DOI: 10.3745/KIPSTC.2010.17C.2.153

모바일 IPv6 바인딩 업데이트의 보안 향상 기법

송 세 화[†] · 최 형 기[††] · 김 정 윤[†††]

요 약

Mobile IPv6는 이동 단말의 이동 중에도 세션을 유지하는 기법 중 하나이다. 기존 Mobile IPv4에서의 삼각라우팅 문제를 해결하기 위해, Mobile IPv6에서는 단말과 대응노드가 서로 직접 통신할 수 있는 기법을 제공하고 있다. 하지만, 현재 Mobile IPv6의 기법은 공격자가 일반적인 사용자의 세션을 뺏어오거나, 그것을 응용한 여러 공격이 가능하도록 하고 있어 개선이 필요하다. 우리는 이러한 문제점을 개선하기 위해 기존에 사용되던 두 개의 토큰에게 연관성을 부여하는 방법을 통하여 보안을 향상시킬 수 있는 방법을 제안한다. 이를 위해 현재 표준의 문제점을 분석하고, 보다 강화된 보안을 제공하기 위한 요구사항을 도출 및 이를 만족하는 프로토콜을 정의하였다. 그리고 여러 방면에서의 성능분석을 수행하였다.

키워드 : 모바일 IPv6, 보안, 경로최적화

Clue for Secure Route Optimization in Mobile IPv6

Sehwa Song[†] · Hyoung-Kee Choi[††] · Jung-Yoon Kim[†††]

ABSTRACT

Mobile IPv6 is one of method can keep Mobile node's session. To solve legacy Mobile IPv4's triangular routing problem, in Mobile IPv6, Mobile Node could directly communicate with Correspond node by Binding Update. But, attacker could interfere Return Routability Procedure that is Correspond node check Home address and Care of address reachable. At this result, Attacker is able to hijack Session to correspond node from Mobile node. In This paper, We propose new Binding Update scheme for solving that problem. Our approach is that MN gives association both home token and care of token using onewayness of keyed hash fuction. From security and performance analysis, we can see that proposed binding Update Scheme can achieve stronger security than legacy scheme and at the same time requires minimal computational overhead.

Keywords : Moble IPv6, Security, Route Optimization

1. 서 론

이동통신 기술은 노트북, PDA, 휴대폰과 같은 많은 장비에 탑재되어 사용되고 있으며, 이동할 수 있는 무선 단말(Mobile Node, MN)의 증가는, 사용자들의 인터넷에 대한 접근성을 높여주고 있다. 이동 중에 통신의 유지에 있어서 Mobile IPv6의 역할을 특히 중요한 부분을 차지한다. Mobile IPv6(MIPv6)는 IPv6를 사용하는 단말에서 이동성을 지원하도록 해주는 프로토콜이다[1]. MIPv6는 IPv6 단말이 이동하여 네트워크가 변경되어도 이미 통신하고 있는 상대 노드(Correspondent node, CN)와의 세션을 유지할 수 있도록 해준다.

MIPv6는 (MN)에게 가는 데이터를 Home agent(HA)가 재지향 시켜주는 방법을 사용한다. 이 과정에서 2개의 IP주소가 사용된다. HA가 MN에게 부여하는 Home address(HoA), MN이 현재 위치한 지역의 Access router가 MN에게 부여한 Care of address(CoA)가 그것이다. MN과 통신하는 CN은 MN의 HoA로 데이터를 전송하면, HA가 CoA로 재지향 시켜주어 MN에게 데이터를 전달하여 준다. 이 과정에서 CN과 MN이 근거리에 있을 경우에도 HA를 거쳐서 라우팅되는 문제인 삼각라우팅(Triangular Routing)이 발생한다[2]. 삼각 라우팅은 전송 지연시간을 증가시키고, HA의 과부하가 걸리게 된다. 이를 해결하기 위해 MIPv6에서는 경로최적화(Route optimization, RO)를 지원한다. RO는 CN에게 MN의 HoA와 CoA를 알려주어, 데이터를 HA를 거치지 않고, 바로 MN에게 전달하는 것이다. Binding Update는 MN이 CN에게 자신의 CoA를 알려주는 과정이다. 이 Binding Update에는 여러 보안이슈가 존재한다.

† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 석사과정
†† 정 회 원 : 성균관대학교 정보통신공학부 조교수
††† 준 회 원 : 성균관대학교 휴대폰학과 박사과정

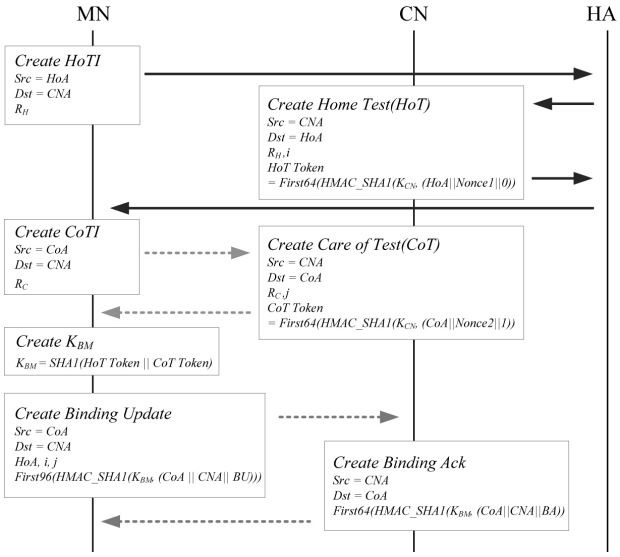
논문접수 : 2009년 8월 6일
수 정 일 : 1차 2009년 11월 30일
심사완료 : 2009년 12월 8일

Binding Update과정에 공격자가 개입하여 정상적인 MN과 CN간의 통신을 방해할 수 있다[3, 4]. 특히, 정상적으로 MN에게 가야 할 데이터가 공격자에게 도달하도록 세션을 가로채는 것은 위협적인 공격이다. 또한, 임의의 IP에게로 flooding 공격과 CN의 연산성능과 저장 공간을 소모시키는 서비스 거부 공격도 가능하다. 본 논문은 MIPv6의 Binding Update 에서의 보안문제를 해결하기 위해 Hash함수를 활용한 방법을 제시한다. 이를 통해 공격자가 개입하지 못하게 하고, CN은 기존 방법에 비해 연산의 양이 줄어들게 된다. 또한 기존 기법의 메시지 흐름을 그대로 사용하고 있기 때문에 쉽게 사용이 가능하다.

본 논문의 구성은 다음과 같다. 제 2장에서는 MIPv6 Binding Update와 보안 문제점에 대해서 언급한다. 제 3장에서는 이전에 제안된 여러 관련연구에 대해 분석하고, 제 4장은 제안하는 MIPv6의 Binding Update를 제안한다. 제 5장에서는 제안된 방법에 대한 보안분석 및 성능분석을 한다. 제6장에서 논문을 마무리한다.

