主題

DiffServ 네트워크에서 QoS를 위한 보안 기법

위덕대학교 컴퓨터멀티미디어공학부 교수 박 수 영
대구가톨릭대학교 컴퓨터정보통신공학부 교수 전 용 희

차 례

1. 개요

차세대 인터넷에서 DiffServ 네트워크는 서비스 품질(QoS: Quality of Service) 제공을 위한 확장성이 높은 구조를 제시하고 있다. 차세대 네트워크에서는 음성이나 비디오 전송 같은 많은 응용들을 지원하기 위하여 QoS 보장 서비스가 필요하다. 차세대 인터넷에서 QoS 제공을 위하여 RSVP(Resource Reservation Protocol), MPLS(Multi-Protocol Label Switching), DiffServ 및 QoS 라우팅 등의 기법이 개발되고 표준화되고 있다[1]. 그러나, 국내에서는 이러한 QoS 능력을 안전하게 제공하기 위한 기법에 대한 연구가 거의 없는 실정이다[2]. 따라서, 본 논문에서는 QoS를 안전하게 제공하기 위한 보안 기법을 DiffServ 네트워크를 중심으로 제시하고자 한다.

DiffServ 네트워크처럼 QoS가 가능한 네트워크에서 직면할 수 있는 것이 QoS 공격이다[3]. 이런 환경에서, 공격자들은 통상적으로 자신들이 지불한 것보다 더 많은 자원(더 나은 서비스 클래스)을 얻도록 노력하는 네트워크의 정규 사용자이다. 서비스 클래스의 지불 모델에서의 차이는 대역폭과 다른 네트워크 자원을 훔치도록 공격자를 유혹할 수 있다. 이러한 공격은 트래픽을 삽입하거나 높은 QoS를 가진 합법적인 사용자의 신분을 속이기 위해 방화벽 필터 규칙에서 알려진 취약성을 사용한다. DiffServ 프레임워크가 서비스 클래스에서 흐름 집합을 기초로 하기 때문에, 합법적인 고객 트래픽은 삽입된 트래픽 때문에 QoS 저하를 경험할 수도 있다. 심한 경우, 공격은 서비스 거부(Denial of Service: DoS)를 초래하기도 한다.

서비스 거부 공격의 목표는 희생자의 자원이나 희생자와 통신하는 경로상의 자원을 소비하는 것이다. 희생자는 호스트, 서버, 라우터, 혹은 네트워크에 연결된 다른 종류의 엔티티일 수 있다. DoS 공격은 희생자와 접촉하는 많은 사용자나 클라이언트를 방해한

다. 잘 알려진 DoS 공격들로 여러 가지 있다[4-7]. DoS 공격은 엄청난 양의 트래픽으로 희생자의 네트워크를 범람시키는 것이 가장 통상적이다. 이런 종류의 공격은 전체 사이트나 네트워크 일부의 차단을 초래한다. 인터넷 상에서 다수의 호스트를 이용한 분산 서비스 거부(DDOS: Distributed DOS) 공격은 훨씬 더 심각하다.

QoS 공격을 탐지하기 위하여 Habib 등[8]은 QoS 도메인에서 네트워크 모니터링 메커니즘을 고안하였다. 이 메커니즘은 지연, 손실, 처리율과 같은 서비스 수준 협상(SLA: Service Level Agreement) 파라미터를 측정하고 서비스 제공자와 사용자간에 협상된 값과 측정을 비교한다. 이런 모니터링 기술을 사용해, 서비스 제공자는 네트워크 도메인 내에서의 서비스 위반을 탐지할 수 있다.

본 논문에서는 QoS 서비스 거부 공격을 일으키는 공격자를 역추적하는 기법과 서비스 거부 공격에 대해 네트워크를 보호하기 위해 사용되는 필터링 메커니즘 기술들, 그리고 네트워크 모니터링에 대해서 기술한다. 본 논문의 나머지는 다음과 같이 구성되어 있다. 2절에서는 DiffServ와 보안 관계, QoS 공격 유형에 대하여 기술하고, 3절에서는 DiffServ의 서비스 거부 공격과 이에 대한 대응책, 4절에서는 QoS 서비스 거부 공격에 대한 모니터링 기술에 대하여 기술하고, 마지막으로 5절에서 요약과 결론으로 끝을 맺는다.

2. DiffServ와 보안

DiffServ(DS) 구조는 네트워크에 진입하는 트래픽을 망의 경계에서 분류하고 조절하며, 다른 행동 집합(BA: Behavior Aggregate)에 할당되는 간단한 모델을 기초로 한다. 각 BA는 단일 코드포인트(DSCP: DS Code Point)로 확인된 후, 패킷은 네트워크 코어에서 DS 코드포인트와 관련 있는 PHB(Per-Hop Behavior)에 따라 전달된다. DSCP에는 Default PHB, EF(Expedited Forwarding) PHB, AF(Assured Forwarding) PHB 등이 있다. 특정 서비스를 요구하지 않는 패킷에 대해서는 DE(Default)로 서비스 해준다. 인터넷 라우터에서 취해지는 패킷 전달 방식인 최선 노력과 같은 정도의 서비스를 나타내며, 지연이나 손실 같은 보장된 전달 행동이 없는 IP 네트워크 상의 서비스로 볼 수 있다. EF는 라우팅 정보 갱신과 실시간 트래픽 전달에 사용되는 우선 순위가 높은 전달 방식이다. 패킷은 작은 지연과 지연 변이, 적은 손실을 가지며 대역폭 보장 서비스를 받을 수 있다. AF PHB에 속하는 트래픽은 망의 혼잡 상황에서도 트래픽의 최소 성능 속도를 보장하는 PHB이다. 이와 같이, 차별 QoS를 제공할 수 있는 DiffServ의 전제는 네트워크 내의 라우터가 패킷을 전달하도록 다른 PHB를 제공함으로서 이종 트래픽 스트림에 있는 패킷을 조절하는 것이다.

