Mobile IPv6를 지원하는 Diameter 프로토콜의 설계

정회원 김 말 희*, 김 현 곤**

The Design of Diameter Application supporting Mobile IPv6

Marie Kim*, Hyungon Kim** *Regular Members*

요 약

본 논문은 Mobile IPv6 프로토콜이 탑재된 이동 노드에 대한 Mobile IPv6 프로토콜과 Diameter 프로토콜 간의 연동 시나리오를 설계한다. 본 논문은 연동 시나리오를 설계하고, 이를 기반으로 이동성 지원 기능을 상세히 설계하며, 이동 노드와 로컬 AAA 클라이언트 간 교환되는 정보 요소를 정의한다. 이동 노드와 로컬 AAA 클라이언트 간 인터페이스는 ICMPv6 메시지를 이용하여 설계한다. 또한 본 논문은 핸드오프가 발생한 경우에 대하여 이동 노드와 로컬 AAA 클라이언트 간 연동 시나리오를 핸드오프 영역별로 상세히 설계한다.

Key Words : Mobile IPv6, Diameter, Mobility Support, ICMPv6, Handoff

ABSTRACT

This paper suggests the cooperation scenarios between Diameter protocol and Mobile IPv6 protocol. First, this paper designs cooperation scenarios and designs mobility support technology based on the designed scenarios. This paper defines the interfaces between mobile node and local AAA client using ICMPv6 messages. In addition, this paper designs handoff procedures according to the area, which mobile node moves to.

Ⅰ. 서 론

Mobile IPv6 프로토콜은 이동 노드로 하여금 현재 위치에서 최소한의 서비스 장애로 인터넷 서비스를 지속적으로 받을 수 있도록 해주는 프로토콜이다[5]. 하지만 Mobile IPv6는 상업적으로 보편화되어 사용되기에는 여러 제약을 안고 있다. 우선 Mobile IPv6 프로토콜은 서로 다른 관리 도메인 간 이동에 대해서는 이동성을 보장하지 못한다. 서로 다른 관리 도메인 간 이동하는 로밍 상태의 이동 노드에 대해서 이동성을 보장하기 위해서는 상위 레벨의 로밍 협약에 대한 처리가 이루어져야 한다. 또한 Mobile IPv6 프로토콜은 기본적으로 이동 노드가 자신의 홈 주소(home address; HoA)를 알고 있고, 또한 자신의 현재 위치를 등록할 홈 에이전트(home agent; HA)의 주소를 알고 있어야 한다. 또한 이동 노드와 홈 에이전트 간 등록 메시지(Binding Update, Binding Acknowledgement)는 이동 노드와 홈 에이전트 간에 존재하는 보안 연관(Security Association SA)으로 보호되어야만 한다[5]. 따라서 통신 기기가 더욱 대중화되어가는 시점에서 Mobile IPv6 서비스를 받기 위한 정보의 사전 설정은 Mobile IPv6 서비스의 실행에 있어서 커다란 제약이 될 수밖에 없다.

Diameter 프로토콜은 망 접속을 요청하는 이동 노드에 대해서 홈 도메인에서뿐만 아니라 다른 도메인에서도 서비스를 지속적으로 받을 수 있도록 로밍 기능을 제공해준다[3]. 이미 상당한 표준화 작업이 이루어진 Mobile IPv4에 대한 Diameter 프로토콜의 이동성 지원은 이러한 로밍 상태의 이동 노드에 대한 인증과 이동 노드가 Mobile IPv4 서비스를 제공받기

* 한국전자통신연구원 AAA정보보호연구팀(mariekim@etri.re.kr), ** 한국전자통신연구원 AAA정보보호연구팀(hyungon@etri.re.kr)
논문번호KISC2004-08-170, 접수일자2004년 8월 27일

위해서 필요한 이동 노드의 홈 주소, 홈 에이전트의 동적 할당, 필요한 보안연관 설정 기능을 제공하도록 설계되어 있다[6][9]. 따라서 Mobile IPv6를 지원하는 Diameter AAA 프로토콜 역시 로밍 협약에 기반을 둔 인증, 권한 검증, 과금 서비스를 제공함과 동시에 이동 노드와 홈 망 AAA 서버와의 보안 연관을 이용하여, 이동 노드의 요청 시 Mobile IPv6 프로토콜이 요구하는 나머지 모든 필요한 정보를 생성하여 제공해줄 수 있어야 한다. 즉, 동적으로 이동 노드의 홈 주소를 할당하고, 동적으로 홈 에이전트를 할당하며, 이동 노드와 홈 에이전트 간 보안 연관 설정 및 이동 노드와 방문 망 AAA 클라이언트와의 보안 연관도 설정해 분배할 수 있어야 한다[1][2].

