IPv6 전환 과정의 보안위협 분석 및 대응방안

김상수* 조기환**
전북대학교 *전자정보공학부, **컴퓨터공학부
e-mail : *kimsangsoo0@gmail.com, **ghcho@jbnu.ac.kr

An Analysis on Security Attacks and Their Response Methods on Transferring into IPv6

Sang-Soo Kim*, Gi-Hwan Cho**
*Div. of Electronics and Information Engineering, Chonbuk National University
**Div. of Computer Science and Engineering, Chonbuk National University

요 약

현재 IPv4 에서 IPv6 로의 전환은 매우 시급한 상태이다. 하지만 IPv6 로의 전환에 앞서 IPv4 에서 제기되었던 많은 보안 문제점이 IPv6 로의 전환에 걸림돌이 되고 있다. 차세대 인터넷 구축에 반드시 필요한 IPv6 로의 변환 과정에 있어, 기존의 IPv4 와 IPv6 의 서로 다른 방식으로 인한 이질성으로 예상치 못한 보안상 문제점들이 드러나고 있다. 본 논문에서는 IPv4 에서 IPv6 로 전환 시 발생할 수 있는 보안상 위협에 대해서 분석한다. 또한 터널링 방법에서의 패킷 헤더 변조 공격을 방지하기 위해 패킷 무결성 검증에 의한 패킷 필터링 방법과 IPv4 주소 할당 방법에 있어 주소 할당 서버의 IP pool 주소 고갈 공격 문제를 해결하기 위한 방안을 제시 하였다.

1. 서론

오늘날 인터넷의 급격한 성장으로 인하여 IPv4 주소 고갈 문제가 대두 되었다. IPv4 는 약 43 억개의 한정된 주소와 보안기능의 고려 없이 설계 되어 많은 문제점을 야기 시켜 왔다. 그에 대한 해결을 위한 차세대 인터넷 프로토콜인 IPv6 가 등장하였다[1].

현재 인터넷 주소체계인 IPv4 의 주소 고갈을 목전에 두고 있는 상황에서 IPv6 주소체계의 도입을 미루는 이유는 전세계적으로 복잡하고 광범위 하게 퍼져 있는 IPv4 주소체계를 바꾸는 것은 거의 불가능 하며 많은 혼란을 야기할 수 있기 때문이다. 또한 IPv4 주소체계와의 변환 및 연동이 완벽히 지원되지 않았고 IPv6 네트워크 환경의 효율적인 보안관리를 위한 보안 요구사항 연구가 제대로 되지 않았기 때문이다[2]. 또한 4~5 년 간은 IPv4 주소와 IPv6 의 주소가 공존할 것이라 예상하기 때문에 서로 다른 프로토콜의 주소를 혼합하여 사용하는 기술이 필요하다. IPv4/IPv6 변환 과정 중 IPv6 패킷을 IPv4 헤더로 캡슐화 하여 전송하는 DoS 공격이 가능하고, IPv6 노드가 IPv4 노드와 통신을 지원하기 위해 IPv4 의 주소를 할당 해주는 IPv4 서버의 주소 고갈 공격이 존재한다. 따라서 IPv4/IPv6 두 프로토콜의 공존에 있어 위 문제점에 관한 연구가 이루어지고 대응방안이 제시되어야 한다.

본 논문에서는 IPv6 와 IPv4 변환간 사용되는 전환기술에 대해 기술하고 전환기술간 발생할 수 있는 보안상 위험요소인 터널링 방법에서 분산 반사 서비스 거부 공격 (DRDoS : Distributed Reflective DoS) 과 IPv4 주소할당 서버의 주소 고갈공격에 대해 분석한다. 터널링 방법에서 패킷 필터링을 위한 패킷 무결성 검증과 주소할당 서버의 신뢰성 있는 주소할당 방법을 제안하고 마지막으로 결론과 향후 연구과제에 대하여 기술 한다