2.1 DiffServ의 구조

트래픽 조절 기능은 DS 도메인에 입력되는 트래픽이 TCA(Traffic Conditioning Agreements)에 명시된 규칙을 따르도록 보장하고, PHB를 기초로 내부 라우터로 트래픽을 전달하도록 DS 도메인에 있는 DS 에지 라우터에 의해 수행된다. (그림 1)는 DiffServ 단일 도메인을 보여주며, (그림 2)는 트래픽 조절기의 블록 다이어그램을 보여준다.

(그림 2)에서 보여주는 트래픽 조절기 요소는 트래픽 분류기(Classifier), 미터(Meter), 마커(Marker), 쉐이퍼(Shaper)로 이루어져 있으며,

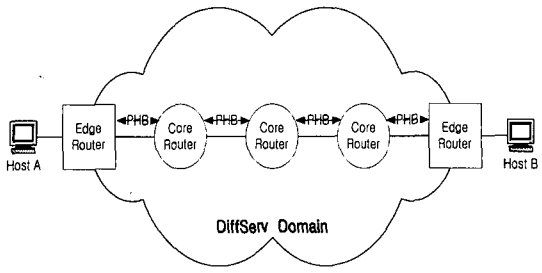

그림 1. DiffServ 단일 도메인

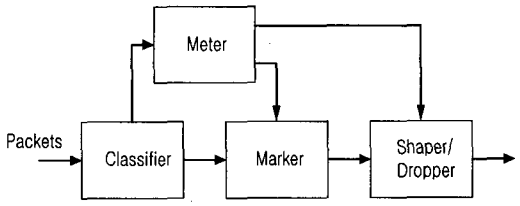

그림 2. 트래픽 조절기 블록 다이어그램

반드시 4가지 모든 요소를 포함할 필요는 없다. 각 요소의 기능은 다음과 같다:

- 분류기: 패킷 헤더의 내용을 기초로 트래픽 스트림에 있는 패킷을 선택한다. BA 분류와 MF (Multi-Field) 분류로 나눈다. BA 분류는 DS 필드만을 기초로 하고, MF 분류는 근원지/목적지 주소, DS 필드, 프로토콜 ID, 근원지/목적지 포트와 같은 전송 계층 헤더 필드 등의 패킷 헤더에 있는 여러 필드의 조합으로 분류를 한다.
- 미터: 미터는 분류기에 의해 선택되어진 트래픽 스트림상의 패킷 도착율을 확인하여 TCA의 트래픽 프로파일에 일치하는지를 결정해 in-profile/out-of-profile을 수행한다.
- 마커: 패킷은 분류된 후에 DE, AF, EF 클래스로 마킹된다. 리마킹은 AF PHB 패킷이 계약된 트래픽율 제한을 위반할 때 발생하고 out-of-profile이 된다. 이런 패킷은 DE 패킷으로 리마킹 된다.
- 드롭퍼/쉐이퍼: 만약 EF 패킷이 out-of-profile이라면 드롭퍼에 의해 즉시 탈락된다. 쉐이핑은 지터를 제거하기 위해 에지 노드나 경계 노드에서 발생한다.

2.2 신용(trust) 지역[9]

DiffServ의 정확한 운영을 위하여 DiffServ 네트워크 내에 여러 개의 신용 지역이 존재한다. 이런 신용 지역은 에지 라우터와 근원지간 신용, 코어 라우터와 에지 라우터간 신용, SLA(Service Level Agreement) 무결성의 신용을 포함한다.

2.2.1 에지 라우터와 근원지간 신용

패킷은 에지 라우터에서 근원지별로 폴리싱 된다. 그러므로, 패킷을 폴리싱하거나 마킹하기 위해, 패킷의 근원지는 에지 라우터에서 SLA와 일치되어야만 한다. SLA에 대한 근원지의 매칭은 물리 계층이나 네트워크 계층에서 발생한다. 에지 라우터는 SLA에 일치하는 소스가 트래픽을 정확하게 폴리싱 하기 위하여 올바르게 수행된다는 것을 신용한다.

2.2.2 코어와 에지 라우터간 신용

코어 라우터는 패킷이 정확하게 마킹되었다는 신용과 패킷이 이미 적당하게 폴리싱 되었다는 어떤 레벨의 신용을 에지 라우터와 가진다.

2.2.3 SLA 무결성의 신용

EF와 AF와 같은 여러 서비스들은 올바른 기능을 위해 SLA 무결성에 의존한다. 만약 클래스가 트래픽 초과로 과부하가 발생한다면 서비스 품질이 낮은 클래스의 성능뿐 아니라 서비스 품질이 높은 클래스의 성능까지도 저하된다. 그러므로 더 엄격한 QoS 클래스의 성능 저하를 일으키도록 네트워크 자원이 과도하게 배치되지 않도록 에지 라우터를 통과하는 SLA들의 무결성을 가진 신용 레벨이 존재한다.

2.3 DiffServ QoS 공격

[10]에서는 RSVP QoS 공격에 대하여 제시하고 있으나, DiffServ에 대하여도 비슷한 개념을 적용하여 아래에 기술하였다.

2.3.1 공격자의 분류

DiffServ 네트워크 보안에서, 공격자는 대개 두 가지 클래스로 분류된다: 내부인과 외부인. 외부인 공격은 통상적으로 접근 제어 메커니즘에 의해 효과적으로 방지될 수 있다. 그러나 내부인 공격은 내부인이 어떤 신뢰적인 구성요소를 접근하는 어떤 특권을 가지기 때문에 다루기가 더욱 어렵다.

