USIM 기반 사용자 인증을 응용한 모바일 오피스 시스템의 안전성 향상 방안

지은화° 이상호
이화여자대학교 공과대학 컴퓨터공학과
jhee0411@ewhain.net, shlee@ewha.ac.kr

The Security Improvement of Mobile Office System through the USIM-based User Authentication

Eun-Wha Jhee° and Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

스마트폰 시장의 규모가 급속하게 확장됨에 따라 모바일에서 다양한 서비스가 제공되면서 기업의 측면에서는 스마트워크 환경에서의 모바일 오피스 시스템 도입 요구가 커지고 있다. 그러나 스마트폰의 이동적 개방성의 특성은 기업 정보의 접근 및 유출의 위험성을 갖고 있어 이에 대한 시스템 구성에서의 보안 및 안전성 확보가 필요하다. 본 논문에서는 USIM을 이용하여 모바일 오피스 사용의 정당한 권한이 있는 사용자임을 등록 및 인증 후 안전한 서비스 사용이 가능하도록 모바일 오피스 시스템을 설계하고 분석한다. 제안 시스템은 모바일 오피스의 시스템 구성 요소 간의 안전한 통신 상태를 보장함으로써 기업 정보의 사용에 있어 보안성을 효과적으로 제공한다.

1. 서론

스마트폰 보급의 급속한 확산은 모바일 시장의 비약적인 발전과 함께 스마트 기술산업의 확장을 이끌었다. 스마트폰은 일반폰과는 달리 연산 및 제어 기능이 가능한 CPU를 장착하여 개방적 범용 운영체제를 탑재한 단말기로서 다양한 환경에 적합한 서비스를 제공할 수 있다. 특히 많은 업무의 빠른 처리를 요하는 기업적 측면에서는 스마트폰을 통하여 시간과 장소의 제약 없이 인터넷에 연결하여 업무를 수행할 수 있는 스마트워크 환경의 구축 및 모바일 오피스 도입을 적극 추진하고 있다. 그러나 PC의 성능을 보유한 스마트폰은 기존 인터넷 접속을 통한 PC 대상의 다양한 보안 위협과 함께 무선 접속 환경에서의 개방성과 휴대성으로 인한 보안 위협 등 모바일 오피스에서의 새로운 보안 사고 위험을 안고 있다. 기업의 경우 사고 위험성에 관하여 금전적인 문제가 동반되기 때문에 보안에 대해 우려하는 바가 더욱 크다. 따라서 스마트폰을 통한 업무자 중심의 편리한 스마트워크 환경 조성에 앞서 모바일 오피스 사용시의 기업과 개인의 정보 유출 및 훼손 등의 문제를 고려한 보안 및 안전성 확보가 우선되어야 한다.

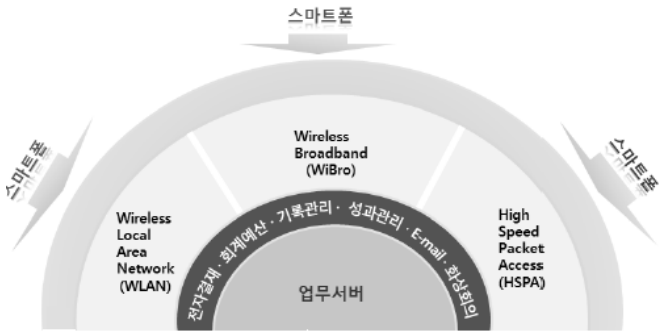
이에 본 논문에서는 USIM(Universal Subscriber Identity Module)을 이용하여 모바일 오피스 사용의 정당한 권한이 있는 사용자임을 등록 및 인증 후 안전한 서비스 사용이 가능하도록 모바일 오피스 시스템을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 스마트워크 환경의 모바일 오피스에 대해 살펴보고 선행 USIM 기반 사용자 인증 프로토콜을 분석한다. 3장에서는 스마트워크 환경에서 USIM을 이용한 모바일 오피스 사용자 등록 및 인증 프로토콜을 통한 안전한 서비스 제공 시스템을 제안한다. 4장에서는 제안 프로토콜에 대하여 안전성을 분석하고 끝으로 결론 및 향후 연구 방향을 제시한다.

* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 대학중점연구소 지원 사업으로 수행된 연구임(2010-0028298)

2. 관련 연구

2.1 스마트워크 환경에서의 모바일 오피스

스마트워크 환경에서의 모바일 오피스는 언제 어디서나 모바일 단말기를 통해 회사업무를 처리할 수 있는 시스템으로 [그림 1]과 같이 세 가지 요소로 구성된다. 모바일 단말로서의 스마트폰과 업무 관련 어플리케이션 솔루션, 이동통신 네트워크망과 모바일 플랫폼, 그리고 기업 업무 서비스와 관련한 기업의 업무 서버이다[1][2]. 이러한 구성은 단말, 네트워크, 서버 측면의 보안 기술 적용이 필요하며, E2E 암호화를 통해 스마트폰 내부에서부터 기업서버까지의 모든 경로에서의 안전한 정보 사용을 위한 보안 기술이 요구된다. 특히 기업의 업무 서버는 외부에서의 접근 및 서비스 요청에 대한 데이터를 모두 처리 해야 하기 때문에 보안 위협에 취약하며 이에 따른 서버 손상 및 데이터 유출을 막기 위하여 비정상 트래픽을 감지하는 릴레이서버 모델, 스마트폰 업무 요청 관련



[그림 1] 스마트폰 기반 모바일 오피스 시스템 구성요소

데이터를 미러 서버에 복사하여 사용 후 업무 서버에 반영하는 서버 이중화 모델 등이 제안되고 있다.

2.2 선행 USIM 기반 사용자 인증 프로토콜 연구

EAP-AKA(Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement) 인증 프로토콜은 USIM의 모바일 단말 고유키를 이용하여 모바일 사용자의 네트워크 접근에 대하여 인증하는 프로토콜이다. 특히 USIM은 3G 네트워크와 무선 네트워크 환경의 서로 다른 네트워크 연동에서의 보안 문제점을 해결하기 위해 데이터의 무결성과 기밀성을 제공한다. USIM의 고유키는 단말 및 가입자의 인증을 통하여 정당한 모바일 사용자의 안전한 네트워크 서비스 및 사용 과금 계산을 위해 필요하다. 그러나 홈네트워크와 지원네트워크 사이의 Bandwidth Consumption문제, 지원네트워크에서 각 사용자에 대한 다수의 인증 벡터 저장으로 인한 데이터 메모리 문제, Sequence Number 비동기화로 인한 인증 실패 등의 한계점으로 계속적인 개선 프로토콜이 제안되고 있다[3][4].

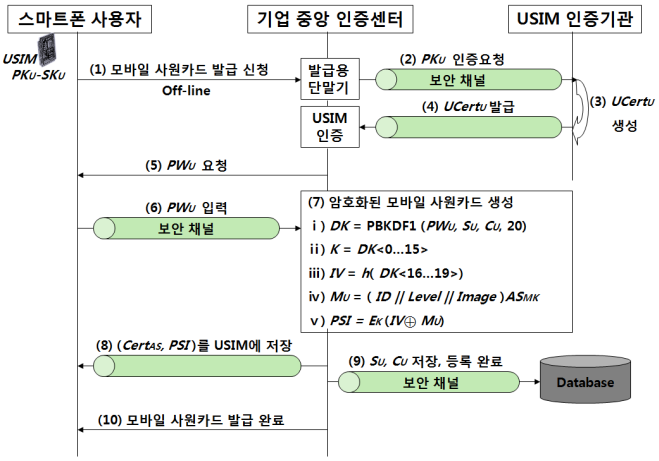
본 논문에서는 USIM 기반의 고유키를 네트워크 접근을 위한 사용자 인증 방식이 아닌, USIM 플랫폼의 응용프로그램에 사용 가능한 공개키 암호화 방식의 키로 가정하여 사용자 인증 프로토콜을 제안한다.