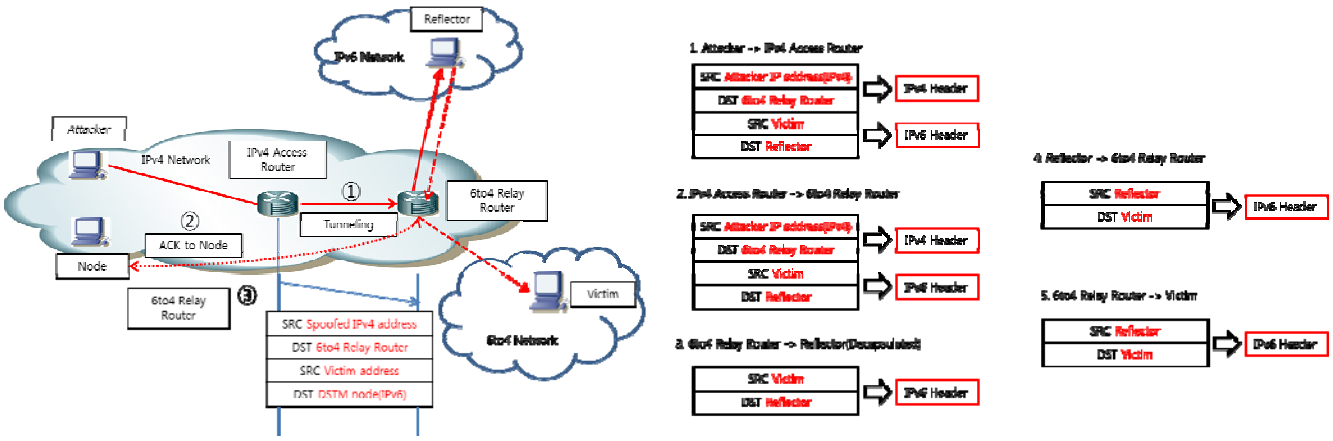
2. IPv6 전환 기술

IPv4/IPv6 전환 기술은 듀얼스택(Dual stack), 터널링 (Tunneling), 변환(Translation) 방법으로 나누어진다.

듀얼스택 방법은 하나의 시스템(호스트 또는 라우터)에서 IPv4 와 IPv6 를 동시에 처리하는 기술이다. 따라서 듀얼스택을 지원하는 시스템은 물리적으로 하나의 시스템이지만 논리적으로 IPv4 와 IPv6 를 지원 하는 두 개의 시스템이 있는 것처럼 볼 수 있다. 이는 IPv6 노드가 IPv4 노드와 호환성을 유지하는 가장 쉬운 방법이다[3].

터널링 방법은 기존 IPv4 망을 전달 망으로 사용해 서로 떨어져 있는 각각의 IPv6 망을 연결 시켜 주는 기술이다. 이러한 방법은 크게 설정 터널링(Configured Tunneling)방법과 자동 터널링(Automatic Tunneling)방법으로 구분된다[4][5]. 설정 터널링은 6Bone 에서 주로 사용되며 IPv4 네트워크를 경유하여 IPv6 네트워크간 통신할 경우 종단 라우터에 터널을 사전에 수동으로 설정하여 사용하는 방식이다. 반면 자동 터널링은 실제 통신이 사용될 때 자동으로 종단간 터널을 설정하는 방식이다.

IPv4/IPv6 변환 방법은 일반적으로 게이트웨이 상에서 계층에 따른 변환을 수행 하는 기법으로서 헤더 변환, 주소 매핑, 프로토콜 변환과 같은 동작을 수행한다. 이러한 변환 방법으로는 DSTM(Dual Stack Transition Mechanism)[6], NAT-PT(Network Address Translation – Protocol Translation)[7], SIIT(Sirindhorn International Institute of Technology)[8], BIS



(그림 1) Relay Router 를 이용한 DRDoS attack

(Bump in the Stack)[9], BIA(Bump in the API)[10] 방법들이 있다. IPv4/IPv6 변환 방법에 있어서 IPv6 주소 체계를 가진 노드는 IPv4 주소 체계를 가진 노드에게 패킷을 전송하기 위하여 IPv4 주소할당 서버에 주소를 할당 받아 사용한다.

