MIPv6에서 권한위임을 이용한 위치수정 방안

이달원* · 이명훈* · 황일선** · 정회경* · 조인준*

The Binding Update Method using Delegation of Rights in MIPv6

Dal-won Lee* · Myoung-hoon Lee* · Il-sun Hwang** · Hoe-kyung Jung* · In-june Jo*

요 약

IETF mip6 WG에서 MN의 위치를 나타내는 '바인딩정보'를 안전하게 CN에게 송신하여 위치정보를 수정하는 RR프로토콜이 2004년 6월에 RFC 3775로 표준화되었다. 표준화된 RR프로토콜은 시작 주체 및 시점이 MN에 의해 이루어짐으로서 위치정보수정 지연에 따른 홈네트워크의 부담 및 통신 지연 증가를 문제점으로 지적할 수 있다. 또한 보안측면에서 CN과 HA간에 위치하는 공격자에게 취약성을 내포하고 있다.

본 논문에서는 MN의 위치정보 수정권한을 HA로 위임시키는 새로운 위치정보수정 방안을 제안한다. 즉, MN의 위치정보를 HA에 등록시 MN의 개인키로 서명된 위치정보 인증서를 사용하여 등록하고 이 인증서를 HA가 CN에 MN의 위치정보 수정시 사용하는 방안이다. 이를 통해서 위치정보수정에 소요되는 시간을 단축하고 교환되는 메시지 수를 감소시켜 통신부담을 경감시키는 효과를 얻을 수 있다. 또한 CN과 HA간에 위치한 공격자에 대한 보안 취약성을 제거하였다.

ABSTRACT

The RR protocole, proposed in IETF mip6 WG and standardized by RFC 3775 at June 2004, send a message 'Binding Update' that express MN's location information to CN safety and update location information. Standard RR protocole has some problems with initiating the protocol by the MN; it causes to increases in communication load in the home network, to increases communication delay between MN and CN. Also, is connoting vulnerability to against attacker who are on the path between CN and HA in security aspect.

This paper proposes doing to delegate MN's location information update rights by HA new location information update method. That is, When update MN's location information to HA, Using MN's private key signed location information certificate use and this certificate using method that HA uses MN's location information at update to CN be. It decreases the route optimization overhead by reducing the number of messages as well as the using location information update time. Also, remove security weakness about against attacker who are on the path between CN and HA.

키워드

MIPv6, Binding Update, Return Routability, 권한위임(Delegation of Rights), 전자서명(Digital Signature)

*배재대학교 컴퓨터공학과

**한국과학기술정보연구원 슈퍼컴퓨팅센터

접수일자 : 2004. 08. 28

Ⅰ. 서 론

MIPv6에서는 MIPv4와는 다르게 MN(Mobile Node)과 CN(Correspondent Node)간에 위치수정을 기본기능으로 제안하고 있다. 위치수정 방법은 MN의 새로운 위치정보를 CN에게 등록함으로서 이루어진다. 하지만 MN의 위치정보를 CN이 수신하여 등록하는 과정에서 위치정보를 불법적으로 활용할 수 있는 보안 위협요소가 존재한다. 이러한 보안 위협에 대응하여 안전하게 위치정보를 보호하면서 등록할 수 있도록 여러 방안들이 연구되었다.[1, 2, 3] 이들 결과물 중에 IETF mip6(Mobility for IPv6) WG에서 제안한 RR(Return Routability) 프로토콜이 2004년 6월에 RFC 3775[4]로 표준화되었다.

참고문헌 [4]에 의하면 MN이 외부 네트워크로 이동을 하면 항상 자신의 변경된 위치정보를 MN과 HA(Home Agent)간에 안전한 IPsec(Internet Protocol Security) ESP(Encapsulating Security Payload) 채널을 활용하여 HA에 등록한다. 이러한 전제 하에서 참고문헌 [4]의 RR프로토콜의 시작 주체 및 시점은 MN이 된다. 즉, MN이 CN으로부터 첫 번째 패킷을 HA을 경유하여 수신하면 MN이 RR프로토콜을 구동시킴을 의미한다. 여기에서 문제점은 MN의 위치정보를 안전한 IPsec ESP 채널을 통해 HA가 유지하고 있음에도 불구하고 MN이 RR프로토콜의 시작 주체 및 시점이 된다는 점이다.

한편 호스트의 신원(Identity)정보와 위치(Location)정보를 분리하고자 IETF hip(Host Identity Protocol) WG에서는 2004년 6월에 HIP(Host Identity Protocol)을 드래프트 문서[5]로 제안하였다. 참고문헌 [5]에서는 새로운 공개키 기반 인터넷 호스트 신원을 정의하고 이를 인터넷 보안시스템 구축에 활용하는 방안을 제안하고 있다. 따라서 외부의 보안인프라 없이도 호스트 신원을 인증할 수 있다. 이러한 환경에서 공개키를 알고 있는 노드는 개인키로 서명된 메시지를 용이하게 인증할 수 있다. 또한 공개키 기반구조에서 노드 A가 자신의 개인키로 서명하여 인증서를 노드 B에게 발행하고 노드 B는 발행된 인증서를 노드 A를 대신하여 노드 C에게 전달할 수 있다. 즉 노드 B가 노드 A의 권한을 위임받아 노드 A의 역할을 할 수 있다.[6]

