Low Latency Handoffs를 위한 세션 키 교환

김현곤*, 최두호, 손승원

한국전자통신연구원, 정보보호연구본부

Session Key Exchange for Low Latency Handoffs

HyunGon Kim*, DoHoo Choi, SungWon Sohn

ETRI, Information Security Research Division

요 약

Mobile IP Low Latency Handoffs[1]는 Mobile IP 등록 요청 절차를 처리하는데 있어서 단말의 지연 때문에 생기는 블록킹 시간을 최소화 시켜 실시간 서비스를 가능하게 해 준다. 그러나 인증, 권한 검증, 과금을 지원하는 AAA 기반의 Mobile IP 망에서는 매 지역 등록이 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 서버가 관여되지 않고, 이전에 할당된 세션 키를 재사용하여 Low Latency Handoffs를 수행하는 기법을 제안한다. 이 기법에서는 이전 방문 에이전트와 새로운 방문 에이전트간 세션 키를 교환하는 단계에서 발생하는 보안 취약성을 해결할 수가 있으며 홈 망까지 트랜잭션이 필요 없고, 세션 키의 기밀성이 제공되므로 이동 노드가 빠르고 안전하게 핸드오프를 수행할 수 있다.

I. 서론

Mobile IP[2][3]는 핸드오프 시, 지연에 민감하고 실시간 서비스에서 지연이나 패킷 손실을 유발할 수 있다. 이러한 지연을 줄이기 위해 Low Latency Handoffs[1](LLH)가 제안되었으며, 현재 IETF에서 표준화가 진행 중이다. 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) 모델에 둘 다 적용 가능하다. 전자의 모델에서는 방문 망과 MN의 홈 망간 거리가 멀면 등록을 위한 신호 지연이 발생할 수 있다. 그러나 후자의 모델에서는 로컬에서 등록이 이루어지므로 이러한 신호 지연을 줄일 수 있다.

한편, AAA (Authentication, Authorization, and Accounting) 기술은 다양한 유무선 서비스에 대한 인증, 권한 검증, 과금 기능을 수행한다. Mobile IP 서비스에 대해서는 MN의 인증, 권한 검증, 과금, 노드간 인증 등의 기능을 수행하며 특히, 최근에 표준화되고 있는 AAA 프로토콜인 Diameter[5]는 Mobile IP 프로토콜과 밀접하게 결합되어 있다.

본 논문에서는 표준에서 고려되지 않은 LLH에 AAA를 적용하는 시나리오를 다룬다. 지역 등록 모델에서 AAA 인프라를 적용한다면, 새로운 세션 키 생성을 위해 홈 망까지 MN 재인증 절차, 세션 키 재 분배 절차가 요구되며, 이를 위해 방문 망에서 홈 망까지의 트랜잭션이 발생되기 때문에 지역 등록의 장점을 살릴 수가 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 채널상에서 전달되기 때문에 공격자가 Mobile IP 등록 메시지를 spoofing하여 사용자 정보를 획득할 수 있다. 이러한 종류의 세션 가로채기(session stealing) 공격을 막기 위해서는 세션 키의 기밀성(confidentiality)이 보장되어야 한다. 유사한 목적으로 공개키 암호를 기반으로 세

션 키의 기밀성을 제공하는 기법이 제안되어 있으나, 공개키 암호 오퍼레이션에서 발생하는 긴지연, 비용, 인프라 구성의 어려움 때문에 현실적으로 적용이 쉽지않다. 이를 위해 본 논문에서는 안전하고 가벼운 세션 키 교환 방법을 제안한다.

II. Low Latency Handoffs 소개

Mobile IPv4는 서로 다른 FA에 의해 서비스되는 서브넷간의 IP 계층 핸드오프 절차를 규정하고 있다. 그러나 어떤 경우 Mobile IPv4에서의 핸드오프 시에 발생되는 지연이 지연에 민감하거나 또는 실시간성을 요하는 서비스에서 요구하는 조건을 만족시키지 못할 경우가 있다. 이러한 지연을 줄이기 위해 제안된 것이 LLH 기법이다. 아래 그림 1에 LLH가 외부에 AAA 인프라를 가질 경우, 네트워크 토폴로지를 나타내었다.