3. IPv6 보안위협 분석

3.1 터널링 방법의 보안위협 분석

IPv4 망과 IPv6 망이 공존하며 이 둘의 복잡도가 증가 할수록 IPv4/IPv6 연동에 있어 많은 보안 문제가 발생한다. IPv4/IPv6 터널링 연동 방법은 여러 가지 형태의 IP-in-IP 터널링 방법을 이용하여 사용된다. 서로 다른 두 프로토콜의 검사 작업이 실행되지 못하는 환경 에서 적절한 보안 정책을 수립할 수 없다. 이로 인하여 IPv4/IPv6 터널링 연동 환경에서 다음과 같은 문제점이 발생할 수 있다. 수동 설정된 터널링에서 IPsec 을 이용하는 방법은 제안 되었으나 자동 터널링 기법은 터널 종단 포인트에 사전 연계가 없기 때문에 IPsec 을 사용할 수 없다.

특히 6to4 라우터를 사용하는 방법은 ingress 필터링을 적용한다 해도 IPv4 네트워크에 위치한 공격자가 IPv6 헤더부분을 조작하여 IPv4 헤더로 캡슐화 후 IPv6 네트워크로 전송할 경우 주소 스푸핑을 이용한 서비스 거부 공격(Dos), 또는 DRDoS 등의 공격이 발생할 수 있다. (그림 1)은 6to4 전환 방법에서 자동 터널링을 이용한 DRDoS 공격을 나타내었고, 시나리오에 대한 패킷 헤더 분석은 다음과 같다.

① 공격자는 전송하고자 하는 패킷의 IPv6 소스 주소를 공격대상으로 설정하고 스푸핑 하여 얻어진 합법적인 IPv4 주소로 패킷 헤더를 캡슐화 하여 엑세스 라우터로 전송한다.

② 공격자로부터 패킷을 받은 엑세스 라우터는 ingress 필터링 수행 후 6to4 릴레이 라우터로 패킷을 전송한다. 이때 공격자로부터 전송된 패킷은 합법적인 IPv4 헤더로 캡슐화 작업을 했기 때문에 ingress 필터링을 무사히 통과한다.

③ 엑세스 라우터로부터 공격자 패킷을 받은 6to4 릴레이 라우터는 IPv4 헤더를 제거 후 IPv6 헤더의 목적지인 반사 노드로 패킷을 전달한다.

④ 반사 노드는 공격패킷에 대한 ACK 로 패킷의 소스 주소인 공격대상을 목적지로 한 IPv6 패킷을 생성해 6to4 릴레이 라우터로 전송한다.

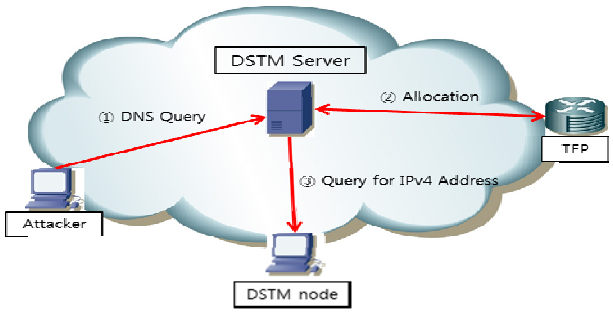
⑤ 6to4 릴레이 라우터는 반사 노드로부터 받은 패킷을 공격대상으로 전송함으로써 DRDoS 공격이 이루어 지게 된다.