이러한 아이디어들을 바탕으로 본 논문에서는 RR프로토콜의 시작 주체 및 시점을 MN에서 HA로 변경함으로서 참고문헌 [4]의 RR프로토콜보다 성능이 개선된 위치수정 방안을 제안하였다. 즉, 제안한 위치수정 방안은 MN의 위치정보 수정권한을 HA로 위임시키는 새로운 위치정보수정 방안을 제안한다. 즉, MN의 위치정보를 HA에 등록시 MN의 개인키로 서명된 위치정보 인증서를 사용하여 등록하고 이 인증서를 HA가 CN에 MN의 위치정보 수정시 사용하는 방안이다. 이를 통해서 참고문헌 [4]의 RR프로토콜보다 위치수정 시간을 단축시키고 교환되는 메시지 수를 감소시켜 통신부담 경감효과를 얻을 수 있다. 그리고 MN의 개인키로 서명된 위치정보 인증서를 사용함으로써 RR프로토콜에서 CN과 HA 사이의 경로에 위치한 공격자에 대한 보안 취약성을 제거하였다.

본 논문의 구성은 다음과 같다. 2장에 위치수정 방안에 관련된 연구들을 정리하였다. 3장에 권한위임을 이용한 위치수정 방안을 제안하였다. 4장에 참고문헌 [4]의 RR프로토콜과 본 논문의 제안방안을 비교하였다. 그리고 5장에 결론을 맺었다.

Ⅱ. 위치수정 방안 관련 연구

IETF RFC 3775로 표준화된 참고문헌 [4]의 RR프로토콜에서는 MN과 CN간에 어떤 보안 인프라 구조도 존재하지 않음을 전제로 한다. 또한 MN이 외부네트워크로 이동을 하면 항상 자신의 위치정보를 IPsec ESP 채널을 사용하여 HA에 등록함을 전제로 한다. 그러나 CN과 HA 사이의 경로에 위치한 공격자에 대해서는 보안 취약성이 존재하지만, 인터넷의 어떤 위치에서나 행할 수 있는 위조된 BU(Binding Update)메시지 사용을 제한할 수 있다.

참고문헌 [4] RR프로토콜의 전체적인 동작절차를 살펴보면 다음 그림 1과 같다.

그림 1에서와 같이 MN이 CN으로부터 HA를 경유하는 첫번째 패킷(그림 1의 ⓪)을 수신했을 때 안전한 위치수정을 위한 RR프로토콜이 시작되며, 메시지 경로들과 메시지들은 다음과 같다.

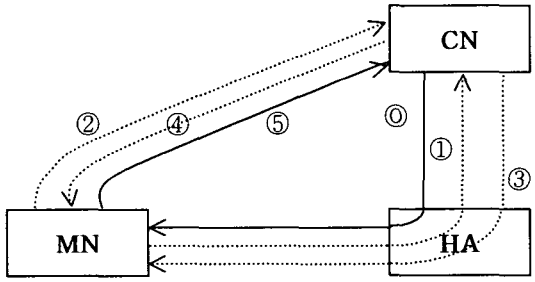

그림 1. 참고문헌 [4]의 위치정보수정
Fig. 1 BU to CN in Reference [4]

① MN→CN(HA 경유): HoTI
② MN→CN: CoTI
③ CN→MN(HA 경유): HoT
④ CN→MN: CoT
⑤ MN→CN: BU메시지

※ HoTI(Home Test Init): (HIC)
※ CoTI(Care-of Test Init): (CIC)
※ HoT(Home Test): (HIC, HNI, HKT)
※ CoT(Care-of Test): (CIC, CNI, CKT)
※ BU메시지: (HoA, seq#, HNI, CNI, HMAC_SHA1 (kbm,(CoA|CNA|BU메시지)))
※ CNA: Correspondent Node Address

참고문헌 [4] RR프로토콜의 특징을 요약하면 다음과 같다.

(1) 최종적인 BU메시지 전달을 위해 총 4개의 메시지(HoTI, HoT, CoTI, CoT)가 교환되며, 이들 메시지가 통과되는 경로는 총 8경로(MN과 CN간 직접 2경로, MN과 HA간 3경로, HA와 CN간 3경로)이다.
(2) CN과 MN간 직접 그리고 HA를 경유하는 서로 다른 두 경로를 통해서 메시지가 송수신되는 이유는 CN에서 MN으로 송신되는 메시지가 MN의 HoA(Home Address)와 CoA(Care-of Address)로 전달이 가능함을 확인하기 위해서이다.
(3) 쿠키(HIC: Home Init Cookie, CIC: Care-of Init Cookie)의 사용은 첫째, HoTI와 HoT 그리고 CoTI와 CoT쌍의 일치성 검증에 사용된다. 둘째, HoTI와 CoTI 메시지를 수신하지 않은 노드에 의해 보내진 위장된 응답을 추출하기 위한 것이다.
(4) 넌스 색인(HNI: Home Nonce Index, CNI: Care-of Nonce Index)을 사용하는 이유는 CN의 넌스값을 노출시키지 않으면서 최종 메시지인 BU메시지를 받을 때 까지 비상태 유지(Stateless) 방식으로 수행됨을 의미한다.
(5) HKT(Home Keygen Token)와 CKT(Care-of Keygen Token)의 역할은 CN과 MN간 직접 그리고 HA를 경유하는 두 경로를 사용하여 CN으로부터 두 메시지(HoT, CoT)를 수신한 MN만이 바인딩관리키(kbm: binding management key) 생성을 통해 BU메시지를 작성할 수 있음을 의미한다. 또한 BU메시지에 포함된 MAC(Message Authentication Code)값을 통해 메시지 무결성 보안 서비스를 제공하며, BU메시지를 받은 CN이 HoA와 발신지 주소인 CoA를 이용하여 MAC값을 생성한 후 BU메시지에 포함된 MAC값과 비교함으로서 메시지 인증 보안 서비스를 제공한다.

