IPTV 접속망에서의 IGMP 플러딩 공격 효과 감소 기법

(Mtigating the IGMP Flooding Attacks for the IPTV Access Network)

김 성 진 † 김 유 나 ††
(SungJin Kim) (Yuna Kim)

김 종 †††
(Jong Kim)

요 약 IPTV 서비스는 주로 여러 수신자에게 채널 전송이 효과적인 멀티캐스트 네트워크를 기반으로 제공된다. 수신자 측에 인접한 접속망에서는 IGMP(인터넷 그룹 관리 프로토콜)가 쓰이는데, 이는 수신자가 특정 채널 전송 중인 멀티캐스트 그룹에 가입하고 탈퇴할 수 있는 기능을 지원한다. 하지만 접속망 내부의 악의적인 공격자는 IGMP 메시지를 이용하여 정상적인 수신자의 서비스 이용에 장애를 줄 수 있다. 공격자는 IGMP 메시지를 위조하여 정상적인 수신자의 채널을 가로채거나 다수의 채널을 요청하여 접속망의 대역폭을 낭비시킬 수 있다. 또한 말단 라우터에 대량의 IGMP 메시지를 보내어 라우터의 자원을 소모하는 공격을 가할 수 있다. 메시지 위조를 방지하기 위한 대책으로 패킷 수준의 인증 기법을 도입할 수 있는데 이것은 말단 라우터에 추가적인 프로세싱 오버헤드를 발생시키므로, IGMP 플러딩 공격에 더욱 취약해질 우려가 있다. 따라서 본 논문에서는 IGMP 플러딩 공격 효과를 감소시킬 수 있도록, IGMP 패킷 속성 인증이 가능한 두 단계 인증 기법을 제안한다.

키워드 : IPTV, 플러딩 공격, 패킷 수준 인증

Abstract In IPTV multicast architecture, the IGMP (Internet Group Management Protocol) is used for access networks. This protocol supports the functionality of join or leave for a specific multicast channel group. But, malicious attackers can disturb legitimate users being served appropriately. By using spoofed IGMP messages, attackers can hi-jack the premium channel, wasting bandwidth and exhausting the IGMP router's resources. To prevent the message spoofing, we can introduce the packet-level authentication methods. But, it causes the additional processing overhead to an IGMP processing router, so that the router is more susceptible to the flooding attacks. In this paper, we propose the two-level authentication scheme in order to mitigate the IGMP flooding attack.

Key words : IPTV, flooding attacks, packet-level authentication

1. 서 론

IGMP[1]는 Internet Group Management Protocol의 약자로, 멀티캐스트 상에서 수신자가 원하는 멀티캐스트 그룹에 가입(Join) 혹은 탈퇴(Leave)하기 위해 사용하는 프로토콜이며 IPTV 서비스에서 사용자의 채널 변경 요청 시 이용된다. IGMP의 구조는 매우 단순하고 별도의 인증 과정을 제공하지 않기 때문에 악의적인 메시지 위조 공격에 매우 취약하다. 공격자는 정상적인 사용자가 보내는 IGMP 메시지인 것처럼 위조하여(IGMP 위조 공격), 프리미엄 채널을 가로채거나 현재 시청하지 않는 다수의 채널 그룹을 요청하여 접속망 내 모든 채널의 품질을 저하시킬 수 있다. 또한 IGMP 메시지를 처리하는 말단 라우터로 다량의 메시지를 전송하여(IGMP 플러딩 공격) 더 이상 정상적인 사용자의 채널 변경 요청을 받아들일 수 없는 상태로 만드는 자원 소모 공격을 가할 수 있다[2].

