

Low Latency Handoffs를 위한 안전한 세션 키 교환 기법 설계

Design of a Secure Session Key Exchange Method for Low Latency Handoffs

김 현 곤* 박 치 향**
Hyun-Gon Kim Chee-Hang Park

요 약

Mobile IP Low Latency 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 에이전트를 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 핸드오버를 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-authentication 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 third party. The proposed method allows the mobile node to perform Low Latency Handoffs with fast as well as secure operation

· · · Keyword : Low Latency Handoffs, Mobile IP

1. 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 에이전

* 정 회 원 : 한국전자통신연구원 선임연구원
hyungon@etri.re.kr(제 1저자)

** 정 회 원 : 한국전자통신연구원 책임연구원
chpark@etri.re.kr(공동저자)

트(GFA ; Gateway Foreign Agent)로부터 패킷을 수신하는 지역 등록(Regional Registration) 모델[4]에 둘 다 적용 가능하다. 전자에서는 방문 망과 MN의 홈 망간 거리가 길어질수록 등록을 위한 지연 시간이 커지나, 후자에서는 이를 개선하여 로컬 등록을 이름으로써 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, 최근에는 AAA 프로토콜로서 표준화되고 있는 Diameter[5-8]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(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 Spoofing하여 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 암호

호를 기반으로 세션 키의 기밀성을 제공하는 기법[9-10]이 제안되어 있으나, 공개키 암호 오퍼레이션에 의해 발생하는 긴 지연, 고비용, 인프라 구성의 어려움 때문에 현실적으로 적용이 쉽지 않다. 따라서 안전하고 가벼운 세션 키 교환 기법이 필요하다.

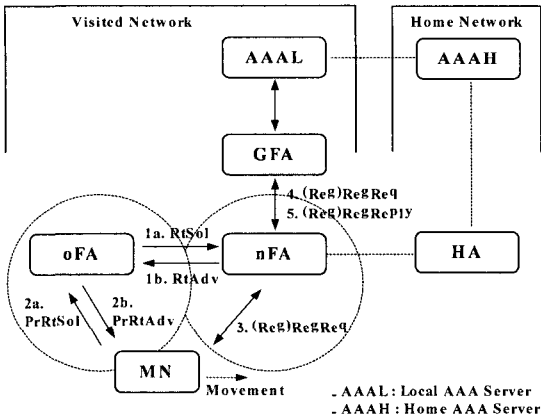
본 논문의 구성은 제 1장의 서론에 이어 2장에서는 관련연구로서 AAA 기반 LLH를 소개하고 제안된 세션 키 교환 기법을 조사했다. 3장에서는 먼저 키 교환 단계에서 세션 가로채기 공격의 가능성을 진단해본 후, 제안한 세션 키 교환 기법을 기술하였다. 4장에서는 제안한 기법이 세션 가로채기 공격에 안전함을 분석하였다. 5장에서는 시뮬레이션을 통해 기본 공개키 암호 오퍼레이션과 제안한 암호 오퍼레이션의 성능을 비교하였으며, 마지막으로 6장에서 결론을 맺는다.

2. 관련 연구

2.1 Low Latency Handoffs 소개

Mobile IP는 서로 다른 FA에 의해 서비스되는 서브넷간의 IP 계층 핸드오프 절차를 규정하고 있다. 그러나 어떤 경우 Mobile IP에서의 핸드오프 시에 발생하는 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 완료 가능하면 사전 등록 핸드오프 방법을



〈그림 1〉 AAA 기반 Low Latency Handoffs

사용하고, 그렇지 못한 경우는 사후 등록 핸드오프 기법을 사용한다.

본 논문에서는 사전 등록 핸드오프 기법만을 그 대상으로 한다. LLH는 방문 망내에서 로컬 등록을 수행하는 지역 등록[1]을 고려하고 있다. 그림 1에 AAA 기반 LLH의 절차를 개념적으로 나타내었다. MN이 Mobile IP 등록 요청을 하여 성공적으로 인증 및 권한 검증이 되면, AAAH(Home AAA server)는 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.

