# 이동 인터넷 프로토콜을 위한 개선된 SKIP Firewall Traversal

김민경[0] 한규호 채동현 마영식 안순신
고려대학교 전자공학과
(damaged[0], garget, hsunhwa, mys, sunshin)@dsys.korea.ac.kr

# Enhancement of SKIP Firewall Traversal for Mobile IP

Min-Gyung Kim[0] Kyu-Ho Han Dong-Hyun Chae Young-Sik Ma
Sun-Shin An
Department of Electronics, Korea University

요 약

최근들어 security가 데이터 통신의 중요한 이슈로 떠오르고 여러 기관들의 망에 Firewall을 설치하여 보호하는 것은 점점 더 일반화 되고있다. Sun의 SKIP Firewall Traversal 방법은 Mobile IP가 Firewall이 설치된 환경에서도 제대로 동작할 수 있도록 고안된 것이다. 그러나 이 방법은 실제 적용에 있어 몇몇 문제점이 발견된다. 본 논문에서는 이 문제점들을 살펴보고 그것을 해결하는 방안을 제시하고자 한다.

## 1. 서 론

Mobile IP[1]는 IP에 이동성을 주기 위해 고안된 프로토콜으로, 사용자가 connection의 끊어짐이 없이 접속점을 바꿀 수 있도록 해준다. 하지만 이런 잇점과 함께 Mobile IP는 네트워크상에 새로운 보안 문제를 야기시킨다.

가령 홈 네트워크가 firewall(FW)로 보호받는 이동 인터넷 환경을 고려해보자. 만약 이동노드가 홈 네트워크에 있다면, FW의 보호를 받게 된다. 마찬가지로 외부망에 있을 때도 이동노드는 보호를 받아야만 한다. 즉, 외부망에 접속한 이동노드와 홈 네트워크의 노드들간에 안전한 데이터 전송 메커니즘이 필요하게 된다.

Sun's SKIP firewall traversal for Mobile IP[4]는 이런 환경에서 Mobile IP가 적절하게 동작할 수 있도록 제안된 방법이다. 하지만 이 방법은 MN측에 몇가지 문제점을 가진다. 본 논문에서는 SKIP Firewall Traversal방법이 가지는 문제점에 대해서 살펴보고, 이에 대한 해결책을 제시하는 것을 목적으로 한다.

## 2. 관련 연구

### 2.1. Sun's SKIP Firewall Traversal for Mobile IP방법의 개요

FW로 보호받는 홈네트워크에 Mobile Node(MN)가 있다고 하면, MN은 홈 네트워크에 접속해 있는 때와 마찬가지로 외부망에서도 FW의 보호를 받아야만 한다. 그리고, MN이 외부망에 접속해 있을때 내부망의 노드와 통신할때는 FW이 그 패킷들을 내부망으로 포워딩 해주어야 한다. Sun's SKIP Firewall Traversal에서는 FW와 MN사이에 SKIP을 이용한 secure tunnel을 형성해서 이런 기능을 제공한다.

secure tunnel의 양단의 FW의 public address와 MN의 CoA로 정의 된다. 이때 MN의 CoA는 collocated CoA이어야 한다. SKIP은 통신하는 두 노드의 Diffie-Hellman(DH) public value와 DH private value을 이용해서 DH shared secret value를 생성하고, 그것을 이용해서 비밀키인 Kp를 암호화한다. Kp는 패킷을 암호화하고, 패킷을 위한 인증 코드(MAC)를 생성시켜 패킷을 보호하는데 사용되어 두 노드사이에 secure tunnel을 형성시킨다.

