

가상 ISIM을 통한 서비스 연속성 제공을 위한 근접 단말 등록 방법

임 종 철*, 김 상 하°, 금 창 섭*

The User Terminal Registration Method in Proximity Using the Virtual ISIM for Providing Service Continuity

Jong-choul Yim*, Sang-ha Kim°, Chang-sup Keum*

요 약

NGN에서는 사용자가 여러 개의 단말을 사용할 수 있는 환경을 지원해야 한다. 특히 사용자가 이동하면서 동적으로 발견하는 단말을 통해 끊김 없는 서비스를 제공받을 수 있어야 하며, 이를 위해서 서비스 연속성 지원이 필수적이다. 현재의 IMS는 서비스 연속성 제어를 위한 세션 제어 방법에 대해서는 다루고 있으나, 세션을 이동할 단말을 어떻게 찾을 수 있는가에 대해서는 제한적인 방법만을 제시하고 있다. 사용자가 이동하면서 발견하는 단말은 물리적으로 사용자와 가까이 위치해 있을 가능성이 상당히 높고, 여러 사람에 의해 공유되어 사용되는 단말일 가능성이 있다. 그러므로 사용자에게 보다 나은 서비스 경험을 제공하기 위해서는 물리적으로 가까이 있는 단말을 사용자가 마치 자신의 단말인 것처럼 사용할 수 있도록 하는 방법이 필요하다고 할 수 있다. 본 논문에서는 전술한 문제를 해결하기 위해 NFC 기반의 가상 ISIM을 통해 사용자가 소유한 기존 단말에 저장된 IMS 가입 정보를 동적으로 발견한 단말로 전달하여 그 단말을 IMS에 등록시키는 방법을 제안하고, 더불어 이를 통해 서비스 연속성 제공이 어떻게 이루어질 수 있는지를 논한다.

Key Words : NGN, IMS, ISIM, Registration, Service Continuity

ABSTRACT

The NGN should support an ubiquitous environment in which users can use multiple devices. Especially, services should be provided to users in a seamless manner across multiple devices which are dynamically found in users' vicinity. Therefore, supporting service continuity is essential in the NGN. Currently the IMS, which is a session control layer for the NGN, deals with session control procedures in detail for service continuity. However, the IMS provides limited methods how users can find target terminals for transferring the session. The target terminals tend to be located near in user's physical location, and could be shared among different users. For providing better service experience in the NGN, The NGN needs to encompass methods to enable for users to use the dynamically-found terminals in users' vicinity seamlessly. In this paper, we introduce a novel registration method based on virtual ISIM by which the target terminals in user's vicinity can register themselves to the IMS, and also we discuss how service continuity is supported.

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발 사업의 일환으로 수행하였음.[14-000-04-001, 초연결 스마트 모바일 서비스를 위한 5G 이동통신 핵심기술 개발]

♦ First Author : Electronics and Telecommunications Research Institute, hector@etri.re.kr, 정희원

° Corresponding Author : Chungnam National Univ. Department of Computer Science & Engineering, shkim@cnu.ac.kr, 정희원

* Electronics and Telecommunications Research Institute, cskeum@etri.re.kr

논문번호 : KICS2014-10-429, Received October 22, 2014; Revised January 8, 2015; Accepted February 12, 2015

I. 서 론

현재의 이동통신망은 사용자가 하나의 단말을 소지한 상태에서 사용자가 이동 중에 통신망 서비스를 제공 받을 수 있는 기능을 제공한다. 최근에는 수많은 장치들이 네트워크에 연결되고, 사용자가 이동하면서 이러한 장치들을 자유롭게 이용할 수 있는 네트워킹 환경으로의 발전이 이루어지고 있다. 이는 곧 사용자가 여러 개의 단말을 사용할 수 있는 환경으로의 발전을 의미한다. 이때, 사용자는 개인 소유의 여러 개의 단말을 사용함은 물론 여러 사람에 의해 공유될 수 있는 단말을 사용할 수도 있을 것이다. 이런 환경에서 사용자의 주 단말에 저장된 IMS 가입 정보를 이용하여 사용자가 주위에서 발견한 단말을 사용할 수 있도록 한다면, 이는 사용자의 서비스 경험을 크게 향상시킬 수 있을 것이다.

사용자가 여러 개의 단말을 사용할 수 있는 환경에서 보다 나은 사용자 경험을 제공하기 위해서는 단말 간 서비스 연속성 제공이 필수적이라 할 수 있다. 단말 간 서비스 연속성이라 함은 사용자가 현재 제공받는 서비스가 단말이 바뀌더라도 끊이지 않고 제공되는 것을 일컫는다. SIP 프로토콜^[8]을 이용하여 어플리케이션 계층에서 단말 간 세션 이동을 제어하는 연구들이 진행되었으나 NGN의 표준 제어 계층인 IMS를 고려하지 않고 있다.

IMS(IP Multimedia Subsystem)는 NGN에서 사용자에게 다양한 서비스를 제공하기 위해 필요한 제어 시그널링을 제공하는 세션 제어 계층으로서, 다양한 멀티미디어 서비스를 위한 세션 설정, 변경 및 해제 등 제어를 SIP 프로토콜을 이용하여 수행한다^[15]. 최근 3GPP가 표준화하고 있는 IMS에는 협업 세션(Collaborative Session)을 통해 단말 간 세션 이동을 제어함은 물론 다양한 서비스 연속성을 가능하도록 하는 방법이 포함되어 있다^[13,14].

단말 간 서비스 연속성을 제공하기 위해서는 크게 2단계의 절차가 필요하다. 첫 번째 단계는 세션 이동을 할 대상 단말을 찾는 단계이며, 두 번째 단계는 실제 시그널링을 통해 세션 이동 제어를 수행하는 단계이다. 현재의 IMS 규격에서는 두 번째 단계에 대한 처리 절차는 상세하게 정의되어 있으나, 첫 번째 단계에 필요한 단말 탐색과 관련된 내용은 부족한 상태이다. 단말 검색과 관련하여, IMS 규격에서는 사용자 단말 내에 정적으로 세션 이동 대상이 될 수 있는 단말 정보가 미리 설정되어 있거나 등록 이벤트 감지를 통해 다른 단말이 등록됨을 통지받음으로써 단말을 탐

색할 수 있다고 규정하고 있다. 이는 사용자가 세션 이동을 할 단말 정보를 대해 미리 알고 있어야 한다는 사전 조건이 만족되어야 한다는 것을 뜻하는데, 그로 인해 NGN의 유비쿼터스 서비스 제공 환경, 즉 사용자가 주위의 단말을 동적으로 발견하여 즉각적으로 사용할 수 있어야 한다는 특성을 지원함에 있어 제약이 있을 수 있다. 사용자가 발견하는 장치는 사용자 자신의 소유의 장치가 아닌 공용 단말일 가능성도 높다. 예를 들어, 대내의 TV나 회의실안의 공용 컴퓨터 등 여러 사람에 의해 공유될 수 있는 단말일 수 있을 것이다. 이러한 공유 단말을 임시로 마치 내 단말인 것처럼 사용할 수 있도록 하는 새로운 방법이 필요하다고 할 수 있다. 영화보기와 같은 멀티미디어 스트리밍 서비스의 경우 Miracast^[19]와 같이 단말 대 단말의 직접 통신을 함으로써, 한 단말에서 다른 단말로 스트리밍을 복사하는 방법을 통해 다수 단말을 사용하는 것이 가능할 수 있으나 이러한 방법은 단지 영상 및 음성을 다른 단말을 통해 볼 수 있을 뿐 다른 단말들을 온전히 내 단말인 것처럼 사용하는 데에는 제약이 있다.

한편, 일반적인 상황에서 서비스 세션을 이동할 대상 단말은 현재 사용자의 근처에 있는 단말이 될 것이다. 사용자가 세션 이동 대상 단말을 시각적으로 인식하며, 대상 단말과의 직간접적인 접촉을 통해 세션 이동을 명시적으로 시작할 수 있음을 암시한다.

