Mobile IPv4 네트워크에서 접속제어리스트와 역터널링을 이용한 IP Spoofing 제거 방안

Defeating IP Source Address Spoofing with Foreign Agent Care-of-Address in Mobile IPv4

김한림, 김성일, 김상언, 박세준, KT 컨버전스연구소
Han-Lim Kim, Sung-Il Kim, Sang-Eun Kim, Se-Jun Park
KT Convergence Laboratory

Abstract

The network ingress filtering is a simple and efficient method for preventing IP source spoofing of fixed nodes. Since mobile hosts cannot communicate with its correspondent nodes if the network ingress filtering is configured in mobile IPv4 network, reverse tunneling was considered as a method for avoiding network ingress filtering. But, unfortunately this method does not solve IP source spoofing of mobile nodes. In this paper, we propose a simple and efficient method for preventing IP source spoofing of mobile nodes assuming that only the mobile hosts connected to foreign agents and the network that foreign agent manages is small.

Keyword

mobile IPv4, IP source spoofing, reverse tunneling, network ingress filtering, access control list

I. 서 론

출발지 주소를 변조한 서비스 거부 공격이 빈번해 지면서 인터넷 서비스 공급자(Internet Service Provider, ISP)에게 이 문제에 대한 해결은 중요하게 여겨져 왔다[1]. 이러한 문제를 해결하기 위해 다양한 해결책들이 제시되었으며[2], 그 중 가장 단순하면서도 효과적인 해결 방안으로 네트워크 진입 여과(Network Ingress Filtering)[3]가 제안되었다 이 정책에서 ISP가 관리하는 각각의 라우터들은 자신이 관리하는 네트워크로부터 들어오는 모든 패킷에 대해 자신의 네트워크에 속하지 않는 출발지 주소를 가지는 패킷은 전부 버림으로써 출발지 주소를 변조한 DoS공격을 해결하려 하였다.

이동 IPv4[4]에서는 통신을 할 때 홈 주소(Home Address, HoA)를 출발지 주소로 하여 상대 노드(Correspondent Node, CN)와 통신을 한다. 이러한 이동 IPv4에 진입 여과 정책을 적용하였을 경우 홈 주소를 출발지 주소로 하는 이동 노드의 패킷들은 실제 그 네트워크에 속하는 주소가아니기 때문에 전부 버려진다. 이를 피하기 위해 나타난 것이 역터널링[5]이다. 이 역터널링을 통하여 진입 여과를 피한 통신에는 성공하였으나, 이동 노드의 출발지 주소 변조를 통한 서비스 거부 공격은 막지 못하게 되었다.

본 논문에서는 이동 IPv4에서 외부 에이전트에 이동 노드들만이 연결되고 외부 에이전트가 관리하는 네트워크가 작다는 가정하에, 이동 노드의 출발지 주소 변조를 이용한 서비스 거부 공격을 효과적으로 막는 방법에 대해 제안하고자 한다.

II. 공중 무선망에서의 이동 IPv4 지역 주소 설정 방식

이동 IPv4에서는 지역 주소를 설정하는 방식을 두 가지로 제공한다. 하나는 C-CoA

(Co-located CoA)라 하여 이동한 네트워크에 속하는 주소를 외부 에이전트로부터 받는 방법이고, 또 하나는 FA-CoA (Foreign Agent CoA)라 하여 외부 에이전트의 인터페이스 주소 중 하나를 이동 노드의 지역 주소로 사용하는 방식이다. C-CoA 방식에 의하면 네트워크가 모든 이동 노드에 대하여 지역 주소를 할당한다. 즉 모든 이동 노드가 홈 주소와 지역 주소의 두 개의 주소를 갖게 된다. 반면에 FA-CoA 방식에서는 이동 노드들이 외부 에이전트의 IP 주소를 지역 주소로 공유하므로, 필요한 IP 주소의 수를 절약할 수 있다. 따라서 이동 노드의 수가 늘어날수록 C-CoA 방식은 FA-CoA 방식에 비하여 사용하는 IP주소의 개수가 두 배씩 증가한다. 인터넷 서비스 공급자 입장에서 사업화와 IPv4의 주소 고갈 문제를 고려할 경우 FA-CoA선택은 필수적이다 따라서 본 논문에서는 외부 에이전트 지역 주소 방식으로 지역 주소를 설정하는 방법만을 고려하기로 한다.

