위치 확인을 위한 효율적인 모바일 IPv6 바인딩 갱신 기법 연구

김미주*, 염흥열*

*순천향대학교 공과대학 정보보호학과

An Efficient Mobile IPv6 Binding Update for Validating Attachment Point of Mobile Node

Mi-Joo Kim*, Heung-Youl Youm*

*Department of Information Security Engineering, SoonChunHyang University.

요 약

모바일 IPv6 환경에서 모바일 노드와 대응 노드간의 바인딩 갱신에 관한 많은 연구가 활발히 진행 중에 있다. 하지만, 지금까지 제안된 대부분의 프로토콜이 바인딩 갱신 메시지에 대한 요청자와 응답자 인증 그리고 갱신 정보의 무결성에 대한 최적의 프로토콜을 찾고자 하고 있지만, 바인딩 갱신을 요청하는 노드의 위치 검증에 대해서는 요청메시지에 대한 응답 메시지를 수신함으로써 간접적인 확인만을 하고 있다. 본 논문에서는 공인 인증체제의 인가 인증서를 바탕으로 효율적인 위치 확인을 제공하는 모바일 IPv6 바인딩 업데이트 기법을 제안한다.

I. 서론

IETF에서는 모바일 IPv6 환경에서 홈 링크에 있던 노드가 외부 링크로 이동해 갔을 경우, 기존에 통신하고 있던 대응노드와의 연결을 지속하고 최적의 경로를 사용하기 위해 RR(Return Routability) 기법을 이용하는 것을 권고하고 있다[1]. 또한 RR기법만으론 모바일 IPv6 보안 요구사항들을 모두 만족시켜주지 않기 때문에 IPsec을 이용하여 바인딩 갱신을 수행할 것을 권장하고 있다[2]. 하지만 단기간의 연결 세션이나 저전력의 모바일 장치에 IPsec을 사용하는 것은 효율성이 떨어 질 수 있다. 이를 극복하기 위해 많은 기법들이 제안되고 있다. 하지만 RR 기법을 비롯한 제안된 대부분의 기법들이 요청자나 응답자에 대한 인증과 바인딩 갱신 정보에 대한 무결성을 보장하지만, 바인딩 갱신을 요청하는 요청자가 자신이 주장하는 주소의 위치에 존재하는지에 검증은 요청메시지에 대한 응답 메시지를 수신함으로써 간접적인 위치 확인만을 하고 있다.

본 논문에서는 공인된 인프라를 바탕으로 효율적인 위치 확인을 제공하는 모바일 IPv6 바인딩 갱신 기법에 대해 제안한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 바인딩 갱신 보안 요구사항에 대해서 설명하고, Ⅲ장에서는 기존 모바일 IPv6 바인딩 갱신 프로토콜에 대해서 설명하고, Ⅳ장에서는 제안 기법을 설명하고, 마지막으로 Ⅴ장에서 결론을 맺도록 한다.

II. 바인딩 갱신 보안 요구사항

바인딩 갱신 과정을 안전하게 수행하지 않는 경우 서비스 거부(Denial-of-Service) 공격, 경로 변경(redirect) 공격, 이웃 폭격(neighbour

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음

bombing) 공격 등에 취약할 수 있기 때문에[2], 바인딩 갱신은 다음과 같은 보안 요구사항을 만족해야 한다[7].

- 요청자 인증: 바인딩 갱신 메시지를 수신하는 노드는 반드시 요청자를 인증할 수 있어야 한다.
- 응답자 인증: 바인딩 갱신을 요청하는 응답자를 인증할 수 있어야 한다.
- 바인딩 갱신 정보의 무결성: 바인딩 갱신 정보는 다른 공격자들로부터 보호되어야 한다.
- 요청자 위치 인증: 응답자는 요청자가 현재 위치(의탁주소)에 존재하는지 검증할 수 있어야 한다.

연구되는 많은 논문에서 요청자 인증, 응답자 인증, 그리고 바인딩 갱신 정보의 무결성은 보장해주고 있지만, 요청자가 과연 그 위치에 있는지에 대한 요청자 위치 인증에 대해서는 확인을 하지 못하고 있다. 이에 본 논문에서는 효율적인 위치 확인을 제공하는 모바일 IPv6 바인딩 갱신 기법을 제안한다.

III. 기존 모바일 IPv6 바인딩 갱신 프로토콜

본 장에서는 기존에 제안된 바인딩 갱신 프로토콜을 모바일 IPv6 바인딩 갱신의 보안 요구사항 중 위치 확인의 관점에서 분석한다.

