# 모바일 서비스 네트워크의 구조적 분석과 보안 취약성

김장환*


## 요 약

최근 국내외적으로 모바일 서비스 산업은 매우 빠른 속도로 변화하고 성장해 나가고 있다. 본 논문에서는, 모바일 서비스 산업에서 일어나고 있는 변화와 미래 범세계적 사회에서의 발생 가능한 모바일 서비스 환경에서의 구조적 보안 취약성을 찾기 위해 노력하였다. 최근 정보통신기술의 급속한 발달로 모바일 인터넷을 이용한 모바일 전자상거래 사용자가 폭발적으로 증가하고, 유선에서 유/무선 통합 환경으로 변화함에 따라, 보안상의 많은 문제점이 노출되고 있다. 특히 모바일 전자상거래에서는 무선 환경의 제한적 특징에 따라 경량화된 보안기술, 종단간 보안 기술 및 프라이버시 보안 등에 관한 연구가 활발하게 진행되고 있다. 또한 IoT 서비스의 확산에 따른 모바일 네트워크에서의 IoT 서비스 연동이 요구되고 있다. 모바일 보안 프로토콜은 무선과 유선을 연계하는 게이트웨이(Gateway)에서 전달되는 데이터의 모든 내용이 누출되는 보안상의 취약점이 있어 종단간 보안도 제공하지 못하는 단점이 있다. 이에 본 논문에서는 모바일 서비스 네트워크를 구성하고 있는 제반 요소의 구조를 살펴본 후, 이로부터 유추할 수 있는 보안 취약성을 제시해 보고자 한다.


# The Structural Analysis and Implications of Security Vulnerabilities In Mobile Srevice Network

Jang-Hwan Kim*


## ABSTRACT

Recently mobile service industry has grown very rapidly. In this paper, We investigated the changes in mobile service network as well as security vulnerabilities of network in future 5G mobile service network, too. Recently, there are rapid developement of information and communication and rapid growth of mobile e-business users. Therefore We try to solve security problem on the internet environment which charges from wire internet to wireless internet or wire/wireless internet. Since the wireless mobile environment is limited, researches such as small size, end-to-end and privacy security are performed by many people. In addition, there is a need of internetworking between mobile and IoT services. Wireless Application Protocol has weakness of leaking out information from Gateway which connected wire and wireless communication. As such, We investigate the structure of mobile service network in order to gain security vulnerabilities and insights in this paper.


**Key words : Mobile Service Network, Security, Vulnerabilities**

접수일(2016년 8월 26일), 수정일(1차: 2016년 9월 22일), 게재확정일(2016년 9월 28일)

* 성결대학교 공과대학 미디어소프트웨어학부

# 1. 서 론

모바일 서비스는 매우 복잡한 장비들 간의 연동으로 이루어지고 있다. 잘 알려져 있는 인터넷 프로토콜(Protocol)인 TCP/IP 와는 전혀 다른 공통선 신호방식(CCS7:Common Channel Signalling No.7) 프로토콜로 음성 서비스가 제공되고 있으며, 모바일 3세대 서비스 이후, 모바일 단말에서의 풀브라우징 서비스를 제공하기 위하여, 인터넷 데이터 처리를 위한 전용 장비들이 모바일 망에 추가되어져 운용되고 있다. 또한 2007년 아이폰 출시와 함께 급속히 확산되고 있는 스마트폰은 다양한 부가 기능들을 탑재하고 있어서, 이들과 결합된 새로운 모바일 서비스 산업 생태계에 대한 관심이 지속되고 있다[1],[2].

그러나 이러한 모바일 서비스 사용의 지속적인 확대와 더불어 필연적으로 발생하게 될, 모바일 환경에서의 정보의 불법유출이 발생할 수 있는 구조적인 문제점을 모바일 음성망과 모바일 데이터망으로 세분화하여 자세히 살펴봄으로써 이로부터 유추할 수 있는 보안 취약성을 제시해 보고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 모바일 음성망의 구조와 보안 취약성을 살펴본다. 3장에서는 모바일 데이터망의 구조와 보안 취약성에 대해 기술하고, 마지막으로 4장에서는 결론과 향후 연구 방향에 대하여 기술한다.

