MIPv6 기반 IPsec을 이용한 보안전송 기법에 관한 연구

문인택*, 류동주*, 노봉남*
*전남대학교 정보보호 협동과정
e-mail:maya71@athena.chonnam.ac.kr

A Study on safe transmission technique that IPsec of MIPv6 base

In-Tack Moon*, Dong-Ju Ryu*, Bong-Nam No*
*Interdisciplinary Program of Information Security, Chonnam University

요 약

최근 무선인터넷의 활발한 보급화에 더불어 이동성 단말을 이용한 전자상거래 등이 활발하게 이루어짐 에 따라서 개인 데이터 보호 및 안전한 통신을 보장 받으려는 모바일 사용자들의 요구가 급속히 증가하고 있다. 이는 무선매체의 공개성에 따른 보안침해의 용이성과 단말이 이동함에 따른 보안 체계 구축의 복잡성에 기인한다. 이러한 이유로 최근 이동성 단말의 통신에서 보안이 중요한 영역으로 인식되고 있다. 따라서 본 논문에서는 이러한 모바일 환경 특히 향후 전개될 MIPv6(Mobile Internet Protocol version 6) 환경에서의 안전한 데이터 전송을 위해 IP 계층 보안 프로토콜인 IPsec(Internet Protocol security)을 이용한 이동 단말의 안전한 데이터 전송을 테스트하고 향후 MIPv6 에서의 보안성 향상을 위한 방안들을 모색해 보고자 한다.

1. 서론

현재의 인터넷 사용자들은 휴대용 컴퓨터나 PDA 등 이동 단말들의 성능 향상과 무선통신 기술의 활발한 보급에 힘입어 무선 인터넷 사용자의 수가 크게 증가하는 추세에 있다. 초기의 모바일 IP 연구는 IPv4 환경에서의 연구가 주를 이루었으나, 증가하는 무선인터넷 사용자의 IP주소 요구량을 충족할 수 없는 이유로 현재는 폭넓은 주소공간을 제공하는 차세대 인터넷 프로토콜인 IPv6를 이용한 MIPv6에 대한 연구가 활발히 진행 중이다[1].

모바일 IP란 단말의 이동을 검출하고, 이동 후의 네트워크에서도 이동 전의 네트워크에서와 동일하게 통신할 수 있게 해주는 프로토콜이다. 그리고 모바일 노드와 통신하는 상대방 역시 해당 단말이 어느 곳에 위치해 있던지 끊임없는 통신을 유지할 수 있도록 지원한다[10].

MIPv6는 기존의 모바일 IP보다 폭넓은 주소 공간을 제공하며 Neighbor Discovery 와 Address auto-configuration 등의 기능을 이용하여 폭넓은 확장성 및 탁월한 이동성을 제공하며, 경로 최적화를 위한 프로토콜이 기본 기능으로 제공되고 있다. 현재까지 국내의 MIPv6 망이 널리 보급되지 않고 있지만 향후 모바일 IP 환경에서의 부족한 주소문제를 극복하기 위해서는 MIPv6의 도입이 필연적이다.

MIPv6가 단말의 이동성을 지원하기위해 뛰어난 메커니즘을 제공하지만 무선매체의 공개성 등으로 인해 보안상 많은 결함을 가지고 있다. 특히 이동 단말에서 전송되는 데이터는 특별한 보호 장치가 없다면 네트워크 스니핑, 데이터 변조 등의 공격에 쉽게 노출되어 데이터 기밀성이 위협받게 된다[11]. 따라서 본 논문에서는 MIPv6 환경의 모바일 노드에서 전송되는 데이터의 기밀성 보장과 안전한 전송을 위해 MIPv6 기반의 테스트 베드를 구축하고 IPv6에 기본으로 내장되어 있는 IPsec을 이용한 보안 전송을 테스트 한다.

