논문 2010-47TC-2-13

MIH 기반의 이기종 네트워크 환경에서 대리 서명을 이용한 인증 연동 프로토콜

(Authentication Interworking Protocol based on Media Independent Handover in Heterogeneous Networks)

노 효 선*, 정 수 환**

(Hyosun Roh and Souhwan Jung)

요 약

본 논문은 IEEE 802.21 WG에서 표준화 진행 중인 MIH (Media Independent Handover) 기반의 이질적인 네트워크 환경에서 RSA 기반의 서명 방식을 적용한 인증 연동 프로토콜을 제안한다. 본 논문에서 제안하는 인증 연동 프로토콜은 이동 단말이 핸드오버 할 경우 발생하는 핸드오버 지연 시간과 보안 기술 적용에 따른 메시지 오버헤드 등을 줄이기 위해 기존 MIH 프레임에 새로운 AIP TLV (Authentication Interworking Protocol TLV)를 정의하였고, MIHIS (MIH Information Server)가 인증 서버를 대신하여 이동 단말에게 서명을 제공할 수 있도록 RSA 기반의 대리 서명 방식을 적용하였다. 제안하는 인증 연동 프로토콜은 이동 단말이 핸드오버 할 경우 사전에 MIH 메시지를 이용하여 이동 단말을 인증 할 수 있는 서명을 전달하게 함으로서 사전 인증을 수행할 수 있도록 하였다. 또한 보안이 적용되지 않은 MIH 프로토콜과의 핸드오버 지연 시간 비교를 통해 인증 연동 프로토콜의 성능을 분석하였다.

Abstract

This paper proposed an authentication interworking protocol (AIP) based on IEEE 802.21 MIH in the heterogeneous networks. The proposed AIP using the RSA signature reduces handover delay time and communication message overhead when the mobile node moves between the heterogeneous networks. It defines new AIP TLV in MIH frame format and uses the MIH Information Server (MIHIS) for proxy signature issue instead of the authentication server for the heterogeneous networks. For low handover delay, the proposed AIP performs pre-authentication processes with MIH protocol before layer 2 handover. Also, this paper analyzed the performance of the handover and compared with the non-secure MIH protocol.

Keywords: MIH, 대리서명, RSA 서명, 사전 인증, 인증 연동

I. 서 론

최근 유무선 통신은 눈부시게 발전하고 있으며, 사용자들의 단말 또한 점차 여러 종류의 접속 기술을 통해 다양한 유무선 네트워크에 접속할 수 있게 되었다. 또한 이러한 통신 기술의 발전은 사용자들에게 보다 다양하고 수준 높은 네트워크 서비스를 제공할 수 있게 되었으며, 이로 인해 새로운 네트워크 요구사항들이 생겨나게 되었다. 최근 사용자 단말은 다중 무선 네트워크 인터페이스가 적용되어 이기종 무선 네트워크를 통해 다양한 네트워크 서비스를 이용할 수 있게 되었으며, 이기종 망을 자유롭게 핸드오버 하면서 필요한 서비스를 제공받을 수 있게 되었다. 그로 인해 이와 같은 네트워크 환경을 자유롭게 핸드오버 하는 사용자에게 끊김

* 정회원, ** 평생회원-교신저자,
숭실대학교 정보통신전자공학부
(School of electronic Engineering,
Soongsil University)
※ 본 연구는 지식경제부 및 정보통신연구진흥원의 IT산업원천기술개발사업의 일환으로 수행하였음. [2008-F015-02, 서비스 가용성을 위한 이동성 관리 기술 연구]
접수일자: 2009년9월6일, 수정완료일: 2010년2월17일

없는 네트워크 서비스를 제공하기 위한 핸드오버 기술이 요구되었다. 이러한 요구사항을 해결하기 위해 IEEE에서는 2004년 3월 802.21 Working Group을 구성하여 이기종 망간 핸드오버 문제를 해결하기 위한 기술 표준화를 시작하였다[1]. 현재 표준화가 진행되고 있는 IEEE 802.21 기술은 사용자에게 끊김 없는 네트워크 서비스가 제공되도록 이질적인 무선 네트워크 환경을 연동할 수 있는 표준기술로서 관심이 집중되고 있다.

IEEE 802.21 WG에서 표준화하고 있는 MIH (Media Independent Handover)는 둘 이상의 다른 네트워크 접속 인터페이스를 갖는 다중모드 단말이 미디어에 독립적으로 이기종 망간 핸드오버를 할 수 있도록 지원하는 기술이다. 표준화 중인 MIH는 MIES (Media Independent Event Service), MICS (Media Independent Command Service) 그리고 MIIS (Media Independent Information Service) 등의 주요한 세 가지 서비스를 정의하고 있으며, 이 세 가지 서비스를 기반으로 MIH 프로토콜을 위한 메시지 프레임워크를 정의하고 있다[2]. 위와 같은 프레임워크로 구성되는 MIH는 또한 MIH 메시지를 안전하게 보호하고, 핸드오버 하는 사용자에게 인증 서비스를 제공하기 위한 보안 기술 표준화도 계속 진행하고 있다[3]. 하지만 아직까지는 기술 제안단계에서 기술 표준화를 위한 연구가 계속 되고 있으며, 현재 IETF의 EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)를 기반으로 하는 사전 인증 기술에 대한 관심이 집중되고 있다. 그러나 MIH가 적용된 이기종 망 환경에서 빠른 핸드오버 지원을 위한 인증 연동 기술에 대한 제안이 필요하다. 기존 인증 기술 중 MIH 기반 환경에 적용 가능한 AAA (Authentication, Authorization and Accounting) 서버 기반의 인증 기술[4]이 있지만 이기종 망을 핸드오버 하는 사용자가 매번 AAA 서버를 통해 인증을 받아야 하고, 인증을 받는 과정에서 추가적인 핸드오버 지연이 발생할 수 있으며, 인증을 위한 추가적인 메시지들로 인해 메시지 오버헤드가 증가하는 문제점이 존재한다.

