Human Recognition 방법을 적용한 DSTM 서버의 IPv4 주소 할당 인증 방법

준회원 최 재 덕*, 종신회원 정 수 환*°, 김 영 한*, 권 택 정**

Authenticated IPv4 Address Allocation Using Human Recognition in DSTM Server

Jaeduck Choi* *Associate Member*,
Souhwan Jung*°, Younghan Kim*, Taekjung Kwon** *Lifelong Members*

요 약

IPv6/IPv4 변환 기술 중 하나인 DSTM 기술은 DSTM 서버가 IPv4 노드와 통신을 원하는 IPv6 노드에게 IPv4 주소를 할당할 때 DoS 공격으로 인해 DSTM 서버의 IPv4 주소 pool 고갈 공격에 노출되어 있다. 본 논문에서는 DSTM 서버의 IPv4 주소 할당 서버인 DHCP의 인증 방법으로 HRAA (Human Recognition Address Allocation) 기법을 제안하였다. HRAA는 사전에 공유된 정보를 필요로 하는 단말의 mac 주소, 패스워드, 지연 인증 방식과는 달리 어떠한 정보도 공유할 필요가 없어 DSTM 도메인 내에서 언제 어디서나 실용적으로 사용될 수 있고, 자동화된 시스템에 의해서 인증값을 생성할 수 없기 때문에 DoS 공격을 통한 DSTM 서버의 IPv4 주소 pool 고갈 공격에 효과적이다.

Key Words : HRAA, DSTM, DHCPv6, Authentication, DoS

ABSTRACT

DSTM is one of the IPv6/IPv4 transition mechanisms using IPv4-in-IPv6 tunneling for communication between IPv6 node with dual stack and IPv4-only node. In DSTM, the DSTM server using the DHCPv6 is vulnerable to DoS attacks which can exhaust the IPv4 address pool. In this paper, an authentication model using a HRAA (Human Recognition Address Allocation) scheme was proposed to protect DHCP server against DoS attacks. The proposed authentication model in DSTM that uses an image file for verification is effective because only human can respond to the challenge for authenticated address allocation. The proposed model can be used anytime and anywhere in a DSTM domain, and is secure against DoS attacks.

Ⅰ. 서 론

최근 IPv6를 사용하는 네트워크 장치의 수가 증가하였고, 이에 따라 IPv6 망이 크게 확산되고 있다. 하지만 아직 대부분의 네트워크 장치는 기존의 IPv4 망에서 사용되는 것이 대다수이기 때문에 IPv6 망과 IPv4 망간의 연동이 필요하고, 이를 위해서 IP 주소의 상호 변환이 필요하다. 현재 IETF에서 많은 변환기술이 표준화되고 있으며, 이 중에 DSTM(Dual Stack IPv6 Dominant Transition Mechanism)[1] 기술은 IPv6 망에 위치하는 단말들이 IPv4와 IPv6의 듀얼 스택을 구현하고 있어서, 이 단말이 IPv6 노드와

* 숭실대학교 정보통신전자공학부 (cjduck@cns.ssu.ac.kr, souhwanj@ssu.ac.kr, younghak@ssu.ac.kr) (° : 교신저자)
** 삼성전자 통신연구소 (tjkwon@samsung.com)
논문번호 : KICS2006-01-050, 접수일자 : 2006년 1월 26일, 최종논문접수일자 : 2006년 11월 6일

통신하는 경우에는 IPv6 스택을 이용하고, IPv4 노드와 접속하는 경우에는 DSTM 서버로부터 임의의 IPv4 주소를 할당 받아 IPv4-in-IPv6 터널링 메커니즘으로 IPv4 노드와 통신할 수 있다. DSTM 서버에서는 IPv4 주소 할당 메커니즘으로 현재 IETF v6ops 워킹그룹에서 DHCP[2][3] 서버가 그 역할을 할 것으로 논의가 활발히 진행되고 있다. 그러나 DHCP와 같은 IP 주소 할당 메커니즘은 악의적인 노드의 DoS 공격에 의해 IP pool 주소가 고갈되는 보안 문제가 발생한다.

IPv4 주소 할당 메커니즘인 DHCP는 단말의 mac (media access control) 주소 인증 방법과 패스워드 기반의 인증[4], DHCP 클라이언트와 서버간의 비밀 정보를 사용하는 지연 (Delayed)[5] 인증 방식을 사용한다. 그러나 기존의 방법들은 mac 주소 사전 등록, 패스워드와 같은 비밀 정보의 공유 문제에 대해서 DHCP 클라이언트와 DHCP 서버 간에 현실적으로 가능한 교환 방법을 정의하지 않았기 때문에 실제 망에 적용하여 사용하는데 어려움이 있다. 이러한 문제로 현재 DHCP에서 IP 할당 인증은 특정 영역 내에서 동일한 패스워드를 그룹으로 사용하거나 인증 방법을 적용하지 않고 사용하기 때문에 DoS 공격으로 인한 IP 주소 고갈 문제가 발생할 수 있다.