본 논문의 구성은 2장에서는 IPv6의 주요한 보안 메커니즘인 IPsec에 대해 살펴보고, MIPv6 구현을 위한 구성 요소 및 요구사항을 살펴본다. 다음으로

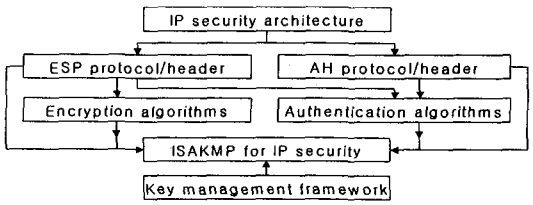
3장에서는 MIPv6 기반 IPsec을 이용한 보안전송을 하며, 마지막으로 4장에서는 결론 및 향후 과제를 기술한다.

2. 관련연구

2.1 IPv6 에서의 IPsec

IPv6는 AH(Authentication Header)와 ESP(Encapsulation Security Payload) 헤더를 기본적으로 포함하고 있다. AH와 ESP는 IPsec에서 진행중인 작업의 일부분이며, IPv4와 IPv6에서 모두 이용 가능한 암호기반의 보안을 제공하는 것을 목적으로 한다. IPsec은 두개의 호스트, 두개의 보안 게이트웨이, 혹은 호스트와 보안 게이트웨이 사이에서 통신 경로를 보호하는 메커니즘을 제공한다[8].

IPv6의 Security architecture는 접근제어(Access Control), 인증(Authentication), 무결성(Integrity, Confidentiality), 암호화(Encryption), SPI(Security parameters Index), SA(Security Association), 보안 게이트웨이(Security Gateway), 트래픽 분석(Traffic Analysis), 신뢰 서브넷(Trusted Subnetwork), 전송모드 SA(Transport Mode Security Association), 터널모드 SA(Tunnel Mode Security Association) 등과 같이 IPsec의 기본적인 정의를 포함하고 있다. 다음의 <그림 1>은 이러한 IPsec의 프레임워크를 나타낸다.

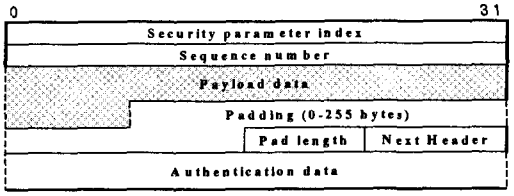


<그림 1> IPsec 프레임워크

SA는 인증 알고리즘, 알고리즘 모드, 암호화 키, 키의 생존시간 등을 포함하고 부가적으로 다양한 매개변수들을 포함할 수 있다. IPsec의 처리는 SA에 의하여 결정되며 각 객체들은 이를 공유하고 있다고 가정한다. 각 SA는 각 종단시스템에서의 속성 집합에 의하여 정의되고 SPI(Security Parameter Index)와 목적지 주소에 의하여 식별된다. SA에 의한 서비스는 AH 또는 ESP에 의해서 제공되며 전송모드(transport mode) 및 터널모드(tunnel mode)의 두 가지로 정의 된다. 종단간 보안(end-to-end security)은 인터넷 혹은 인트라넷을 사이에 둔 두 호스트들 간에는 전송모드나 터널 모드를 사용하고, 보안 게이트웨이 사이에서는 터널 모드를 사용할 것을 정의하고 있다[2][7].

AH는 비연결형 무결성(connectionless integrity), 데이터 원본에 대한 인증, 그리고 옵션으로 anti-replay 서비스를 제공한다. AH는 호스트와 호스트 간에는 전송모드 및 터널 모드로, 호스트와 보안 게이트웨이 사이에서는 터널모드로 사용된다. IPv6에서 AH는 종단간 페이로드로 간주되므로 hop-by-hop, 라우팅, fragmentation 헤더 뒤에 위치한다. 전송모드 및 터널모드 모두에서 AH는 IPv6 패킷 전체를 보호한다. 이때 ICV(Initial Check Value) 계산을 위해 사용되는 인증 알고리즘으로는 MD5를 이용하는 HMAC(keyed-Hashing for Message Authentication Code)과 SHA-1을 사용하는 HMAC이 있다[2].