3.2 IPv4 pool 서버의 주소 고갈 공격

IPv6 노드가 IPv4 노드와 통신을 하기 위해서는 사전에 IPv4 주소 할당 서버로부터 IPv4 주소를 받아야만 한다. 이러한 과정에서 IPv6 네트워크에 존재하는 악의적인 사용자가 자신의 IPv6 헤더의 소스주소를 달리하여 연속적인 IPv4 주소 요청 패킷을 전송할 경우 DSTM 서버가 관리하는 IPv4 pool 이 바닥날 수 있다. 이는 기타 다른 서비스를 원하는 정상적인 IPv6 노드 입장에서는 서비스 거부 공격을 당하게 하는 효과를 낳는다.

DSTM 서버에서는 IPv4 pool 이라는 IPv4 주소 목록을 가지고 주소 할당 과정이 수행된다. 하지만 IPv4 주소를 부여 하는데 인증 매커니즘의 부재로 이러한 서버의 주소 고갈 공격이 발생할 수 있는 취약점이 발생한다.

(그림 2)는 DSTM 주소 고갈 공격의 상황을 나타내고 시나리오는 다음과 같다.



(그림 2) DSTM server 를 이용한 주소 고갈 공격

① 공격자는 자신의 패킷의 소스 주소를 위조 후 IPv4 주소를 얻기 위하여 DSTM 서버에 요청 패킷을 전송한다.

② DSTM 서버는 공격자의 요청 메시지를 받아 자신이 가지고 있는 IPv4 pool 속의 비할당된 IPv4 주소와 공격자의 IPv6 주소를 맵핑 시킨 후 맵핑 정보를

TEP(Tunnel End Point) 라우터에 전송한다.

③ DSTM 서버는 공격자로부터 전송된 소스 주소로 IPv4 주소를 포함한 응답 패킷을 전송한다. 이때 응답 패킷의 목적지는 공격 패킷의 소스 주소가 된다. 공격자는 스푸핑된 여러 주소로 패킷을 보냈음으로 실질적으로 전송된 패킷의 주소를 가지고 있는 DSTM 노드는 존재하지 않거나 혹은 요청을 요구하지 않은 노드이다.

④ 위의 방법을 반복하여 DSTM 서버의 주소 고갈 공격이 이루어 진다.

4. IPv6 전환과정에서 보안위협 대응방안

4.1 터널링 방법에서 패킷 무결성 검사

터널링 방법에서 문제는 패킷 캡슐화 과정에서 발생한다. 공격자는 DoS 공격을 유발 시키는 악의적인 패킷을 연속적으로 전송한다. 이때 공격자는 자신이 보내는 공격패킷을 위장하기 위해 합법적인 IPv4 헤더로 캡슐화하고 ingress 필터링을 통과 한다. 패킷의 전송 과정 중 릴레이 라우터는 IPv4 주소 헤더가 합법적인가의 유무만 판단하기 때문에 공격자는 IPv4 헤더로 캡슐화하기 전 IPv6 헤더의 소스 주소를 변조하여 합법적인 수 많은 패킷을 만들어 낼 수 있다. 위와 같은 문제 때문에 자동 터널링을 지원하는 6to4 라우터는 전송 되는 패킷의 주소 무결성 검사를 지원해야 한다. (그림 3)은 패킷 무결성 검증을 수행하기 위한 방법을 보이고 있다.

① 6to4 릴레이 라우터가 공격자의 주소가 변조된 악의적인 패킷을 받은 후 합법적 주소로 캡슐화 되어 있는 IPv4 헤더와 IPv6 헤더를 분리 한다.

② 6to4 릴레이 라우터는 전송된 패킷의 무결성을 검사하기 위하여 패킷을 전송한 소스로 ACK 패킷을 전송한다.