본 논문에서는 전술한 IMS에서의 단말 탐색 관련 제약을 극복하고, 사용자가 이동하면서 발견한 단말을 마치 자신의 단말처럼 이용할 수 있도록 하는 NFC(Near Field Communication) 기반의 가상 ISIM(IP Multimedia Services Identity Module)을 소개하고, 이를 이용한 단말 간 서비스 연속성 제공 방법에 대해 논하고자 한다.

II. 관련 연구

2.1 서비스 연속성 관련 연구

SIP 프로토콜을 이용한 세션 이동성 제어 방법은 많이 연구되어 왔다. 가장 기본적인 방법은 3PCC(Third-Party Call Control)^[9] 혹은 refer^[10] 방법을 사용하여 단말끼리 SIP 시그널링을 사용하여 현재 진행 중인 세션을 옮기는 방법이다^[1]. IMS에서의 서비스 연속성 제어 방법은 SIP을 이용하여 제어를 한다는 측면에서 기본적으로는 위와 유사한 방법을 사용한다고 할 수 있다. 좀 더 세밀한 세션 이동성 제어를 위해 SIP 헤더를 확장함으로써 세션을 쪼개어 제

어할 수 있는 방법을 제시되었지만 확장한 헤더를 인식할 수 있는 특별한 UA(User Agent)가 필요하다는 단점이 있을 수 있다^[2].

몇몇 논문은 사용자가 이동하면서 동적으로 발견하는 단말로의 서비스 연속성 제공이 필요한 유비쿼터스 네트워크 환경에서 세션 이동성 제공이라는 주제를 다루고 있다. “Virtual Device”라는 개념을 통해 이동하면서 발견한 장치를 사용자의 “Virtual Device”로 포함시켜 이를 자유롭게 제어할 수 있는 방법을 제시하였고, 사용자가 현재 위치를 기반으로 하여 동적으로 장치를 발견할 수 있는 방법을 제시하였다^[3] 특히 [4]는 사용자의 프로파일을 다른 장치로 이동할 수 있는 방법을 제시하여 프로파일 이동성(Profile Mobility)을 제공하였다. 그러나 이러한 논문들은 NGN의 실질적인 표준이 되고 있는 IMS를 고려하고 있지는 못하다.

세션 이동성 제어 측면에 초점을 두지 않고 단말 탐색에 초점을 둔 논문들도 찾아볼 수 있다. [6]은 사용자의 위치 정보를 기반으로 사용자가 세션 이동 대상 단말을 쉽게 찾을 수 있는 방법을 제공하고 있으나, 단말 정보를 제공하는 별도의 서버를 필요로 한다는 제약이 있다. 단말 간 세션 이동에 있어서 세션을 이동할 단말은 사용자와 아주 가까이 있을 가능성이 아주 높다. 그러한 특성을 이용하여, 사용자 단말과 세션 이동 대상 단말 사이의 NFC 통신을 통해 세션 이동과 관련된 세션 파라미터 정보를 직접 교환함으로써 세션 이동을 할 수 있는 방법에 대한 연구도 진행되었다^{[7][21]}.

2.2 IMS

IMS는 이동통신망을 포함한 NGN에서 사용자에게 IP 기반의 다양한 멀티미디어 서비스를 제공하기 위한 세션 제어 기능을 제공하는 핵심적인 시스템이다. 세션 시작과 이동, 종료 등 세션을 제어하기 위한 프로토콜로서 SIP을 사용하고 있으며, CSCF(Call Session Control Function)에 의해 단말 등록, 메시징 라우팅, 서비스 접근 등 세션 제어와 관련된 기본적인 기능들이 제공되며, 다양한 부가 서비스를 위한 별도의 AS(Application Server)를 구비할 수 있다. IMS에서 사용자 단말은 UE(User Equipment)로서 정의된다.

사용자가 IMS 기반의 서비스를 제공받기 위해서는 사용자 단말이 먼저 IMS에 등록되어야 한다. 사용자가 LTE(Long Term Evolution)와 같은 이동 액세스 망을 이용할 경우 이동통신망 접속 자체에 대한 인증이 필요하고 이러한 기능은 USIM(Universal

표 1. ISIM에 저장된 정보
Table 1. Information in ISIM

Name	Description
IMS Private Identity (IMPI)	사용자의 개인 아이디로서, IMS에서 가입자를 식별
IMS Public Identity (IMPU)	사용자의 공개 아이디로서 다른 사람에게 알려주는 아이디 (예: 전화번호)
Home Network Domain Name	가입 통신망의 도메인 네임
P-CSCF Address	IMS의 네트워크 요소 중 P-CSCF의 주소
Long-term Secret Key	사용자와 통신망 사업자 사이에 공유되는 비밀 키, 노출되어선 안 됨

Subscriber Identity Module)에 의해 제공되지만, 본 논문에서는 IMS 기반의 서비스 제공 측면에서 접근하고 있기 때문에, USIM에 의한 망 접속 인증에 대해서는 다루지 않는다. 3GPP에서는 IMS 등록과 관련하여 ISIM을 정의하고 있다^[6]. ISIM에는 표 1과 같이 IMS에 등록에 필요한 중요한 정보들이 저장되어 있으며 IMS AKA(Authentication and Key Agreement) 기반의 인증을 수행하기 위한 기능을 포함하고 있다^[17].

롱텀 비밀 키는 ISIM과 HSS(Home Subscriber Server)간에 사전에 공유되는 키로서 단말 등록 시 사용된다. 단말의 IMS 등록 처리는 S-CSCF에 의해 이루어진다. 단말이 IMS에 등록하려 할 때, 단말과 S-CSCF 사이에 롱텀 비밀키를 직접 교환하는 대신 롱텀 비밀 키를 이용하여 계산한 “challenge”와 “response”를 주고받는 방식을 사용한다.

최근 서비스 연속성에 대한 필요성으로 인해 현재 진행 중인 세션을 다른 단말로 이동할 수 있는 방법이 IMS에 포함되어 표준화 되고 있다^{[13][14]}. IMS에서는 단말 간 세션을 이동하는 기능을 IUT(Inter-UE Transfer)라고 정의하고 있으며, 그림 1과 같은 구조

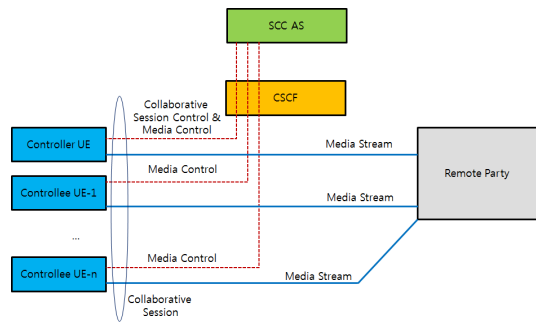


그림 1. IUT를 위한 IMS 구조
Fig. 1. IMS Architecture for IUT

를 통해 서비스 연속성을 제공하고 있다. 3GPP 릴리즈 9 이전 규격에 따르면 IUT에 관여하는 두 단말은 같은 가입자의 단말이어야 한다는 제약이 있다. 최근 규격을 통해 다른 가입자 단말과의 IUT를 제공할 수 있도록 확장되었으나 상당히 복잡한 절차를 통해 서비스 제공이 가능하다.

IUT에 관여하는 단말은 역할에 의해 크게 두 가지로 구분을 한다. 단말 간 세션 이동을 통제할 수 있는 단말(Controller UE)과 세션 이동의 대상이 되는 단말(Controllee UE)이다. 이 때, Controller UE와 Controllee UE에 의해 조작되는 세션을 Collaborative Session이라 한다. SCC AS(Service Centralization & Service Continuity Application Server)는 3PCC(Third Party Call Control) 방식으로 Controller UE와 Controllee UE간 IUT를 제어하기 위한 핵심 기능을 제공한다. Controller UE는 진행 중인 세션 전체 혹은 일부를 Controllee UE로 옮길 수가 있는데, 전체를 옮길 경우, 이를 세션 핸드오프라고 하고, 이 경우에는 Controller UE와 Controllee UE의 구분은 필요하지 않다.

