. 이는 공격 트래픽의 발생률이 합법적인 트래픽에 비해 훨씬 크기 때문에 합법적 트래픽은 상대적으로 폐기될 확률이 높아진다. 반면 제안한 기법에서는 NCP가 공격 여부를 판단하여 플로우 정보를 SR에게 전송하므로 공격 패킷이 망에 유입되기 전에 폐기된다. 따라서 일정 시간 후 공격 트래픽의 전송양이 감소하고 점차적으로 합법적인 패킷의 전송이 보장되는 것을 확인할 수 있다.

그림 9와 10은 모니터링 주기가 1초 일 때, high-flow 판별 임계값 변화에 따른 SR과 VR의 큐 크기를 나타낸다. 그림 9에서 공격 패킷이 3초에 발생하면 큐의 크기가 크게 증가한다. 이때 임계값을 기반으로 high-flow를 감지한 SR이 NCP에게 이를 알리고, NCP로부터 받은 폐기율에 따라 자신의 큐에서 해당 패킷을 폐기시키므로 SR의 큐는 감소한다. 또한 임계값이 작을수록 플로우 증가에 민감하게 반응하므로 임계값이 큰 경우보다 빨리 안정화되는 것을 알 수 있다. 임계값이 3.8Mbits인 경우

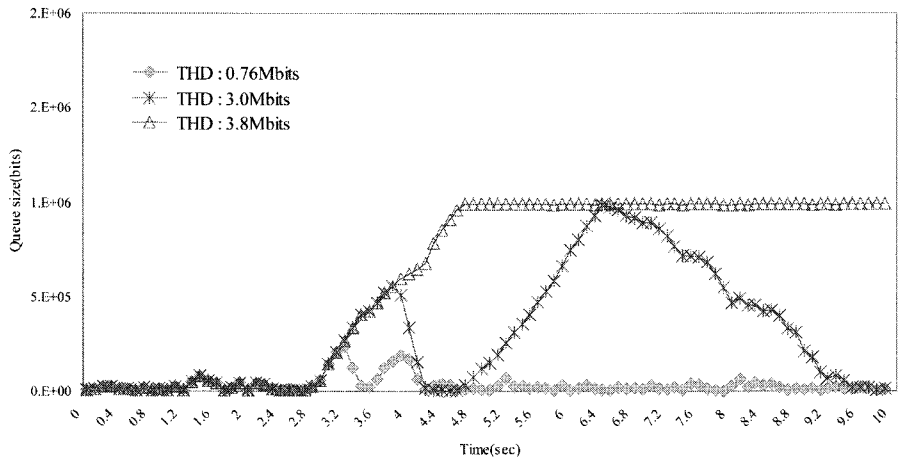


그림 10. VR의 큐 크기 (T_m = 1sec)
Fig. 10. Queue size of VR (T_m = 1sec)

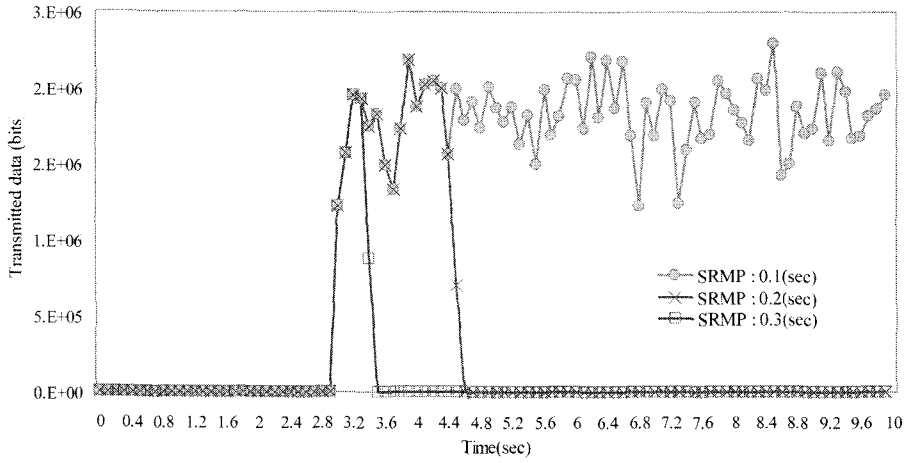


그림 11. SR에서의 공격 트래픽 전송량 (Th_{hf}= 0.76Mbits)
Fig. 11. Amount of attack traffic transmitted at SR

