IPSec 환경에서 연속적인 이동성 제공을 위한 MBB 시스템 설계

김선영* · 조인준*

Design of MBB System for provide Mobility continuity in Environment IPSec

Seon-Young Kim* · In-June Jo*

요 약

이동 노드가 이동했을 경우 MIPv6에서는 새로운 연결을 위한 인증과정이 진행된다. 잦은 바인딩 갱신작업과 인증과정은 많은 트래픽을 초래하므로 서비스를 지연시킨다. 이러한 문제를 해결하기 위해 PMIPv6에서는 이동 노드의 부담을 덜고자 네트웍 기반의 이동성 프로토콜을 지원한다. 그러나 도메인간 혹은 도메인내에서 옮겨질 경우 새로운 주소를 생성해야 함으로 MIPv6의 문제점을 그대로 내포하게 된다. IPSec에서도 외부망으로 이동시 신규협상이 이루어져야 한다. 이는 이동 노드에 부담을 발생시킨다. 본 논문에서는 주소 변화 및 보안 재협상으로 인한 끊김 현상과 지연을 해결하기 위해 MBB(Make Before Break) 시스템을 제안한다. 이동 노드가 CoA 주소를 받을 경우 IPsec 협약이 진행된다. 기존 협약내용에 사용된 식별자를 제안한 BID 메시지를 통해 CN(Correspondent Node)에게 전송하여 신원을 확인시킨다. 그후 협약을 간소화하여 협상하므로 연결 끊김을 방지할 수 있고, IPSec 협약단계에서 이동 노드의 부담을 덜고, 두개의 주소로 동시에 통신함으로 패킷 손실의 확률을 줄일 수 있다.

ABSTRACT

When a mobile node moves, MIPv6 operates an authentication process for the new connection. These kinds of frequent binding update and authentication processes cause much traffic and delay the service. To solve this problem, PMIPv6 provides a network-based mobility protocol in order to lessen the load on a mobile node. However, when it is moved from a domain to a domain or in a domain, there still lies a need for a new address, so MIPv6's demerit still exists. In IPsec, too, a new negotiation should be made when it is moved to WAN (Wide Area Network). This causes load to the mobile node. In this paper suggests MBB (Make Before Break) system to eliminate disconnections or delays resulted from the address change or renegotiation for security. When the mobile node receives a CoA address, IPsec negotiation gets operated. Its identity is authenticated by sending the identifier used for the prior negotiation to CN(Correspondent Node) through the BID message suggested. After that, negotiation gets simplified that disconnections can be eliminated, and in the IPsec negotiation, the load on the mobile node can be lessened as well; moreover, two addresses are used for the communication simultaneously, so the probability of packet loss can be reduced.

키워드

MBB, Mobility, IPSec Negotiation, IKE

* 배재대학교 컴퓨터공학과

접수일자 : 2008. 1. 29

Ⅰ. 서 론

인터넷 기술이 급진적으로 발전하여 무선 통신 기술과 단말기의 확산으로 무선 인터넷 환경이 빠르게 변하고 있다.

이와 같은 접속환경의 변화와 확장은 네트워크 계층에서의 보안성을 더욱 강조하게 되었다. IP 네트워크 보안으로 가장 잘 알려진 표준은 IPSec(IP Security)이다. IPSec은 보안이 취약한 인터넷에서 전달되는 IP 패킷을 대상으로 무결성, 기밀성 서비스를 제공하는 인터넷 보안 메커니즘이다. IPSec은 IPv6에서 기본으로 제공하는 서비스로 IPv4에서 IPv6로 변이되고 있다.

IPSec 협약은 이동중인 노드에게 주소가 변경될 경우 신규협약을 해야 한다는 새로운 문제점을 제기한다. 이동 노드가 다른 망으로 이동하였을 경우 기존 IPSec 협약은 무시되고 새로운 주소로 신규협약이 진행된다.

그러나 이동 노드의 빈번한 이동이라는 특성으로 바인딩 갱신 작업이 많이 발생하고 그에 따른 인증절차로 대량의 트래픽을 유발하여 핸드오프 현상과 서비스 지연, 품질 저하의 문제를 발생한다. 특히 기존의 인터넷 키 교환(Internet Key Exchange) 프로토콜은 기능이 복잡하고 표준화가 난해하여 시스템의 구현은 물론 구현된 시스템의 상호 연동이 어려웠다.