RSVP와 유사하게 DiffServ에 대해서도, 세 가지 클래스의 공격자를 정의할 수 있다: 내부자$_{DiffServ}$, 외부자$_{OnPath}$, 외부자$_{Other}$. 내부자$_{DiffServ}$는 송수신자간 전송 경로에 있는 DiffServ가 가능한 라우터이다. 네트워크 시스템이 강력한 인증과 접근 제어 스킴 하에서 보호된다 할지라도, 그것은 DiffServ 메시지 교환에 참가하기 위하여 신용된다. 반면, 외부자$_{OnPath}$는 경로 상에 있는 DiffServ 불가능한 라우터이고, DiffServ 운용에 관여하지 않는다. 공격자의 가장 약한 유형이 외부자$_{Other}$이고, 경로 상에 있지 않는 라우터이거나 종단 호스트이다. 어떠한 보호 스킴을 배치함에 관계없이, 이 세 가지 클래스의 공격 등급은 내부자$_{DiffServ}$≥외부자$_{OnPath}$≥외부자$_{Other}$ 순이다. 즉, 확실한 보안 대응방안을 가지는 DiffServ 네트워킹 시스템에서, 외부자$_{Other}$에 의해 수행될 수 있는 공격은 내부자$_{DiffServ}$나 혹은 외부자$_{OnPath}$에 의해서도 공격이 시작될 수 있다.

2.3.2 공격의 유형

공격자의 주된 목적은 DiffServ QoS 공격에 대한 것이다. QoS 공격은 네트워크 공급 프로세스 공격과 데이터 전달 프로세스 공격으로 분류될 수 있다. 네트워크 공급은 QoS 네트워크에서 라우터의 구성을 포함한다. 프로세스에는 가짜 메시지의 삽입, 실제 메시지의 내용 수정, 혹은 그런 메시지들을 지연시키거나 탈락시킴으로서 공격할 수 있다. 네트워크는 신호 프로토콜의 구성 메시지 암호화를 사용함으로서 네트워크 공급 프로세스 공격에 대해 보호될 수 있다. 사실상 데이터 전달 프로세스에 대한 공격이 더욱 심각하다. 이 공격은 다른 고객 흐름이 긴 지연, 높은 손실율, 낮은 처리율을 경험하도록 함으로서 대역폭을 훔치거나 QoS 저하를 일으키려는 의도로 네트워크에 트래픽 삽입을 수반한다. 이와 같은 공격은 주로 2가지 목적으로 이루어질 수 있다:

1) QoS 서비스 거부: DiffServ에서의 서비스 거부는 DiffServ 네트워크를 통한 완전한 자원의 절도를 나타낸다. 공격자는 정당한 사용자가 희망하는 서비스 획득을 방지해 이용가능하지 못하게 하거나 혹은 고가의 서비스처럼 보이게 혼란시킬 수 있다. 또한 공격자는 사용자에게 서비스를 거부하기 위하여 QoS 요청을 위한 차등서비스 패킷을 직접 탈락시킬 수 있다. 서비스 거부는 DiffServ에서 중요한 보안 위험이고 다음과 같이 여러 장소에서 발생할 수 있다.

첫 번째 서비스 거부 공격은 출력 트래픽을 가지는 에지 라우터에서 발생할 수 있다. 흐름의 폴리싱은 서비스 거부 공격 문제를 일으키기 위하여 이용될 수 있는 공격 점을 나타낸다. 에지 라우터가 근원지별로 폴리싱하기 때문에, 간단한 서비스 거부 공격은 근원지에서 발생하는 합법적인 트래픽에 피해를 주기 위하여 가짜 근원지를 가지고 에지 라우터를 범람시키는 것이다. 이것은 에지 라우터에서 채택된 SLA와 근원지를 일치시키는 방법론에 대한 지식을 요구한다.

두 번째 공격 장소 역시 첫 번째 경우처럼 에지 라우터에서 발생할 수 있는데, 이 경우는 다른 도메인에 대하여 ISP의 네트워크 에지에 있는 에지 라우터

를 의미한다. ISP도 각자의 네트워크 에지에서 다른 도메인과 SLA를 유지하기 때문에, 출력 트래픽에 대하여는 네트워크 내부에서 입력 트래픽에 대하여는 네트워크 외부에서 서비스 거부 공격이 수행될 수 있다. 이것은 SLA를 위반하기 위하여 에지 라우터를 과부하 시키고 목표 패킷에게 과도한 피해를 준다. 이런 공격은 네트워크 하부구조의 지식을 요구한다.

세 번째 서비스 거부 공격은 코어 라우터 내에서 라우터 자신이 발생시키고, 네트워크를 위한 SLA가 근간이 된다. 네트워크 상의 한 클래스를 과부하 시킴으로서, 그 클래스가 아주 나쁜 성능을 경험하도록 하는 것이 가능하다. 심지어 다른 클래스의 트래픽에 나쁜 영향을 미치고, DiffServ에 의해 정상적으로 제공되는 서비스 차별을 거부하는 것도 가능하다. 이것은 에지 라우터에서 SLA의 과도한 할당이나 특정 코어 라우터 주변의 지나친 혼잡 때문에 발생할 수 있다.

2) QoS 서비스 도난: 공격자는 서비스를 훔치기 위하여 적절한 지불 없이 QoS 메시지를 위조할 수 있다. 이런 자원의 절도는 DiffServ 하에서 여러 가지 형태로 발생할 수 있다. DiffServ에 관한 절도는 패킷 PHB의 불법적인 증진, 네트워크 대역폭의 절도를 포함하기도 한다. 대역폭의 절도가 발생할 수 있는 장소는 다음과 같다.

