IPv6 주소자동설정 기능을 악용한 서비스거부공격 대응 기법

강성구°, 김재광, 고광선, 엄영익
성균관대학교 정보통신공학부
{lived°, linux, rilla91, yieom}@ece.skku.ac.kr

A Response Mechanism for Denying DoS Attacks abusing IPv6 Address Auto-configuration

Seong Goo Kang°, Jaekwang Kim, Kwangsun Ko, and Young Ik Eom
School of Information and Communication Engineering, Sungkyunkwan University

요 약

IPv6 프로토콜은 현재 인터넷 프로토콜로 사용되고 있는 IPv4 프로토콜이 가지고 있는 주소 고갈 문제, 미흡한 QoS 지원, 그리고 다양한 보안 문제를 해결하도록 설계되었다. 이 중에서 이동기기의 원활한 IPv6 네트워크와의 접속을 위하여 IPv6 프로토콜에서는 주소자동설정 기능이 추가되었으나, 이 기능을 악용한 서비스거부 공격 발생 가능성이 존재한다. 이에 본 논문에서는 IPv6 프로토콜의 주소자동설정 기능을 악용한 서비스거부공격에 대응할 수 있는 메커니즘으로써 RA 메시지에 일회용 키를 사용하는 방법을 제안한다.

1. 서 론

IPv6 프로토콜은 현재 쓰이고 있는 IPv4 프로토콜을 대체할 차세대 프로토콜로서, IPv4 프로토콜이 가지고 있던 주소 고갈 문제, 미흡한 QoS 지원, 그리고 다수의 보안 관련 문제를 해결하도록 설계되었다. 또한 IPv6 프로토콜은 IPv4 프로토콜에서 별개로 존재했던 IPsec을 통합시키는 등 많은 보안 문제점을 해결해 줄 수 있을 거라고 기대되고 있다. 그러나 IPv4 네트워크와 IPv6 네트워크 간 터널링 과정에서 나타나는 보안 문제 또는 주소자동설정 기능을 악용한 서비스거부 공격 가능성이 존재한다[1][2][3]. 이에 본 논문에서는 IPv6 프로토콜의 주소자동설정 기능을 악용한 서비스거부공격에 대응할 수 있는 메커니즘으로써 RA 메시지에 일회용 키를 사용하는 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 IPv6 프로토콜, 주소자동설정 기능, 그리고 서비스거부공격에 대해 서술하고, 3장에서는 IPv6 네트워크에서의 보안 문제와 주소자동설정 기능을 악용한 서비스거부 공격에 대해 설명한다. 4장에서는 3장에서 설명한 서비스거부공격에 대한 대응 기법을 제안한다. 마지막 5장에서는 결론 및 향후 연구계획을 설명한다.

2. 배경지식

본 장에서는 IPv6 프로토콜의 주요 특징들에 대해서 설명하고 그 중에서 보안 문제가 발생할 가능성이 있는 주소자동설정 기법에 관하여 자세히 설명한다. 그리고 서비스거부공격에 대해서 설명한다.

2.1. IPv6 프로토콜의 특징

주소 길이가 32비트인 IPv4는 최대 2^{32}개, 약 46억개 정도의 주소를 가질 수 있다. 반면, IPv6 프로토콜에서는 128비트 주소 길이를 사용하여 2^{128}개의 IP주소를 가질 수 있다[4]. 또한, IPv6 헤더는 IPv4 헤더에서 사용률이 낮았던 필드들을 제거하거나 단순화시켜 40바이트의 고정 크기가 되었다. 이로써 라우터에서 헤더 분석의 오버헤드를 줄였다. 그리고 추가 기능은 확장 헤더를 통해 지원한다. IPv6 프로토콜에서는 IPv4 프로토콜에서 명목상으로만 존재했던 QoS를 플로우 레이블 필드를 이용해 효과적으로 보장한다[5]. 그리고, IPv4 프로토콜에서는 옵션으로 보안 프로토콜인 IPsec를 따로 설치해야했지만, IPv6 프로토콜에서는 확장헤더 기능을 이용하여 IPsec의 기능을 지원한다[6].

