情報保護學會論文誌
第14券 第1號, 2004. 2

AAA 기반 Mobile IP 환경에서 안전하고 빠른 핸드오프 기법 설계

김 현 곤†

한국전자통신연구원

Design of a Secure and Fast Handoff Method for Mobile IP with AAA Infrastructure

Hyun Gon Kim†

ETRI

요 약

Mobile IP Low Lattency Handoffs[1]는 Mobile IP 등록 요청 절차를 처리하는데 발생하는 지연을 최소화시켜 실시간 서비스를 가능하게 해준다. 그러나 인증, 권한 검증, 과금을 지원하는 AAA 기반의 Mobile IP 망에서는 매 지역등록이 일어날 때마다 새로운 세션 및 세션 키가 필요하며, 이를 위해 홈 망까지 등록 절차가 수행되어야 한다. 이로 인해, 이동 노드 재인증 절차와 방문 망에서 홈 망까지의 트랜잭션으로 인한 통신 지연이 발생한다. 이러한 지연을 줄이기 위해서 본 논문에서는 홈 망의 AAA 서버를 관여시키지 않고, 이전에 할당된 세션 키를 재사용하여 Low Latency Handoffs를 수행하는 기법을 제안한다. 이 기법에서는 이전 방문 에이전트와 새로운 방문 에이전트가 세션 키를 교환하는 단계에서 발생하는 보안 취약점을 해결하기 위하여 게이트웨이 방문 에이전트로 하여금 신뢰할 수 있는 제 3자 역할을 수행하도록 하고 이를 통해 키를 공유한다. 제안한 기법에 의하면 홈 망까지의 트랜잭션이 필요없고, 세션 키의 기밀성과 무결성이 보장되므로 이동 노드가 빠르고 안전하게 핸드오프를 수행할 수 있다.

ABSTRACT

Mobile IP Low Latency Handoffs[1] allow greater support for real-time services on a Mobile IP network by minimizing the period of time when a mobile node is unable to send or receive IP packets due to the delay in the Mobile IP Registration process. However, on Mobile IP network with AAA servers that are capable of performing Authentication, Authorization, and Accounting(AAA) services, every Registration has to be traversed to the home network to achieve new session keys, that are distributed by home AAA server, for a new Mobile IP session. This communication delay is the time taken to re-authenticate the mobile node and to traverse between foreign and home network even if the mobile node has been previously authorized to old foreign agent. In order to reduce these extra time overheads, we present a method that performs Low Latency Handoffs without requiring further involvement by home AAA server. The method re-uses the previously assigned session keys. To provide confidentiality and integrity of session keys in the phase of key exchange between agents, it uses a key sharing method by gateway foreign agent that performs a trusted thirty party. The proposed method allows the mobile node to perform Low Latency Handoffs with fast as well as secure operation

Keywords: *Low Latency Handoffs, Mobile IP, AAA*

접수일: 2003년 10월 15일; 채택일: 2004년 1월 15일

† hyungon@etri.re.kr

Ⅰ. 서 론

Mobile IP[2,3]는 지연이나 패킷손실을 유발할 수 있어 지연에 민감한 실시간 서비스에 적용하기에는 부적합하다. 이러한 지연을 줄이기 위해 Low Latency Handoffs(LLH)[1]가 제안되었으며, 현재 IETF에서 표준화를 진행하고 있다. LLH는 이동 노드(MN; Mobile Node)가 홈 에이전트(HA; Home Agent)로부터 패킷을 수신하는 기본적인 Mobile IP 모델[3]과 게이트웨이 방문 에이전트(GFA; Gateway Foreign Agent)로부터 패킷을 수신하는 지역 등록(Regional Registration) 모델[9]에 둘 다 적용 가능하다. 전자에서는 방문 망과 MN의 홈 망간 거리가 길어질수록 등록을 위한 지연 시간이 커지나, 후자에서는 이를 개선하여 로컬 등록을 이룸으로써 지연을 줄이고 있다.

한편, AAA(Authentication, Authorization, and Accounting)는 다양한 유무선 서비스에 대하여 인증, 권한 검증, 과금을 수행한다. 이 중 Mobile IP 서비스에 대해서는 MN의 인증, 권한 검증, 과금, 노드간 인증 등의 기능을 수행하며 특히, 최근에 AAA 프로토콜로서 표준화되고 있는 Diameter[5~7]는 Mobile IP 프로토콜과 밀접하게 결합되어 있다.

본 논문에서는 표준에서 고려하고 있지 않는 LLH에 AAA 인프라를 적용하는 시나리오를 다룬다. 이러한 환경에서 핸드오프로 인한 Mobile IP 등록이 요청되면 Mobile IP의 인증 메커니즘에 의해서 단말과 새로운 FA 그리고 HA간 보안 연관(SA; Security Association)이 새롭게 설정되어야 한다. 이를 위해서 홈 망의 AAA 서버에 의해 세션 키의 생성 및 분배가 이루어져야 한다. 즉, Mobile IP 등록이 이루어질 때마다 새로운 세션 키 생성을 위해 MN의 재 인증 및 세션 키 분배 절차가 요구된다. 이로 인해 방문 망에서 홈 망까지 트랜잭션이 발생하며, 빠른 핸드오프를 기하는 LLH의 장점을 살릴 수 없다. 이러한 built-in delay 요소를 제거하기 위하여 본 논문에서는 AAA 기반 Mobile IP에서 LLH의 장점을 살릴 수 있는 기법을 제안하고자 한다.

제안한 기법은 이전에 할당된 세션 키를 재사용함으로써 핸드오프로 인해 요구되는 새로운 세션 키 할당의 필요성을 없앴다. 그러나 세션 키가 안전하지 않는 공개된 채널상에서 전달되기 때문에 공격자가 Mobile IP 등록 메시지를 Sniffing하여 세션 정보를 획득할 수 있다. 이러한 세션 가로채기(Session Stealing) 공격을 막기 위해서는 세션 키의 기밀성(Confidentiality)과 무결성(Integrity)이 보장되어야 한다. 유사한 목적으로 공개키 암호를 기반으로 세션 키의 기밀성을 제공하는 기법[7]이 제안되어 있으나, 공개키 암호 오퍼레이션에 의해 발생되는 긴 지연, 고비용, 인프라 구성의 어려움 때문에 현실적으로 적용이 쉽지 않다. 따라서 안전하고 가벼운 세션 키 교환 기법이 필요하다.