③ 패킷을 보낸 노드가 일반 노드일 경우 6to4 릴레이 라우터로부터 받은 ACK 패킷에 응답을 하면 정상적인 패킷 전송이 완료되고 6to4 릴레이 라우터가 전송한 ACK 에 응답을 하지 않을 경우 6to4 릴레이 라우터는 악의적인 패킷이라 판단하고 패킷을 폐기한다.

④ 패킷을 보낸 노드가 일반 노드일 경우 6to4 릴레이 라우터로부터 받은 ACK 패킷에 응답을 하면 정상적인 패킷 전송이 완료되고 6to4 릴레이 라우터가 전송한 ACK 에 응답을 하지 않을 경우 6to4 릴레이 라우터는 악의적인 패킷이라 판단하고 패킷을 폐기한다.

6to4 릴레이 라우터가 공격자의 패킷 전송에 대한 응답 패킷 전송으로 패킷 무결성을 검증하여 필터링을 실시한다. 위와 같은 방법으로 악의적인 패킷을 사전에 차단함으로써 보다 신뢰성 있는 패킷 전송 기법이 될 수 있다.

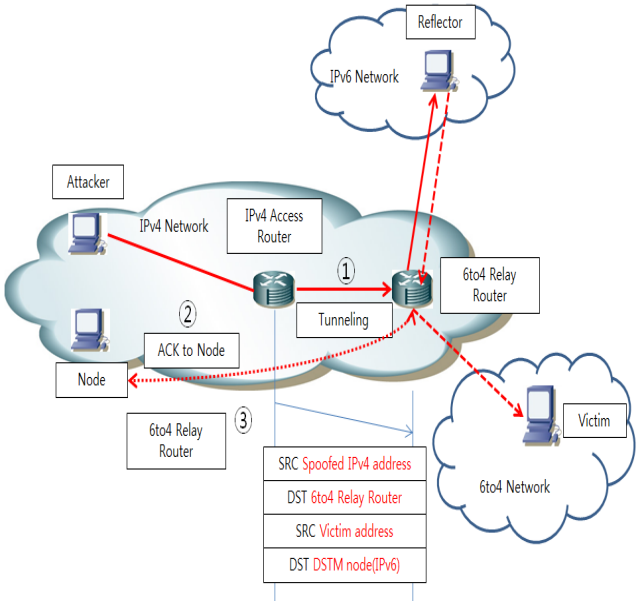
4.2 DSTM 서버에서의 신뢰성 있는 IPv4 주소할당 기법

IPv6 주소 체계를 사용하는 노드가 IPv4 주소 체계를 사용 하는 노드에 패킷을 전달할 경우 IPv4 주소를 할당해주는 서버의 IP pool 주소 고갈 공격이 발생할 수 있는 요인은 이들 서버와 노드간 주소할당에 관한 보안 체계가 정립되지 않아서 이다. 이러한 IPv4 주소를 할당하는 서버에 관하여 주소 고갈 공격은 공격자가 서로 다른 IPv6 주소를 이용하여 계속적으로 서버에 IPv4 주소를 요구하기 때문이다. 하지만 공격자가 IPv4 주소 요구 시 사용하는 IPv6 주소는 실제로 존재하지 않는 노드 이거나 또는 IPv4 주소를 요청하지 않은 노드 일 경우이다. 따라서 IPv4 주소를 할당하는 서버는 IPv4 주소를 요청하는 노드가 합법적인지 또는 비합법적인지를 확인할 필요가 있다.