2.2 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[9]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[8]하고 있다. 이 기법에서는 MN이 관여되지 않으며, Mobile IP 엔티티들과 AAA 엔티티들간에 노드간 상호 인증을 위해 공개키 인증 기법을 적용한다. 참고문헌[14]에서 제안하고 있는 전자서명을 첨부한 공개키 인증 기법은 이동 노드에 전자서명을 함으로써 부인방지 서비스를 제공하고 최소로 공개키를 사용함으로써 효율성을 제공한다. 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.

3. 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 공개키 Jacobs[9]가 제안한 공개키를 기반으로 하여 기밀성을 제공하는 기법을 제안하였다. 그러나 이 기법의 단점은 모든 FA가 공개키 암호 오퍼레이션을 수행함으로써 인해 지연이 크고 공유키 방식에 비해 높은 비용으로 인해 현실적인 솔루션이 되지 못하고 있다. 따라서 안전하고 가벼운 오퍼레이션이 가능한 새로운 세션 키 교환 기법이 제안되어야 한다.

3.2 제안한 세션 키 교환 기법

제안한 기법은 지역 등록을 적용하며, 이를 위해

서 이전에 할당된 세션 키를 재사용 한다. 그리고 공개키 오퍼레이션 대신에 신뢰할 수 있는 제 3자를 두어 키를 공유하는 프로토콜을 적용한다. 이 기법에서는 GFA가 FA들간에 신뢰할 만한 제 3자 역할을 수행한다. 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.

- ◎ $S_{MN-FA}, S_{FA-HA}, S_{MN-HA}$: MN과 FA간, FA와 HA간, 그리고 MN과 HA간 Mobile IP 공유 세션 키
- ◎ $K_{oFA-nFA}$: 임시로 계산되고 저장되지 않는 oFA와 nFA간 동적 세션 키
- ◎ $\langle M \rangle K$: 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-FA}, S_{FA-HA} 를 재 사용한다. 이 세션 키들을 암호화하고 복호화하기 위해서 oFA와 nFA사이에 short-lived 비밀 키인 $K_{oFA-nFA}$ 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 2에 제안한 NI 핸드오프의 흐름 및 오퍼레이션을 보였으며, 다음과 같이 동작한다.

- ◎ Proxy Router Advertisement 준비
 - oFA는 랜덤값 R 을 선택
 - oFA는 $K_{oFA-nFA} = \langle R, Id_{oFA} \rangle K_{oFA}$ 를 계산
 - oFA는 $E = \{S_{MN-FA}, S_{FA-HA}\} K_{oFA-nFA}$ 를 계산

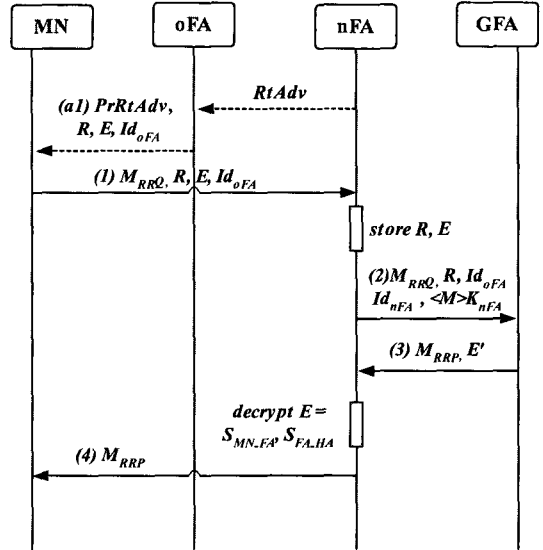
- ◎ Proxy Router Advertisement(PrRtAdv)
 - (a1) oFA → MN : Pr RtAdv, R, E, Id_{oFA}

