선택적 역 터널링시 외부 에이전트에서의 패킷 필터링

최도민*, 전문석
숭실대학교 컴퓨터학과

A scheme for Foreign Agent's Packet Filtering in Selective Reverse Tunneling

Domin Choi*, Moonsuk Jun
Dept. of Computing, Soongsil University

요 약

Mobile IP 기술에 의해 시간 및 장소의 제한을 받지 않고 사용자가 원격지 또는 이동 중에도 정보를 처리할 수 있는 환경이 제공된다. 패킷 필터링 기술 같은 경우에는 패킷의 출발지, 목적지 주소뿐만이 아니라 패킷의 이동 방향도 고려하므로 Mobile IP의 동작이 방해를 받게 될 수가 있다. 이러한 문제점을 해결하기 위해 나온 것이 역 터널링 기법인데 이 경우는 효율성이 떨어지므로 상황에 따라 역 터널링을 수행하는 선택적 역 터널링 기법이 나오게 되었다. 효율성을 증진시킨 선택적 역 터널링 기법은 외부 네트워크의 보안 정책에 위배되는 패킷 전송이 이루어질 수 도 있으므로 새로운 보안 정책이 절실히 요구된다. 본 논문에서는 선택적 역 터널링시 외부 에이전트가 패킷 필터링 기능을 갖는 기법에 대해 제안한다. 이 기법을 적용함으로써 이동노드가 선택적 역 터널링시 외부 네트워크의 보안 정책에 부합되게 행동할 수 있도록 하였다.

1. 개 요

휴대용 컴퓨터가 대중화되고 이동전화, 무선 LAN과 같은 이동 통신 기술이 보편화됨으로써 휴대용 컴퓨터를 이용하여 시간 및 장소의 제한을 탈피한 네트워크의 접속이 가능하게 되었다. 그러나 기존의 인터넷상에서는 접속점이 바뀔 때마다 자신의 IP address를 변경시켜야만 하므로 인터넷상에서 자신의 link-layer 접속 지점을 변경한 후에도 IP address를 변경하지 않고 다른 node들과 통신을 가능하게 하는 기술이 필요하게 되었다. 이러한 문제를 해결하기 위해 IETF(Internet Engineering Task Force)에서 Mobile IP 기술을 제안하였다[1][2].

최근에 제안된 경계 라우터의 스펙을 살펴보면 하나의 물리적인 관리 도메인 내의 경계 라우터는 외부에서 발생시킨 것으로 보이는 내부 도메인의 주소를 갖는 데이터그램은 버리도록 권고되고 있다. 이러한 기능을 진입 필터링(Ingress Filtering)이라 한다.

진입 필터링에 의해 Mobile IP의 동작이 방해를 받게 될 수가 있는데 이 것을 해결하기 위한 방법이 역 터널링(Reverse Tunneling) 기법이다. 하지만 이 역 터널링 기법의 경우에는 삼각 라우팅(Triangular Routing)이 아닌 사각 라우팅(Quadrilateral Routing)을 수행하므로 홈 네트워크를 거쳐 통신을 하게된다. 이 때문에 효율이 많이 감소하게 된다. 선택적인 역 터널링 기법을 사용하면 효율성을 높일 수는 있지만 외부 네트워크의 노드와 통신시 패킷 필터링 규칙에 위배되는 패킷 전송을 허용할 수 있는 문제점이 있다.

본 논문에서는 외부 에이전트에 패킷 필터링 기능을 추가함으로서 선택적 역 터널링시 패킷 필터링 규칙에 위배되는 패킷 전송을 막을 수 있는 기법을 제시한다. 본 논문의 구성은 2장에서 패킷 필터링, Mobile IP, 그리고 역 터널링에 관한 연구를 간단히 설명하고, 3장에서 선택적 역 터널링 시의 문제점 및 문제점 해결을 위해 제시한 기법을 설명한다. 마지막으로 4장에서는 결론 및 향후 관련연구에 대해 서술한다.

2. 관련 연구

2.1. 패킷 필터링(Packet Filtering)

패킷 필터링은 어떤 데이터가 네트웍으로부터 흘러나가거나 들어오는 것을 통제하는 식으로 작동하는 네트웍 보안 메카니즘이다[4].

패킷 필터링은 다음과 같은 내용에 근거해서 데이터 전송을 통제(허용 혹은 거부) 할 수 있게 해준다.