참고문헌 [7]에서 제안한 BU 인증 메커니즘은 전체적으로 2단계의 BU 인증과정을 거치도록 하여 바인딩관리키의 보안 취약성을 최소화하였다. 1단계는 상대 노드에게 최초로 BU 인증을 요구할 때 MN과 CN간에 공유키를 생성하여 바인딩관리키를 만드는데 활용한다. 2단계는 이후 이어지는 BU 인증 요구에 1단계에서 협상된 공유키를 사용하여 인증한다. 이 제안은 RR프로토콜에서 바인딩관리키만을 보호하는 측면에서 접근하였다.[7]

참고문헌 [8]에서는 RR프로토콜에서 MN의 위치정보가 MN과 HA간에 IPsec ESP 보안채널을 사용하여 HA에 등록된다는 점에 착안하여 RR프로토콜 시작 시점을 MN에서 HA로 변경하여 위치정보수정 시간을 단축하는 방안을 제안하였다. 이 제안은 RR프로토콜의 성능향상만을 고려하였기 때문에 기존 RR프로토콜의 보안 문제점을 그대로 안고 있다.[8]

참고문헌 [9]에서는 HA와 CN간에 공개키(PKI: Public Key Infrastructure)와 Diffie-Hellman 세션키 생성과정을 통해 보안채널을 생성하여 기존의 RR프로토콜에서 HA와 CN간에 위치한 공격자에 취약한 보안성을 제거하였다. 하지만 이의 지원을 위한 인프라구조의 복잡성 때문에 성능상의 과부하 문제점을 안고 있다.[9]

III. 권한위임을 이용한 위치수정 방안 제안

3.1 개 요

MIPv6에서 MN과 CN간에 최적경로 설정을 위해서는 MN의 위치정보가 CN에 등록되어야 한다.

하지만 CN에 MN의 위치정보가 잘못 등록될 경우에는 심각한 보안 취약성을 지닌다.[10] 제 II 장에서 살펴본바와 같이 안전하게 MN의 위치정보를 CN에게 등록하는 여러 방안이 제시되었다. 하지만 IETF mip6 WG에서 RFC 문서로 제안한 RR프로토콜을 비롯하여 각각의 방안이 성능 및 보안상의 문제점을 지니고 있다.

본 논문에서는 이러한 문제점 개선을 위해 첫째, 모든 MN이 공개키와 개인키 쌍을 생성하여 동작하고, 둘째, DNS를 통해서 MN의 공개키를 분배하고, 셋째, 모든 통신 노드는 도메인 이름으로 통신을 시작하고, 넷째, MN의 위치정보 인증서 및 이를 통한 권한위임 개념 등을 도입하여 새로운 위치정보 수정방안을 제안하였다. 이렇게 함으로써 제 II 장에서 살펴본 여러 제안들보다 성능 및 보안성이 우수한 위치수정방안을 이룩하였다.

3.2 제안 시스템 구조

제안 시스템은 그림 2에서 본바와 같이 크게 4개의 구성 요소(MN, HA, CN, DNS)로 이루어진다. 이들 각각을 설명하면 다음과 같다.

MN은 참고문헌 [4]에서 정의한 기능에 다음의 기능을 추가적으로 행한다. 첫째, 자신의 {공개키(K+MN), 개인키(K-MN)}쌍을 생성하여 개인키는 자신이 보관하고, 공개키는 MN의 HA와 DNS에 각각 등록한다. 둘째, MN의 위치정보 인증서((HoA, CoA)K-MN)를 생성하여 BU메시지에 피기백시켜 HA에 등록하는 기능을 한다.

HA는 참고문헌 [4]에 정의된 기능에 다음의 기능을 추가적으로 행한다. 첫째, MN의 BU메시지로부터 피기백되어 수신한 위치정보 인증서를 MN의 공개키로 검증하고 이를 보관한다. 둘째, 검증된 인증서 내의 MN의 위치정보를 등록한다. 셋째, CN으로부터 MN으로 향하는 첫 번째 패킷을 수신하면 MN의 위치정보 인증서가 피기백된 BU메시지를 CN에 전송한다.

CN은 참고문헌 [4]에 정의된 기능에 다음의 기능을 추가적으로 행한다. 첫째, DNS로부터 MN의 도메인 이름에 대응하는 IP주소 및 MN의 공개키를 분배 받아 등록한다. 둘째, HA로부터 수신된 BU메시지 내의 MN의 위치정보 인증서를 등록되어 있는 MN의 공개키로 검증한다. 셋째, 검증된 위치정보 인증서 내의 MN의 위치정보를 자신의 BCE(Binding Cache Entry)에 등록한다.

마지막으로 DNS는 DNS 고유기능에 MN이 요구한 MN의 공개키를 추가적으로 유지한다. 그리고 CN으로부터 MN의 도메인 이름에 대응하는 IP주소 반환 시 MN의 공개키도 추가적으로 반환한다.

3.3 제안 시스템 동작절차

제안 시스템의 동작절차는 3.2절에서 정의한 구성요소를 바탕으로 다음 그림 2와 같이 동작한다.

