논문 2005-42CI-3-1

IPv6기반 이동인터넷 환경에서 이동노드의 안전한 시동에 관한 방법

(Secure Bootstrapping Methods of a Mobile Node on the Mobile IPv6 Network)

나 재 훈*, 정 교 일*, 한 치 문**

(Jaehoon Nah, Kyoil Chung, and Chi-Moon Han)

요 약

IETF (Internet Engineering Task Force) 표준화 기구에서 최근에 완료된 MIPv6 (Mobile IPv6) 관련 표준 RFC3775, RFC3776는 이동노드와 홈에이전트 사이에 사전에 보안연계 (SA : Security Association)가 설정 된 이후에 이동중에 홈에이전트와 상대노드에게 이동사실을 안전하게 통보하는 위치갱신에 관한 방법을 제시하고 있다. 그러나 이 표준 규격에는 이동노드의 시동(Bootstrapping)과 시동의 경우에 이동노드와 홈에이전트 간에 보안연계를 설정하는 문제에 대하여 제시된 방식이 없다. 본 논문에서는 이동노드와 홈에이전트간의 안전한 시동을 위한 방식을 제시하였다. 이 방식은 인증, 위치갱신, 홈에이전트 할당 그리고 보안연계 분배를 AAA의 안전한 채널을 통하여 이동노드와 홈에이전트간에 수행한다. 그리고 제안된 방식을 기능, 라운드트립 그리고 보안강도 관점에서 특성분석 하였다.

Abstract

At IETF (Internet Engineering Task Force), recently RFC3775, RFC3776 documents about the mobile IPv6 were standardized by IETF (Internet Engineering Task Force). Those specifications propose that during the roaming, the mobile node sends securely the binding update to the home agent and the correspondent node after setting the security association between Mobile Node and Home Agent. But there is no secure bootstrapping method between a mobile node and a home agent at the two RFC documents. This paper proposed a method for the secure bootstrapping between a mobile node and a home agent. This makes the authentication, binding update, home agent assignment, security association distribution through the AAA-based secure channel between mobile node and home agent. And the proposed method was analyzed in the view of the procedure, round trip and security strength.

Keywords : Mobile, IPv6, AAA, Bootstrapping, IKE

I. 서 론

이동 인터넷 환경에서 이동성 서비스 제공 표준으로 MIPv6 (Mobile IPv6) 프로토콜이 구체화 되면서 IETF (Internet Engineering Task Force) mip6 워킹 그룹에서는 보안 문제를 제기하였다.

2004년 6월에 IETF에서는 MIPv6 관련 두개의 기본 표준이 제정 되었지만 두개의 표준을 살펴보면 HA (Home Agent)와 MN (Mobile Node)간에 보안연계 (SA: Security Association)가 사전에 설정되어야 한다는 전제 조건을 기본으로 하며, 그 이후에 일어나는 위치갱신 (BU : Binding Update)에 대하여 안전성을 제공하고 있다[1],[2]. 즉 IETF mip6 워킹그룹에서는 사전에 보안연계 설정을 위한 시동에 대한 완전한 메커니즘을 제시한 것이 없으며, 최근에서야 이 문제를 해결하기 위한 표준화가 시작되는 시점이 되고 있다.

시동 관련한 주요 연구로 두개의 IETF 기고문을 참

* 정회원, 한국전자통신연구원 정보보호연구단
(Information Security Research Division, ETRI)
** 정회원, 한국외국어대학교 전자정보공학부
(Hankuk University of Foreign Studies)
접수일자: 2004년11월3일, 수정완료일: 2005년5월3일

고 할 수 있다. 참고문헌 [3]에서는 시동을 위하여 AAA (Authentication, Authority and Accounting) 서버와의 연동을 제안한 최초 방식으로, 인증 메시지를 이용하여 피기백 방식을 사용하고 있다. 피기백을 사용하면 위치갱신을 위한 두개의 메시지를 줄일 수 있는 장점을 갖는다. 그러나 MN과 AAA Client (또는 AR : Access Router)의 무선구간은 보안 취약점을 보이고 있으며 이에 대한 전송 프로토콜과 보안 방안에 대하여는 언급된 바가 없다. 참고문헌 [3]은 다이어미터(Diameter) 프로토콜을 사용하는 연동에 관한 것으로서 인증 메시지 교환 회수(Round Trip)를 줄이기 위해 제안한 방법이다. AAA 메시지에 위치갱신 메시지를 피기백 하는 경우, 초기 단계에서 이동 노드와 AAA Client간에 세션 키가 설정되지 않는 상태에서 위치갱신 내용을 AAA 메시지의 옵션으로 내장하게 되면 악의적인 노드에 의해 이동 노드 및 홈 에이전트간의 정보가 노출될 수 있으며, 이 정보를 통해 공격자는 홈 에이전트에 대한 분산 서비스 거부 공격 (DDoS : Distributed Denial of Service)을 감행할 수 있게 된다. 그러므로 메시지의 내장 데이터에 아무런 보안장치 없이 바인딩 갱신 메시지를 실어 보내는 것은 바람직하지 못하다. 또한 HoA (Home of Address)와 HA의 주소가 사전에 고정적으로 설정되어 주소 재설정 (Renumbering)과 같은 홈네트워크 변경에 대하여 적절히 대응하지 못하는 문제점을 보이고 있다.

