IP Agent 기반 IPv6 주소 관리 시스템

이동일[1], 홍윤환[2], 김명균[1]

[1]울산대학교 전기공학부, [2](주)닥터소프트

IPv6 Address Management System Based on IP Agents

Dong-Il Lee[1], Yoon Hwan Hong[2] , Myung-Kyun Kim[1]

[1]School of Electrical Engineering, University of Ulsan, [2]Doctorsoft

E-mail : poweriyldi@gmail.com

요 약

기존의 IPv4주소의 한계성 때문에 전세계적으로 IPv6의 도입이 점점 가속화되고 있다. IPv6 시스템에서는 자동주소설정 기능으로 인해 각 호스트가 주소를 자동적으로 얻을 수 있다. 하지만 어떤 허가되지 않은 사용자가 악의적인 목적으로 주소를 얻고 접근할 수 있는 가능성도 존재하기 때문에 IP 주소에 대한 관리가 더욱더 중요시된다. 이를 위해서 IPv6 환경에서 인가된 호스트를 관리, 인가되지 않은 호스트의 접근을 차단하고 특정한 웹페이지로 유도하여 시스템의 보안을 유지하는 IP Agent 기반 IPv6 주소 관리 시스템을 제안한다.

ABSTRACT

Because of the limitations of traditional IPv4 address, the adoption of IPv6 has been accelerated. In IPv6 system, each host can obtain the IP address automatically using auto-configuration functionality, which is one of the features of IPv6. However, the auto-configuration functionality can allow a malicious user to get its IPv6 address and access the network without permission, the IP address management functionality becomes more important than IPv4. In this paper, we propose an IPv6 address management system based on IP agents, which protects the unauthorised users from accessing the network and redirects the web access of those users to a specific web page to induce them to access the network after installing the IP agents.

키워드

IPv6, ICMPv6, NDP(Neighbor Discovery Protocol), DAD(Duplicated Address Detection), 접속차단

I. 서 론

전 세계적으로 정보화가 급속도로 진행됨에 따라 정보기기간의 통신 또한 증가하고 있다. 최근 몇 년 사이에 스마트폰의 등장과 다양한 모바일 기기들의 등장으로 한 개인이 여러 대의 기기, 즉 여러 개의 IP 주소를 사용하고 있다. 과거에는 약 43억개의 주소를 가질 수 있는 IPv4로도 충분하다고 전망했으나, 현재 기하급수적으로 늘어나는 IP 주소의 수요를 감당하지 못하고 있다. 이런 문제를 해결하기 위하여 IETF(Internet Engineering Task Force)에서 IPv6를 도입하였고 주요국가와 사업자들은 본격적으로 도입을 하고 있다.

IPv6는 IPSec(Internet Protocol Security)라는 보안요소를 탑재하고 주소공간을 확대, 플로우 레이블(Flow Label)을 이용한 패킷별 품질제어 및 자동 주소 설정 등의 기능이 추가된 인터넷 프로토콜로서 관리자와 일반 사용자의 편의성이 증대될 것이다. 한편으로는 자동 주소 설정 기능을 이용하여 악의적인 목적을 가진 사용자가 제약 없이 주요 네트워크 장비에 접속할 수 있는 문제점도 있기 때문에 그에 대한 해결책도 필요하다. IPv6 환경에서 호스트 탐색 및 네트워크 접속 차단 에이전트 시스템”[1]에서 사용된 알고리즘은 NDP(Neighbor Discovery Protocol)의 NS(Neighbor Solicitation)와 NA(Neighbor Advertisement) 메시지를 이용하여 각 호스트들의 주소를 얻는 것인데 아직 주소를 얻지 못한 호스트는 차단할 수 있지만 이미 주소를 얻은 호스트는 차단하지 못하는 문제점이 있다.

본 논문에서는, IP agent를 이용한 IPv6 주소관리 시스템을 개발하였다. 본 IPv6 주소관리 시스템은 인가된 호스트에 설치된 IP agent와 전체 네트워크 IPv6 주소를 관리하기 위한 IPv6 주소관리 서버로 구성되어 있다. IP agent는 각 인가된 호스트에 설치되어, 해당 호스트의 IP주소를 포함한

하드웨어 및 소프트웨어 자원을 관리하는 기능을 수행한다. IPv6 주소관리 서버는 IP agent들로부터 인가된 호스트의 IPv6 주소 및 MAC 주소를 수집하고, 인가되지 않은 호스트 접속시 IP 주소를 획득하지 못하도록 하고, 이미 IP 주소를 획득한 미인가된 호스트의 경우에는 웹 접속시 특정 웹페이지로 redirect 하여 IP agent 설치 후에 사용하도록 유도하는 기능을 수행한다.