본 논문에서는 이러한 보안 요구사항과 문제점을 해결하기 위한 인증 연동 프로토콜을 제안한다. 제안하는 기법은 기존에 많은 연구가 진행되고 있는 대리 서명 방식을 MIH 프로토콜에 적용하여 이기종 망간 인증 연동 및 핸드오버 하는 사용자 단말의 빠른 인증을 지원할 수 있도록 제안하였다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 본 논문에서 제안하는 기법과 관련된 기술들을 설명하고, Ⅲ장에서 본 논문에서 제안하는 기법에 대해서 자세하게 설명한다. 그리고 Ⅳ장에서 제안 기법에 대한 안전성 분석 및 보안 프로토콜 적용에 따른 성능을 평가하고, 마지막 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 기술

이번 장에서는 현재 IEEE 802.21 WG에서 표준화가 진행되고 있는 MIH 표준 기술과 본 논문에서 인증 연동을 위해 적용한 대리 서명 기법에 대해서 간략하게 설명한다.

1. IEEE 802.21 Media Independent Handover

둘 이상의 다른 네트워크 접속 인터페이스를 갖는 다중모드 단말에서 MIH는 미디어에 독립적으로 이기종 망간 핸드오버를 지원하기 위해 하위 물리 계층의 정보를 이용한다. 이를 위해 MIH에는 그림 1에서처럼 MIES (Media Independent Event Service), MICS (Media Independent Command Service) 그리고 MIIS (Media Independent Information Service) 등의 세 가지 주요 서비스를 정의하고 있다.

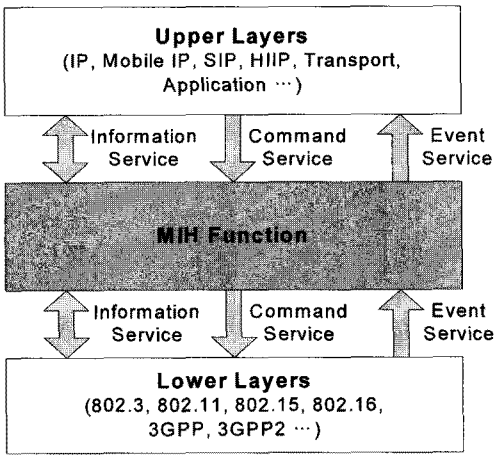


그림 1. MIH의 주요 서비스
Fig. 1. Key Service of MIH.

- MIES: MIES는 이벤트를 관리하는 서비스로 물리계층과 MAC 계층에서 발생하는 정보를 SAP (Service Access Point)를 통해 상위 계층으로 전달하는 기능을 담당한다. 여기서 사용되는 정보는 물리계층 및 MAC 계층에서 인지된 상태 변화에 대한 정보를 의미하고, 이때 발생한 이벤트는 단말의 상위 계층에 제공 된다.

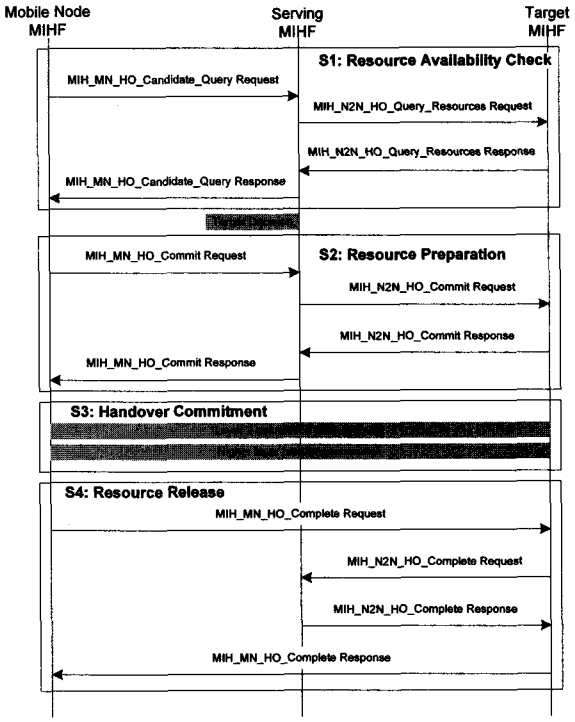


그림 2. MIH 프로토콜 핸드오버 동작 절차
Fig. 2. Handover Procedure of MIH Protocol.

- MICS: MICS는 상위 계층에서 결정된 내용을 하위 계층으로 전달하거나 하위 계층의 동작을 제어하는 기능을 제공한다.
- MIIS: MISS는 이기종 망간 핸드오버를 위해 필요로 하는 다양한 망 정보를 수집하고, 수집된 정보를 바탕으로 핸드오버를 수행할 수 있도록 지원한다.

위와 같은 세 가지 주요 서비스를 통해 MIH는 이기종 망간 핸드오버를 지원한다. 다음 그림 2는 사용자 단말에서 시작하는 이기종 망간 핸드오버 절차를 보여준다. 사용자 단말에서 핸드오버를 시작하는 경우 크게 네 가지 절차를 통해 핸드오버를 수행한다[1].