Mobile IPv4에 대한 Diameter 프로토콜의 확장 기능[6]은 이미 상당 부분 표준화되었지만, Mobile IPv6에 대한 Diameter 프로토콜의 지원에 대한 표준화 작업은 미비하다[8]. Mobile IPv4와 Mobile IPv6는 프로토콜상 구성 노드와 동작이 상이함으로 Mobile IPv4 확장 기능을 Mobile IPv6에 그대로 적용하는 것은 불가능하다.

본 논문은 Mobile IPv6를 위한 Diameter 프로토콜의 연동 기법을 설계한다. 본 논문은 연동 시나리오를 설계하고, 이동성 지원 기능으로 홈 망 및 방문 망에서의 홈 에이전트, 홈 주소 할당 기법 및 필요한 보안 연관 설정 기법을 설계한다. 이를 기반으로 이동 노드의 핸드오프에 따른 Mobile IPv6와 AAA 시스템간의 연동 시나리오에 대해서 상세히 기술한다. 이동 노드의 핸드오프를 동일 AAA 클라이언트 영역 안, 다른 AAA클라이언트 간, 다른 도메인 간으로 분류하여, 이동 노드에 대한 AAA 절차 수행 및 Mobile IPv6 절차 수행간의 인터페이스를 상세히 정의한다.

II. Mobile IPv6의 Binding

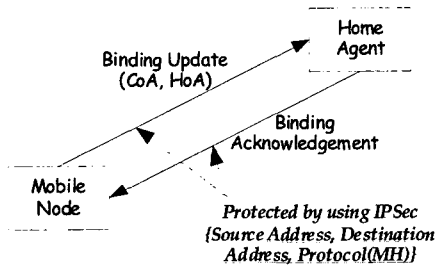


그림 1. Mobile IPv6의 Binding 연산

그림 1은 이동 노드의 이동성을 보장하기 위해서 이동 노드가 홈 에이전트에 현재 위치에서의 주소(Care-of Address; CoA)를 등록하는 Binding 과정을 나타낸다. 이동 노드와 홈 에이전트 간에 교환되는 Binding 메시지는 사전에 설정되어 있는 IPSec SA ESP(IP Encapsulating Security Payload)를 통해서 보호되어야만 한다[5].

이러한 IPSec SA는 사용 주체인 이동 노드와 홈 에이전트가 각기 SPD(Security Policy Database)와 SADB(Security Association Database)를 이용하여 관리한다. 메시지를 전송하는 노드의 홈 주소와 메시지를 수신하는 노드의 주소, 그리고 전송되는 메시지의 종류 등에 따라서, 이용되는 IPSec SA는 유일하게 정의된다[4]. 따라서 Mobile IPv6 프로토콜은 이동 노드가 이미 홈 주소를 보유하고 있어야 하며, 더불어 등록할 홈 에이전트의 주소도 알고 있어야 한다. 이동 노드와 홈 에이전트 간 IPSec SA는 사전에 고정적으로 설정할 수도 있고, IKEv1(Internet Key Exchange version 1)[8]과 같은 키 교환 프로토콜을 이용하여 동적으로 생성할 수 있다.

III. 로밍 환경에서의 AAA 모델

Mobile IPv6 서비스를 이용하는 이동 노드에 대한 AAA 모델은 두 가지로 분류할 수 있다. 홈 망의 홈 에이전트를 이용하는 경우와 방문 망의 홈 에이전트를 이용하는 경우이다.