III. 이동 IPv4에서의 역터널링 문제

본 절에서는 이동 IPv4에서의 역터널링 문제를 분석하기 위하여 테스트베드를 구축하여 실험한 결과에 대하여 설명한다. RFC3024를 참조하면 네트워크 진입 여과를 피하기 위한 역터널링 기술에는 크게 두 가지 형태가 있다. 이것은 이동 노드 등록 요청 시에 설정될 수 있으며 외부 에이전트가 특정 형태를 지원할 경우 받아들여진다. 첫 번째는 캡슐화 전달 형태(Encapsulation Delivery Style)라고 하여 이동 노드에서부터 패킷을 캡슐화하여 보내는 형태이고, 두 번째는 직접 전달 형태(Direct Delivery Style)로서 이동 노드에서는 외부 에이전트로 캡슐화 없이 패킷을 보내고, 외부 에이전트는 방문자 리스트를 확인하여 패킷을 캡슐화 후 보내는 형태, 이 두 가지이다.

이 실험에서는 네트워크 진입 여과를 적용하였을 때 이동 노드가 통신을 할 수 있는지, 그리고 네트워크 진입 여과가 설정되었을 때 역터널링이 제대로 동작하는 지를 확인하고자 하였다.

실험 환경은 그림 1. 과 같이 구성하였다.

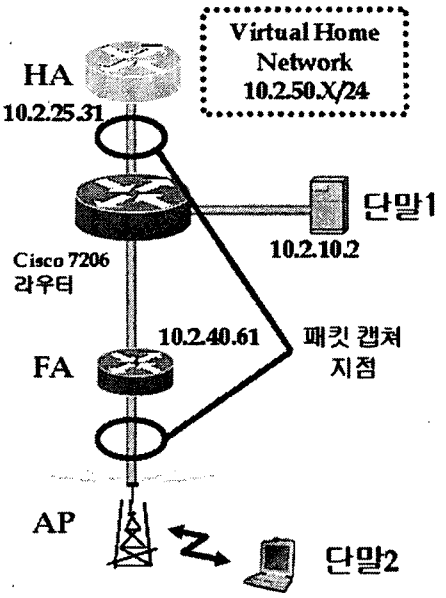

그림 1. 테스트베드 구성도
Figure 1. the diagram of testbed

각 실험 장비들은 다음과 같다.

홈 에이전트(HA): Cisco 7206 Router
IOS: c7200-js-mz.123-11.T.bin

외부 에이전트(FA): Cisco 3725 Router
IOS: c3725-jsx-mz.v6

무선 접속 장비(AP): Cisco AIR-AP1210
IOS: c1200-k9w7-mx.122-15.JA

이동 노드(MN): 802.11g를 지원하는 인터페이스를 가진 노트북

단말용 이동 IP 클라이언트: BirdStep Mobile IP v1.4.99

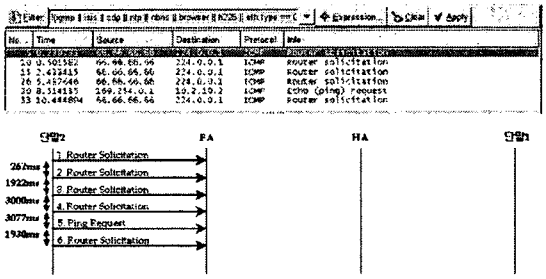

그림 2. 네트워크 진입 여과만을 적용하였을 때
Figure 2. when only the network ingress filtering is applied

실험결과 네트워크 진입 여과만을 설정하였을 때 그림 2. 와 같이 통신이 안 된다는 것을 확인하였으며, 네트워크 진입 여과를 외부 에이전트에 설정을 하고, 단말이 직접 전달 형태의 역터널링을 사용할 때도 통신이 되지 않음을 확인하였다.

먼저 직접 전달 형태를 적용하였을 때의 결과를 보면, 단말이 처음 라우터 추출 단계에서 사용하는 주소가 이동 IP 클라이언트가 활성화되기 이전에 받은 주소(66.66.66.66)이기 때문에 네트워크 진입 여과에서 버려졌다. 또한 이 주소에 대해 허용했을 경우 첫 Registration 시 주소가 0.0.0.0이기 때문에 마찬가지로 통신이 되지 않았다. 따라서 그림 3. 에서는 네트워크 진입 여과에 이러한 주소(0.0.0.0, 66.66.66.66)에 대해서만 통신을 허가시켰다.