- Step 1 (Resource Availability Check): 사용자 단말에서 이기종 망간 핸드오버를 하기 위해 MIIS에게 MIH_Get_Information Request/Response 메시지를 통해 이용 가능한 주변 망 (Candidate Networks)에 대한 정보를 얻어 오는 과정이다.
- Step 2 (Resource Preparation): 주변 망에 대한 정보를 수신한 이동 노드에서 핸드오버 할 망 (Target Network)을 선택한 후 Serving PoS (Point of Service)와 Target PoS 간에 MIH_MN_HO_Commit Request/ Response 메시지를 주고받음으로서 핸드오버를 준비한다.
- Step 3 (Handover Commitment): 핸드오버 준비가 끝난 후 사용자 단말은 L2 계층에서의 정보를 기반으로 L2 및 L3 핸드오버를 수행한다.
- Step 4 (Resource Release): 정상적으로 핸드오버가 완료되면 사용자 단말은 MIH_MN_HO_Complete Request/Response 메시지를 Target PoS와 Serving PoS 간에 주고받으며 이전 망에서 할당되었던 네트워크 자원 해제 절차를 수행한다.

위와 같은 과정으로 사용자 단말에서 시작하는 이기종 망간 핸드오버를 지원하고, PMIPv6[5]를 적용하여 네트워크에서 이기종 망간의 핸드오버를 지원할 수도 있다.

2. 대리서명 기법

대리 서명 기법은 1996년 Mambo, Usuda, Okamoto가 그 개념을 처음 소개하였다[6]. 대리 서명 기법은 서명을 생성할 수 있는 원래의 서명자가 자신의 서명 권한을 지정한 대리 서명자에게 위임하여 자신을 대신하여 서명을 할 수 있도록 하였다. 이들이 처음 소개한 대리 서명은 서명 권한을 어떻게 위임하는가에 따라서 부분 위임 (Partial Delegation), 완전 위임 (Full Delegation), 보증 위임 (Delegation by Warrant) 등으로 구분된다[7]. 최근에는 보안상의 이유로 부분 위임과 보증 값을 이용하여 서명 권한을 위임하는 대리 서명 방식이 주로 사용된다. 이러한 대리 서명 방식은 서명 권한을 위임 받은 대리 서명자가 생성하는 대리 서명을 원 서명자도 생성할 수 있는지, 오직 대리 서명자만 생성할 수 있는지에 따라 다시 대리 서명자 보호형 (Proxy-protected) 대리서명 방식과 대리 서명자 비보호형 (Proxy-unprotected) 대리 서명 방식으로 분류할 수 있다. 다음은 Mambo가 제안했던 대리 서명 방식에 대해서 간략하게 살펴본다.

먼저 원 서명자는 임의의 큰 소수 p를 선택한다. 그 다음 $g \in Z_p^*$를 구하고, 자신이 생성하는 서명에 사용하는 개인 키 x_o를 이용하여 공개 키를 $y_o = g^{x_o} (\mathrm{mod}\, p)$와 같이 생성한다. 이후 선택된 대리 서명자에게 서명 권한을 위임하기 위해 서명을 생성한다. 이때 원 서명자는 임의의 k를 $k \in_R Z_p^*$와 같이 선택 후 K를 $K = g^k$와 같이 구한 다음 서명을 $\sigma = x_o + kK$와 같이 생성

하여 대리 서명자에게 σ와 K를 함께 전달한다. 원 서명자가 전송한 서명 정보를 대리 서명자가 수신하면 $g^{\sigma} = y_A K^K$를 계산하여 원 서명자의 서명을 검증하고, 검증에 성공하면 원 서명자의 서명을 이용하여 대리 서명을 생성할 때 사용하는 개인 키 x_p를 $x_p = \sigma + x_B y_B$와 같이 생성한다. 대리 서명에 사용하는 개인 키를 생성한 다음 공개 키는 $y_p = g^{x_p}$와 같이 생성한다. 이렇게 대리 서명용 개인 키와 공개 키를 생성함으로써 안전하게 대리 서명 권한을 위임 받게 된다. 이후 대리 서명자는 자신의 대리 서명용 개인 키로 메시지를 $S_{x_p}(m)$와 같이 서명한 후 서명 수신자에게 m, K, y_B 정보를 함께 전송하여 대리 서명을 검증 할 수 있게 한다. 사용자에게 전달된 대리 서명은 대리 서명자의 공개 키 y_p를 $y_p = y_o K^K y_B^{y_B}$와 같이 검증함으로써 확인 할 수 있다.

III. 제안 기법

본 장에서는 앞서 관련기술에서 설명했던 대리 서명 기술을 MIH 기반 이질적인 네트워크 환경에 적용하여 사용자가 이질적인 네트워크를 핸드오버 할 때 필요한 인증 연동을 지원할 수 있는 인증 연동 프로토콜에 대해서 설명한다.

먼저 본 논문에서는 WLAN, WiBor/WiMAX 그리고 3GPP LTE (Long Term Evolution) 환경을 가정한다. 사용자 인증을 위해 WLAN과 WiBor/WiMAX를 위한 AAA 서버와 3GPP LTE에서 non-3GPP 망과의 연동을 위해 가정하고 있는 non-3GPP AAA 서버를 가정한다[8]. 본 논문에서는 이러한 이기종 망을 핸드오버 하는 이동 단말을 고려하였으며, 이동 단말은 최소 둘 이상의 다중 인터페이스를 사용하는 멀티 인터페이스 단말을 가정한다. 그리고 인증 연동을 통한 사전 인증을 제공하기 위해 RSA 서명 기법[9]과 Diffie-Hellman 알고리즘을 적용하였다. 다음의 표 1에서는 본 논문에서 제안하는 인증 연동 프로토콜에서 사용하는 주요 용어들을 정리하였다.