II. IPv6 주소체계

II.1 IPv6의 확장된 주소체계

IPv6에서는 주소의 한계성을 극복하기 위해서 주소공간을 확장시켰는데 IPv6는 3가지 유형의 주소가 있다.

1) 유니캐스트(Unicast) : 단일 인터페이스에 대한 주소, 유니캐스트 주소로 전송되는 패킷은 해당 주소로 식별되는 인터페이스로 전달된다.
2) 애니캐스트(Anycasat) : 인터페이스 집합에 대한 주소, 대부분의 경우 인터페이스들은 서로 다른 노드에 속하고 애니캐스트 주소로 전송되는 패킷은 해당 주소로 식별된 인터페이스 가운데 라우팅 프로토콜에 의해 측정된 가장 가까운 인터페이스로 전달된다.
3) 멀티캐스트(Multicast) : 서로 다른 노드에 속한 인터페이스 집합에 대한 주소로 멀티캐스트 주소로 전송되는 패킷은 해당 주소로 식별되는 모든 인터페이스로 전달된다. IPv6에는 브로드캐스트 주소가 따로 존재하지 않고, 멀티캐스트의 특수한 형태로 처리된다.

구분	IPv4	IPv6
주소크기	32 bits	128 bits
	약 43억개	약 43억X43억X43억X43억개
주소표기	8비트씩 4부분으로 10진수 표기	16비트씩 8부분으로 16진수 표기
	예) 201.12.33.51	예)2001:1234:5678:2233:5555:6666:aaaa:bbbb
멀티캐스트 주소 할당	A~E의 5클래스 중 D클래스 228개 주소	주소 상위 8bits가 '1'값인 2^{112}개 주소
	224.0.0.1 ~ 238.255.255.255	FFxx:0:0:0:0:0:0:0 ~ FFxx:F:F:F:F:F:F:F

그림 1 IPv4와 IPv6의 주소체계 비교

IPv6주소 중, 유니캐스트 주소 부분을 상세하게 구분하면 다음과 같다.

1) 링크 로컬 주소(Link-Local Address) : 동일한 링크에 있는 인접 노드들간의 통신에서 사용되는데 단일 링크 IPv6 네트워크에서 호스트들은 이 주소를 사용하여 통신할 수 있다. 128비트중 64비트가 정해진 특정주소로 시작되며 나머지 64비트는 인터페이스 자신의 고유한 ID를 참조하여 구성한다. 이렇게 만들어진 주소는 단일한 링크 내에서만 유효하고 라우터를 거쳐서 다른 세그먼트로는 전송될 수 없다.
2) 글로벌 유니캐스트 주소(Global Unicast Address) : 인터넷에서 범용적으로 사용할 수 있는 IPv6 주소이다. 일반적으로 라우터에서 64비트 프리픽스를 받고 나머지 64비트는 링크로컬주소와 마찬가지로 고유한 ID를 참조하여 구성한다.
3) 루프백 주소(Loopback Address) : 어떤 노드가 스스로에게 패킷을 보낼 수 있는 루프백 인터페이스를 식별하는데 사용하는데 IPv6에서는 (0:0:0:0:0:0:0:1 또는 ::1)으로 표현한다.

II.2 IPv6의 주소 습득 과정

IPv6에서는 자동주소설정 기능으로 주소를 얻을 수 있는데 그 과정은 다음과 같다.

1) 링크 로컬 주소는 Link-local prefix + Interface ID로 생성하는데 prefix는 fe80::/10 64비트, 나머지 64비트의 Interface ID는 48비트의 MAC 주소에 의해 modified EUI-64 포맷으로 생성한다. 이렇게 만들어진 주소는 한 네트워크에서 유일함을 ICMPv6 NS메시지와 NA메시지로 DAD과정을 통해서 검증한다.
2) 글로벌 유니캐스트 주소는 Global Routing prefix + subnet ID + Interface ID로 생성하는데 Global Routing prefix는 IANA에서 각 대륙에 배정하고 각 ISP에 배정, subnet ID는 각 사이트에서 네트워크를 분배하는 용도로 사용한다. Interface ID는 위의 링크 로컬 주소에서 쓰이는 것과 동일하게 생성한다.

III. 전체 시스템 구성 및 알고리즘

IP Agent 기반 IPv6 주소관리 시스템은 그림 2와 같이 인가된 각 호스트에 설치된 IP Agent 와 전체 네트워크의 IPv6 주소를 관리하는 기능을 수행하는 IPv6 주소관리 서버로 구성되어 있다. 인가된 호스트의 IP agent는 해당 호스트의 IP 주소를 포함한 하드웨어 및 소프트웨어 자원을 관리하는 기능을 수행한다.