본 논문에서는 이동 노드가 홈 네트워크를 이동하여 외부망으로 접속하더라도 연속적인 서비스를 지원받도록 MBB(Make Before Break) 시스템을 제안하였다. MBB는 이동으로 연결이 두절되기 전에 또다른 연결을 시도하여 통신두절 현상을 사전에 막는 개념으로 이미 그 연구결과가 보고 되고 있다[1]. 참고문헌 1에서는 다중 네트웍 인터페이스를 통하여 다중 신호를 처리한 실험을 보고하였고 이 논문에서 제안한 MBB 시스템은 BID (Binding Unique ID) 메시지를 통하여 신규협약의 복잡한 단계를 간소화하고 그에 따른 트래픽 감소로 핸드오프시 연결 끊김 문제를 축소시켰다. 이동 단말은 연속적인 이동시에도 서비스를 제공받을 수 있고 IPSec 협약에 따른 단말 부하를 최소화 할 수 있다.

본 논문의 구성은 2장에서는 관련 연구에 대하여 살펴본다. 3장에서는 IPSec IKE 개요와 제안한 MBB 시스템을 비교하여 보고 결론으로 4장을 마친다.

Ⅱ. 관련 연구

2.1 IPSec

IPSec은 IP 패킷이 전송중에 변하지 않고 발신자의 인증 및 데이터 암호화를 제공하는 인터넷 보안 메커니즘이다. IPSec은 AH (Authentication Header)[2], ESP (Encapsulating Security Protocol)[3], IKE(Internet Key Exchange)[4][5]의 3가지 프로토콜로 구성된다.

2005년 12월에 제출된 RFC 4306에서는 IKEv2의 향상된 키 교환 프로토콜을 표준화 했다. 기존의 IKEv1에서는 상호 호환성이 부족하기 때문에 구현이 어렵고 DoS(Denial of Service) 공격이나 MITM(Man in the Middle Attack) 공격에 취약하다는 단점을 가지고 있었다.

이러한 단점을 개선한 IKEv2는 무거운 협상단계를 줄였고 재협상시 기존 상태 값들을 재활용함으로써 효율성을 증가 시켰다는 연구결과가 보고 되었다.[6][7]

2.2 MIPv6

MIPv6는 크게 3가지 동작과정으로 구분되며 MN (Mobile Node)과 CN(Correspondent Node), CN과 HA(Home Agent)간에 호스트 이동성을 지원한다.

MN이 CN으로부터 HA를 경유하여 첫 번째 패킷을 수신하면 RR프로토콜이 시작된다. MN과 HA사이에서는 IPSec ESP로 인하여 보호되지만 이 경로를 제외한 CN과 MN사이 그리고 CN과 HA 사이의 경로에 모두 접근이 가능하므로 보안상 취약점이 발생한다는 것과 RR 과정에서도 연결의 끊김 현상은 나타난다.

2.3 PMIPv6

MIPv6의 문제점을 인식한 인터넷 프로토콜 개발자들은 노드에게 부담을 덜어주는 클라이언트 기반 이동성 프로토콜이 아닌 네트워크 기반 이동성 프로토콜인 PMIPv6(Proxy MIPv6)를 표준화[8] 했다.

이 프로토콜의 특징을 살펴보면 이동 노드가 어떠한 IP 이동성 프로토콜 시그널링에도 관여하지 않는다는 것이다. 기존에는 이동 노드가 이동 정보에 관한 사항을 HA에 등록하고 새로운 주소로 CN과 협약을 하였으나 이런 과정을 네트웍상의 장비들이 대리 업무를 수행함으로 이동 노드의 부담을 줄였다. 그러나 장비들의 대리

업무에도 제한점이 있다. 한 도메인 안에서만 가능하기 때문에 도메인 밖을 벗어나게 되면 기존 도메인과의 연결이 끊어지게 되므로 지연현상이 발생된다.