본 논문에서는 HIP(Human Interactive Proof) 방법을 사용하여 DSTM 서버의 IPv4 주소 할당 방법으로 사용되는 DHCP 서버의 DoS 공격에 효과적으로 대응하고 실제 적용 가능한 실용성 있는 HRAA (Human Recognition Address Allocation) 기법을 제안한다. HRAA는 문구가 있는 이미지 파일을 사용하여 IP 주소 할당 요청에 대해 사람만이 확인하고 응답할 수 있고 이미지 패턴 인식이 불가능하여 자동화된 시스템에 의해 무작위로 IP 주소 할당 요청을 하는 DoS 공격에 효과적이다. 또한, 사전에 공유된 정보가 필요 없어 이동성이 제공되는 DSTM 도메인의 어떤 노드들도 언제 어디서나 DSTM 기술을 사용하여 IPv4 노드와 통신할 수 있다.

본 논문의 2장에서는 DSTM과 DSTM에서 IPv4 주소 할당 문제 분석, 기존의 IP 주소 할당 방법에 대해서 알아보고, 3장에서는 DSTM의 IP 주소 할당 서버 DHCP에 HRAA 기법을 제안하고 기존의 DHCP 인증 방법과 비교 분석한다. 4장에서는 DHCP 서버에 HRAA 기법을 구현하여 기존의 방법들과 비교 실험을 통해 실제 적용 가능함을 보여주고, 5장에서 결론을 맺는다.

Ⅱ. DSTM 서버의 IPv4 주소 할당 문제 보안 분석

이 장에서는 IPv6/IPv4 변환 기술인 DSTM과 DSTM에서 DHCPv6의 IPv4 주소 할당시 보안 문제점에 대해서 살펴본다.

2.1 DSTM

DSTM은 IPv6 망에 위치하는 단말들이 IPv4와 IPv6의 듀얼 스택을 구현하고 있어서, 이 단말이 IPv6 노드와 통신하는 경우에는 IPv6 스택을 이용하고, IPv4 노드와 접속하는 경우에는 IPv4-in-IPv6 터널링 메커니즘과 IPv4 스택을 이용해 통신할 수 있도록 하기 위한 구조이다. DSTM은 DSTM 서버, TEP (Tunnel End Point), 그리고 DSTM 노드 (IPv6 노드)로 구성되며, DSTM 노드가 IPv4 망에 있는 IPv4 노드와 접속하고자 하는 경우에는 자신이 IPv4-in-IPv6에 임시로 사용하기 위한 전역 IPv4 주소를 DSTM 서버로부터 할당 받는다. TEP는 DSTM 서버로부터 DSTM 노드의 IPv6 주소와 할당된 IPv4 주소 정보를 받아 TEP가 DSTM 노드의 패킷을 받았을 때 할당된 IPv4 주소를 소스 주소로 하여 IPv4 노드와 통신이 가능하도록 한다.

2.2 DSTM 서버에 대한 IPv4 주소 고갈 공격

DSTM 노드가 IPv4 노드와의 통신을 위한 IPv4 주소를 획득하는 과정을 살펴보면, DSTM 노드는 IPv4 주소를 얻기 위해서 DSTM 서버로 주소 할당 요청 메시지를 전송한다. 주소 할당 요청을 받은 DSTM 서버는 자신이 갖고 있는 IPv4 주소 중에 하나를 선택하여 DSTM 노드에게 IPv4 주소를 할당한다. DSTM 서버의 IPv4 할당 서버인 DHCPv6에서는 인증 방법으로 사전에 공유된 비밀 정보를 사용하여 생성된 MAC (Message Authentication Code)을 통해 인증하는 지연 인증 메커니즘을 사용한다 [5]. 그러나 지연 인증 기법 표준 문서에서는 사전에 비밀 정보를 공유하는 방법에 대한 구체적인 언급이 없고, 실제로 모바일 환경과 같은 곳에서는 노드들의 이동성 때문에 사전에 비밀 정보를 공유하는 것이 어렵기 때문에 적용하기 어렵다. 따라서 DSTM 서버에서 적절한 인증 기법을 사용하지 않을 경우에는 DoS 공격에 의해서 DSTM 서버의 IPv4 주소가 고갈될 수 있는 위협이 존재한다. 그림 1은 DSTM 서버의 IPv4 주소 고갈 공격 시나리오를 나타낸다.