참고문헌 [4]에서는 Perkins가 제안한 방식을 기본으로 하고 있으나, Perkins의 제안 방식을 사용하는 경우, 메시지 교환 회수는 줄일 수 있지만 많은 옵션 및 AVP (Attribute Value Pair) 파라미터들이 존재하므로 각 AAA 엔티티에서의 처리가 복잡하고 보안상 심각한 문제점을 야기 시킬 수 있으므로 이러한 옵션들을 최적화하고 메시지 교환 회수가 다소 증가하더라도 보안상 더 나은 방법을 제안하고 있다. MIPv6 시그널링(바인딩 갱신 및 바인딩 응답) 이전에 행해지는 키 분배를 위한 프로토콜인 IKE (Internet Key Exchange)의 성능이 이동 환경에서 기대에 못 미치는 것으로 실험적으로 보고됨에 따라 Dupont은 AAA 인프라와 결합된 방법을 통해 해결책을 제시하고 있다. MN과 HA간의 단순 세션 키를 분배하는 메커니즘을 갖고 있으며 무선구간에 대한 취약성에 대비하여 키분배 기능을 제공하고 있다. 이 방법을 사용할 경우 인증을 위해 모든 이동 노드는 총 12 단계의 인증 과정을 거치게 되나 전반적인 처리 부하는 Perkins 제안에 비해 적게 든다.

본 논문에서는 동적 홈주소 할당, 키분배,키 재분배, 그리고 MN-HA 터널 보안연계와 같은 기능들을 제공하는 안전한 시동 방식 설계를 위하여 제 Ⅱ장에서는 이동노드의 시동과 관련하여 설계 요구사항 및 개념 방식을 제안하고, 제 Ⅲ장에서 방식의 효율성 및 보안강도 측면에서 특성 분석하고, 제 Ⅳ장에서 결론을 맺는다.

Ⅱ. MIPv6 네트워크에서 이동 노드의 안전한 시동 방식

시동(Bootstrapping)은 이동노드가 적절한 홈에이전트에 자신의 주소를 등록하기에 필수적인 정보를 얻는 과정으로 정의 된다[5]. 특히, 사전에 협약된 것이 없이 이동인터넷 IPv6 환경에서 홈에이전트의 주소, 홈주소 그리고 보안 인증서를 상호간에 인증하고 설정하는 과정을 의미한다.

1. 안전한 시동을 위한 MIPv6와 AAAv6의 연동 요구사항

가. 가 정

이동인터넷 IPv6 환경에서 안전한 통신을 위한 IETF MIPv6 RFC(Request For Comment)[1],[2]의 가정은 이동노드와 이동통신 사업자 (MSP : Mobility Service Provider) 간에는 신뢰적 관계가 있어야 한다. 그 신뢰적 관계는 하나의 이동통신 사업자와 계약을 갖고 있는 접속 네트워크 사업자(ASP : Access Service Provider) 간의 직접 또는 간접적 채널이며, 이 신뢰 채널은 이동노드의 시동에 사용되며 전형적인 방안은 AAA를 사용하는 것이다.

또 다른 가정은 참고문헌 [6], [7]에서 정의된 것과 같이, NAI (Network Access Identifier)와 같은 인식자가 접속(방문) 네트워크에서 이동노드가 인식될 수 있어야 하며, 또 역으로 이동노드가 접속(방문)네트워크를 인식할 수 있는 인식자(NAI)가 이동노드에 설치되어야 한다.

나. 이동노드 요구사항

시동을 위한 방식은 시동 후에 이동노드가 홈에이전트에 등록을 할 수 있도록 다음 항목의 정보를 획득하여야 한다.

. 이동노드 홈주소 (HoA : Home of Address)
. 이동노드 홈에이전트 주소 (HaA : Home agent Address)

. 이동노드와 홈에이전트 간의 IPsec 보안연계 또는 이동노드 홈에이전트 간의 Pre-shared 키

다. 네트워크 요구사항

MIPv6 베이스 규격[1]에서의 디폴트 시동은 홈주소와 홈에이전트 주소에 대하여 고정 바인딩을 갖는다. 그러나 홈주소와 홈에이전 주소에 대하여 고정 바인딩은 홈 서브 네트워크 재구성, HA의 부하분산에 대처하지 못하는 문제를 일으키므로[5], 다음과 같이 동적 홈주소, 홈에이전트 할당 요구사항을 제시한다.

(1) 동적 홈주소 할당

고정 홈주소를 할당하는 것은 안전한 시동 방안이 될 수 있지만 다음과 같은 기능들과의 연동을 위하여 동적 홈주소 할당이 네트워크에서 관장되어야 한다.

- DHCP 기반 주소 할당

접속네트워크 사업자는 홈네트워크에서 홈주소를 형성하기 위하여 DHCPv6를 이용을 제공하여야 한다.