단말 간 세션 이동을 하기 위해서는 대상 단말을 찾는 일이 선행되어야 한다. 현재의 IMS 규격에서는 단말 내에 대상 단말이 미리 정적으로 설정되어 있다고 여기거나, 등록 이벤트 패키지를 통해 대상 단말을 확인하는 방법을 제시하고 있다. 이러한 IMS의 단말 검색 방법은 사전에 세션을 이동할 대상 단말에 대한 정보를 알고 있어야 한다는 점에서 다양한 단말을 동적으로 발견하면서 사용할 수 있는 유비쿼터스 환경의 요구사항을 만족시킬 수 없을 것이다.

III. 단말 발견 및 등록 방법의 확장

앞으로의 네트워킹 환경에서는 사용자가 다수의 단말을 사용하고, 사용자가 이동하면서 발견하는 단말을 자유롭게 사용할 수 있는 환경이 될 것이다. 이때, 사용자에게 끊임 없는 서비스 이용 경험을 제공하기 위해서는 발견한 단말을 마치 사용자의 단말처럼 사용할 수 있도록 하는 기법이 필요하다. 우리는 앞서 NGN에서의 서비스 제공은 IMS를 통해 이루어진다는 것을 살펴보았다. 따라서 현 사용자의 IMS 가입 정보를 이용하여 ‘발견한 단말’을 IMS에 등록시킬 수 있다면, 전술한 요구사항을 만족시킬 수 있을 것이다. 그림 2는 본 논문이 대상으로 하는 전체 시스템의 참조 구조이다. 사용자가 소지한 마스터 단말은 IMS에 가입되어 SIP 기반 서비스 세션 제어를 통해 NGN에

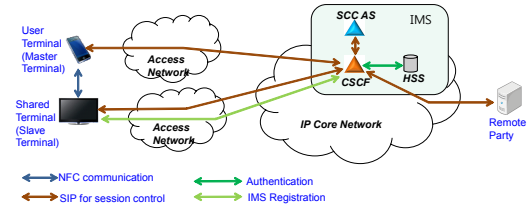


그림 2. 전체 시스템 구조
Fig. 2. Overall System Architecture

서 제공하는 다양한 서비스를 이용할 수 있다. 사용자가 이동하면서 발견하는 단말은 사용자와 물리적으로 가까이 있을 가능성이 매우 높다. 따라서 근접 통신 기술을 이용하여 마스터 단말의 IMS 가입 정보를 슬레이브 단말에 전달하여 슬레이브 단말이 IMS에 등록되도록 할 수 있다면 슬레이브 단말을 통해 IMS 기반의 다양한 서비스를 끊임 없는 서비스 경험을 통해 이용할 수 있게 되며, IUT 기능을 통해 현재 대국(Remote Party)과 진행 중인 멀티미디어 세션을 슬레이브 단말로 전송하는 것도 가능할 것이다. 본 논문에서는 사용자가 발견한 단말은 IMS 가입 정보를 가지지 않는, 여러 사람에 의해 사용될 수 있는 공용 단말이라고 가정하고, 사용자 단말에 이미 존재하는 IMS 가입 정보를 근접 통신 기술인 NFC를 이용하여 공용 단말에 전달함으로써 공용 단말을 IMS에 등록시키는 새로운 방법에 대해서 논의하고자 한다. 본격적인 논의에 앞서 다음과 같이 단말에 대한 정의를 내린다.

- 슬레이브 단말 - 자체적인 인증 정보를 갖지 않고 있으며, 마스터 단말로부터 인증 정보를 받아 인증을 수행할 수 있는 단말 (예: 사용자가 이동하면서 발견하는 공용 단말)
- 마스터 단말 - 사용자 인증 정보가 저장된 단말로서, 슬레이브 단말에 인증 정보를 제공하는 단말 (예: 사용자의 휴대 단말)

슬레이브 단말을 IMS에 등록시키기 위해 마스터 단말에서 슬레이브 단말로 모든 IMS 가입 정보를 전송하게 된다면, 정보 전달 과정에서 인증정보가 유출될 가능성과 마스터 단말로부터 인증 정보를 받은 슬레이브 단말이 인증 정보를 이용하여 악의적인 행동을 할 위험성에 노출되게 된다. 인증 정보 전송 단계의 인증 정보 유출 문제는 NFC 통신 시 보안 채널을 이용함으로써 해결 할 수 있다. NFC의 경우 매우 근접한 거리에서 통신하기 때문에 비교적 안전하고 통신 시 보안 채널을 사용한다면 정보 유출을 효과적으로 막을 수 있다⁵⁾. 슬레이브 단말의 인증 정보 악용 문제는 마스터 단말에 포함된 인증 정보 중 가장 중요

한 인증 정보인 롱텀 비밀 키를 전송하지 않도록 함과 동시에 마스터 단말이 슬레이브 단말의 등록 여부를 결정할 수 있도록 함으로써 해결할 수 있다.

IMS에서의 사용자 단말 인증은 IMS AKA 방법을 이용한다. 이를 위해 사용자 단말에는 ISIM이 탑재가 되고, ISIM에는 표 1에 설명된 바와 같은 인증에 필요한 정보들이 저장되어 있다. IMS AKA를 이용한 인증 방법은 기본적으로 “Challenge and Response” 기법을 이용한다고 할 수 있다. 그림 3에 도시된 것과 같이 단말이 IMS에 등록하기 위해 REGISTER 메시지를 전송하면(4) S-CSCF는 단말에게 401 Unauthorized 메시지를 전송하게 되는데, 이 메시지 안에 IMS에 등록에 필요한 정보와 질문(Challenge)이 포함되어 있다. 단말이 “challenge”에 대한 올바른 응답을 S-CSCF에 전송하게 되면 등록이 성공하게 된다. 이 때 challenge에 해당하는 것이 nonce 값이고, 응답에 해당하는 것이 response 값이다. nonce 값과 response 값을 계산하기 위해서는 롱텀 비밀 키가 필수적이다. 본 논문에서는 동적으로 발견한 단말을 IMS에 등록시키기 위해 그림 3과 같은 확장된 등록 절차를 제안한다.

가장 먼저 마스터 단말과 슬레이브 단말 사이에 NFC의 통신 모드 중 Peer to Peer 모드의 통신 채널을 연다(1). 이 통신 채널은 아주 근거리에서 동작하고, NFC의 보안 통신 메커니즘을 적용할 수 있기 때문에 도청 등에 보안 위협에 대해 안전하다고 볼 수 있다. 이 후, 마스터 단말과 슬레이브 단말의 통신은 이 통신 채널을 이용한다. 마스터 단말이 슬레이브 단말의 IMS 등록을 유도하기 위해 활성화 요청 메시

지를 슬레이브 단말로 전송한다(2). 활성화 요청을 받은 슬레이브 단말은 IMS 등록에 필요한 정보를 마스터 단말로부터 읽게 된다(3). 이때 포함되는 정보는 개인 단말의 ISIM 저장되어 있는 정보 및 부가 정보로서 IMPI, IMPU, 홈 네트워크 도메인 이름, P-CSCF 주소, Registration Owner 등으로 구성된다. Registration Owner는 사용자의 단말을 마스터 단말로 사용하기 위해 필요한 값으로서 마스터 단말의 GRUU(Globally Routable User Agent URI) 값이다.

슬레이브 단말은 단말 등록에 필요한 정보 획득 후, IMS에 등록을 하기 위해 REGISTER 메시지를 S-CSCF로 전송한다(4). 실제 메시지 전송은 P-CSCF와 I-CSCF를 거쳐 갈 수 있지만, P-CSCF와 I-CSCF는 단순히 메시지가 거쳐 가는 노드로 사용되기 때문에 본 논문에서 별도의 설명은 하지 않는다. 이 때 전송되는 REGISTER 메시지에는 IMS 등록 표준 절차에 따른 헤더들이 모두 포함되고, 다음과 같은 Registration-Owner 헤더를 추가적으로 포함한다. Registration-Owner 헤더에는 owner_uri가 포함되는데, 그 값은 전 단계에서 마스터 단말로부터 획득한 마스터 단말의 GRUU 값이다.