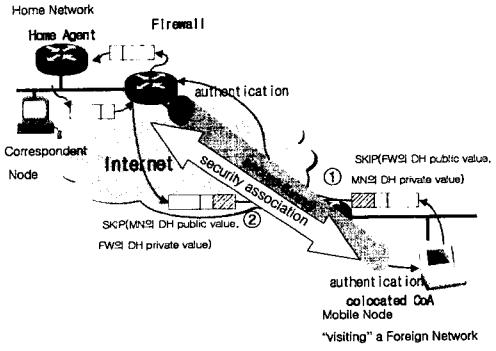


**그림 1 Sun's SKIP Firewall Traversal**

SKIP을 사용하면, MN이 등록을 위해서 registration request 메시지를 보낼 때 MN과 FW사이에 security association이 맺어진다. registration request 메시지는 MN과 FW사이의 shared secret value를 이용 해서 SKIP으로 보호되어 FW로

전달된다. FW은 그 메시지를 받으면, 메시지에 대해서 인증과정을 거친 후에 패킷이 올바른 것으로 판단되면, registration request 메시지를 다시 복구시켜서 Home Agent(HA)로 전달한다.

Registration Request를 받은 HA는 그에 대한 응답으로 Registration Reply메시지를 보낸다. HA가 Registration Request이 거쳐온 FW로 메시지를 보내면, FW은 MN에 registration reply메시지를 SKIP으로 보호해서 보낸다. MN은 메시지에 대해서 인증과정을 거친후, 원래의 메시지로 복구시켜서 처리한다.

홈 네트워크의 Correspondent Node(CN)가 MN사이에 데이터를 교환 할때도 마찬가지의 절차를 거치게 된다. 먼저 노드가 MN으로 보낸 패킷이 HA에서 가로채어져서 FW로 전해지고, MN과의 security association을 통해서 패킷이 SKIP으로 보호되어 전달된다. 이동 노드에서 CN으로 전해질때도, SKIP으로 보호되어 FW로 전달된후, 인증과정을 거쳐서 CN으로 전해진다.

### 3. 기존 SKIP Firewall Traversal방법의 문제점

MN은 홈 네트워크와 통신할 때 FW와 security association을 생성하고, FW를 통해서 통신에 필요한 패킷을 주고 받게 된다. 그러므로, MN은 FW에 대한 정보를 사전에 가지고 있어야 한다.

만약 MN이 하나의 FW에 대한 정보만 가지고 그것을 통해서만 통신한다면, 망상태의 변화나 FW자체의 문제 때문에 그 FW와 통신을 할 수 없는 때에는 Mobile IP를 이용하는 IP통신은 불가능해진다. 그러므로 MN이 인터넷 환경의 변화에 보다 적절하게 대처하기 위해서 MN은 하나이상의 FW에 대한 정보를 가지고, 환경변화에 맞추어서 그들 중 적합한 하나를 선택해야 할 것이다.

그러나, MN의 입장에서 통신에 가장 적합한 FW를 선택하는 것은 쉽지 않은 일이다. 통신 노드로써의 MN은 망과 FW의 상태에 대한 정보가 부족하기 때문에 자신이 선택할 FW가 통신에 최적인 것인지 알기도 어려울뿐더러, 안다고 하더라도 그 비용이 상당할 것이기 때문이다.

게다가 MN이 홈네트워크의 상태에 맞는 FW들에 대한 정보를 관리하는 것도 어려운 일이다. FW에 대한 정보가 MN에서 정적인 상태로 보유·관리한다면 홈네트워크 상에서 FW의 숫자나, 위치 등이 바뀔 때마다 MN의 정보도 수정되어야 할 것이다. MN이나 FW의 숫자가 작다면 큰 어려움이 없겠지만, 그 숫자가 커질수록 FW의 정보가 유효하게 유지하는 데에는 어려움이 따르게 된다. 더욱이 MN이 외부망에 접속해 있는 상태에서 홈네트워크의 FW에 대한 정보가 변한다면 문제는 더욱 커지게 될 것이다.

### 4. 망과의 Security Association 도입을 통한 SKIP Firewall Traversal방법의 개선

앞절에서 언급된 문제점은 MN이 FW와 Security Association을 생성하기 위해서 FW를 선택하기 때문에 발생한다. 만약 홈네트워크에 key를 할당하고, MN이 홈네트워크와 Security Association을 생성해서 통신할 수 있도록 한다면, MN은 FW를 선택할 필요가 없지게 된다.