접속망에서 메시지 위조 공격을 근본적으로 차단하는 한 가지 방법으로 패킷 수준의 인증 기법[3-6]을 도입할 수 있다. 하지만 패킷 수준의 인증 기법은 말단 라우터에 프로세싱 오버헤드를 발생시켜 IGMP 플러딩 공격에 더욱 취약해질 우려가 있다. 말단 라우터가 처리할 수 있는 양에 비해 더 많은 요청 패킷이 몰려들 경우 큐 오버플로로 인해 패킷이 손실되거나 채널 변경 서비스가 지연될 수 있다. 채널 변경 지연 시간은 IPTV 서비스 QoS에서 중요하게 다루는 요소 중 하나로, 일반적

· 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성·지원사업의 연구결과로 수행되었음
· 이 논문은 2009 한국컴퓨터종합학술대회에서 'IPTV 접속망에서의 IGMP 플러딩 공격 효과 감소 기법'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 포항공과대학교 정보통신대학원
carp1230@postech.ac.kr
†† 비 회 원 : 포항공과대학교 컴퓨터공학과
existion@postech.ac.kr
††† 종신회원 : 포항공과대학교 컴퓨터공학과 교수
jkim@postech.ac.kr
(Corresponding author임)

논문접수 : 2009년 8월 13일
심사완료 : 2009년 10월 5일

으로 IGMP 메시지를 처리하는데 100ms 이내의 시간이 적합하다고 권장한다[7].

본 논문에서 제안하는 기법은 두 단계 인증 방식을 통하여 높은 보안성을 유지하면서 동시에 IGMP 플러딩 공격이 있을 때에도 빠른 인증이 가능하다. 본 논문의 구성은 2장에서 IGMP 프로토콜과 IPTV 접속망의 구조, IGMP 메시지를 통한 공격에 대해서 소개를 할 것이다. 3장에서는 기존의 패킷 인증 기법과 관련된 연구들을 소개하고 4장에서 본 연구의 동기와 목적을 제시한다. 5장에서는 제안하는 두 단계 인증 기법의 명세에 대해 설명한다. 6장에서는 시뮬레이션을 통해 플러딩 공격 상황에서의 공격 감소 효과를 측정한 후 7장에서 결론을 맺는다.

2. 배경 지식

2.1 IGMP 프로토콜

IGMP 프로토콜[1]은 IGMP 호스트와 IGMP 라우터 사이에서 혹은 IGMP 라우터와 다른 IGMP 라우터 사이에서 동작하며 재전송 과정이 없는 단순한 프로토콜이다. IPTV 서비스에서 사용자가 채널을 변경하고자 할 때는 LEAVE와 JOIN 두 가지 타입의 IGMP 메시지에 대한 처리가 필요하다. 따라서 공격자는 언급한 두 가지 타입의 메시지를 위조하여 플러딩 공격을 시도할 수 있다.

2.2 IPTV 접속망 자원

IPTV 접속망의 네트워크 자원[8]은 STB(Set Top Box), DSLAM(Digital Serial Line Access Multiplexer) 크게 두 가지로 구성되어 있다. STB는 사용자측의 단말기로 사용자의 채널 요청을 받아들여 말단 라우터에 해당 채널에 대한 요청 정보를 담고 있는 IGMP 메시지를 전송하는 것이다. 또한 여러 대의 STB가 한 대의 DSLAM에 연결되어 있으며 자신에게 연결된 STB에서 전송된 IGMP 메시지를 처리하여 상위 라우터에 채널을 요청하는 기능을 지원한다. DSLAM은 일반적으로 2000~6000대까지의 STB를 지원할 수 있다.

본 논문에서는 공격자의 공격대상인 말단 라우터로서, 언급한 네트워크 자원 중 IGMP 처리를 지원하면서 가장 사용자 위치에 근접한 DSLAM을 선정하였다.

2.3 공격 유형

IPTV 접속망에서 IGMP 메시지를 이용한 공격[2]은 다음과 같다. 서비스 가로채기는 특정 채널 스트림에 대한 비인가된 접근을 의미한다. 별도의 인증 메커니즘이 없을 경우 공격자는 IGMP 메시지를 위조하여 무상으로 프리미엄 채널에 대한 접근이 가능하다. 또한 공격자는 존재하는 다수의 멀티캐스트 채널 그룹에 대한 수신을 요청하여 해당 접속망의 수신 대역폭을 소모시켜 채널 품질을 저하시킬 수 있다. 플러딩 공격은 IGMP 라우터에 부담을 주어 해당 시스템이 자원 소모 상태에 이르도록 하여 정상적인 사용자의 채널 요청을 받아들일 수 없는 상태로 만드는 것이다.