2.2. 주소자동설정 기능

IPv4 프로토콜에서 네트워크에 접근하기 위한 방법에는 두 가지가 있다. 첫 번째는 수동으로 네트워크 설정을 하는 방법이다. 두 번째는 주소 배분을 위한 DHCP 서버를 이용해서 그 곳으로부터 IP와 기타 정보를 받아 설정하는 방법이다.

IPv6 프로토콜에서는 IPv4 프로토콜의 DHCP 서버와 같은 서버가 없는 호스트만으로 구성된 네트워크에서 주소자동설정을 지원한다. 이로 인해 모바일 환경에서 이동시에도 재설정 없이 계속 네트워크를 사용할 수 있다. 주소자동설정은 라우터의 네트워크 프리픽스 정보와 MAC(Media Access Control) 주소를 사용한다.

주소자동설정에는 상태 보존형과 상태 비보존형의 2가지 종류가 있다.

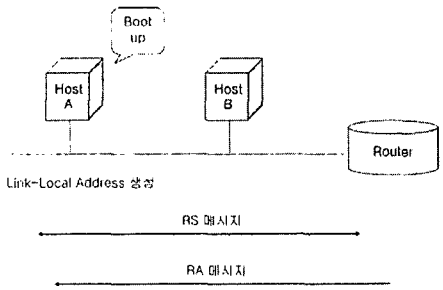
2.2.1. 상태 보존형 자동 설정

상태 보존형 자동설정은 DHCPv6 서버로부터 주소를 비롯한 모든 네트워크 정보를 받는 방식이다. 이 방식을 통해서 주소 이용을 효율적으로 할 수 있고, 인증을 통한 보안 관리가 가능하다는 장점이 있는 반면 서버가 데이터베이스에 그만큼의 인증 데이터를 가지고 있어야 한다는 단점이 있다. 이 방식은 IPv4 프로토콜의 DHCP와 같은 방법이므로 IPv6 프로토콜에서 새롭게 선보인 기술이라고는 할 수 없다.

2.2.2. 상태 비보존형 자동설정

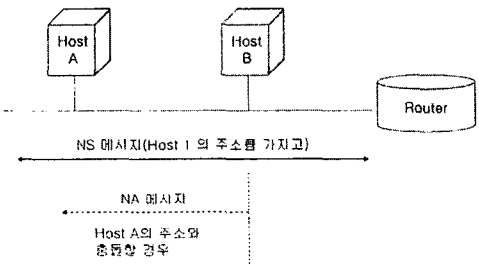
상태 비보존형 자동설정은 IPv6 프로토콜에서 새로 고안된 주소자동설정 기능으로 호스트가 라우터의 네트워크 정보와 자신의 인터페이스 정보를 이용하여 자체적으로 IPv6 주소를 생성한다.

상태 보존형 방식과는 달리 별도의 서버가 필요 없지만 인가되지 않은 호스트의 접근등으로 인한 보안 문제가 발생할 수 있다. 본 논문에서 이후로 언급하는 IPv6 프로토콜 프로토콜의 주소자동설정은 모두 상태 비보존형 방식이다.



(그림 1) 상태 비보존형 주소자동설정

그림 1에서 보이는 바와 같이 라우터가 Router Advertisement(RA) 메시지를 자신의 노드 내의 호스트에게 보내면 주소자동설정을 하려는 호스트가 Router Solicitation(RS) 메시지를 보낸다. 그리고 RA에서 라우터의 네트워크 프리픽스 정보를 얻어낸 호스트가 자신의 인터페이스 정보와 합쳐서 링크-로컬 주소를 생성한다. 그리고 디폴트 라우터를 등록하고 글로벌 주소를 생성한다[7].



(그림 2) 주소 설정 후 NS 메시지를 보내는 과정

그리고 그림 2에서와 같이 주소가 중복되었는지 확인을 위해 Neighbor Solicitation(NS) 메시지를 해당 네트워크의 노드의 호스트들에게 보낸다. 만약 Neighbor Advertisement(NA) 메시지가 돌아온다면, 주소가 중복된 것이다[7].

2.3. 서비스거부 공격

서비스거부공격은 인터넷상에 서비스되고 있는 자원을 더 이상 이용 불가능하도록 하는 공격이다. 네트워크 접속이나 서비스를 일시적으로 이용 불가능하게 만드는 공격이 악의적인 공격자에 의해 발생될 수도 있지만 프로그램의 버그 등으로 인해 우연히 발생하는 경우도 있다.