- 중복주소 충돌에 의한 회복

홈네트워크에서 주소충돌에 의한 회복이 필요 하다.

- 주소 할당 프라이버시

RFC 3041에서와 같이 임의 주소를 생성하여 단기간에 사용하는 것에 대한 고려를 하여야 한다.

- 전개(Deployment)의 용이성

MIPv6 전개를 용이하게 하기 위해서는 이용자나 관리자를 홈주소 할당과 보안정책 관리와 같은 일에서 자유롭게 해주어야 한다. 이것은 자동(동적)으로 주소를 할당하는 것을 말하며 IPv6의 서브네트워크의 자동형상(Autoconfiguration) 기능과도 일목상통 하는 것이다.

- 홈네트워크에서 프리픽스 변경

MIPv6 규격은 이동노드가 홈주소를 홈서브네트의 프리픽스 발견 메시지를 사용하여 서브네트워크의 자동형상 기능을 지원하고 있다[1]. 결과적으로, 이동노드는 홈에이전트에서 새롭게 형성된 홈주소를 등록하기 위하여 동적으로 위치갱신을 수행할 수 있어야 한다.

(2) 동적 홈에이전트 할당

홈에이전트의 주소는 보안정책 데이터베이스에 수록되어 있는 것이 보편적이지만 동적 홈에이전트 할당은 다음과 같은 이유에서 지원되어야 한다.

- 홈에이전트 탐색

MIPv6 규격은 이동노드가 탐색 프로토콜에 기초하여 홈에이전트 주소를 자동할당 (Autoconfigure) 하는 것을 지원하고 있다[1].

- 독립 네트워크 관리

접속 네트워크는 동적으로 서로 다른 홈에이전트 할당을 할 수 있다.

- 로컬 홈에이전트

이동노드의 홈 네트워크 사업자가 그 이동노드를 위하여 홈로컬 에이전트를 접속네트워트 사업자에게 허용할 수 있어야 한다.

- 전개의 용이성

이동성 서비스 사업자는 시의 적절한 탐색으로 이동성 서비스를 사용하도록 허용할 수 있어야 한다. 이러한 시나리오는 동적 홈주소 할당을 필수로 요구한다.

라. AAA 요구사항

RFC 3776에 기술되어진 IKEv1 기반의 키교환 프로토콜은 AAA 기술과는 연동이 없다. 그러나 인증서를 이용하는 것은 PKI (Public Key Infrastructure)를 도입하도록 요구하지만, 이동환경에서는 PKI 적용이 용이하지 않고 또 불가능하기까지 하다.

안전한 시동을 위하여 이동노드에 키교환으로 인한 과부하를 줄이기 위해 AAA는 MN과 HA를 삼자적 인증을 수행을 하여야 한다. 즉 AAA가 삼자적 상호 인증을 해주면 이후에 MN과 HA간에 IPSec 보안연계를 직접적으로 설정할 수 있는 채널을 열어 주는 것이 되는 것이다.

2. 안전한 시동방식

유선 네트워크에서는 호스트나 게이트웨이는 PKI 기반으로 공인인증서를 발급 받으므로 상대에 대한 인증을 제 삼자가 수행하므로 안전한 키교환을 할 수 있다. 그러나 이동인터넷 환경에서는 컴퓨팅 자원이 열악한 이동노드와 협소한 무선 통신 대역폭으로 인하여 PKI와 같은 무거운 메카니즘을 이용할 수 가 없다. 이동인터넷 환경에서는 이에 해당하는 차선의 선택을 위하여

여러가지 대안중 대다수가 AAA와의 연동이 필요한 것으로 의견이 수렴되고 있다[3],[4],[5],[8],[9],[10],[11].

순수 MIPv6 네트워크에서는 이동노드가 타 네트워크로 이동(로밍)을 하였을 때에 이동노드에 대한 인증 메커니즘이 없다는 것이 문제가 된다. 즉 아무런 제약없이 접속네트워크에 이동노드가 접속을 할 수 있다면 문제가 없지만 과금, 관리 그리고 보안을 위하여 이동노드와 홈에이전트간에 신뢰 채널을 설정하기 위해서는 상호 인증을 하는 것이 필수가 된다. 그러나 MIPv6 표준 규격은 이와 같은 절차가 없으므로 AAAv6의 인프라를 이용하여 상호인증을 수행하는 방안이 선호되고 있다[3].

AAAv6 이용을 권고하는 또 다른 이유는 AAA 인프라는 이미 그 서비스가 입증이 되었으며 신뢰 받을 수 있는 인터넷 제어평면을 제공할 수가 있다는 것이다. 즉 AAA의 사전에 설정되어 있는 신뢰채널을 이용하여 이동노드와 홈에이전트간의 보안연계를 설정하려는 것이 기본 개념이 된다[3],[4],[8],[10].

시동의 요구사항으로 상호인증과 더불어 이동노드의 홈주소, 홈에이전트 주소, 위치갱신, 그리고 보안연계가 시동 이후에는 확정이 되고 이동노드와 홈에이전트 상호간에는 보안연계를 확보되어야 한다. 이러한 4가지의 행위를 수행하기 위해서 생각 할 수 있는 방식은 인증을 기본으로 하고 3가지의 행위를 경우의 수로 나열하면 8가지의 수가 발생한다.