본 논문의 구성은 제 1장의 서론에 이어, 2장에서는 관련연구로서 핸드오프 시 AAA를 이용한 등록 및 인증과정과 AAA 기반 LLH를 소개하고, 기존에 제안된 세션 키 교환 기법을 조사했다. 3장에서는 먼저 키 교환 단계에서 세션 가로채기 공격의 가능성을 진단해본 후, 제안한 세션 키 교환 기법을 기술하였다. 4장에서는 제안한 기법이 세션 가로채기 공격에 안전한지를 분석하였다. 5장에서는 시뮬레이션을 통해 기본 공개키 암호 오퍼레이션과 제안한 암호 오퍼레이션의 성능을 비교하였으며, 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

이 장에서는 먼저 Mobile IP 인프라와 AAA 인프라가 결합된 경우, Mobile IP 등록과 사용자 인증에 대해 설명한다. 그리고 LLH 및 지역 등록의 기본 동작에 대해 소개한다.

2.1 핸드오프 시 AAA를 이용한 등록 및 인증과정

사용자 인증은 가입자의 홈 망에 위치한 AAAH (Home AAA server)가 수행한다. 핸드오프시 즉, Mobile IP등록 시, AAAH는 Mobile IP 엔티티들이 사용할 세션 키를 생성하고, 이 키들을 동적으로 분배하는 키 분배 센터 역할을 수행한다. 키의 분배는 사전에 이루어지지 않고 Mobile IP 등록 시점에 동적으로 분배되며, AAA 메시지내에 세션 키들이 embedded되어 전달된다.

그림 1을 기준으로 사용자 인증 및 동적 SA 키 분배 동작을 설명한다. 매 Mobile IP 세션마다 할당되는 세션 키는 lifetime을 가지며, 등록의 효율성을 기하기 위해 lifetime은 Mobile IP 등록 lifetime보다 길게 지정된다. 즉, 한번 인증된 결과

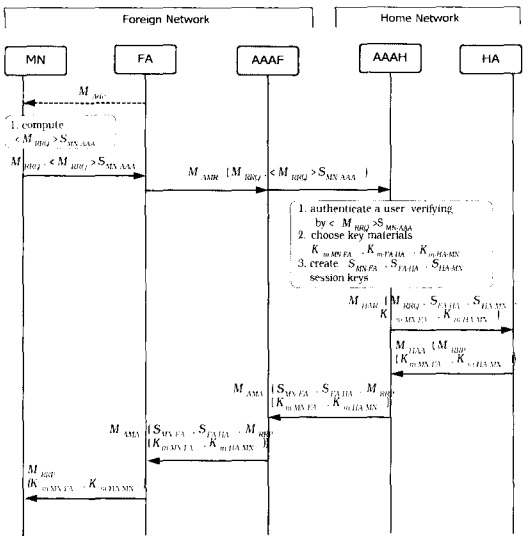

그림 1. AAA 기반 Mobile IP 등록 인증

를 계속된 다수의 Mobile IP 등록에서 활용된다.

2.2.1 사용자 인증 및 메시지 무결성 검사

⊙ Mobile IP 등록을 요청하는 MN은 자신이 AAAH와 사전에 공유하고 있는 비밀키 S_{MN-AAA}를 가지고 Mobile IP 등록 요청 메시지인 M_{RRQ} (Mobile IP Registration Request Message)를 해쉬하고, 그 결과 값을 MN-AAA 확장자를 만들어 M_{RRQ}내에 인캡슐레이션 시켜서 FA로 전달한다.

⊙ 이를 수신한 FA는 AAA서버에게 등록 인증을 요청하는 M_{AMR}(AA-Mobile-Node-Request)를 만들고 MN-AAA 확장자를 그대로 전달한다.

⊙ 인증 요청을 받은 방문망의 AAAF(Foreign AAA Server)는 MN의 ID인 NAI(Network Access Identifier)를 확인하여 자신의 가입자가 아님을 판단하고, 홈 망의 AAAH에게 라우팅한다.

⊙ AAAH는 자신이 MN과 사전 공유하고 있는 비밀키 S_{MN-AAA}를 가지고 수신한 M_{RRQ}를 해쉬한 후, 수신한 해쉬 값과 비교하여 사용자 인증과 메시지 무결성을 검증한다.

2.2.2 세션 키 생성 및 분배 과정

⊙ 사용자 인증이 성공하면, AAAH는 해당 등록에 해단 세션 키 생성과정에 들어간다. 해쉬 함수의 입력으로 들어갈 키 재료인 랜덤 값 $K_{M-MN-FA}$ (MN과 FA간 사용될 랜덤 값), $K_{M-FA-HA}$(FA와 HA간 사용될 랜덤 값), $K_{M-HA-MN}$(HA와 MN간 사용될 랜덤 값)들을 생성한 후, 아래와 같이 해쉬 함수를 이용하여 세션 키들을 생성한다.

$$S_{MN-FA},\ S_{FA-HA},S_{HA-MN} = HMAC\text{-}MD5$$
$$(S_{MN-AAA}, \{K_{m-xx-xx} \mid node's\_IP\})$$

⊙ AAAH는 세션 키를 생성한 후, 홈 에이전트에게 등록을 요청하는 M_{HAR}(Home-Agent-MIP-Request Message)를 만들고 MN과 FA간 세션 키 S_{MN-FA}과 FA와 HA간 세션 키 S_{FA-HA}를 메시지내에 인캡슐레이션 시켜 HA에게 전달한다. 추가적으로 MN이 자신과 관련된 세션 키를 계산할 수 있도록 키 재료인 $K_{m-mn-FA}$과 $K_{m-HA-MN}$를 전달한다.

⊙ HA는 M_{HAR}를 디캡슐레이션 시켜서 M_{RRQ}를 분석하고 Mobile IP 등록을 수행한다. 등록이 성공하면, 등록 응답 메시지인 M_{RRP}(Mobile IP Registration Reply)를 만들고 수신한 두개의 키 재료들을 덧붙인다. 그리고 M_{HAA}(Home-Agent-MIP-Answer Message)를 만들고 M_{RRP}를 인캡슐레이션 시켜서 AAAH에게 전달한다.

⊙ AAAH는 M_{AMA}를 만들고 FA에서 필요한 세션키 S_{MN-FA}과 S_{FA-HA}를 AAAF를 거쳐 FA에게 전달한다.

⊙ FA는 M_{AMA}를 디캡슐레이션 시켜서 M_{RRP}를 분석하여 등록 응답을 처리한다. 그리고 이를 MN에게 전달한다.