그림 3은 현재 IEEE 802.21 WG에서 표준화가 진행되고 있는 MIH 표준 문서 중 이동 단말에서 핸드오버를 시작하는 경우의 MIH 프로토콜의 기본 동작 절차에 본 논문에서 제안하는 인증 연동 프로토콜을 적용하여 인증 연동이 수행되는 과정을 보여준다. 그림 3에서처럼 본 논문에서 제안하는 인증 연동 프로토콜은 기존 MIH 프로토콜 기본 동작 절차에서 사용되는 메시지를

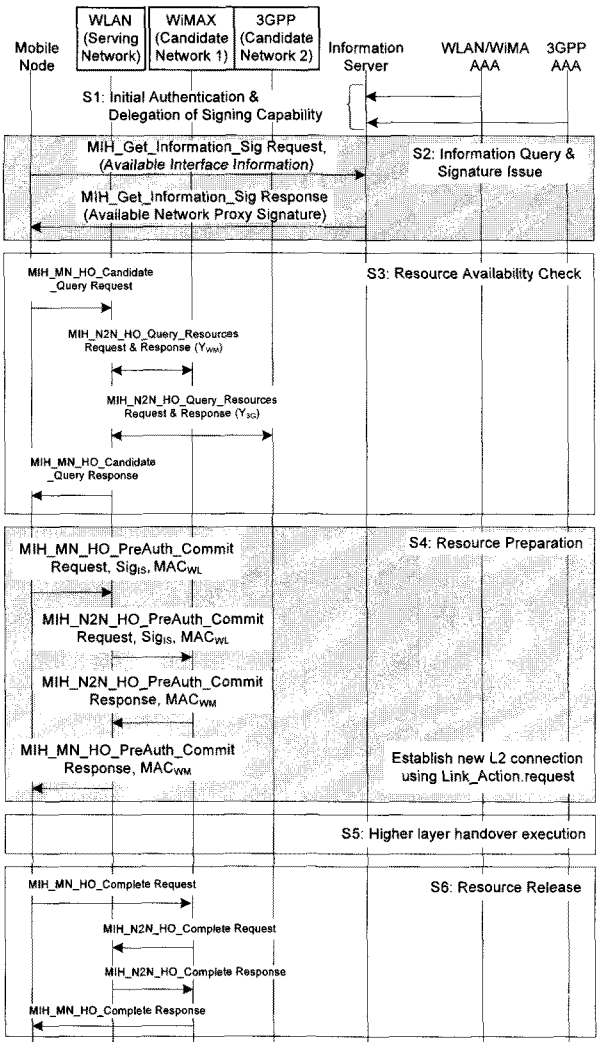


그림 3. 이동 단말이 시작하는 핸드오버 인증 연동 과정

Fig. 3. Mobile-Initiated Handover Authentication Interworking Procedure.

표 1. 프로토콜 표기법

Table 1. Definition.

표 기	정 의
s_x	원서명자 x의 서명 (AAA 서버)
s_{p-x}	MIHIS가 원 서명자 x를 대신하여 생성하는 서명
e_x, d_x	RSA 공개 키 및 개인 키
$h(\ )$	일방향 해쉬 함수
MAC_x	x가 일방향 해쉬 함수를 통해 생성한 메시지 인증 값
ID_x	x의 식별자
X_i, Y_i	Diffie-Hellman 비밀 및 공개 값
t	타임 스탬프 값

그대로 사용하기 때문에 인증 연동을 위해 추가적인 메시지가 필요 없다. 다만 서명 생성 및 분배 과정에서 필요한 정보를 제공하기 위해 MIH 기본 메시지 형식에 보안 정보를 함께 보내기 위한 추가 필드가 요구된다.

1. 제안 프로토콜의 동작과정

제안하는 인증 연동 프로토콜은 크게 초기 인증, 서명 정보 생성 및 분배 그리고 서명 정보를 이용한 이동 단말 인증 등의 과정으로 분류할 수 있다. 다음에서 각 단계에 대해서 설명한다.