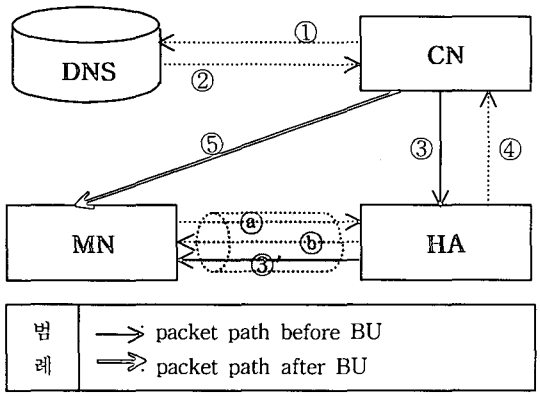

그림 2. 제안 시스템 구조
Fig. 2 Proposal System Structure

그림 2에서 MN의 위치정보 수정흐름을 중심으로 제안시스템의 동작절차를 살펴보면 다음과 같다.

먼저 MN이 새로운 위치로 이동했을 때 MN과 HA간의 동작절차는 아래의 (step 1)~(step 4)와 같다.

(step 1) MN이 외부네트워크로 이동하여 새로운 IP주소를 부여 받으면 위치정보 인증서를 생성하여 BU메시지에 피기백시켜 HA에게 전송한다(그림 2에서 ⓐ).

ⓐ MN→HA: BU{HoA, seq#, (HoA, CoA)K-MN}

위 메시지에서 seq#는 MN이 보낸 BU메시지에 대응되는 BA(Binding Acknowledgement)메시지를 수신할 때 두 메시지에 대한 일치성 검증을 위한 것이다. (HoA, CoA)K-MN은 MN이 HA에게 위치정보 수정권한을 위임하기 위한 위치정보 인증서이다.

(step 2) HA가 (step 1)의 BU메시지를 수신하면 다음의 절차에 따라 MN의 위치정보를 HA의 BCE에 등록한다.

첫째, BU메시지로부터 HoA를 추출하여 HA가 보유하고 있던 HoA에 대응하는 MN의 공개키

(K+MN)를 획득한다. 둘째, 획득된 MN의 공개키로 위치정보 인증서((HoA, CoA)K-MN)를 검증하고 이를 보관한다. 셋째, 검증된 위치정보 인증서에서 MN의 위치정보((HoA, CoA))를 추출하여 BCE를 생성한다.

(step 3) BU메시지를 수신한 HA는 BU메시지에 대한 처리결과(정상처리 또는 에러발생)를 BA메시지를 통해서 MN에게 전송한다(그림 2에서 ⓑ).

ⓑ HA→MN: BA{seq#, BU메시지 처리결과}

seq#는 이전의 BU메시지에 대응되는 BA(Binding Acknowledgement)메시지임을 나타내는 식별자이다.

(step 4) MN이 BA메시지를 수신하면 다음의 절차에 따라 처리한다.

BA 메시지의 seq#를 추출한 후 자신이 보낸 BU메시지에 적용한 seq# 값과 비교하여 적절한 BA메시지임을 판단한다. 그리고 BU메시지 처리결과 항목에 따라 MN의 위치정보가 HA에 수정유무를 확인한다.

다음으로 제안 시스템에서 정의한 CN이 MN과 통신을 시작할 경우 구체적인 동작절차는 아래의 (step 1)~(step 5)와 같다.

(step 1) CN이 MN의 IP주소와 공개키를 반환받기 위해 MN의 DN(Domain Name)을 DNS에게 전송한다(그림 2에서 ①).

① CN→DNS: {MN의 DN}

(step 2) DNS가 MN의 DN에 대응하는 IP주소와 공개키를 반환한다(그림 2에서 ②).

② DNS→CN: {MN의 IP주소, 공개키}

(step 3) 이를 수신한 CN은 MN의 공개키를 보관하고 취득된 IP주소로 첫 번째 패킷을 전송한다(그림 2에서 ③).

③ CN→HA: {MN으로 향하는 첫 번째 패킷}

(step 4) 이를 수신한 HA는 첫째, MN에게 수신된 첫 번째 패킷을 보낸다(그림 2에서 ③'). 둘째, HA가 보관하고 있는 MN의 위치정보 인증서를 BU메시지에 피기백시켜 CN에게 보낸다(그림 2에서 ④). 즉, MN으로부터 위치정보 인증서를 통해서 위임받은 위치정보수정 권한을 대행한다.

③' HA→MN: {MN으로 향하는 첫 번째 패킷}
④ HA→CN: BU{HoA, (HoA, CoA)K-MN}

위의 BU메시지에서 HoA는 CN이 보관하고 있는 MN의 공개키를 추출하기 위한 것이고, (HoA, CoA)K-MN은 MN의 위치정보 인증서이다.

CN이 HA로부터 전송된 BU메시지를 수신하면 다음의 절차에 따라 MN의 위치정보를 CN의 BCE에 등록한다.

BU메시지를 수신한 CN은 다음과 같이 이를 검증한다. BU메시지로부터 HoA를 추출하고 이를 이용하여 자신이 보관하고 있는 MN의 공개키를 획득한다. 획득된 MN의 공개키를 이용하여 BU메시지 내의 MN의 위치정보 인증서를 검증한다. 검증이 완료된 MN의 위치정보를 자신의 BCE에 등록한다.