⊙ 마지막으로 MN은 M_{RRP}내에서 키 재료들 $K_{m-MN-FA}$과 $K_{m-HA-MN}$를 가지고 AAAH와 동일한 해쉬 함수를 이용하여 자신이 필요한 S_{MN-FA}과 S_{HA-MN}을 생성한다. 이와 같은 일련의 과정을 통해 Mobile IP 등록과 Mobile IP 엔티티들간에 세션 키 분배가 동시에 이루어진다.

2.2 Low Latency Handoffs 및 지역 등록 소개

Mobile IP는 서로 다른 FA에 의해 서비스되는 서브넷간의 IP 계층 핸드오프 절차를 규정하고 있다. 그러나 어떤 경우 Mobile IP에서의 핸드오프 시에 발생되는 지연이 지연에 민감하거나 또는 실시간성을 요하는 서비스에서 요구하는 조건을 만족시키지 못할 경우가 있다. 이러한 지연을 줄이기 위해 제안된 것이 LLH 기법이다.

LLH는 사전 등록(pre-registration) 핸드오프,

사후 등록(post-registration) 핸드오프, 그리고 이 두가지 기법을 결합한 혼합 등록 핸드오프로 나뉘어진다. 사전 등록 핸드오프는 MN이 네트워크의 도움을 받아 2 계층 핸드오프 완료 이전에 3 계층 핸드오프를 수행하는 기법이다. 사후 등록 핸드오프는 이전 FA(oFA)와 새로운 FA(nFA)간에 양방향 터널을 설정하여 MN이 nFA영역으로 이동하여도 oFA를 계속 사용될 수 있다. 즉, 2 계층 핸드오프 완료 이전에, 3 계층 핸드오프 완료가 가능하면 사전 등록 핸드오프 방법을 사용하고, 그렇지 못한 경우는 사후 등록 핸드오프 기법을 사용한다.

본 논문에서는 사전 등록 핸드오프 기법만을 그 대상으로 한다. 이의 이유로서 사후 등록의 경우, 기존 oFA와 MN이 이동하려는 새로운 nFA간 핸드오프 이전에 양방향 또는 단방향 터널이 설정되어 있으므로 세션 키 또한 사전에 서로 주고 받을 수 있다. 따라서 본 논문에서 적용하고자 하는 동적 세션 키 전달이 필요 없다.

LLH는 방문 망내에서 로컬 등록을 수행하는 지역 등록[1]을 고려하고 있다. 그림 2에 AAA 기반 LLH의 절차를 개념적으로 나타내었다. MN이 Mobile IP 등록 요청을 하여 성공적으로 인증 및 권한 검증이 되면, AAAH는 Mobile IP 엔티티들 즉, MN, FA, 그리고 HA를 위한 세션 키들(mobile-foreign, foreign-home, and mobile-home session key)을 생성하고 분배한다. 이후, 핸드오프가 발생하면 로컬에서 지역 등록이 수행된다.

메시지 1a는 Router Solicitation(RtSol)이며, 1b는 Router Advertisement(RtAdv)이다. 이 메시지는 oFA가 요청한 것이며, oFA는 nFA로부터 수집한 정보를 캐쉬 한다. 메시지 2a는 Proxy Router Solicitation (PrRtSol)이며, 이 메시지를 수신한 라우터는 다른 라우터에게 광고를 요청한다. 메시지 2a를 수신하면 oFA는 Proxy Router Advertisement (PrRtAdv)를 응답한다. MN은 이동했음을 감지하고, nFA에게 메시지 3a를 보내 지역 등록((Reg)RegReq)을 요청한다. 메시지 4와 5는 지역 등록들의 요청과 응답이다. 만약 지역 등록이 성공하면, MN은 GFA와 nFA를 통해 통신을 이룬다.

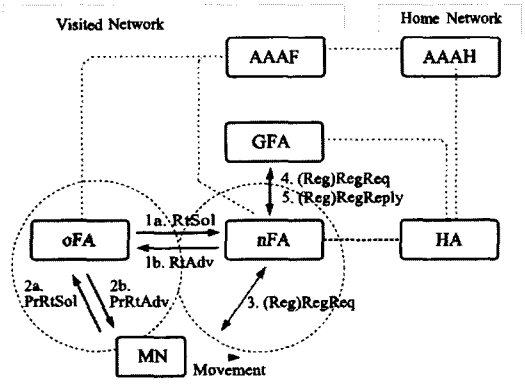

그림 2. AAA 기반 Low Latency Handoffs

2.3 관련된 세션 키 교환 기법

본 논문에서와 같이 세션 키를 안전하게 전달하기 위해서는 제안된 다음과 같은 공개키 인증 기법들을 적용할 수 있다. Jacobs는 Mobile IP에 공개키 인증 기법[8]의 도입을 제안하였다. 이 기법에서는 등록 메시지들의 안전성을 위하여 MN과 FA 및 HA들간에 인증서를 사용하고 X.509 전자서명을 수행한다. MN, FA, HA 각기 상호간에 공개키 인증 기법을 따른 인증 동작을 수행한다. 메시지를 새로 만들거나 받은 메시지를 전달하는 경우, 메시지 뒤에 전자서명을 추가함으로써 메시지의 무결성과 부인 봉쇄 기능을 제공한다.

Sufatrio, K. Lam의 Mobile IP를 위한 최소 공개키 인증 기법[10]을 제안하였다. 이 기법에서는 Jacobs의 공개키 인증 기법이 갖는 단점을 개선하기 위해 공개키 암호 연산을 최소화하였다. 그리고 공개키 방식과 비밀키 방식을 조합하여 적용함으로써 Jacobs의 기법에서 생기는 오버헤드를 최소화하였다.

IETF에서는 Mobile IP를 위해 공개키 인증 기법을 적용하는 방안을 표준화[7]하고 있다. 이 기법에서는 MN이 관여되지 않으며, Mobile IP 엔티티들과 AAA 엔티티들간에 노드간 상호 인증을 위해 공개키 인증 기법을 적용한다.

그러나 상기의 공개키 인증 기법들을 적용할 수 있으나 공개키 암호 연산에 소요되는 긴 지연시간은 빠른 핸드오프에 부적합하다. 또한, 공개키 인프라가 구축에 비용이 많이 든다는 단점이 있다.

Ⅲ. 안전한 세션 키 교환 기법

AAA 환경에서도 지역 등록을 이루기 위해서는 몇 가지 방안이 있을 수 있으나, 본 논문에서는 이전에 할당된 세션 키를 재사용하는 방법을 사용하였다.

그리고 세션 키 재사용에 따른 보안 취약성을 해결하였다. 이 장에서는 Mobile IP 세션의 가로채기 공격 가능성을 점검해보고, 이를 방지하기 위한 안전한 세션 키 교환 기법을 제안한다.