- Step 1 (Initial Authentication & Delegation of Signing capability): 이동 단말, MIHIS (Media Independent Handover Information Server), 그리고 네트워크에 존재하는 장치들은 부팅과 함께 EAP-TLS를 통해 인증 서버와 초기 인증 과정을 수행한다. 이때 MIHIS가 WLAN, WiBro/ WiMAX AAA, 3GPP AAA 서버와 성공적으로 초기 인증을 완료하면 각 인증 서버는 자신의 서명 권한을 MIHIS에게 위임하는 과정을 수행한다.
- Step 2 (Information Query & Signature Issue): WLAN 환경에 있던 사용자가 다른 무선 망 환경으로 핸드오버를 할 경우 이동 단말의 MIH는 MIHIS에게 주변 네트워크 정보를 MIH_GET_Information_Sig Request 메시지를 통해 요청한다. 이때 전송되는 요청 메시지에는 이동 단말에서 이용 가능한 무선 인터페이스 정보와 MIHIS에서 서명 생성을 위해 필요한 이동 단말의 식별 정보 ID_{MN}, 시간 t_{MN}, 디피헬만 공개 값 Y_{MN} 등이 함께 전달한다. 메시지를 수신한 MIHIS는 이동 단말이 핸드오버 가능한 무선 망에서 사용할 수 있는 대리 서명을 생성한 후 MIH_GET_Information_Sig Response 메시지를 통해 이동 단말로 전달한다.
- Step 3 (Resource Availability Check): MIHIS로부터 주변 네트워크에 대한 정보를 수신한 후 이동 단말의 MIH는 MIHIS가 알려준 정보를 기반으로 주변 망으로 MIH_Candidate_Query Request/ Response 메시지를 보내 네트워크 자원상태를 검사한다. 이때 각 망에서 이동 단말로 보내는 응답 메시지에는 각 망의 Diffie-Hellman 공개 값이 포함되어 전달된다.
- Step 4 (Resource Preparation): 핸드오버 할 수 있는 무선 망에 대한 네트워크 자원 검사가 끝나면 이동 단말의 MIH는 Target Network를 결정하고, Target PoS와 MIH_HO_Commit_PreAuth Request/ Response 메시지를 주고받아 핸드오버를 준비한다. 이때 요청 메시지에는 이동 단말에 대한 사전 인증을 수행 할 수 있도록 MIHIS가 생성한 서명 Sig_{IS}과 MAC_{WL} 값이 포함된다. 요청 메시지에 함께 전달되는 MAC_{WL}은 Target Network의 Diffie-Hellman 공개 값을 이용하여 생성한 공유 비밀 키인 SK_{WL-WM}을 이용하여 생성한다. 이 서명을 이용하여 이동 단말이 핸드오버하기 전에 Target Network에서 이동 단말에 대한 사전 인증을 수행한다. 사전 인증 수행과정에서 이동 단말의 Diffie-Hellman 공개 값을 통해 동일한 SK_{WL-WM}를 생성하게 되고 이 키는 이후 이동 단말이 핸드오버 한 후 Target Network에서 채널 보안을 위해 사용된다.
- Step 5 (Higher Layer Handover Execution): 사전 인증이 성공하면 사용자 단말은 L2 계층에서의 정보를 기반으로 L2 및 L3 핸드오버를 수행한다.
- Step 6 (Resource Release): 정상적으로 핸드오버가 완료되면 사용자 단말은 Target Network의 Target PoS와 MIH_HO_Complete Request/ Response 메시지를 주고받음으로서 Serving Network에서 할당되었던 네트워크 자원을 해제하고 핸드오버를 완료한다.

2. 인증 연동을 위한 서명 발급 및 검증 과정

다음은 MIH가 적용된 환경에서 인증 연동을 위해 사용한 서명의 생성 및 분배, 그리고 검증 과정을 자세하게 살펴본다.

- 서명 권한 위임: Step 1에서 MIHIS의 초기 인증이 성공하면 각 인증 서버는 자신의 서명 권한을 MIHIS에게 위임한다. 서명 권한의 안전한 위임을 위해 각 인증 서버는 RSA를 이용하여 서명 권한을 위임을 위한 서명을 생성한다. 이를 위해 각 인증 서버와 MIHIS는 사전에 RSA 기반의 공개 키 (e,n)와 개인 키 (p,q,d)를 가진다. 각 인증 서버는 다음의 식 1과 같이 서명 권한을 위임하기 위한 서명을 생성하고, 생성된 서명 s_x와 서명이 생성된 시간 t_x를 MIHIS로 전송 한다 이때 생성된 서명에 포함된 ID_{AA}는 서명 권한을 위임하는 인증 서버의

식별정보 이고, ID_{IS}는 서명 권한을 위임받는 MIHIS의 식별정보 이다.

$$s_x = h(ID_{AA} \| ID_{IS} \| t_x \| e_{IS})^{d_x} \bmod n_x \quad (1)$$

• 서명 권한 위임 검증: MIHIS는 각 인증 서버가 전송한 서명 권한 위임을 위한 서명을 수신한 다음 각 서명에 대한 검증과정을 수행한다. 검증은 다음의 식 2와 같이 일방향 해쉬 함수를 이용하여 $H' = h(ID_{AA} \| ID_{IS} \| t_x \| e_{IS})$를 계산한 해쉬 값을 통해 검증한다.

$$H' = s_x^{e_x} \bmod n_x \quad (2)$$

• 이동 단말의 인증 연동을 위한 서명 생성: Step 2에서 이동 단말이 Serving Network에서 Target Network로 핸드오버 할 경우 이동 단말의 MIH는 MIHIS에게 가용한 주변 무선 망에 대한 정보를 MIH_GET_Information_Sig 메시지를 통해 요청한다. 전송하는 메시지에는 서명 생성 시 필요한 ID_{MN}, Y_{MN}, t_{MN} 등의 정보가 포함되어 전달된다. MIHIS에서 이동 단말을 위해 다음 식 3과 같이 서명을 생성한다.

$$S_{IS-x} = (s_x \oplus h(ID_{MN} \| Y_{MN} \| t_{MN} \| e_{IS}))^{d_{IS}} \bmod n_{IS} \quad (3)$$

• 이동 단말의 사전 인증: 이동 단말은 MIHIS로부터 서명을 발급 받은 후 서명을 검증한다. 검증은 다음 식 4와 같이 일방향 해쉬 함수를 이용하여 계산한 $H' = h(ID_{AA} \| ID_{IS} \| t_x \| e_{IS})$ 값을 이용하여 전달받은 서명을 식 4와 검증함으로써 원 서명자인 인증 서버와 대리 서명자인 MIHIS를 확인한다. 이후 Step 3 과정을 통해 이동 가능한 망의 Diffie-Hellman 공개 값을 알게 되고, Step 4에서 실제 핸드오버 할 Target Network를 결정한 다음 핸드오버 후 무선 채널에서 전달하는 메시지 등을 암호화하는데 사용하는 비밀 세션 키를 Diffie- Hellman 공개 및 개인 값을 이용하여 생성한다. 생성된 비밀 세션 키를 통해 식 5와 같이 MAC_{WL} 값을 계산하여 서명 정보와 함께 전달하고, 이 서명과 MAC_{WL}을 이용하여 이동 단말에 대한 사전 인증을 수행한다.

