MIPv6망에서 IKEv2 인증 교환 모델 및 성능 분석

정회원 류 동 주*, 종신회원 김 광 현**, 정회원 김 동 국***

Analysis of Performance and IKEv2 Authentication Exchange model in Mobile IPv6 Network

Dong-ju Ryu* ***Regular Member***, Gwang-hyun Kim** ***Lifelong Member***,
Dong-kook Kim*** ***Regular Member***

요 약

본 논문에서는 모바일 환경의 이동 노드에서 전송되는 데이터의 기밀성 보장과 안전한 전송을 위한 무선 기반의 네트워크 실험환경을 설계·구축하고, MIPv6에서 기본적으로 탑재하고 양단간의 신뢰성 있는 인증키의 관리와 분배를 위해 사용되는 IKEv2 프로토콜을 모델링하여 실험하였다. 무선 네트워크에서 이동 노드의 핸드오프 시 빈번하게 발생되는 인증키 재설정 및 재교환 문제를 한정된 대역폭이 키 교환에 미치는 영향을 분석하였고 멀티 인터페이스를 이용한 인증 설정 및 교환 과정에 대한 성능 및 지연시간에 대한 연구를 진행하였다. 결론으로 모바일 노드가 IPSec을 이용하여 전송 시 발생하는 키의 재인증이 기존의 무선 네트워크가 지닌 대역폭의 한계에 따라 재설정이 불가능할 수도 있을 것으로 파악했으며 실험 결과를 통해 제안된 네트워크간의 멀티 인터페이스 사용은 보안 전송 시 핸드오프로 인한 키 교환 지연시간을 최소화 할 수 있을 것으로 예상된다.

Key Words : Mipv6, IPSec, IKEv2, Mobile Security, Handoff

ABSTRACT

For an experiment in this paper, designed test bed to secure confidentiality of data and safe transmission that Mobile node exchanges in Mobile network. And, For IPsec use that support basically in MIPv6, modeling and experimented IKEv2 protocol that is used for reliable authentication key management and distribution between End Point. When Mobile node handoff in Mobile network, analyzed effect that authentication key re-exchange and limited bandwidth that happen often get in key exchange. And studied about Performance and latency about authentication setting and exchange process that use multi interface.

To conclusion, when Mobile node transmits using IPSec, re-authentication of key confirmed that re-setting by limit of bandwidth that existent Mobile network has can be impossible. According to other result, proposed MN's multi interface is expected to minimise key exchange latency by hand-off when transmit IPSec.

Ⅰ. 서 론

이동통신의 급속한 확대로 인하여 무선 네트워크 역시 이동통신처럼 지역에 관계없이 누구나 쉽게 접속하기를 원하고 이동하면서 끊김 없이 통신할 수 있는 요구가 많아지고 있다. 그러나 현재 무선랜은 노드의 이동으로 인한 접속의 재설정과 전송 패킷 분실의 문제점을 갖고 있다. 또한 무선 환경에서

※ 본 연구는 정보통신연구진흥원 2005년 IT기초기술연구지원사업(05-기초-015)으로 수행되었습니다.
* 전남대학교 정보보호협동과정 (ryu@gwangju.ac.kr), ** 광주대학교 정보통신학과 (ghkim@gwangju.ac.kr)
*** 전남대학교 전자컴퓨터정보통신공학부 (dkim@chonnam.ac.kr)
논문번호 : KICS2006-04-168, 접수일자 : 2006년 4월 11일, 최종논문접수일자 : 2006년 10월 26일

Mobile IP 사용자가 늘어남에 따라 개인정보 보호의 측면에서 무선 매체의 공개성으로 인해 보안 취약점을 가지고 있다. 이 해결방안으로 IPSec 보안 프로토콜의 사용이 표준화 되었다. 그러나 인증체계나 빠른 핸드오프 등과 같은 이동성에 따른 메커니즘에 IPSec은 상당한 오버헤드를 가지고 있고 IPv6의 특성상 Auto-Config uration을 하기 때문에 무선 단말 인증에 걸리는 과정과 주소 지정 때 일어나는 Binding Update 전송 패킷의 보안 취약점이 노출되어있어 이를 해결하고자 하는 방안이 IKEv2이다. 따라서 기존 설계된 무선 네트워크에서 IKEv2를 이용하고자할 경우 발생하는 트래픽을 측정하여 원활한 키 전송과 네트워크가 미치는 영향을 사전 연구하여 실제 구현 시 발생될 수 있는 문제점에 대한 해결방안을 제시하는 연구가 필요하다[1-5][12].