- 데이터가 출발한 주소
- 데이터가 향하는 주소
- 데이터를 전송하기 위해 사용 중인 세션과 어플리케이션 프로토콜

2.2. Mobile IP

만약 한 노드가 IP 주소의 변화 없이 인터넷상에서 이동하게 되면 그 노드로 정확하게 라우팅 되는 것이 가능하지 않다. 이러한 문제를

극복하기 위해서 Mobile IP가 소개되었다. Mobile IP에는 기본적으로 세 가지 구성요소가 있다. 이 세 가지 구성요소는 이동 노드(Mobile Node, MN), 홈 에이전트(Home Agent, HA), 그리고 외부 에이전트(Foreign Agent, FA)이다.

이동 노드는 홈 네트워크(Home Network)라 불리는 하나의 네트워크를 가진다. 홈 에이전트의 일은 홈 에이전트에 있는 모든 이동 노드에 관한 현재 위치 테이블을 가지고 그 이동 노드들의 현재 위치로 데이터 그램을 전달한다. 이동 노드로 전해진 모든 데이터그램은 홈 에이전트에 의해서 가로채어진 뒤 외부 에이전트로 보내고 이 외부 에이전트에 의해서 이동 노드로 데이터가 전달된다[1][2].

2.3. 역 터널링(Reverse Tunneling)

보안정책에 의해서 경계 라우터의 경우에 내부의 IP인 출발지 주소를 가진 패킷이 외부로부터 들어올 경우에는 버리도록 되어있다. 목적지 노드(Correspondent Node, CN)가 이동 노드의 홈 네트워크와 같을 경우 이동 노드가 목적지 노드로 전송하려는 패킷은 경계 라우터에 의해 접근이 거부된다. 이 문제점을 해결하기 위해 나온 것이 역 터널링이다[3].

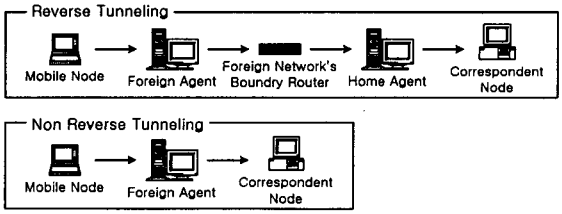
역 터널링시 이동 노드에서 외부 에이전트로 데이터를 전송하는 방법이 두 가지가 있다.

첫째, Direct Delivery Style - 이 경우에는 데이터를 받은 외부 에이전트에서 encapsulate를 한 다음 홈 에이전트로 전송하게 된다.

둘째, Encapsulating Delivery Style - 이 경우에는 데이터를 받은 외부 에이전트는 우선 받은 패킷을 decapsulate하여 내부의 패킷으로 복구한 뒤 그 패킷을 re-encapsulate 하여 홈 에이전트로 전송하게 된다.

2.3.1. 선택적 역 터널링(Selective Reverse Tunneling)

만약 목적지가 외부 네트워크에 속해 있는 경우에는 진입 필터링의 영향을 받지 않으므로 역 터널링을 하지 않아도 된다. 이 경우에는 역 터널링을 사용하지 않음으로 해서 [그림 1]에서 보여지는 것과 같이 좀더 효율적인 경로를 사용할 수 있다.



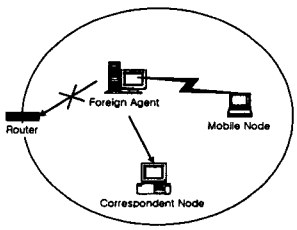
[그림 1] Reverse Tunneling vs Non Reverse Tunneling

선택적 역 터널링을 사용하기 위해서는 이동 노드에서 외부 에이전트로 데이터 전송 시 역 터널링의 사용 유무에 따라서 다른 방법의 데이터 전송을 사용하여야 한다. 역 터널링을 사용하지 않는 패킷의 경우에는 Direct Delivery Style을 사용하여 패킷을 전송을 하고 만약 역 터널링을 사용하는 패킷의 경우에는 Encapsulating Delivery Style을 사용하여 패킷을 전송하여야 한다. 선택적 역 터널링 에서 Direct Delivery Style의 패킷을 받은 외부 에이전트는 기본적인 역 터널링과 다른 처리 방법을 가진다. Direct Delivery Style의 경우 외부 에이전트는 받은 패킷을 encapsulate 한 뒤 홈 에이전트로 전송을 하는 것이 아니라 일반 패킷으로 생각을 하고 표준 IP 라우팅을 통해 패킷을 전달한다[3].