1. 홈 망에 홈 에이전트가 위치하는 기본 AAA 모델

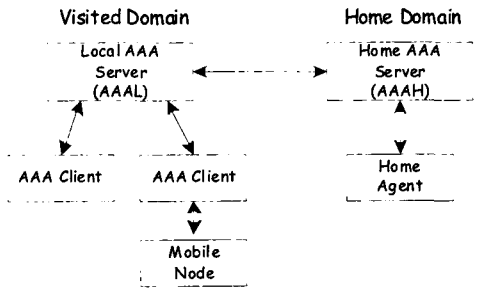


그림 2. Mobile IPv6를 지원하는 기본 AAA 모델

그림2는 Mobile IPv6에 대한 AAA 서비스를 제공하기 위한 기본 모델로 홈 에이전트는 홈 망에 위치한다.

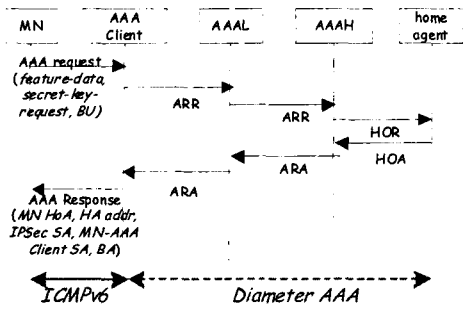


그림 3. 기본 AAA Model의 정보 흐름도

그림 3은 기본 모델에 의한 AAA 처리를 하기 위한 정보의 흐름도이다.

방문 망에 위치한 이동 노드는 방문 망의 AAA 클라이언트로 망 접속 요청(AAA-Request)을 전송하고 이를 수신한 로컬 AAA 클라이언트는 로컬 AAA 서버(AAAL)에게 Diameter 인증 요청 (AA-Registration-Request; ARR)[8] 메시지를 전송한다. 인증 요청은 로컬 AAA 서버를 거쳐서 이동 노드의 홈 망으로 전송되며, 홈 AAA 서버(AAAH)에 의해서 인증 처리된다. 홈 서버에 의한 AAA 인증 처리가 종료되면, 홈 에이전트에 의한 Mobile IPv6 처리를 위해서 홈 AAA 서버는 홈 에이전트로 MIPv6 등록 요청 메시지 (Home-Agent-MIPv6-Request HOR)[8]를 전송한다. 이를 처리한 홈 에이전트는 응답 메시지(Home-Agent-MIPv6-Answer HOA)[8]를 홈 서버에 전송하고, 홈 서버는 인증 결과와 권한 검증 정보를 (AA-Registration-Answer; ARA)[8] 메시지를 통해서 로컬 AAA 클라이언트로 전송하고, 로컬 AAA 클라이언트는 인증 결과를 이동 단말로 전송한다(AAA-Response).

본 논문은 Diameter 프로토콜이 Mobile IPv6의 Bootstrapping 기능을 지원하도록 한다. 즉, 이동 노드가 power-up하면서, 이동 노드 홈 주소, 홈 에이전트에 관한 정보가 필요한 경우, Feature-Data를 설정하여 홈 AAA 서버에게 요청한다. 또한 이동 노드와 홈 에이전트 간 SA 정보(Mobile IPv6의 필수 정보) 및 이동 노드와 로컬 AAA 클라이언트 간 SA 정보가 필요한 경우, 이동 노드는 Secret-Key-Request를 이용하여, 홈 AAA 서버에게 해당 SA 설정을 요청한다. 해당 정보는 로컬 AAA클라이언트에 의해서, MIPv6-Feature-Vector AVP와 MIPv6-Secret-Key-Request AVP로 변환되어 ARR 메시지에 포함되어 홈 AAA 서버로 전송된다. 각 AVP는 이동 노드로부터의 Feature-Data와Secret-Key-Request를 담고 있다.