3.1 키 교환 단계에서 세션 가로채기 공격

세션 키의 lifetime은 잦은 키 분배로 인한 지연을 줄이기 위해 충분히 크게 설정되도록 권장하고 있다. 한때, AAAH에 의해 세션 키가 분배되면 oFA는 두개의 세션 키 즉, mobile-foreign과 foreign-home 세션 키를 가지게 된다. 정상적으로 통신이 이루어지는 상태에서 MN이 nFA 영역으로 이동하면 LLH가 수행된다. 그러나 이 때, nFA는 세션 키가 없으므로 키 획득을 위해 홈 망의 AAAH를 거쳐 정상적인 Mobile IP 등록 절차를 수행해야 한다. 이 경우, LLH가 갖는 장점인 지역 등록은 수행될 수 없게 된다. 지역 등록의 장점을 살리기 위해서 본 논문에서는 lifetime이 충분한 이전 세션 키를 재사용하여 지역 등록을 수행한다. 이 경우, 홈 망의 AAAH까지 재 등록 절차가 생략되므로 지연을 최소화할 수 있다.

그러나 이 기법이 feasibility를 제공하기 위해서는 oFA가 보유한 세션 키들을 nFA에게 안전하게 전달해야 하는 문제점을 해결해야 한다. 특히 HA와 oFA와 사용되었던 foreign-home 세션 키는 64비트의 랜덤 값이고, 해쉬되지 않으므로 쉽게 노출될 수 있다. 이러한 보안 취약점을 해결하기 위해 키 교환 단계에서 반드시 기밀성이 보장되어야 한다. 유사한 목적으로 Jocobs[8]가 공개키를 기반으로 하여 기밀성을 제공하는 기법을 제안하였다. 그러나 이 기법의 단점은 모든 FA가 공개키 암호 오퍼레이션을 수행함으로 인해 지연이 크고 공유기 방식에 비해 높은 비용으로 인해 현실적인 솔루션이 되지 못하고 있다. 따라서 안전하고 가벼운 오퍼레션이 가능한 새로운 세션 키 교환 기법이 제안되어야 한다.

3.2 제안한 세션 키 교환 기법

제안한 기법은 지역 등록을 적용하며, 이를 위해서 이전에 할당된 세션 키를 재사용 한다. 그리고 공개키 오퍼레이션 대신에 신뢰 할 수 있는 제 3자를 두어 키를 공유하는 프로토콜을 적용한다. 이 기법에서는 GFA가 FA들간에 신뢰할 만한 제 3자 역할을 수행하도록 하였다.

지역 등록에서 정의된 바와 같이 GFA는 hierarchy 상에서 상위에 정적으로 존재하며, 다수의 FA들을 하위에 두고 있다. GFA는 로컬 망내에 위치하는 AAAF와 사전 SA가 설정되어 있으며, 해당 망내에서 trusted area 내에 존재한다고 가정한다. 인접한 GFA간에 발생하는 핸드오프는 LLH 및 제안한 알고리즘이 동작하지 않고, 홈 망까지의 재등록 및 재인증 절차가 수행된다.

아래의 설계 원칙과 가정을 따른다.

- ⊙ MN의 관리 비용과 컴퓨팅 파워를 최소화한다.
- ⊙ 추가적인 메시지를 정의하지 않고 LLH에 정의된 메시지만을 사용하여 기존 LLH와 호환성을 유지한다.
- ⊙ GFA와 FA 사이에 보안 연관이 있다고 가정한다. 즉, GFA는 FA를 인증할 수 있다.
- ⊙ 세션 가로채기 공격을 막기 위해 세션 키들은 암호화되고 안전한 방법으로 교환되어야 한다.

아래의 기호를 사용하였다.

- ⊙ $S_{MN\text{-}FA}$, $S_{FA\text{-}HA}$, $S_{MN\text{-}HA}$: MN과 FA간, FA와 HA간, 그리고 MN과 HA간 Mobile IP 공유 세션 키
- ⊙ $K_{oFA\text{-}nFA}$: 임시로 계산되고 저장되지 않는 oFA와 nFA간 동적 세션 키
- ⊙ $<M>K$: 키 K에 의한 메시지 M의 MAC 값
- ⊙ $\{M\}K$: 키 K에 의한 메시지 M의 암호화
- ⊙ K_{FA}: FA와 GFA 사이의 공유 키
- ⊙ R: 랜덤 값
- ⊙ Id_{FA}: FA의 identity (예: FA의 IP 주소)
- ⊙ M_{RRQ}: Mobile IP의 지역 등록 요청 메시지
- ⊙ M_{RRP}: Mobile IP의 지역 등록 응답 메시지

상기에 기술한 바와 같이, 이전에 할당된 $S_{MN\text{-}FA}$, $S_{FA\text{-}HA}$를 재 사용한다. 이 세션 키들을 암호화하고 복호화하기 위해서 oFA와 nFA사이에 short-lived 비밀 키인 $K_{oFA\text{-}nFA}$를 사용한다. 이 키는 신뢰할 수 있는 GFA에 의해 동적으로 분배되고 공유된다. 아래에 LLH의 Network-Initiated Handoff와 Mobile-Initiated Handoff 에 제안한 기법을 각기 적용하였다.

3.2.1 Network-Initiated(NI) Handoff

NI 핸드 오프에서 단말은 nFA의 라우터 광고

(RtAdv: Router Advertisement) 메시지, 실제로는 프락시 라우터 광고(PrRtAdv: Proxy RtAdv) 메시지를 oFA를 통해 수신한다. 그림 3에 제안한 NI 핸드오프의 흐름 및 오퍼레이션을 보였으며, 다음과 같이 동작한다.

⊙ **라우터 광고**

(a1) nFA → oFA : *RtAdv*

- oFA choose a random number R
- oFA computes $K_{oFA\text{-}nFA}=<R, Id_{oFA}>K$
- oFA computes $E=\{S_{MN\text{-}FA}, S_{FA\text{-}HA}\}K_{oFA\text{-}nFA}$

(a2) oFA → MN : PrRtAdv, R, E, Id_{oFA}

먼저 nFA가 *RtAdv*를 주변 FA들에게 전송한다. 이를 수신한 oFA는 랜덤 생성 함수로부터 랜덤 값을 생성한다. 그리고 자신과 GFA 사이의 공유 비밀키인 K_{oFA}로 R과 Id_{oFA}에 대한 MAC 값을 취해 ($K_{oFA\text{-}nFA}=\langle R, Id_{oFA}\rangle K_{oFA}$) oFA와 nFA간에 동적 공유 비밀 키인 $K_{oFA\text{-}nFA}$를 생성한다. oFA는 이 키를 이용하여 이전 Mobile IP 등록에서 할당 받은 세션 키 $S_{MN\text{-}FA}$ 및 $S_{FA\text{-}HA}$를 암호화($E=\{S_{MN\text{-}FA}, S_{FA\text{-}HA}\}K_{oFA\text{-}nFA}$)) 한다.