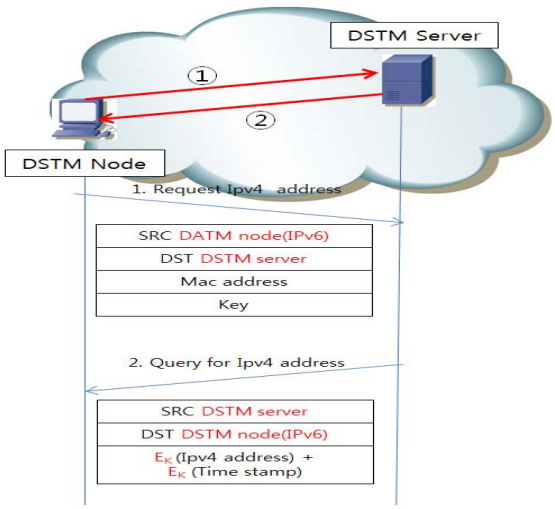
본 논문에서는 DSTM 서버의 IP pool 주소 고갈 공격을 방지하기 위해 기존의 할당 방식과 다른 인증 절차를 제안한다. (그림 4), (그림 5)는 주소할당 시 신뢰성 있게 주소를 할당하는 방법을 보이고 있다. 또한 이 방법의 절차는 다음과 같다.

① DSTM 노드는 외부의 IPv4 노드와 통신을 하기 위하여 DSTM 서버로 IPv4 주소할당 요청 패킷을 보낸다. 이때 DSTM 노드는 자신의 Mac 주소와 DSTM 서버로부터 할당될 IPv4 주소 암호화에 사용될 Key 값을 포함하여 전송한다.

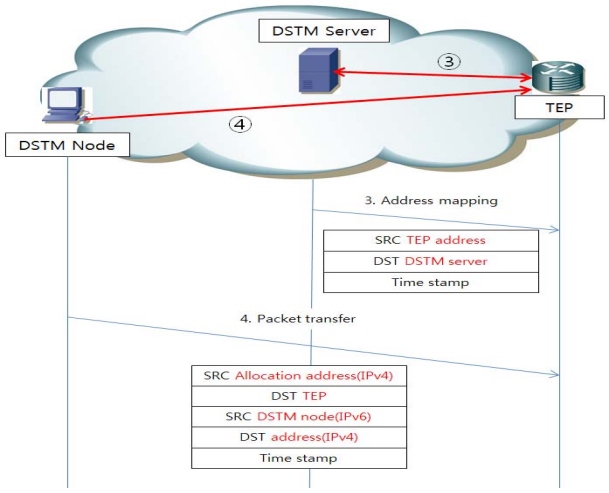
② 요청 패킷을 받은 DSTM 서버는 자신의 주소 테이블에 요청 패킷의 IP 주소와 Mac 주소를 맵핑하여 저장하고, 패킷에 동봉된 Key 값으로 IPv4 address 와 Time stamp 를 암호화 하여 응답 패킷에 첨부하여 전송한다.



(그림 3) Relay Router 를 이용한 패킷 무결성 검사



(그림 4) DSTM 서버를 이용한 신뢰성 있는 주소할당



(그림 5) DSTM 서버를 이용한 신뢰성 있는 주소할당

③ DSTM 서버는 노드에 대한 응답패킷을 전송 후 TEP 라우터에 매핑정보와 Key 값으로 암호화 된 time stamp 를 전송한다.

④ DSTM 서버로부터 응답패킷을 받은 노드는 Key 값을 이용해 패킷을 복호화 하여 얻은 IPv4 주소로 전송하고자 하는 패킷을 캡슐화 하고 TEP 라우터로 전송한다. 이때 TEP 라우터와 신뢰성을 확인하기 위해 Time stamp 를 첨부하여 패킷을 확인한다.

만약 IPv6 노드의 IP 주소가 변경된 후 IPv4 주소를 요청할 경우 DSTM 서버는 자신의 주소 테이블에 매핑되어 있는 IP 주소와 Mac 주소를 갱신한다. 또한 Mac 주소는 동일하나 서로 다른 IP 주소로 연속적인 IPv4 주소할당 요청이 들어오는 경우 DSTM 서버의 맵핑되어 있는 주소 테이블을 참조하여 악의적인 주소 요청 패킷 임을 감지 할 수 있기 때문에 보다 신뢰성 높은 주소할당 방법이 될 수 있다.