홈 AAA서버는 인증이 성공한 경우, 두 AVPs 값을 확인하여 해당하는 이동성 정보를 생성한다. 생성된 이동 노드의 홈 주소는 MIPv6-Mobile-Node-Address AVP, 할당된 홈 에이전트 정보는 MIPv6-Home-Agent-Address AVP와 MIPv6-Home-Agent-Host AVP에 설정된다. 이동 노드와 홈 에이전트 간 SA 즉, IPSec SA 정보는 이동 노드로는 MIPv6-MN-HA-Key AVP, MIPv6-HA-MN-Key AVP, MIPv6-MN-HA-Key-Material AVP를 설정하여 ARA 메시지를 통하여 전달하고, 홈 에이전트로는 MIPv6-MN-HA-Key AVP, MIPv6-HA-MN-Key AVP, MIPv6-HA-MN-Session-Key AVP를 HOR 메시지를 통해서 전달한다. MIPv6-MN-HA-Key AVP와 MIPv6-HA-MN-Key AVP에는 각각 이동 노드에서 홈 에이전트 방향으로의 키를 제외한 IPSec SA 파라미터, 홈 에이전트에서 이동 노드로의 IPSec SA 파라미터들이 포함된다. 이와 같은 정보들은 로컬 AAA 클라이언트에 의해서 AAA-Response 메시지로 변환되어 이동 노드에게 전달된다. 이동 노드가 홈 주소, 홈 에이전트 정보를 모두 알고 있는 경우에는 Binding Update(BU)/Binding Acknowledgement(BA) 메시지를 Diameter 인증 메시지에 piggybacking하여 처리함으로써, 인증 지연 시간을 최소화한다.

2. 방문 망에 홈 에이전트가 위치하는 확장 AAA 모델

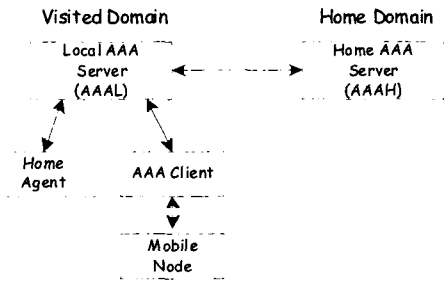


그림 4. Mobile IPv6를 지원하는 확장 AAA 모델

그림 4는 방문 망에 홈 에이전트가 위치하는 경우의 AAA 확장 모델을 나타낸다.

이동 노드에 대한 인증 처리 과정은 홈 망에 홈 에이전트가 위치하는 경우와 동일하다. 단, 이동 노드의 홈 에이전트가 방문 망에 동적으로 할당되는 경우,

로컬 AAA 서버는 ARR을 수신한 경우, 이동 노드의 요청 정보(feature-data)를 확인하여 방문 망에서 할당 가능한 경우, 관리하는 홈 에이전트를 할당한다. 이 경우, 이동 노드의 홈 주소 역시 함께 할당된다. 할당된 홈 주소는 MIPv6-Mobile-Node-Address AVP, 할당된 홈 에이전트 정보는 MIP-Candidate-Home-Agent-Host AVP, MIPv6-Home-Agent-Address AVP에 설정된다. 또한 홈 에이전트를 할당한 로컬 AAA 서버는 자신의 정보를 MIP-Originating-Foreign-AAA AVP에 설정한 ARR을 홈 AAA 서버에게 전송한다. ARR을 수신한 홈 AAA 서버는 정책에 따라서, 홈 에이전트를 방문 망에 할당 가능한 정책이라면, 로컬 AAA 서버로부터의 정보를 이용하여, 홈 에이전트의 정보를 MIPv6-Home-Agent-Address AVP와 MIPv6-Home-Agent-Host AVP로 설정한 HOR을 MIP-Originating-Foreign-AAA AVP에 포함된 로컬 AAA 서버를 통해서 방문 망의 홈 에이전트에 전송한다. HOA 역시 로컬 AAA 서버를 통하여 홈 AAA 서버로 전송된다.

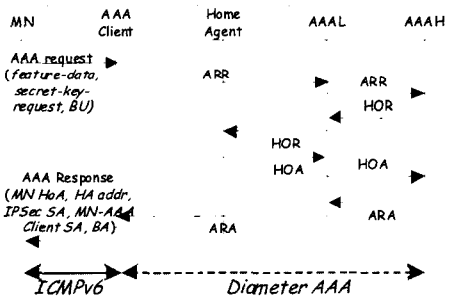


그림 5. 확장된 AAA Model의 정보 흐름도

그림 5는 이와 같은 처리를 하기 위한 정보의 흐름도이다.

3. 이동 노드와 로컬 AAA 간 인터페이스

본 논문은 이동 노드와 AAA 클라이언트 간 통신은 ICMPv6를 이용하도록 하며, AAA 클라이언트에서 홈 에이전트 간 통신은 Diameter 프로토콜을 이용하도록 한다. 이동 노드와 AAA 클라이언트 간 인증 요청 메시지(AAA-Request)와 인증 응답 메시지(AAA-Response)를 표1과 같이 정의한다.