3. 외부 에이전트에서의 동적 패킷 필터링

3.1. 외부 에이전트에서의 패킷 필터링의 필요성

기존의 삼각 라우팅을 이용할 경우에는 진입 필터링에 의해 홈 네트워크에 있는 노드와 통신을 할 수 없는 경우가 발생하게 된다. 이 점을 해결하기 위해 사각 라우팅을 사용하는 역 터널링 기법이 나오게 되었다. 하지만 역 터널링 기법은 사각 라우팅을 사용함으로 해서 효율성이 많이 떨어진다는 단점이 있다. 선택적인 역 터널링 기법을 사용할 경우 홈 네트워크의 노드와 통신을 하고자 할 경우에는 역 터널링을 사용함으로써 진입 필터링의 영향을 받지 않는 상태에서 통신을 할 수 있고 홈 네트워크가 아닌 경우에는 삼각 라우팅을 사용함으로서 효율성을 높일 수 있다. 하지만 선택적 역 터널링의 경우 보안상의 문제는 있다. 만약 [그림 2]와 같이 통신을 하고자 하는 노드가 외부 네트워크에 속해 있을 경우 스크리닝 라우터(Screening Router) 또는 패킷 필터링 서버에 설정된 필터링 규칙이 적용되지 않으므로 원하지 않는 접근이 이루어 질 수 있다는 것이다. 이러한 접근을 막기 위해서 항상 역 터널링을 하게 하는 것은 효율성이 떨어짐을 2.3절에서 이미 설명한 바 있다. 본 논문에서는 선택적 역 터널링시 외부 에이전트에 패킷 필터링 기능을 넣음으로써 이와 같은 문제점을 해결 하고자 한다.



[그림 2] 필터링 규칙이 적용되지 않는 경우

3.2. 외부 에이전트에서의 패킷 필터링

3.2.1. 제약 사항

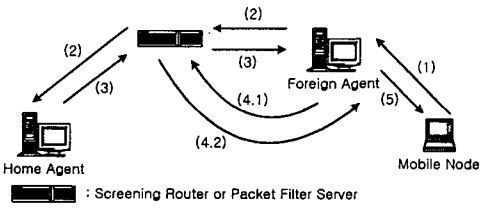
본 논문에서 제안하는 시스템은 다음과 같은 제약 사항을 갖는다.

- 터널링되어가는 패킷은 방화벽을 거쳐서 지나가지 않는다.
- 방화벽을 거쳐서 지나갈 경우에는 인증이나 암호화 같은 특정 목적을 위한 헤더가 필요시 추가 될 수도 있다.
- 이동 노드가 패킷을 전송하거나 받을 시에는 외부 에이전트를 반드시 거친다.
- 이동 노드는 Direct Delivery Style 과 Encapsulating delivery Style의 전송법이 모두 가능해야 한다.

· 외부 에이전트는 Encapsulation 기능이 있어야 한다.

3.2.2. 동작 과정

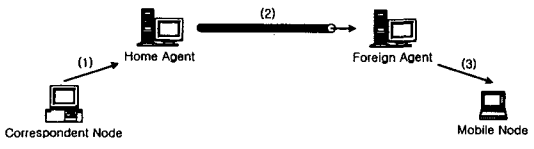
2.3.1에서 설명한 선택적 역 터널링을 사용하게되면 [그림 2]에서 보이는 바와 같이 패킷 필터링 룰에 적용되지 않는 경우가 있으므로 외부 에이전트에서 패킷 필터링을 적용함으로 문제를 해결하려한다. 본 논문에서 제안하는 선택적 역 터널링시의 외부 에이전트에서의 패킷 필터링 기법의 동작 과정은 다음과 같다.