2. Mobile IPv6의 경로 최적화

이 장에서는 MIPv6의 경로최적화 과정에 대해서 설명한다. MN은 통신을 지속하기 위해, MN이 이동하여 CoA가 바뀌면, 이 CoA를 HA에게 Binding Update메시지를 통해 등록시킨다. 이 메시지는 IPSec을 통해 보호된다. HA는 MN의 HoA로 데이터가 오면, 데이터를 MN이 HA에게 등록한 CoA로 보내준다. 한편, MN은 통신하는 상대방인 CN과 데이터를 주고받기 위해 두 가지 경로를 사용할 수 있다. 첫 번째 경로는 MN의 HoA를 통하여 MN의 정보를 MN의 HA가 재지향 해주는 간접경로이다. 이 때, MN과 HA사이의 경로는 IPSec을 통해 보호되며, 반면에 HA와 CN사이의 경로는 보호되지 않는다. 두 번째 경로인 직접경로는 MN의 CoA를 통해 직접 MN과 CN이 통신하는 것이다. 직접경로는 간접경로에 비해 라우팅이 빠르기 때문에 통신의 성능에 향상을 가져올 수 있다. 직접경로를 사용하기 위해서 MN은 CN에게 Binding Update메시지를 통해 자신의 CoA를 등록시켜, CN이 HoA로 데이터를 전송하던 것을 CoA로 전송하도록 해야 한다. MN이 CN에게 수행하는 Binding Update과정은 (그림 1)와 같이 총 6개의 메시지가 사용된다. 이 중에 다섯 번째 메시지가 실질적으로 MN의 CoA를 CN에게 등록하는 Binding Update 메시지이다. Binding Update메시지를 받은 후 CN이 CoA를 MN의 IP주소로 등록하는 과정에서, CN이 MN의 CoA가 정상적인 MN의 IP주소인지 확인해야 데이터가 MN이 아닌 다른 자에게 전송되는 것을 막을 수 있다. 이를 위해 (그림 1)의 1~4번 메시지에 해당하는 Return Routability(RR)과정을 수행하여 CN은 CoA가 HoA와 동일한 목적지, 즉 MN으로 라우팅 되는지 확인한다. RR과정은 CN이 생성한 두 개의 서로 다른 토큰을 HoA와 CoA로 각기 전송한다. 그리고 Binding Update메시지에서 두 개의 토큰이 사용되어 메시지 인증 코드(MAC)가 생성되었는지 확인하게 된다. 각 메시지의 자세한 내용은 다음과 같다. 우선 MN이 Home Test Init(HoTI)메시지와 Care of Test Init(CoTI)메시지를 CN에게 전달하며 RR과정은 시작된다. HoTI와 CoTI메시지는 CN에게 토큰을 요청하는 메시지이다. 이 두 메시지는 출발지 주소로 HoA와 CoA를 가지고 있기 때문에 서로 다른 경로로 CN에게 전달된다. CN은 HoTI/CoTI메시지를 받으면, HoA와 CoA를 각기 사용하여 토큰을 생성하고, Home of Test(HoT)/Care of Test(CoT) 메시지를 통해 MN에게 전달한다. 각기 토큰은 HoA 혹은 CoA와 CN의 비밀값은 K_{CN}, 그리고 CN이 생성한 랜덤값을 해쉬함수를 사용하여 생성된다. 랜덤값은 CN이 인덱스를 붙여서 저장하고 있으며, 이 인덱스값은 HoT/CoT메시지에 포함되어 있다. CN은 해당 토큰이 어떠한 IP주소와 랜덤값을 사용하여 만들었는지 알 수 있다. MN은 자신의 HoA와 CoA를 사용하여 생성된 두 개의 토큰을 확보하면, 이를 사용하여 Binding Update메시지를 생성한다. (그림 1)에서와 같이 두 개의 토큰에 해쉬함수를 사용하여 K_{BM}값을 생성하고, 이 값을 사용하여 Binding Update메시지의 MAC을 생성하다. Binding Update메시지에는 HoA와 CoA, 두 개의 토큰에 사용되었던 랜덤값을 가리키는 인덱스값들 등이 포함되어 있다. CN은 Binding Update메시지를 받으면, 인덱스들을 통해 두 개의 랜덤값을 얻고, 두 개의 토큰을 생성한 후에 K_{BM}을 생성하고, MAC을 검증하여 정상적으로 RR과정을 거쳐서 MN이 CN이 보낸 두 개의 토큰을 받을 수 있었는지 확인한다. 그리고, MN의 HoA대신에 CoA로 향후 통신을 지속한다.



(그림 1) RFC 3775의 경로최적화

2.1 Mobile IPv6 Binding Update의 문제점

우리는 RFC 3775에서 정의하고 있는 Binding Update의 보안상 문제점의 원인을 세 가지로 분석하였다. 첫째, 간접경로와 집접경로 중에 MN과 HA 구간은 IPSec으로 보호받지만, 그 의외의 보호받지 못한다. 이것은 HA와 CN사이의

구간에서 공격자가 MN의 HoA와 연관을 가지는 토큰을 획득할 수 있음을 의미한다. 둘째, 메시지의 인증이 다섯 번째 메시지인 Binding Update메시지에서 이루어지기 때문에, 악의적인 공격자의 CoTI메시지등을 막을 수가 없다. 셋째, 두 개의 토큰이 서로 독립적으로 구성이 되어 있다. 즉, CN은 Binding Update메시지에 사용되는 토큰이 동일한 MN이 요청하여 생성된 것인지 확인할 수 없다. 각 토큰에는 HoA 혹은 CoA와 CN의 secret만이 포함된다. 따라서, HoA의 토큰은 MN이 요청하여 생성하고, CoA의 토큰은 공격자가 요청하여 생성할 때, 토큰의 생성에 사용된 MN의 HoA, 공격자의 CoA, 두 개의 랜덤값만 옳다면, Binding Update메시지의 공격자의 CoA를 올바른 MN의 IP주소로 인식한다.