(THD=3.8Mbits)는 큐가 지속적으로 증가하는 양상을 보인다. 이는 임계값이 너무 크게 설정되어 공격 플로우를 감지하지 못하는 경우이다. 따라서 3.8Mbps보다 작은 임계값을 선택할 때 적절한 공격 대응이 이루어질 수 있다. 그림 10에서 공격이 발생하면 VR의 큐 크기가 증가하나 NCP가 전송한 폐기율에 따라 자신의 큐에서 해당 플로우을 폐기시키므로 큐 크기가 감소한다. 이때, NCP가 결정된 폐기율과 플로우 정보를 SR과 VR에게 동시에 전송하므로 VR에서 해당 플로우의 패킷을 우선적으로 제거할 수 있다. 따라서 처음 감소는 이에 대한 결과로 이루어지며, 나중 감소는 SR에서의 rate-limiting 수행 결과로 인하여 VR로 유입되는 트래픽양이 감소하기 때문에 나타난 결과이다.

그림 11과 12는 high-flow 임계값이 0.76Mbits일 때 모니터링 주기에 따른 공격 트래픽과 정상 트래픽의 전송량을 나타낸다. 그림 11에서 임계값이 일정한 경우 모니터링 주기가 짧으면 주기 당 수집되

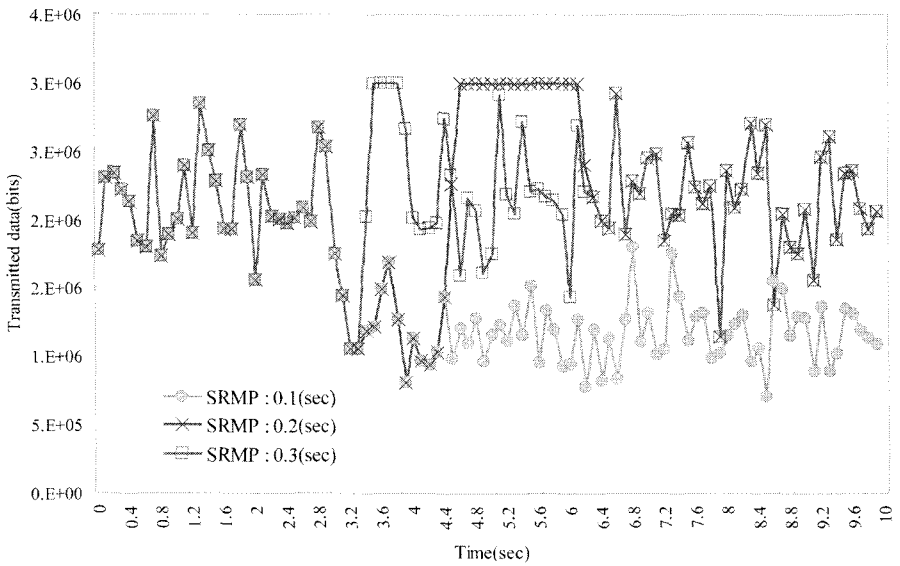


그림 12. SR에서의 정상 트래픽 전송량
Fig. 12. Amount of normal traffic transmitted at SR

는 트래픽 양이 적다. 따라서 공격 플로우를 합법적인 플로우로 인식할 수 있다. 모니터링 주기가 0.1초(SRMP = 0.1sec)일 때는 짧은 모니터링 주기로 인하여 공격 플로우가 대부분 전송된다. 모니터링 주기가 0.2초(SRMP = 0.2sec)인 경우는 초기에는 짧은 모니터링 주기로 정상 플로우로 인지되어 전송되었으나 트래픽의 버스트니스(burstness) 특성으로 인하여 임계값을 초과하면서 공격 플로우로 인식된 경우를 보여준다. 임계값과 전송데이터를 고려하였을 때, 모니터링 주기가 0.3초(SRMP = 0.3sec)일 때 가장 좋은 성능을 보인다. 그림 12에서는 공격 트래픽의 차단 정도에 따라 상대적으로 보장되는 합법적인 트래픽의 전송량을 보여준다.