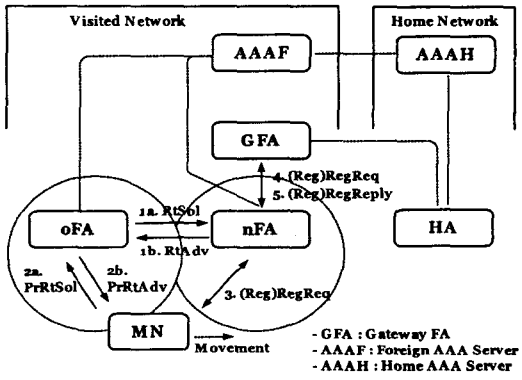

그림 1: LLH with AAA network topology

본 논문에서는 사전 등록 핸드오프 기법만을 그 대상으로 한다. LLH는 방문 망내에서 로컬 등록을 수행하는 지역 등록을 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 세션키들(mobile-foreign, foreign-home, and mobile-home session key)을 생성하고 분배한다. 이후, 핸드오프가 발생하면 로컬에서 지역 등록이 수행된다.

III. 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 키교환 기법을 제안한다

1. 세션 가로채기 공격

세션 키의 lifetime은 잦은 키 분배로 인한 지연을 줄이기 위해 충분히 크게 설정되도록 권장하고 있다. 한때, AAAH에 의해 세션 키가 분배되면oFA는 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 Jocobs가 제안한 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.

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 제3자를 두어 키를 공유하는 프로토콜을 적용한다. 이 기법에서는GFA가 FA들간에 신뢰할 만한 제3자 역할을 수행한다. GFA와 FA 사이에 보안 연관(security association)이 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
- $<M>K$: 키 K에의한 메시지 M의 MAC
- $\{M\}K$: 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(NI) Handoff에 적용하였다.

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 키 교환의 흐름 및 오퍼레이션을 보였으며, 다음과 같이 동작한다.

- Proxy Router Advertisement 준비
  + oFA는 랜덤값 R을 선택
  + oFA는 $K_{oFA-nFA} =< R, Id_{oFA} > K_{oFA}$
  + oFA는 $E = \{S_{MN-FA}, S_{FA-HA}\}K_{oFA-nFA}$
- 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 R과 E를 저장
  + nFA는 $<M>K_{nFA}$를 계산,
    여기서 $M = M_{RRQ}, R, Id_{oFA}, Id_{nFA}$

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

  + GFA는 $<M>K_{nFA}$를 검증하여 nFA를 인증
  + GFA는 $K_{oFA-nFA} =< R, Id_{oFA} > K_{oFA}$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 E를 가져온 후, 키 $K_{oFA-nFA}$로 복호화, S_{MN-FA}, S_{FA-HA} 획득