첫 번째, 대역폭 절도는 에지 라우터와 코어 라우터에서 발생할 수 있다. 에지 라우터 레벨에서, 만약 패킷이 근원지를 성공적으로 속일 수 있다면, 패킷은 실제 근원지의 SLA 할당된 대역폭의 부분을 훔칠 수 있을 것이다. 코어 라우터 레벨에서의 대역폭 절도는 에지 라우터가 SLA를 초과하여 트래픽을 전송하거나 에지 라우터를 우회한 트래픽이 코어로 직접 전송되는 경우 발생할 수 있다.

두 번째, 패킷 PHB의 불법 증진은 에지 및 코어 라우터 모두에서 발생할 수 있다. 에지 라우터에서, 불법 증진은 패킷이 부정확하게 폴리싱 되거나 전혀 폴리싱이 되지 않은 경우에 발생할 수 있다. 코어 라우터에서, 불법 증진은 정확한 PHB 행동이 시행되지 않은 경우 발생할 수 있다. 이 경우의 코어 라우터는 기능이 불량이거나 혹은 라우터 자신이 절도를 하는 경우이다.

3. QoS 서비스 거부 공격과 DiffServ 보안 솔루션

이 절에서는 위에서 언급한 여러 가지 DiffServ QoS 공격 중에서 특히 QoS 서비스 거부 공격에 대한 대응 방안에 대해 기술한다. QoS 보안에 대한 관심이 커짐에 따라 IETF DiffServ WG에서도 DiffServ 사용을 위한 여러 가지 보안 방법을 기술하고 있는데, 현재, 구조 RFC[11]는 auditing과 IPSec만을 고려하고 있다. 이외에, QoS 서비스 거부 공격을 탐지하고 방지하는 방법들이 여러 가지 소개되었는데, (그림 3)에서 방법들을 보여준다[8].

서비스 거부 공격을 발생시키는 근원지(소스)를 탐지하는 여러 가지 방법이 있다. IP 역추적(traceback)은 그것들 중 하나이다. IP 역추적은 ICMP 역추적 메시지나 라우터에서 패킷 마킹을 사용함으로서 실행될 수 있다. 라우터에서 마킹 전략은 결정적 유형과 확률적 유형이 있다. 해쉬-기반 IP 역추적은 적은 패킷 양에 대해서도 공격자를 추적하도록 근원지 경로 분리 엔진(SPIE)을 제공한다. 네트워크 모니터링은 DoS 공격 탐지를 도울 수 있다. 분명한 모니터링의 한 가지 방법은 네트워크 도메인의 다양한 장소에서 패킷을 기록하는 것이다. QoS 네트워크에서, SLA 위반 탐지는 대역폭 도난과 DoS 공격을 탐지하는 것을 도울 수 있다. 위장(spoofed) 패킷 필터링은 네트워크를 DoS 공격으로부터 막아준다. 인터넷에서 서비스 거부 공격을 방지하는 두 가지 접근 방법으로는 입구/출구 필터링과 라우트-기반 필터링이 있다.

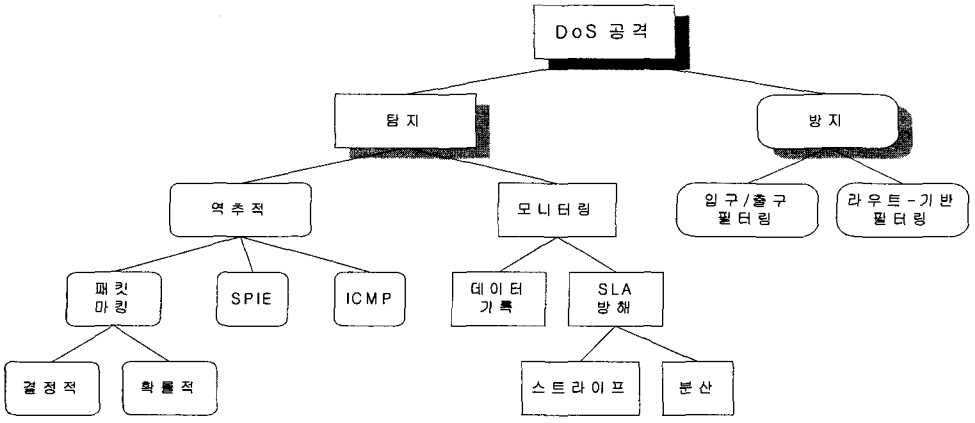

그림 3. DoS 공격과 서비스 위반을 탐지하는 접근의 분류

3.1 auditing(감사)

감사는 DiffServ 도메인에서 의심스러운 이벤트들을 모니터링하기 위한 방법 중 하나이다. 감사는 DiffServ 도메인의 부분으로서 요구되는 것이 아니라 감사를 지원하는 시스템(전체 프레임워크)에 포함될 때 권고되는 것이다. 감사가 가능한 이벤트의 예는 코어 라우터에서 미사용 코드포인트에 대한 트래픽이다. 감사는 네트워크의 보안과 견고성 모두를 증진시키기 위해 사용될 수 있다. 그러나 잠재적인 QoS 서비스 거부 공격을 피하기 위하여, 송신자라고 알려진 곳으로 메시지를 전달하기 위하여 감사가 가능한 이벤트를 탐지하는 노드를 위한 요구사항은 없다.

3.2 IPSec

IPSec은 안전한 IP 기반 전송을 위해 허용되는 IP의 확장이다[12,13]. IETF에서 표준화된 IPSec은 ESP, AH, ISAKMP, IKE 등과 같은 프로토콜 모음을 정의하며, IP 계층에서 트래픽을 보호하기 위한 전체 보안 구조를 형성한다[10].