① DSTM 공격자는 IPv6 소스 주소를 스푸핑하

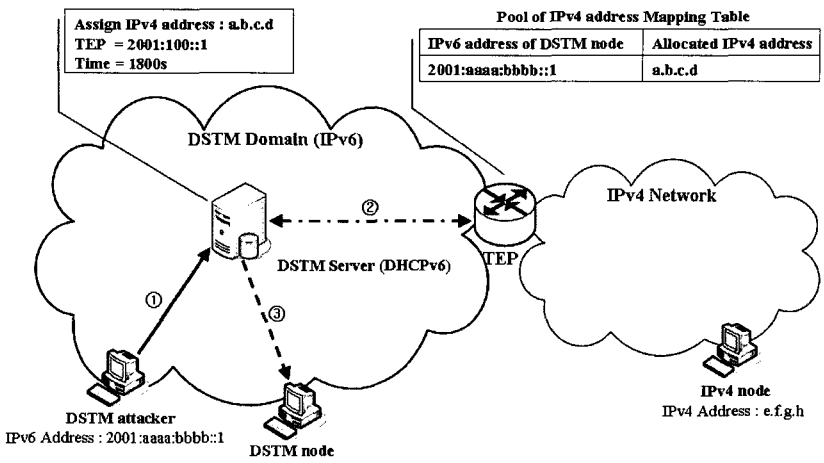

그림 1. DSTM 서버에 대한 IPv4 주소 고갈 공격

여 IPv4 주소 할당 요청 메시지를 DSTM 서버에게 전송한다.

② DSTM 서버는 IPv6 주소에 대한 IPv4 주소를 할당하여 자신의 IPv4 주소 매핑 테이블에 해당 정보를 기록하고, DSTM 도메인의 경계 라우터인 TEP에게 해당 매핑 정보를 전달한다.

③ DSTM 서버는 IPv4 주소 할당 요청 메시지에 대한 응답으로서 IPv4 주소 할당 응답 메시지를 DSTM 노드에게 응답한다. 이 때, IPv4 주소 할당 요청 응답 메시지를 받은 노드는 실제로 존재하지 않거나 할당 요청 메시지를 생성하지 않은 노드일 것이다.

④ 공격자는 IPv6 소스 주소를 계속적으로 변화시키면서 위의 ①에서 ③까지의 과정을 반복함으로써 DSTM 서버가 갖고 있는 IPv4 주소를 고갈 시킬 수 있다.

2.3 DHCP 인증 메커니즘 분석

DHCP 또는 DHCPv6에서 사용되는 인증 방법은 크게 세 가지로 분류된다. 먼저, 단말의 mac 주소를 이용한 인증 방법이다. 노드의 mac 주소 인증 방법은 DHCP 통신망에서 DHCP 서비스를 이용할 단말이 자신의 mac 주소를 DHCP 서버에 등록 한다. 이 등록 과정은 DHCP 통신망의 관리자에 의해서 이루어진다. 등록된 mac 주소는 DHCP 단말이 IPv4 주소 할당 요청 메시지를 보낼 때 인증값으로 사용된다. 두 번째는 IETF 표준인 지연 인증 방법이다[5]. 이 방법은 DHCP 단말과 서버 사이에 임의의 공유된 정보와, DHCP 서버에서 IPv4 주소 할당 요청 메시지에 대한 응답으로 DHCP 노드에게 메시지를 보낼 때 같이 보내진 nonce 값을 해쉬 알고리즘 MD5를 사용하여 DHCP 단말이 인증값을 생성해서 보내는 방법이다. 마지막으로 패스워드를 사용한 인증 방법이 있다[4]. 패스워드 기반의 인증 방식은 DHCP 노드와 서버 간에 메시지를 패스워드를 사용하여 암호화해서 주고받는 방식이다.

이러한 기존의 인증 방법들은 DHCP 서버에 등록된 사용자들에게 IP 주소 할당에 대한 인증과 권한 기능 제공으로 IPv4 pool 주소 고갈 공격에 대응할 수 있지만, 단말이 이동하는 모바일 환경이나 다른 통신망으로 처음 이동한 단말이 통신 할 때, DHCP 서버와 비밀 정보 공유를 통한 등록이 이루어져야 하기 때문에 실제 이동성이 제공되는 DHCP 환경이나 공개된 DHCP 환경에서 사용하는데 제약이 따른다. 따라서 IPv6 인프라 구축에 있어서 반드시 거쳐야 할 IPv6/IPv4 변환 기술에서 기존의 인증 기술 사용 제약에 따른 DHCP 서버의 IPv4 주소 고갈 공격에 대응하기 위해 새로운 방법이 필요하다.