Security association은 SPI, destination address, security protocol identifier에 의해서 정의된다. Security assocation에서 destination address는 기본적으로 unicast주소이다. 네트워크와의 security association이라는 개념을 도입하기 위하여 destination address에 망을 나타내는 IP주소가 사용되는 것을 허락한다. 단 그 망은 FW들로 보호받는 망이어야 한다.

망을 나타내는 주소가 security association을 위한 destination address로 사용되면 적절하게 선택된 경로에 의해서 그 망을 보호하는 FW가 선택되고, 그 FW과 망의 key 값을 사용하여 security association이 생성된다. 따라서 SKIP을 지원하는 망의 FW들은 그 자신의 DH value와 망의 DH value 두가지를 가지게 된다. 망에 대해서 생성된 security association은 망의 FW중 하나를 선택하여 망의 key를 사용해서 만들어진 가상의 security association이라 할 수 있을 것이다.

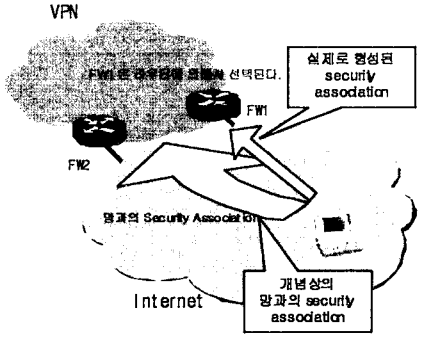


그림 2 망과의 Security Association

#### 4.1 동작 과정

MN이 홈 네트워크에 접속해 있다면, 일반적인 IP에 따라서 통신이 이루어진다. 만약 MN이 외부망에 접속하면 colocated CoA를 얻고, 얻은 CoA를 HA에 등록하기 위해서 Registration Request 메시지를 HA로 전송한다.

##### 4.1.1 Registration Request 메시지의 전송

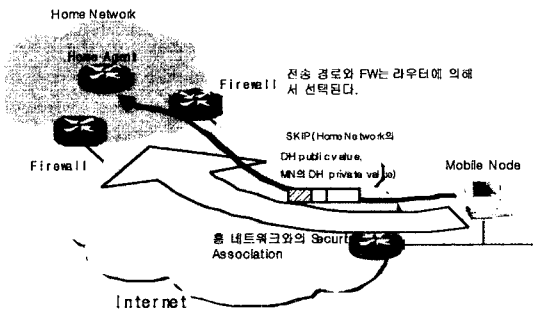


그림 3 Registration Request Message의 전송

그림 3은 Registration Request 메시지의 전송을 나타낸 것

이다.

외부망에서 전송되는 Registration Request메시지는 SKIP으로 보호되어야 한다. 먼저 MN은 홈 네트워크의 DH public value와 MN의 private value로부터 생성된 shared secret key를 이용하여 패캣 단위의 encryption에 사용할 key인 Kp를 암호화하여 SKIP 헤더에 저장한다. 그런후, SKIP 헤더의 source NSID와 destination NSID를 각각 MN의 주소와 홈네트워크의 주소로 설정하고, Registration Reqeust 메시지를 페이로드에 실어서 암호화하여 HA의 주소로 전송한다.