Ⅲ. MBB를 적용한 IKE 제안

3.1 IKEv1 개요

IKE는 RFC에 규정되어 있으며 일반적으로 데이터를 암호화하는데 세션마다 다른 암호화키를 생성하여 사용한다. IKE는 ISAKMP(Internet Security Association and Key Management Protocol), Oakley, SKEME(Secure Key Exchange Mechanism for Internet Exchange)의 세 프로토콜이 결합된 하이브리드 형태의 프로토콜이다. ISAKMP에서는 프레임 워크, 메시지 포맷, Phase 개념 등을 인용하였고 Oakley는 키 교환 모드를, SKEME는 공개키 암호화 방식을 채용하였다.

3.2 MBB 시스템을 적용한 IKE 제안

모든 단말기는 PKI(Public Key Infrastructure) 기반의 IPSec 보안 서비스를 제공한다. MN은 통신중에 위치 이동이 가능한 노드이다. MN의 네트워크 인터페이스가 모든 신호를 받아들이도록 Setting되어 있다면 새로운 네트워크 프리픽스를 받게 되고 새로운 주소를 생성할 준비를 한다. 기존 연결정보를 이용하여 기존 통신을 유지하면서 신규주소로 신규협상에 들어간다. ID와 키값을 BID 메시지에 탑재하여 CN에게 협상을 요청한다. CN에서는 통신중인 MN가 이동중에 다른 주소를 획득했음을 감지하고 새로운 주소로 협상을 수락하는 패킷을 전송한다. MN과 CN은 동시에 두 개의 주소를 통해 통신을 하게 된다. MN이 이동된 망으로 완전진입을 하게 되면 이동전의 주소는 통신중에 두절된다. 결국 약해진 신호는 연결에서 제거하고, 신호가 강한 주소만을 선택하여 통신하게 되므로 이동중 연결 끊김 현상을 사전에 방지한다.

두가지 측면에서 새로운 제안을 요약하면 첫째, 이동노드의 통신이 두절되기 전에 새로운 신규협약을 체결하자는 MBB 개념을 적용하여 통신두절을 해결하고, 둘째 복잡한 IKE 협상으로 인해 지연되는 시간을 효과적으로 줄이기 위해 BID 메시지를 사용하였다. 이를 통해서, 이동 노드가 다른 영역의 망으로 이동하여 주소가 변경될 경우에 신규협약에 소요되는 부하를 줄였다.

3.3 MBB 시스템 통신절차

표 1에서는 통신과정에 사용되는 메시지들을 나타냈다. BU 메시지는 MN이 CoA를 획득한 후 HA에게 등록시 사용되는 메시지이다. 필드중 'Seq#'은 응답 메시지와 일치성 검증을 위하여 사용하는 16bit UI(Unsigned Integer)값이다. 'Lifetime'은 현재의 위치정보에 대한 유효 시간을 기록한 생존시간을 의미한다.

표 1. MBB 메시지 종류
Table. 1 Kind of MBB message

◈ Binding Update Message(BU)

					Sequence#
A	H	L	K	Reserved	Lifetime
Mobility options					

◈ Binding Acknowledgement Message(BA)

	Status	K	Reserved
Reserved	Lifetime		
Mobility options			

◈ BID Sub-Option

	Type=TBD	Length			
Binding Unique ID(BID)	Status	C	O	H	Reserved
Care-of address(CoA)					

다음은 BA 메시지이다. 구성요소의 필드중 '상태(Status)'는 BU 메시지의 처리결과를 의미한다. 'Seq#'는 BU 메시지와의 일치성 검증을 위하여 BU 메시지에 포함되어 있던 'Seq#'을 복사하여 포함시킨다. Lifetime은 해당 노드의 위치정보를 저장할 때에 저장되는 위치정보에 대한 유효생존 시간을 시간단위로 표현한 값이다.

여기서 중요한 것은 BID 메시지[9]이다. Binding Unique ID는 통신하기 위해 협약 단계에서 교환하는 식별자 값이다. 이 식별자를 통하여 MN가 이동했을 경우에도 MN 자신임을 증명한다. 결국 이 메시지를 통하여 다른 망으로 이동했을 경우 신원을 확인하고 Phase 2의 단계를 진행함으로 Phase 1의 협약 과정을 간소화 한다. CoA의 값에는 실제 이동된 새로운 주소값을 나타낸다.