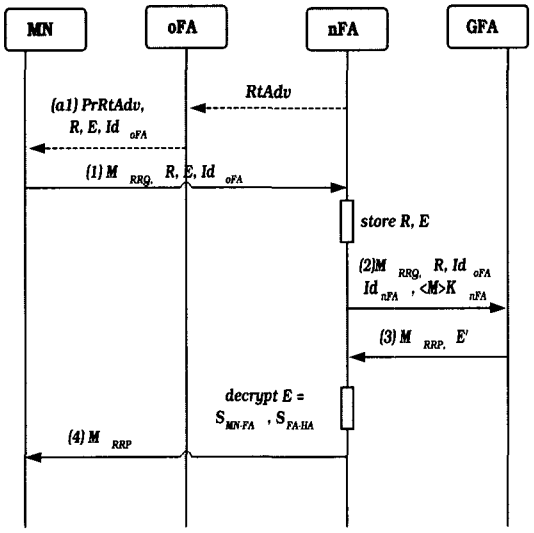

그림 3. 제안한 NI 핸드오프 오퍼레이션

⊙ **Mobile IP 등록 요청**

(1) MN → nFA : M_{RRQ}, R, E, Id_{oFA}

- nFA stores E
- nFA computes $<M>K_{nFA}$ where $M=M_{RRQ}$, R, Id_{oFA}, Id_{nFA}

(2) nFA → GFA: $M_{RRQ}, RId_{oFA}, Id_{nFA}, <M>K_{nFA}$

- GFA authenticates nFA validating $<M>K_{nFA}$
- GFA computes $K_{oFA\text{-}nFA}=<R, Id_{oFA}>K_{oFA}$
- GFA computes $E'=\{K_{oFA\text{-}nFA}\}K_{nFA}$

MN은 Mobile IP 등록 메시지를 생성한 후, 무선 인터페이스를 통해 수신한 에이전트 광고 메시지로부터 R, E, Id_{oFA}를 추출한 후, 등록 메시지내에 임베디드시켜 nFA로 전송한다. nFA는 MN이 요청한 Mobile IP 등록을 수행하고, 암호화된 세션 키인 E를 저장한다. 그리고 자신과 GFA 사이의 공유 비밀키인 K_{nFA}로 $M=M_{RRQ}, R, Id_{oFA}, Id_{nFA}$에 대한 MAC 값을 취한다. nFA는 M_{RRQ}, R, Id_{oFA}에다 자신의 ID인 Id_{nFA}와 계산된 MAC 값을 포함시켜 GFA로 전송한다.

GFA는 HA역할을 수행하여 Mobile IP 지역 등록을 수행한다. 그리고 K_{nFA}를 가지고 M에 대한 MAC 값을 취해($<M>K_{nFA}$) nFA를 인증한다. 인증이 성공하면 K_{oFA}를 가지고 R과 Id_{oFA}에 대한 MAC을 취해($K_{oFA\text{-}nFA}=<R, Id_{oFA}>K_{oFA}$) oFA와 nFA간에 동적 비밀 공유 키인 $K_{oFA\text{-}nFA}$를 재생한다. 그리고 K_{nFA}로 $K_{oFA\text{-}nFA}$를 암호화하여($E'=\{K_{oFA\text{-}nFA}\}K_{nFA}$) E'을 생성한다. 정상적인 Mobile IP 응답 메시지를 생성하고 E'을 포함시켜 nFA로 전송한다.

⊙ **Mobile IP 등록 응답**

(3) GFA → nFA : M_{RRP}, E'

- nFA obtains $K_{oFA\text{-}nFA}$ by decrypting E' under the key K_{nFA}
- nFA retrieves E and decrypts it under the key $K_{oFA\text{-}nFA}$

(4) nFA → MN : M_{RRP}

GFA로부터 Mobile IP 등록 응답 메시지를 수신한 nFA는 등록 응답 처리를 수행한 후, K_{nFA}로 E'을 복호화하여 $K_{oFA\text{-}nFA}$를 $K_{oFA\text{-}nFA}$ 추출한다. 그리고 저장되어 있는 E를 가져온 후, $K_{oFA\text{-}nFA}$로 복호화하여 이전 Mobile IP 등록에서 할당 받은 세션 키인 $S_{MN\text{-}FA}$ 및 $S_{FA\text{-}HA}$를 획득한다. 최종적으로 얻어진 이 세션 키들은 핸드오프 이후, 트래픽이 송수신될 때 암호화 및 복호화 키로 사용된다. nFA는 Mobile IP 등록 응답 메시지를 MN에게 송신하면 절

차가 완료된다.

3.2.2 Mobile-Initiated(MI) Handoff

MI 핸드 오프에서 MN은 프락시 라우터 요청(PrRtSol: Proxy Router Solicitation)을 oFA에게 요구한다. 그림 4에 제안한 MI 핸드오프의 흐름 및 오퍼레이션을 보였으며, 다음과 같이 동작한다.

⊙ 라우터 요청 및 광고

(a1) MN → oFA : **Pr***RtSol*

- oFA choose a random number R
- oFA computes $K_{oFA\text{-}nFA}$=<R, Id_{oFA}>K_{oFA}
- oFA computes E={$S_{MN\text{-}FA}$, $S_{FA\text{-}HA}$}$K_{oFA\text{-}nFA}$

(a2) oFA → nFA : $RtSol$,R,Id_{oFA},E

- nFA stores R,Id_{oFA},E

(a3) nFA → oFA : $RtAdv$

(a4) oFA → MN : **Pr***RtAdv*,R,Id_{oFA}

MN은 이동 중에 새로운 FA 영역에 진입했음을 판단하고, 네트워크 측에 프락시 라우터 요청(**Pr***RtSol*: Proxy Router Solicitation)를 요청한다. 이를 수신한 네트워크측의 oFA는 nFA에게 $RtSol$을 요청하기 전에 랜덤 생성 함수로부터 랜덤 값 R을 생성한다. 그리고 oFA와 GFA 사이의 공유 비밀키인 K_{oFA}로 R과 Id_{oFA}에 대한 MAC 값을 취해($K_{oFA\text{-}nFA}$ =<R,Id_{oFA}>K_{oFA}) oFA와 nFA간에 동적 공유 비밀키인 $K_{oFA\text{-}nFA}$를 생성한다.