따라서 본 논문에서는 무선 네트워크 환경에서 이동성을 제공할 수 있도록 제안된 MIPv6(Mobile Internet Protocol version 6)를 이용하여 무선 네트워크를 구축 할 때 보안 메커니즘으로 사용되는 IPSec(IP Security)에 대한 네트워크 간 대역폭이 키 교환에 미치는 영향을 조사하고 노드의 이동시 제약되는 사항을 시뮬레이션을 통해 도출된 결론을 확인하였다[16]. 이를 통해 데이터의 보안이 이동노드에 연결성을 유지할 수 있는지 규명하고 빠른 핸드오프와 빈번한 핸드오프에서도 적용이 가능한지를 검토했다. 마지막으로 결론을 통하여 네트워크의 대역폭이 키 교환을 맺을 때 끼치는 영향에 대한 해결방안을 제시하였다.

Ⅱ. IKEv2 기술 연구 동향

Mobike는 한 호스트가 다수의 IP를 소유하는 경우나 IPSec환경에서 로밍이나 단말의 이동성으로 인해 IP 주소의 변경이 발생하는 경우, 이를 지원하며 IKEv2 프로토콜을 확장하기 위해 구성된 IETF 워킹그룹이다. 대표적 지원방안은 다음 두가지 경우이다[11][12].

- 한 호스트 당 multiple IP 주소가 존재
- IPSec환경에서 로밍이나 mobility로 인한 IP 주소 변경 발생

현재 Mobike에서 연구 진행하는 것은 NAT를 사용가능하게 하기 위한 방안에 대해서 초점이 맞추어져 있으며 키 인증과정에 대한 부분은 많은 검토대상으로 남아 있다. 무선 네트워크 설계 시 제안되어진 기본 설계는 VPN이다. 따라서 해당 노드와 서버간의 통신은 터널링 개념에서 시작된다. 그림 1은 Mobike에 대한 기본적 구조 디자인이다[7][11][12].

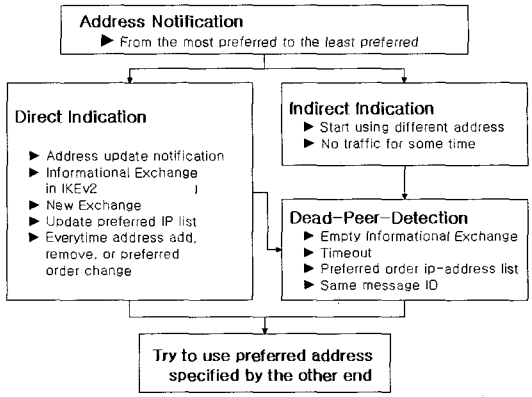

그림 1. Mobike Design

2.1 MIPv6 보안

MIPv6는 IETF에서 표준화가 지연되고 있으며 표준화 지연의 가장 큰 쟁점은 보안에 관련된 문제로써 기존의 MIPv6 관련 드래프트 문서에서는 BU(Binding Update) 전송 시에 IPSec의 AH(Authentication Header)를 사용하여 메시지를 보호 및 인증하는 것을 기본으로 하였으나, 글로벌 PKI(Public Key Infras tructure)를 기본으로 하는 IPSec의 도입은 현실적으로 어려움이 많고, MIPv6 에서 이동하는 모바일 노드와 대응하는 노드 사이에 수시로 일어나는 키 교환은 IPSec을 사용하는데 어려움이 있다[2]. 이에 MIPv6 워킹그룹에서는 MN (Mobile Node)이 BU를 전송할 때 HA로는 IPSec ESP(Encapsulation Security Pay load)를 사용하여 패킷을 보호하고, 대응 노드로 BU를 전송할 때는 보안을 위한 기본 메커니즘으로 RR(Return Routability)을 이용하여 HoA(Home of Address)와 CoA (Care of Address)가 도달 가능한지를 확인한 후 메시지를 전송하는 방식을 적용한다. 또한, 필요에 따라 RR보다 더욱 강력한 메커니즘을 추가로 적용하기로 의견을 모으고 있다.