표 1 에서 정리한 것과 같이 위치갱신을 AAA 인프라를 이용하지 않고 MIPv6의 고유기능을 이용하는 방식 I (인증) 있고, 시동에서 종국적인 목적인 위치갱신을 AAA 인프라를 이용한 방식 II (인증+위치등록), 동적 홈주소와 홈에이전트주소 설정 기능을 추가한 방식 III (인증+위치등록+HAA), 그리고 IPSec SA를 AAA 인프라를 이용하여 분배하는 방식 IV (인증+위치등록+HAA+SA)와 같이 4 가지의 방식을 생각할 수 있다. 8가지의 경우의 수에서 IPSec SA를 분배 하려고 하면 사전에 HoA, HaA를 알아야 하기 때문에 순번 4, 6, 7은 순번 8(방식 IV)에 통합을 하여 고려하고 순번 3은 HoA, HaA를 AAA 인프라를 이용하는 의미가 분명하지 않기 때문에 순번 1(방식 I)에 통합하여 고려한다.

표 1. AAA를 이용한 안전한 시동방식
Table 1. Secure bootstrapping methods based on AAA infra.

순번	기능항목	실효성	비고
1	인증	있음	방식I
2	인증,위치갱신	없음	방식II
3	인증,HoA/HaA할당	없음	(방식I에 통합)
4	인증,IPSec SA 설정	없음	(방식 IV에 통합)
5	인증,위치갱신,HoA/HaA 할당	있음	방식 III
6	인증, HoA/HaA 할당, IPSec SA 설정	없음	(방식 IV에 통합)
7	인증, 위치갱신, IPSec SA 설정	없음	(방식 IV에 통합)
8	인증, 위치갱신, HoA/HaA 할당, IPSec SA 설정	있음	방식 IV

가. 방식 I (AAA 인증)

AAA는 과금을 위해 MN을 인증하는 AAA 고유 기능만을 제공하고, MN의 이동성 지원을 위해 필요한 과정인 BU전송, SA 설정, 홈 에이전트 할당 등의 기능은 MIPv6의 고유기능을 이용하는 방식이다. 이 방식은 네 가지 방식 중 가장 AAAv6와 Loosely Coupled 된 방식이다. 장점은 MIPv6 프로토콜을 구현한 타 시스템과 상호운용성을 제공한다는 것이다. 이는 MIPv6의 기본 구조를 변경하지 않은 형태로 AAA 인증을 위해 기능을 추가하는 형태로 구성되었기 때문이다. 또한 이러한 이유로 AAA 인프라가 구축되지 않은 환경에서도 독자적으로 동작이 가능하다는 장점을 갖는다. 나머지 세 개의 방식의 경우 AAA 인프라가 구축되지 않은 경우에 정상적인 MIPv6 동작이 불가능 하다. 단점으로는 나머지 세 개의 방식에 비해 신호부하가 높다는 것이다. 이는 AAA인프라를 이용하는 경우와 비교하여 추가로 IKE협상, 위치갱신 전송 등의 작업을 위해 추가적인 메시지가 발생하기 때문이다[12],[13].

그림 1 은 방식 I에 따른 AAA 와의 연동 과정을 보여준다.

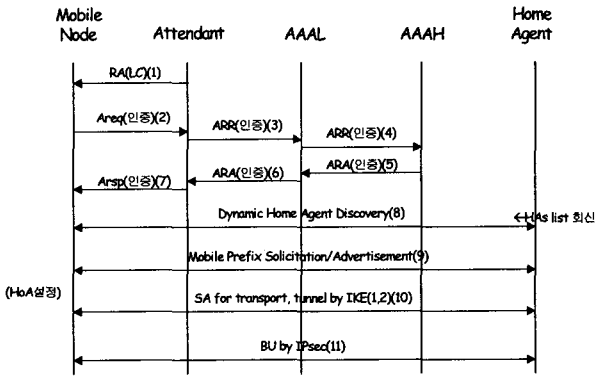

그림 1. AAA 인증 연동방식
Fig. 1. Interworking method with AAA authentication.

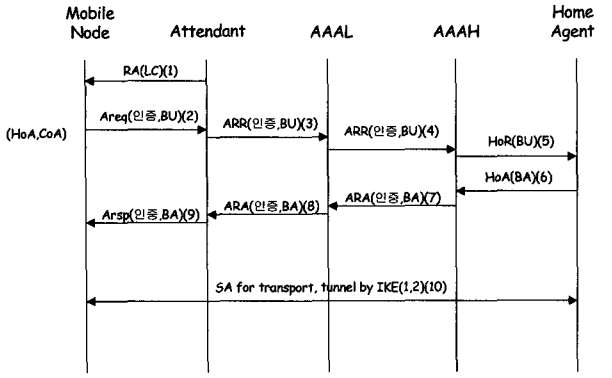

그림 2. AAA 인증, BU 연동방식
Fig. 2. Interworking method with AAA authentication, BU.