5. 결론

차세대 인터넷의 핵심 기술인 IPv6 망을 일시적으로 대체하는 것은 현실적으로 매우 어렵다. 그러므로 일정기간 동안은 IPv4 망과 IPv6 망의 공존이 불가피한 상황이다. 이러한 상황에서 각각의 프로토콜에 관한 보안상의 문제점도 노출되는 반면 두 프로토콜의 터널링 과정에 있어 보안 문제점이 새로이 발생한다. 이러한 문제점을 보완하고자 IETF 에서는 IPng(IP Next Generation), NGTrans WG(New Generation Transition Working Group)를 중심으로 IPv6 표준화를 진행하여 왔다.

본 논문에서는 IPv6 전환 기술에 관하여 알아보았다. 또한 6to4 릴레이 라우터를 이용한 DRDoS 공격과 IPv4/IPv6 연동 환경에서 발생 가능한 위험 요소를 분석하고, 패킷 무결성 검증으로 인한 필터링 방법과 IPv4 주소할당 서버의 IP pool 주소 고갈 공격에 관한 대응 방안을 제시하였다. 6to4 릴레이 라우터에서 ACK 패킷으로 인한 패킷 무결성을 검증하여 보다 안전한 전송기법을 제안하였지만 무결성 검증을 위한 ACK 패킷 전송으로 시간 지연이 발생한다. DSTM 서버의 IPv4 주소할당 시 발생하는 IP pool 주소 고갈 공격 문제의 대응 방안으로 DSTM 노드의 Mac 주소와 대칭키 암호화 알고리즘 사용으로 인하여 신뢰성 높은 주소 할당 매커니즘을 제안하였다. 주소할당 방식에서는 인증 과정의 복잡성과 패킷의 크기 증가가 발생하여 시간 지연이 발생 가능하다.

향후 과제로는 제안한 매커니즘을 실제 IPv6 망에 적용하여 효율성 점검과, 시간 지연을 줄이기 위한 패킷 최소화 방법과, 효율성 높은 암호화 알고리즘에 관한 해결 방안이 필요하다. 이외에 IPv6 망에서 발생 가능한 보안 위협을 찾고 그에 따른 문제 해결을 위한 지속적인 연구가 진행되어야 할 것이다.

참고문헌

[1] 박정수, 신명기, 김용운, 김용진, “차세대 인터넷 프로토콜 소개,” IPv6 포럼 코리아 기술문서 2000-001, 2000

[2] R. Gilligan and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers," IETF, RFC 2893, August 2000

[3] 최인석, 정수환, 김영한, “IPv6 전환 기술의 보안 위협 분석 및 보안 설계에 대한 연구,” 한국통신학회 눈문지, 30 (11B), pp. 689-697, 2005

[4] J. Wiljakka, et. al., “Analysis on IPv6 Transition in 3GPP Networks,” Internet Draft, draft-ietf-v6ops-3gpp-analysis-09.txt, Mar. 2004

[5] E. Nordmark and R. E. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers,” Internet Draft, draft-ietf-v6opsmech- v2-02.txt, Jan. 2004

[6] J. Bound, “Dual Stack Transition Mechanism,” Internet Draft, draft-bound-dstm-exp-01.txt, Apr. 2004

[7] G. Tsirtsis and P. Srisuresh, “Network Address Translation-Protocol Translation (NATPT),” IETF, RFC 2766, Feb. 2000

[8] E. Nordmark, “Stateless IP/ICMP Translation Algorithm (SIIT),” IETF, RFC 2765, Feb. 2000

[9] K. Tsuchiya, H. Higuchi, and Y. Atarashi, “Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS),” IETF, RFC 2767, Feb. 2000

[10] S. Lee, M. Shin, Y. Kim, E. Nordmark, and A. Durand, “Dual Stack Hosts Using “Bump-in-the-API” (BIA),” IETF, RFC 3338, Oct. 2002