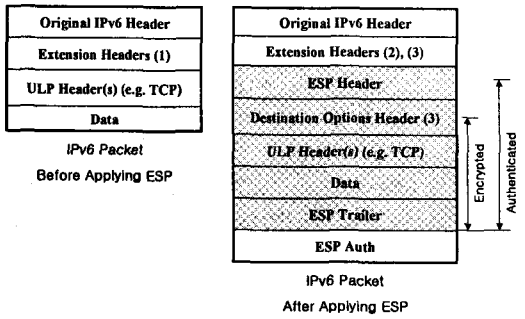
ESP는 AH에서 제공하는 서비스를 포함하며, 추가로 비밀성, 데이터 원본증명 서비스 등을 제공한다. IPv6 데이터그램 안에 ESP가 삽입될 경우 ESP 뒤의 데이터는 암호화 되며, 수신 측 에서는 미리 교환한 키를 이용하여 데이터를 복호화 하게 된다. 다음의 <그림 2>는 ESP 헤더의 포맷을 나타낸다.



<그림 2> ESP 헤더 포맷

그림에서 payload data 부분에 실제 암호화된 데이터그램이 위치하게 되며 전송모드와 터널모드에 사용될 수 있다. 전송모드의 경우는 호스트 구현에만 적용될 수 있으며 상위계층 프로토콜을 보호한다. 터널모드 ESP는 IPv6 패킷 전체를 암호화하고 새로운 IP 헤더를 더하며, IP 헤더까지 암호화하게 되므로 헤더정보에 대한 보안을 할 수 있다. 사용되는 암호화 및 인증 알고리즘에는 MD5를 이용하는 HMAC과 SHA-1을 이용하는 HMAC, DES-CBC, Null 인증 알고리즘, Null 암호화 알고리즘 등이 있다[3].

IPv6 상에서 ESP는 헤더 뒤쪽에 위치한 데이터만을 보호하기 때문에 Destination Option 헤더는 ESP 헤더 뒤쪽에 놓여지는 것이 바람직하다[7]. <그림 3>은 전송모드 ESP 사용시의 IPv6 패킷의 포맷을 나타낸다.



(1) If present
(2) Hop-by-Hop, Destination Options, Routing, Fragmentation Headers, if present
(3) The Destination Options header, if present could be before ESP after ESP or both

<그림 3> 전송모드 ESP

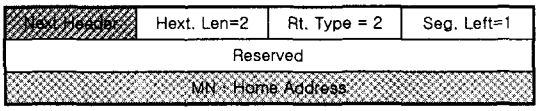
일반적으로 ESP가 제공하는 인증 범위는 AH보다 폭넓지 않지만 데이터 암호화를 제공하기 때문에 보안측면 에서는 AH보다 우수하다. 따라서 본 논문에서는 AH는 사용하지 않고 종단간에 ESP를 사용한 데이터 전송을 테스트 했다.

2.2 MIPv6 구현 요구사항

Mobile IPv6를 구성하는 주요 구성요소는 다음과 같다. 자신의 망 접속위치를 바꾸는 호스트 또는 라우터인 MN(Mobile Node), MN과 통신하는 호스트 또는 라우터인 CN(Correspondent Node), MN이 이동하기 전에 홈 링크의 프리픽스를 따르는 홈 주소를 가지고 통신하고 있던 네트워크인 HN(Home Network), MN의 HN에 있는 라우터 중 MN의 등록 정보를 가지고 있어서 MN이 HN을 떠나 이동하였을 경우 MN의 현재 위치로 데이터 그램을 전송해 주는 라우터인 HA(Home Agent) 등으로 구성된다.