MIPv6에서 보안 문제를 해결하기 위해 RFC3776이 제정되었고 BU와 관련된 메시지를 교환하기 위해 IPv6에서 Mobility헤더를 정의하여 사용하는 것과 HA와 MN사이에서 IPSec을 사용하는 등 많은 부분이 정의되었다[4][5]. 특히 Mobility헤더를 정의한 부분에서는 Next Header 필드 값 "62"와 라우팅 헤더 "Type2"를 사용하는 부분을 정의하였다.

Next Header	Hext. Len=2	Rt. Type=2	Seg. Left=1
Reserved			
MN · Home Address			

그림 2. MIPv6 헤더 구조

MIPv6 헤더의 구조는 그림 2와 같으며 IPv6의 라우팅 헤더 Type2로 나타난다[4][5].

2.2 MIPv6에서의 IPSec 기술 동향

IPv6의 기본적인 정의는 IPSec을 옵션으로 포함하고 있으며 이를 위한 구현은 BSD계열에서는 KAME 프로젝트가 있고 리눅스 계열에서는 기존의 IPv4에서 사용하던 FreeSwan을 IPv6에 적용하도록 하는 작업을 IABG(International Association of Botanic Gar dens)에서 진행 중에 있다. IPv6에서 IPSec을 기본적으로 포함하고 있으나 이를 위한 구현상의 문제는 각 벤더들에게 맡겨 놓고 있는 상태이며, MIPv6 워킹그룹에서도 IPSec을 사용하는 것에 초점을 맞추고 있다.

현재 MIPv6와 관련되어 추진 중인 프로젝트로는 MIPv6와 IPSec를 통합하는 문제와 관련하여 USAGI (UniverSAl playGround for Ipv6) 프로젝트에서 각종 모듈을 통합한 커널을 지속적으로 발표하고 있으며 TAHI(Tiny software and system Architecture for non Computer Appliances)에서는 이들을 이용한 각종 테스트를 진행하였다. 직접적인 구현은 아니지만 기존의 NS-2(Network Simulator -2)를 확장하여 MIPv6를 테스트 할 수 있는 MobiWan 시뮬레이터와 IKEv2를 IPv4 네트워크에서 측정한 NIIST 시뮬레이터가 있다. 아직 NIIST는 IPv6에 대한 모듈은 구성되지 않았다[13-16].

USAGI그룹에서 MIPv6 및 IPSec 관련 통합 모듈을 제공하고 있으나 공개용인 안정화버전의 경우 MIPv6 모듈을 제공하고 있으며 snapshot버전으로도 제공하고 있다. 그리고 USAGI나 IABG, MediaPoli에서 MIPv6 및 IPSec에 관련된 프로젝트를 진행하고 있으나, 이들 각 프로젝트에서 개발되는 모듈간 통합에서의 문제점은 계속해서 보완해야 할 문제점으로 남아있다.

2.3 IPSec over IPv6

IPv6 full implemention은 AH(Authentica tion Header)와 ESP Header을 가지고 있다. 그림 3은 IPSec의 프레임워크를 나타낸다[8].

AH와 ESP는 IPSec에서 진행 중인 작업의 일부

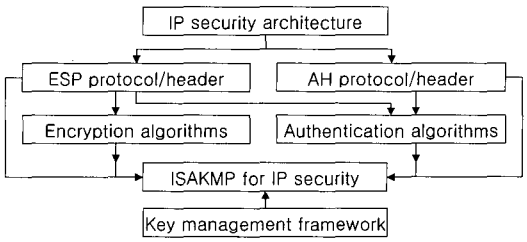

그림 3. IPSec 프레임워크

분이며 IPv4와 IPv6에서 모두 이용 가능한 암호 기반의 보안을 제공하는 것을 목적으로 하고, IPSec은 두 개의 호스트 사이나 두 개의 보안 게이트웨이 사이 혹은 호스트와 보안게이트웨이 사이에서 통신 경로를 보호하는 메커니즘을 제공한다.