· 예) Registration-Owner:

```
owner_uri="sip:master_public1@home1.net;
gr=f71dlifa-9avc-1lia-d997-89ks";
```

Registration-Owner 헤더를 사용하는 이유는 지금 등록하려는 단말(슬레이브 단말)의 제어권을 가진 마스터 단말을 S-CSCF에게 알려주기 위함이다. S-CSCF는 이 바인딩 정보를 기반으로 슬레이브 단말의 등록 진행 상황을 마스터 단말에게 알려줄 수 있다.

슬레이브 단말로부터 REGISTER 메시지를 받은 S-CSCF는 Registration-Owner 헤더로부터 마스터 단말의 GRUU를 획득한 후, 마스터 단말의 인증 정보를 이용하여 IMS에 등록하려는 단말이 있음을 마스터 단말에게 NOTIFY 메시지를 통해 통보한다(5). 이때, NOTIFY 메시지에는 REGISTER 메시지에 포함된 Registration-Owner 헤더가 그대로 포함되며, registration event package 규격(RFC 3680, RFC 5628)^{[11],[12]}에 따른 슬레이브 IMS 단말의 등록 상태가 포함된다. registration event package 규격에 따르면 reginfo라는 XML 양식을 사용하여 단말의 여러 가지 등록 상태를 표현하게 된다. 상기 규격에 의하면 등록 상태로서 “registered”, “created”, “refreshed”, “shortened”, “expired”, “deactivated”, “probation”, “unregistered”, “rejected”가 정의되어 있는데, 새로운 상태인 “registering”을 추가하여 사용한다.

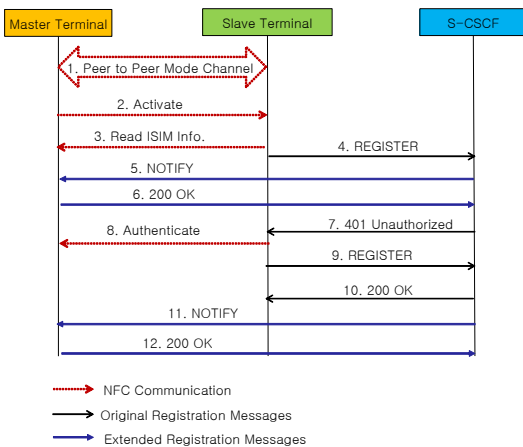


그림 3. 슬레이브 단말의 등록 절차
Fig. 3. Registration of the Slave Terminal

“registering”은 단말이 등록을 시도한다는 의미로서 사용된다. NOTIFY 메시지를 수신한 마스터 단말은 슬레이브 단말이 마스터 단말의 IMS 가입 정보를 통해 IMS에 등록하려 한다는 사실을 알게 되고, 그 후 뒤따르는 메시지 절차에서 슬레이브 단말이 요청하는 인증 정보 요청에 대응할 수 있게 된다.

한편 NOTIFY를 마스터 단말에게 전송한 후, S-CSCF는 표준적인 IMS 등록절차에 따라 nonce 값이 포함된 401 Unauthorized 메시지를 슬레이브 단말에 전송한다(7). 이때 S-CSCF는 등록을 요청하는 단말에 대한 인증 정보(Authentication Vector)가 없다면 HSS에 질의하여 획득하여야 한다. 401 Unauthorized 메시지를 수신한 슬레이브 단말은 마스터 단말에게 인증 정보를 요청하여 획득하고(8), 인증 정보를 포함한 REGISTER 메시지를 S-CSCF에 전송한다(9). S-CSCF는 인증이 성공되었음을 200 OK를 통해 슬레이브 단말에 전송하고(10), NOTIFY를 통해 마스터 단말에도 알린다(11). (7)에서 슬레이브 단말은 401 Unauthorized 메시지의 Authorization 헤더에 포함되어 있는 nonce 값을 마스터 단말에게 전달하고, 마스터 단말은 슬레이브 단말의 인증 요구가 적절한가를 먼저 검증한 후에, 마스터 단말에 저장되어 있는 롱텀 비밀 키와 파라미터로 전달 받은 nonce 값을 기준으로 response 값을 생성하고 이를 슬레이브 단말에게 전달한다. 슬레이브 단말은 (9)에서 REGISTER 메시지의 Authorization 헤더 안에 획득한 response 값을 포함하여야 한다.

우리는 이 확장된 등록 절차에서 마스터 단말에 저장되어 있는 IMPU, IMPI 등 IMS 등록에 필요한 정보가 슬레이브 단말로 전송된다는 사실을 확인하였다. 또한 슬레이브 단말의 IMS 등록과 관련된 시그널링은 슬레이브 단말이 직접 수행하였다. 악의적인 슬레이브 단말이 마스터 단말로부터 획득한 정보를 기반으로 독립적으로 IMS에 등록을 시도할 수 있기 때문에 이에 대한 대비책이 필요하다. 이에 대한 대비책으로서 본 논문에서는 두 가지의 메커니즘을 도입하였다.

- 가) 롱텀 비밀 키는 전송하지 않음
- 나) NOTIFY 메시지를 통한 등록 과정 감시 및 자격 검증

첫 번째 방법은 IMS 등록 시 반드시 포함되어야 하는 Authorization 헤더 안에 포함되는 response 값 생성과 관련된 것이다. IMS AKA 인증 방법에 따르면 롱텀 비밀 키 자체는 단말과 S-CSCF 사이에 교환되지 않고, 롱텀 비밀 키로부터 유도된 nonce 값과 response 값이 교환된다. 슬레이브 단말이 IMS에 등

록을 수행할 때 nonce 값에 대한 response 값을 생성해야 하는데, 이 때 롱텀 비밀 키가 필요하다. 이를 위해 슬레이브 단말이 롱텀 비밀 키 자체를 마스터 단말에게서 획득한다면, 슬레이브 단말이 임의로 IMS에 등록하는 것을 방지할 수가 없다. IMS 등록 시 필요한 정보는 롱텀 비밀 키 자체가 아니라 nonce에 대응하는 response 값이라는 점을 이용하여 본 논문에서는 ISIM에 저장된 값 중 보안 측면에서 가장 중요한 값인 롱텀 비밀 키를 슬레이브 단말에게 전송하지 않는 대신 마스터 단말이 nonce 값을 전달 받아 response 값을 생성하도록 하였다. 슬레이브 단말은 단말 등록 시 필요한 response 값을 스스로 만들어 낼 수 없기 때문에 임의로 IMS에 등록할 수 없다. 그러나 비교적 중요한 값인 IMPI는 전달되기 때문에, 이에 대한 보완책이 필요하다고 여겨진다. 두 번째 방법에서는 Registration-Owner 헤더를 이용하여, S-CSCF가 슬레이브 단말이 IMS에 등록하려 할 때마다 NOTIFY를 통해 마스터 단말이 그 사실을 알도록 하였다. 슬레이브 단말이 마스터 단말에게 인증을 요청할 때, 마스터 단말은 그와 관련된 NOTIFY를 사전에 수신했는가를 검증함으로써, 이 인증 요청이 적법인지를 확인할 수 있다.