# 2. 모바일 음성망의 구조

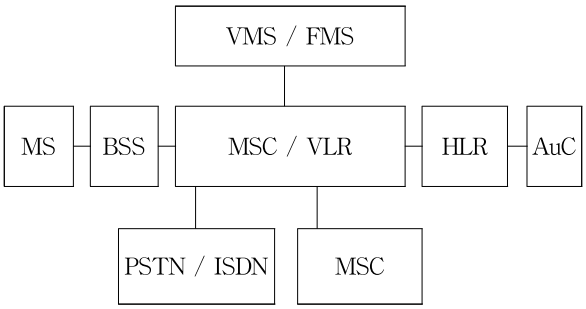
컴퓨터 네트워크(computer network)란 TCP/IP 등의 통신 규약에 의해 연동되는 환경이다. 이에 비해 모바일 서비스 네트워크는 다음 그림1과 같은 매우 다양한 네트워크 요소 시스템들을 연결하여 공통선 신호방식(CCS7:Common Channel Signalling No.7)프로토콜에 의하여 연동되는 복잡한 네트워크이다.

## 2.1 모바일 음성망의 통신 구조

### 2.1.1 모바일 음성망의 호 처리 구조

먼저 모바일 서비스 망의 구조를 이해하기 위하여, 호의 성립 과정과 위치 정보의 변경 과정의 두 가지 동작에 대하여 설명한다[3].

그림 1은 이동 통신 네트워크의 구성요소를 나타낸다. 그림에서 HLR 시스템은 MSC/VLR(Mobile Switching Center/ Visitor Location Register)과 공통선 신호방식에 의하여 연결되어 MSC/VLR로부터 가입자에 대한 위치 정보의 갱신 및 조회 요구 등에 대한 처리 기능을 제공하며, 가입자 정보 변경의 경우에는 이를 MSC/VLR로 통보하는 기능도 수행한다. 또한 MSC/VLR과 인증센터(AuC:Authentication Center)간의 메시지를 전달하는 기능도 포함하고, 경우에 따라서는 MSC/VLR을 통하여 VMS/FMS와 같은 부가 서비스 시스템과 연동하기도 하는 매우 복잡한 네트워크 요소 시스템이다.

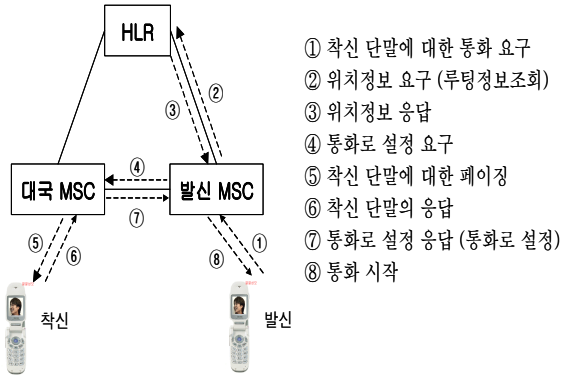



| | | | |
|---|---|---|---|
| MS | Mobile Station | FMS | Fax Mail System |
| BSS | Base Station System | HLR | Home Location Register |
| MSC | Mobile Switching Center | AuC | Authentication Center |
| VLR | Visitor Location Register | PSTN | Public Switched Telephony Network |
| VMS | Voice Mail System | ISDN | Integrated Service Digital Network |