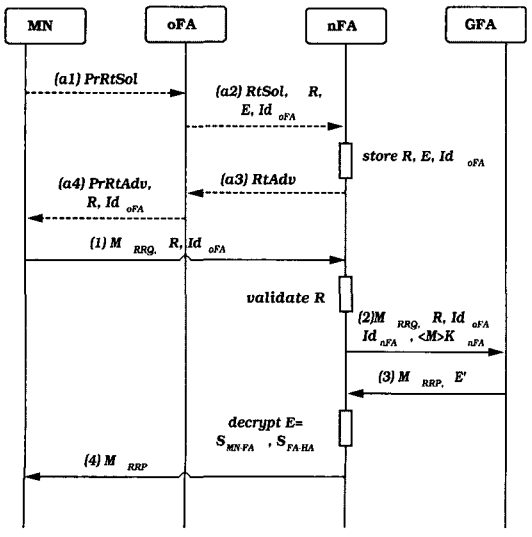

그림 4. 제안한 MI 핸드오프 오퍼레이션

oFA는 이 키를 이용하여 이전 Mobile IP 등록에서 할당 받은 세션 키인 $S_{MN\text{-}FA}$ 및 $S_{FA\text{-}HA}$를 암호화(E={$S_{MN\text{-}FA}$, $S_{FA\text{-}HA}$}$K_{oFA\text{-}nFA}$) 한다. 최종적으로 oFA는 이동 노드로부터 수신한 $RtSol$ 메시지에 랜덤 값 R, 자신의 ID인 Id_{oFA}, 그리고 암호화된 E를 포함시켜 nFA에게 $RtAdv$를 요청한다.

$RtSol$ 메시지를 수신한 nFA는 $RtAdv$ 메시지를 생성하고 이를 oFA에게 전송한다. oFA는 **Pr***RtAdv*를 메시지를 생성하고 R, Id_{oFA}, E를 포함시켜 MN에게 송신한다.

⊙ Mobile IP 등록 요청

(1) MN → nFA : M_{RRQ},R,Id_{oFA}

- nFA retrieves R,Id_{oFA} and validates R

M_{RRQ},R,Id_{oFA},Id_{nFA}

- nFA computes <M>K_{nFA} where M=

(2) nFA → GFA :

M_{RRQ},R,Id_{oFA},Id_{nFA},<M>K_{nFA}

- GFA authenticates nFA validating <M>K_{nFA}
- GFA computes $K_{oFA\text{-}nFA}$=<R,Id_{oFA}>K_{oFA}
- GFA computes

MN은 Mobile IP 등록 메시지를 생성한 후, 무선 인터페이스를 통해 수신한 에이전트 광고 메시지로부터 R 및 Id_{oFA}를 추출한 후, 등록 메시지내에 임베디드 시켜 nFA로 전송한다.

nFA는 이전에 저장한 R과 Id_{oFA}를 가져와서 R을 검증한다. 그리고 자신과 GFA 사이의 공유 비밀키인 K_{nFA}로 M(M_{RRQ},R,Id_{oFA},Id_{nFA})에 대한 MAC 값을 취한다. nFA는 M_{RRQ},R,Id_{oFA}에다 계산된 MAC 값을 포함시켜 GFA로 전송한다.

GFA는 HA역할을 수행하여 정상적인 Mobile IP 지역 등록을 수행한다. 그리고 K_{nFA}를 가지고 M에 대한 MAC 값을 취해(<M>K_{nFA}) nFA를 인증한다. 인증이 성공하면 K_{oFA}를 가지고 R과 Id_{oFA}에 대한 MAC을 취해($K_{oFA\text{-}nFA}$=<R,Id_{oFA}>K_{oFA}) oFA와 nFA간 동적 공유 비밀키인 $K_{oFA\text{-}nFA}$를 재생한다. 그리고 K_{nFA}로 $K_{oFA\text{-}nFA}$를 암호화하여(E'=K{$K_{oFA\text{-}nFA}$}K_{nFA})E'을 생성한다. 정상적인 Mobile IP 응답 메시지를 생성하고 E'을 포함시켜 nFA로 전송한다.

⊙ Mobile IP 등록 응답

(3) GFA → nFA : M_{RRP},E'

- nFA obtains $K_{oFA\text{-}nFA}$ by decrypting E' under the key K_{nFA}
- nFA retrieves E and decrypts it under the key $K_{oFA\text{-}nFA}$

(4) nFA → MN : M_{RRP}

GFA로부터 Mobile IP 등록 응답 메시지를 수신한 nFA는 등록 응답 처리를 수행한 후, K_{nFA}로 E'을 복호화하여 $K_{oFA\text{-}nFA}$를 추출한다. 그리고 저장되어 있는 E를 가져온 후, $K_{oFA\text{-}nFA}$로 복호화하여 이전 Mobile IP 등록에서 할당 받은 세션 키인 $S_{MN\text{-}FA}$ 및 $S_{FA\text{-}HA}$를 획득한다. 최종적으로 얻어진 이 세션 키들은 핸드오프 이후, 트래픽이 송수신될 때 암복호화 키로 사용된다. nFA는 Mobile IP 등록 응답 메시지를 MN에게 송신하면 절차가 완료된다.

Ⅳ. 세션 가로채기 공격 분석

이 장에서는 제안한 기법이 세션 가로채기 공격에 대해 안전한지를 몇가지 시나리오를 통해 분석해 보았다.

⊙ 공격자가 그림 3의 NI 핸드오프 절차 중 1번 메시지 또는 그림 4의 MI 핸드오프 절차 중 (a1) 메시지를 가로챘다고 가정하자. 공격자는 암호화된 메시지 E를 알 수 있다. 그러나 공유 키 $K_{oFA\text{-}nFA}$가 없으므로 E를 복호화 할 수 없다. 또한, 공격자가 R과 Id_{oFA}를 안다고 하더라도 K_{oFA}를 알 수 없으므로, 공유 키 $K_{oFA\text{-}nFA}$를 추출할 수 없다.

⊙ 공격자가 그림 3의 NI 핸드오프 절차와 그림 4의 MI 핸드오프 절차 중 3번 메시지를 가로챘다고 가정하자. 이 경우에는 K_{nFA}를 알 수 없기 때문에 E'으로부터 공유 키 $K_{oFA\text{-}nFA}$를 추출할 수 없다.