Ⅲ. HRAA 인증 기법 제안

이 장에서는 DSTM 서버의 IPv4 주소 할당 서버인 DHCP의 DoS 공격을 통한 IP 주소 고갈 공격에 효과적으로 대응하기 위한 HRAA 기법을 제안하고 기존의 인증 방법들과 비교 분석한다.

3.1 Challenge Database(CDB)

HRAA는 임의의 노드들이 IPv4 주소 할당을 요청할 때 시스템의 자동화된 방법으로 응답할 수 없

인증 요청 데이터	응답 값	플래그	체크섬
school.gif	h	Invalid	14a9fe
asbcds.gif	h	Using	4ec8aa
cjdlsy.gif	h	Available	cc6b54
hyman.gif	m	Available	473c32

그림 2. Challenge DB(CDB)

고, 오직 사람만이 DHCP 서버의 응답을 식별하여 주소를 할당하는 기법이다. IPv4 주소 할당 서버에서는 사람이 식별할 수 있는 문구가 표현된 이미지 파일을 그림 2와 같이 Challenge DataBase (CDB)에 저장한다. CDB의 데이터는 인증 요청 데이터, 응답 값, 인증 요청 데이터 플래그, 체크섬 값으로 구성된다. 인증 요청 데이터는 IPv4 주소 할당 서버가 IPv4 주소 요청 노드에게 인증을 요청할 때 사용되는 값으로 사람이 인식할 수 있는 텍스트 문구가 나타난 이미지 파일이다. 응답 값은 IPv4 주소 할당 서버로부터 받은 인증 요청 데이터에 대해서 사용자가 입력하는 인증값이다. 인증 요청 데이터 플래그는 이미지 파일의 상태 값으로 'Available', 'Invalid', 'Using'의 값을 갖는다. 'Available' 값은 인증 이미지 파일을 인증 요청 데이터로 사용할 수 있는 상태를 나타내고, 'Invalid'는 인증 요청에 대한 응답이 없는 이미지 파일 또는 이미 IP 주소 할당 인증에 사용되었던 파일의 상태를 나타내며 인증 정보로 사용할 수 없다. 'Using' 상태 값은 현재 단말의 IP 주소 할당에 의해서 사용되고 있음을 나타낸다. 체크섬 값은 인증 이미지 파일에 대한 체크섬 값으로 악의적인 노드에 의해 이미지 파일 패턴 인식 및 재전송 공격을 차단한다. 제안 기법은 동일한 이미지 파일이 사용될 경우 악의적인 노드로부터 이미지 파일 데이터의 체크섬 값을 통해서 패턴 인식이 가능하다. 따라서 DHCP 서버는 악의적인 노드가 인증 요청 데이터의 패턴 인식을 불가능하게 하기 위하여 한번 사용된 이미지 파일은 그림 2와 같이 사람이 식별할 수 있는 문구를 유지하는 범위 내에서 파일명 변경 및 파일의 이미지 변환을 수행한다. 여기서 이미지 변환은 이미 널리 사용되고 있는 이미지 밝기, 채도, 감마, 선명도 변환 기술들에 의해서 변환된다.

3.2 DSTM 서버의 IPv4 주소 할당 인증 기법

HRAA는 DSTM 서버에서 IPv4 주소 할당 방법인 DHCP 서버의 DoS 공격을 통한 IPv4 주소 고갈 공격을 효과적으로 대응하기 위해 사용된다. 그