Type 필드 값은 임의로 설정하며, 추후 결정한다. 추가적으로, 인증 받지 않은 이동 노드로부터의 Binding 연산을 불가하기 위하여 ICMPv6 Error 메시지를 추가 정의한다.

표 1. 이동 노드와 로컬 AAA 클라이언트간 ICMPv6메시지.

ICMPv6 msg	contents
AAA-Request (Type=TBD)	- NAI(Network Access Identifier) - Authentication data - Mobile node home address(*optional*) - Home agent address(*optional*) - Binding Update(*optional*) - Feature-Data - Security-Key-Request
AAA-Response (Type=TBD)	- NAI(Network Access Identifier) - Authentication data - Mobile node home address - Home agent address - Binding Acknowledgement(*optional*) - Feature-Data - Security-Key-Response
ICMPv6 Error (Type=1, Code=TBD)	- Destination Unreachable Error 중 AAA-Request requested

IV. Diameter 프로토콜의 보안 연관 설정 기법

Diameter 프로토콜은 망 접속 요청에 대해서 인증, 권한 검증 이외에 요청 시 필요한 노드를 위한 SA를 설정해 주어야 한다[1][2]. Trusted-Third party로서의 Diameter는 이동 노드의 요청에 따라서 두 가지 SA를 제공해야 한다. 하나는 이동 노드와 로컬 AAA 클라이언트간의 SA이고, 다른 하나는 이동 노드와 홈 에이전트 간 SA 이다. 두 가지 SA 모두 이동 노드가 요청한 경우 설정되며, MIPv6-Security-Key-Request AVP에 포함된다.

(1) 이동 노드와 로컬 AAA 클라이언트간의 보안 연관

- 인증 처리가 완료된 이후, 홈 망 AAA 서버는 두 노드 간에 이용할 SA를 생성한다. SA의 구성 요소는 키와 기타 부가 정보로 이동 노드와 로컬 AAA 클라이언트 간의 링크 계층(PPP, Wireless, etc)에 따라서 부가 정보는 내용이 달라진다.
- 이동 노드는 홈 AAA 서버와 이동 노드 간 소유하고 있는 AAA key와 사전 설정된 해쉬 알고리즘, 그리고 홈 AAA 서버가 생성하여 전달하는 Key Material을 이용하여 키를 생성한다. Key Material은 랜덤 넘버를 이용할 수도 있고, 인증 방식으로 EAP를 이용할 경우,

인증 과정 중에 발생되는 Master Secret Key를 이용할 수도 있다. 생성된 Key는 AAA 메시지를 통해서 로컬 AAA 클라이언트로 전송되고, 이동 노드와 AAA 클라이언트 구간이 안전하지 않으므로 이동 노드에게는 Key Material을 전송한다.

(2) 이동 노드와 홈 에이전트 간의 보안 연관(IPSec SA)

- Mobile IPv6가 명시하고 있는IKEv1과 같은 동적 키 교환 프로토콜을 이용할 수도 있지만, 인증 절차 완료 후에 이루어져야 하므로, 여러 번의 round-trip이 발생된다. 따라서 본 논문은 홈 망 AAA 서버가 해당 IPSec SA를 설정하여, 이동 노드와 홈 에이전트로 전송한다.
- 홈 망 AAA 서버는 인증을 완료한 시점에 이동 노드의 요청에 따라서 필요한 모든 정보를 설정한다. 이동 노드 요청 시 이미 결정된 이동 노드의 홈 주소와 홈 에이전트 기반으로 IPSec SA를 설정한다. IPSec SA는 기본적으로 단 방향이므로, 홈 망 AAA 서버는 이동 노드 -> 홈 에이전트, 홈 에이전트 -> 이동 노드에 대한 IPSec SA 쌍을 생성하도록 한다. 홈 에이전트로의 분배는 HOR 메시지에 해당 키 정보, SPI, key 등의 정보를 포함하여 전달하며, 이동 노드에는 ARA 메시지에 해당 키 정보 및 SPI, key material을 전달한다.
- 보안 키 생성 및 전달 방법은 이동 노드와 로컬 AAA 클라이언트 SA 키 생성 방법과 동일하다.