$$h(ID_{AA} \| ID_{IS} \| t_x \| e_{IS}) = (S_{IS-x}^{e_{IS}} \bmod n_{IS} \oplus h(ID_{MN} \| Y_{MN} \| t_{MN} \| e_{IS}))^{e_x} \bmod n_x \quad (4)$$

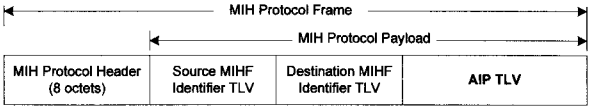


그림 4. 확장된 MIH 프로토콜 프레임 형태
Fig. 4. Expended MIH Protocol General Frame Format.

$$MAC_{WL} = h(SK_{MN-nPoA} \| Sig_{IS-x}) \quad (5)$$

위에서와 같이 이동 단말이 핸드오버 하기 전에 Target PoS에게 서명 정보를 전달함으로서 이동 단말에 대한 사전 인증을 수행한다. 이렇게 이동 단말에 대한 사전 인증이 마무리 되면 MIH_HO_PreAuth_Commint Response 메시지에 MAC_{TN} 값을 추가하여 이동 단말에 전달함으로써 핸드오버하기 전에 이동 단말의 사전 인증 및 비밀 세션 키를 공유하게 된다. 이후 Step 5와 Step 6 과정을 통해 L2, L3 핸드오버가 수행되고 마무리 된다.

3. 확장된 MIH 메시지

그림 4는 현재 IEEE에서 표준화 중인 MIH WG에서 정의하고 있는 MIH 프로토콜 프레임에 본 논문에서 제안하는 인증 연동 프로토콜을 적용하기 위해 새로운 AIP (Authentication Interworking Protocol) TLV (Type Length Value)를 정의한 것을 보여준다. 다음은 새롭게 정의한 AIP TLV에 대한 내용이다.

• AIP (Authentication Interworking Protocol) TLV
  - Data Type: OCTET_STRING
  - Content: AIP Message

위에서처럼 AIP TLV는 MIH 프로토콜에서 정의하고 있는 프로토콜 프레임 형식을 따른다. AIP TLV에 포함되는 정보들은 ID_x, t_x, Y_x, MAC_x, s_x 등 서명 생성과 분배, 그리고 이동 단말의 사전 인증을 위해 필요한 정보들이 AIP TLV 필드에 AIP 메시지로 포함되어 MIH 프로토콜 메시지와 함께 전달된다. 이를 위해 우리는 인증 연동 프로토콜이 적용된 MIH 프로토콜 메시지를 다음과 같이 정의하였다.

• MIH_GET_Information_Sig Request/Response: MIHIS에게 가용한 주변 네트워크 정보와 함께 서명 발행을 요청하는 메시지
• MIH_HO_PreAuth_Commint Request/Response: 핸드오버를 준비하는 과정에서 MIHIS가 발행한

서명 정보를 이동할 네트워크로 전달하여 이동 단말의 사전 인증과 이동할 네트워크의 접속 장비의 인증을 요청하는 메시지

위와 같이 본 논문에서 제안하는 인증 연동 프로토콜은 현재 IEEE 802.21 WG에서 표준화 중인 MIH 프로토콜을 최소한으로 수정하여 적용할 수 있도록 제안하였다.

Ⅳ. 분석 및 비교

이번 장에서는 본 논문에서 제안하는 인증 연동 프로토콜에 대한 안전성 분석과 성능 평가에 대해서 설명한다.

1. 제안 프로토콜의 안전성 분석

본 논문에서 제안하는 인증 연동 프로토콜은 기존 대리서명 기법에서 요구되는 다음과 같은 보안 요구사항을 만족한다.