다음으로 Mobile IPv6를 구현하기 위한 HA, CN, MN의 요구사항은 다음과 같다. 첫째, HA는 Proxy Neighbor Discovery 기능, IPv6 encapsulation 능력, Home Agent Address Request/Reply 메시지 처리 능력을 필요로 한다. 둘째, CN은 BU(Binding Update) 처리 능력, Home Address option 처리 능력을 필요로 한다. 셋째, MN은 IPv6 de-capsulation 능력, BU/Request/Acknowledgement option 처리 능력, HA Address Request/Reply 메시지 처리 능력을 필요로 한다[4][5][9].

MIPv6와 관련한 인터넷 드래프트 문서는 현재 draft-ietf-mobileip-ipv6-24.txt까지 제안되었고 BU와 관련한 모든 메시지를 교환하기 위해 IPv6에서 Mobility 헤더를 정의하여 사용하는 것과 HA와 MN 사이에서 IPsec의 사용을 정의하는 등 많은 부분이 제안되어 있다. 특히 Mobility 헤더를 정의한 부분에서는 Next Header 필드 값 "62"와 라우팅 헤더 "Type2"를 사용하는 부분을 정의하고 있다[6]. <그림 4>은 IPv6의 Mobility 헤더 구조를 도식화한 것이다.



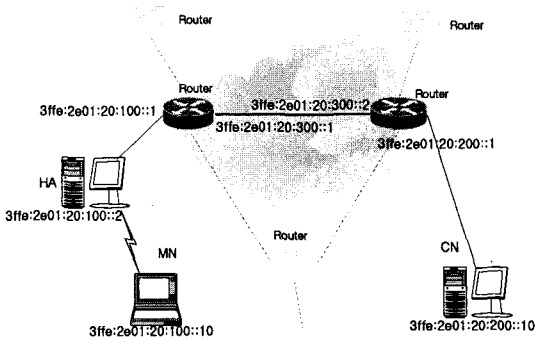
<그림 4> IPv6 Mobility 헤더

Mobility 헤더는 라우팅 옵션 헤더 Type2로 나타나며, 이를 지원하기 위해 Linux-2.4.20 커널에서 정의한 코드는 다음과 같다.

```
/* Type 2 Routing header for Mobility Protocol */
struct ip6_rthdr2 {
        uint8_t  ip6r2_nxt;       /* next header */
        uint8_t  ip6r2_len;       /* length : always 2 */
        uint8_t  ip6r2_type;      /* always 2 */
        uint8_t  ip6r2_segleft;   /* segments left: always 1 */
        uint32_t ip6r2_reserved; /* reserved field */
        struct in6_addr ip6r2_homeaddr; /* Home Address */
};
```

3. MIPv6기반 IPsec 전송

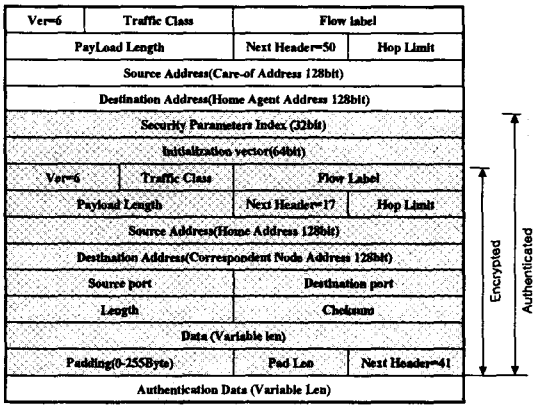
구성된 MIPv6 망은 Native IPv6로 구성된 2개의 IPv6 라우터와 HA, MN, CN 등으로 구성 하였다. 이를 이용하여 각 끝단에 위치한 MN과 CN간의 전송을 시도하였으며, 이것을 도시하면 <그림 5>와 같다.



<그림 5> MIPv6 망 구성도

각 MN과 HA 및 CN은 MIPL과 FreeSwan을 응용하여 MIPv6와 IPsec을 적용할 수 있도록 하였고 보안전송시의 네트워크 성능은 고려하지 않았다. 보안전송 형태로는 ESP 전송모드를 통한 암호화된 패킷 전송을 하며, 인증 알고리즘으로는 hmac-md5를 사용하고, 암호 알고리즘으로는 3des-cbc를 사용했다[12][13][14].