위조 공격을 원천적으로 차단하기 위해 패킷 수준의 인증 기법을 도입할 수 있지만 이 기법이 오히려 말단 라우터에 더욱 부담을 줄 수 있다. 다음 장에서 패킷 인증 기법의 유형에 대해 알아보기로 한다.

3. 관련 연구

관련 연구에 대한 조사를 진행하면서, 패킷 수준 인증 기법을 보안성과 인증 연산 시간에 따라 아래와 같은 두 가지로 분류하였다.

3.1 강한 인증(Strong Authentication) 기법

IPsec 프로토콜[3]은 독립적인 보안 레이어를 제공하며 안전한 단 대 단 혹은 단 대 말단 라우터 통신 기능을 제공한다. IPsec은 각각의 패킷에 대해 주소 인증, 데이터 무결성과 기밀성을 제공해준다. 네트워크 상의 홉 간 무결성 연구[4]에서는 IPsec과 유사하게 독립적인 보안 레이어를 제공하는 프로토콜을 기반으로 MD5 알고리즘[9]을 사용하여 HMAC을 생성한다. 언급한 두 가지 프로토콜은 IP 패킷 전체에 대해 해쉬 다이제스트를 수행하기 때문에 공격자가 말단 라우터와 STB사이에서 패킷을 가로채어 일부분을 변조하는 공격(MITM 공격)을 방지할 수 있다. 하지만 제시한 관련 연구들을 IGMP 메시지 인증에 사용할 경우, 추가적인 인증 연산 시간에 따른 오버헤드로 인해 말단 라우터의 패킷 처리량이 감소하는 단점이 있다. VoIP 환경에서 IPsec 프로토콜을 사용할 경우 IPsec을 사용하지 않을 경우 보다 대역폭이 50% 이상 감소하는 것을 볼 수 있다[10].

3.2 약한 인증(Weak Authentication) 기법

데이터 스트림을 전송하는 경우 모든 데이터 패킷에 대해 강한 인증 기법을 사용하는 것은 오버헤드가 클 수 있으므로, 성능 향상을 위해 적은 비트 수를 차지하는 의사 난수 기반의 인증 기법[5,6]을 도입할 수 있다. 의사 난수는 의사 난수 생성 함수를 통해 생성되며 데이터 스트림을 구성하는 각각의 패킷에 덧붙여져 말단 라우터 혹은 단말에서 인증을 받게 된다. 이때, 말단 라우터와 단말은 각자가 공유하고 있는 키를 의사 난수 생성 함수에 시드값과 함께 입력으로 취하여, 공격자가 다음 의사 난수를 쉽게 예측할 수 없도록 한다. 임의 비트 인증 프로토콜(RBWA)[5]의 경우 의사 난수 생성 함수로서 NIST에서 제안하는 G-DES, G-SHA[11] 등을 사용하여 16비트의 의사 난수를 생성한다. 또한 IP EZ-Pass[6]의 경우 RC-5 알고리즘[12]을 사용하여 64비트의 의사 난수를 생성한다. 인증 헤더가 적은 비트

수를 차지하는 만큼 헤더의 생성 시간과 인증 시간은 적게 걸릴 수 있다. 하지만 제시한 관련 연구들을 IGMP 메시지 인증에 사용할 경우, 두 가지 프로토콜의 단점은 첫 번째로 적은 비트 수의 사용으로 인해 무차별 대입 공격에 취약하다는 점이다. 두 번째는 공격자가 호스트와 말단 라우터 사이에서 패킷을 가로채 의사 난수 필드를 제외한 부분에 수정을 가할 경우, 위조 공격이 일어났음에도 인증 메커니즘을 그대로 통과할 수 있는 우려가 있다는 점이다.