- 강한 위조 방지 (Strong non-forgeability): 제안 기법은 인증 서버가 MIHIS에게 자신의 서명 권한을 위임하기 위해 전달하는 서명과 서명 권한을 위임받아 MIHIS가 생성하는 대리 서명에 대해 강한 위조 방지를 제공한다. 먼저 권한 위임을 위해 인증 서버가 생성하는 서명은 서명 권한을 위임하는 인증 서버의 ID_{AA}, 서명 권한을 위임받는 MIHIS의 ID_{IS}, 디피헬만 공개 값 Y_{IS}, MIHIS의 RSA 공개 키 e_{IS}를 해쉬한 결과를 인증 서버의 RSA 개인 키 d_x로 서명하여 전달하기 때문에 인증 서버 이외의 노드는 서명 권한 위임을 위해 생성되고 MIHIS에게 전달되는 인증 서버의 서명을 위조할 수 없다. 그리고 MIHIS가 인증 서버를 대신하여 생성하는 서명을 임의의 노드가 위조하기 위해서는 인증 서버가 서명 권한 위임을 위해 생성하는 서명에 포함되는 $h(ID_{AA}\|ID_{IS}\|t_x\|e_{IS})$ 값을 위조할 수 있어야 한다. 그러나 이 값은 초기 인증 과정에서 공유하는 비밀 키로 암호화된 채널을 통해 인증 서버로 전달되고, 전달된 값은 인증 서버의 개인 키 d_x로 서명되기 때문에 임의의 노드가 위조할 수 없으며, 대리 서명 검증 과정을 통해 위조 여부를 확인할 수 있다. 마지막으로 제안 기법의 경우 RSA 개인 키를 이용하여 서명을 생성하기 때문에 인증 서버 또는 MIHIS 또한 서로의 서명을 임의로 생성 할 수 없다.
- 강한 신원 확인 (Strong Identifiability): MIHIS가 생성하는 대리 서명은 서명에 포함된 $h(ID_{AA}\|ID_{IS}\|t_x\|e_{IS})$ 값을 통해 검증한다. 따라서 서명 검증 과정에서 사용되는 ID_{AA}, ID_{IS}, e_{IS} 등의 정보를 통해 MIHIS를 확인할 수 있으며, 제안 기법에서 제공하는 각 서명들은 초기 인증 과정을 통해 상호 인증된 각 노드들 간에 공유하는 비밀 키를 통해 암호화되어 전달되므로 상호 간에 강한 신원 확인이 제공된다.
- 강한 부인 방지 (Strong non-deniability): 제안 기법에서는 서명을 생성 및 발행 한 노드가 자신의 서명에 대해서 부인하는 것은 매우 어렵다. 우선 서명 권한 위임을 위해 생성하는 서명은 서명자의 개인 키로 서명하기 때문에 부인 할 수 없으며, MIHIS가 생성하는 서명 또한 MIHIS의 개인 키로 서명하기 때문에 역시나 자신이 생성한 서명에 대해서 부인할 수 없다.
- 검증가능성 (Verifiability): 제안 기법은 MIHIS가 정상적으로 인증 서버에게 서명 권한을 위임 받아 서명을 생성했는지를 누구나 쉽게 검증할 수 있다. 서명 권한 위임 검증은 $h(ID_{IS}\|Y_{IS}\|t_x\|e_{IS})$ 값을 계산하여 MIHIS가 생성하여 분배한 서명을 검증함으로서 확인할 수 있다. 검증에 사용되는 해쉬 값은 인증 서버가 MIHIS에게 인증 권한을 위임하기 위해서 자신의 개인 키로 서명 권한을 위임 받게 되는 노드의 식별 정보를 서명하기 때문에 이 정보는 위조 되거나 수정될 수 없다. 또한 해쉬 값을 계산하기 위해 필요한 ID_{IS}, Y_{IS}, e_{IS} 등의 정보는 모두에게 공개된 정보이고, t_x는 서명을 제공할 때 함께 전달되는 값이므로 누구나 검증에 필요한 해쉬 값을 생성할 수 있다.

2. 인증 연동 프로토콜의 성능 평가

다음은 본 논문에서 제안하는 인증 연동 프로토콜을 MIH 프로토콜에 적용하였을 경우 보안이 적용되지 않은 MIH 프로토콜과의 핸드오버 지연 분석을 통해 제안 기법에 대한 성능을 평가한다.

이기종 망 환경에서 이동 단말에게 끊김 없는 서비스를 제공하기 위해서는 현재의 PoA (Points of

표 2. 용어 정리
Table 2. Definition.

표 기	정 의
D_{IQ}	Information Query 과정 시간
D_{RC}	Resource Availability 검사과정 시간
D_{RP}	Resource Preparation 과정 시간
D_{RR}	Resource Release 과정 시간
D_{L2}	Layer 2 핸드오버 지연 시간
D_{L3}	Layer 3 핸드오버 지연 시간
T_{SI}	서명 생성 시간
T_{SV}	서명 검증 시간

Attachment)와 새롭게 핸드오버 하는 무선 망의 PoA와의 새로운 연결을 맺고 패킷을 전달 받는 과정을 빠르게 처리할 수 있어야 한다. 이를 위해 빠른 핸드오버를 지원하기 위한 다양한 기술들이 연구되어 왔다. 그러나 기존의 다양한 연구 결과에 따르면 제안된 빠른 핸드오버 기술의 경우에도 보안을 적용할 경우 핸드오버 지연 시간이 증가하는 경향이 있었다. 이는 보안 적용을 위해 추가되는 인증 메시지의 수가 증가하거나, 인증, 암호화 또는 복호화를 위해 필요한 계산량이 증가하기 때문이었다. 본 논문에서 제안하고 있는 인증 연동 프로토콜은 앞서 설명한 것과 같은 문제들을 피하기 위해 이동 단말이 핸드오버 할 때 계산량을 최소화하였고, 인증을 위해 메시지를 추가하지 않았다. 다음 표 2에서 성능평가를 위해 사용된 변수들을 정리하였다.

다음 그림 5는 본 논문에서 제안하는 인증 연동 프로토콜이 적용된 MIH 환경에서 이동 단말이 이기종 망으로 핸드오버 할 경우 발생하는 핸드오버 지연 시간을 보여주고 있다. 다음 식 5는 보안이 적용되지 않은 MIH 환경에서의 핸드오버 지연 시간을 나타낸다.

$$TD = 2D_{IQ} + 6D_{RC} + 4D_{RP} + 4D_{RR} + D_{L2} + D_{L3} \quad (5)$$

다음 식 6은 MIH 프로토콜에 인증 연동 프로토콜을 적용하였을 경우의 핸드오버 지연 시간을 나타낸다.

$$TD_{AIP} = TD + T_{SI} + 2T_{SV} \quad (6)$$

위의 식 6에서처럼 본 논문에서 제안하는 기법의 경우 인증 연동을 위해 MIHS가 서명을 생성하기 위해 필요한 시간, 그리고 이동 단말에서 MIHS가 발급한 서명을 검증하는 시간, 핸드오버 할 무선 망의 PoA에서 서명을 검증하는 시간 등이 추가로 필요하게 된다. 또