그래서 다음과 같은 공격들이 가능하다. 첫째, 공격자는 정상적인 MN의 세션을 가로챌 수 있다. HA와 CN의 사이에 위치한 공격자는 HA와 CN 구간에서 전송되는 암호화되지 않은 MN의 HoA를 사용하여 생성된 토큰을 획득할 수 있다. 그 다음, 공격자는 자신의 CoA로 CN에게 CoTI를 보내고, 토큰을 받는다. 이제, 공격자는 MN의 토큰과 자신의 토큰을 사용하여 CN에게 Binding Update메시지를 전송한다. CN은 Binding Update메시지를 받고, 두 개의 토큰을 정상적으로 재생성하여 Binding Update메시지를 인증하게 된다. 따라서, 향후 MN과 CN의 통신은 공격자의 CoA를 통해 이루어지게 된다. 둘째, 공격자 임의의 IP주소를 향해 Flooding 공격을 가할 수가 있다. 이 공격은 세션 가로채기 공격과 유사한 방법으로 수행할 수 있다. 공격자는 다수의 단말의 HoA가 사용된 토큰들을 확보하고, 임의의 IP주소의 토큰를 사용하여 Binding Update를 시도한다. 이 공격을 통해 공격자는 다수의 MN이 통신이 불가능하게 함과 동시에 임의의 IP주소가 정상적인 동작을 하지 못하게 할 수 있다. 마지막으로, 공격자는 CN에 대해 서비스거부공격(DoS)을 할 수 있다. CN은 Init메시지가 올 때마다, 랜덤값과 토큰을 생성하고 유지하기 위해 메모리를 사용한다. 또한, Key Hash연산을 수행해야 한다. 이를 이용하여, 공격자가 CoTI 메시지로 DoS를 시도하면, CN의 연상능력과 메모리를 소모하게 된다.

3. 관련 연구

MIPv6의 경로최적화의 보안문제는 기존에 여러 논문에서 다루어진 바가 있다. 우선, MN과 CN간에 신뢰관계를 수립하고, 각 메시지를 암호화하여 수행하는 기법들이 주로 제안되어 왔다. Certificate-based Binding Update(CBU)[5], Hierarchical Certificate-Based Binding Update(HCBU)[6], Leakage-Resilient Security Architecture(LR-AKE)[7] 등이 이 분류가 된다. 이들 기법은 공개키 암호화기법을 사용하여 신뢰관계를 수립하고, 암호화하여 Binding Update를 수행하기 때문에 공격자가 이들 메시지를 악의적인 목적으로 수정하거나 개입하지 못한다.

그리고, Greg와 Michael이 제안한 Child-Proof Authentication for MIPv6(CAM)[8]의 경우, 비밀/공개키 쌍을 IPv6의 주소로 활용하는 기법을 적용해서 CoA가 MN이 가지고 있는 IP임을 보장하게 한다. 이는 기존의 IPv6 주소의 생성과는 별개의 방법으로 수행되므로 추가적인 요구사항이 존재하게 된다.

마지막으로 Veigner와 Rong이 제안한 Route Optimization protocol for MIPv6(ROM)[9, 10]의 경우, 위의 예와는 달리 Hash함수를 사용해서 CoA가 MN이 가지고 있음을 CN이 확인할 수 있게 해준다. 하지만, 표준과는 많은 차이가 있고, CoA로 전송되는 데이터가 실제 MN에게 전송되는지 CN이 확인할 수 있는 방법을 제시하고 있지 않다.

4. 제안하는 Binding Update 기법

앞장에서 분석한 바와 같은 문제점을 보완하기 위해서, 우리는 새로운 프로토콜의 요구사항을 도출하고, 이를 만족하는 프로토콜은 제시한다.