(4) nFA->MN : M_{RRP}

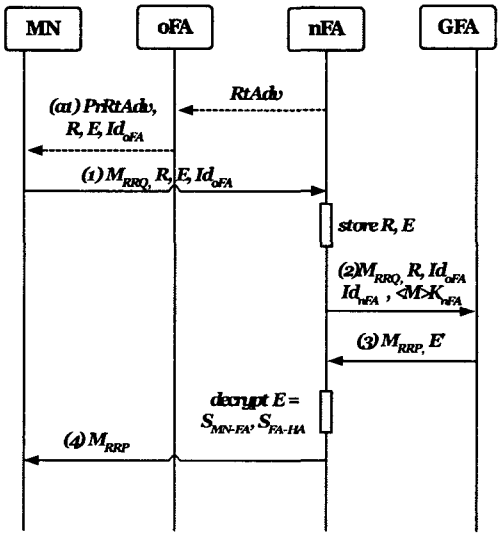

그림 2.: 제안한 세션 키 교환

IV. 세션 가로채기 공격에 대한 분석

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

- 공격자가 그림 2의 NI 핸드오프 절차 중 1번 메시지를 가로챘다고 가정하자. 공격자는 암호화된 메시지 E를 알 수 있다. 그러나 공유 키 $K_{oFA-nFA}$가 없으므로 E를 복호화 할 수 없다. 또한, 공격자가 R과 Id_{oFA}를 안다고 하더라도 K_{oFA}를 알 수 없으므로, 공유 키 $K_{oFA-nFA}$를 추출할 수 없다.
- 공격자가 그림 2의 NI 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 $M_{RRQ}, R, Id_{oFA}, Id_{nFA}, < M > K_{nFA}$ 를 가로챈 후, nFA로 가장해서 동작(impersonate)한다고 가정하자. 공격자는 RtAdv 메시지를 광고한다. 이를 수신한 oFA는 랜덤 값을 생성하고 $K_{oFA-nFA} = < R, Id_{oFA} > K_{oFA}$ 를 계산한다. 공격자는 유효한 메시지를 사용하여 2번 메시지를 재생하여 공격한다(replay attack). 이 때 GFA가 nFA로서의 공격자를 인증하고, GFA는 이전 동적 세션 키 $K'_{oFA-nFA} =< R', Id_{oFA} > K_{oFA}$ 를 계산한다. 그렇다 할지라도 공격자는 E'을 복호화하지 못하기 때문에서 세션 키들을 추출해 낼 수 없다.

이와 같이 제안한 기법은 세션의 기밀성을 제공하며, 로컬에서 LLH를 안전하게 수행한다. 이 기법을 위해서 oFA와 nFA가 세션키의 암복호화를 수행해야 하기 때문에 추가적인 오퍼레이션이 필요하다. 그러나 제안된 방법은 공개키 암호화 오퍼레이션에 비해 지연과 비용이 훨씬 적다.

V. 실험적인 성능 비교

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

구현 환경으로써, 각 노드는 별도의 플랫폼으로 구성하였으며, 리눅스 기반 XENON P-III 시스템과RedHat 6.2인 LINUX 운영체계를 사용하였다. 실험에서 비교 대상으로서, 하나는 공개키 기반핸드오프 절차를 따르고 다른 하나는 제안한 핸드오프 절차를 따른다. 공개키 기반 핸드오프에서는 매 Mobile IP 등록이 홈 망에 위치하는 HA와 AAAH를 통해서 수행되고 인증된다. 로컬 AAA 서버인 AAAF(Foreign AAA Server)과 홈 AAA 서버인 AAAH 사이는 노드간 인증을 위해 공개키 기반의 CMS(Cryptographic Message Syntax) 기술이 적용된다. 즉, 이 사이에 송수신되는 메시지내 특정AVP(Attribute-Value Pair)들은 RSA로 암호화.복호화 그리고 서명.검증절차를 거친다.

그림 3의 실험결과에서는 실험시스템에서 측정한 핸드오프 소요 시간이다. 로컬 핸드오프률(Local Handoff Ratio)은 홈 등록과 로컬 등록의 비로써, 1 에 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 0.9일때 약 2msec의 지연을 나타내고 있다. 공개키 기반의 암호화 기법에서는 64msec의 지연을 나타내고 있다.

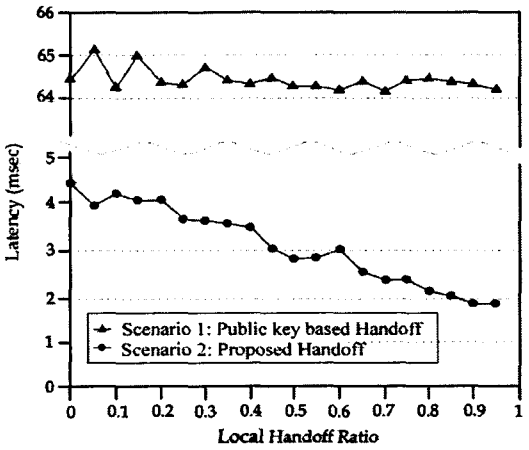

그림 3: 공개키 기반과 제안한 핸드오프 성능

VI. 결 론

본 논문에서는 Mobile IPv4와 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 막을수 있도록 세션 키의 기밀성을 제공한다. 실험 결과에 의하면 제안한 핸드오프의 소요 시간이 현격하게 적게 나옴을 알 수 있었다.

참고문헌

[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 Reg. Reg", <draft-ietf-Mobileip-reg-tunnel-06.txt>, March, 2002.