- ◎ Mobile IP Registration Request/Reply
 - (1) MN → nFA : M_{RRQ}, R, E, Id_{oFA}
 - nFA는 R 과 E 를 저장
 - nFA는 $\langle M \rangle K_{nFA}$ 를 계산, 여기서 $M = M_{RRQ}, R, Id_{oFA}, Id_{nFA}$

- (2) nFA → GFA :
 - $M_{RRQ}, R, Id_{oFA}, Id_{nFA}, \langle M \rangle K_{nFA}$
 - GFA는 $\langle M \rangle K_{nFA}$ 를 검증하여 nFA를 인증
 - GFA는 $K_{oFA-nFA} = \langle R, Id_{oFA} \rangle K_{oFA}$ 를 계산
 - GFA는 $E' = \{K_{oFA-nFA}\} K_{nFA}$ 를 계산

- (3) GFA → nFA : M_{RRP}, E'
 - nFA는 E' 을 복호화하여 $K_{oFA-nFA}$ 을 추출
 - nFA는 저장되어 있는 E 를 가져온 후, 키 $K_{oFA-nFA}$ 로 복호화하여 세션 키 S_{MN-FA}, S_{FA-HA} 를 획득 함

- (4) nFA → MN : M_{RRP}



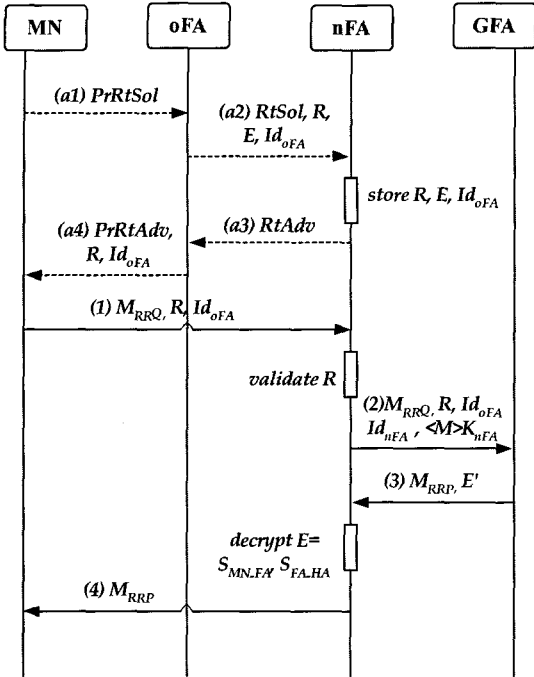
〈그림 2〉 제안한 NI 핸드오프 오퍼레이션

3.2.2 Mobile-Initiated(MI) Handoff

MI 핸드 오프에서 MN은 프락시 라우터 요청(PrRtSol ; Proxy Router Solicitation)을 oFA에게 요구한다. 그림 3에 제안한 MI 핸드오프의 흐름 및 오퍼레이션을 보였으며, 다음과 같이 동작한다.

- ◎ PrRtAdv/Proxy Router Solicitation(PrRtSol)
 - (a1) MN → oFA : Pr RtSol
 - oFA는 랜덤값 R 을 선택
 - oFA는 $K_{oFA-nFA} = \langle R, Id_{oFA} \rangle K_{oFA}$ 를 계산
 - oFA는 $E = \{S_{MN-FA}, S_{FA-HA}\} K_{oFA-nFA}$ 를 계산
 - (a2) oFA → nFA : RtSol, R, E, Id_{oFA}
 - nFA는 R, E, Id_{oFA} 를 저장
 - (a3) nFA → oFA : RtAdv
 - (a4) oFA → MN : Pr RtAdv, R, Id_{oFA}

- ◎ Mobile IP Registration Request/Reply
 - (1) MN → nFA : M_{RRQ}, R, Id_{oFA}
 - nFA는 저장된 R, Id_{oFA} 를 가져오고, R 을 검증



(그림 3) 제안한 MI 핸드오프 오퍼레이션

- nFA는 $\langle M \rangle K_{nFA}$ 를 계산, 여기서 $M = M_{RRQ}, R, Id_{oFA}, Id_{nFA}$

