

DoS 공격에 안전한 DSTM 서버의 IPv4 주소 할당 인증 방법

*문형권, *최재덕, *정수환, *김영한, **김선기

*숭실대학교 정보통신전자공학부, **삼성전자 정보통신 연구개발센터

{sysmoon, cjduck}@cns.ssu.ac.kr, {souhwanj, younghak}@ssu.ac.kr,

**sungj21.kim@samsung.com

Athentication Scheme of IPv4 Address Allocation against DoS Attack in DSTM Server

*Hyoungkwon Moon, *Jaeduck Choi, *Souhwan Jung, *Younghan Kim, **Sungi Kim

*School of electronic engineering, Soongsil University,

**Telecommunication R&D Center Samsung Electronics Co. Ltd.

요 약

IPv6/IPv4 변환 기술 중 하나인 DSTM 기술은 DSTM 서버가 IPv4 노드와 통신을 원하는 IPv6 노드에게 IPv4주소를 할당할 때, DoS 공격으로 인해 DSTM 서버의 IP pool 주소 고갈 공격에 노출되어 있다. 본 논문에서는 DSTM 서버의 IPv4 할당 방법으로 사용되는 DHCPv6의 인증 방법으로 Human Recognition (HR)을 제안하였다. HR 방법은 단말의 mac 주소를 이용하거나 delayed 방식과 같이 사전에 공유된 정보를 필요로 하지 않아 DSTM 도메인 내에서 언제, 어디서나 사용될 수 있고, 자동화된 시스템에 의해서 인증값을 생성할 수 없기 때문에 DoS 공격을 통한 DSTM 서버의 IP pool 주소 고갈 공격에 안전하다.

I. 서론

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, 그 중에서 DSTM (Dual Stack Transition Mechanism) [1] 기술은 IPv6 망에 위치하는 단말들이 IPv4와 IPv6의 듀얼 스택을 구현하고 있어서, 이 단말이 IPv6 노드와 통신하는 경우에는 IPv6 스택을 이용하고, IPv4 노드와 통신하는 경우에는 DSTM 서버로부터 임의의 IPv4 주소를 할당 받아 IPv4-in-IPv6 터널링 메커니즘으로 IPv4 노드와 통신할 수 있다. DSTM 서버의 IP 주소 할당 메커니즘으로는 현재 IETF v6ops 워킹그룹에서 DHCPv6 서버가 그 역할을 할 것으로 논의가 활발히 진행되고 있다[2]. 그러나 DHCPv6 [3]와 같은 IP 할당 메커니즘은 악의적인 노드의 DoS 공격에 의해 IP pool 주소가 고갈되는 보안 문제가 있다.

본 논문에서는 HR (Human Recognition) 방법을 사용하여 DSTM 서버의 IP 할당 메커니즘으로 사용되는 DHCPv6의 DoS 공격에 안전하고 실제 적용 가능한 실용성 있는 메커니즘을 제안한다. HR 인증 메커니즘은 문구가 있는 이미지 파일을 사용하여 인증 요청에 대해 사람이 확인하여 응답할 수 있고,

이미지 패턴 인식이 불가능하여 자동화된 시스템에 의해 무작위적으로 인증값을 생성하는 DoS 공격에 강하다. 또한, 사전에 공유된 정보가 필요 없어 DSTM 도메인의 어떤 노드들도 언제, 어디서나 DSTM 기술을 사용하여 IPv4 노드와 통신할 수 있다.

본 논문의 2장에서는 DSTM과 DSTM 서버의 IPv4 주소 할당 문제에 대해서 알아보고, 3장에서는 제안하는 HR 방법에 대해서 자세히 설명한다. 또한, 4장에서는 기존의 IP 할당 방법과 HR 방법을 비교 분석하고, 마지막으로 5장에서 결론을 맺는다.

II. DSTM 서버의 IPv4 주소 할당 문제 분석

이 장에서는 IPv6/IPv4 변환 기술인 DSTM과 DSTM에서 DHCP IP 할당 메커니즘을 사용할 때 나타나는 보안 문제점에 대해서 살펴본다.

1. DSTM

DSTM은 IPv6 망에 위치하는 단말들이 IPv4와 IPv6 듀얼 스택을 구현하고 있어서, 듀얼 스택 단말이 IPv6 노드와 통신하는 경우에는 IPv6 스택을 이용하고, IPv4 노드와 접속하는 경우에는 IPv4-in-IPv6 터널링 메커니즘을 이용하여 통신할 수 있도록 하기 위한 구조다. DSTM은 DSTM 서버, TEP (Tunnel End Point), 그리고 DSTM 노드 (IPv6 노드)로 구성되며, DSTM 노드가 IPv4 망에 있는 IPv4 노드와 접속하