IPSec은 두 가지 보안 프로토콜, 즉 캡슐화 보안 페이로드(Encapsulating Security Payload: ESP)와 인증 헤더(Authentication Header: AH)를 가진다. ESP는 인증을 가지는 암호화를 위한 것인 반면 AH는 오로지 인증만을 위한 것이다. 각 프로토콜에 대한 어트리뷰트는 Security Parameter Index(SPI), Sequence Number (재생 반대 목적으로) 등과 같은 필드를 가지는 확장 헤더에 전달된다. 암호화나 인증을 위해 사용되는 다른 많은 알고리즘들이 있다. 희망하는 알고리즘은 ipsec_action을 가지는 IPSec 정책에 명시될 수 있다.

ipsec_action에는 두 가지 모드가 있다: 전송 모드와 터널 모드. 전송 모드에서는 페이로드만이 안전하다. 터널 모드에서는 전체 IP 패킷이 안전하고 새로운 IP 헤더는 새로운 근원지와 목적지 주소로서 터널 입출력 장소 그리고 새로운 프로토콜로서 보안 프로토콜을 가지고 암호화된다. 터널링 기술은 전체적인 원래 패킷을 보호할 수 있고 공격자의 분석으로부터 실제 근원지와 목적지를 숨길 수 있다. 패킷을 선택하도록 명시된 헤더 필드는 새롭게 암호화된 외부의 헤더나 혹은 새로운 ESP나 AH 확장 헤더 뿐 아니라 오리지널 헤더에 있는 필드일 수도 있다.

IPSec의 기본 기능은 접근 제어와 선택적인 보안 시행이다. 즉 선택된 IP 패킷만이 통과하도록 허용되고 특정 보안 기능을 가지고 보호된다. 디폴트 모드

에서, IPSec은 암호 계산에서 DS 필드를 포함하지 않는다. 그러므로 디폴트 모드는 DiffServ 도메인을 위한 보안 제공에 적합하지 않다. 그러나 IPSec 터널 모드는 DiffServ 도메인에 직접 사용될 수 있는 보안을 제공한다. 터널 모드는 두 가지 IP 헤더 버전을 포함한다: 헤더의 내부 암호 버전과 전송을 위해 사용되는 외부 버전. 그러나 디폴트 모드에서처럼, 외부 IP 헤더는 여전히 암호 계산에서 포함되지 않는다. 그리하여, 중간자(man-in-the-middle) 공격에 취약하다[9].

IPSec 터널 모드를 사용하기 위해, 몇 가지가 고려되어야 한다. 첫째, 코어 라우터는 외부 IP 헤더만을 조사한다. 내부 IP 헤더는 도메인의 입구 혹은 출구 노드에서 조사될 수 있다. 입구 노드는 근원지를 적당한 SLA와 정확하게 일치시키기 위해 IPSec을 사용할 수 있는 반면에 출구 노드는 패킷의 종단간 무결성을 확인하기 위해 IPSec를 사용할 수 있다. 이런 스킴의 보안은 사용되는 무결성 확인의 강도에 의존한다.

출구 노드에서 고려할 사항은 다음과 같다. 현재처럼, DiffServ 도메인간의 출구 노드는 트래픽 조절을 적용하기 위해 내부 DS 필드를 수정하는 것이 허용되지 않는다. 그러나 만약 수정이 허용된다면, 그것은 보안 비용으로 네트워크 적응성을 증진시킨다. 그러므로 두 개 DiffServ 도메인간 출구 노드는 입구 노드에서 적당한 보안을 포함해야만 한다. 그리하여 DiffServ 도메인간 노드의 복잡성이 많이 증가한다. 본질적으로, 네트워크는 내부 DS 필드 수정이 없는 '가상 회선'으로 혹은 내부 DS 필드 수정을 허용하는 다중홉 네트워크로 볼 수 있다.

3.3 역추적

역추적은 공격 소스를 결정하기 위한 효율적인 스킴이다[8]. 공격자가 종종 소스 IP 주소를 속이기 때문에 공격 소스를 추적하는 것이 어렵다. 더욱이 인터넷은 패킷이 라우터를 통과할 때마다 라우터는 그 패킷에 대한 어떤 정보(추적)도 저장하지 않는 stateless이다. 호스트가 패킷을 인터넷상의 다른 호스트로 전송할 때, 패킷은 그 경로 상의 여러 라우터를 통해 이동하는데, 공격 트래픽이 따라가는 네트워크 경로를 추적할 수 있다. 어떤 공격이 발생할 때 공격 소스를 역추적하는 방법에 대한 여러 가지 기존 연구들이 있다.

3.3.1 ICMP 역추적

Bellovin은 ICMP 역추적 메시지를 제안했는데[14], 모든 라우터는 매우 낮은 확률(1/20,000)을 가지고 전달 패킷을 표본 추출하고 목적지까지 ICMP 역추적 메시지를 전송한다. 이 메시지는 이전 및 다음 라우터의 홉 주소, 타임스탬프, 추적된 패킷의 부분, 인증 정보를 포함한다. DiffServ 네트워크에서, 패킷이 공격자 A에서 희생자 V까지 네트워크 경로를 따라 이동하는 동안, 중간 라우터 R은 이런 공격 패킷의 약간을 표본 추출하고 목적지 V로 ICMP 역추적 메시지를 보낸다. 충분한 ICMP 역추적 메시지를 이용해, 나중에 희생자는 네트워크 경로 $V-A$를 추적할 수 있다. 이 방법은 공격에 포함된 희생자에서 근원지까지 경로를 구축하기 위한 유망한 솔루션을 보여준다. 이 접근의 단점은 때때로 ICMP 패킷이 라우터에서 무시될 수 있다는 것과 이런 역추적 패킷이 탈락될 수 있다는 것이다. 공격자/소스는 라우터가 단지 몇 개의 메시지만을 전송하기 때문에 희생자를 혼란시키는 많은 가짜 ICMP 역추적 메시지를 전송함으로서 인증 메커니즘을 뚫을 수 있다.