III.1 인가된 IPv6 주소 수집 과정

본 IP 주소 관리 시스템에서 IPv6 주소관리 서버는 인가된 호스트의 MAC주소를 미리 수집했다는 가정 하에 IP Agent를 이용하여 아래와 같은 과정을 통해 인가된 IPv6 주소들을 수집한다.

1) Agent Program 실행시 자동적으로 설치된 Host의 주소(MAC Address, Link-local Address, Global Unicast Address)를 수집하여 IP 주소관리 서버측으로 전송한다.
2) IP 주소관리 서버는 각 Host로부터 받은 IP주소를 테이블 형태로 저장하여 관리한다.

III.2 비인가 호스트의 IPv6 주소 획득 차단

특정 호스트를 차단하는 과정은 IPv6의 자동주소설정 중 DAD 동작을 이용하여 구현하였는데

그 방법은 다음과 같다.

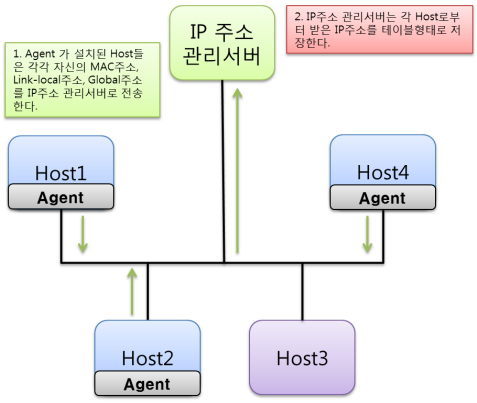

그림 2 Agent가 설치된 호스트들의 주소수집 및 관리

1) 특정 호스트는 DAD과정을 하기 위해서 NS 메시지를 멀티캐스트로 전송한다.
2) 에이전트 시스템이 이 호스트의 NS메시지를 받아서 차단해야할 호스트인지 판단한다.
3) 차단할 필요가 있는 호스트라면 변조된 NA메시지를 그 특정 호스트로 전송한다.
4) NA메시지를 받은 특정 호스트는 DAD과정의 결과로서 자신이 사용할 IP가 이미 사용되고 있는 IP라고 판단하여 IP주소를 가지지 못하게 된다.

이 경우, 아직 주소를 얻지 못한 호스트들은 차단이 가능하지만 이미 IP주소를 얻고 IP agent가 설치되어있지 않은 호스트들은 차단할 수 없기 때문에 이 호스트들이 웹 접속을 시도하였을 경우 특정한 웹사이트로 Redirection 하는 방법을 사용하였다.

Ⅲ.3 IP agent 미설치 호스트에 대한 설치유도

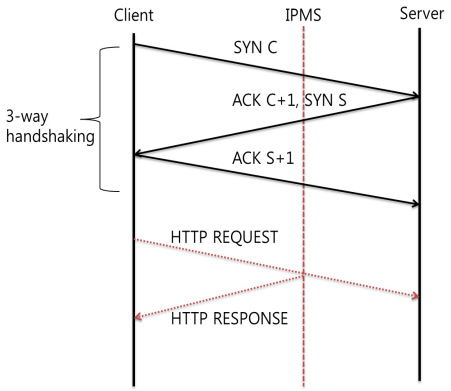

그림 3 비인가 호스트 웹페이지 요청 redirect

그림 2의 Host3과 같이 Agent Program이 설치되어 있지 않은 호스트가 있다고 가정하면, 이 호스트는 웹에 접속하기 위하여 다음과 같은 과정을 거치게 된다.

1) 특정 웹사이트의 주소를 입력하면 DNS서버에 접속하여 결과적으로 그 도메인에 해당하는 IP주소를 받아온 뒤 그 주소로 웹서버에 접속하게 된다.
2) 웹페이지를 요청하기 전에 TCP연결을 초기화하기 위한 3-way handshaking을 하게 되는데 호스트측에서 SYN 세그먼트를 보낸다.
3) 웹서버측에서는 클라이언트와 서버와의 세션을 확립하기 위해 SYN 세그먼트를 받았다는 승인 메시지 ACK와, 서버와 클라이언트의 세션을 맺기 위한 SYN 세그먼트를 Host 측으로 보낸다.
4) 호스트는 웹서버에서 보낸 SYN에 응답하기 위하여 ACK를 포함한 세그먼트를 웹서버측으로 보낸다.