(step 5) CN에 MN의 위치정보가 등록이 완료되면 그 이후의 MN과 CN간의 통신은 HA를 경유하지 않고 등록된 MN의 위치정보를 이용하여 직접통신하게 된다(그림 2에서 ⑤).

⑤ CN→MN: {BCE 등록후 MN으로 향하는 패킷}

IV. 권한위임을 이용한 위치수정 방안 비교

4.1 비교 기준

제안 시스템의 비교 평가를 위해 크게 성능과 보안성 비교를 실시하였다. 비교평가에 본 논문의 제안방안과 제 II 장에서 살펴본 여러 방안들 중 비교 대상 선정을 위해 표 1에 위치수정 방안들에 대한 비교 내용을 정리하였다.

표 1. 위치수정 방안 비교
Table. 1 BU methods comparison

비교 항목	참고문헌				제안 방안
	[4]	[7]	[8]	[9]	
BU to HA	IPsec	IPsec	IPsec	IPsec	권한 위임
BU 시작주체	MN	MN	HA	MN	HA
전체 메시지수	6	6	5	9	1
전체 경로수	8	8	6	9	1
도달가능성	O	O	O	X	X
보안 특징	취약	안전	취약	안전	안전
공개키 유무	X	O	X	PKI	O
기타 특징	RFC 3775	암복호화	성능 향상	보안 채널	전자 서명

첫째, 성능 비교대상으로 IETF RFC 3775의 RR 프로토콜[4]을 선정하고 참고문헌 [8]을 참고로 하였다. 이유는 참고문헌 [7]과 [9]는 RR프로토콜에서 보안 취약성 개선을 위한 제안으로서 RR프로토콜의 기본골격을 그대로 유지하기 때문이다. 하지만 참고문헌 [8]은 본 논문에서 제안하는 방안과 동일하게 BU메시지 시작 주체가 HA이기 때문에 상대적인 비교 대상이 될 수 있다. 따라서 참고문헌 [4]를 기준으로 성능평가를 하였고 참고문헌 [8]에 대해서는 상대적 비교평가를 실시하였다.

둘째, 보안성 비교대상으로는 참고문헌 [4]의 보안 취약점을 개선한 방안인 참고문헌 [7]과 [9]를 비교 대상으로 선정할 수 있다. 그러나 참고문헌 [9]의 경우에는 HA와 CN간에 PKI 기반의 공개키와 Diffie-Hellman 세션키를 이용한 인프라구조의 복잡성 때문에 이동노드에 적합하지 않다고 판단되어 비교 대상에서 제외하였다.

4.2 성능 비교

우선, 참고문헌 [4]와 본 논문의 제안방안과 성능 비교 평가를 위해서 두 프로토콜의 상세한 동작 절차를 그림 3과 그림 4에 각각 보여주고 있다. 두 그림을 바탕으로 프로토콜의 성능을 다음과 같이 3가지 측면에서 비교할 수 있다.

첫째, 위치수정에 필요한 메시지가 네트워크를 통과하는 경로 수를 비교할 수 있다. 이는 네트워크 부하에 영향을 주는 요소이다. 그림 3과 그림 4에서 BU메시지를 포함하면 참고문헌 [4]는 총 9개인데 반해 제안방안에서는 2개이다. 이는 전체적인 네트워크 부담을 경감시키고 있음을 의미한다.

둘째, CN이 'first packet' 전송 후 CN에서 MN에 대한 BCE 생성까지 소요되는 위치수정 시간을 비교할 수 있다. 이는 BCE가 생성되기 전에 MN으로 보내지는 패킷들(first packet, HoTI, HoT)은 HA를 경유하기 때문에 이 패킷들에 대한 소요시간이 단축될수록 홈네트워크 및 HA의 부하를 경감시키기 때문이다. 그림 3과 그림 4에서 위치수정 시간은 다음 식 ①과 ② 같이 계산할 수 있다.

위치수정 시간 =N(노드에서 메시지 처리 및 생성시간)+T(메시지 전송시간)

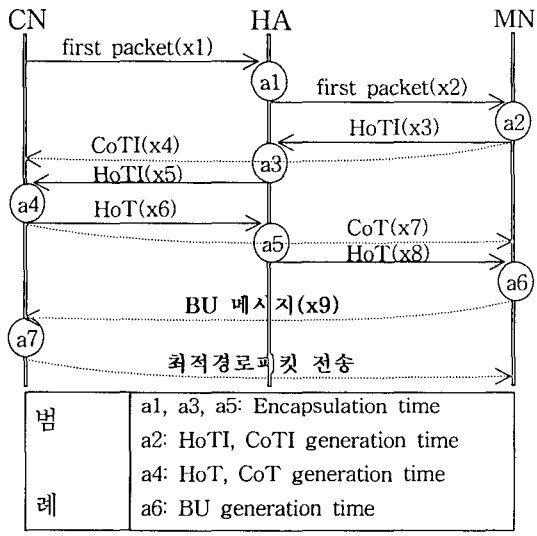

그림 3. 참고문헌 [4] 위치수정 시간
Fig. 3 BU time to CN in Reference [4]