3. 안전한 모바일 오피스 시스템 프로토콜 제안

본 장에서는 스마트워크 환경에서 모바일 오피스 실행을 위하여 스마트폰의 USIM 탑재 기술을 응용한 정당한 사용자의 등록 프로토콜을 제시한다. 또한 정당한 사용자를 인증하여 안전한 모바일 오피스 환경에서의 서비스 제공 프로토콜을 제안한다. 제안된 모바일 오피스의 모델은 안전한 통신을 위하여 서버 이중화 모델을 전제로 한다.

3.1 등록 및 발급 단계

본 절에서는 모바일 오피스 접근에 정당한 권한이 있는 사용자에 대하여 [그림 2]와 같은 단계로 스마트폰에 탑재된 USIM에 모바일 사원카드 등록 및 발급 프로토콜을 제안한다. 이에 PKCS#5 (Public Key Cryptography Standards #5)에서 정의한 PBES1(Password Based Encryption Scheme 1)을 바탕으로 하며, 본 단계에서 사용하는 기호는 [표 1]과 같다.



[그림 2] 스마트폰 기반 모바일 사원카드 등록 및 발급

(1) 스마트폰 사용자 *U*는 기업이 관리하는 중앙 인증센터에서 스마트폰에 탑재된 USIM에 모바일 사원카드 발급을 요청한다.
(2) 중앙 인증센터 *AS*는 *U*의 신원 확인 후 안전한 통신 채널을 통하여 USIM 등록 인증 기관에 *U*의 USIM 공개키 PK_U에 대하여 인증 요청을 한다.
(3) USIM 인증 기관은 *U*의 신원 및 USIM 등록 확인 후, *U*의 USIM 등록 인증서 $UCert_U$를 생성한다.
(4) *IS*는 USIM 인증 기관으로부터 받은 $UCert_U$에 의하여 *U*의 USIM 등록을 인증한다
(5) *AS*는 *U*의 모바일 사원카드 발급하기 위해 *U*에게 카드 비밀번호 PW_U 6 자리를 요청한다.
(6) *U*는 안전한 통신 채널을 통하여 PW_U를 입력한다.
(7) *AS*는 *U*로부터 받은 PW_U를 기반으로 암호화된 모바일 사원카드를 생성한다.

ⅰ) *U*가 PW_U를 입력하면 *IS*는 *U*를 위한 난수 S_U와 계산 반복 횟수 C_U를 생성한다. PBES1에서 사용하는 키 추출 함수인 PBKDF1는 PW_U, S_U, C_U와 함께 SHA-1 해시함수의 사용으로 20바이트의 추출키 *DK*를 생성한다.

[표 1] 등록 및 발급 단계에서 사용하는 기호 및 의미

PW_U	*U*가 설정하는 6 자리 사원카드 비밀번호
S_U	인증센터 난수 생성기에 의한 8 바이트 salt
C_U	반복회수 값
DK	추출키
K	암호화된 비밀키
IV	초기벡터
h()	암호학적 16 바이트 추출 일방향 해시 함수
ID	실제 사원 이름에 해당하는 사원 번호
Level	실제 사원의 부서 및 직급에 해당하는 권한
Image	실제 사원의 이미지
AS_{MK}	중앙 인증센터의 마스터키
M_U	사원 정보로 생성한 중간 암호문
PSI	암호화된 사원정보의 암호문
$Cert_{AS}$	기업 중앙 인증센터의 모바일 사원카드 발급을 위한 공개키 PK_{IS}와 함께 중앙 인증센터 신뢰에 대한 인증서