3.3.2 라우터에서 패킷 마킹

Burch와 Cheswick은 데이터 패킷 자신의 헤더에 있는 라우터의 IP 주소를 등록함으로서 패킷을 마킹하도록 제안했다[15]. 즉 라우터에서 발행되는 별개의 메시지가 없다. 이 마킹의 목적은 공격 후, 희생자는 높은 확률을 가지고 마킹된 패킷에 있는 정보를

사용해 공격의 네트워크 경로를 재구축 할 수 있다는 것이다. 이런 마킹은 결정적이거나 확률적일 수 있다. 결정적 마킹에서, 라우터는 모든 패킷을 마킹하고 패킷들은 모든 라우터에서 마킹된다. 결정적 패킷 마킹의 분명한 단점은 경로를 따라 홉의 수가 계속 증가하는 것과 같이 큰 패킷 헤더를 요구한다는 것이다. 라우터의 오버헤드는 모든 패킷을 마킹하기 위해 증가할 것이다. 확률적 패킷 마킹은 패킷 헤더에서 확률 $p \ll 1$을 가지고 지역 경로 정보를 부호화한다. 플러딩 공격동안 거대한 양의 트래픽은 희생자 쪽으로 이동한다. 그러므로 이런 많은 패킷은 소스에서 희생자까지 그들의 행로를 통해 라우터에서 마킹되는 많은 기회가 있다. 그것은 희생자로부터 공격 소스까지 네트워크 경로를 추적하기에 충분한 정보를 줄 것으로 보인다.

확률적 패킷 마킹(PPM)과 역추적은 Savage 등[7]에 의해 자세히 연구되었다. [7]에서는 마킹될 패킷에 있는 주소와 거리 메트릭을 부호화하는 효율적인 방법을 설명한다. 거리 메트릭은 공격자가 희생자로부터 몇 홉 떨어져 있는지를 나타낸다.

Snoeren 등[16]은 소스 경로 분리 엔진(SPIE)을 사용하는 해쉬-기반 IP 역추적 기술을 제안하였다. SPIE는 트래픽의 감사 흔적을 생성하고 최근의 과거에 네트워크에 의해 전달된 한 개의 IP 패킷의 출처도 추적할 수 있다. SPIE는 패킷이 어떤 특정 라우터를 통과하였는지의 정보를 저장하기 위한 매우 효율적인 방법을 사용한다.

ICMP 역추적 메시지와 PPM에 비하여 SPIE의 중요한 장점은 SPIE가 희생자에서 수신되는 적은 양의 패킷에 대하여도 공격 경로를 역추적할 수 있다는 것이다.

3.4 필터링

필터링은 IP 위조에 의해 발생되는 DoS 공격에 대한 예방 솔루션이다. 가짜 패킷이 탐지될 때마다 필터링을 하는 것이 확실한 예방 솔루션이다. 아래에 몇 가지의 패킷 필터링 기술을 토의한다.

3.4.1 입구(ingress) 필터링

네트워크 도메인으로 들어오는 패킷은 방화벽이나 고객-유형 확인을 수행하는 입구 라우터에서 필터링 될 수 있다. 방화벽은 프로토콜, 포트, IP 주소 정보를 기초로 공격을 저지하는데 효과적이다. Farguson과 Senie[17]에 의해 제안된 입구 필터링은 입구 라우터에 연결된 도메인 prefix와 일치하지 않는 IP 주소를 가지는 트래픽을 탈락시키는 더욱 엄격하고 제한적인 메커니즘이다.

입구 필터링과는 달리, 출구(egress) 필터링[18]은 네트워크 도메인의 출구점에 존재하고 출구 패킷의 소스 주소가 이 도메인에 속하는지를 조사한다. 만약 속하지 않는다면, 출구 필터는 위조된 패킷에 의한 공격을 멈추도록 패킷을 탈락시킬 것이다. 출구 필터는 패킷이 발생되는 도메인의 자원 낭비를 줄이는 것을 돕지는 못하지만, 그러나 이들 패킷에 의해 가능한 공격으로부터 다른 도메인을 구한다. 입구와 출구 필터는 비슷한 행동을 가진다.

3.4.2 라우트-기반 필터링

[19]에서는 라우트(route)-기반 분산 패킷 필터링을 제안하였다. 입구 필터링과는 달리 라우트-기반 필터는 위조된 IP 패킷을 필터링하기 위해 라우트 정보를 사용한다. 라우트-기반 필터의 능력은 필터링을 위해 개별 호스트 주소를 사용/저장하지 않고, 오히려 그것은 자율 시스템(AS)의 토폴로지 정보를 사용한다는 것이다.