V. 이동 노드의 핸드오프 처리 절차

본 논문은 이동 노드가 핸드오프한 경우, Mobile IPv6와 Diameter 프로토콜간의 연동 시나리오를 동일 AAA 클라이언트 영역 내, 다른 AAA 클라이언트 간, 다른 도메인 간으로 분류하여 정의한다. 하나의 로컬 AAA 클라이언트는 복수개의 Access Router(AR)를 관리한다.

그림 6은 동일 AAA 클라이언트 영역 내 핸드오프를 나타낸다. 방문 망에서 power-up한 이동 노드는 AAA 인프라를 이용하여 첫 인증 절차를 수행한다. 성공적으로 인증이 처리된 경우, 홈 AAA 서버로부터 ARA를 통해서 인증 결과 및 권한 검증 정보를 수신한 로컬 AAA 클라이언트는 필터링 정보를 자신이 관리하는 모든 AR로 전달한다.

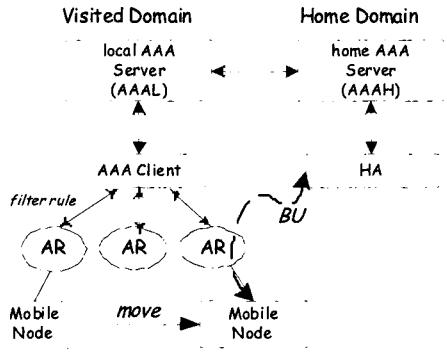


그림 6. 동일 AAA 클라이언트 내 핸드오프 처리

이동 노드가 동일 AAA 클라이언트 영역 내 다른 AR 영역으로 이동한 경우, 이동 노드는 새로운 CoA로 설정되고, BU를 발생시킨다. 발생된 BU는 인근 AR로 전송된다. 해당 AR은 필터링 정보에 의해서 BU를 AAA 인프라를 거치지 않고, 직접 홈 에이전트로 라우팅하여 Mobile IPv6 등록 절차를 수행한다.

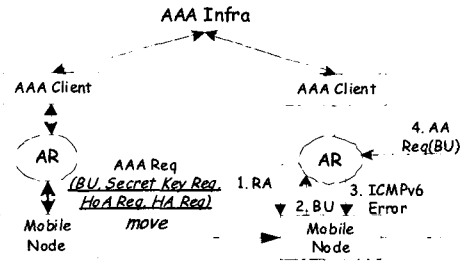


그림 7. AAA에 의한 재인증 처리 흐름도

그림 7은 서로 다른 AAA 클라이언트 간 핸드오프 시 AAA에 의한 재인증 처리 흐름도를 나타낸다.
방문 망에서 power-up한 이동 노드는 AAA 인프라를 이용하여 인증 절차를 수행한다. 성공적으로 인증이 처리된 경우, 인증 결과를 ARA를 통해서 수신한 로컬 AAA 클라이언트는 필터링 정보를 자신이 관리하는 모든 AR에게 전달한다.

이동 노드가 다른 AAA 클라이언트 영역으로 이동한 경우, 이동 노드는 수신한 Router Advertisement의 정보를 이용하여 CoA를 변경하고, BU를 생성하여 인근 AR로 전송한다. BU를 수신한 AR은 필터링 규칙에 따라서 수신한 BU에 대해서 오류 처리하고, ICMPv6 Error Message 중 Destination Unreachable

Error(Type=1, Code=TBD; AAA-Request requested) 메시지를 생성하여 이를 이동 노드로 전달한다. 전달 오류를 수신한 이동 노드는 AAA-Request를 생성, AAA 인프라를 통하여 다시 인증 절차를 수행한다. 이 경우, 이동 노드는 첫 인증에 따라 획득된 이동 노드의 홈 주소, 홈 에이전트 정보, IPSec SA 정보를 그대로 이용하고, 새롭게 설정된 CoA에 대한 BU를 생성하여 인증 요청 메시지에 포함시킨다.

이 경우, BU는 AAA 인증 요청 메시지에 그리고, HA에 의해서 처리된 BA역시 AAA 인증 응답 메시지에 piggybacking된다.