서비스거부공격의 발전된 형태인 분산서비스거부공격은 다수의 시스템이 하나의 표적을 향해 서비스거부공격을 하는 공격 방법을 말한다. 분산서비스거부공격 악의적인 공격자가 자신이 제어할 수 있는 시스템들을 이용해서 명령 한번으로 공격 대상에 많은 양의 패킷을 보내는 방법이다. 이로써 목적이 된 호스트는 정상적인 서비스를 제공하지 못하거나 과부하로 인하여 다운 될 수 있다.

3. IPv6 네트워크에서의 보안 문제

IPv6 프로토콜의 보안 문제점에는 상태 비보존형 주소자동설정에서 인가되지 않은 호스트의 액세스 문제 혹은 NS 메시지의 악용한 공격 문제, 악의적인 공격자가 RA 메시지를 보내서 자신을 라우터로 속이는 문제, 그리고 IPv4와 IPv6 프로토콜이 같이 쓰이는 네트워크에서 IPv4와 IPv6 프로토콜 간 터널링을 이용해서 방화벽을 넘을 수 있는 문제점 등이 존재한다[1][3]. 이 중에서 주소자동설정을 이용한 공격을 살펴본다.

3.1 IPv6 프로토콜 주소자동설정을 이용한 공격

어느 라우터에게 인가되지 않은 다수의 호스트들이 동시에 주소자동설정을 요청하게 되면 서비스거부공격이 될 수 있다. 모바일 환경이라면 악의적인 공격자가 소형의 IPv6 네트워크 기기를 다량 가지고 공격하고자 하는 라우터의 네트워크 범위 경계선을 반복적으로 출입해서 서비스거부공격을 할 수 있다.

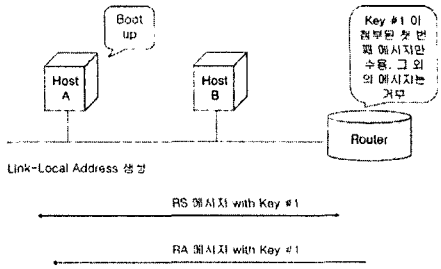
각 메시지의 헤더를 제외한 크기는 RA 메시지가 20바이트, RS 메시지가 12바이트, NS 메시지가 28바이트이다[8]. 그림 1과 그림 2가 보이는 바와 같이 한 번의 주소자동설정을 위해서는 RA, RS 그리고 NS 메시지가 1번씩 해당 네트워크의 노드에 뿌려지게 된다. 즉, 주소자동설정이 1번 시도될 때마다 최소한 180바이트(= 40 × 3 + 20 + 12 + 28)의 대역폭이 소모된다. 이 대역폭을 d 라고 한다. 그리고 우선 네트워크의 상황을 가정하였으므로 네트워크의 대역폭 자원 b 는 11Mbps로 가정한다.

$b = 11 \times 1024 \times 1024 \div 8 = 1441792$ Bps 이고, $b \div d \fallingdotseq 8010$, 약 8000이다. 즉, 1초에 약 8천개의 IPv6 모바일 기기가 출입을 반복하게 될 경우 이 공격이 성립된다.

4. 제안 기법

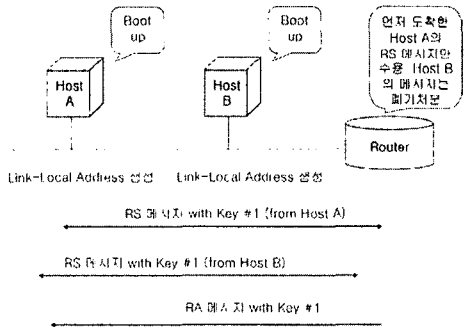
라우터가 자신의 노드들에게 RA 메시지를 보낼 때 임의의 키 값을 첨부해서 이후부터 해당 노드들로부터 오는 메시지에도 그 키 값을 첨부해야만 인가된 메시지로 판단하는 방법이 있다.

이 때, 그 키 값을 생성할 때 시간 정보를 넣어서 일정 주기로 변하게 하면 어느 정도 메시지에 신뢰성을 높일 수 있다.