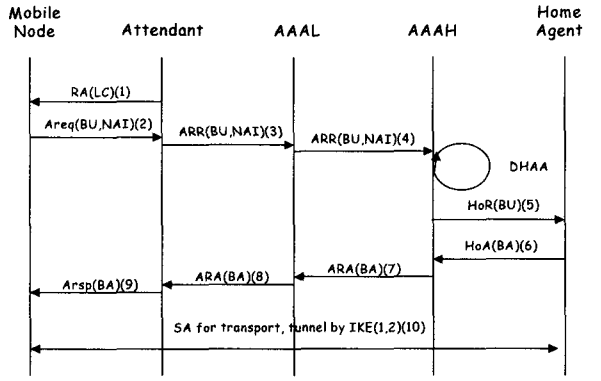

그림 3. AAA 인증, BU, HAA 연동방식
Fig. 3. Interworking method with AAA authentication, BU, HAA.

나. 방식 II (AAA 인증, BU)

AAA 인증에 위치갱신을 피기백킹 하는 것은 AAA 와 MIPv6의 연동을 하는 방식이다. 이것은 MN이 AAA서버에 인증을 요청하는 페이로드에 위치갱신을 실어 보내는 것으로서 위치갱신을 받은 AAA는 MN을 대신하여 HA에 MN의 위치정보를 갱신 하는 방식이다. 그림 2는 이러한 연동 과정을 각 노드별로 나타내고 있다.

이 방식은 AAA 인증에 BU를 피기백 함으로써 인증 절차와 MN의 홈등록을 각각 수행하는 것보다 효율성을 주고자 하는 것이다.

다. 방식 III (AAA 인증, BU, HoA/HaA 할당)

본 방식은 AAA 기반구조와 MIPv6를 연동함으로써 MIPv6가 독립적으로 수행하던 작업의 효율성을 높이려는 방식들 중의 하나이다. 본 방식은 나. 항에 설명한 방식에 추가하여 MN이 사용할 HA 할당까지도 AAA 기반구조 하에서 통합된 과정으로 처리하려는 방식으로

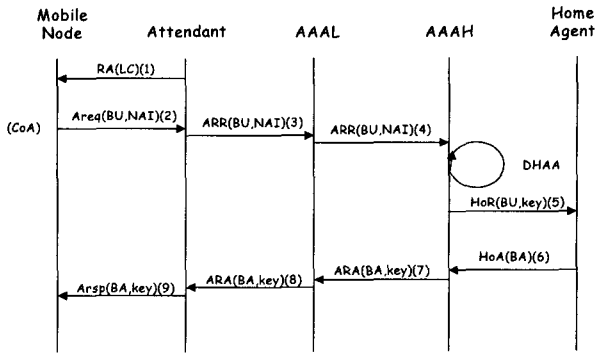

그림 4. AAA 인증, BU, HAA 및 SA 분배 연동방식
Fig. 4. Interworking method with AAA authentication, BU, HAA, SA negotiation.

기존에 HA 할당을 위해서 필요했던 별도의 메시지 교환을 줄일 수 있다.

그림 3 은 AAA 기반구조와 연동되어 MIPv6 관련 작업을 수행하기 위해서 교환되는 메시지들 및 관련 개체들의 동작을 보여준다.

라. 방식 IV (AAA 인증, BU, HoA/HaA 할당, SA)

AAA 의 인증 처리를 위한 하나의 Round-trip에 이동노드의 위치이동을 등록하기 위한 위치갱신, 이동노드의 HoA/HaA 할당 및 차후 MN 과 HA 사이의 통신 채널을 보호하기 위한 IPSec SA를 AAA 인프라를 통해서 분배하는 방식이다.

기존의 MIPv6 프로토콜 동작방식에서는 MN 과 HA 사이의 통신채널을 보호하기 위해 IPSec SA 를 미리 매뉴얼 방식으로 설정하거나 IKEv1 을 사용하도록 권고하고 있다. 하지만 이러한 방식은, 고정적인 MN 의 홈주소와 HA 주소를 기설정하여 동작하므로, MN 의 홈 네트워크의 환경이 변화될 경우 대처가 유연하지 못하다는 단점을 갖는다. 또한, IKEv1 에서 IPsec SA 를 설정하기 위한 시그널링 부하가 높다는 점에서 IPSec SA 의 재설정 등에 적합하지 못한 방식이다.

방식 IV는 상기에서 언급한 MIPv6 프로토콜 동작방식의 단점을 해결하기 위한 것으로, AAA 인프라를 최대한 활용하여 MN 과 HA 의 통신채널을 보호할 수 있으며 HA 의 설정 또한 동적으로 할당할 수 있다는 장점을 갖는다. 최근 IETF mip6 워킹그룹을 중심으로 MN 의 최초 IPSec SA 설정을 동적으로 제공하기 위한 시동기법이 주목을 받고 있는데, 본 방식은 이러한 시동 방식을 지원할 수 있다는 점에서 효과적이라 평가된다. 본 절에 제시한 연동방식은 그림 4 에 예시되어 있다.