(2) nFA→GFA :

$M_{RRQ}, R, Id_{oFA}, Id_{nFA}, \langle M \rangle K_{nFA}$

- GFA는 $\langle M \rangle K_{nFA}$ 를 검증하여 nFA를 인증

- GFA는 $K_{oFA-nFA} = \langle R, Id_{oFA} \rangle K_{oFA}$ 를 계산

- GFA는 $E' = \{ K_{oFA-nFA} \} K_{nFA}$ 를 계산

(3) GFA→nFA : M_{RRP}, E'

- nFA는 E' 을 복호화하여 $K_{oFA-nFA}$ 을 추출

- nFA는 저장된 E 를 가져온 후, 키 $K_{oFA-nFA}$ 로 복호화하여 세션 키 S_{MN-FA}, S_{FA-HA} 를 획득함

(4) nFA→MN : M_{RRP}

4. 세션 가로채기 공격 분석

이 장에서는 제안한 기법이 세션 가로채기 공격에

대해 안전한지를 몇가지 시나리오를 통해 분석해 보았다.

⊙ 공격자가 그림 2의 NI 핸드오프 절차 중 1번 메시지 또는 그림 3의 MI 핸드오프 절차 중 (a1) 메시지를 가로챘다고 가정하자. 공격자는 암호화된 메시지 E 를 알 수 있다. 그러나 공유 키 $K_{oFA-nFA}$ 가 없으므로 E 를 복호화할 수 없다. 또한, 공격자가 R 과 Id_{oFA} 를 안다고 하더라도 K_{oFA} 를 알 수 없으므로, 공유 키 $K_{oFA-nFA}$ 를 추출할 수 없다.

⊙ 공격자가 그림 2의 NI 핸드오프 절차와 그림 3의 MI 핸드오프 절차 중 3번 메시지를 가로챘다고 가정하자. 이 경우에는 K_{nFA} 를 알 수 없기 때문에 E' 으로부터 공유 키 $K_{oFA-nFA}$ 를 추출할 수 없다.

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

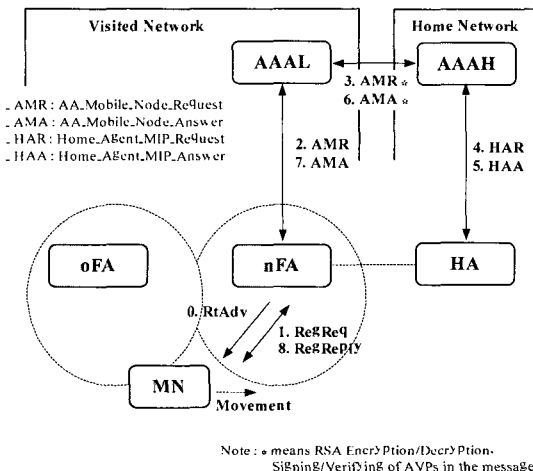
이와 같이 방법으로 제안된 기법은 세션의 기밀성과 무결성을 제공하며, 로컬에서 LLH를 안전하게 수행한다. 이 기법을 위해 별도로 oFA와 nFA가 세션키

의 암호화.복호화를 수행해야 하기 때문에 추가적인
오퍼레이션이 필요하다. 그러나 제안된 방법은 공개
키 암호화 오퍼레이션들에 비해서 지연과 계산 비용
이 훨씬 적다.