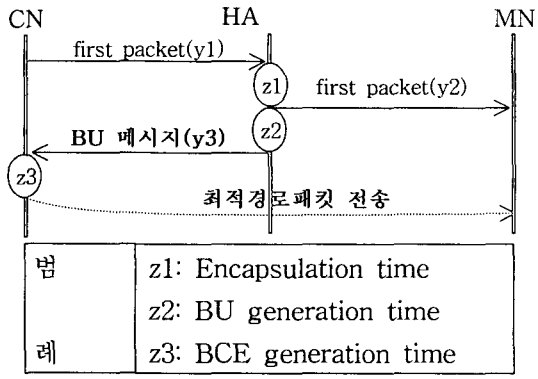

그림 4. CN에 권한위임을 이용한 위치수정 시간
Fig. 4 BU time to CN using Delegation of Rights

참고문헌 [4]의 위치수정 시간=N(a1 + a2 + a3 + a4 + a5 + a6 + a7)+T(x1 + x2 + x3 + x5 +

x6 + x8 + x9) …①

제안방안의 위치수정 시간=N(z1 + z2 + z3) +T(y1 + y2 + y3) …②

먼저 식 ①과 ②에서 메시지 처리 및 생성시간인 N을 살펴보면 다음과 같다.

인켑슐레이션 시간은 참고문헌 [4]와 제안방안 모두 같다고 가정한다. 즉, 그림 3에서 a1, a3, a5 각각은 그림 4에서 z1 시간과 같다. 그리고 그림 3에서 a6는 MN이 수신한 HoT와 CoT 메시지의 HKT와 CKT를 이용하여 바인딩관리키를 생성한 후 이를 이용하여 (CoA, CNA, BU메시지)를 해쉬한 값과 (HoA, seq#, HNI, CNI)로 구성된 BU메시지를 생성하는 시간이다. 이에 반해 그림 4에서 BU메시지 생성 시간인 z2는 MN으로부터 수신했던 위치수정 인증서((HoA, CoA)K-MN)와 HoA로 구성되기 때문에 그림 3의 a6에 비해 짧게 소요된다. 마지막으로 그림 3에서 a7은 CN이 수신한 BU메시지의 구성요소로부터 HKT와 CKT를 생성한 후 이를 이용하여 바인딩관리키를 생성하고 이를 이용하여 (CoA, CNA, BU메시지)를 해쉬한 값과 CN이 수신한 BU메시지의 해쉬값을 비교하여 검증한 후 두 값이 일치한다면 BCE를 생성하는 시간으로 구성된다. 이에 반해 그림 4에서 BCE 생성 시간인 z3는 BU메시지에 포함된 HoA를 이용하여 DNS에 해당 MN의 공개키를 조회한 후 조회된 공개키값으로 위치수정 인증서를 복호화한 후 복호화가 성공하였다면 위치수정 인증서에 포함된 CoA를 이용하여 BCE를 생성하기 때문에 그림 3의 a7과 근접한 소요시간이 된다. 이를 반영하여 두 프로토콜의 메시지 처리 및 생성시간인 N을 계산하면 식 ①과 ②가 다음 식 ③과 ④ 처럼 정리된다.

참고문헌 [4]의 N 시간=a2+a3+a4+a5 …③
제안방안의 N 시간 = 0 …④

식 ③과 ④가 의미하는 것은 제안방안이 참고문헌 [4]보다 메시지 처리 및 생성시간인 N에서 (a2 + a3 + a4 + a5) 시간 만큼 빠르다는 것을 나타낸다.

다음으로 메시지 전송시간인 T를 살펴보면 다음과 같다. 참고문헌 [4]에서 MN과 CN간의 메시지 전송은 두 방향으로 이루어진다. 한 방향은 MN과 CN간에 직접 이루어지고, 다른 방향은 HA를 경유하여 이루어진다. 전자의 메시지 전송시간은 후자의 메시지 전송시간보다 빠르다. 따라서 메시지 전송시간의 비교를 위해서는 후자의 전송시간만을 고려할 수 있다. 이를 반영하여 생성한 식이 참고문헌 [4]에서 T 시간과 제안방안에서 T 시간이다.

상기의 두 방안의 각 단계별 전송시간을 비교하면 x1 = y1, x2 = y2, x5 = y3 관계가 성립된다. 따라서 위 식에서 동일한 전송시간을 소거하면 다음과 같은 식 ⑤와 ⑥을 얻을 수 있다.

참고문헌[4]의 T 시간 = x3 + x6 + x8 + x9 …⑤
제안방안의 T 시간 = 0 …⑥

따라서 제안방안이 참고문헌 [4]보다 메시지 전송시간인 T에서 (x3 + x6 + x8 + x9) 시간 만큼 빠르다는 것을 나타낸다.

위에서 두 프로토콜의 비교를 위해 메시지 처리 및 생성시간인 N과 메시지 전송시간인 T를 반영하면 다음과 같은 위치수정 시간을 식 ⑦과 ⑧처럼 계산할 수 있다.

참고문헌 [4]의 위치수정 시간
=(a2+a3+a4+a5)+(x3+x6+x8+x9) …⑦
제안방안의 위치수정 시간 = 0 …⑧

위의 식 ⑦과 ⑧에서 살펴본바와 같이 제안방안이 참고문헌 [4]보다 전체적인 위치수정에 소요되는 시간에서 {(a2+a3+a4+a5)+(x3+x6+x8+x9)} 만큼 빠르게 생성함을 의미한다.