ESP 전송모드를 이용하여 MN과 CN사이에 전송되는 대량의 데이터는 FTP로 전송하며, 이때 전송되는 패킷의 포맷은 <그림 6>과 같다.



<그림 6> MIPv6 에서의 ESP 전송모드 패킷 포맷

그림에서 보듯이 중요한 데이터들은 ESP를 통해 암호화 되어 전송되게 되며, 이는 전송되는 패킷에 대해 비밀성, 데이터 원본증명, 무결성 등을 제공하여 각 노드간 데이터 전송 중에 공격자에 의한 불법적인 행동을 차단할 수 있게 된다.

그러나 IPsec을 사용한 데이터 전송은 각 노드간에 전송중인 패킷에 대한 보안성을 제공하지만 설치 및 사용의 어려움으로 인한 문제점을 가지고 있다. 또한 MIPv6 모듈과 IPsec 모듈은 현재까지 테스트 상태의 개발이 진행 중이기 때문에 두 모듈간의 적절한 결합을 위해서는 많은 보완이 필요하다.

4. 결론 및 향후 연구과제

현재 MIPv6와 IPsec6를 위한 연구가 각 연구단체에서 개별적으로 진행되고 있으므로 MIPv6기반 IPsec 구성과 사용이 매우 어렵다. 또한 MIPv6 환경에서의 IPsec을 실제 모바일 노드에 적용하기 위한 편리한 키 관리 모듈과 IPsec 모듈의 최소화를 위한 연구가 진행 중이지만 MIPv6에서의 보안전송에 대한 표준이 제정되지 않아 많은 전송 기법이 혼재되어있다. 본 논문에서는 다양한 전송기법을 제안하기 보다는 현재 사용되어지는 대표적 전송방법인 IPsec을 이용하여 데이터 보안전송을 테스트 하였다. 이결과 보안에 취약한 모바일 환경에서 IPsec을 사용한 종단간 전송은 데이터를 안전하게 보호하기 위한 훌륭한 방안중 하나라고 판단되며 향후 IPsec을 이용한 BU와 키 교환에 대한 이동성의 보안전송에 대한 추가적 연구가 절실히 필요할 것으로 예상된다.

참고문헌

[1] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998

[2] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998

[2] S. Kent and R. Atkinson, "IP Authentication Header", RFC 2402, 1998

[3] S. Kent and R. Atkinson, "IP Encapsulating Security Payload", RFC 2406, 1998

[4] D. Johnson, C. Perkins and J. Arkko "Mobility Support in IPv6", IETF Internet Draft, draft-ietf-mobileip-ipv6-24.txt, June 30, 2003

[5] J. Arkko, V. Devarapalli and F. Dupont "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", IETF Internet Draft, draft-ietf-mobileip-mipv6-ha-IPsec-06.txt, June 30, 2003

[6] Samita Chakrabarti and Erik Nordmark "Extension to Sockets API for Mobile IPv6", IETF Internet Draft, draft-chakrabarti-mobileip-mipext-advapi-00.txt, February, 2003

[7] Mark A. Miller "Implementing IPv6: Supporting the Next generation Internet Protocols", 2002

[8] Silia Hagen, "IPv6 Essentials" O'REILLY, July 2002

[9] Wolfgang Fritsche and Florian Heissenhuber, "Mobility support for the Next Generation Internet", Mobile IPv6-White paper, 2000

[10] 이광수, "MIPv6에서의 바인딩 갱신 인증", TTA저널 81호

[11] 이경진, 이승윤, 김용진, "Mobile IPv6 개발동향", IPv6 포럼 코리아 기술문서, 2001

[12] MIPL, http://www.mipl.mediapoli.com

[13] FreeS/WAN, http://www.ipv6.iabg.de

[14] USAGI Project, http://www.linux-ipv6.org