(그림 1) 이동 통신 네트워크 요소 시스템

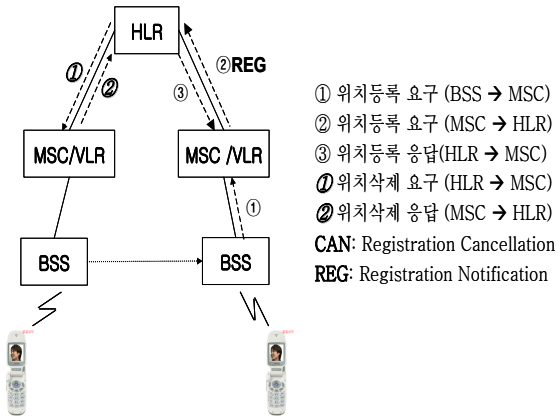
다음의 그림 2는 HLR 시스템을 포함하여 호가 성립되는 과정을 보여 준다. 가입자는 먼저 전화번호를 누름으로써 착신 단말에 대해 통화 요구를 한다. 이는 BSS를 거쳐 MSC에 전달되고, MSC에서는 루팅정보 조회라는 MAP(Mobile Application Part) 동작을 발생시켜 HLR 시스템에 위치 정보를 요구한다. 이 요구를 받은 HLR 시스템은 자신의 주기억장치 데이터베이스를 검색하여 해당 가입자의 위치 정보를 내려주고, MSC는 이 정보를 이용하여 대국 MSC에 호 설정을 요구한다. 다음으로 대국 MSC는 착신 단말에 대

하여 페이징(paging)을 시도하여 응답이 있으면 통화로가 설정되어 통화가 이루어지게 된다. 따라서 HLR 입장에서는 루팅정보조회라는 MAP 동작을 처리하여 호의 성립에 도움을 주는 역할을 한다.




(그림 2) 호의 성립 과정

다음의 그림 3은 가입자, 즉 단말의 이동에 따른 위치 정보의 변경 과정을 나타낸다. 그림과 같이 가입자가 이동하면 위치등록과 위치삭제의 두 가지 MAP 동작이 발생한다. 먼저 이동한 위치에서 위치등록 동작이 BSS를 거쳐 MSC/VLR에 전달된다. 위치등록 요구를 받은 MSC/VLR에서는 이를 HLR에 전달하며, 그 결과를 받아 자신의 데이터베이스에 해당 가입자 정보를 저장한다. 위치등록 요구를 받은 HLR 시스템은 해당 가입자의 위치 정보를 갱신하고, 위치가 변경된 경우에는 위치삭제 동작을 발생시킨다. 위치삭제 동작에 의하여 가입자가 존재하였던 이전 MSC/VLR에서는 그 정보가 삭제됨으로써 가입자의 이동이 완료된다. 따라서 HLR 시스템 입장에서는 위치등록 요구를 받아 이를 저장하고 위치가 변경되었으면 위치삭제를 사용하여 가입자의 위치를 변경하는 기능을 한다. 이렇게 변경된 새로운 위치는 다음의 호처리 과정에 사용된다.




(그림 3) 단말의 이동에 따른 위치 변경

### 2.1.2 모바일 음성망의 공통선 신호 방식 프로토콜

인터넷 패킷(packet) 통신 네트워크와는 대조적으로 모바일 전화통신 네트워크에는 음성 데이터 네트워크와 함께, 이를 제어하는 신호 네트워크가 존재한다. 전화 통신 네트워크는 컴퓨터 기술을 사용한 프로그램 축적 제어형 교환기를 사용하게 진화되어 왔고, 통신 네트워크도 디지털화가 추진되어, 전통적인 전화 서비스의 고도화에 추가하여 비전화 서비스의 제공도 가능하게 되었다. 공통선 신호방식은 이와같은 프로그램 축적 제어형 교환기로 구성된 디지털 통신 네트워크에 있어서, 교환기와 같은 제어 장치 간에 제어정보 전송 수단을 제공하는 것으로, 통신 네트워크가 제공하는 서비스의 고도화, 다양화에 없어서는 안되는 기술이다. 신호방식은 가입자선 신호방식, 국간 신호방식과 같이 적용구간에 대응하는 분류와 실현기술에 대응하는 분류가 있다. 공통선 신호방식은 후자의 실현기술을 표시하는 용어이다. 공통선 신호방식에 대조적인 용어로는 개별선 신호방식이란 것이 있다. 공통선 신호방식은 통화 회선과는 별도로 신호전송 전용 회선을 구성하여, 그 신호회선을 사용하여 수개의 통화 회선을 제어하는 신호를 전송하는 방식으로서, 디지털 기술이 발전함으로서 실용화가 가능하게 된 신호방식이다. 모바일 음성망 요소 장비들 간에는 공통선 신호방식의 신호망으로 연결되어 있어서, 모바일 데이터 망의 인터넷 패킷 통신 네트워크의 단일 회선