Ⅲ. 제안방식 특성분석

제 I 장에서 안전한 시동을 위한 초기 시동 방식들에 대하여 검토한 결과 주로 AAA 인프라를 이용하여 시동을 하는 메커니즘을 선호하고 있다. IETF의 mip6 워킹그룹에서는 MIPv6 프로토콜에 안전한 시동을 위한 기능을 추가 하고자 하는 부류도 있지만 다른 네트워크로 로밍을 하는 경우에는 안전한 시동을 위한 신뢰적 채널을 제공할 수 없다는 커다란 한계의 벽에 직면함을 시인하고 있다.

표 2 은 제 I 장에서 언급한 초기 시동 방식에서 제공해야 할 기능들을 요약한 것이며[5], 동적 홈주소 할당, 키 재분배, MN-HA 터널 보안연계 같은 기능들이 대부분 제공 되지 않는 문제점을 보이고 있다.

제 II 장에서 제안된 방식들을 기능적, 성능적 측면에서 비교분석 하기위해서 먼저 네트워크의 안전성을 고려한 기능측면에서 평가한다. 각 방식에 대하여 기능적 평가를 위하여 표 2의 초기 시동방식을 분석한 파라미터를 적용한다. 동적 홈주소 할당(홈에이전트 주소 할당과 동시에 실행)은 제안된 방식들에서 방식 II를 제외하고는 모든 방식이 제공할 수 있다 (단, 방식 I에서는 사전에 공용 HoA를 MN이 가지고 있어야 하는 전제 조건이 있다). BU 피기백 기능 관점에서는 방식 I을 제외하고는 4가지 방식이 모두 이기능을 제공 할 수 있다. 그러나 이 기능은 MN-Attendant 구간의 보안성이 보장되지 않으면 사용을 할 수 없는 기능이 되므로 BU 피기백 기능 제공에 대하여는 좀 더 보안측면에서 보완을 할 필요가 있다. 그 외 키분배와 Rekey 기능은 이동인터넷 환경에서의 보안성을 강화 할 수 있는 기능을 제공하고 있다는 측면에서 초기시동 방식보다 많은 진보가 있음을 알 수 가 있다.

안전한 시동을 위한 네트워크 전반적인 성능의 부하 정도를 분석하기 위하여 RT(Round Trip) 회수(IKE의 키교환은 실제적으로 4.5 라운드, 9 개의 메시지를 송수신을 추가로 계수 한다), 시그널링 부하(메시지 총 개수로 계수 : Signaling Load), 신호 복잡도와 시동시간을 측정하였다. RT 회수는 시동을 위하여 각 방식에서 처리하는 교환회수를 계수하였고, 시그널링 부하는 기능처리를 위하여 네트워크에서 소요되는 자원의 양을 의미하는데 기능 처리를 위해 소요 되는 총 메시지 개수를 계수한다. 신호 복잡도는 순수 MIPv6나 AAAv6의 메시지 처리를 기본값으로 (추가 정보요소=0, 추가 정보크기=0)를 설정하고 추가적인 메시지 내용, 즉 AAAv6는 AVP와 MIPv6는 옵션 필드의 사이즈를 계수한다. 그리고 각 방식에서 메시지 전달시간과 각 옵션필드의 처리 단위시간을 메시지 전달은 1, 이동탐지는 1, 인증 데이터 생성 및 검증은 2, 암복호는 2, 메시지 단순 전달은 1, 메시지 형식 변환전달은 2로 정하고 메시지 처리에 따르는 총 시간을 계수하기 위하여 아래 (식 1)에 대입 하여 시동을 위한 각 방식의 시동시간을 측정 하였으며 표 4 에 그 결과를 표시 하였다.

$$\text{시동시간} = \sum \text{메시지 전송시간} + \sum \text{메시지 처리시간} \quad (1)$$

본 논문에서 제안한 4 가지 방식들은 이동인터넷에 적용을 위하여 보안강도를 충족시키면서 효율적인 방식이 어떤 것이냐를 살펴보아야 한다. 표 3 에는 기능적인 측면에서 각 방식이 제공하는 항목을 표시한 것이다. 이중에 네트워크에 적용을 위한 중요한 요소는 보안 관점에서 MN-HA 트랜스포트 SA 분배, MN-HA 터널 SA 분배, 키 재분배(Rekeying) 그리고 동적 HoA 설정이 되겠다. 표 3 에서 방식 II 는 동적 HoA 설정 기능이 없다. 이 방식은 실현을 재고 할 필요가 없는 것으로 평가 되며, 또 나머지 3가지의 방식들은 다른 기능들을 충족하고 있지만 위치갱신(BU) 기밀성 항목에 있어서 방식 I 만이 이 기능을 제공하고 있다. 이것은 위치갱신을 AAA 인프라 기반에서 피기백 기능을 이용하여 발생되는 문제점으로 분석된다.

각 방식들에 대하여 위치갱신을 안전하게 수행하는

표 2. 초기 시동방식 기능비교
Table 2. Function comparision of early bootstrapping methods.