IPv6의 Security Architecture는 접근제어(Access Control), 인증(Authentication), 무결성(integrity), 신뢰성(Confidentiality), 암호화(Encryption), SPI(Security Parameters Index), SA(Security Association), 보안 게이트웨이(Security Gateway), 트래픽 분석(Traffic Analysis), 신뢰 서브넷(Trusted Subnetwork), 전송 모드 SA(Transport Mode Security Association), 터널 모드 SA(Tunnel Mode Security Association) 등과 같이 IPSec의 기본적인 정의를 포함하고 있다[1-3][5][7].

SA는 인증 알고리즘, 알고리즘 모드, 암호화 키, 키의 생존시간 등을 포함하며 부가적으로 여러 가지 다양한 매개변수들을 포함할 수 있다. IPSec의 처리는 SA에 의하여 결정되며 각 객체들은 이를 공유하고 있다. 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 정의되어지는데 종단간 보안(end-to- end security)은 인터넷 혹은 인트라넷을 사이에 둔 두 호스트들 사이에서는 전송모드나 터널 모드를 사용하고, 보안 게이트웨이 사이에서는 터널 모드를 사용할 것을 정의하고 있다[2][7][9][10].

Ⅲ. 인증 교환 모델링

본 논문에서는 첫째, 멀티 인터페이스를 이용하여 키를 교환했을 때의 지연시간을 측정하고 모바일 노드가 이를 수용하고 재 통신하는데 걸리는 시간을 실험해 보았다. 둘째, 무선 네트워크의 대역폭

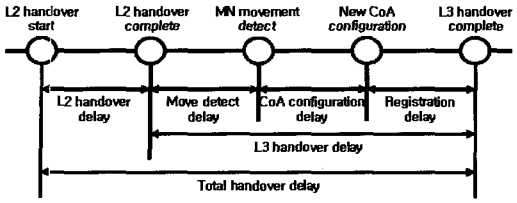

그림 4. MIPv6의 레이어별 지연

에 따른 지연시간과 그 성능을 실험하고 측정하였다. 모바일 단말에서의 기본적 핸드오프에 대한 지연은 레이어2와 레이어3의 두 가지 형태에서 볼 수 있다. 그림 4는 전체적 지연시간과의 관계를 보여주고 있다[15].

현재 무선 랜에서 사용 중인 인터페이스들은 사용가능한 접속 망을 확인하여 전송하지만 두 대의 인터페이스가 동시에 적용하여 전송하지는 못한다. 그러나 사전에 미리 키를 교환하여 전송구간에서 설정해 놓으면 핸드오프가 발생 시 원활하게 전송이 가능할 것으로 예상했다. 이를 위해 각 SA구간에서 설정하는 타임라인을 30초로 두었고 이시간이 지나면 키 설정을 삭제하도록 설계하였다. 그림 5.는 모바일 노드의 이동 후 예상 연결 모델이며 기본적인 핸드오프과정 완료의 그림이다. 그림 5.의 MN이 다른 네트워크로 이동할 경우 키 교환 후 새로운 주소를 인식해야 하지만 이동전의 과정은 ①의 HA에서 주소와 사용자를 인증 받고 연결하는데 있어 SA과정을 단계적으로 거치게 된다. 그 이후 새로운 주소를 받는 라우터에게 정보를 요청하고 그 정보를 재설정하는 과정을 거치게 된다. IKEv2에서 모바일 노드가 서버에 접속할 경우 초기 설정을 맺는 SA는 그림 6, 그림 7과 같다[5][10][11].

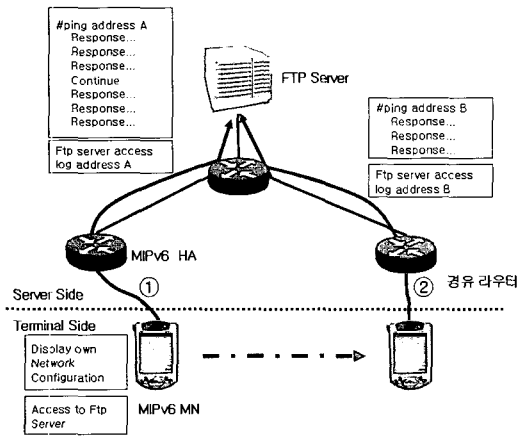

그림 7. 모바일 노드의 이동 후 예상 연결모델

각각의 인증키 연결과정은 기본 IKEv2 기본 설계를 따른다.