연결 방식과는 상이한 구조로 동작하게 되어 있다.

### 2.2 모바일 망의 위치등록기 구조와 보안 취약성 분석

이동 통신 망에서는 가입자의 위치가 지속적으로 변하므로 이에 대한 위치 정보(Location Information)의 관리가 필요하다. HLR 시스템은 이러한 가입자의 위치 정보 관리를 주요 기능으로 하여 현재 이동통신 서비스 분야에서 호처리 및 부가서비스 지원 등의 중요한 역할을 하고 있다. 주요 문제점으로는 현재의 국내 이동통신 서비스는 HLR과 VLR간에 교환되는 가입자 관련 정보들에 대해 효과적인 정보 보호 조치가 취해지지 않고 있다는 점이다.

현재의 국내 이동통신 서비스의 HLR DB Scheme의 릴레이션의 attribute로는 이동가입자의 고유한 식별 번호인 Mobile Identification Number, 이동국의 고유한 32-bit Electronic Serial Number인 Mobile Serial Number, 이동국의 활성/비활성 상태를 표시하는 CSS_Status를 포함한 총 49개 attribute의 ROAM_TBL, 3개 attribute의 PFX_TBL, 2개 attribute의 STLN_TBL, 5개 attribute의 MAIL_TBL로 구성되어져 있다[4],[5].

글로벌한 차세대 서비스로의 진화에 있어서 가장 큰 변화는 국가간 roaming과 multimedia 서비스 빈도의 증가이며, 이를 기반으로 하여 mobile commerce가 확산될 것으로 예상된다. 금전 거래에 있어서 가장 중요한 요구 사항은 보안 기능일 것이다. 이러한 기능 수행을 위해 현재의 HLR DB Scheme과 관련하여 변화되어야 할 최소한의 attribute는 다음과 같다. session key 설정 및 인증 protocol 수행을 위해서, 인증 algorithms 수행의 결과로 산출된 결과값, 산출된 session key, 사용된 random number 각각을 저장할 수 있는 attribute들이 추가되어져야 한다.

또한 HLR과 VLR간에 교환되는 가입자 관련 정보들에 대해 효과적인 정보 보호 조치가 취해지지 않고 있는 상태에서, HLR 시스템과 MSC/VLR시스템 간의 실제 망 연결 거리는 매우 원거리이면서 관리 사각지대로 방치된 상태여서, 의도적 공격자에 의한 물리적인 보안 취약성에 노출된 상태이다. HLR 시스템에 저장되는 가입자의 전화 번호는 일정한 규칙에 의하여 관리되는데 이는 HLR 시스템이 특정 지역을 중심으로 가입자를 수용하므로서 나타나는 규칙이다. 망을 관리하는 서비스 사업자는 특정한 범위의 국번을 각 지역별로 할당하게 되고, 이에 따라 해당지역의 HLR 시스템은 특정한 범위의 국번만을 수용하게 된다. 그리고 치국 계획에 따라 특정 국번의 가입자 번호가 어느 정도 사용되기 이전까지는 다른 국번을 사용하지 않는다. 따라서 특정 HLR 시스템에서 관리하는 국번의 수는 해당 시스템의 가입자 수용 능력에 따라 일정한 비율로 정해진다. 이러한 치국 계획의 특성에 의하여 가입자를 수용하는 HLR 시스템의 개수는 결정되는데, 글로벌하게 가장 성능이 좋은 HLR 시스템의 경우에, 한 HLR 시스템 당 최대 가입자 수가 100만명이내이므로, 매우 많은 HLR 시스템과 MSC/VLR 시스템이 매우 원거리에 떨어져 있는 상태로 케이블로 연결되어져 있어서, 관리상 소홀함을 악용한 외부 공격이 상대적으로 용이함으로 물리적으로도 보안 취약성에 노출된 상태이다. 또한 HLR 시스템과 MSC/VLR시스템 간에 교환되는 가입자 관련 정보들에 대해서는 별도의 정보 보호 조치가 취해지지 않고 있어서, 사실상 외부 공격자와 시스템 내부 공모자에게 무방비 상태로 노출되어져 있다.