다음 그림 1은 MBB 통신 절차이다. MN이 CN과 통신 중 이동하여 새로운 주소를 받았을 경우 수행과정을 나타냈다.

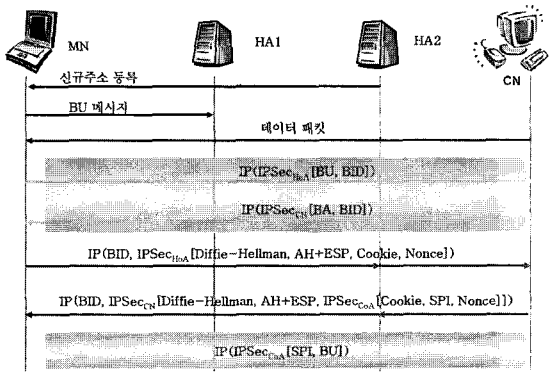

그림 1 MBB 통신 절차
Fig. 1 MBB Communication process

(step 1) 신규주소 등록

HA2 -> MN : 새로운 네트워크 프리픽스를 HA2로부터 광고 받았다. 외부망으로 접근했음을 확인하고 새로운 주소를 생성한다.

(step 2) BU Message

MN -> HA1 : MN는 새로운 주소를 HA1에 BU 메시지를 통해 등록한다. HA1은 BA 메시지를 통해 MN에게 등록되었음을 확인하고 이 바인딩 정보를 유지한다.

(step 3) 데이터 패킷

CN -> MN : CN은 MN과 통신하기 위해 HA1을 경유하여 메시지를 보낸다.

(step 4) BU, BID 전송

MN->HA1->CN : MN는 HA1을 통해 CN에게 BU, BID 메시지를 전송한다. CN은 BID 메시지의 식별자를 확인하고 MN가 이동했음을 인식한다. 동시에 CoA 주소를 확인한다. 개선된 사항은 이미 선행 협약된 보안 알고리즘으로 보안 통신을 한다.

(step 5) BA, BID

CN -> MN : CN은 MN에게 확인메시지인 BA 메시지에 Seq#를 복사하여 전송한다. MN가 전송한 BID 메시지를 다시 전송함으로 CN임을 확인한다. 이 메시지들은 암호화 되어 전송한다.

(step 6) 협약 내용 전송

MN->HA2->CN : IP(BID, IPSec$_{HoA}$ [Diffie-Hellman, AH+ESP, Cookie, Nonce]

· *BID* : MN과 CN 사이를 구별할 수 있는 식별자와 이동한 MN 주소가 포함된 sub-option. 식별자 값으로는 최초 IPSec 협상의 phase2 단계에서 교환한 ID와 키값이 탑재되는 부분이다.

· *IPSec$_{HoA}$* : 이동하기 전 기존에 교환한 암호화 키로 다음에 오는 내용들을 암호화한다.

· *Diffie-Hellman* : 앞으로 암호통신을 위해 키를 생성하기 위한 키 교환 알고리즘.

· *AH+ESP* : IPSec에서는 두가지 프로토콜 모두 지원이 가능하다. AH이거나 혹은 ESP, 두가지 병행해서 모두 사용 가능하며, 인증과 암호기능과 그에 필요한 매개변수값을 지정한다.

· *Cookie* : 개시자와 응답자의 IP주소값을 포함하고 있다.

· *Nonce* : 임의의 값.

(step 7) 협상 내용 확인

CN->HA2->MN : IP(BID, IPSec$_{CN}$ [Diffie-Hellman, AH+ESP, IPSec$_{CoA}$[Cookie, SPI, Nonce]])

· *BID* : 식별자 확인에 대한 응답.

· *IPSec$_{CN}$* : 기존에 통신하던 암호화 알고리즘으로 다음에 나오는 내용을 암호화한다.

· *Diffie-Hellman* : 앞으로 암호통신을 위해 키를 생성하기 위한 키 교환 알고리즘.

· *AH+ESP* : IPSec에서는 두가지 프로토콜 모두 지원이 가능하다. AH이거나 혹은 ESP, 두가지 병행해서 모두 사용 가능하며, 인증과 암호기능과 그에 필요한 매개변수값을 지정한다.