처음 MN이 HA에게 보내는 정보는 초기화설정 과정에서 나타나듯이 단말정보를 요구하고 HA는 이를 확인하는 절차를 수행하게 된다. 본 논문에서는 순수 IKEv2의 성능만을 측정하는 것으로 규정하여 워킹그룹에서 제안된 기본 설계로 모델링을 설정하였다.

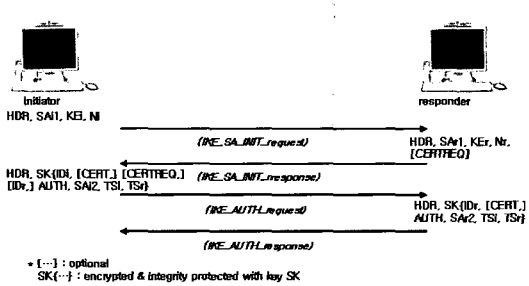

그림 6. Phase 1 과정

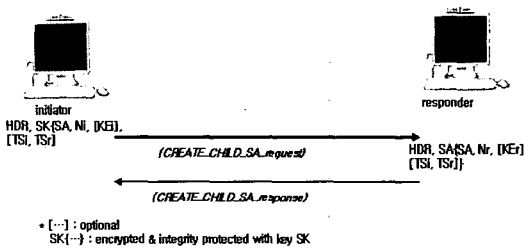

그림 7. Phase 2 과정

그림 6, 7 과정에서 노드 간 전송되는 패킷이 상호간에 완전하게 관계를 맺어야 보안 통신이 가능하다.

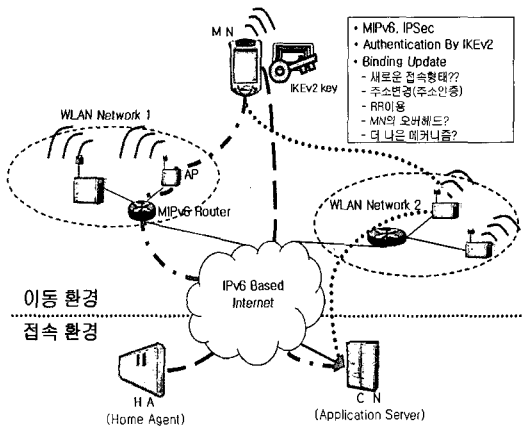

그림 10. 다중 인증키를 가진 노드의 실험 모델 연결과정

Ⅳ. 실험 모델

본 논문에서 실험환경은 리눅스를 기반으로 구성되어져 있으며 자바를 이용한 시뮬레이션 네트워크인 SSFNET(Scalable Simulation Framework Network Models)를 이용하였다. 또한 키의 성능을 측정하기 위해 NIST(National Institute of Standards and Technology)의 NIIST(NIST IPSec and IKE Simulation Tool)를 이용하여 키 관리와 교환을 측정, 수행하였다[16][17]. 그림 9는 실험 환경을 위해 구축한 가상 네트워크와 실제 구현 네트워크이다.

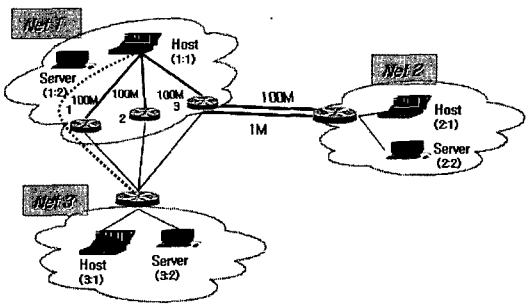

그림 11. 네트워크 구성도

Net1과 Net2는 무선 네트워크의 대역폭에 따른 지연시간과 그 성능을 실험하고 측정하기 위해 100Mbps와 1Mbps로 전송 대역폭을 정하였다. 이는 Net1의 노드가 모바일 노드로 다른 망과 접속할 때를 고려하여 설계되었기 때문이다. Net1의 호스트(1:1)가 Net2의 호스트(2:1)와 통신을 시작할 때 각각의 라우터는 SG(Security Gateway)로 설정되어져 있다.