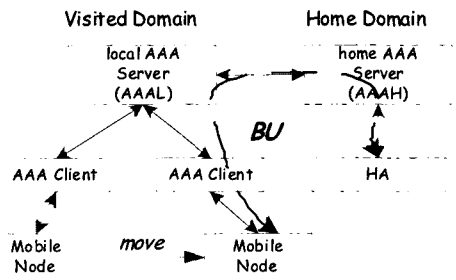


그림 8. 다른AAA 클라이언트 간 핸드오프 처리

그림8은 다른 AAA 클라이언트 간 핸드오프가 발생한 경우의 BU의 처리 흐름을 나타낸다.

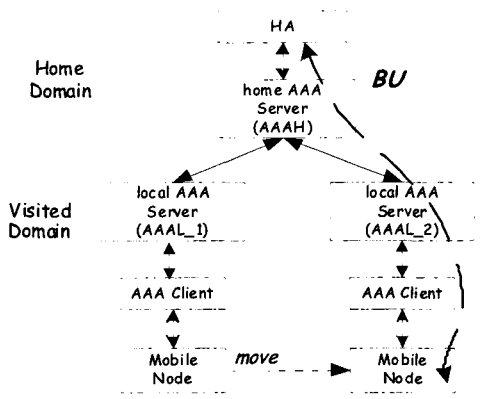


그림 9. 다른 도메인 간 핸드오프 처리

그림 9는 다른 도메인간 핸드오프가 발생한 경우의 BU의 처리 흐름을 나타낸다. 이동 노드가 다른 도메인으로 이동한 경우에는, 위 그림 7과 동일한 절차를 수행하여, AAA 인프라를 이용한 재인증 절차를 수행한다. 이때, BU/BA는 Diameter 메시지에 piggybacking되어 처리된다. 즉, 이동 노드는 처음 획득된(보유한) 홈 주소, 홈 에이전트, 보안 연관 정보들을 이용한다.

VI. 자료 구조

아래 표2는 홈 AAA 서버가 생성하여 이동 노드와 홈 에이전트에게 전달하는 이동 노드와 홈 에이전트 간 IPSec SA 파라미터이다.

표 2. IPSec SA entry items created by AAAH

filed	description
Source Address	Sender IP address
Destination Address	Receiver IP address
SPI	Security Parameter Index
IPSec Protocol	AH, EAP
Mode	Transport, Tunnel
Transform Id(s)	Transform id for IPSec Protocol
SA secret key(material)	Secret key(material)
SA Life Type	Seconds, bytes
SA Life Time	Life duration

다음 표3은 이동 노드가 홈 주소 및 홈 에이전트 정보, 보안 연관 설정 요청 정보를 담는 Feature-Data(MIPv6-Feature-Vector AVP)와 Security-Key-Request(MIPv6-Security-Key-Request AVP)의 값을 정의한다.

표 3. 상수값 정의

MIPv6-Feature-Vector : TBD	
Home_Agent_Requested	1
Mobile_Node_Home_Address_Requested	2
Home_Address_Allocatable_Only_In_Home_Domain	4
Home_Agent_In_Visited_Domain	8
Home_Agent_Available	16
MIPv6-Security-Key-Request :TBD	
REQ_NO_SA	0
REQ_MN_AR_SA	1
REQ_MN_HA_SA	2

다음 표4는 키를 제외한 IPSec SA 파라미터를포함하는 그룹 형식의 MIPv6-HA-MN-Key AVP와 MIPv6-MN-HA-Key AVP의 구조를 나타낸다.

표 4. PSec SA 파라미터 구조

MIPv6-IPsec-SPI AVP
MIPv6-Key-LifeType AVP
MIPv6-Key-LifeDuration AVP
MIPv6-IPsec-Protocol-Id AVP
MIPv6-IPsec-Transform-Id AVP
MIPv6-IPsec-EnCap-Mode

VII. 보안 관련 사항

Mobile IPv6 서비스를 지원하기 위한 Diameter 프로토콜은 다음과 같은 사전 요구 사항을 갖고 있다.

- 이동 노드와 홈 AAA 서버는 사전에 보안 연관(long term AAA key, authentication method, hash algorithm, etc)을 갖는다.
- 로컬 AAA 서버(AAAL)와 홈 AAA 서버(AAAH) 간에는 안전한 통신 채널이 존재한다.
- Diameter AAA 프로토콜은 End-to-End 보안이 제공되지 않으므로, End-to-End 보안이 반드시 필요한 경우, Redirect 기법을 이용하여 두 노드간 직접 통신이 가능하도록 한다.