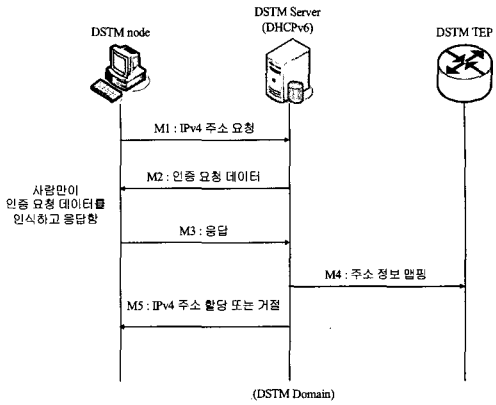

그림 3. HRAA 인증 기법을 사용한 IPv4 주소 할당

림 3은 IPv4 노드와 통신을 원하는 DSTM 노드가 HRAA 기법을 사용하여 DSTM 서버로부터 IPv4 주소를 할당 받는 모습을 보여준다. DSTM 노드가 DSTM 서버에게 IPv4 주소 할당을 요청하면 DSTM 서버는 'Available' 상태의 인증 요청 데이터를 선택하여 DSTM 노드에게 전송한다. DSTM 서버로부터 인증 요청을 받은 후, DSTM 노드는 사용자에게 인증 요청 데이터를 보여준다. DSTM 노드는 사용자로부터 입력 받은 값과 DSTM 서버로부터 받은 인증 요청 데이터를 DSTM 서버에게 전송한다. DSTM 서버는 DSTM 노드로부터 받은 인증 요청 데이터와 사용자가 입력한 값을 사용하여 DSTM 노드를 인증한다. DSTM 노드에 대한 인증이 성공적으로 이루어지면 IPv4 주소를 할당하고, 그렇지 않으면 IPv4 주소 할당 거부 메시지를 전송한다. 이와 같은 HRAA 인증 기법은 사전에 비밀 정보를 공유할 필요가 없어 이동성이 제공되고 공개된 DSTM 망에서 언제 어디서나 적용하여 DoS 공격을 통한 IPv4 주소 고갈 공격에 효과적으로 대응할 수 있다.

3.3 기존 인증 방법과 제안 방법 비교 분석

본 절에서는 기존의 IPv4 주소 할당 인증 방법인 단말기의 mac 주소를 이용한 인증, IETF 표준인 지연 인증, 패스워드를 사용한 인증 기법과 본 논문에서 제안한 HRAA 기법을 비교 분석한다. HRAA 기법은 이동성 제공 및 DoS 공격을 효과적으로 차단하기 위한 기법으로써 기존의 인증 기법들이 제공하는 IPv4 주소 할당에 대한 인증과 엄격한 권한 부여의 기능과는 차이가 있다. 그러나 본 절에서는 표 1과 같은 항목을 기준으로 비교 분석한다.

표 1. DHCP IPv4 주소 할당 고갈 공격 대응 기법 비교

	mac 주소 인증	지연 인증	패스워드 인증	HRAA 기법
공유정보 필요성	○	○	○	×
DoS 공격	△	△	△	×
유출된 인증정보 재사용	○	△	△	×
핸드오버 지원	×	×	×	△
사용자 제한	○	○	○	×

표 1은 이동성이 제공되고 공개된 DSTM 망에서 IPv4 주소 할당 고갈 공격에 대응하기 위한 기존 기술들과 HRAA 기법을 비교한 표이다. 첫째, HRAA 기법은 mac 주소, 패스워드, 지연 인증과 같이 사전에 미리 공유된 정보가 필요 없다. 일반적으로 많이 사용되는 mac 주소 인증은 DHCP 네트워크 관리자에 의해서 단말들의 mac 주소를 미리 등록해야 한다. IETF 표준인 지연 인증 방법은 DHCP와 DHCPv6에 정의된 인증 방법으로써 사전에 공유된 임의의 정보를 기반으로 HMAC-MD5[6][7] 또는 HMAC-SHA1[8]을 사용하여 MAC (Message Authentication Code) 값을 생성한 후 사용자를 인증하는 방식이다. 패스워드 인증은 안전한 DHCP 사용을 위하여 사전에 사용자 ID와 패스워드를 DHCP 인증 서버에 등록해야 한다. 이와 같이 기존의 방법들은 서로 공유하고 있는 비밀 정보에 대해서 온라인 또는 오프라인 상에서 서버에 등록을 해야 한다. 그러나 HRAA는 그러한 과정 없이 이동성이 제공되는 DSTM 도메인에서 언제 어디서나 실시간으로 IPv4 주소 할당 요청에 대해 간단한 인증으로 주소를 할당 할 수 있다. 이러한 특징은 모바일 환경에서 매우 중요하며 실제 현실 세계에 적용하는데 있어서도 큰 장점을 갖는다.