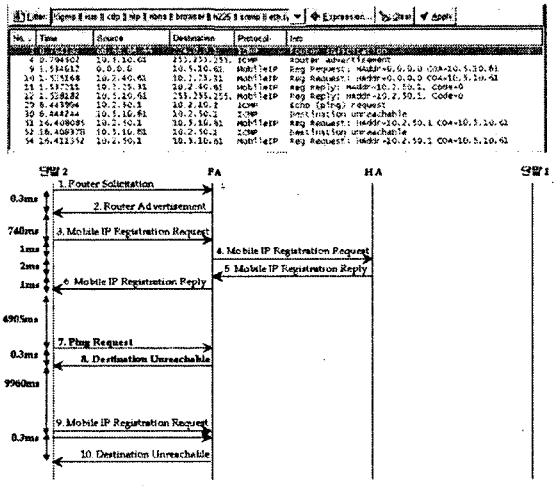

그림 3. 네트워크 진입 여과(0.0.0.0, 66.66.66.66 은 허용), 직접 전달 형태의 역터널링을 허용하였을 때

Figure 3. when reverse tunneling of direct delivery style is allowed

직접 전달 형태의 역터널링에서는 외부 에이전트에서 캡슐화를 하게 되어 있기 때문에 실제로 패킷의 출발지 주소는 홈 주소이다. 따라서 네트워크 진입 여과 정책에 의해 패킷이 그림 3. 과 같이 버려졌다. 설사 이것이 라우터 구현상의 문제라 하더라도, 다른 네트워크로 이동했을 경우 이동 노드 등록 요청의 출발지 주소가 홈 주소가 되기 때문에 이동 노드 해지 패킷이 그림 3. 에서 버려진 것처럼 버려진다.

이 결과로부터 이동 IPv4에서는 외부 에이전트 지역 주소를 사용하여 통신을 할 때 직접 전달 형태의 역터널링은 진입 여과 정책을 우회하지 못하고 패킷들이 버려짐을 확인하였다.

캡슐화 전달 형태의 경우 이동 IP 클라이언트에서는 설정할 수 있었으나 Cisco의 외부 에이전트 장비에서 직접 전달 형태만을 지원했기 때문에 이동 노드 등록 요청에 대해 이동 노드 등록 거부만이 외부 에이전트에서 이동 노드로 돌아왔다. 그러나 캡슐화된 내부의 패킷을 직접 보지 않는 이상 인터넷 서비스 공급자의 망 쪽에서 출발지 IP 변조(Source IP spoofing)를 이용한 서비스 거부 공격을 막는 방법은 터널이 끝나는 홈 에이전트에서 제거하는 방법 이외에는 없고, 이러한 방법도 캡슐화된 패킷들이 일단 망으로 들어와 네트워크 자원을 소모하기 때문에 효율적이지 못하다. 또한 캡슐화 전달 형태를 이용할 경우 단말에서부터 캡슐화하기 때문에, 통신 시 무선 자원을 더 소모하며, 이러한 캡슐화 처리 자체가 단말에 부담을 줄 수 있다. 물론 직접 전달 형태의 경우에 멀티캐스트(multicast)와 브로드캐스트(broadcast)를 단말에서 할 수 없다는 단점이 있지만 이것은 그러한 서비스가 필요하느냐에 따라, 또 인터넷 서비스 공급자의 정책에 따라 그 중요도가 다르다.

IV. 이동 IPv4에서의 네트워크 진입 여과 대체

위에서 실험한 결과처럼 네트워크 진입 여과만을 적용하였을 경우 통신이 되지 않았고, 직접 전달 형태의 역터널링은 네트워크 진입 여과 자체를 피할 수 없었다. 캡슐화 전달 형태의 역터널링은 일단 단말 쪽과 무선 구간에 부담을 줄 수 있고, 이동 노드의 출발지 IP 변조를 이용한 서비스 거부 공격을 망 쪽에 부담을 주지 않고 처리하기가 어렵다

따라서 이 절에서는 네트워크 진입 여과을 피하면서 이동 노드의 서비스 거부 공격을 막는 방법을 생각하기보다 이러한 이동 노드들에게 적합한, 등록된 사용자만이 통신할 수 있으

면서 출발지 IP변조를 막는 방법을 제시하고자 한다.

