원격교육 망에서 QoS 보장을 위한 보안 기법

*이 근무, **박 수영
위덕대학교 {*정보통신공학부, **컴퓨터멀티미디어 공학부}

email: {*kmrhee, **sypark}@mail.uiduk.ac.kr

The Security Technology For QoS Assurance on Distance Learning Network

*Kun-Moo Rhee, **Soo-Young Park.

*Division of Inforamtion & communication Engineering, Uiduk University.
**Division of Computer & Multimedia Engineering, Uiduk University.

요 약

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. 원격 교육 역시 주로 인터넷이 주도하고 있다는 면에서는 QoS 의 문제를 피해 갈 수 없는 것이다. 그러나, 국내에서는 이러한 QoS 능력을 안전하게 제공하기 위한 기법에 대한 연구가 거의 없는 실정이다. 따라서, 본 논문에서는 QoS를 안전하게 제공하기 위한 보안 기법을 DiffServ 네트워크를 중심으로 제시하고 원격 교육에 적용시의 문제들을 고려하고자 한다.

1. 서론

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]. 원격 교육 역시 주로 인터넷이 주도하고 있다는 면에서는 QoS 의 문제를 피해 갈 수 없는 것이다. 원격 교육에서 서비스질의 문제는 지금까지 원격교육이 원격교육 매체 제작기술 , 혹은 저작을 위한 도구의 확보와 컨텐츠 확보 및 다양한 매체의 영역확장의 과정이라 볼 수 있다. 인터넷 상에서 단순히 텍스트를 제시하고 이에 적절한 답을 피드백 하는 구조에서 적절한 그래픽 인터페이스구사 동영상 및 효과음 등의 멀티미디어 적 요소로의 진행 과정이 그것이다. 이제 이러한 초기 단계에서 사이버대학, 상업적 원격교육 등이 점차 중요한 현재 교육의 대안으로 되면서 원격교육의 서비스 품질이 중요하게 되었다. 이러한 인터넷의 서비스 품질 확보를 위해 현재 제안되고 있는 대표적 기술이 DiffServ Network이다[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]. 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. 잘 알려진 DoS 공격들로 여러 가지 있다[4-7]. DoS 공격은 엄청난 양의 트래픽으로 희생자의 네트워크를 범람시키는 것이 가장 통상적이다. 인터넷 상에서 다수의 호스트를 이용한 분산 서비스 거부(DDOS: Distributed DOS) 공격은 훨씬 더 심각하다. QoS 공격

을 탐지하기 위하여 Habib 등[8]은 QoS 도메인에서 네트워크 모니터링 메커니즘을 고안하였다. 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 기술들에 대해서 기술한다. 본 논문의 나머지는 다음과 같이 구성되어 있다. 2절에서는 원격교육 망과 보안 관계, QoS 공격 유형에 대하여 기술하고, 3절에서는 서비스 거부 공격과 이에 대한 대응책에 대하여 기술하고, 마지막으로 4절에서 결론으로 끝을 맺는다.

2. 원격교육 망과 보안

2.1 DiffServ 원격교육 망의 구조

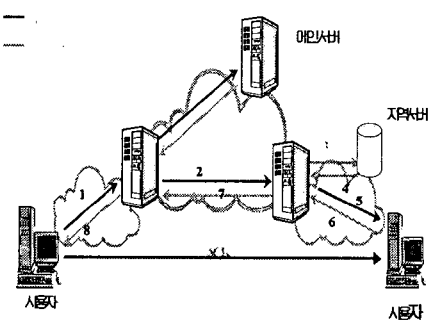

그림 1 원격교육망의 구조

원격교육 망 역시 상용적 서비스를 전제 할 때는 위와 같은 QoS 보장을 위한 네트워크 구조를 가져야 할 것이다.