IV. 마스터 단말과 슬레이브 단말 간 인증정보 교환

그림 4는 마스터 단말과 슬레이브 단말의 기능적인 구조를 설명한다. 마스터 단말에는 ISIM이 존재하고, IMS UE는 ISIM을 통해 IMS에 등록할 수 있다. 슬레이브 단말에는 ISIM이 존재하지 않는다. 슬레이브 단

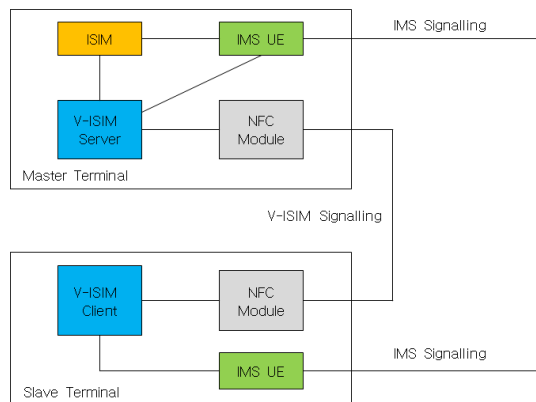


그림 4. 마스터/슬레이브 단말의 기능 구조
Fig. 4. Functional Architecture of Master and Slave Terminal

말은 마스터 단말에 있는 ISIM을 마치 내 것처럼 사용할 수 있도록 하는 기능인 가상의 ISIM(V-ISIM Client)을 구비한다. 슬레이브 단말에 있는 IMS UE는 가상의 ISIM으로부터 IMS 등록에 필요한 정보를 얻고 인증을 수행한다. 마스터 단말은 슬레이브 단말이 요청하는 ISIM 관련 정보를 처리하기 위해 V-ISIM 서버 기능을 가지고 있다. V-ISIM 서버와 클라이언트는 NFC Peer to Peer 모드를 통해 통신하기 때문에 NFC 모듈과 연동된다. V-ISIM 서버와 V-ISIM 클라이언트와의 NFC를 이용한 통신은 SNEP(Simple NDEF Exchange Protocol) 프로토콜¹⁸⁾을 사용하는데, 이는 기본적으로 V-ISIM 서버와 클라이언트가 제공하는 기능에 대한 NFC 태그를 정의함으로써 가능하다. NFC 태그의 이름은 기능 이름과 유사한 형태로 정의한다. 예를 들어, "ACTIVATE"라는 기능 호출 위해서는 "ACTIVATE" 태그를 읽으면 된다. SNEP에 따라 서버가 클라이언트의 기능을 호출하기 위해서 GET 명령을 이용하여 해당 기능과 매핑되는 태그 이름을 읽고, 파라미터 전달을 위해서는 PUT 명령을 사용한다.

표 2는 V-ISIM 서버 및 Client의 기능을 보여준다. 사용자는 슬레이브 단말을 이용하기 위해 마스터 단말을 슬레이브 단말에 가까이 가져갈 수 있다. 이러한 행동은 V-ISIM 클라이언트의 ACTIVATE(c1) 기능 호출로 연결된다. 이에 따라 슬레이브 단말의 IMS UE는 IMS 등록에 필요한 정보를 얻기 위해서 슬레이브 단말 내의 가상 ISIM 기능(V-ISIM Client)을 호출하게 된다. IMS UE는 IMPI, IMPU, 홈 네트워크 도메인 이름 및 P-CSCF 주소를 획득하기 위해 V-ISIM Client의 상응되는 기능(c2~c5)을 호출하게 되는데, 이 명령은 NFC 통신을 통해 V-ISIM 서버의 대응되

는 기능의 호출로 연결된다(s1~s4). V-SIM 서버가 s1에서 s4까지의 기능에 대한 호출을 받으면 ISIM에서 해당 정보를 얻어 V-ISIM 클라이언트로 전송한다. 그림 5는 가상 V-ISIM 클라이언트와 서버간 전형적인 메시지 흐름을 보여준다.

슬레이브 단말이 IMS에 등록을 하기 위해서는 Registration-Owner 헤더가 REGISTER 메시지에 포함되어야 한다. 슬레이브 단말의 IMS UE는 V-SIM Client의 ISSUE_OWNER_HEADER(c6) 기능을 호출하고 이 호출은 V-ISIM Server의 동일한 기능으로 전달되어 Registration-Owner 헤더 값을 획득할 수 있다. V-ISIM 서버는 ISSUE_OWNER_HEADER가 호출되면 마스터 단말 내의 IMS UE의 GRUU 값을 획득하여 Registration-Owner 헤더 값을 생성하고 이를 클라이언트로 전송한다.

IMS UE가 처음으로 S-CSCF에 등록을 시도하게 되면 401 Unauthorized를 수신하게 되는데, Authorization 헤더에 nonce 값이 포함되어 있다. 이 nonce 값을 이용하여 응답 메시지에 포함할 Authorization 헤더의 response 값을 계산하여야 하는데, 이때 AUTHENTICATE 기능(c7)을 호출함으로써 계산할 수 있다. V-ISIM 서버가 클라이언트로부터 AUTHENTICATE 기능을 호출 받으면, 파라미터로 받은 nonce 값과 ISIM내의 룬텀 비밀 키로부터 유도한 키를 사용하여 response에 실릴 값을 생성하고 이를 클라이언트에 전달한다. V-ISIM 서버의 VERIFY_OWNER_HEADER(s8) 기능은 마스터 단말 내의 IMS UE가 슬레이브 단말이 등록을 요청하고 있다는 사실을 알리는 NOTIFY 메시지를 수신했을 때, 이를 V-ISIM 서버에 알리기 위해 호출하는 기능으로서 V-ISIM 서버가 V-ISIM 클라이언트의 AUTHENTICATE 기능 호출을 받았을 때 그 자격의 적법성을 판단하는 상태를 저장하기 위한 용도로 사용된다. 즉 마스터 단말로부터 Registration_Owner 헤더를 발급받은 슬레이브 단말에 대해서만 인증정보를

표 2. 가상 ISIM 제공 API
Table 2. API list provided by Virtual ISIM

V-ISIM Client Function	V-ISIM Server Function
c1) ACTIVATE	s1) Read IMPI
c2) Read IMPI	s2) Read IMPU
c3) Read IMPU	s3) Read Home Network Domain Name
c4) Read Home Network Domain Name	s4) Read P-CSCF Address
c5) Read P-CSCF Address	s5) Read GRUU
c6) ISSUE_OWNER_HEADER	s6) ISSUE_OWNER_HEADER
c7) AUTHENTICATE	s7) AUTHENTICATE
	s8) VERIFY_OWNER_HEADER

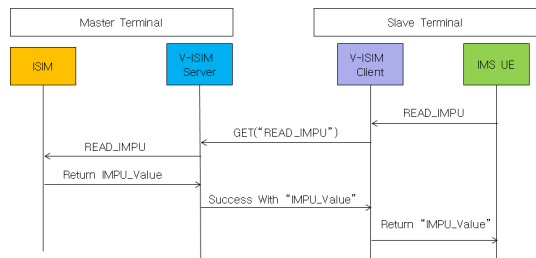


그림 5. 가상 ISIM 메시지 흐름도
Fig. 5. Message Flows for Virtual ISIM

생성하기 위해서이다.

V. IUT 적용 예

우리는 앞서 사용자가 여러 개의 단말을 사용하기 위한 사전 조건으로서 공용 단말을 효과적이고 안전한 방법으로 IMS에 등록하는 방법에 대하여 알아보았다. 이 장에서는 사용자가 여러 개의 단말을 이용하는 사례 중 대표적인 사례라고 할 수 있는 IUT에 이를 적용해 보고자 한다. IMS의 IUT는 NGN의 유비쿼터스 네트워크를 지원하는 대표적인 기술로서, 하나의 단말에서 진행 중인 세션을 다른 단말로 이동하는 것이 가능하도록 한다. 이 때 세션을 이동할 단말을 찾는 절차가 필요한데, 현재의 IMS 규격에서는 단말 내에 대상 단말이 미리 정적으로 설정되어 있다고 여기거나, 등록 이벤트 패키지를 통해 대상 단말을 확인하는 방법을 제시하고 있다. 이는 다양한 단말을 동적으로 발견하면서 사용할 수 있는 유비쿼터스 환경의 요구사항을 만족시킬 수 없을 것이다. 본 논문에서는 사용자가 이동하면서 발견하는 단말을 IMS에 일시적으로 등록시켜서 사용할 수 있기 때문에, 이러한 제약을 극복하는데 상당 부분 기여한다고 할 수 있다. 그림 6은 본 논문이 제시한 IMS의 단말의 등록 방법이 결합된 IUT 절차를 도시한다.