(기능구비 : o, 기능미비 : x)

기능 / 방식	동적 HoA	MN-HA 키분배	Rekey	피기백	MN-HA 터널 SA	MN-AR 세션키
퍼킨스 방식	x	o	x	o	x	o
듀폰 방식	x	o	x	x	x	o

표 3. 안전한 시동방식 기능비교
Table 3. Function comparision of secure bootstrapping methods.

(o: 기능보유, x:기능미비)

	동적HoA	MN-HA 트랜스포트 SA	Rekey	BU피기백	MN-HA 터널 SA	BU 기밀성
방식 I	o	o	o	x	o	o
방식 II	x	o	o	o	o	x
방식 III	o	o	o	o	o	x
방식 IV	o	o	o	o	o	x

표 4. 안전한 시동방식 성능비교
Table 4. Efficiency comparision of secure bootstrapping methods

	신호부하	신호 복잡도	RT 회수	시동시간
방식 I	22	(0,0)	8	89
방식 II	18	(1,20)	5	64
방식 III	18	(2,40)	5	66
방식 IV	9	(4,138)	1	32

절차에 대하여 집중 연구를 하였으며 그 결과 방식 I 은 홈네트워크에 동적 HoA 할당을 요청하기 위해 메시지 전달을 위한 주소가 사전에 설정이 되어 있어야 한다는 문제점을 갖고 있음이 분석 되었다. 나머지 3 가지 방식들에서 안전하게 위치갱신을 수행하는 것에 있어서 피기백 기법을 사용은 완전한 보안을 제공하지 못하고 있음을 표 3 에서 나타내었다.

표 4 에서 시동을 위한 MN 측면과 네트워크 측면에서 시그널링의 부하를 적게 주는 방안이 4번째 방식이 되겠다. 방식 IV는 보안강도 측면에서 보안연계가 AAA 구조를 통해서 분배되기 때문에 MN-AR 구간에서 보안연계 정보의 노출이 우려되는 문제점을 갖고 있다. 즉 AAA메시지는 AR에서 종단이 되므로 MN와 AR간에는 EAP (Extensible Authentication Protocol)에 상응하는 적절한 프로토콜이 PANA (Protocol for carrying Authentication for Network Access) 또는 ICMP (Internet Control Message Protocol) 가 될 수 있으나 이에 대한 보안 메커니즘이 확보가 되지 않았으며 보안연계 정보의 노출이 우려 되는 지점이 된다.

이에 반해 1~3번째 방안은 II장의 방식의 절차에서도 알 수 있지만 시동후 최종 보안 강도가 높음을 보이고 있다. 즉 End-to-End 로 MN에서 HA까지 IKE 협상을 하는 방식인 것이다(방식 IV는 무선 구간의 기밀성을 확보하지 못한 시점에서 IPSec SA를 분배한다). 이것은 모두 IKE 수행이 별도로 진행되어야 함을 내포하고 있으며 IKE 절차에 의한 9개의 (Phase 1 : Main 모드에 6개, Phase 2 : Quick 모드에 3개) 메시지가 추가 되어야 함을 의미한다.

IV. 결 론

IETF의 mip6 워킹그룹에서는 유무선통합 이동통신 환경에서 이동성 서비스를 위한 보다 편리하고, 효율적이며 안전한 프로토콜을 구비하기 위한 연구의 결과로 2004년 6월까지 MIPv6 관련 두개의 기본 표준이 제정되었다[1],[2]. 그러나 MIPv6 표준 문서의 내용에는 HA와 MN간에 사전에 보안연계 (SA : Secrutiy Association)가 설정되는 과정은 생략되어 있다.

이에 본 논문에서는 MN과 HA간에 안전한 시동을 위한 방식 제안을 위하여 제 I 장에서 보안 문제점과 현재까지의 연구결과에 대하여 검토하였다. 제 II 장에서는 안전한 시동 방식을 위한 요구사항과 인증, 위치갱신, 동적 HoA/HaA 할당, IPSec SA 설정 기능 제공을 중심으로 가능한 4가지의 방식을 제시하였으며 제 III 장에서는 I 장의 초기 시동방식과 기능 측면에서 방식 들을 비교분석 하였고 제안한 방식들을 신호 부하, 신호 복잡도, RT 회수, 시동시간을 기준으로 성능 분석하였다.

본 논문에서 제안된 시동방식은 초기 시동 방식과 기능면에서 동적 HoA/HaA 할당, Rekey, MN-HA 간의 IPSec SA, 위치갱신 메시지의 기밀성을 보장할 수 있도록 기능이 개선된 방식임을 보였다. 그리고 효율성 관련하여 표 4에서는 방식 IV가 우수함을 그리고 보안강도 관련하여 표 3에서는 방식 I이 가장 우수함을 보였다. 즉 이와 같은 결과는 위치갱신을 보안연계 분배를 수행하고 난 이후에 독립적인 절차로 수행하도록 하여야 완전한 보안성을 제공한다는 것을 입증 하였다.

향후 연구과제로는 시동에 있어서 단순 인증 서비스를 기반으로 하는 이동노드와 홈에이전트간의 시동 프로토콜에서 키교환의 경량화 연구가 필요하다. 즉 IKE 키교환 절차를 PKI 기반의 AAA 인프라를 이용하여 줄이는 방안이 필요하다.