⊙ 공격자가 이전에 성공적인 Mobile IP 등록 절차로부터 그림 3의 NI 핸드오프 절차에 있는 2번으로부터 유효한 메시지 $M_{RRQ}, R, Id_{nFA}, Id_{nFA}, <M>K_{nFA}$를 가로챈 후, nFA로 가장해서 동작(impersonate)한다고 가정하자. 공격자는 RtAdv 메시지를 광고한다. 이를 수신한 oFA는 랜덤 값을 생성하고 $K_{oFA\text{-}nFA}=<R, Id_{oFA}>K_{oFA}$를 계산한다. 공격자는 유효한 메시지를 사용하여 2번 메시지를 재생하여 공격한다(replay attack). 이 때 GFA가 nFA로서의 공격자를 인증하고, GFA는 이전 동적 세션 키 $K'_{oFA\text{-}nFA}=<R', Id_{oFA}>K_{oFA}$를 계산한다. 그렇다 할지라도 공격자는 E'을 복호화하지 못하기 때문 세션 키들을 추출해 낼 수 없다.

이와 같이 방법으로 제안된 기법은 세션의 기밀성과 무결성을 제공하며, 로컬에서 LLH를 안전하게 수행한다. 이 기법을 위해 별도로 oFA와 nFA가 세션키의 암호화 및 복호화를 수행해야 하기 때문에 추가적인 오퍼레이션이 필요하다. 그러나 제안된 방법은 공개키 암호화 오퍼레이션들에 비해서 지연과 계산 비용이 훨씬 적다.

Ⅴ. 실험적인 성능 비교

이 장에서는 공개키 기반의 오퍼레이션 소요 시간과 제안한 기법의 오퍼레이션의 소요 시간을 비교하기 위하여 두개의 실험 시스템을 구현하고 상대적인 성능을 비교하였다.

구현 환경으로서 홈 망과 방문 망은 각기 다른 인접 서브넷으로 구분하였다. 홈 망의 HA 및 AAAH 그리고 방문 망의 MN, nFA, oFA, AAAF는 모두 별도의 리눅스 기반 XENON P-III 플랫폼과 RedHat 6.2인 리눅스 운영체계를 사용하였다. 그리고 실험 시스템에 각 노드에서 필요한 Mobile IP

표 1. 구현한 암호 라이브러리 및 알고리즘

알고리즘	용 도
SHA-1	MN-HA key, MN-AAAH key hashing
RSA	CMS 보안 응용에서 Key encryption, Asymmetric key transport
SHA-1, RSA	CMS 보안 응용에서 Signature/ Verification
id-alg-CMS 3DESwra	CMS 보안 응용에서 Symmetric Key Encryption

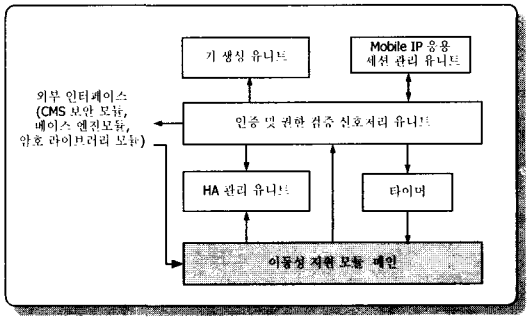

그림 5. Mobile IP 보안 응용 모듈의 구현 예

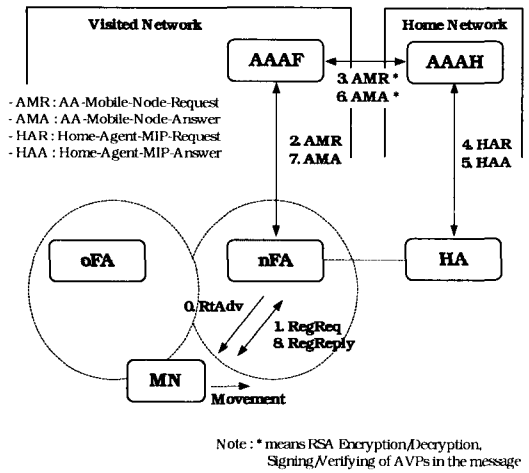

그림 6. 시나리오 1: 공개키 기반의 핸드오프 절차

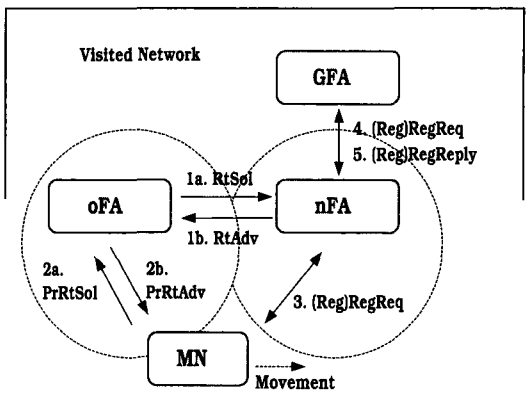

그림 7. 시나리오 2: 제안한 핸드오프 절차

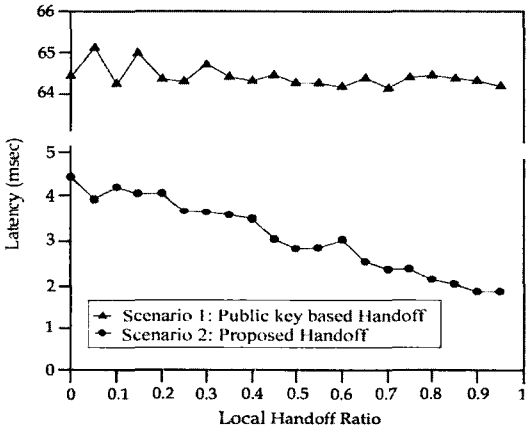

그림 8. 공개키 기반 핸드오프와 제안한 핸드오프의 성능 비교

기능[1,2]들과 Diameter 기반 AAA 기능들을 구현하였다. 공개키 방식은 IETF에서 정의한 기법[7]을 구현하여 적용하였다. 구현한 시스템은 아래의 알고리즘을 사용하였다.

구현한 Mobile IP 보안 응용 모듈의 소프트웨어 구조를 예로 보였다. 권한 검증 타이머, 세션 타이머, HA 및 홈 주소 할당 여부, 방문 망에서의 HA 할당 여부, CMS 보안 기능 지원 여부 등을 설정하고 관리할 수 있는 제어 화면이다.