4.1 프로토콜 요구사항

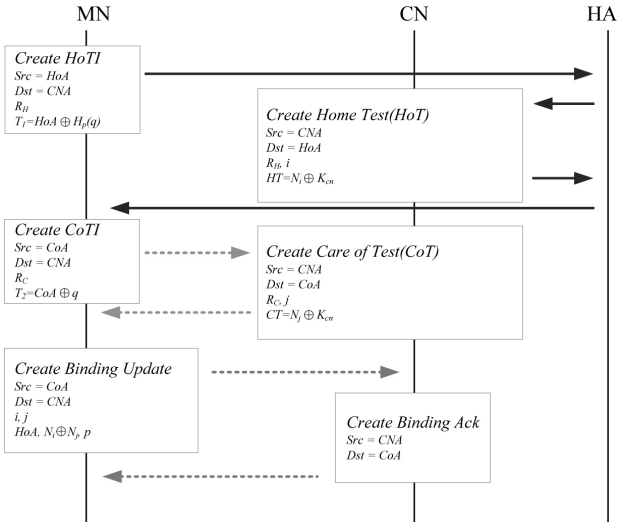
1) ownership : MN은 CN에게 새로운 CoA가 자신이 소유하고 있는 IP주소임을 보여주어야 한다.
2) Routability : 새로운 CoA로 CN이 데이터를 보내는 것은 MN의 HoA로 보내는 것과 동일한 것을 증명해야 한다.
3) Dependency : 기존의 RR과정에서 CN이 생성하는 두 개의 토큰이 아무런 연관성을 가지고 있지 않다. 이는 공격의 주요 원인을 제공하고 있다.
4) Compatibility : 기존의 기법과 차이를 최소한으로 하여 쉽게 구현 및 적용이 가능해야 한다.
5) No Degradation of performance : Binding Update는 단말이 이동하여 네트워크가 변경될 때 사용되며, 이 때 발생하는 지연시간은 성능에 많은 영향을 끼친다. 따라서 새로운 프로토콜은 성능을 떨어뜨리지 않아야 한다.

최초 두 개의 요구사항은 기존의 기법에서의 요구사항과 일치하며, 세 번째 요구사항은 보안상 문제점을 해결하기 위해 필요하다. 그리고 마지막 두 개의 요구사항은 성능에 관한 것이다.

4.2 제안하는 프로토콜

제안하는 프로토콜은 기존의 프로토콜의 메시지 흐름을 그대로 유지하면서 앞에서 살펴봤던 문제점을 해결한다. CN은 생성하는 두 개의 HoT와 CoT메시지 간의 연관성을 MN의 참여하에 생성한다. 자세한 메시지의 구성은 (그림 2)와 같다.

MN은 HoTI와 메시지와 CoTI메시지를 생성해서 각기 경로로 CN에게 전달한다. 이 때, R_H와 R_C는 MN이 생성한 랜덤값이다. 또한 p와 q도 MN이 생성한 임의의 수로, T_1과

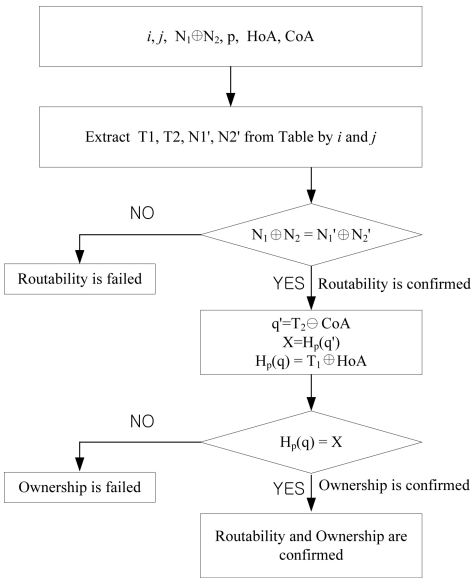


(그림 2) 제안하는 경로최적화 기법

T_2에 생성에 사용된다. $H_p()$는 p를 key로 사용하는 keyed hash 함수이다. 이 때 T_1과 T_2는 $H_p(q)$ 그리고 q가 포함되어 있다. 이 값은 CN으로 전송되면, CN은 테이블을 구축하여 저장하고 있고, 이 테이블에는 인덱스가 부여되며, CN이 HoT와 CoT메시지를 위해 생성할 Ni, Nj도 함께 저장된다. Bindign Update 메시지를 MN이 보낼 때, p를 공개하여 HoTI/CoTI 메시지를 보낸 것이 MN임을 증명하게 된다.