제안은 다음과 같다. 이동 노드는 직접 전달 형태의 역터널링으로 통신을 하며 외부 에이전트에서는 진입 여과를 하지 않는다. 다만 출구 인터페이스(egress interface)에 외부 에이전트 지역 주소(FA-CoA)를 출발지 주소로 가지는 패킷만이 통과할 수 있도록 접근 제어 리스트(Access Control List, ACL)을 설정한다. 또한 외부 에이전트 진입 인터페이스(FA ingress interface)들에 출발지 주소로 외부 에이전트 지역 주소(FA-CoA)로 들어오는 모든 패킷을 버리도록 접근 제어 리스트를 설정한다. 이렇게 설정할 경우 단말에서 캡슐화 하지 않기 때문에 단말에 부담이 적고, 무선망의 자원을 더 소모하지도 않는다. 또한 설정 방법이 간단하며 이동 노드 등록이 허락된 이동 노드만이 통신을 할 수 있고, 이동 노드 등록 시 사용한 홈 주소만을 출발지 주소로 하는 패킷만이 망 진입이 허용된다.

V. 실험 결과

제안한 방법을 실험한 결과는 그림 4. 와 같다.

그림 4. 에서의 동작을 보면, 이동 노드는 외부 에이전트에게 패킷을 보내고 외부 에이전트는 출발지 주소를 그림 5. 에서의 방문자 리스트와 비교를 하여 해당 이동 노드가 맞는지 확인을 한다. 확인된 패킷은 외부 에이전트 지역 주소를 출발지 주소로 하여 캡슐화한다. 이 때 외부 에이전트 지역 주소를 출발지 주소로 하는 패킷은 외부 에이전트에 들어갈 수 없으며, 오직 외부 에이전트에서 캡슐화된 패킷만이 나갈 수 있다. 따라서 오직 이동 노드 등록에 성공한 이동 노드의 홈 주소를 출발지 주소로 하는 패킷만이 통신이 허용된다.

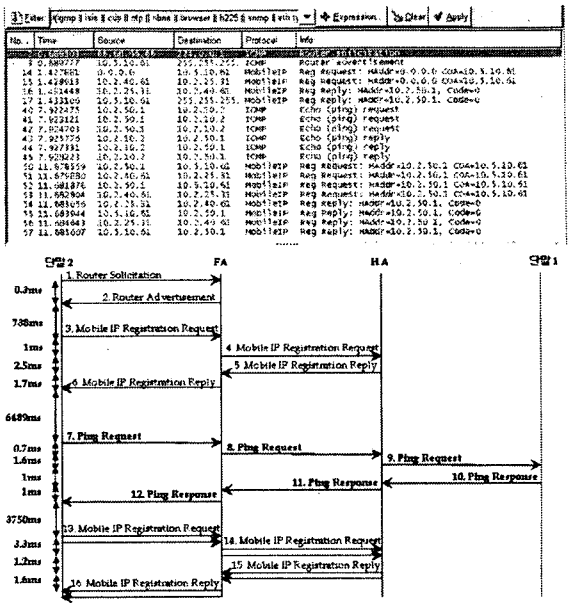

그림 4. 제안된 방법의 통신

Figure 4. the commuication of proposed solution

Mobile Visitor List
Total 1
HApool@no.aaa.dynamic:
Home addr 10.2.50.1
Interface FastEthernet0/0, MAC addr 000e.354a.23f0
IP src 0.0.0.0, dest 10.5.10.61, UDP src port 3723
HA addr 10.2.25.31, Identification C53469D9.6D420378
Lifetime 00:03:00 (180) Remaining 00:02:59
Tunnel0 src 10.5.10.61, dest 10.2.25.31, reverse-allowed
Routing Options - (T)Reverse Tunneling

그림 5. 제안된 실험에서 외부 에이전트(FA)의 방문자 리스트(visitor list)

Figure 5. the visitor list of Foreign Agent in previous communication

VI. 결론 및 평가

위 실험결과를 통해 기존의 네트워크 진입 여과(network ingress filtering)가 이동 노드에 적용되었을 경우 통신이 안 된다는 것을 확인하였고, 이 여과를 피하기 위한 방법인 역터널링이 직접 전달 형태의 경우 마찬가지로 통신이 안 되는 것을 확인할 수 있었다. 또한 캡슐화 전달 형태의 경우 네트워크 진입 여과를 적용하더라도 이동 노드의 IP 주소 변조를 이용한 서비스 거부 공격을 망에 부담을 주지 않고 해결하기 어렵다는 것을 알 수 있었다.