Net1과 Net3은 멀티 인터페이스를 이용하여 키를 교환했을 때의 지연시간을 측정하고, 모바일 노드가 이를 수용하여 재 통신하는데 걸리는 시간을 실험하기 위해 설계하였다.

Ⅴ. 실험 결과 및 분석

그림 9에서 Net1의 모바일 노드가 Net2의 서버에 접속할 경우 기본 전송 단위는 IPSec 전송 초기값 즉, SA 초기 설정 단계인 init값을 전달하는 과정을 분석하였고, 두 번째 재전송시 발생하는 재설정 키 즉, Re-Keying을 측정하였다. 실험 데이터의 공정성을 위하여 20번 이상을 전송하고 초기화를 통해 연결될 때까지의 평균값을 구하여 전체적인

표 1. 대역폭 별 IKEv2 키 초기화 및 재설정 측정 분석값

	Initial Delay				Rekeying Delay			
Bandwidth	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4
100MB	0.464	0.262	0.300	0.100	0.300	0.100	0.301	0.100
1MB	0.266	0.473	0.100	0.309	0.100	0.582	0.100	0.994

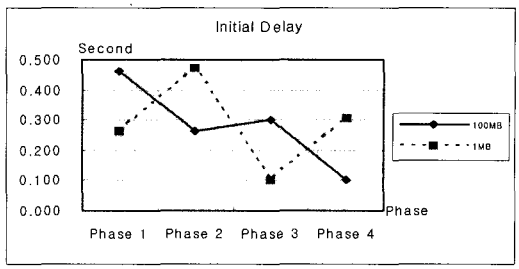

그림 12. 대역폭에 따른 초기 설정 측정값

지연 시간을 분석하여 보았다. 마지막으로 가상 실험망을 실제 망으로 구축하여 무선 IPSec 데이터 전송 과정을 확인하였다.

표 1은 100Mbps와 1Mbps 전송 대역폭을 가진 실험 환경에 의해 측정된 분석 값이다. 측정된 분석값은 소수점 이하 3자리까지만 표시하였다. 처음 초기화 과정에서 100Mbps는 인데 평균값으로 약 0.46초이며 이를 재전송 즉 노드와 망 사이에서 재전송하고 재설정할 경우 약 0.3초의 평균값을 가졌다. 이를 보면 Phase 1에서 상당한 오버헤드가 발생되었으나, 전체적인 평균 측정치에서 상당히 안정적으로 상호 연동되는 모습을 보였다. 그러나 1Mbps에서의 인증과정은 많은 시간적 변화를 보였으며 현재 사용 중인 일반적 이동 통신의 대역폭으로는 보안 전송 시 많은 문제가 될 것으로 예상된다.

그림 10과 그림 11은 각 대역폭 별 측정된 값을 그래프로 표현한 것이다. 그림 10에서 보면 마지막으로 완전 연결 후의 Phase 4의 변화 값에 상당한 차이가 있음을 보여주고 있다.

그림 10은 대역별로 처음 IPSec을 연결하기위한 키 초기 설정 교환 과정을 측정한 것이다.

그림 11에서 보듯이 1Mbps에서 핸드오프가 발생한다면 재설정 과정의 시간이 오래 걸리게 되므로 핸드오프가 일어나는 순간에 보안전송은 단절되고 다시 키를 맺을 때 이미 통신가능 지역을 벗어날 것으로 추측된다. 일련의 동작들을 통해 예상되는 결과는 보안 접속과정을 이용한 전송설정 과정이 실제 데이터를 주고받는 과정보다 더 길어지므로 패킷별 요금부과를 하고 있는 현 요금 제도로서는