4. 제안 방법

4.1 두 단계 인증 기법

제안하는 기법에서 인증 헤더(AH)는 그림 1과 같이 약한 인증 헤더(L1)와 강한 인증 헤더(L2)를 모두 보유한다. 두 단계로 인증을 받게 하는 이유는, L2 헤더의 인증에 걸리는 시간이 L1헤더에 비해 크므로 L2 헤더 인증을 받기 전에 상대적으로 적은 연산 시간이 걸리는 L1 헤더 인증을 통해 공격 패킷을 우선적으로 폐기시키기 위함이다. 들어온 패킷은 첫 번째로 L1 필드에 대한 인증을 받게 된다. 적절하지 않은 L1 필드 값을 가진 공격 패킷은 L1 헤더 인증을 통해 L2 헤더 인증을 받지 않고 폐기될 수 있다. 따라서 IGMP 플러딩 공격 상황에서, 공격 패킷과 정상 패킷 모두 강한 인증을 받게 하는 것보다 약한 인증 과정을 통해 공격 패킷의 수를 감소시킨 후에 강한 인증을 받도록 하는 것이 말단 라우터에 보다 적은 부담을 주면서 패킷 수준의 인증 기능을 수행할 수 있다. L1 헤더는 16비트의 의사 난수를 포함하며, 의사 난수 생성 함수는 IP EZ-Pass에서 사용하는 RC5 알고리즘에 기반한다. L2 헤더는 MD5 알고리즘을 이용하여 전체 IP 패킷을 다이제스트 한 128 비트의 HMAC 값을 갖는다.

그림 2에서는 DSLAM이 하나의 드롭 테일 큐(큐 오버플로 발생 시 큐 끝에서 패킷 손실이 발생하는 큐)를 갖는다고 가정한다. 공격자가 다수의 공격 패킷을 말단 라우터로 전송할 때, 말단 라우터의 큐는 다수의 공격 패킷과 소수의 정상 요청 패킷으로 채워진다. L1 헤더의 크기가 16비트이므로 공격자가 L1 필드의 값을 모른다고 가정했을 경우, 1/ 2^{16}의 확률로 L1 헤더 인증을 통과하게 된다. 본 논문에서 사용하는 의사 난수 생성

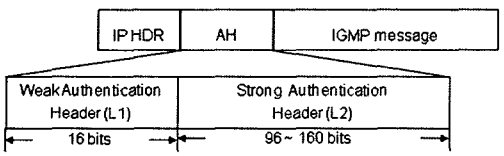

그림 1 두 단계 인증 기법 패킷 형태

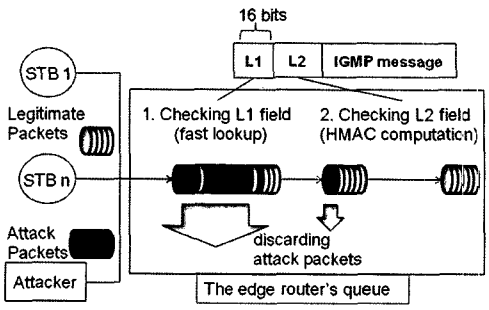

그림 2 두 단계 인증 기법

함수는 시드 값 이외에 공유키 값이 필요하므로 공격자가 키 값을 모르면 다음에 생성될 PRN 값을 예측할 수 없다. 따라서 약한 인증은 일회성 키(One Time Password) 시스템[13]처럼 동작하고 키 값을 모르는 공격자는 무차별 대입 공격만을 시도할 수 있다. 따라서 L1 헤더 인증을 통과한 소량의 남은 공격 패킷과 사용자가 요청한 정상 패킷만이 강한 인증을 받게 된다.

4.3 PRN(의사 난수) 윈도우 동기화

STB와 말단 라우터간의 약한 인증 과정이 제대로 이루어지기 위해서는 두 기기의 PRN이 서로 동기화 되어야 한다. 두 기기 간에 하나의 PRN만을 공유하고 있을 경우, 한 번의 패킷 손실로 약한 인증 과정 자체가 동작하지 않을 수 있다. 따라서 패킷 손실에 대비할 수 있는 PRN 윈도우 기법이 필요하다. 그림 3에서와 같이 두 기기는 항상 윈도우 크기(W)만큼의 PRN 집합을 공유하며, 이는 W번 이하의 패킷손실 시에는 약한 인증이 가능함을 의미한다. 만약 인증 받는 패킷의 PRN이 현재 윈도우내의 PRN을 가리킨다면 약한 인증은 성공한 것이므로 강한 인증 과정으로 넘어간다.