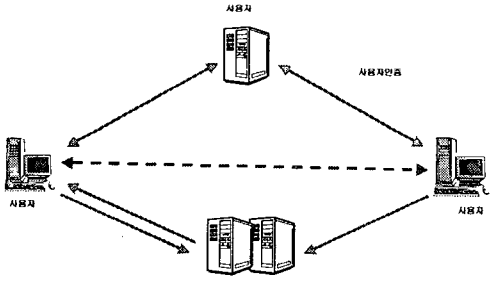

그림 2 원격 교육 사용자 인증 및 서비스 구조

위의 그림 2 에서와 같이 사용자 등록을 한후 인증 DB 에서 사용자 인증을 받고 필요한 교육 서비스에 대한 REQUEST 가 발생하면 적절한 교육에 대한 REPONSE 가 보내 지게 된다. 이러한 원격 교육의 전단계에서 교육 서비스의 질을 위협 받는 다양한 QoS 공격을 받을 수 있다.

2.2 원격교육 망에서 QoS 공격

공격자의 주된 목적은 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 QoS 서비스 거부와 QoS 서비스 도난을 목적으로 이루어질 수 있다.

첫째, QoS 서비스 거부 : DiffServ 원격교육 망에서의 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 에지 라우터나 코어 라우터 등 여러 장소에서 발생할 수 있다

둘째, QoS 서비스 도난 : 공격자는 서비스를 훔치기 위하여 적절한 지불 없이 QoS 메시지를 위조할 수 있다. 이런 자원의 절도는 DiffServ 원격교육 망에서 여러 가지 형태로 발생할 수 있다. DiffServ에 관한 절도는 패킷 PHB의 불법적인 증진, 네트워크 대역폭의 절도를 포함하기도 한다. 이런 형태의 절도들은 에지 라우터와 코어 라우터에서 발생할 수 있다.

3. QoS 서비스 거부 공격과 원격교육 망 보안기법

이 절에서는 위에서 언급한 여러 가지 원격교육 망 QoS 공격 중에서 특히 QoS 서비스 거부 공격에 대한 대응 방안에 대해 기술한다. 현재, 구조 RFC[11]는 auditing과 IPSec 만을 고려하고 있다. 이외에, 서비스 거부 공격을 발생시키는 근원지를 탐지하는 여러 가지 방법이 있다. IP 역추적은 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 엔진을 제공한다. 위장 패킷 필터링은 네트워크를 DoS 공격으로부터 막아준다. 인터넷에서 서비스 거부 공격을 방지하는 두 가지 접근 방법으로는 입출구 필터링과 라우트-기반 필터링이 있다.

3.1 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), 재생 반대 목적으로 Sequence Number 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 모드에서, 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.

3.2 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. 어떤 공격이 발생할 때 공격 소스를 역추적하는 방법에 대한 여러 가지 기존 연구들이 있다.

3.2.1 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 원격 교육 망에서, 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 접근의 단점은 때때로 ICMP 패킷이 라우터에서 무시될 수 있다는 것과 이런 역추적 패킷이 탈락될 수 있다는 것이다.

3.2.2 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 재구축할 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.

3.3 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.

3.3.1 입구(ingress) 필터링

네트워크 도메인으로 들어오는 패킷은 방화벽이나 고객-유형 확인을 수행하는 입구 라우터에서 필터링될 수 있다. 방화벽은 프로토콜, 포트, IP 주소 정보를 기초로 공격을 저지하는데 효과적이다. Farguson과 Senie[15]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 필터링[16]은 네트워크 도메인의 출구점에 존재하고 출구 패킷의 소스 주소가 이 도메인에 속하는지를 조사한다.

3.3.2 라우트-기반 필터링

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. 결론

본 논문에서는 DiffServ 원격교육 망에서의 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. 향후연구는 원격교육 망에서 각 사용단계와 서버 혹은 사용자 또는 외부 침입자에 의한 공격의 종류를 확인하고 다양한 보안 전략의 효과성을 확인 과정이 계속되어야 할 것이다.

참고문헌

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

[2] 전용희, 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] 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.

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