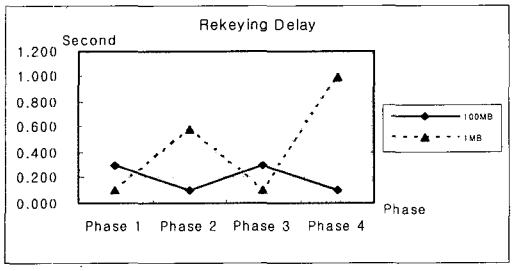

그림 13. 대역폭에 따른 키 재설정 측정값

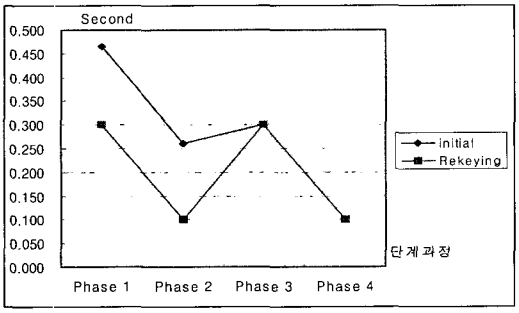

그림 14. 키 초기화 및 재설정

사용이 어려울 것으로 보인다.

두 번째 실험으로 멀티 인터페이스를 이용한 실험결과이다. 그림 9에서 Net1의 모바일 노드가 Net3의 서버에 접속할 경우 각 경유 라우터의 번호가 있는데 1번 라우터가 단절됐을 때 라우터를 2번으로 교환하고, 다시 키를 생성해야만 계속적인 IPSec 전송이 가능하도록 설계하였다. 따라서 이러한 전송 형태로 보아 무선 랜에서 전송 되어질 때 핸드오프가 발생되면 시간에 대한 패킷의 전송률은 상당히 중요할 것으로 예상된다.

제시된 표 1을 이용하여 100Mbps 전송 대역폭의 IKEv2 키 초기화 및 재설정 측정 분석값을 그래프 형태로 나타낸 것은 그림 12이다. 그림 12에서 키의 재 교환은 초기화 재설정보다 상대적으로 훨씬 빠른 것으로 측정됐다. 키 재전송에서 Phase1의 SA설정 과정은 제안된 멀티 인터페이스를 이용한 기존의 보유키를 확인하고 재 교환하는 것이 전송 구간에서 좀 더 효율적임을 확인하였다.

그림 13은 실험을 위해 설계된 가상 망을 실제 망으로 구축하여 MN과 IPSec으로 연결된 CN 사이의 FTP 전송 과정을 캡처한 화면이다. 실험과정에서 MN이 SG(Security GW)와 사전 협의를 통해 전체 암호화인 ESP로 전달하고 있는 모습을 확인하였다.

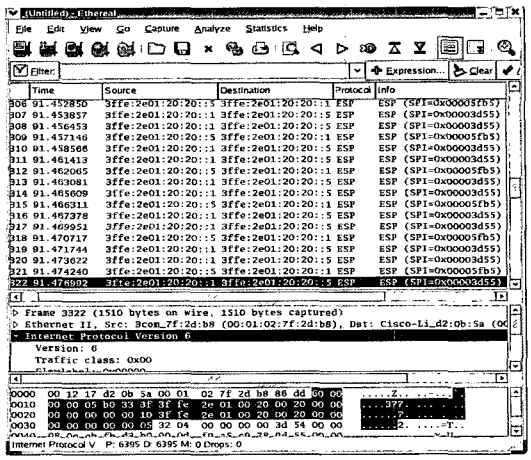

그림 15. 실제 구현망의 FTP에서 무선 IPSec ESP전송

VI. 결 론

본 논문에서 살펴본 바로는 IKEv2에서의 초기 설정 시간은 무선 단말간의 보안 전송 시 매우 중요할 것으로 예상되어지며 기존의 무선 단말 즉, 모바일 폰을 이용하여 전송할 때에는 작은 대역폭으로 인하여 완전한 보안 전송이 이루어지기는 힘들 것으로 예상되어진다. 그러나 일반 무선 랜 환경에서의 Mobile IP를 이용한 전송은 대역폭이 기본 11Mbps로 전송되어지고 802.11g에서와 같이 54Mbps로 전송되어진다면 크게 문제 될 것은 없을 것으로 보인다. 그러나 이동 단말의 경우 핸드오프 발생 시 빠른 속도로 기지국 혹은 AP(Access Point)를 경유하여 지나갈 때, 소요되는 시간이 얼마나 빠르냐에 따라 보안전송의 유무가 판가름 날것으로 보인다. 따라서 안전한 무선 보안 네트워크의 설계 시 초기 보안 전송의 설정 시간에 초점을 맞추어 대역폭을 적절하게 확보해야 할 것으로 판단된다. 이에 본 논문에서는 사용자의 이동성에 중점을 두게 되면 보안전송을 하지 못할 수도 있음을 확인했다.