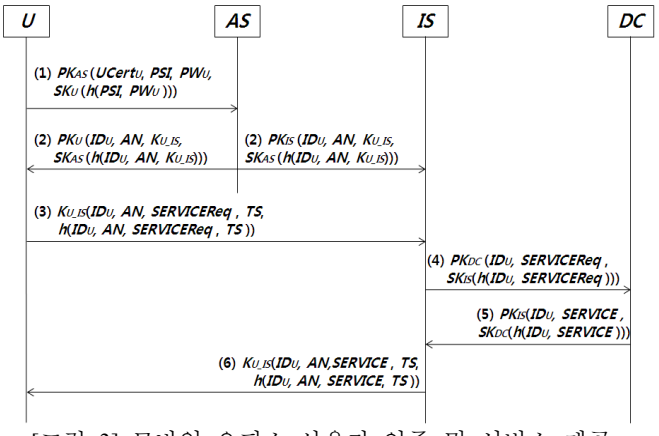
ii) 생성된 DK에서 처음 16바이트를 암호화된 비밀키 K로 한다.
iii) IV는 DK에서 나머지 4바이트에 대한 일방향 해시 함수에서 계산한 16바이트를 사용한다.
iv) 실제 사원 정보로서 사원번호 ID와 사원 권한 $Level$ 및 사원 이미지 $Image$ 정보에 대하여 인증기관의 마스터키 AS_{MK}로 대칭키 암호화에 의하여 암호화된 중간 암호문 M_U를 생성한다.
v) 생성된 M_U에 대하여 IV와 비밀키 K를 사용하여 SEED 블록 암호화 알고리즘에 의해 사원 정보를 암호화 한 암호문 PSI를 생성한다.

(8) 자신이 발행한 암호화 된 모바일 사원 정보인 PSI와 함께 중앙 인증센터는 자신의 인증서 $Cert_{AS}$를 모바일 사원카드를 사용하고자 하는 스마트폰 USIM 내에 안전하게 저장시킨다.
(9) 인증센터는 차후 U의 모바일 사원 카드 사용자 인증을 위하여 S_U, C_U 만을 인증센터의 안전한 저장장치에 저장한다. 이후 모든 과정의 데이터는 삭제하고 U의 모바일 사원카드 등록을 완료한다.
(10) AS는 U의 USIM 기반의 암호화된 모바일 사원카드 발급을 완료함으로써 U의 스마트폰을 통한 모바일 사원카드 사용이 가능하다.

3.2 사용자 인증 및 서비스 제공 단계

본 절에서는 스마트폰을 통한 모바일 오피스 접근을 위하여 USIM 기반 사원카드를 이용한 사용자 인증 및 서비스 제공 단계를 [그림 3]와 같은 순서로 보인다. 프로토콜 구조의 참여자는 기업의 사원으로서 모바일 오피스에 접근하고자 하는 스마트폰 사용자 U, 모바일 오피스 사용자를 인증하고 관리하는 중앙 인증센터 AS, 기업 서버 IS, 모바일 오피스에서 접근 가능한 기업 데이터센터 DC로 구성한다. 본 단계에서 사용하는 기호는 [표 2]와 같다.

(1) U는 스마트폰 상의 모바일 오피스 로그인 화면에서 ID 입력 대신 암호화된 사원 카드인 PSI를 호출하고, 6자리의 패스워드 PW_U를 입력한다. 또한 자신의 입력 정보에 대해 해시하여 USIM 개인키 SK_U로 전자서명 후 모바일 사원카드와 함께 배부된 인증센터 AS의 공개키 PK_{AS}로 암호화 하여 인증센터에 전달한다.



[그림 3] 모바일 오피스 사용자 인증 및 서비스 제공

[표 2] 인증 및 서비스 제공 단계에서 사용하는 기호 및 의미

ID_n	n의 기업 사원번호ID
PK_n	n의 공개키
SK_n	n의 개인키
AN	로그인에 의해 인증 센터가 부여하는 인증 번호
$SERVICEReq$	모바일 오피스 상에서의 서비스 요청
$SERVICE$	모바일 오피스 상에서의 요청에 의한 제공 서비스
TS	재전송 공격을 막기 위한 타임 스탬프
$h(D)$	데이터 D에 대한 일방향 해시 함수
$PK_n(D)$	n의 공개키로 암호화된 데이터 D
$SK_n(D)$	n의 개인키로 암호화된 데이터 D
$K_{i\_j}(D)$	i와 j가 공유하는 세션키 K로 암호화된 데이터 D

(2) AS는 자신의 개인키 SK_{AS}로 받은 메시지를 복호화하고 U가 보낸 인증서 $UCert_U$를 통해 U의 공개키 PK_U를 획득하여 메시지 서명 및 ID_U를 확인한 후 정당한 기업사원 U의 모바일 오피스 로그인을 기록 및 사용자 인증 처리를 한다.