· *IPSec$_{CoA}$* : 새로 협약을 맺을 보안 통신 관련 사항으로 다음에 나오는 내용을 암호화 한다.

· *Cookie* : MN으로부터 받은 값, 개시자와 응답자의 IP주소값을 포함하고 있다.

· *SPI* : Security Parameter Index, 보안 매개변수.

· *Nonce* : MN로부터 받은 임의의 값.

(step 8) 최종 BU 메시지 전송

MN -> CN : IP(IPSec$_{CoA}$ [SPI, BU])

· *IPSec$_{CoA}$* : 신규협약 내용으로 암호화를 한다는 의미, 다음의 내용을 암호화한다.

· *SPI* : Security Parameter Index, 보안 매개변수.

· *BU* : 갱신된 내용을 확인하는 메시지, 검증의 의미가 있다.

이 과정이 종료되면 MN는 HA1과 HA2를 통해 각각 CN과 다중 주소로 통신을 하게 된다.

3.4 IKE와 MBB 시스템을 적용한 IKE 비교

제안한 MBB 시스템의 중심 기술은 첫째로 BID 메시지를 통한 간소화된 협상과정이다. 둘째로 이동 노드가 이동했을 경우 HoA, CoA 2개의 주소를 통해 모두 통신 가능하다는 것이다. 그러므로 핸드오프상의 서비스 지연과 연결 끊김 현상을 줄였다.

BID 메시지를 적용함에 있어 특징을 살펴보면 반드시 MN은 IPSec IKE 과정을 통해 보안 통신중이어야 함을 전제로 한다. 물론 MN은 최초 한번은 IPSec IKE 협약을 기존 절차에 따라 수행하고 외부망으로 이동하였을 경우 적용함을 원칙으로 한다. 핸드오프의 총 지연요소를 고려해 보면, 이동 검출, 새로운 임시주소 구성, 등록 및 데이터 전송단계로 다음과 같이 표현할 수 있다.

$$T_{total} = T_m + T_{CoA} + T_{BU+BA} + T_{trans}$$

여기서는 Phase 1의 단계만을 축소하여 살펴보겠다. 다음 그림 2와 3은 기본 IKE 절차와 BID 메시지를 적용한 교환단계를 보였으며 각각 수행시간을 분석하면 다음과 같다.

총 수행시간 =
P(*Process*, 노드에서 처리시간) +
t(*time*, 전송시간)

첫 번째로 그림 2는 Phase 1의 메인모드와 그림 3의 BID 수행시간을 노드별로 비교하였다.