## 3. 모바일 데이터망의 구조

모바일 망을 이용한 데이터 서비스의 경우는 단문 문자 서비스인 SMS(Short Message Service)로부터 시작 확산 사용되어 오다가, 점점 유선인터넷 수준의 데이터 서비스를 제공하기 위하여 별도의 데이터망 전용 장비와 프로토콜 개발이 이동통신 2,3,4세대를 통하여 지속적으로 전개되어져 왔다[6]. 또한 5세대 모바일 서비스에서 IoT(Internet of Things) 서비스와의 효과적인 연동 처리 방안이 추진되고 있다[7],[8],[9].

### 3.1 WAP을 이용한 데이터 서비스

#### 3.1.1 WAP

모바일 인터넷 구현을 위한 기술로는 WAP (Wirelesee Application Protocol)기술을 들 수 있다. WAP은 이동 네트워크와 유선 인터넷 망 사이에

WAP 게이트웨이를 두어 데이터를 처리하는 인터넷 이동성 지원 프로토콜이다. WAP은 통신 품질의 불안정으로 전송 속도가 느린 휴대 전화 네트워크의 특성을 고려, 게이트웨이 방식을 채용해서 단시간에 많은 정보를 전송할 수 있도록 하였다. WAP은 무선 네트워크에서 인터넷 서비스를 효율적으로 제공하기 위해 정의된 무선 인터넷 프로토콜로, 기존의 유선 인터넷 표준의 특징과 기능을 이용하여 무선 단말기에 인터넷 서비스를 제공하는 것이다.

### 3.1.2 WAP 게이트웨이

게이트웨이란 통신 네트워크에서 서로 다른 네트워크들을 연결시켜 주는 장비를 말한다. 인터넷 망은 TCP/IP 프로토콜로 동작되나, 이동전화의 네트워크는 TCP/IP 프로토콜과는 전혀 다른 CCS No.7 프로토콜로 동작되므로, 모바일 단말기 상에 인터넷 서버로부터 전송되어져 오는 정보를 제공하기 위해서는, 서로 다른 프로토콜로 동작되는 네트워크들을 연결시켜 주는 게이트웨이가 필요한다. WAP 게이트웨이는 TCP/IP 기반의 유선 인터넷 망과 무선 네트워크를 연결하여 주는 장비이다. WAP 게이트웨이는 WAP 프로토콜(WSP, WTP, WTLS, WDP)과 IP 기반의 패킷 네트워크 사이에서 데이터를 변환하는 중개자 역할을 수행한다[11].

## 3.2 모바일 데이터 서비스 구조의 보안 취약성 분석

유선인터넷에서 보안은 현재 표준으로 자리 잡은 TLS 프로토콜을 사용하여 이루어진다. 공개키와 개인키를 이용한 키 교환(Key Exchange)기법을 이용하여 클라이언트와 서버가 공유하는 세션키(Session key)를 안전하게 생성한 다음 이 세션키를 이용하여 클라이언트와 서버 사이의 모든 전송 데이터를 암호화/복호화한다. TLS에서 사용자와 서버 양쪽을 연결해주는 유선인터넷은 다음의 보안요소들을 충족시킨다. 우선, 로그인 과정을 통해 사용자의 당사자 여부를 판단하는 인증이 보장 받게 되며, 세션키를 알지 못하는 제3자는 클라이언트와 서버에서 암호화된 데이터의 내용을 알 수 없으므로 기밀성이 보장된다. 클라이언트에서 암호화된 데이터는 서버에 도착하는 동안 누군가에 의해 가로채어 질 수 있지만 데이터를 임의로 변화시키게 되면 데이터의 해쉬(Hash)값이 변하게 되므로 무결성이 보장된다. 인증을 받은 특정 사용자에 대해 적절한 권한 부여를 하여 인증을 최종적으로 수행한다.