VIII. 결 론

Mobile IPv6 서비스가 상업망에서 보다 널리 사용되기 위해서는 Diameter 프로토콜이 제공하는 인증, 권한 검증, 과금 기능 및 이동성 지원 기능과 원활한 연동이 가능해야 한다. 본 논문은 Diameter 프로토콜과 Mobile IPv6 프로토콜과의 연동 시나리오를 정의하고, 특히 이동 노드의 요청에 따라서 이동 노드의 홈 주소 설정, 홈 에이전트 할당, 이동 노드와 홈 에이전트 간 IPSec SA, 이동 노드와 로컬 AAA 클라이언트 간 SA를 설정해서 분배함으로써, Mobile IPv6에 대해서 탄력성을 제공한다. 또한 이동 노드의 영역별 이동에 따른 핸드오프 시 연동 과정에 대해서 상세히 설계하였다.

Diameter 프로토콜이 제공하는 IPSec SA 설정 기능을 이용하는 경우, 보안 정책 및 SPI와 같은 값이 IKE와 같은 키 교환 프로토콜을 이용하는 경우와 충돌이 발생하지 않도록 운용 관리하는 정책 서버가 필요하다. 이러한 정책 서버로 하여금, 이동 노드가 Diameter 프로토콜이 제공하는 보안 연관을 이용하거나, 이를 이용할 수 없는 경우 자체적으로 홈 에이전트와 키 교환 프로토콜을 이용하는 경우에 대해서 모두 정상 운용될 수 있도록 하는 연구가 보완적으로 필요하다.

IX. 참 고 문 헌

[1] Stefano M. Faccin, Franck Le, Basavaraj Patil, and Charles E. Perkins, "Mobile IPv6 AAA Requirements", *IETF* Internet-draft, draft-le-aaa-mipv6-requiremets-03.txt, February 2004

[2] S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP AAA Requirements", *IETF* RFC2977, October 2000

[3] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol", *IETF* RFC3588, September 2003

[4] J. Arkko, V. Devarapalli, and F. Dupong, "Using IPSec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", *IETF* Internet-draft, draft-ietf-mobileip-mipv6-ha-ipsec-06.txt, June 30, 2003

[5] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", *IETF* Internet-draft, draft-ietf-mobileip-ipv6-24.txt, June 30, 2003

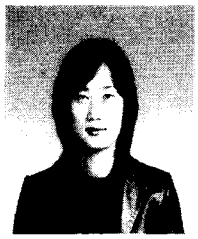
[6] Pat R. Calhoun, Tony Hohansson, C. Perkins, and T. Hiller, "Diameter Mobile IPv4 Application", *IETF* Internet-draft, draft-ietf-aaa-diameter-mobileip-16.txt, February 2004

[7] D. Harkins, and D. Carrel, "The Internet Key Exchange (IKE)", *IETF* RFC2409, November 1998

[8] Stefano M. Faccin, Franck Le, Basavaraj Patil, and C. Perkins, "Diameter Mobile IPv6 Application", *IETF* Internet-draft, draft-le-aaa-diameter-mobileipv6-03.txt, April 2003

[9] 김말희, 김현곤, "이동성을 지원하는 Diameter 기반 AAA", *추계종합학술대회*, 26권, 2002.11.23

김 말 희(Marie Kim) 정회원



1996년 1월 : 서강대학교 전자계산학과 학사
1998년 1월서강대학교 전자계산학과 석사
1998년 1월~2000년 11월 : 삼성전자 통신연구소 근무
2004년 11월 현재한국전자통신연구원 정보보호연구단 AAA정보보호연구팀 근무
E-mailmariekim@etri.re.kr

<관심분야> 이동통신, 정보보호

김 현 곤

1992년 2월 : 금오공과대학교 전자공학과 학사
1994년 2월 금오공과대학교 전자공학과 석사
2003년 2월 : 충남대학교 대학원 전자공학과 박사
1994년 현재한국전자통신연구원 정보보호연구단 AAA정보보호연구팀장 근무
E-mailhyungon@etri.re.kr

<관심분야> IP 기반의 이동통신 정보보호, RFID/USN 정보보호