2.1 RR 프로토콜

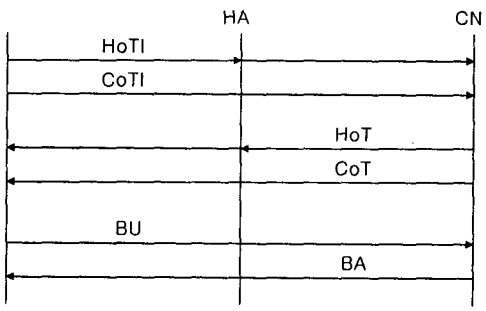

그림 1 : RR 프로토콜

RR 프로토콜은 IETF에서 권장하는 모바일 IPv6의 바인딩 갱신 프로토콜이다. 이 프로토콜은 바인딩 갱신 요청 이전에 MN가 자신의 HoA와 CoA를 사용하여 메시지를 수신할 수 있는지 확인하기 위해 CN으로 HoTI와 CoTI라는 독립적인 메시지를 전송하고, 그에 따른 응답으로 HoT와 CoT를 수신한다. 이 경우, CoT가 MN가 의탁주소를 전달된 메시지에 대해 응답할 수 있는지 CN이 확인할 수 있도록 함으로써 간접적인 위치 확인의 역할을 하고 있다.

2.2 CBID/SUCV 프로토콜

CBID(Crypto-Based IDentifier), 다른 말로 SUCV(Statistically Unique and Cryptographically Verifiable identifier)프로토콜[4,5]은 Montenegro와 Castellucia에 의해 제안된 CGA[6] 방식을 사용하는 기법이다.

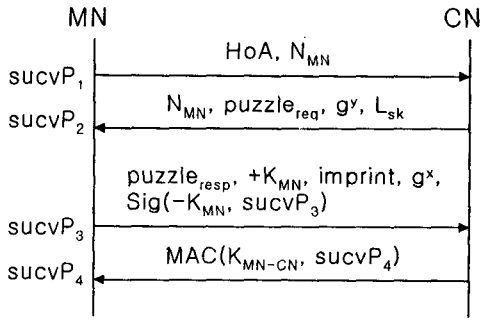

그림 2 : CBID/SUCV 프로토콜

MN가 CN에게 HoA와 난스 등이 포함된 $sucvP_1$ 메시지를 전송하면, CN은 MN로부터 받은 난스 값과 서비스 거부 공격을 방지하기 위한 퍼즐, 공개키 값 들이 포함된 $sucvP_2$ 메시지를 MN에게 전송한다. MN는 CN으로부터 받은 난스가 자신이 전송한 값과 동일한지 확인하고, 공개키 값과 난스 그리고 MN의 위치에 의존하는 64비트 imprint 값을 가지고 세션키를 생성하고, 퍼즐에 대한 응답을 생성한다. 마지막으로 MN의 개인키로 전체 메시지를 서명한 후 CN에게 $sucvP_3$ 메시지를 전송하고, CN은 $sucvP_3$ 메시지에 대한 확인을 한 후 응답을 한다. 이 프로토콜에서는 $sucvP_2$ 메시지에 대한 응답 메시지인 $sucvP_3$ 메시지를 전송함으로써, RR 기법에서와 같이 간접적으로 위치를 확인한

다.

이 밖에도 많은 프로토콜이 제안되었지만, 역시 위치 확인에 대한 확실한 대안을 내놓지는 못하고 있다.

IV. 제안 방식

본 장에서는 II장에서 설명한 전제를 바탕으로 위치 확인에 효율적인 모바일 IPv6 바인딩 갱신 기법을 설명한다.

4.1 전제조건

제안되는 기법은 공인 인증체제가 전제가 된다. 각 네트워크는 에이전트를 두고 있으며, 각 에이전트는 자신의 네트워크에 속한 노드에 주소를 부여할 경우, 부여되는 주소를 검증하기위해 인가 인증서(authorization certification)를 발급한다. 인가 인증서는 X.509 인증서 프로파일을 이용하며, 인가 인증서의 수명은 일반적으로 24시간 이내를 가지며, 이 유효 기간이 지나면, 모바일 노드는 다시 인가 인증서를 발급 받아야 한다. 인가 인증서는 주체 필드에 사용자의 공개키에 대한 해쉬 값을 가지며, 인가 인증서 체인을 이용하며 신뢰를 확장한다. 또한, 두 개의 도메인 간에 믿음은 인가 인증서의 공개키를 교환함으로써 이루어진다. 인가 인증서에는 현재의 위치를 확인할 수 있는 Alternative subject 필드가 존재하며, 이 필드에는 이동노드에게 부여될 CoA를 포함하고 있다.

인가 인증서를 발급 받는 절차는 본 논문의 범위 밖이므로 생략한다.

4.2 제안 방식

다음의 그림 3은 본 논문에서 제안하는 기법의 초기 구동을 나타낸다.