본 논문에서는 네트워크 진입 여과가 추구하는 IP 주소 변조를 이동 노드에 대해서도 망에 부담을 주지 않고 막기 위해, 이동 노드만이 외부 에이전트에 연결된다는 가정하에 그에 준하는 방법을 제시하고 이를 적용해 보았다. 제시하는 방법은 출구 인터페이스(egress interface)에 외부 에이전트 지역 주소(FA-CoA)를 출발지로 하는 패킷만이 통과하도록 접근 제어 리스트(Access Control List, ACL)를 설정하고, 또 외부 에이전트로 들어오는 패킷 중 출발지 주소로 외부 에이전트 지역 주소를 사용하는 패킷들을 버리도록 접근 제어 리스트를 설정하는 방법이다. 이 때 이동 노드는 직접 전달 형태의 역터널링을 사용하여 통신한다.

위와 같은 방법을 사용할 경우 이동 노드 등록에 성공한 이동 노드의 홈 주소를 출발지 주소로 하는 패킷만이 통신을 할 수 있기 때문에 등록되지 않은 사용자는 통신을 할 수 없으며, 네트워크 진입 여과가 추구하고자 했던 것 이상의 효과를 거둘 수 있다. 예를 들어 네트워크 진입 여과의 경우 같은 서브넷 안에서 출발지 주소를 변경하여 서비스 거부 공격을 하는 패킷들을 막을 수 없었다. 다만 이러한 정책은 이동 IPv4를 사용하지 않는 노드가 외부 에이전트를 게이트웨이로 하여 통신을 할 수 없다는 단점이 있으며, 또한 외부 에이전트는 이동 노드의 서비스 거부 공격 대상이 될 수 있다. 이것은 인터넷 서비스 공급자의 요구사항에 따라 다르나 망을 관리하는 입장에서 볼 때, 새로운 무선 통신망을 구축할 경우, 그리고 외부 에이전트가(FA) 관리하는 네트워크가 작을 경우 이러한 문제는 크게 부각되지 않을 것이다.

[참 고 문 헌]

[1] CERT Advisory CA-96.21; *TCP SYN Flooding and IP Spoofing Attacks*, September 24, 1996.

[2] W.R. Cheswick and S.M. Bellovin, "*Firewalls and Internet Security: Repelling the Wily Hacker*,"Addison-Wesley Publishing Company, 1994; ISBN 0-201-63357-4.

[3] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC2827, May 2000.

[4] C. Perkins, "IP Mobility Support for IPv4," RFC 3344, August 2002.

[5] G. Montenegro, "Reverse Tunneling for Mobile IP, revised," RFC 3024, January 2001.

국문 요약문

Mobile IPv4 네트워크에서 접속제어리스트와 역터널링을 이용한 IP Spoofing 제거 방안

Defeating IP Source Address Spoofing with Foreign Agent Care-of-Address in Mobile IPv4

김한림 (KT), 김성일 (KT), 김상언 (KT), 박세준 (KT)

고정된 호스트의 출발지 주소 변조(IP Source Address Spoofing)를 막는 가장 단순하면서도 효과적인 해결방법으로 네트워크 진입여과(Network Ingress Filtering)가 있다. 이동(Mobile) IPv4 네트워크에서는 이러한 네트워크 진입 여과가 설정될 경우 이동 호스트의 통신이 불가능해지기 때문에 이를 피하기 위한 방법으로 역터널링(Reverse Tunneling)이 고안되었지만 이에 따라 이동 호스트의 출발지 주소 변조를 통한 서비스 공격을 막을 수가 없게 되었다. 본 논문에서는 이동 IPv4 네트워크에서 외부 에이전트에 이동 호스트들만이 연결되고 각각의 외부 에이전트(Foreign Agent)가 관리하는 네트워크가 작다는 가정하에, 이동 호스트의 출발지 주소 변조를 효과적으로 막는 방법에 대해 제안하고자 한다.