AS는 U로부터 PSI와 PW_U를 획득한다. ID_U에 의해 안전한 곳에 저장되어있던 S_U, C_U와 함께 DK = PBKDF1(PW_U, S_U, C_U, 20)을 계산하여 K= DK<0…15>와 IV = h (DK<16…19>)를 구한다. SEED 블록 암호화 알고리즘에 기반하여 PSI를 K와 IV로 복호화 한 후 M_U를 획득한다. AS의 마스터키 AS_{MK}를 이용해 M_U를 다시 복호화하여 U의 실제 사원 정보인 ID_U, $Level$, $Image$를 확인한다. AS의 데이터베이스에서 찾은 U의 정보와 모바일 사원카드를 통해 획득한 U의 정보가 일치하면, U를 모바일 오피스의 정당 접근 사용자로 인증하고 U의 로그인 시각에 의해 발생한 인증번호 AN, 기업의 서버와 U의 통신을 위해 생성한 세션키 K_{U_IS}와 U의 사원 번호 ID_U를 U의 공개키로 암호화하여 U에게 보낸다. 또한 AS는 동일한 메시지를 기업 서버 IS에도 보냄으로써 U와의 세션키 성립을 알린다.
(3) U는 AS로부터 받은 정보를 복호화하고 AS의 전자서명을 확인한다. 또한 U는 모바일 오피스에서 업무를 처리하기 위해 $SERVICEReq$을 자신의 ID와 AN 값 및 재전송 공격을 막기 위한 TS를 붙여 세션키 K_{U_IS}로 암호화 하여 기업 서버에 전송한다.
(4) 기업 서버는 세션키 K_{U_IS}로 복호화한 U의 메시지에서 모바일 오피스 상의 데이터센터를 접근하기 원하는 U의 요청을 확인 한다. U가 요청한 업무 데이터에 접근할 권한이 있는지에 대하여 기업의 보안 정책에 따른 서비스 정당 사용자 확인 및 서비스 처리를 위해 기업서버는 데이터센터의 공개키로 암호화 하여 요청 서비스와 ID_U를 연접해 보낸다.
(5) 데이터센터는 IS의 메시지에서 ID_U의 요청을 확인하고 정보의 접근 권한이 있으면 요청한 업무 관련 데이터를 처리한다. 요청에 대한 결과를 기업서버의 공개키로 암호화 및 해시된 메시지 다이제스트의 서명을 함께 기업 서버에 보낸다.
(6) 기업 서버는 데이터 센터 결정에 따라 요청 업무

결과를 기업 서버에 반영하며, 재전송 공격을 막기 위한 *TS*를 붙여 *U*가 요청한 서비스에 대하여 세션키 K_{U_IS}로 암호화 한 후 *U*에게 전달한다. 따라서 모바일 오피스 사용자의 정당성 검증이 된 *U*만이 기업의 정보에 대하여 안전하게 접근 및 사용이 가능하다.