[그림 3] 등록 절차

1) 등록 절차

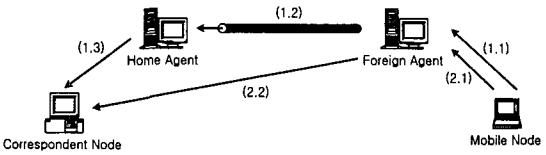
1. 외부 네트워크로 이동한 이동 노드는 Mobile Agent Advertisement 메시지를 듣고 외부 에이전트의 COA를 획득한 후 외부 에이전트에게 Registration Request 메시지를 보낸다.
2. Registration Requesta 메시지를 받은 외부 에이전트는 Request 메시지를 확인한 후 홈 에이전트에게 전송한다.
3. 외부 에이전트로부터 Registration Request 메시지를 받은 홈 에이전트는 Request 메시지를 확인한 후 외부 에이전트에게 Registration Reply 메시지를 보낸다.
4. 홈 에이전트로부터 Registration Reply 메시지를 받은 외부 에이전트는 메시지를 확인한 후 허용 메시지일 경우에는 방문자 리스트를(Visitor List) 갱신한다. 전송 받은 Registration Reply 메시지를 이동 노드에게 전송한다. 패킷 필터링 규칙 설정의 자동화가 가능할 경우에는 4.1에서 4.2의 과정을 추가로 수행한다.
   4.1 패킷 필터링 규칙 설정을 위해 스크리닝 라우터나 패킷 필터링 서버에게 이동 노드의 주소가 속해 있는 패킷 필터링 규칙의 전송을 요구한다.
   4.2 전송 받은 이동 노드에 대한 패킷 필터링 규칙을 저장한다.(자동의 경우 이동 노드별로 독립적인 패킷 필터링 규칙이 있다.)
5. 외부 에이전트로부터 Registration Reply 메시지를 받은 이동 노드는 메시지를 확인한다.



[그림 4] 상대 노드로부터 이동노드로의 패킷 전송 절차

2) 상대 노드로부터 이동 노드로의 패킷 전송

1. 이동 노드로 전송될 패킷은 표준 IP 라우팅을 통해 홈 에이전트에 전달된다.
2. 홈 에이전트는 패킷을 가로채서, COA로 터널링한다.
3. 외부 에이전트로 터널링된 패킷은 외부 에이전트에 의해 디터널링되어 이동 노드로 전달된다.



[그림 5] 이동 노드로부터 상대노드로의 패킷 전송 절차

3) 이동 노드로부터 상대 노드로의 패킷 전송

1. 역 터널링이 적용 되어야하는 패킷의 경우
   1.1 이동 노드는 패킷을 Encapsulating Delivery Style로 외부 에이전트에 전송한다.
   1.2 Encapsulation 된 패킷을 받은 외부 에이전트는 받은 패킷을 Decapsulate하여 내부의 패킷을 복구한 뒤 이 패킷을 Re-encapsulate하여 홈 에이전트로 전송하게 된다.
   1.3 홈 에이전트로 터널링 된 패킷은 홈 에이전트에 의해 디터널링되어 상대 노드로 전달된다.
2. 역 터널링이 적용되지 않는 패킷의 경우
   2.1 이동 노드는 패킷을 Direct Delivery Style로 외부 에이전트에 전송한다.
   2.2 Direct Delivery Style의 패킷을 받은 외부 에이전트는 이동 노드에 대해 설정된 패킷 필터링 규칙을 참조하여 허용되지 않은 패킷의 경우에는 전송을 금지하고 전송이 허용된 패킷의 경우에는 상대 노드로 표준 IP 라우팅을 통해 전달한다.

4. 결론 및 향후 연구과제

역 터널링을 하지 않을 경우 외부 네트워크의 노드와 통신시 필터링 규칙이 적용되지 않는 경우가 발생할 수 있다. 본 논문에서는 외부 에이전트에 패킷 필터링 기능을 추가함으로써 이 문제를 해결하였다.

외부 네트워크나 홈 네트워크에 스크리닝 라우터나 패킷 필터링 서버가 설치되어 있을 경우 터널링된 패킷이 통과되지 못하는 경우가 생길 수 있으므로 이동 노드 등록시 패킷 필터링 규칙을 자동으로 설정하는 기법이 향후 연구 되어야 한다.

5. 참고문헌

[1] Charles E. Perkins, "IP Mobility Support," RFC 2002, Oct 1996.

[2] Charles E. Perkins, "Mobile IP Design Principles and Practices," Addison Wesley, 1998.

[3] Gabriel E. montenegro, "Reverse Tunneling for Mobile IP," RFC 2344, May. 1998.

[4] D. Brent Chapman and Elizabeth D. Zwicky, "Building Internet Firewall," O'Reilly, 1995.