그림 6은 시나리오 1로서 기존 공개키 기반의 핸드오프 절차 및 실험 시스템 구성을 보였다. 이 시스템에는 Diameter 기본 프로토콜,[5] Diameter Mobile IP 보안 응용,[6] 그리고 공개키 방식의 노드간 인증을 위한 CMS(Cryptographic Message Syntax) 보안 응용[7] 프로토콜을 구현하여 적용하였다. 이 시나리오에서는 매 Mobile IP 등록이 홈 망에 위치하는 HA와 AAAH를 통해서 수행되고 인증된다. 로컬 AAA 서버인 AAAF와 홈 AAA 서버인 AAAH 사이는 노드간 인증을 위해 공개키 기반의 CMS 기술이 적용된다. 즉, 이 사이에 송수신되는 메시지내 특정 AVP(Attribute-Value Pair)들은 RSA로 암호화.복호화 그리고 서명.검증절차를 거친다.

그림 7은 시나리오 2로서 제안한 핸드오프 절차 및 실험 시스템 구성을 보였다. 제안한 핸드오프는 그림 3과 그림 4에서 기술한 바와 같이 LLH에 직접 결합되어 동작한다. 이전의 홈 망을 통해 Mobile IP 등록이 성공적으로 수행된 후, 이 과정에서 획득한 세션 키는 oFA가 nFA로 안전하게 전달하여 재 사용된다. 즉, Mobile IP 등록은 홈 망의 HA나 AAAH와 인터렉션 없이 로컬에서 수행된다.

그림 8은 그림 6와 그림 7의 실험 시스템에서 시뮬레이션한 결과를 나타낸 것으로서, 각 시스템에서 측정한 핸드오프 소요 시간을 그래프로 나타내었다. 이 실험에서는 무선 구간으로 정의된 MN과 FA 사이는 Ethernet으로 연결하여 실험하였다. 그리고 방문 망과 홈 망이 인접한 서브넷에 위치하므로 전송 지연을 무시하였다. 또한, nFA와 GFA간 또한 인접하게 위치하므로 전송 지연을 무시하였다. 만약 전송 지연을 고려한다면, 방문 망과 홈 망의 거리가 멀어지면 이에 따른 전송지연이 길어지게 되어 시나리오 2의 Latency가 길어질 것이다.

로컬 핸드오프률(local handoff ratio)은 홈 등록과 로컬 등록의 비로써, 1에 가까울수록 로컬 등록이 많음을 의미한다. 실험 결과에 의하면 제안한

핸드오프 기법이 공개키 기반의 핸드오프 기법에 비해 소요 시간이 현격히 적음을 알 수 있다. 제안한 핸드오프 기법은 로컬 핸드오프률이 0.9일 때 약 2msec의 지연을 나타내고 있다. 이해 비해 공개키 기반의 암호화 기법에서는 64msec의 지연을 나타내고 있다.

시나리오 1인 경우, Latency는 Mobile IP 등록이 MN에서 nFA, AAAF, AAAH, HA까지 그리고 등록 응답이 MN까지 도달하는 RTT를 MN에서 측정한 값이다. 시나리오 2인 경우, Latency는 유사하게 Mobile IP 등록이 LLH의 절차에 따라 MN, nFA, oFA, GFA까지 그리고 이의 응답이 MN까지 도달하는 RTT를 MN에서 측정하였다. Latency는 10회 mean 값을 표시하였다.

Ⅳ. 결 론

본 논문에서는 Mobile IP와 AAA 인프라가 결합된 환경에서 LLH를 안전하고 빠르게 수행할 수 있는 안전한 세션 키 교환 기법을 제안하였다. 이 기법은 안전하고 빠른 LLH 핸드오프를 가능하게 하며, 세션 가로채기 공격을 막을 수 있도록 세션 키의 기밀성과 무결성을 제공한다. 또한, 기존 공개키 암호기반의 오퍼레이션에 소요되는 시간과 제안한 핸드오프 오퍼레이션에 소요되는 시간을 비교하기 위하여 실험 시스템을 구성하고 성능을 비교하였다. 실험 결과에 의하면 제안한 핸드오프의 소요 시간이 현격하게 적음을 알 수 있었다. 한편, LLH에서 세션 키를 적용하는 문제에 있어서 세션 키의 재사용 방법 이외에 LLH의 장점인 로컬 등록을 수용하여 빠른 핸드오프를 기하고, 안전성을 보장하는 다른 기법에 대한 연구가 필요하다.

참 고 문 헌

[1] Karim El Malki, Pat R. Calhoun, Tom Hiller, James Kempf, et al., "Low Latency Handoffs in Mobile IPv4," ⟨*draft-ietf-Mobileip-lowlatency-handoffs-v4-04.txt*⟩, July 2002.

[2] Charles E. Perkins, "IPv4 Mobility Support," *RFC2002*, October 1996.

[3] Charles E. Perkins, "IP Mobility Support for IPv4," *RFC3220*, January 2002.

[4] Eva Gustafsson, Annika Jonsson, Charles E. Perkins, "Mobile IPv4 Regional Registration," ⟨*draft-ietf-Mobileip-reg-tunnel-06.txt*⟩, March 2002.

[5] Pat R. Calhoun, "Diameter Base Protocol,"⟨*draft-ietf-aaa-diameter-17.txt*⟩, December 2002.

[6] Pat R. Calhoun, Tony Johansson, Charles E. Perkins, "Diameter Mobile IPv4 Application," ⟨*draft-ietf-aaa-diameter-mobileip-13.txt*⟩, October 2002.

[7] Pat R. Calhoun, Stephen Farrell, William Bulley, "Diameter CMS Security Application," ⟨*draft-ietf-aaa-diameter-cms-sec-04.txt*⟩, March 2002.

[8] S. Jacobs, "Mobile IP Public Key Based Authentication," ⟨*draft-jacobs-Mobileip-pki-auth-03.txt*⟩, July 2001.

[9] E. Gustafsson, et al., "Mobile IP Regional Tunnel Management," ⟨*draft-ietf-Mobileip-regtunnel-06.txt*⟩, March 2002.

[10] Sufatrio, Kwok Yan Lam, "Mobile IP Registration Protocol: A Security Attack and New Secure Minimal Public-Key Based Authentication, "*ISPAN'99*, pp. 364-369, June 1999.

〈著者紹介〉

김 현 곤 (Hyun Gon Kim) 정회원
1992년 금오공과대학교 전자공학과 학사
1994년 금오공과대학교 전자공학과 석사
2003년 충남대학교 전자공학과 박사
1994년~현재 한국전자통신연구원 정보보호연구본부 AAA정보보호연구팀장
〈관심분야〉: IP 기반의 이동통신 네트워크의 보안, 무선 분산 보안