둘째, HRAA는 기존 방법과 달리 시스템의 자동화된 응답이 불가능하기 때문에 DoS 및 DDoS 공격과 같은 IPv4 주소 고갈 문제에 대해서 효과적으로 대응할 수 있다. 기존의 방법들이 제한적으로 mac 주소, 비밀정보, 패스워드 등을 엄격하게 적용하여 DoS 공격을 차단할 수 있지만 이동성이 제공되고 공개된 DSTM 환경에서 DHCP를 사용하는데 효과적이지 못하다. 이러한 이유로 기존의 방법들은 사용자들에게 동일한 정보를 분배하여 사용하게 되고, 인증할 때 시스템의 자동화된 방법으로 쉽게 DoS 또는 DDoS 공격을 통해 서버의 IPv4 주소가 고갈 될 수 있다. 또한, 기존의 인증 방법은 사전에 비밀 정보를 공유해야 한다는 문제점 때문에 실제 망에 적용하여 사용하기가 쉽지 않아 인증 메커니즘이 사용되지 않을 경우에는, DoS 및 DDoS 공격에 노출되는 문제점이 있다. 그러나 HRAA는 오직 사용자만이 DHCP 서버의 요청에 대해 응답할 수 있고, 악의적인 공격자들이 이미지 파일의 패턴 분석하는 것을 차단하기 위해 인증 요청 데이터를 사람이 식별 가능한 범위 내에서 무한정으로 이미지 변환을 하기 때문에 시스템의 자동화된 방법으로 서버의 인증 요청에 응답할 수 없다. 따라서 HRAA는 IP 주소 고갈 공격에 효과적으로 대응할 수 있다.

셋째, 기존의 방법들은 유출된 인증 정보로 지속적으로 IPv4 주소 할당을 받을 수 있다. mac 주소 인증 방법은 쉽게 무선 채널에서 스니핑이 가능하고, 지연 인증 방법은 임의 값의 비밀 정보를 사용할 경우 인증 정보 유출이 어렵지만, 패스워드 인증 방법과 같이 패스워드를 사용할 경우 사전 공격(Dictionary Attacks)에 의해 유출 위험성이 있다. 이렇게 유출된 정보는 인증 정보가 변경될 때까지 악의적으로 사용될 수 있는 문제점이 있다. HRAA는 패킷 스니핑에 의해서 손쉽게 유출 될 수 있지만, 이미지 변환으로 무한정 생성된 이미지 파일을 생성하기 때문에 한번 사용된 이미지 파일은 사용하지 않는다. 따라서 공격자에 의해 이미지 파일 재사용으로 인한 DoS 공격이 불가능하다.

넷째, 기존의 인증 방법들은 이동 환경에서 핸드오버가 이루어질 경우, DHCP 클라이언트와 서버 간에 필요한 비밀 정보를 온라인이든 오프라인이든 공유해야 하기 때문에 핸드오버에 문제가 있다. 온라인으로 비밀 정보를 공유해야 할 경우, 비밀 정보가 노출되지 않도록 보호할 수 있는 메커니즘이 추가적으로 요구되지만 현재 그러한 방법이 제공되고 있지 않다. 오프라인으로 비밀 정보를 공유할 경우에는 실질적으로 핸드오버가 불가능하다. HRAA는 핸드오버시 사용자가 매번 이미지 파일을 확인하고 입력해야 하는 번거로움이 있지만 단말과 DHCP 서버 간에 비밀 정보를 공유하는 과정 없이 실시간으로 인증을 받을 수 있기 때문에 기존 방법에 비해 핸드오버를 지원할 수 있다.

마지막으로, HRAA이 공개된 네트워크에서 DoS 공격에 효과적으로 대응할 수 있지만 IP 주소 할당이 특정 사용자에게만 이루어져야 하는 제한된 네트워크 환경에서는 사용자에 대한 인증과 권한 기

능 부여가 어렵다. 만약 DHCP 네트워크에서 인증과 권한 기능을 부여해야 한다면, 제안 기법 HRAA와 기존의 DHCP 인증 기능을 혼합하여 사용하면 이러한 문제를 해결할 수 있다.

Ⅳ. 인증 주소 할당 구현 및 실험

본 논문에서는 DHCP에서 HRAA 인증 기법을 설계하고 구현하여 인증 기법이 적용되지 않은 DHCP와 단말의 mac 주소 인증 기법을 적용한 DHCP들과 IPv4 주소 할당에 소요되는 시간을 측정하여 제안 기법 HRAA가 DoS 공격에 보다 효과적임을 확인하는 실험을 하였다. DHCP 클라이언트와 DHCP 서버의 운영체제는 Redhat Linux 2.4.20-8을 기반으로 하고 DHCP 모듈은 오픈 소스 DHCP 3.0.4b[9]를 사용하였다.