셋째, 제안방안에서 HA의 부하 비교이다. 참고문헌 [4]에서는 HA가 단순히 인켑슐레이션 기능만을 담당하는데 반해 제안방안에서는 MN이 송신한 위치수정 인증서와 해당 MN의 HoA로 구성된 BU메시지를 생성하여 CN에게 송신하는 기능을 추가하고 있다. 즉, 제안방안에서는 BU메시지 생성시간이 추가적 부담이다. 그러나 이는 MN이 보내온 위치수정 인증서와 해당 MN의 HoA로 구성된 패킷의 생성이기 때문에 소요시간이 짧다. 그리고 둘째 비교분석에서 본 바와 같이 제안방안에서 HA를 경유하는 패킷 수가 감소되기 때문에 이러한 HA 부담을 상쇄할 수 있다.

상기의 성능비교 분석결과를 정리하면 다음과 같은 이점이 있다. 첫째, HA가 MN으로 향하는 첫 번째 패킷 수신 시점에서 제안방안이 시작되기 때문에 CN에서 MN으로 전송되는 패킷의 최적경로 설정 확률을 높인다. 이는 HA를 경유하는 패킷의 수를 줄임으로서 통신지연 현상 및 네트워크 부하를 경감시킴을 의미한다. 둘째, MN이 보내온 단순한 위치수정 인증서를 이용하여 HA가 CN에게 직접 BU메시지를 보냄으로서 참고문헌 [4]에서 CN과 MN간 직접 그리고 HA를 경유하는 두 경로를 이용하여 전송하게 되는 HoTI, CoTI, HoT, CoT

메시지가 제거되어 네트워크의 부하를 줄인다.

다음으로 본 논문의 제안방안과 참고문헌 [8]과의 비교 평가를 위해 참고문헌 [4]와 참고문헌 [8]의 성능 비교 결과를 살펴보면 다음과 같다.

참고문헌 [8]의 위치수정 시간 = 0 …⑨
참고문헌 [4]의 위치수정 시간
=(a1 + a5) + (x2 + x3) …⑩

위의 식 ⑩을 기준으로 상대 비교하기 위하여 그림 3을 살펴보면 a1 = a3, x2 = x8 관계가 성립함을 알 수 있다. 따라서 식 ⑩을 ((a3 + a5) + (x8 + x3))으로 변화가 가능하다. 결국 제안방안과 참고문헌 [8]을 변화된 식 ⑩을 적용하여 소거하면 다음과 같은 식 ⑪과 ⑫을 얻을 수 있다.

참고문헌 [8]의 위치수정 시간
=(a2 + a4) + (x6 + x9) …⑪
제안방안의 위치수정 시간 = 0 …⑫

위의 식 ⑪과 ⑫에서 살펴본바와 같이 제안방안이 참고문헌 [8]보다 전체적인 위치수정에 소요되는 시간에서 {(a2 + a4) + (x6 + x9)} 만큼 빠르게 생성함을 의미한다.

4.3 보안성 비교

참고문헌 [4]는 여러 보안 취약성을 내포하고 있다. 이의 개선을 위해 참고문헌 [7]이 제안되었다. 이들을 대상으로 본 논문의 제안 방안에 대한 보안성을 비교하면 다음과 같다.

먼저 참고문헌 [4]의 보안 취약점을 살펴보면 다음과 같다. 참고문헌 [4]에서도 기술하였듯이 MN과 HA간의 IPsec ESP 보호 경로를 제외한 나머지 경로에서는 평문을 통해 RR프로토콜이 동작되기 때문에 보안 취약성이 존재한다. 즉, CN과 MN 사이 그리고 CN과 HA 사이에서 전달되는 메시지는 암호화되지 않음을 의미한다.

다음으로 참고문헌 [4]와 [7]을 본 논문의 제안방안과 3 가지 측면에서 보안성을 비교하면 다음과 같다.

첫째, MitM(Man-in-the-Middle) 공격에 대한 안전성 분석이다. 참고문헌 [4]에서 만약 공격자가 MN-CN, HA-CN의 두 경로 모두 접근 가능할 경우 바인딩관리키를 생성할 수 있어 전송되는 패킷의 내용을 변경하여 MitM 공격을 수행할 수 있다. 이에 대해 본 논문의 제안방안에서는 참고문헌 [7]의 제안방안 중 두 번째 제안방안과 유사한 방법을 적용하였다. 즉, MN의 개인키를 이용한 BU메시지의 전자서명을 통해 MN만이 위치정보 인증서를 생성할 수 있다는 묵시적인 인증을 제공한다. 따라서 MN의 개인키를 알지 못하는 공격자는 MN을 위장하여 정당한 형태의 BU메시지를 생성할 수 없어 MitM 공격은 불가능하게 된다.

둘째, DoS(Denial of Service) 공격에 대한 안정성 분석이다. DoS 공격을 방어하기 위해서는 양 상대 노드가 각 상대 노드에 대한 확실한 인증을 확보하기 전에는 그 노드에 대한 어떠한 정보라도 생성(저장)하지 않음으로써 달성할 수 있다. 이에 대해 본 논문의 제안방안에서는 참고문헌 [7] 그리고 참고문헌 [4]에서 제안한 방법과 동일한 방법을 적용하였다. 즉, HA가 전송한 MN의 위치정보 인증서가 피기백된 BU메시지에 대하여 MN의 공개키를 적용한 검증후에 CN의 BCE에 MN의 위치정보를 생성하거나 수정하기 때문에 DoS 공격에 대한 위협을 최소화하였다.