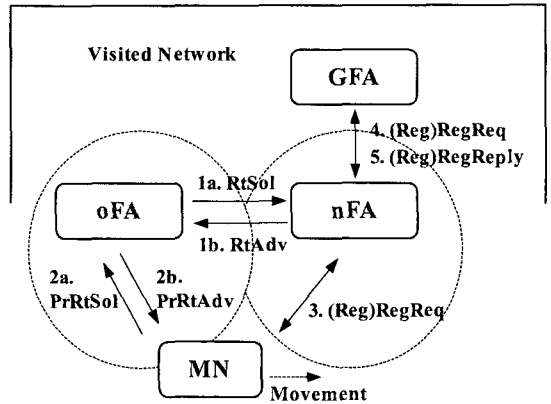
5. 실험적인 성능 비교

이 장에서는 공개키 기반의 오퍼레이션 소요 시간
과 제안한 기법의 오퍼레이션의 소요 시간을 비교하
기 위하여 두개의 실험 시스템을 구현하고 상대적인
성능을 비교하였다. 구현 환경으로서, 각 노드는 별
도의 플랫폼으로 구성하였으며, 리눅스 기반
XENON P-III 시스템과 RedHat 6.2인 리눅스 운영체
제를 사용하였다. 그리고 실험 시스템에 각 노드에서
필요한 Mobile IP 기능[1,2]들과 Diameter 기반 AAA
기능들을 구현하였다.

그림 4는 시나리오 1로서, 공개키 기반의 핸드오
프 절차 및 실험 시스템 구성을 보였다. 이 시스템에
는 Diameter 기본 프로토콜[5], Diameter Mobile IP 보
안 응용[7], 그리고 공개키 방식의 노드간 인증을 위
한 CMS(Cryptographic Message Syntax) 보안 응용[8]
프로토콜을 구현하여 적용하였다. 이 시나리오에서
는 매 Mobile IP 등록이 홈 망에 위치하는 HA와
AAAH를 통해서 수행되고 인증된다. 로컬 AAA 서



〈그림 4〉 시나리오 1 ; 공개키 기반의 핸드오프

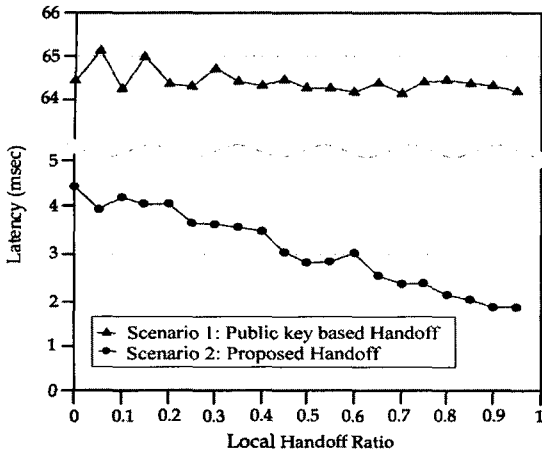


〈그림 5〉 시나리오 2 ; 제안한 핸드오프 절차

버인 AAAL(Local AAA Server)과 홈 AAA 서버인
AAAH 사이는 노드간 인증을 위해 공개키 기반의
CMS 기술이 적용된다. 즉, 이 사이에 송수신되는 메
시지내 특정AVP(Attribute-Value Pair)들은 RSA로 압
축.복호화 그리고 서명.검증절차를 거친다. 이 실
험에서는 방문 망과 홈 망 사이의 propagation 지연은
무시하였다.

그림 5에 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 사용
된다. 즉, Mobile IP 등록은 홈 망의 HA나 AAAH와
인터랙션없이 로컬에서 수행된다.

그림 6은 그림 4와 그림 5의 실험 시스템에서 시뮬
레이션한 결과를 나타낸 것으로서, 각 시스템에서 측
정한 핸드오프 소요 시간을 그래프로 나타내었다. 로
컬 핸드오프율(local handoff ratio)은 홈 등록과 로컬
등록의 비로써, 1 에 가까울수록 로컬 등록이 많음을
의미한다. 실험 결과에 의하면 제안한 핸드오프 기법
이 공개키 기반의 핸드오프 기법에 비해 소요 시간이
현저히 적음을 알 수 있다. 제안한 핸드오프 기법은
로컬 핸드오프율이 0.5일 때 약 3msec의 지연을 나타
내고 있다. 이해 비해 공개키 기반의 암호화 기법에
서는 64msec의 지연을 나타내고 있다.