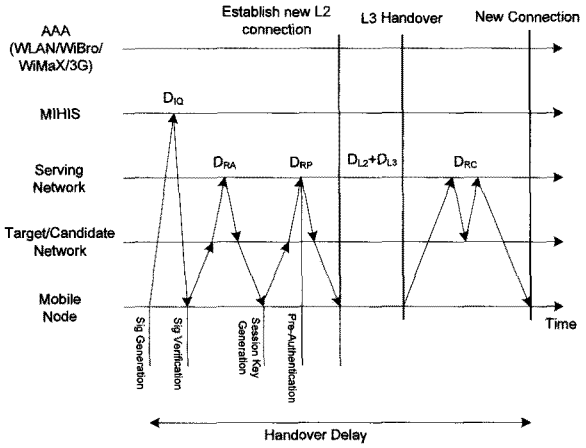


그림 5. AIP의 핸드오버 지연 시간
Fig. 5. AIP Signaling Message Flow Showing Handover Delay.

한 각 메시지들을 안전하게 전달하기 위해 사용되는 암호화와 복호화 시간이 추가적으로 필요하기 때문에 전체적인 핸드오버 지연 시간이 보안이 적용되지 않은 MIH 프로토콜에 비해 증가하는 것처럼 보인다. 그러나 제안 기법의 경우 서명을 생성하고, 검증하는 과정은 이동 단말이 핸드오버 할 무선 망을 결정하고 L2 핸드오버를 시작하기 전에 끝나기 때문에 핸드오버 지연시간에 크게 영향을 미치지 않는다. 다만 제안 기법의 경우 주고받는 메시지의 안전성을 위해 암/복호화가 필요하기 때문에 이에 따른 핸드오버 지연시간은 증가할 수 있다.

V. 결 론

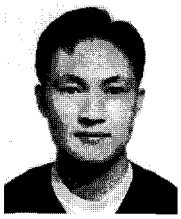
본 논문은 이기종 망간 핸드오버를 지원하기 위해 IEEE 802.21 WG에서 표준화 진행 중인 MIH 프로토콜이 적용된 WLAN, WiBro/WiMAX, 3GPP LTE 등의 이기종 망 환경에서 이동 단말이 핸드오버 할 때 필요한 인증 연동 프로토콜을 제안하였다. 제안하는 인증 연동 프로토콜은 RSA 서명을 이용한 대리 서명 기법을 적용하여 각 이기종 망의 인증 서버들이 초기 인증을 성공적으로 수행한 MIHIS에게 자신의 서명 생성 권한을 위임하고, MIHIS는 이기종 망으로 핸드오버하는 이동 단말이 사전 인증을 수행할 수 있도록 MIH 프로토콜에서 사용하는 기본 메시지에 생성한 서명을 전달하게 하였다. 또한 보안 적용에 따른 메시지 추가 없이 MIH 프로토콜 프레임에 새롭게 AIP TLV를 정의하여 사용하였다. 이렇게 함으로써 보안이 적용된 MIH 프로

토콜을 적용하였을 경우에도 보안을 위한 추가 메시지가 필요 없게 되었고, 사전 인증에 따른 핸드오버 지연시간에도 크게 영향을 주지 않도록 하였다. 마지막으로 제안하는 인증 연동 프로토콜에 대한 보안 분석과 핸드오버 지연시간을 분석해 봄으로써 MIH 기반 이기종망 환경에 효과적으로 적용할 수 있음을 보였다.

참 고 문 헌

[1] IEEE P802.21, "Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services," April 2008.
[2] Rahman, U. Olvera-Hernandez and M. Watfa, "Transport of Media Independent Handover Message Over IP," draft-rahman-mipshop-mih-transport-03.txt (work in progress), July 2007.
[3] IEEE P802.21, "Proactive Authentication and MIH Security," July 2009.
[4] M. Nakhjiri, et al., "AAA based Keying for Wireless Handovers: Problem Statement," Internet-Draft, draft-nakhjiri-aaa-hokey-ps-03, Work in progress, June 2006.
[5] S. Gundavelli, V. Devarapalli, K. Chowdhury and B. Patil, "Proxy Mobile IPv6," IETF RFC 5213, August 2008.
[6] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures: Delegation pf the power to sign message," IEICE Teans, E79-A, pp. 1338-1354, 1996.
[7] S. Kim, S. Park and D. Won, "Proxy Signatures, Revisited," ICICS'97, LNCS 1334, Springer-Verlag, pp. 223-232, 1997.
[8] 3GPP TR 23.882 V0.11.0, "3GPP System Architecture Evolution: Report on Technical Options and Conclusions," 2006.
[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem," Commun. ACM, pp. 120-126, 1978.

저 자 소 개



노 효 선(정회원)
2005년 숭실대학교 정보통신전자공학부 학사
2007년 숭실대학교 정보통신전자공학과 석사
2007년~현재 숭실대학교 전자공학과 박사과정
<주관심분야 : 네트워크 보안, 이동 네트워크 보안, IPTV 보안>

정 수 환(평생회원)-교신저자
1985년 서울대학교 전자공학과 학사
1987년 서울대학교 전자공학과 석사
1996년 University of Washington 박사
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 부교수
2009년~현재 지식경제부 지식정보보안 PD
<주관심분야 : 이동 네트워크 보안, 차량 네트워크 보안, VoIP 보안, RFID/USN 보안>