V. 결 론

본 논문에서는 NCP 기반의 제어망에서 DDoS 공격의 효과적인 감지 및 대응을 위한 기법을 제안하였다. 제안한 기법에서 NCP는 대량의 비정상적인 트래픽의 범람을 방지하고 합법적인 트래픽 전송을 보장하기 위하여 SR과 VR로부터 수집된 정보를 기반으로 망 상태 및 DDoS 공격 여부를 감지하여 트래픽을 제어하는 기능을 수행한다. SR의 high-flow 감지를 위한 임계값은 큐 크기, 링크 용량, 유입되는 플로우 수를 고려하여 결정하였으며 NCP에서의 패킷 폐기율은 평균 지연시간, 큐점유율 및 증가율을 기반으로 결정하였다. 시뮬레이션을 통하여 제안한 기법이 DDoS 공격을 정확히 감지하고 효과적으로 차단함으로써 합법적 트래픽의 전송을 보장하는 것을 확인할 수 있었다.

참 고 문 헌

[1] J. Mirkovic, M. Robinson, P. Reiher and G. Oikonomou, "Distributed Defense Against DDOS Attacks," Technical Report, University of Delaware CIS Department, Feb., 2006.

[2] R. Manajan, S. M. Bellovin, S. Floyd, J. Loannidis, V. Paxson and S. Shenker, "Controlling High Bandwidth Aggregates in the Network," ACM SIGCOMM Computer Communication, Vol.32, pp.62-73, July, 2002.

[3] M. Kim, H. Kong, S. Hong, S. Chung and J. Hong, "A Flow-based Method for Abnormal Network Traffic Detection," Proceedings of NOMS'04, pp.599-612, April, 2004.

[4] G. Zhang and M. Parashar, "Cooperative Defense against Network Attacks," Proceedings of WOSIS'05, ICEIS'05, INSTICC Press, pp.113-122, May, 2005.

[5] Y. Fan, H. Hassanein and P. Martin, "Proactive Control of Distributed Denial of Service Attacks with Source Router Preferential Dropping," Computer Systems and Applications'05, April, 2005.

[6] J. Mirkovic, G. Prier and P. Reiher, "Attacking DDoS at the Source," Proceedings of the ICNP'02, November, 2002.

[7] D. Xuan, R. Bettati and W. Zhao, "A Gateway-based Defense System for Distributed DoS Attacks in High-speed Networks," Proceedings of 2001 IEEE workshop on Information Assureance and Security, June, 2001.

[8] J. Mirkovic, "D-WARD:Source-End defense Against Distributed Denial-of-Service Attacks", Ph.D Thesis, 2003.

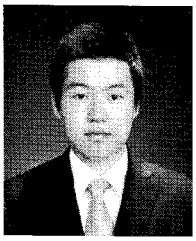
[9] K. Jozic, "Tracing back DDoS attacks", Masters Thesis, 2002.

한 경 은 (Kyeon-Eun Han) 정회원
한국통신학회 논문지 제 33권 제8호 참조

양 원 혁 (Won-Hyuk Yang) 정회원
한국통신학회 논문지 제 33권 제 8호 참조
현재 전북대학교 컴퓨터공학과 박사과정

유 경 민 (Kyoung-Min Yoo) 정회원
한국통신학회 논문지 제 33권 제3호 참조

유 재 영 (Jae-Young Yoo) 학생회원



2003년 3월~현재 전북대학교 컴퓨터공학과 학사과정

<관심분야> 네트워크 보안, BcN

김 영 선 (Young-Sun Kim) 종신회원

한국통신학회논문지 제31권 제8B호 참조

현재 한국전자통신연구원 부장

김 영 천 (Young-Chon Kim) 종신회원

한국통신학회 논문지 제 33권 제8호 참조

현재 전북대학교 컴퓨터공학과교수