앞서 설명한 바와 같이 HoTI/CoTI메시지를 받은 CN은 HoT/CoT메시지를 <그림 2>와 같이 생성하여 전송한다. 이 때 R_H와 R_C는 HoTI/CoTI메시지에 포함된 값이고, HT와 CT를 생성하는데 사용된 N_i, N_j는 랜덤값이며, T_1/T_2와 함께 저장되며, 후에 인덱스인 i, j를 통해 복원할 수 있다. K_{cn}은 CN의 비밀값이다.

CN으로부터 HoT와 CoT를 받은 MN은 Binding Update



(그림 3) CN의 검증과정

메시지를 생성한다. HoT와 CoT에 포함되어 있던 i, j와 HT와 CT를 XOR연산을 수행한 결과인 N_i XOR N_j, 그리고 p가 Binding Update메시지에 포함된다.

CN은 Binding Update메시지를 받은 후에 (그림 3)과 같이 검증과정을 수행하여 ownership과 routability 를 검증한다. 그리고, 검증을 통과하면 Binding Ack 메시지를 MN에게 전송하고 모든 과정을 종료한다.

5. 성능 분석

제안하는 기법을 보안분석 및 연산속도 및 전송 지연시간을 통해 분석하였다. 기본적으로 메시지의 횟수가 동일하기 때문에 전송 지연시간은 큰 차이는 보이지 않고 있으며, 해쉬 연산의 횟수가 감소하여 연산 속도 면에서 향상을 확인하였다.

5.1 보안분석

제안하는 기법을 사용함으로서, CN은 CoA의 Ownership과 Routability를 보장받게 된다. 이 두 개의 성질은 Mobile IPv6에서 handover시 필요한 최소한의 요구사항이고, 이 장에서는 이 두 가지 요구사항이 어떻게 만족되는지 설명한다.

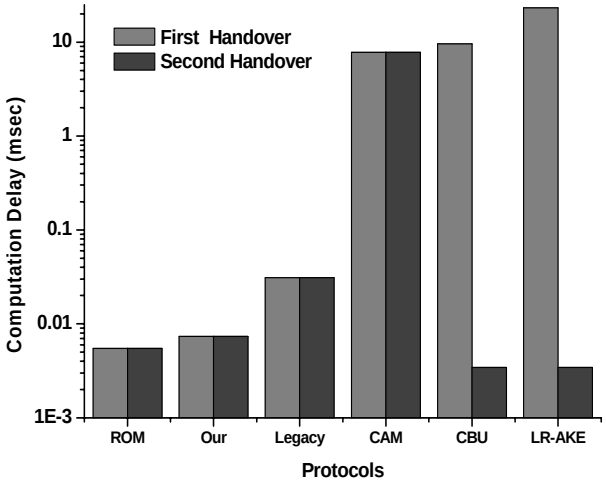
CN이 생성하는 HoT와 CoT메세지에는 두 개의 랜덤값 N_i, N_j가 포함되어 MN에게 전송된다. 이 두 개의 랜덤값은 CN의 비밀값인 Kcn으로 숨겨져 있다. 이점은 MN이 CN의 메시지를 받지 않으면 Ni XOR Nj를 만들지 못하는 것을 의미한다. MN은 N_i XOR N_j를 계산하여 CN에게 전해준다. CN은 자신이 유지하고 있는 랜덤값과 MN으로부터 받은 값을 비교하여 서로 다른 경로로 전달된 두 개의 메시지가 MN에게 전달되었음을 확신할 수 있다.