이 메시지는 중간 라우터들에 의해서 선택된 경로를 따라 홈네트워크의 FW들중 하나에 도착하게 된다. FW는 홈네트워크의 DH private value와 MN의 DH public value를 이용하여 인증을 하고, 올바르면 encapsulation된 Registration Request메시지를 복구하여 HA로 포워딩하게 된다.

| IP Header (SKIP) | SKIP Header | AH | ESP | Inner IP Header | Reg. Req. |
|---|---|---|---|---|---|

IP Header(SKIP)
Source : MN's CoA
Dest. : HA's Address
SKIP Hdr
Source : NSID = 1
MKID = MN's Address
Dest. : NSID = 1
MKID = Home Network's Address
Inner IP Hdr
Source : MN's Source Address
Dest. : HA's Address

그림 4 MN에서 FW로 가는
Registration Request 메시지의 구조

4.1.2 Registration Reply 메시지의 전송

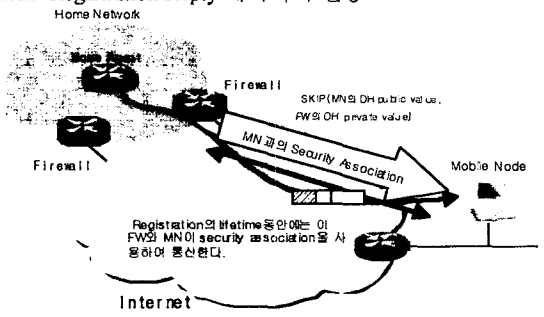


그림 5 Registration Reply의 전송

Registration Request 메시지를 받은 HA는 메시지를 분석하여 Registration의 가능여부를 결정한 후, Registration Reply 메시지를 Registration Request를 전해준 FW로 전송한다. 이 메시지를 받은 FW는 자신의 DH private value와 MN의 public value를 사용하여 security association을 형성하여 메시지를 암호화하고 전송한다. 메시지를 받은 MN은 Registration이 이루어졌는지를 판단하고, 성공했다면 Registration의 lifetime동안은 Registration Reply가 전해져온 FW와 서로 통신하여 패킷을 주고 받게 된다.

| IP Header (SKIP) | SKIP Header | AH | ESP | Inner IP Header | Reg. Reply |
|---|---|---|---|---|---|

IP Header(SKIP)
Source : FW's public address
Dest. : MN's CoA
SKIP Hdr
Source : NSID = 0
MKID = none
Dest. : NSID = 1
MKID = MN's Address
Inner IP Hdr
Source : HA's Address
Dest. : MN's CoA

그림 6 FW에서 MN으로 전송되는
Registration Reply 메시지의 구조

4.1.3 데이터의 전송

MN이 CN과 통신을 할 때에는 기존의 SKIP Firewall Traversal 방법을 따른다. 이 때, 사용되는 FW는 Registration 과정에서 선택되어진 FW을 이용하게 된다. 이 FW와의 통신은 Registration lifetime동안 유지되며, lifetime이 지나면 새로운 registration을 거치면서 FW가 다시 선택된다. 만약 MN의 통신 도중에 FW의 failure등으로 FW와 통신할 수 없다면, 새로운 Registration 과정을 거쳐서 FW를 다시 선택하게 된다.

## 5. 결론 및 향후 연구 과제

본 논문에서는 SKIP Firewall Traversal방법에서 발생할 수 있는 문제점을 알아보고, 그에 대한 해결책으로 홈 네트워크와의 security association 개념을 도입하였다. 그럼으로써 기존의 방법의 문제점을 해결하고 성능이나 확장성 측면에서도 장점을 가지게 된다.

FW간에 key를 공유함으로써 생길 수 있는 보안 문제점은 홈네트워크의 key사용을 Registration Request로 한정하고, key의 변경 주기를 좀더 짧게 함으로써 적절한 수준에서 해결가능하다. 하지만, 홈 네트워크에 key를 할당하고, 그 key를 안전하게 분배하는 방법은 좀더 깊은 연구가 필요할 것이다.

## 6. 참고 문헌

[1] Perkins. C, "IP Mobility Support", RFC 2002, October, 1996

[2] Perkins. C, "IP Encapsulation within IP", RFC 2003, Octorber, 1996

[3] Solomon J., "Mobile IP", Prentice Hall, 1998

[4] G. Montenegro, V. Gupta, "Sun's SKIP Firewall Traversal for Mobile IP", June, 1998

[5] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", November, 1998