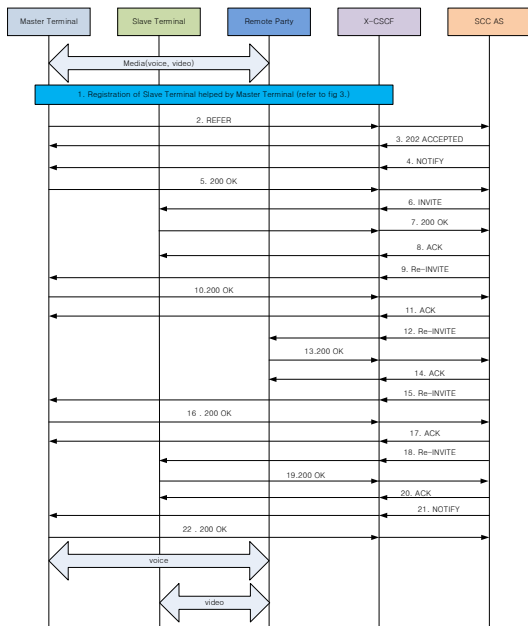


그림 6. IUT 메시지 흐름도
Fig. 6. Message Flows for IUT

단 대국(Remote Party)과 마스터 단말 간에 멀티미디어 호가 이미 연결되어 있다는 가정을 한다. :

1. 마스터 단말이 슬레이브 단말의 IMS 등록 절차가 시작되도록 유도한다. 마스터 단말은 슬레이브 단말이 IMS에 등록 완료되면 그 상태를 NOTIFY 명령어를 통해 알 수 있다(그림 3 참조).
2. 마스터 단말이 비디오를 슬레이브 단말로 옮기는 요청을 REFER 명령어를 사용하여 SCC AS에 전송한다. 이때 REFER 명령어에는 미디어를 이동할 대상 UE(슬레이브 단말) 및 이동할 미디어 정보가 포함된다.
3. SCC AS는 REFER에 대한 응답을 마스터 단말에게 전송한다.
- 4-5. SIP REFER 요청 처리 결과 이벤트에 대한 서브스크립션이 묵시적으로 됐음을 알린다. 세션 이동 결과를 나중에 마스터 단말에게 알려주기 위함이다.
6. SCC AS가 대국과 슬레이브 단말과의 비디오 세션 연결을 진행 위하여, 대국의 미디어 정보를 포함한 INVITE을 슬레이브 단말에게 전송한다. 이때 오디오 세션은 연결하지 않을 것과 비디오 전송은 대기 상태에 있도록 요청한다.
7. 슬레이브 단말이 6에 대한 응답을 전송한다. 응답 메시지 속에는 슬레이브 단말의 미디어 정보가 포함된다.
8. SCC AS가 슬레이브 단말에 ACK 명령어를 전송한다.
- 9-11. SCC AS가 마스터 단말이 비디오 전송을 일시 중단하도록 요청한다.
12. SCC AS는 SIP re-INVITE 명령어를 대국에 전송한다. 이 명령어에는 마스터 단말의 오디오 정보 및 슬레이브 단말의 비디오 정보가 포함된다.
13. 대국은 12에 대한 응답에 자신의 미디어 정보를 포함하여 SCC AS에 전송한다.
14. SCC AS가 대국에 ACK 명령어를 전송한다.
- 15-17. SCC AS가 마스터 단말에게 re-INVITE 명령어를 전송하여, 마스터 단말로부터 비디오를 제거하는 절차를 수행한다.
- 18-20. SCC AS가 슬레이브 단말에게 re-INVITE 명령어를 전송하여, 슬레이브 단말이 비디오 전송을 시작할 수 있도록 한다.
- 21-22. SCC AS가 미디어 이동이 성공적으로 완료되었음을 알리는 NOTIFY 명령어를 마스터 단말

에 전송한다.

VI. 성능 분석

6.1 IMS 등록 시뮬레이션

본 논문이 제시하는 마스터 단말의 정보를 활용한 슬레이브 단말의 IMS 등록 방법에 대한 실현 가능성을 확인하기 위한 시뮬레이션을 수행하였다. 시뮬레이션 환경은 그림 7과 같이 구성하였다.

Master Terminal과 Slave Terminal은 하나의 자바 어플리케이션으로 구현하였으며, 내부 모듈로서 그림 7과 같은 블록들을 가지도록 하였다. 내부 블록간의 통신은 같은 VM내의 Method 호출로 이루어진다. ISIM 블록은 표 1에 정리된 것과 같은 정보를 저장하도록 구현하였고, V-SIM Server 블록과 V-ISIM Client 블록은 표 2에 정의된 기능을 인터페이스로서 제공하도록 구현하였다. NFC 모듈 블록은 NFC 통신을 통해 NFC tag를 읽고 쓰는 기능을 시뮬레이션하기 위한 것으로서 read와 readAndWrite를 API로서 제공하고, NFC 모듈간 통신은 RMI(Remote Method Call)을 이용하여 시뮬레이션 하였다. read는 SNEP 프로코콜의 get에 해당하고, readAndWrite는 파라미터 전달을 위해 SNEP put을 한 후, 그 결과를 SNEP get을 통해 얻어오는 것을 하나의 API로 구현한 것이다. IMS UE 블록은 IMS 등록 시그널링을 시뮬레이션 하기 위하여 기본적인 SIP UA(User Agent) 기능을 구현하였고, 표준 SIP 시그널링을 통해 S-CSCF에 등록을 수행하도록 하였다. S-CSCF를 시뮬레이션하기 위해 asterisk 서버^[20]를 사용하였다. 마스터 단말, 슬레이브 단말 및 asterisk 서버는 각각 2.27 Ghz 8 개 코어로 구성된 CPU를 가진 리눅스 시스템에서 구동하였으며, 100 mbps Ethernet을 통해 같은 서브넷에 구성하였다. 마스터 단말에 대한 등록을 처리할 수 있도록 asterisk 서버에 마스터 단말에 대한 가입 정보를 설정하였다. 그림 8은 시뮬레이션에 의해 마스터 단말

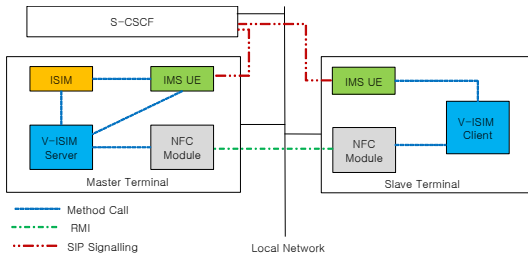


그림 7. 시뮬레이션 환경
Fig. 7. Simulation Environment

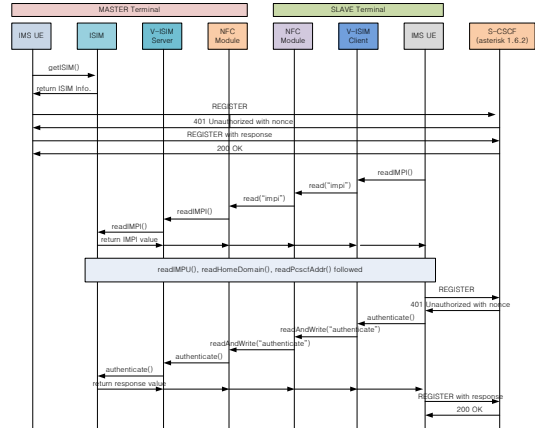


그림 8. IMS 등록 시뮬레이션
Fig. 8. Registration by Simulation

과 슬레이브 단말이 본 논문이 제안한 방법에 따라 성공적으로 등록되는 과정을 도시한다. 메시지 흐름에 대한 설명은 3장과 4장에서 다루어졌으므로 생략한다. 50회 반복 실험 결과 슬레이브 단말의 등록완료에 걸리는 시간은 평균 666ms 이었다.