MN은 최초에 HoTI와 CoTI 메시지를 생성하여 두 개의 경로로 MN에게 전달한다. 이 때, 두 개의 랜덤값인 p와 q를 사용하여 HoTI에는 $H_p(q)$, 그리고 CoTI에는 q가 포함된다. 그리고, Binding Update메시지에 p값이 포함되어 CN에게 전달된다. Hash함수는 $H_p(q)$와 q를 공격자가 알아도, p을 알 수 없도록 한다. 이 점은 공격자가 별도의 CoTI메시지를 만들고, CoT메세지를 받아서 Binding Update에 사용하려해도, p를 알 수 없기 때문에 불가능하게 만든다. p는 유일하게 MN이 알고 있으며 CN에게 제시할 수 있기 때문에, HoTI와 CoTI메시지가 MN이 생성했음을 증명할 수 있게 된다. 이로서 Binding Update메시지를 받은 CN은 HoA와 CoA가 동일한 MN의 소유임을, Ownership을 확신하게 된다.

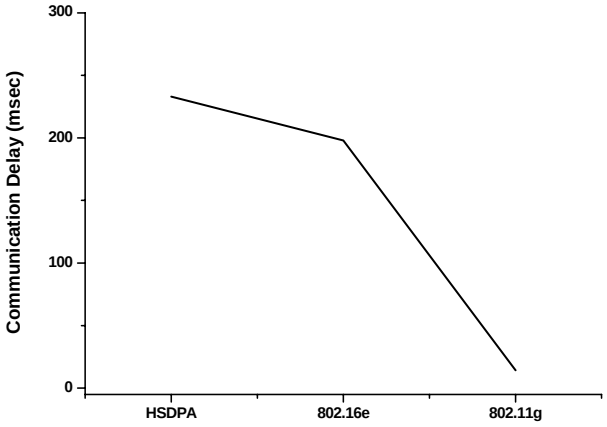
5.2 성능분석

제안하는 기법은 기존 기법과 비교했을 때 동일한 메시지 흐름을 가지고 있기 때문에 전체적인 성능은 기존 기법과 유사하다. 하지만 필요한 연산과 동작흐름이 유사하기 때문에 빠르게 구현 및 적용이 가능한 장점이 있다. 우리는 제안하는 기법을 3장 관련연구에서 언급했던 기법들과 비교하

여 연산 성능을 검증하고, 현재 사용이 가능한 무선 통신망에서 얼마나 성능이 나오는지 확인하였다. 이를 위해 각 기법들의 필요한 연산들을 C언어로 구현하여 성능을 비교하였고, 제안하는 기법은 HSDPA, Wibro, WLAN상에서 실제적으로 지연시간이 얼마나 걸리는지 구현 및 검증하였다. (그림 4)은 제안하는 기법과 기존의 여러 기법들의 연산성능을 비교한 것이다. ROM과 제안하는 기법, 그리고 표준, CAM의 경우 최초 Handover와 그 이후의 Handover간에 연산이 동일하지만, CBU와 LR-AKE의 경우 MN과 CN간의 신뢰관계를 통해 키를 생성하고, 향후 메시지에 대해서는 동일한 키로 암호화하여 수행하므로 두 번째 Handover부터 연산량이 감소하게 된다. 두 번째 Handover의 경우, 제안하는 기법은 0.0074msec, CBU의 경우 0.0034msec로 약 0.002msec 정도 성능에서 떨어진다. 하지만 최초 Handover의 경우 제안하는 기법은 동일하지만, CBU의 경우 9.58msec로 차이가 크게 된다. (그림 5)는 제안하는 기법이 현재 사용이 가능한 무선통신망(Wibro, HSDPA, WLAN)에서의 성능을 보여준다. Wibro와 WLAN는 KT의 서비스를 사용했고, HSDPA는 SK telecom의 서비스를 활용하였다. HSPDA와 Wibro에서는 200msec가 넘는 지연시간을 보여주었다. 이는 실시간 서비스에는 지장을 주는 지연시간으로 문제가 될 수 있다. 하지만 WLAN에서는 크게 감소하여 약 14msec의 지연시간을 보여주었다. 네트워크를 구성하는 다른 부분은 다 동일하기 때문에 Delay의 큰 부분이 무선구간에서의 전파시간으로 파악할 수 있다. 우리는 실험환경에서 WLAN은 하향링크의 속도가 10.3Mbps, 그리고 상향링크의 속도가 9.4Mbps로 이는 향후 차세대 무선 네트워크인 Long Term Evolution (LTE)와 802.16m이 고려하고 있는 30Mbps에 비해 느린 점에 주목하였다[12]. 이는 향후 LTE 혹은 802.16m 등 차세대 네트워크에서는 지연시간이 더 줄어들어 실시간 서비스에서도 적용할 수 있음을 예상해볼 수 있다.