그림 4는 DHCP 서버에서 HRAA의 구현을 위한 순서도를 나타낸다. HRAA에서 인증 요청 데이터 선택 및 검증은 CDB를 통하여 이루어진다. 본 논문에서는 그림 5와 같이 기존의 밝기 조절 이미지 변환과 같은 기술들을 사용하여 적용한 10개의 파일들을 CDB에 저장하고 DHCP 클라이언트의 IPv4 주소 할당 요청시 인증 요청 데이터로 사용하였다. 여기서, 본 논문은 실험을 위해 10개의 이미지 파일을 사용하였지만 DHCP 서버는 매번 이미지 변환을 통해 새로운 이미지 파일들을 생성하여 인증 요청에 사용할 수 있기 때문에 악의적인 공격자가

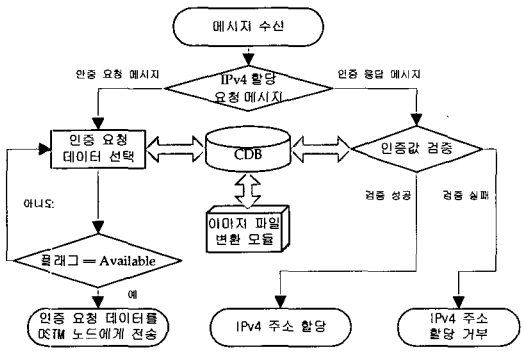

그림 4. HRAA 기법 순서도

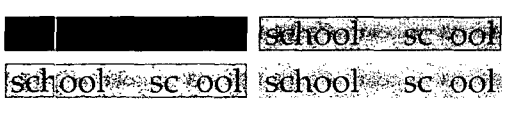

그림 5. 밝기 조절된 CDB 이미지 파일의 예

이미지 패턴을 인식할 수 없도록 할 수 있다.

HRAA 기법 실험에서 악의적인 공격자가 패킷 스니핑에 의해 인증 정보인 이미지 파일을 쉽게 스니핑하여 재사용 할 수 있는 문제점이 있기 때문에 본 실험에서는 타임아웃을 10초로 설정하여 인증 요청에 대해 응답하지 않을 경우 사용된 이미지 파일의 플래그를 'Invalid'로 설정하여 다른 IPv4 주소 할당 요청에 사용하지 못 하도록 하였다. 또한 한번 사용되었던 이미지 파일도 'Invalid'로 플래그 값을 설정하여 재사용되지 못 하도록 하였다.

인증용 이미지 파일이 포함된 DHCP Offer 패킷을 받은 DHCP 클라이언트는 이미지 파일을 사용자에게 보여주고 사용자가 직접 인증값을 입력하도록 하였다. 인증 이미지의 구성은 완성된 왼쪽 단어와, 문자 하나가 빠진 단어로 구성된다. 사용자는 빠진 문자를 인지하여 입력하면 DHCP 클라이언트는 인증값과 인증용 이미지가 포함된 DHCP Request를 DHCP 서버로 전송한다. DHCP 서버는 DHCP 클라이언트가 보낸 DHCP Request 패킷을 받고, 인증값에 대한 일치여부를 검사한다. 일치할 경우 DHCP ACK 패킷을 전송하여 DHCP 클라이언트가 IPv4 주소 할당을 받게 되지만, 인증값 검사가 실패할 경우에는 DHCP 클라이언트에게 DHCP NAK 패킷을 보내어 IPv4 주소 할당을 거절한다.

표 2는 인증 기법이 적용되지 않은 DHCP 방식과 단말의 mac 주소를 확인하여 인증하는 방식, 제안 기법 HRAA를 적용하였을 때 소요되는 IPv4 주소 할당 시간을 측정한 값이다. 표에서 보듯이 인증 기법이 적용되지 않은 DHCP는 평균 0.025s 내에서 할당을 받고, mac 주소 인증 방식은 0.053s, HRAA는 평균 3.533s가 소요되었다. (여기서, HRAA 기법은 사용자 반응에 따라서 다양하게 나타날 수 있지만 본 실험에서는 최대한 빠른 응답을 통해서 얻은 수치이다.) 따라서 HRAA 기법이 적용되었을 경우 DoS 공격을 통한 IPv4 주소 할당 공격에 많은 소요 시간이 요구됨을 확인할 수 있다. 또한 이동성이 제공되는 DSTM 환경에서 기존의 인증 기법들이 mac 주소 등록 또는 패스워드 등록

표 2. DHCP IPv4 주소 할당 소요 시간 비교

단위 : 초 (s)

	1회	2회	3회	4회	5회
인증 미적용	0.023	0.024	0.026	0.028	0.026
mac 인증	0.051	0.052	0.053	0.062	0.046
HRAA	3.191	4.083	4.247	3.211	2.934

과 같은 과정이 요구되기 때문에 실질적으로 핸드오버 지원이 어려운 반면, HRAA는 실시간으로 인증 정보인 이미지 파일을 전송 받아 사용자가 응답하면 되기 때문에 실험을 통해 소요된 3.5s 정도에서 핸드오버를 지원 할 수 있다.