(그림 3) 일회용 인증 키 값을 이용하여 메시지를 송수신하는 과정

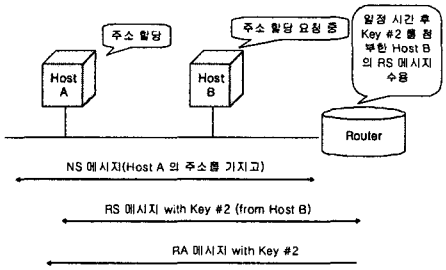
이 방법을 활용하여 그림 3이 보이는 바와 같이 3.1절에서 제기된 다량의 소형 IPv6 모바일 기기를 이용한 공격을 막을 수 있다. RA 메시지에 첨부하는 키를 일회용으로 사용하는 방법이다. 즉, 라우터가 키 #1을 RA에 실어서 보내고 난 후 어떤 노드가 키 #1을 사용하여 메시지를 보내면, 그 메시지는 인가된 메시지로 처리하고, 그 이후 키 #1을 이용한 메시지는 무시하고 새로운 키 #2를 RA 메시지에 실어서 보내는 것이다.



(그림 4) 2대의 호스트가 동시에 주소자동설정을 요청하는 상황

그림 4가 보이는 바와 같이 2대 이상의 호스트가 라우터에게 주소자동설정을 요청하는 상황을 가정해본다. 호스트 A와 호스트 B는 RA 메시지에서 키 #1이라는 키 값을 받은 상태에서 RS 메시지에 똑같이 키 #1을 첨부해서 보낸다. 이 때 라우터는 인가된 키인 키 #1을 가진 메시지 중에서 먼저 도착한 호스트 A의 메시지만 받아서 처리한다. 즉, 호스트 A는 주소를 할당받지만, 호스트 B는 주소를 할당받지 못하고 재시도하게 된다.

그림 5가 보이는 바와 같이 일정 시간이 지난 후, 라우터가 새로운 키 #2를 첨부한 RA 메시지를 보낸다. 호스트 A은 주소를 할당받고 NS 메시지를 네트워크에 보낸다. 호스트 B는 새로운 키 #2를 첨부한 RS 메시지를 다시 라우터에게 보내서 주소할당을 요청한다. 호스트 B의 RS 메시지는 이 때 라우터에게 수용되고 호스트 B는 주소를 할당 받게 된다.



(그림 5) 호스트 A만 주소할당을 받고 호스트 B는 재시도하는 과정

이 방법을 사용하면 많은 숫자의 IPv6 모바일 기기가 동시에 들어오고 나가는 상황이 발생해도 라우터가 처리 가능한 속도로 모바일 기기들이 네트워크에 출입하게 되므로 서비스거부공격을 방지할 수 있다.

5. 결론 및 향후 연구계획

IPv6 프로토콜은 현재 인터넷 연결을 위하여 사용되고 있는 IPv4 프로토콜이 가지고 있는 보안 문제를 해결하도록 설계되었다. 대표적으로 IPsec 프로토콜을 사용함으로써 많은 부분에서 발생할 수 있는 보안 문제를 해결할 수 있지만, IPv6 프로토콜에서 새로이 추가된 기능으로 인하여 새로운 보안 문제가 발생할 가능성이 존재한다. 이에 IPv6 프로토콜의 주소자동설정 기능을 이용한 서비스거부 공격에 대해서 설명하였고, 이러한 공격에 대응하기 위하여 일회용 키를 이용하는 기법을 제안하였다. 향후 연구 계획으로는 제안 기법에 대한 테스트를 통하여 실질적인 성능평가를 실시하고자 한다.

[참고문헌]

[1] A. Conta, Generic Packet Tunneling in IPv6 Specification, RFC 2473.
[2] S. Thomson, T. Narten, IPv6 Stateless Address Autoconfiguration, RFC 2462.
[3] B. Carpenter, Connection of IPv6 Domains via IPv4 Clouds, RFC 3056.
[4] R. Desmeules, Cisco Self-Study: Implementing IPv6 Networks (IPv6), Cisco Press, 2003.
[5] C. Partridge, Using the Flow Label Field in IPv6.
[6] P. Loshin, IPv6: Theory, Protocol, and Practice 2nd ed., Morgan Kaufmann Publishers, 2004.
[7] T. Narten, Neighbor Discovery for IP Version 6 (IPv6), RFC 2461.
[8] J. Davies, Understanding IPv6, Microsoft Press, 2003.