(그림 4) 연산성능 비교



(그림 5) 여러 무선 통신망에서의 전송지연시간

6. 결 론

Mobile IPv6는 Mobility를 지원하는 Key Protocol이다. 기존 Mobile IPv6의 표준은 Routing Optimization에 있어서 안전하게 하려는 노력을 하였다. 이는 새로운 IP주소에 대한 MN의 Ownership과 Routability의 보장으로 달성될 수 있다. 하지만 기존 기법들에서는 이들이 완벽하게 지원되지 않고 있으며, 본 논문은 표준의 메시지 흐름 및 보안 요구사항을 만족하는 새로운 기법을 제안하고 있다. 또한 우리는 요구사항의 만족의 증명과 연산 및 전송지연시간을 구현을 통해 검증하였다. 다른 제안된 기법에 비해 연산적으로는 대체적으로 우수하거나 대등한 성능을 보여주었고, 전송성능은 현재의 무선전송망에서는 실시간 서비스에 부적합하나, 향후 차세대 무선접속망에서는 실시간 서비스에 접목이 가능함을 확인하였다.

참 고 문 헌

[1] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” RFC 3775, June, 2004.

[2] C. Perken, “IP Mobility Support,” RFC 2002, October, 1996.

[3] T. Aura, “Mobile IPv6 Security,” in Security Protocols, 2004, pp.3-13.

[4] K. Elgoarany and M. Eltoweissy, “Security in Mobile IPv6: A survey,” Information Security Technical Report, Vol.12, pp.32-43, 2007.

[5] R. H. Deng, J. Zhou, and F. Bao, “Defending against redirect attacks in mobile IP,” in 9th ACM Conference on Computer and Communications Security (CCS), Washington, 2002, pp.59-67.

[6] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou, and R. H. Deng, “Routing optimization security in mobile IPv6,” Computer Networks, Vol.50, pp.2401-2419, 2006.

[7] H. Fathi, S. SeongHan, K. Kobara, S. S. Chakraborty, H. Imai, and R. Prasad, “Leakage-resilient security architecture for

mobile IPv6 in wireless overlay networks," Selected Areas in Communications, IEEE Journal on, Vol.23, pp.2182-2193, 2005.

[8] O. S. Greg and R. Michael, "Child-proof authentication for MIPv6 (CAM)," SIGCOMM Comput. Commun. Rev., Vol.31, pp.4-8, 2001.

[9] C. Veigner and C. Rong, "A new Route Optimization protocol for Mobile IPv6 (ROM)," in International Computer symposium Taipei, 2004.

[10] C. Veigner and C. Rong, "Flooding Attack on the Binding Cache in Mobile IPv6," 2007.

[11] P. Nikander, J. Arkko, T. Aura, and G. Montenegro, "Mobile IP version 6 (MIPv6) route optimization security design," in Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, 2003, pp.2004-2008 Vol.3.

[12] S. Ortiz, "4G Wireless Begins to Take Shape," Computer, Vol.40, pp.18-21, 2007.

송 세 화

e-mail : dreaminsh@ece.skku.ac.kr

2008년 성균관대학교 정보통신공학부(학사)

2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정

관심분야 : 네트워크 보안, 이동통신망 보안

최 형 기

e-mail : hkchoi@ece.skku.ac.kr

1992년 성균관대학교 전자공학과(학사)

1996년 Polytechnic University in Brooklyn, NY(석사)

2001년 Georgia Institute of Technology in Atlanta, GA(박사)

2001년~2004년 Lancope 근무

2004년~현 재 성균관대학교 정보통신공학부 조교수

관심분야 : 네트워크보안, Traffic characterization and modeling

김 정 윤

e-mail : steal83@ece.skku.ac.kr

2004년~2005년 안철수연구소 인턴사원 근무

2006년 성균관대학교 컴퓨터공학전공(학사)

2008년 성균관대학교 전자전기컴퓨터공학과 (석사)

2008년~현 재 성균관대학교 휴대폰학과 박사과정

관심분야 : 차량 간 통신 보안, Pay-TV 보안, 무선통신망 보안