각 네트워크의 에이전트는 자신의 네트워크에 속한 노드에게 공개키의 해쉬 값과 부여되는 주소 정보 등이 포함된 인가 인증서를 발급한다. 초기 홈 네트워크에 위치한 MN는 HA로부터 인가 인증서가 발급된다.

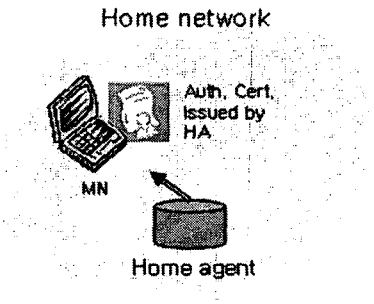

그림 3 : 초기 구동

다음의 그림 4는 MN가 홈 네트워크가 아닌 외부 네트워크로 이동한 모습이다.

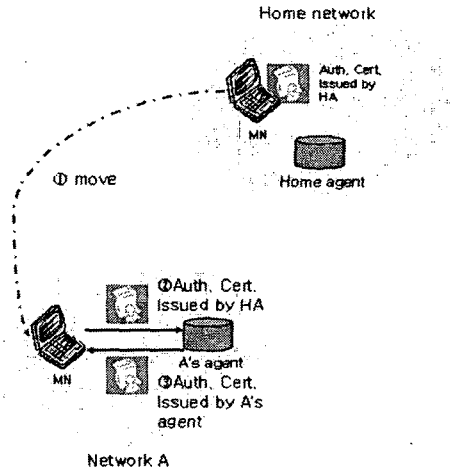

그림 4 : MN의 외부 네트워크로의 이동

MN가 A라는 네트워크로 이동한다고 가정하였을 때, MN는 자신의 홈 에이전트로부터 발급받은 인증서를 새로운 네트워크의 에이전트에게 자신을 인증하는 목적으로 제시하여 새로운 주소를 요청한다. 네트워크의 A의 에이전트는 MN에게 받은 인증서를 확인하고, 적합한 사용자라고 판단되었을 경우, 새로운 주소 CoA와 함께 그 주소를 보증해주는 인가 인증서를 네트워크 A 에이전트로부터 발급받는다. MN는 CN과의 통신에서 네트워크 A의 에이전트로부터 발급받은 인증서를 첨부함으로써 확실한 위치 인증을 받을 수 있다. 또한 교환되는 메시지는 인가 인증서의 공개키에 대응되는 개인키로 서명되어 전달됨으로써, 암호학적으로 안전한 위치 확인이 수행될 수 있다.

4.3 제안 기법 분석

	상호인증		무결성	위치확인
	MN	CN		
RR	×	×	×	△
CBID/SUCV	○	○	○	△
제안 기법	○	○	○	○

표 1 : 각 기법의 보안 요구사항 충족여부

각 기법에 대한 보안 요구사항 충족여부는 표 1과 같다. RR과 CBID/SUCV 프로토콜은 MN에 할당된 CoA에 실제로 MN가 위치하는지에 대해서 직접적으로 확인할 방법은 없으나, 요청된 메시지에 대한 응답 메시지를 수신하는지 여부에 따라 간접적으로 확인하고 있다.

하지만 본 논문에서 제안하는 기법은 노드들이 제 3의 공인된 에이전트로부터 주소와 주소를 보증해주는 인가 인증서를 발급받음으로써 확실한 위치 인증이 가능하다. 또한 CN의 이동 여부에 상관없이 네트워크 내에 공인된 에이전트가 존재하면 이용 가능한 매우 효율적인 방식이다.

V. 결론

본 논문에서는 효율적인 위치 확인을 위한 모바일 IPv6 바인딩 갱신 기법을 제안하였다. 결과적으로 바인딩 갱신 메시지 요청자의 확실한 위치 인증이 가능해졌지만, 인증서를 발급하고 검증하는 에이전트의 부하나 인증서에 포함될 항목 등에 대한 구체적인 내용에 대한 연구가 차후 수행되어야 한다.

[참고문헌]

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

[2] P. Nikander, J. Arkko, T.Aura, G. Montenegro, E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", IETF RFC 4225, Dec. 2005.

[3] J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Node and Home Agents", IETF RFC 3776, Jun. 2004.

[4] G. Montenegro, C. Castelluccia, "Crypto-Based Identifiers (CBID): Concepts and Application", ACM Trans. on Information and System Security. Vol.7, No. 1, pp. 97-127, Feb. 2004.

[5] G. Montenegro, C. Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Address", ISOC Symp. on Network and Distributed System Security (NDSS 2002), Feb. 2002.

[6] T. Aura, "Cryptographically Generated Addresses(CGA)", IETF RFC 3972, Mar. 2005.

[7] 구중두, 김상진, 오희국, "모바일 IPv6의 바인딩 갱신 기법에 관한 고찰", 한국정보보호학회 학회지 제16권 제1호, 2006년 02월.