4. QoS 서비스 거부 공격에 대한 모니터링

QoS 네트워크 도메인은 가능한 서비스 위반과 대역폭 절도 공격에 대하여 연속적인 네트워크 모니터

링이 필요하다. 공격자는 플로우의 신원을 속임으로서 합법적인 고객으로 위조할 수 있다. 라우터에서 네트워크 필터링[17]은 만약 공격자와 위조 고객이 다른 도메인에 있다면 그런 위조를 탐지할 수 있다, 그러나 그렇지 않다면 공격은 인식되지 않은 채 계속된다. 다른 트래픽 클래스 외에, QoS 도메인은 에지 라우터가 BE 트래픽에 대하여 제어를 가지지 않기 때문에 SLA 위반을 야기하는 BE 트래픽을 지원해야만 한다. 서비스 제공자는 다른 사용자가 협상된 QoS를 얻는 것을 어렵게 하는 서비스 위반을 탐지한다. DoS 공격의 경우, 다른 소스로부터 수많은 플로우들이 한 희생자에게 향한다. 이런 플로우들은 희생자에게 근접할수록 경로상에서 집합된다. 모니터링은 다운스트림 도메인에서 DoS 공격을 야기할 수 있는 높은 대역폭 집합을 탐지하기 위하여 업스트림 네트워크 도메인을 도울 수 있다[8, 20].

지연, 패킷 손실, 처리율과 같은 SLA 파라미터는 모든 사용자가 목표 몫을 얻는 것을 보장하기 위해 측정된다. 지연은 종단간 지연을 측정한다; 패킷 손실은 도메인으로 입력된 동일한 흐름의 전체 패킷에 대해 플로우로부터 탈락된 전체 패킷의 비율이다; 처리율은 도메인 내부 플로우에 의해 소비된 전체 대역폭이다. 지연과 손실은 네트워크 도메인을 모니터링하기 위한 중요한 파라미터이다. 공격으로 인한 과도한 트래픽은 네트워크 도메인의 내부 특성을 변경한다. 이런 내부 특성 변경은 네트워크 도메인을 모니터링하기 위한 중요한 점이다. 대역폭은 어떤 플로우가 다른 플로우에게 손해를 입혀 그것의 몫보다 더 많이 얻어지는지 아닌지를 탐지하기 위해 사용된다. SLA 위반과 DoS 공격을 탐지하기 위해 위의 3가지 파라미터가 사용될 수 있다. 비록 지터가 다른 중요한 SLA 파라미터일지라도, 그것은 플로우-특유의 것이므로 네트워크 모니터링에 사용되기에는 적합하지 않다. SLA 파라미터는 네트워크 도메인에 있는 내부(코어) 라우터와 함께 측정될 수 있고 혹은 그들의 도움 없이 추론될 수 있다. 많은 부분의 연구가 인터넷에서 지연, 손실, 처리율 측정에 초점을 맞춘다[21, 22].

SLA 위반을 탐지하기 위해 두 가지 모니터링 스킴이 있다[8]: 스트라이프(stripe)-기반 모니터링과 분산 모니터링. 스트라이프-기반 모니터링은 QoS 네트워크 도메인을 감시하기 위해, 지연, 손실, 처리율과 같은 SLA 구성요소가 측정되고 서비스 위반을 탐지하기 위해 먼저 정의된 값과 검증된다. 지연, 손실, 대역폭 소비가 먼저 정의된 임계값을 초과할 때, 모니터는 가능한 SLA 위반을 결정한다. 모니터는 기존 트래픽 클래스와 클래스별 수락 가능한 SLA 파라미터를 알고있다. 높은 지연은 네트워크 도메인 내에 있는 이상한 행동의 표시이다. 만약 보장된 클래스에 대해 어떤 손실이 있고 다른 트래픽 클래스의 손실 비율이 확실한 레벨을 초과한다면, SLA 위반은 신호로 알려진다.

두 번째, 분산 모니터링은 모든 에지 라우터를 통해 probing 에이전트를 분산시킴으로서 단일 장소를 probing하는 스트라이프-기반 스킴의 기능을 개선시켰다. 이런 분산 모니터링 접근은 서비스 위반과 DoS 공격을 탐지하기 위한 감시 오버헤드를 감소시킨다. 이 메커니즘은 오버레이 네트워크 하부구조를 사용한다.

5. 요약 및 결론

컴퓨터 시스템의 보안에 대하여 많은 연구가 집중되어졌지만, DiffServ 서비스 품질 제공 거부 공격에 대하여 보호하기 위한 보안 메커니즘에 대한 연구는 거의 이루어지지 않았다. 개별적인 QoS 메커니즘을 위해 명확한 보안 이슈가 IETF 워킹 그룹 도처에 보안을 고려하는 섹션에서 RFC와 draft에서 언급되고 있지만, DiffServ의 QoS 제공에서 중요한 보안 문제를 포괄적이고 조직적으로 분석하고 해결하기 위한 연구는 거의 수행되지 않았다.

따라서 본 논문에서는 지금까지 제안되어진

DiffServ QoS 공격 유형과 특히 QoS 서비스 거부 공격을 탐지하는 여러 가지 방법에 대해서 알아보았다. IP 역추적은 라우터에서 확률적으로 마킹함으로서 아주 근접하게 공격의 근원지를 알아내는 효과적인 방법이다. 이것은 공격이 발생한 것을 인식한 후에 사용된다. 입구 필터링은 패킷의 근원지 주소를 확인함으로서 IP 위조에 대하여 안전성을 제공한다. 라우트-기반 패킷 필터링은 위조 패킷을 필터 아웃되도록 네트워크의 토폴로지 정보를 사용한다. 라우트 기반 필터의 배치 전략은 도달할 수 있는 배치를 만든다. 두 가지의 필터링 접근은 실제로 예방적이고 역추적 메커니즘과 같이 사용될 수 있다. 필터가 공격 탐지에 실패할 때, 역추적은 공격자를 알아내고 완전하게 대응하는 방법을 제공한다. DoS 공격뿐 아니라 서비스 위반도 탐지할 수 있는 네트워크 모니터링 기법으로 스트라이프-기반과 분산 네트워크 모니터링 스킴에 대해서 기술하였다. 모니터링 스킴의 주문형 probing은 probe에 의해 삽입되는 여분 트래픽을 감소시킨다. 모니터링 접근은 동적으로 트래픽을 조절(통제)하는 수락 제어 스킴과 통합될 수 있고 탐지되자마자 공격을 멈추게 할 수 있다. 향후, 모니터링 기술은 QoS 네트워크 구조에 사용될 수 있다.