그림 3의 3-way handshaking을 거치게 되면 클라이언트와 서버의 세션이 확립되고, 이후 호스트 측에서 웹서버로 웹페이지를 요청하게 된다. 이 때 IP주소 관리서버는 각 호스트들의 주소를 가지고 있는 테이블을 검사하여 웹 페이지를 요청한 호스트가 인가된 호스트인지 아닌지를 판단하게 된다. Host3는 Agent Program이 설치되어 있지 않은 호스트이므로 IP주소 관리서버(IPMS)는 웹서버를 가장하여 변조된 패킷을 생성하여 Host3의 요청에 응답한다. IP주소 관리서버로부터 패킷(특정 웹피이지)을 받은 Host3는 Agent Program을 설치하라는 웹페이지로 유도되어 프로그램을 설치한다. Host3은 다른 호스트들과 마찬가지로 IP Agent Server로 자신의 주소(MAC Address, Link-local Address, Global Unicast Address)를 전송하여 관리하에 놓인다.

Ⅳ. 구현 및 실험

본 실험은 windows7 운영체제와 Visual Studio 2010 C++, winpcap 4.1.2을 사용하여 진행하였고 실험구성은 그림 2와 같이 하였다.

Ⅳ.1 IP 주소를 얻지 못한 호스트의 차단

Host3는 windows 부팅 시 링크 로컬 주소를 얻기 위해 자동주소설정을 하고 NS 패킷을 전송하여 자신의 주소가 유일한지를 판단하는데 IP 주소 관리 서버에서 NA변조 패킷을 전송하여 Host3이 수행하는 DAD과정에서의 모든 IPv6주소를 이미 중복된 주소라고 판단하게끔 설정하여 어떤 주소도 얻지 못하게 하였다. 그림 4는 주소를 얻지 못한 Host3의 화면을 보여준다.

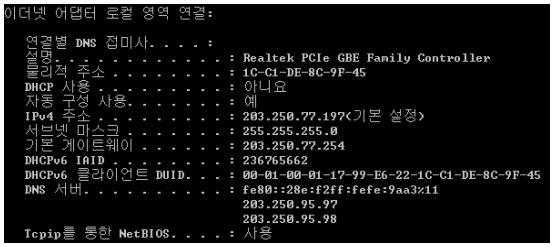

그림 4 주소를 얻지 못한 Host3.

정상적인 상태라면 Host3는 링크 로컬 주소와 글로벌 주소를 가지고 있어야 하지만 IP주소 관리 서버에 의해 IP를 얻지 못하였다.

Ⅳ.2 주소를 가진 호스트의 웹페이지 리다이렉션

Host3가 이미 IPv6 주소를 획득했을 경우, 웹 접속을 차단하기 위해 IP주소 관리 서버는 Host3의 Http Request 메시지를 감시한다. 그림 3과 마찬가지로 IP주소 관리 서버, 즉 IPMS는 Http Response에 설치 유도 웹페이지를 전송하게 된다.

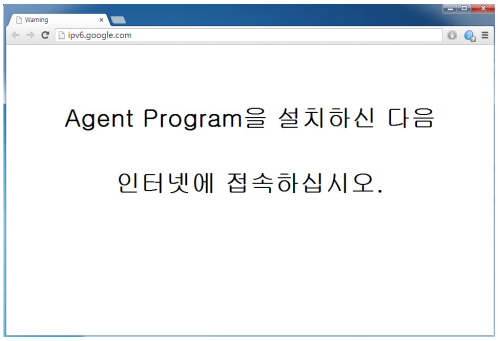

그림 5 Host3에서 받은 리다이렉션 된 웹페이지

그림 5는 IPv6 주소를 가지고 있지만 Agent가 설치되지 않은 Host3에서 ipv6.google.com 웹페이지를 접속했을 경우 IP주소 관리 서버에서 생성한 리다이렉션 웹페이지다.

Ⅴ. 결 론

본문에서 제시한 시스템은 각 Host에 에이전트 프로그램을 설치함으로써 네트워크상에 불필요한 패킷을 여러번 전송하지 않고 주소를 수집할 수 있고, 설치되지 않은 호스트는 적절한 프로그램 설치 유도 웹페이지를 전송함으로서 결과적으로 모든 호스트가 IP Agent 관리하에 인가된 IP를 부여받는다.

참고문헌

[1] 정연기, 문해은, “IPv6 환경에서 호스트 탐색 및 네트워크 접속 차단 에이전트 시스템”, Journal of Korea Multimedia Society Vol. 14 No. 1. (pp. 144-152), January 2011

[2] A. Conta, S. Deering, “Internet Control Message Protocol(ICMPv6) for the internet Protocol Version 6 (IPv6)” IETF RFC 1885, December 1995

[3] S. Deering, R Hinden, “Internet Protocol Version 6 (IPv6)”, IETF RFC 2460, December 1998