모바일 망과 기존 유선인터넷과의 연동으로 이루어지는 모바일 데이터망 상황에서 무선망 상의 단말기에서부터 유선인터넷 상의 서버에 이르는 효율적인 종단간(End to End) 보안 서비스 제공은 계속해서 문제가 되고 있다. 특히 WAP과 같이 무선 망에서 별도의 프로토콜을 사용하는 경우 이 문제는 더욱 심각하다. 모바일 데이터망에서의 보안은 무선구간에서는 WTLS를 이용하고 유선구간에서는 기존 유선인터넷의 TLS/SSL을 그대로 적용하여 유선, 무선 각각에서 보안을 달성할 수 있도록 구성되어 있다. WAP에서의 보안 프로토콜인 WTLS는 SSL을 모델로 만들어지기 때문에 그 구조에는 큰 차이가 없다. 차이점은 WTLS에서 메시지 크기를 조금씩 줄인 것과 ECC 알고리즘의 수용, 작은 크기의 인증서 지원 등이다. 이 중 인증서는 기존의 표준인 X.509 인증서를 지원하며 추가로 WTLS 인증서, X9.68 인증서 형식을 지원한다. WTLS 인증서는 컴팩트한 사이즈의 인증서 형식으로 정의한 것으로 X.500 DN 대신 Identifier만을 사용함으로써 크기를 줄이고 있다. 하지만, 모바일 데이터망 보안에서의 문제점은 유무선 각 구간별 보안에서 발생하는 것이 아니라, 안전한 유무선 구간 쌍방을 연결하는 WAP 게이트웨이에서 발생하게 된다. 사용자 컨텐츠가 WAP 게이트웨이를 통과하는 동안에 프로토콜 변환 과정시 보안이 침해당할 우려가 있다.

# 4. 결 론

1990년 WWW의 확산, 2000년 Google등의 검색 엔진과 Cloud DBMS의 밀결합에 의한 고속 검색 서비스의 확산, 2010년 Mobile Internet의 확산, 2020년 IoT의 확산 등, ICT분야는 매 10년 주기로 매우 빠른 변혁이 일어나고 있다. 최근 정보통신기술의 급속한 발달로 모바일 인터넷을 이용한 전자상거래 사용자가 폭발적으로 증가되고 있다. 글로벌한 차세대 서비스로의 진화에 있어서 가장 큰 변화는 국가간 roaming과