6.2 IUT 성능 분석

본 논문은 새로운 IUT 방식을 제안하지는 않는다. 본 논문은 사용자와 근접해 있는 단말을 동적으로 IMS에 등록시킴으로서 NGN에서의 서비스 연속성 제공을 보다 효과적으로 할 수 있다는 점을 다루고 있다. 효과적이라는 것은 두 가지의 측면을 포함하고 있다. 첫 번째는 이동할 단말에 대한 사전 정보가 없이도 세션 이동을 할 수 있다는 점이고, 두 번째는 세션 이동을 시작하는 것이 최소한의 사용자 개입을 필요로 하기 때문에 사용자의 서비스 이용 경험을 향상시킬 수 있다는 점이다. 이는 두 단말 간 NFC 통신을 통해 세션 이동을 시작할 수 있음에서 비롯된다. IUT의 성능은 세션 이동에 걸리는 Total Transfer Latency(세션 이동에 걸리는 총 시간)와 세션 이동 중 미디어가 끊기는 시간(이동 중인 미디어를 어느 단말에서도 보거나 들을 수 없는 시간)을 분석함으로써 평가할 수 있다. 그러나 본 논문이 IUT의 성능 개선을 다루고 있는 것이 아니므로 전술한 평가지표를 직접 분석하기 보다는 본 논문에서 제안한 NFC를 이용한 등록방법이 기존 IUT 성능에 얼마나 영향을 끼치는가를 평가하고자 한다.

순수한 IUT 절차를 처리하는데 걸리는 Total Transfer Latency인 IUT_{net} 은 아래 수식처럼 IUT를 수행할 때 전송되는 개별 시그널링의 전송지연의 합으

로 표현할 수 있다. SIG_i 는 IUT를 수행할 때 사용되는 개별적 시그널링 메시지의 노드와 노드간 전송 지연을 의미한다. 보다 정교한 Total Transfer Latency에 대한 값을 구하기 위해서는 전송구간의 속도, 각 노드의 처리 속도, 시그널링 메시지의 크기, 망 부하 상태 다양한 요소가 고려되어야 하지만, 본 논문에서는 이를 고려하지 않는다.

$$IUT_{net} = \sum_{i=1}^n SIG_i \quad (1)$$

시그널링을 수행하는 노드 및 시그널링 절차는 그림 6을 따른다. SIG_i 는 시그널링 구간별로 다음과 같이 정의한다.

SIG_{ue} : 단말과 CSCF와의 전송 지연, 단말에는 마스터 단말, 슬레이브 단말, 대국이 포함됨

SIG_{core} : CSCF와 SCC AS와의 전송지연

그림 6의 시그널링 절차에 따른 IUT_{net} 은 아래와 같이 구할 수 있다.

$$IUT_{net} = 21SIG_{ue} + 21SIG_{core} \quad (2)$$

본 논문에서는 마스터 단말과 슬레이브 단말간 NFC 통신을 시작함으로써 IUT 절차가 시작되도록 하였다. 따라서 사용자가 체험하는 지연에 NFC 통신 및 슬레이브 단말의 등록 시그널링에 의한 지연을 포함시킬 필요성이 있다. 사용자가 체험하는 지연을 다음과 같이 IUT_p 로 정의한다. IUT_p 는 그림 3에 따른 절차를 이용한다.

$$IUT_p = NFC_c + SLAVE_{reg} + IUT_{net} \quad (3)$$

NFC 통신으로 인한 지연 NFC_c 는 SNEP을 이용하여 마스터 단말과 슬레이브 단말간 데이터 통신에 소요되는 시간으로 초기 연결 설정 시간과 데이터 전송시의 전송지연의 합으로 구할 수 있다. 여기서 전송지연은 RTT(Round Trip Delay)로서 정의된다. 그림 3에 따른 절차에 따르면 “ACTIVATE”, “Read IMPI”, “Read IMPU”, “Read Home Network Domain Name”, “Read P-CSCF Address”, “AUTHENTICATE” 라는 기능 호출이 이루어지므로, 총 6번의 데이터 전송이 필요하다. NFC는 초기 설정 시간을 100ms 이하가 될 것을 요구하고 있으며, 최대 424 kbit/s 전송 속도를 가질 수 있다. [21]에 의하면 NFC의 초기 설정 시간은 대략 59ms가 소요된다. 실

제 사용자 데이터의 전송속도를 의미하는 유효 전송속도는 최대 전송속도에 비해 많이 떨어지는 것으로 나타나고 있으며 사용하는 장비나 실험 환경에 따라 수 kbps에서 수십 kbps의 속도를 가진다고 말할 수 있다^[21-24]. 본 논문에서는 이러한 데이터를 참고하여 초기 설정 시간은 50ms, 사용자 데이터 전송 속도는 15kbps로 가정한다. 데이터 전송크기는 실제 ISIM에 저장된 정보에 따라 약간 차이가 있을 수 있으나 20bytes의 크기를 가진다고 가정한다. 이러한 가정에 NFC_c 의 값은 아래 수식에 의해 구하여 질수 있고, 그 값은 188 ms이다.

$$NFC_c = 60ms + 6 \times 2 \times \frac{20 \times 8}{15} ms \quad (4)$$

슬레이브 단말의 IMS 등록에 필요한 전송 지연 $SLAVE_{reg}$ 는 $8 \times SIG_{ue}$ 로 계산될 수 있다. 그림 9는 SIG_{core} 값에 따른 IUT_{net} 과 IUT_p 의 값을 보여준다. 일반적으로 액세스 망의 속도는 코어망의 속도에 비해 떨어지기 때문에, SIG_{ue} 는 SIG_{core} 보다 2배의 값을 가지는 것으로 추정하였다. IPTV에서의 서비스 경험 지표로 활용되는 채널 변경 시간(Channel Zapping Time)에서 사용자가 감내할 만한 최소의 값을 2초로 보는 것에 대비하여 본다면 코어 망 요소에서의 시그널링 지연이 30ms 이하가 되어야 어느 정도의 사용자 체감 성능을 발휘할 수 있다. 그림 10은 IUT_{net} 대비 IUT_p 의 오버헤드를 도시한다. 코어 망 요소의 시그널링 지연이 커질수록 NFC 통신과 슬레이브 단말의 등록으로 인한 영향이 상당히 작아지는 것을 알 수 있다.

IUT_{net} 은 순수하게 IUT를 진행할 때 소요되는 지연을 의미하고, 사용자가 IUT를 지시한 행위 자체의 시간은 포함되지 않는다. 그러나 실제 IUT를 하기 위해서는 사용자가 대상 단말을 찾고, 그 대상 단말로 세

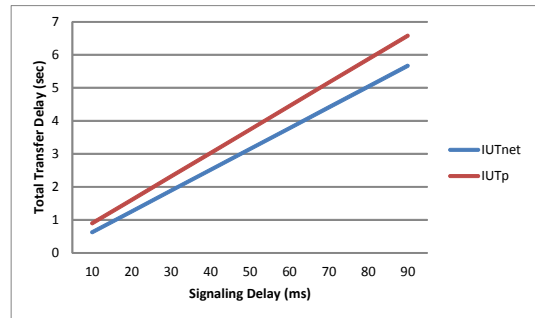


그림 9. 세션 이동 지연 비교
Fig. 9. Total Transfer Delay Comparison

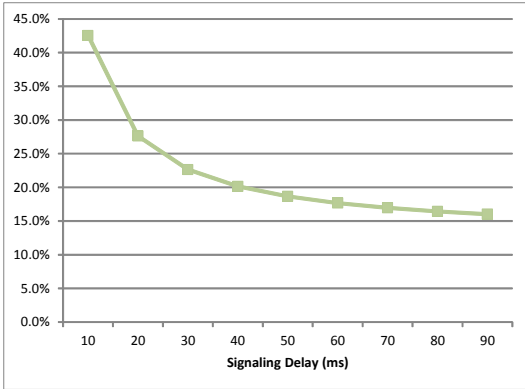


그림 10. NFC 통신 및 IMS 등록 오버헤드
Fig. 10. Overhead

션을 이동하라는 지시를 내려야만 한다. 이러한 요소는 사람이 개입하는 요소로서 객관적인 값으로 수치화하기는 힘들 것이다. 그러나 일반적인 사용자라면 이러한 개입에 소요되는 시간이 수 초가 될 것이라 주장해도 무리는 없을 것이다. 본 논문에서 의하면 사용자는 아주 간편한 방법으로 세션 이동을 지시할 수 있으며, 오버헤드 또한 크지 않기 때문에 IMS 기반의 IUT에서의 사용자 경험을 향상시킬 수 있다고 말할 수 있다.