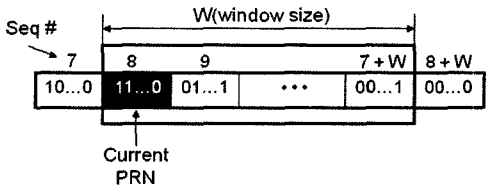

그림 3 PRN 윈도우

말단 라우터에서 PRN 윈도우는 현재 인증 받는 패킷이 약한 인증과 강한 인증 과정을 모두 통과했을 경우에만 쉬프팅이 일어나고, 약한 인증 과정을 통과하고 강한 인증에 실패했을 경우 공격 패킷으로 판명되어 폐기된 후 PRN 윈도우는 그대로 유지된다. 윈도우 크기 W는 해당 접속망에 존재하는 STB의 수와 DSLAM의 큐 용량에 의해 결정될 수 있다. 접속망에 STB가 2000대

있고 윈도우 크기 W가 20이라고 할 경우, DSLAM에서 각 STB에 대한 PRN 윈도우를 유지하지 위한 메모리 크기는 80 KB (= 20 × 2000 × 16 bits)가 된다. 따라서 큰 메모리 오버헤드 없이 PRN 윈도우를 동기화 할 수 있다.

4.4 초기화 과정

STB와 말단 라우터간의 PRN이 공유되기 위해서는 별도의 초기화 과정이 필요하다. 먼저 새로운 STB가 특정 IGMP 도메인에 처음 설치될 경우에는, IPTV 서비스 공급자가 공유키와 PRN 시드값을 DSLAM과 STB에 입력한다. 또한 같은 공유키를 계속 사용하면 공격자에 의해 분석 당할 우려가 있으므로, 초기 설치 이후에는 STB가 새로 부팅될 때 마다 그림 4와 같이 Diffie-Hellman 프로토콜[14]을 통해 말단 라우터와의 공유키를 갱신할 수 있다. STB는 부팅 시 a, g, p값을 생성하여 A를 계산한다. 그리고 그 값을 이전 공유키로 암호화하고 두 단계 인증 헤더를 붙여서 DSLAM에 전송한다. DSLAM은 전송받은 g, p, A를 이용하여 B와 새로운 공유키 K를 생성하고 B를 이전 공유키로 암호화하여 STB에 되돌려 준다. STB는 B를 이용하여 새로운 공유키 K를 생성할 수 있고 이로써 두 기기 간의 키 갱신 과정을 마치게 된다.

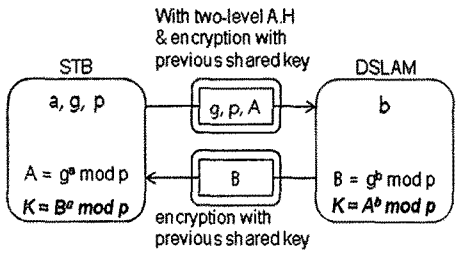

그림 4 키 갱신 과정

5. 성능 평가

5.1 시뮬레이션 설정

NS-2는 이벤트 기반의 시뮬레이터로서 유무선 환경의 다양한 시뮬레이션 설정을 가능케 한다. 하지만 이벤트 스케줄링 시 걸리는 이벤트 시간이 실제 컴퓨터 시스템의 연산 시간을 반영하지 않으므로, 본 논문에서 제시하는 인증 기법이 소요하는 실제 인증 연산 시간을 시뮬레이터에 반영하는 것은 어렵다. 따라서 여기서는 인증 연산 시간을 반영하기 위해 기존 연구[5,6]에서 제시한 실제 연산 시간 측정 데이터를 시뮬레이터 상에 스케줄링 한다. 적용한 지연 시간은 아래 표 1과 같다.