알려진 신호를 탐지함으로서 알려진 공격이나 변칙 행동을 탐지함으로서 알려지지 않은 공격을 탐지하는 많은 다른 침입 탐지 메커니즘이 있다. QoS 공격자는 서비스 성능을 저하시키는 것이 목적이다. 비록 그들이 다양한 방법으로 패킷을 탈락시키거나 지연시키더라도, 그들이 발생시키는 변칙 행동(성능)을 탐지함으로서 QoS 공격을 탐지할 수 있다. 따라서 향후 연구로는 QoS 공격의 침입 탐지에 기존 기술을 적용하여 성능을 평가하는 것이다.

참고문헌

[1] 전용희, 박수영, "DiffServ를 이용한 인터넷 QoS 보장 기술", 한국통신학회지, 제 17권 9호, pp.1152-1173, 2000년 9월.

[2] 전용희(편집자), 네트워크 Security & QoS, 한국통신학회지, 제 18권 9호, 2001년 9월.

[3] 이동훈, 정일영, 한치문, 장종수, "인터넷에서의 라우팅 및 QoS 보안", 한국통신학회지, 제 18권 9호, pp. 1235-1246, 2001년 9월.

[4] D. Moore, G. M. Voelker, and S. Savage, "Inferring Internet denial-of-service activity," in Proc. USENIX, 2001.

[5] L. Garber, "Denial of Service attacks rip the Internet," IEEE Computer, vol. 33, 4, pp. 12-17, April 2000.

[6] G. Spafford and S. Garfinkel, Practical Unix and Internet Security, O'Reilly & Associates, Inc., second edition, 1996.

[7] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," IEEE/ACM Transactions on Networking, vol. 9:(3), pp. 226-237, June 2001.

[8] A. Habib, S. Fahmy, S. R. Avasarala, V. Prabhakar, and Bharat Bhargava, "On detecting service violations and bandwidth theft in QoS network domains," Tech. Report., CSD-01-22, Department of Computer Sciences, Purdue University, Dec. 2001.

[9] Aaron Striegel, "Security Issues in a Differentiated Services Internet", http://www.public.iastate.edu/~magico.

[10] Zhi Fu, Network Management and Intrusion Detection For Quality Of Network Services, Ph.D. Dissertation, Computer Science Department, North

Carolina State University, Raleigh, U.S.A. 2001.

[11] K. Nichols, S. Blake, and D. L. Black, "Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers", RFC 2474, IETF, Dec. 1998.

[12] S. Kent and R. Atkinson, "IP Encapsulating Security Payload(ESP)", RFC 2406, IETF, Nov. 1998.

[13] S. Kent and R. Atkinson, "IP Authentication Header", RFC 2402, IETF, Nov. 1998.

[14] C. Barros, "A proposal for ICMP traceback messages", Internet Draft http://www.research.att.com/lists/ietf-itrace/2000/09/msg00044.html. Sept. 18, 2000.

[15] H. Burch and H. Cheswick, "Tracing anonymous packets to their approximate source", in Proc. USENIX Conference, pp. 319-327, DEc. 2000.

[16] A. Snoeren et al., "Hashed-based IP traceback", ACM SIGCOMM, Aug. 2001.

[17] P. Ferguson and D. Senie, "Network Ingress filtering: Defeating denial of service attacks which employ IP source address spoofing agreements performance monitoring", RFC 2827, May 2000.

[18] SANS Institute, Egress filtering v 0.2.,", http://www.sans.org/y2k/egress.htm, Feb. 2000.

[19] K. Park and H. Lee, "A proactive approach to distributed DoS attack prevention using route-based packet-filtering," in Proc. ACM SIGCOMM, Aug. 2001.

[20] M Mahajan et al., "Controlling high-bandwidth aggregates in the network," Technical Report, ACIRI, Feb. 2001.

[21] V. Paxon, Measurement and Analysis of End-to-End Internet Dynamics, Ph.D. Thesis, University of California, Berkeley, Computer Science Division, 1997.

[22] V. Paxon, G. Almes, J. Mahdavi, and M. Mathis, "Framework for IP performance metrics," IETF RFC 2330, May 1998.

박 수 영

1991년 대구가톨릭대학교 전산통계학과 졸업(학사), 1996년 대구가톨릭대학교 대학원 전산통계학과 졸업(석사), 2002년 대구가톨릭대학교 대학원 전산통계학과 박사, 1990년~1992년 대구백화점(주) 정보시스템부 근무, 1996년~1999년 대구미래대학 멀티미디어정보과학과 겸임교수, 2001년 3월~현재 위덕대학교 컴퓨터멀티미디어공학부 전임강사, 관심분야: 차세대 인터넷, QoS 보장 기술, 고속통신망 응용 서비스

전 용 희

1978년 고려대학교 전기공학과 졸업(BS), 1987년 미국 플로리다공대 대학원 컴퓨터공학과 수료, 1989년 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 졸업(MS), 1992년 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 졸업(Ph. D.), 1978~1978년 삼성중공업(주) 근무, 1978~1985년 한국전력기술(주) 근무, 1989~1989년 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA, 1989~1992년 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA, 1992~1994년 한국전자통신연구원 교환전송기술 연구소 선임 연구원, 1994~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 학부장, 공과대학장, 관심분야: 초고속 통신망 프로토콜, 통신망 성능분석, QoS 보장 기술, 고속통신망 응용 서비스, 통신망 보안