셋째, 이전의 세션키가 노출되는 경우의 안정성 분석이다. 암호 시스템에서 매 세션마다 동일한 키를 이용하여 암호문을 생성하는 경우에 한 세션의 키만 노출되면 이전의 모든 암호문이 공개되므로 매 세션마다 서로 다른 키를 사용하여 메시지를 암호화하는 것이 바람직하다. 이에 대해 본 논문의 제안방안에서는 참고문헌 [4]에서 사용된 바인딩관리키 그리고 참고문헌 [7]에서 사용된 세션키들이 사용되지 않았다. 결과적으로 MN이 생성한 개인키가 노출되지 않는다는 전제에서 본 논문의 제안 시스템이 참고문헌 [4] 그리고 참고문헌 [7] 보다도 단순한 구조임을 알 수 있다.

상기의 보안성비교 분석결과를 정리하면 다음과 같다. 첫째, 참고문헌 [4]에서 내포하고 있는 CN과 HA간에 위치한 공격자에 대한 보안 취약성이 참고문헌 [7]에서 제시한 세가지 보안성 분석을 통해 본 논문의 제안방안에서 제거됨을 알 수 있다. 둘째, 이전의 세션키가 노출됨으로 인해서 파생되는 보안 취약성 문제는 상기의 '셋째'항의 안정성 분석을 통해 알 수 있듯이 본 논문에서 제안방안이 참고문헌 [4] 그리고 참고문헌 [7] 보다 단순한 구조를 가지면서도 참고문헌 [7]과 동일한 보안수준을 유지하고 있음을 알 수 있다.

V. 결 론

본 논문에서는 각각의 노드들이 공개키를 생성하여 전자서명에 활용한다는 환경에서 참고문헌 [4] RR프로토콜에 내재한 보안 취약성을 제거하면

서 성능이 향상된 위치정보수정 방안을 제안하였다. 참고문헌 [4]와 마찬가지로 MN의 변경된 위치정보를 HA에 등록하지만 본 제안방안에서는 단순한 위치수정 인증서를 이용하여 MN의 위치정보수정 권한을 HA에게 위임함으로서 위치수정 시작 주체 및 시점을 HA로 변경하였다. 이를 통해서 위치수정에 소요되는 시간을 단축하고 교환되는 메시지 수를 감소시켜 통신부담을 경감시키는 효과를 얻을 수 있음을 보였다. 또한 HA와 CN 사이의 경로에 위치한 공격자에 대한 보안 취약성이 제거됨을 보였다.

참고문헌

[1] M. Roe, T. Aura, G. O'Shea, J. Arkko, "Auth- entication of Mobile Ipv6 Binding Updates and Acknowledgements," <draft-roe-mobileip- updateauth-02.txt>, February 2002.

[2] C. Perkins, D. Johnson, "Mobility Support in Ipv6," <draft-ietf-mobileip-ipv6-21.txt>, February 2003.

[3] P. Nikander, C. Perkins, "Binding Authentication Key Establishment Protocol for Mobile Ipv6," <draft-perkins-bake-01.txt>, July 2001.

[4] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, June 2004.

[5] R. Moskowitz, P. Nikander, P. Jokela, T. He- nderson, "Host Identity Protocol," <draft-ietf- hip-base-00.txt>, June 2004.

[6] P. Nikander, J. Arkko, "Delegation of Signalling Rights," Security Protocol Workshop 2002.

[7] 임강규, 남길현, "Mobile IPv6 BU(Binding Up- dates)인증 방안에 관한 연구," CISC-W' 03, 2003년 12월.

[8] 나재훈, 이달원, 손승원, 조인준, "MIPv6에서 RR프로토콜 성능개선 방안," CISC-W'03, 2003년 7월.

[9] Robert H. Deng, Jianying Zhou, Feng Bao, "Defending against redirect attacks in mobile IP," ACM Conference on Computer and Communications Security 2002.

[10] A. Mankin, B. Patil, D. Harkins, E. Nordmark, P. Nikander, P. Roberts, T. Narten, "Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6," <draft-ietf-mobileip-mipv6-scrty-reqts-02. txt>, November 2001.

저자소개

이달원(Dal-won Lee)

1996년 충남대학교 화화과 이학사
2000년 배재대학교 컴퓨터공학과 공학석사
2001년~현재 배재대학교 컴퓨터공학과 박사과정
※관심분야 : 정보보호, 컴퓨터네트워크

이명훈(Myoung-hoon Lee)

2001년 배재대학교 컴퓨터공학과 공학사
2003년 배재대학교 컴퓨터공학과 공학석사
2003년~현재 배재대학교 컴퓨터공학과 박사과정
※관심분야 : 컴퓨터통신, 정보보호, 무선인터넷

황일선(Il-sun Hwang)

1996년 시스템공학연구소 실장
1998년 한국전자통신연구원 초고속정보망 실장
현재 한국과학기술정보연구원 초고속연구망사업실 실장
※관심분야 : Grid 네트워킹, IPv6 네트워킹

정회경(Hoe-kyung Jung)

1985년 광운대학교 컴퓨터공학과 공학사
1987년 광운대학교 컴퓨터공학과 공학석사
1993년 광운대학교 컴퓨터공학과 공학박사
1994년~현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 멀티미디어, 문서정보처리, XML, SVG, Web service, MPEG-21

조인준(In-june Jo)

1982년 전남대학교 계산통계학과 공학사
1985년 전남대학교 전자계산학과 공학석사
1999년 아주대학교 컴퓨터공학과 공학박사
1983년~1994년 한국전자통신연구원 선임연구원
1991년 전산조직응용기술사
1994년~현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 정보보호, 컴퓨터네트워크