두 단계 인증의 공격 패킷은 L1 헤더 인증에서 우선 폐기될 경우 6.5 μs, 1/ 216의 확률로 약한 인증을 통과

표 1 인증 기법에 따른 인증 지연 시간

	강한 인증	두 단계 인증
공격 패킷	37 μs	6.5 μs / 37.5 μs
정상 패킷	37 μs	37.5 μs

할 경우 37.5 μs의 지연 시간을 적용받는다. 측정하고자 하는 항목은 아래와 같다.

1) DSLAM에서의 정상 패킷 손실률

큐 오버플로로 인해 정상 패킷이 손실되는 것은 사용자의 채널 요청이 거부되는 것을 의미하므로 패킷 손실률이 어느 정도 감소하는지 측정하는 것이 필요하다.

2) DSLAM에서의 정상 패킷 지연 시간

채널 변경 지연 시간은 IPTV 사용자 QoS에서 중요한 요소이다. 따라서 강한 인증 기법 시 발생하는 패킷 지연시간을 플러딩 공격 상황에서 얼마나 감소시킬 수 있는지 측정하는 것이 필요하다.

5.2 공격 시나리오

공격자는 정상적인 사용자의 STB와 같은 도메인에 포함되어 있고 해당 도메인의 STB들을 관리하는 말단 라우터인 DSLAM에 여러 명의 공격자가 IGMP 플러딩 공격을 가하여 자원 소모 상태에 이르게 한다. 이때, DSLAM에서는 IGMP 위조 공격[2]을 방지하기 위하여 홉 간 무결성 연구[4]에서 사용한 강한 인증 기법을 적용하고 있다고 가정한다. 각 공격자의 노드는 초당 1000개의 IGMP 메시지의 인증 헤더를 위조하여 플러딩 공격을 시도한다. 또한 플러딩 공격 시, 정상적인 100대의 STB들은 채널 변경을 위해 DSLAM에 평균 1초의 지수분포를 따르는 IGMP 메시지 전송 과정을 발생시키고 DSLAM은 1000개의 패킷을 수용할 수 있는 드롭 테일 큐를 갖는다고 가정한다.

5.3 시뮬레이션 결과

약 10초의 시간 동안 플러딩 공격 상황에서 평균 1초의 지수 분포를 따르는 정상 IGMP 메시지 전송 과정이 있을 경우, 강한 인증 기법과 두 단계 인증 기법에서의 패킷 손실률은 그림 5와 같다.

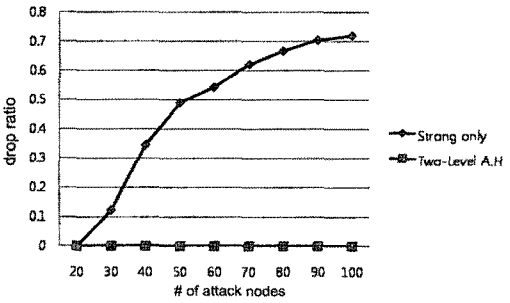

그림 5 공격 노드 수에 따른 패킷 손실률

하나의 공격 노드는 초당 1,000개의 패킷을 플러딩하므로 20개의 노드가 있을 경우 초당 20,000개의 공격 패킷이 DSLAM에 도착하게 된다. 강한 인증 과정에서 최대 100명의 공격자가 IGMP 플러딩 공격을 시도 할 경우, 정상 패킷의 손실률은 72.1%에 이른다. 하지만 두 단계 인증에서 약한 인증을 통해 공격 패킷이 사전 폐기될 경우 정상 패킷의 손실은 발생하지 않았다.

표 2는 공격 비율에 따른 평균 패킷 지연시간을 나타낸다. 표에 나타낸 큐 길이는 정상 패킷이 DSLAM의 큐에 도착했을 때, 큐에 남아있는 패킷의 평균 개수를 의미한다. 제안하는 기법에 비해 강한 인증 기법은 가정한 큐 크기가 1,000이므로 약 1,000배에 가까운 인증 지연 시간을 발생 시킨다. 공격 비율이 증가함에 따라 평균 인증 지연 시간이 조금씩 증가하는 이유는 평균 큐 길이가 증가하기 때문이다.