또 자신의 정보를 비밀로 하고 싶지 않은 일반 사용자들의 요구사항도 반영을 하여야 한다. 기밀성 서비스를 위한 과도한 자원의 소모를 줄이고 현재의 이동인터넷 환경에서 상호 인증 서비스만을 제공하는 보안 메커니즘이 필요하다.

그리고 RR (Return Routability) 프로토콜이 이동노드와 홈에이전트 구간을 제외한 다른 곳에서는 끼여들기 (MITM : Man In The Middle) 공격이 가능하다. 그러므로 상대노드와 통신을 위하여 세션을 설정할 때에 RR보다 강한 보안 서비스를 제공하는 메커니즘이 필요하다. 이것은 보안 인프라가 구축되어 있지 않다는 것이 현실적으로 풀기 어려운 문제이다. 통신 세션을 설정하지도 않은 상대노드를 언제 사용할지도 모르면서 사전에 보안연계를 나누어야 한다는 것은 매우 불합리한 것이다. 그러므로 이동노드와 상대노드가 세션을 열 때에 동적으로 보안연계를 설정할 수 있는 보안 인프라를 구축하는 것에 대한 연구가 시급히 추진되어야 할 과제이다.

참 고 문 헌

[1] Johnson, D., Perkins, C. and J. Arkko, Mobility Support in IPv6, RFC 3775, July 2003.

[2] Arkko, J., Devarapalli, V. and F. Dupont, Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents, RFC 3776, July 2003.

[3] Stefano M. Faccin, Frank Le, Basavaraj Patil and Charles E. Perkins, Diameter Mobile IPv6 Application, draft-le-aaa-diameter-mobileipv6-03.txt, Internet Draft, IETF, April 2003.

[4] F. Dupont, J. Bournelle, AAA for Mobile IPv6, draft-dupont-mipv6-aaa-01.txt, Internet Draft, IETF, Nov. 2001.

[5] Alpech. Patel, Problem Statement for bootstrapping Mobile IPv6, draft-ietf-mipv6- bootstrap-ps-00. txt, Internet Draft, IETF, July 9, 2004.

[6] Patel, A., Leung, K., Akthar, H., Khalil, M. and K. Chowdhury, Network Access Identifier Option for Mobile IPv6, draft-ietf-mip6-nai-option-00.txt, Internet Draft, IETF, February 2004.

[7] Calhoun, P. and C. Perkins, Mobile IP Network Access Identifier Extension for IPv4, RFC 2794, March 2000.

[8] Miyoung Kim, Youngsong Mun, Jaehoon Nah, Seungwon Sohn, "Localized Key Management for AAA in Mobile IPv6, draft-mun-aaa-localkm-mobileipv6-01.txt, Internet Draft, IETF, Nov. 2002.

[9] 지정훈, 나재훈, 남택용, 손승원, 빠른 사용자 세션 정보 전달에 의한 Mobile IPv6와 AAAv6의 연동 방안, NCS2003, 휘닉스파크, 2003.12

[10] Miyoung Kim, Youngsong Mun, Jaehoon Nah, Seungwon Sohn, Dynamic Binding Update using AAA, draft-mun-aaa-dbu-mobileipv6-00.txt, Internet Draft, IETF, Nov. 2002.

[11] 문영성, Mobile IPv6에서의 초기구동(Bootstrapping) 표준화 동향, *IT Standard Weekly,* 2004-41호, 2004-10.18.

[12] H. K. Lee, Jae-Hoon Nah, Sung-Won Sohn, The Efficient SA negotiation Protocol between HA and MN in Mobile IPv6, APIS 2002, Jakarta, Indonesia, 2002.12

[13] 이형규, 나재훈, 손승원, IPsec 시스템에서 IKE 프로토콜 엔진의 연동에 관한 연구, *정보보호학회 논문지,* 2002.11.

저 자 소 개

나 재 훈(정회원)

1985년 중앙대학교 컴퓨터공학과 학사.

1987년 중앙대학교 컴퓨터공학과 석사.

2005년 한국외국어대학교 전자정보공학과 박사.

1987년~현재 ETRI/P2P보안연구팀장

<주관심분야 : IPv6/MIPv6 보안, P2P보안>

정 교 일(정회원)

1981년 한양대학교 전자공학과 학사.

1983년 한양대학교 전자공학과 석사.

1997년 한양대학교 전자공학과 박사.

1987년~현재 ETRI/정보보호기반그룹장

<주관심분야 : IC카드, 국가기반보호, 신호처리, 생체인식>

한 치 문(정회원)

1977년 경북대학교 전자공학과 학사.

1983년 연세대학교 전자공학과 석사.

1990년 일본 동경대학교 전자정보공학과 박사.

1977년~1983년 한국과학기술연구원 연구원

1983년~1997년 ETRI/계통연구부장

1997년~현재 한국외국어대학교 전자정보공학부 교수

<주관심분야 : 차세대스위칭기술, 개방형네트워크기술, VoIP기술, 네트워크보안기술>