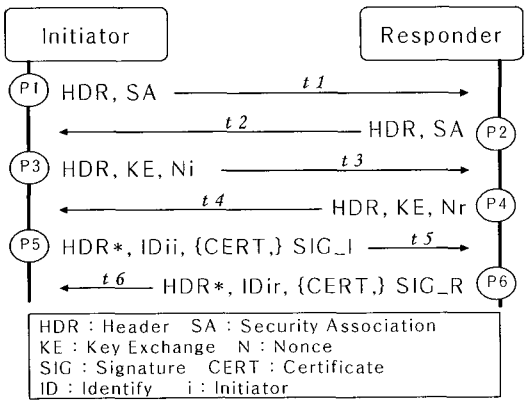

그림 2. Phase1 메인모드의 메시지 교환
Fig. 2 Phase1 Message Exchange of Main Mode

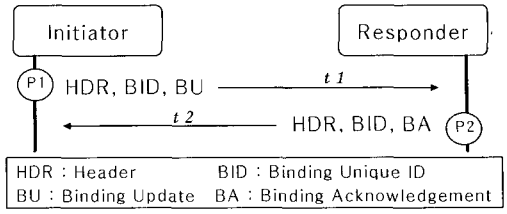

그림 3. BID 메시지 교환
Fig. 3 Message Exchange of BID

IKEv1 Phase 1 메인모드 수행시간

$$P = P1+P2+P3+P4+P5+P6 \text{ ..... 1)}$$

BID를 적용한 IKE 메시지 수행시간

$$P = P1+P2 \text{ ..... 2)}$$

먼저 1)과 2)의 메시지 처리시간을 비교하면 다음과 같다. 1)은 여섯 단계가 모두 마감되면 Phase 2의 협상단계를 수행한다. 이것은 노드가 외부로 이동했을 경우 어떤 망과 어떤 상황에서든 반드시 처음부터 수행해야 하는 것과 비교하여 2)에서는 기존 통신이 지속되고 있다는 전제하에 두 단계만 마감되면 Phase 2의 협상단계로 넘어간다. 1)의 *P1+P2+P3+P4+P5+P6* 만큼의 메시지 생성 소요에 비하여 2)에서는 *P1+P2* 만으로 처리가 가능하고 수행 시간을 빠르게 진행할 수 있다.

또다른 관점은 1)에서는 5, 6번에서 실제적으로 보안통신이 적용된다. 반면 2)에서는 1, 2단계 모두 보안통신이 적용되므로 훨씬 안정적이다. MIPv6는 공격자에 대해 DoS 공격이나 MITM 공격에 노출되어 있다. 이것은 신규협약에 따른 문제점이다. 새로운 주소를 등록하기 위해 MN은 CN과 IPSec 협상을 진행한다. 그러나 CN과 HA사이, CN과 MN사이에 보안 채널이 생성되지 않음은 이미 알려진 바이다. MBB 시스템에서는 기존의 협약내용에서 결정된 암호 알고리즘을 노드가 이동한 후에도 자신임을 인증하고 암호 통신을 적용하므로 보안 채널이 생성되는 것이다.

다음으로 전송시간을 비교해 보면,

Phase 1 메인모드 전송시간

$$t = t1+t2+t3+t4+t5+t6 \text{ ..... 1)}$$

BID 메시지 수행시간

$t = t1 + t2$ ..... 2)

1)에서는 6번의 데이터가 교환되므로 6번 전송에 필요한 시간을 요구한다. 그러나 2)에서는 2번의 데이터 교환으로 모든 과정이 종료되므로 2번 전송에 필요한 시간만 필요하게 된다.

종합해 보면, 노드에서 처리수행 *P*의 경우 암호하는 처리량과 시간이 1), 2) 모두 같다고 가정하더라도 단계의 감소로 인하여 2)의 단계가 훨씬 가볍고 빠른 시스템이다. 전송시간에서도 총 6번의 교환시간에 비해 2)의 경우 2번의 수행으로 모든 과정이 마감되므로 시간절감 효과를 가져온다.

다음은 핸드오프 및 지연에 대한 분석이다.

그림 4에서 이동 노드는 새로운 망으로 진입하여 신규협상이 진행되는 현재의 과정을 나타냈다. 이동성으로 인하여 노드가 신규협상을 진행할 경우 TCP 통신이든 UDP 통신이든 핸드오프 현상과 패킷 손실이 있었음을 증명하는 연구 결과[1]가 있다.

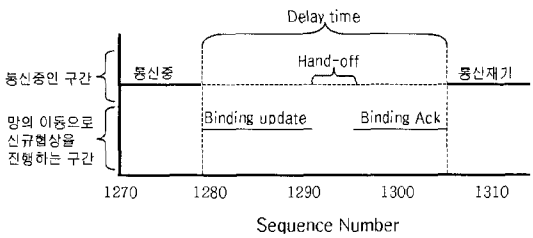

그림 4. IKE 신규협상
Fig. 4 New Negotiation of IKE

Sequence Number를 그림과 같이 가정하였을 경우 Binding Update가 전송된 후 Binding Ack 메시지를 받을 때까지 상황에 따라 유동성 있는 지연시간이 초래된다. 이러한 노드의 이동성 문제는 실시간 통신에서 가장 취약하다.

그림 5에서는 MBB 시스템을 적용한 이중 통신을 나타내고 있다. 이동 노드는 이동중에 새로운 네트웍 프리픽스를 받고 BID와 함께 Binding Update를 시작한다. 특징으로는 HA를 통하여 기존 통신을 유지하면서 새로운 신규협상에 들어가므로 핸드오프 현상이 문제되지 않는다. 신규협상 절차가 마감되면 새로운 정보가 Binding Cache에 저장되고 HoA, CoA의 주소로 이중 통신이 진행된다.