표 2 공격 비율에 따른 인증 지연 시간

공격 비율 (pps)	강한 인증 기법		두 단계 인증 기법	
	지연시간	큐 길이	지연시간	큐 길이
20,000	0.08 ms	1.51	38.2 μs	0.15
40,000	36.96 ms	998.51	38.8 μs	0.33
60,000	36.98 ms	998.83	39.7 μs	0.48
80,000	36.98 ms	998.91	40.9 μs	0.76
100,000	36.98 ms	998.98	43.7 μs	1.26

위의 두 가지 시뮬레이션 결과를 통해서 제안하는 두 단계 인증 기법이 IGMP 플러딩 공격 상황 시 패킷 손실을 전혀 발생시키지 않았고 큐가 오버플로가 일어날 경우 패킷 지연 시간 면에서 기존 연구에 비해 평균 906배, 최대 953배 적은 지연 시간을 보여주었다.

6. 결론 및 향후 계획

본 논문에서는 IPTV 접속망에서 패킷 인증 기법을 적용할 때의 문제점을 극복하기 위하여 두 단계 인증 기법을 제안하였다. 제안한 방법을 사용하면 기존의 강한 인증 기법을 적용할 때 발생할 수 있는 패킷 손실을 막을 수 있고 패킷 지연 시간 역시 감소시킬 수 있었다. 따라서 패킷 손실에 의해 발생할 수 있는 채널 변경 서비스 거부를 막을 수 있고 사용자에게 보다 적은 채널 변경 지연 시간을 제공할 수 있다. 향후 연구 과제로서, IPTV 환경뿐만이 아니라 일반적인 접속망 환경에서도 플러딩 공격에 대해 안전하다는 것을 실제 구현을 통해 보여주는 것이 필요하다.

참 고 문 헌

[1] "Introduction to IGMP for IPTV Networks," white paper, Juniper Networks, 2007.

[2] David Ramirez, "IPTV security: Protecting High Value Digital Contents," Willey, pp.118~125, 2008.

[3] S. Kent and R. Atkinson, "Security architecture for the internet protocol," *In RFC 2401*, November 1998.

[4] M. G. Gouda, E. N. Elnozahy, C.-T. Huang, and T. M. McGuire, "Hop integrity in computer networks," *IEEE/ACM Transactions on Networking*, 10(3), June 2002.

[5] F. Zhao, Y. Shin, S.F. Wu, H. Johnson, A. Nilsson, "RBWA: An Efficient Random-bit Window-based Authentication Protocol," *GLOBECOM '03*. vol.3, pp.1379~1383. 2003.

[6] Wang, H., Bose, A., El-Gendy, M., Shin, K.G., "IP Easy-pass: a light-weight network-edge resource access control," *IEEE/ACM Transactions on Networking*, 13(6), 2005.

[7] Jae-Hyung Bae, Hong-Shik Park, Jin-Ho Hahm, "Consideration on Channel Zapping Time in IPTV Performance Monitoring," *Focus Group on IPTV*, 4thFGIPTVmeeting, 2007.

[8] David Ramirez, "IPTV security: Protecting High Value Digital Contents," Willey, pp.53~60, 2008.

[9] C. Madson and R. Glenn, "The Use of HMAC-MD5-96 Within ESP and AH," *RFC 2403*, Nov 1998.

[10] R. Barbieri, D. Bruschi, and E. Rosti, "Voice over IPsec: Analysis and solutions," In *Proceedings of 18th Annual Computer Security Applications Conference*, 2002.

[11] "Random Number Generation and Testing," http://csrc.nist.gov/rng/.

[12] R. L. Rivest. The RC5 encryption algorithm. *LNCS (1008)*, 1995.

[13] N. Haller, C.Metz, P. Nesser, and M. Straw, "RFC 2289-A One-Time Password System," 1998.

[14] Whitefield Diffie and Martin E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, 22(6), 1976.