V. 결 론

본 논문은 IPv6/IPv4 변환 기술인 DSTM에서 IPv4 주소 할당 서버로 사용되는 DHCP에서 DoS 공격을 통한 IPv4 주소 고갈 공격에 효과적으로 대응하기 위해 HRAA 기법을 제안하였다. DHCP 인증 방법은 사전에 미리 공유된 비밀 정보를 통해 인증하는 방법인 지연 인증을 사용하고 있다. 지연 인증 방법은 비밀 정보를 공유할 수 있는 방법에 대해서 구체적이지 않아 실제 망에 적용하기 힘들기 때문에 DSTM 서버에서 IPv4 주소 할당 서버로 DHCP가 사용될 경우 DoS 공격에 의한 IPv4 주소 pool 고갈 문제가 있다. HRAA 기법은 사람이 식별할 수 있는 문구가 포함된 이미지 파일을 사용하여 사용자를 인증하는 방법이다. HRAA 기법은 이동성이 제공되고 공개된 DSTM 환경에서 단말기의 mac 주소와 패스워드, 지연 인증과 같이 사전에 미리 공유된 정보가 필요 없고, 시스템의 자동화된 응답이 불가능하기 때문에 DoS 및 DDoS 공격과 같은 IPv4 주소 고갈 문제에 대해서 효과적으로 대응할 수 있다.

HRAA 인증 방법은 IPv6/IPv4 이전 기술인 DSTM 서버에서 IPv4 주소 고갈 문제에 대한 구체적인 해결책으로써 차세대 IPv6 망으로의 이전에 큰 역할을 할 것으로 기대된다. 또한, IPv4 주소 할당 서버인 DHCP 서버에 적용하여 IPv4 주소 할당 도메인 망에서 폭 넓게 사용될 것으로 기대된다.

참 고 문 헌

[1] J. Bound, "Dual Stack IPv6 Dominant Transition Mechanism," IETF, Internet Draft draft-bound-dstm-exp-04, October 2005.

[2] R. Droms, J. Bound, B. Volz, T. Lemon, C.Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6," IETF, RFC 3315, July 2003.

[3] R. Droms, "Dynamic Host Configuration Protocol," IETF, RFC 2131, March 1997.

[4] T. Komori and T. Saito, "The Secure DHCP System with User Authentication," in Proc. LCN2002, November 2002.

[5] R. Droms, "Authentication for DHCP Messages," IETF, RFC 3118, June 2001.

[6] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," IETF, RFC 2104, February 1997.

[7] R. Rivest, "The MD5 Message-Digest Algorithm," IETF, RFC 1321, April 1992.

[8] "Secure Hash Standard," National Institute of Standards and Technology, FIPS-180-1, April 1995.

[9] Internet Systems Consortium, DHCP 3.0.4b, http://www.isc.org/index.pl?/sw/dhcp/

최 재 덕 (Jaeduck Choi) 준회원

2002년 2월 숭실대학교 정보통신전자공학부 졸업

2004년 2월 숭실대학교 정보통신공학과 석사

2005년~현재 숭실대학교 정보통신전자공학과 박사과정

<관심분야> 이동 네트워크 보안, VoIP 보안, 네트워크 보안

정 수 환 (Souhwan Jung) 종신회원

1985년 2월 서울대학교 전자공학과 학사

1987년 2월 서울대학교 전자공학과 석사

1998년~1991년 한국통신 전임연구원

1996년 6월 University of Washington 박사

1996년~1997년 Stellar One SW Engineer

1997년~현재 숭실대학교 정보통신전자공학부 부교수, 개방형컴퓨터통신연구회 TG 의장

<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안

김 영 한 (Younghan Kim) 종신회원

1984년 2월 서울대학교 전자공학과 학사
1986년 2월 한국과학기술원 전기 및 전자공학과 석사
1990년 8월 한국과학기술원 전기 및 전자공학과 박사
1987년 1월~1994년 8월 디지콤 정보통신연구소 데이터통신연구부장
1994년 9월~현재 숭실대학교 정보통신전자공학부 부교수, 통신학회 인터넷 연구회 위원장, VoIP포럼 차세대기술분과위원장
<관심분야> 컴퓨터네트워크, 인터넷 네트워킹, 이동 데이터 통신망

권 택 정 (Taekjung Kwon) 정회원

1995년 2월 서울대학교 전기공학과 학사
1997년 2월 서울대학교 전기공학과 석사
1997년 2월~현재 삼성전자 통신연구소 책임연구원
<관심분야> 인터넷 네트워킹, 이동통신 시스템