〈그림 6〉 공개키 기반 핸드오프와 제안한 핸드오프의 성능 비교

결과를 고찰해보면 2.2절에 언급한 Sufatrio, K. Lam의 최소 공개키 인증 기법은 IETF에서 제안한 공개키 인증기법에 비해서 57%의 지연이 축소되고, 전자서명을 첨부한 공개키 인증 기법은 40%의 지연이 축소된다[14]. 그림 6의 참조하여 예로 들면, IETF의 공개키 인증기법이 64msec가 소요된다면, 최소 공개키 인증 기법은 27.52msec 그리고 전자서명을 첨부한 공개키 인증은 38.4msec의 지연을 보일 것이다. 제안한 기법은 이에 비해 대략 3msec로써 참고 문헌 [14]의 비밀키 인증 소요시간과 거의 동일함을 알 수 있었다.

6. 결론

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 적

음을 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.

참고 문헌

- [1] Karim El Malki, Pat R. Calhoun, Tom Hiller, James Kempf, et al., "Low Latency Handoffs in Mobile IPv4", <draft-ietf-Mobileip-lowlatency-handoffs-v4-05.txt>, June, 2003.
- [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-08.txt>, November, 2003.
- [5] Pat R. Calhoun, J. Loughnery, G. Zone, "Diameter Base Protocol", RFC3588, September, 2002.
- [6] B. Aboba, J. Wood, "Authentication, Authorization and Accounting(AAA) Transport Profile", RFC339, June, 2003.
- [7] Pat R. Calhoun, Tony Johansson, Charles E. Perkins, "Diameter Mobile IPv4 Application", <draft-ietf-aaa-diameter-mobileip-15.txt>, November, 2003.
- [8] Pat R. Calhoun, Stephen Farrell, William Bulley, "Diameter CMS Security Application", <draft-ietf-aaa-diameter-cms-sec-04.tx>, March, 2002.
- [9] S. Jacobs, "Mobile IP Public Key Based Authentication", <draft-jacobs-Mobileip-pki-auth-03.txt>, July, 2001.
- [10] Sufatrio, Kwok Yan Lam, "Mobile IP Registration Protocol : A Security Attack and New Secure Minimal Public-Key Based Authentication",

- ISPAN'99, June, 1999.
- [11] Hui Jong Yu, Mal-hee Kim, Hyun Gon Kim, "Efficient Implementation of Diameter CMS Security Application in Mobile IP", CIC2003, pp.535-pp.541, October 2003.
- [12] DooHo Choi, et. al., "Mobile IP Authentication based on One Way Function", CIC2003, pp.395-pp.399, October 2003.
- [13] 박상준, 홍춘선, 이대영, "Mobile-IP 등록 프로토콜에서 공개키를 이용한 인증 방안", 한국통신학회 논문지, 제27권, pp.211-pp.219, 2002년 3월
- [14] 정선이, 채기준, 장중수, 손승원, " Mobile-IP 망에서의 효율적인 인증 방안", 한국정보과학회 논문지 제28권 제3호, pp.321-pp.335, 2001년 9월

● 저자 소개 ●



김 현 곤

1992년 금오공과대학교 전자공학과 졸업(공학사)
1994년 금오공과대학교 대학원 전자공학과 졸업(공학석사)
2003년 충남대학교 대학원 전자공학과 졸업(공학박사)
1994 ~ 현재 : 한국전자통신연구원 정보보호연구본부 AAA정보보호연구팀장
관심분야 : IP 기반의 이동통신 정보보호, 무선인터넷 정보보호
E-mail : hyungon@etri.re.kr



박 치 항

1974년 서울대학교 응용물리학과 졸업(이학사)
1980년 한국과학원 전자계산학과(이학석사)
1987년 파리 6대학 전자계산학과(공학박사)
1974년~1978년 한국과학기술연구소(KIST) 연구원
1978년~현재 : 한국전자통신연구원 책임연구원
관심분야 : 멀티미디어, 분산시스템, 네트워크 정보보호
E-mail : chpark@etri.re.kr