VII. 결 론

사용자가 여러 개의 단말을 사용할 수 있는 환경을 지원하는 것은 NGN의 필수적인 요소이다. 특히 사용자가 이동하면서 동적으로 발견하는 단말을 통해 끊임없는 서비스를 사용할 수 있도록 하기 위해서는 발견된 단말이 IMS에 등록이 되어야 한다. 한편, 사용자가 주로 사용하는 단말은 IMS 가입정보가 저장되어 있다. 만약 이 IMS 가입정보를 이용하여 다른 단말을 IMS에 등록시킬 수 있다면 동적으로 발견한 단말을 통해 끊임없는 서비스를 받는 것이 가능할 것이다. 본 논문에서는 마스터 단말과 슬레이브 단말을 정의하고 마스터 단말의 IMS 가입정보를 슬레이브 단말로 전송하여 슬레이브 단말을 IMS에 등록시키는 새로운 IMS 등록 방법을 제시하였다. 사용자가 발견하는 단말은 대부분 물리적으로 가까운 곳에 있을 것이라는 가정 하에 가입정보의 이동은 NFC 통신 채널을 사용하였다. 사용자가 여러 단말을 이용할 때의 대표적으로 이용될 수 있는 서비스는 IUT이다. 따라서 본 논문에서는 NFC를 이용하여 단말을 IMS에 등록시키고 이를 IUT에 적용하는 방법에 대하여 논하였다. ISIM에 저장된 IMS 가입자 정보는 민감한 정보이다. 만약

이 정보가 그대로 슬레이브 단말에 전달된다면 슬레이브 단말이 이 정보를 유용할 가능성을 배제할 수 없다. 따라서 본 논문에서는 슬레이브 단말이 마스터 단말로부터 받은 가입정보를 이용하여 허가 없이 IMS에 등록하는 것을 방지하는 기법을 소개하고 있다.

앞으로의 연구과제는 보안을 향상시키는 기법을 연구하는 것이다. 본 논문에서 의하면 ISIM 정보 중 가입인증에서 있어서 가장 중요한 정보인 롱텀 비밀 키는 슬레이브 단말로 전송되지 않지만 IMPI 정보는 슬레이브 단말로 전송이 된다. 보다 안전하기 위해서는 IMPI 정보도 숨길 필요성이 있다.

References

- [1] H. Shulzrinne and E. Wedlund, "Application-layer mobility using SIP," *ACM Mob. Comput. Commun. Rev.*, vol. 4, no. 3, Jul. 2000.
- [2] M.-X. Chel, et al., "SSIP: Split a SIP session over multiple devices," *Comput. Standard & Interfaces* 29, pp. 531-545, 2007.
- [3] R. Shacham, et al., "The virtual device: Expanding wireless communication services through service discovery and session mobility," *Netw. Commun.*, vol. 4, pp. 73-81, Aug. 2005.
- [4] R. Shacham, et al., "Ubiquitous device personalization and use: The next generation of ip multimedia communications," *ACM Trans. Multimedia Comput., Commun. Appl.*, vol. 3, no. 2, Dec. 2007.
- [5] M. A. A. Mohamed, "Strengths and weaknesses of near field communication (NFC) technology," *Global J. Comput. Sci. Technol.*, vol. 12, no. 3, Mar. 2011.
- [6] J. Yim, H. Bae, and S. Kim, "Supporting service continuity in ubiquitous network environment with IMS extension," *J. KICS*, vol. 37, no. 12, pp. 1148-1159, Dec. 2012.
- [7] Z. Vassilis, B. Petros, and S. Christos, "NFC-triggered IMS flow mobility across different devices," in *Proc. PETRA '13*, no. 12, May 2013.
- [8] IETF, *Sip: Session initiation protocol*, IETF RFC 3261, Jun. 2002.
- [9] IETF, *Best current practices for third party*

call control (3pcc) in the session initiation Protocol (SIP), IETF RFC 3725, 2004.

[10] IETF, *The session initiation protocol (SIP) refer method*, IETF RFC 3515, 2003.

[11] IETF, *A session initiation protocol (SIP) event package for registrations*, IETF RFC 3680, Mar. 2004.

[12] IETF, *Registration event package extension for session initiation protocol (SIP) globally routable user agent URIs (GRUUs)*, IETF RFC 5628, Oct. 2009.

[13] 3GPP, *IP multimedia subsystem (IMS) service continuity; Stage 2*, 3GPP TS 23.237 v11.10.0, Rel.11, Jun.2014.

[14] 3GPP, *IP multimedia (IM) core network (CN) subsystem IP multimedia subsystem (IMS) Inter-UE transfer; Stage 3*, 3GPP TS 24.337 v11.4.0, Rel.11, Mar. 2013.

[15] 3GPP, *IP multimedia subsystem (IMS); Stage 2*, 3GPP TS 23.228 V9.4.0, Rel.9. 2010.

[16] 3GPP, *Characteristics of the IP multimedia services identity module (ISIM) application*, 3GPP TS 31.103 v11.2.0, Rel.11, Mar. 2011.

[17] 3GPP, *Access security for IP-based services*, 3GPP TS 33.203 v11.2.0, Rel.11, Jun. 2012.

[18] NFC Forum, *SIMPLE NDEF exchange protocol*, Technical Specification, NFCForum-TS-SNEP 1.0, 2011.

[19] Wi-Fi Alliance, *Wi-Fi CERTIFIED Miracast*, Retrieved Nov., 30, 2014, <http://www.wi-fi.org>.

[20] Asterisk, <http://www.asterisk.org>

[21] N. Anders, M. Miquel, and S. Hans-Peter, "Service migration protocol for NFC links," *Networked Services and Appl. Eng., Control and Management, LNCS*, vol. 6164, pp. 41-50, 2010.

[22] O. Geoffrey, V. D. B. Sam, and G. Jean-Pierre, "Measuring the NFC peer-to-peer data rate," in *Proc. ECUMICT 2014*, vol. 302, pp. 109-122, 2014.

[23] U. Akshay, S. N. Nambi, T. V. Prabhakar, H. S. Jamadagni, G. Kishan, B. K. Pramod, C. M. Rakesh, and N. R. Sanjay, "Near field communication - applications and performance studies," *Wirel. Netw. and Computational*

Intell. Commun. in Comput. Inf. Sci., vol. 292, pp. 1-10, 2012.

[24] M., Erick and W. Josh, *NFC active and passive peer-to-peer communication using the TRF7970A*, Application Report SLOA192, TEXAS INSTRUMENTS, 2014.

임 중 철 (Jong-choul Yim)



2000년 2월 : 서울시립대학교 전 산통계학과 석사
 2000년 10월~현재 : 한국전자통신연구원 근무
 2011년 3월~현재 : 충남대학교 컴퓨터공학과 박사과정
 <관심분야> IoT, 미래 인터넷, 근접 서비스

김 상 하 (Sang-ha Kim)



1980년 : 서울대학교 학사
 1984년 : University of Houston 석사
 1989년 : University of Houston 박사
 1992년~현재 : 충남대학교 컴퓨터공학과 교수

<관심분야> Internet Routing, Wireless Sensor Networks, MANET, 4G, Mobility, Multicast

금 창 섭 (Chang-sup Keum)



1992년 2월 : 서울시립대학교 전 산통계학과 석사
 2005년 8월 : 카네기멜론 대학 소프트웨어 공학 석사
 2013년 8월 : 한국과학기술원 공학박사

1994년 2월~현재 : 한국전자통신연구원 유무선융합서비스플랫폼연구실 실장
 <관심분야> 5G 모바일 엣지 클라우드, 서비스 플랫폼, 소프트웨어 아키텍처