또한 IKEv2를 다중 키로 형성하여 통신하게 함으로써 핸드오프 시 발생하는 재전송과 재교환시 일어나는 시간적 차이를 극복하고자 하는 실험을 하였다. 실험 결과에서 보듯이 재설정 값이 초기화보다 좀 더 빠른 것을 볼 수 있으며 이를 통해 상대적이기는 하지만 라우터의 단절은 핸드오프를 발생하는 과정으로 인식하고 재설정 및 키 재생성을 하는 것을 보았다. 따라서 멀티 인터페이스를 통해 교환해야 하는 이기종 레이어별 보안전송에 많은 활용이 가능할 것으로 보인다. 현재 수행중인 연구

는 이를 좀 더 세부적인 핸드오프 과정과 보안 과정으로 분리하여 키 지연 시간과 이기종망간의 보안 전송 측정을 통하여 다양한 보안 전송 네트워크를 구현 할 예정이다.

참 고 문 헌

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

[2] S. Kent and R. Atkinson, "IP Authentica- tion Header", RFC 2402.

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

[4] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC3776.

[5] J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC3776.

[6] Samita Chakrabarti, ErikNordmark, "Extension to Sockets API for Mobile IPv6", IETF Internet Draft, draft-ietf-mipv6-mipext-advapi -04.

[7] Mark A. Miller, "Implementing IPv6: Su- pporting the Next generation Internet Pro- tocols".

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

[9] Wolfgang Fritsche, florian Heissenhuber, "Mobility support for ther Next Generation Internet", *Mobile IPv6-White paper*, 2000.

[10] F. Dupont, "Address Management for IKE version 2", draft-dupont-ikev2-addrmgmt-07. txt.

[11] T. Kivinen, H. Tschofenig, "Design of the MOBIKE Protocol", draft-ietf-mobike-design -03.txt.

[12] Mobike WG, http://www.vpnc.org/

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

[14] MIPv6 for Linux, http://www.mip1.mediapoli.com

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

[16] NIIST Sinulation Tool, http://www.antd.nist.gov/niist/

[17] SSFNet(Scalable Simulation Framework Net -work Models), http://www.ssfnet.org

류 동 주 (Dong-ju Ryu) 정회원

1999년 2월 광주대학교 컴퓨터학과 졸업

2002년 2월 광주대학교 정보통신공학과 석사

2003년 3월~현재 전남대학교 정보보호협동과정 박사과정

<관심분야> MIPv6, MoBike, NGN Security

김 광 현 (Gwang-hyun Kim) 종신회원

1989년 2월 광운대학교 전자전자계산학과 졸업

1991년 2월 광운대학교 전자계산학과 이학석사

1997년 2월 광운대학교 전자계산학과 이학박사

1997년 2월~현재 광주대학교 정보통신학과 부교수

2001년 8월~2002년 7월 Pennsylvania State University, Post-doc

<관심분야> 차세대 네트워크, 인터넷 QoS, 네트워크 관리

김 동 국 (Dong-kook Kim) 정회원

1989년 2월 전남대학교 전자공학 공학사

1991년 2월 포항공과대학 전자전기공학과 공학석사

2003년 2월 서울대학교 전기컴퓨터공학부 공학박사

1991년 2월~1993년 3월 삼성전자 정보통신연구원

1993년 3월~1992년 2월 삼성종합기술원 전문연구원

2002년 2월~2002년 12월 (주)넷더스 기술이사

2003년 4월~2004년 2월 전남대학교 전자컴퓨터정보통신공학부 조교수

<관심분야> 패턴인식, 음성처리, 침입탐지