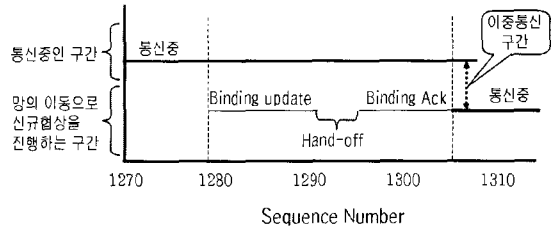

그림 5. BID를 적용한 신규협상
Fig. 5 New Negotiation thought BID

홈 네트워크와의 통신이 두절되기 전에 새로운 링크로 신규협약을 가동하고 외부망으로 진입한 MN는 CoA를 통해서 통신을 유지한다. 실제적으로 지연시간은 그림 5에 비해 그림 4에서는 Binding Update와 Binding Ack가 이루어지는 시점까지이다. 통신이 진행되다가 새로운 링크로 연결되어 통신이 재기되기까지 그 시간동안 통신은 지연되는 것이다.

Ⅳ. 결 론

본 논문에서는 이동 노드의 이동성에도 연결이 두절되지 않고 연속적인 통신을 지원하는 MBB 시스템에 대하여 제안하였다.

MIPv6에 대한 최소한의 보안 요구사항이 현재의 IPv4의 보안 수준을 더 악화시켜서는 안된다는 지적과 안전성 제공에 공개키 암호방식을 사용하는 방안이 무선장비들에게는 연산부담이 너무 크다는 이유로 보안 취약성은 과제로 남아 있었다. 이러한 상황에서 MBB 시스템에서는 새로운 BID 메시지를 도입했고 간편해진 협약단계로 노드의 연속적인 통신을 지원한다.

그러나 MBB 시스템에서는 바인딩 캐쉬의 관리가 별도로 필요하다. 두개의 주소로 동시에 통신을 하기 위해 협약된 내용에 맞추어 각기 보안 통신을 해야함으로 또 다른 자원을 요구한다.

향후의 연구과제로는 BID 메시지 교환과 식별자값에 대한 보안강도를 높이기 위한 더 구체적인 보안기법에 관한 연구가 필요하다.

참고문헌

[1] 홍성백, 이경호, 김남, "이종 무선망에서 L3 핸드오버 이동성 관리 성능 향상", 한국통신학회논문지, Vol. 32 No. 6, pp. 382~389, 2007.

[2] S. Kent, et, al. "IP Authentication Header", RFC 2402, IETF 1998.

[3] S. Kent, et, al. "Encapsulating Security Payload", RFC 2406, IETF 1998.

[4] D. Harkins, et, al. "The Internet Key Exchange", RFC 2409, IETF 1998.

[5] 이계상, "인터넷 키 프로토콜에 관한 연구", 정보처리학회 논문지, 제10-C권 제2호, pp. 133~140, 2003.

[6] 김성찬, 천준호, 전문석, "IPSec System에서 IKEv2 프로토콜 엔진의 구현 및 성능 평가", 정보보호학회논문지, 제16권 5호, pp. 35~46, 2006, 10.

[7] 엄희정, 김락현, 염홍열, "IKEv2 설계 및 구현", 정보보호학회지, 제16권 제3호, pp. 55~62, 2006, 6.

[8] http://weekly.tta.or.kr/weekly/files/20075703025754_admin.pdf

[9] http://www.ietf.org, "draft-ietf-monami6-multiplecoa-03.txt"

저자소개

김 선 영(Seon-Young Kim)

1999년 배재대학교 전자계산학과 (공학사)
2001년 배재대학교 컴퓨터공학과 (공학석사)
2004년 ~ 현재 배재대학교 컴퓨터공학과 (박사수료)
※관심분야 : 네트워크 보안, 컴퓨터 네트워크, MIPv6

조 인 준(In-June Jo)

1982년 전남대학교 계산통계학과 (공학사)
1985년 전남대학교 전자계산학과 (공학석사)
1999년 아주대학교 컴퓨터공학과 (공학박사)
1983년~1994년 한국전자통신연구원 선임연구원
1994년~현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 정보보호, 컴퓨터 네트워크, 전산조직응용