multimedia 서비스 빈도의 증가이며, 이를 기반으로 하여 mobile commerce가 확산될 것으로 예상된다. 금전 거래에 있어서 가장 중요한 요구 사항은 보안 기능일 것이다. 지금까지 Mobile 네트워크에서의 해킹 사례가 유선 인터넷보다 적었던 것은, Mobile 네트워크가 상대적으로 계획된 폐쇄적 망이며, 유선인터넷의 통신 규약인 TCP/IP보다 Mobile 네트워크의 통신 규약인 공통선 신호방식 CCS7이 상대적으로 해커들에게 덜 알려져 있음에 기인하고 있다. 그러나 앞으로 글로벌한 국가간 roaming 환경의 확대와 유/무선 통합 환경으로의 진화에 따라, 여러 이질적인 네트워크들과의 연동 환경에서는 HLR 시스템과 MSC/VLR시스템 간에 교환되는 가입자 관련 정보들이 별도의 정보 보호 조치가 취해지지 않은 상태로, 사실상 외부 공격자와 시스템 내부 공모자에게 무방비 상태로 노출되어져 있다. 또한 모바일 데이터 망에 있어서 핵심적 역할을 수행하고 있는 게이트웨이는 무선 구간의 WTLS와 유선 구간의 TLS를 연결해 주기 위해서 사용자로부터 전달된 데이터를 해독하고 다시 암호화하여 Web Server로 전달하며, 반대로 Web Server로부터 전달된 데이터를 해독하고 이를 다시 암호화하여 사용자에게 전달한다. 이 과정에서 게이트웨이는 사용자와 서버사이의 전달되는 데이터의 모든 내용을 해독하므로 보안의 허점이 발생할 수 있다. 따라서 무선 애플리케이션 프로토콜에서는 "어느 정도 신뢰 있는 보안"을 제공하지만 완벽한 종단간 보안은 제공하지 못한다. 따라서 효율적인 종단간 보안 제공 방안이 필요하다. 향후 모바일 인터넷 보안기술의 발전은 유/무선 통합은 물론, IoT 게이트웨이까지 연동되는 새로운 환경으로 변화해 감에 따라 기존의 인터넷이나 무선통신에서의 보안 서비스와는 다른 새로운 패러다임에 대한 연구 및 개발이 시급한 상황이다. 그리고 무선통신 환경에서의 대역폭, 단말기 등의 제한을 고려한 인증서 프로파일, 암호 알고리즘, 키 크기, 인증서 취소 여부 확인 메커니즘 등의 효율적인 연구개발이 이루어져야 한다.

## 참 고 문 헌


[1] Wikipedia, Ecosystem, Retrieved Mar. 17, 2013, from http://ko.wikipedia.org/

[2] G. Gueguen and T. Isckia, “The borders of mobile handset ecosystems: is coopetition inevitable?,” *Telematics and Informatics*, vol. 28, pp. 5-11, Jan. 2011.

[3] J.H.Kim, “Performance enhancement architecture for HLR system based on distributed mobile embedded system,” *J. KICS*, vol. 29, no. 12B, pp. 1022-1036, Dec. 2004.

[4] S.Tabbane,Handbook of mobile radio networks,Artech House Publishers,2000.

[5] TIA/EIA, *IS-41(A)*, Initial Version. Jan. 1991.; IMT-2000 3GPP2-International Implementation of Wireless Telecommunication Systems Compliant with TIA/EIA-41 Revision A, Oct. 2002.

[6] J.H.Kim, “The Structural Analysis and Implications of Mobile Service Industry,” *J.KICS*,vol.38C,no.09,pp.733-739,September 2013.

[7] J.H.Kim and Seung Chang Park, “A Study about M2M Technology Policy and Nano-fusion Sensor SoC Functioning in the IHN(Intelligent Home Networking) Mode”, SKT Review, Vol.20 No.4, pp.541~555, August 2010.

[8] Seung Chang Park, The analysis of Big Data/IoT technology commerccialization strategy, Jinhanbook, August 2015.

[9] J.H.Kim and Seung Chang Park, “IoT Relationship Between Korea and the Philippines”,IJUNESST, Vol.9 No.7, July 2016.

[10] Tim Dierks and Christopher Allen, "The TLS Protocol Version 1.0" IETF RFC 2246, January 1999

[11] WAP Fourm, "Wireless Application Protocol Wireless Transport Layer Security Spectification version 18-FEB-2000", 2000

## [저 자 소 개]

**김 장 환 (Jang-HwanKim)**

1980년 서울대학교 경제학학사
1997년 한국과학기술원 전산학석사
2003년 충북대학교 전산학박사
1984년~1988년 쌍용정보통신 연구원
1988년~1993년 Qnix Data System 연구원
1993년~1998년 SK Telecom 중앙연구원 연구원
1998년~2005년 대덕대 교수
2005년~현재 성결대 공대 미디어소프트웨어학부 교수
2011년 9월~2012년 8월 University of California, Los Angeles / Visiting Professor

email : jhkim@sungkyul.ac.kr