4. 제안 시스템의 안전성 분석

(1) 스마트폰 사용자: 스마트폰 사용자는 기업의 중앙 인증센터로부터 패스워드 기반 암호화에 따른 모바일 사원카드를 자신의 USIM카드에 발급 받음으로써 PW_U를 아는 정당한 사용자인 사원만이 모바일 오피스의 접근이 가능하다. 특히 인증에 필요한 정보에 대하여 미리 암호화하여 사용하므로 악의적 제 3자의 위장 공격의 위험성 및 훔쳐보기 공격에 강하다. 또한 스마트폰 단말기의 도난, 분실시에도 PW_U를 알지 못하는 사용자는 기업 정보의 접근이 불가능하므로 정보 유출에도 안전하다. 인증을 통해 모바일 오피스에 로그인한 사용자는 인증센터에서 제공한 기업 서버와의 세션키 K_{U_IS}를 통하여 자신의 서비스 요청 및 업무 처리를 안전하게 수행할 수 있다.
(2) 네트워크: 스마트폰과 기업 서버와의 접속에 있어 인증센터와 스마트폰 간의 공개키 기반 암호화, 인증센터의 인증을 통해 세션키 K_{U_IS}를 통한 스마트폰과 기업 서버간의 서비스 요청 및 처리의 대칭키 기반 암호화, 모바일 오피스에서의 사용 정보에 대하여 기업 데이터로의 반영을 위한 기업 서버와 데이터 센터 간의 공개키 기반 암호화가 진행된다. 이는 네트워크에서 발생 할 수 있는 패킷 가로채기로 인한 데이터 유출의 위험성에 강하다. 또한 기업서버와 정당 권한 사용자 간의 데이터 전송에 있어 타임스탬프 *TS*를 사용함으로써 재전송 공격에 안전하다.
(3) 기업서버: 기업서버는 크게 세 부분으로 모바일 오피스 시스템을 구성한다. 기업의 중앙 인증센터 *AS*는 정당 사용자의 인증 프로토콜에 의해 모바일 오피스 사용을 위한 사원 로그인 기록 *AN*을 남긴다. *DC*는 모바일 오피스에서 사용되는 데이터에 대한 데이터 센터로 미러 서버의 역할을 하며 정당 사용자 권한에 맞는 데이터 요청에 대해 처리하여 기업 서버 *IS*로 전송한다. 특히 *IS*와 *DC*는 공개키 기반의 데이터 전송으로 데이터 무결성을 보장하며, *DC*의 데이터 처리 결과에 따라 기업서버는 정당사용자 ID_U와 요청 업무 결과를 기업 서버에 반영한 후 *U*에게 전달함으로써 *U*의 행위에 대한 부인 방지를 보장한다.

5. 결론

스마트워크 환경의 모바일 오피스는 시공간의 제약이 없는 스마트폰의 특성으로 많은 양의 업무를 빠르게 처리할 수 있는 장점이 있는 반면, 휴대성과 개방성으로 인한 기업 정보의 접근 및 유출 위험의 취약점을 가지기 때문에 시스템 구성에서의 보안 및 안전성 확보가 필요하다.

이에 본 논문에서는 USIM을 이용한 정당한 권한을 가진 기업 사원의 사용자 등록 및 인증 방법과 안전한 서비스 사용이 가능하도록 모바일 오피스 시스템을 설계하였다. USIM을 통한 인증은 암호화된 모바일 사원카드를 스마트폰에 등록시킴으로써 이를 이용한 정당 사용자만의 모바일 시스템 접근을 허용한다. 또한 인증에 의해 발생한 키 기반 암호화로 모바일 오피스 시스템의 구성 요소간의 안전한 통신 상태에서 기업 정보의 요청 및 사용에 대한 데이터 기밀성과 무결성 그리고 부인 방지를 보장 받는 효과를 가진다.

앞으로 스마트폰을 통한 스마트워크 환경의 모바일 오피스 시스템 구축과 구현방법에 대하여 보안 요소를 고려한 표준화 연구가 더욱 필요하다.

참고문헌

[1] S. Na, Y. Lee and S. Jhee “Security Issue and Response Strategy for Smartphone and Mobile Office,” *Proc. of the CIO Report by National Information Society Agency* 2010, vol. 26, pp.1-40, 2010. (in Korean)
[2] J. Kim and H. Kim, “A Study on Server Security for Secure Smartphone-based Work Environment of Government Bodies,” *Journal of Security Engineering*, vol.7, no.6, pp.685-692, 2010. (in Korean)
[3] S. Lim, O. Yi, S. Jun and J. Han, “A Study on EAP-AKA Authentication Architecture for WiBro Wireless Network,” *Journal of Korea Information and Communication Society*, vol.31, no.4(3), pp.441-450, 2006. (in Korean)
[4] D. Kim and S. Jung, “Improved AKA Protocol for Efficient Management of Authentication Data in 3GPP Network,” *Journal of the Korea Institute of Information Security and Cryptology*, vol.19, no.2, pp.93-103, 2007. (in Korean)
[5] E. Jhee, A. Kim and S. Lee, “The Security Improvement of Mobile Credit Card Payment Protocol for USIM-based Smart Phone,” *Proc. of the KIISE Korea Computer Congress* 2010, vol.37, no.2(A), pp.86-87, 2010. (in Korean)
[6] Y. Kim, H. Kim and M. Jun, “A Study on User Authentication Method for Using Cloud Computing in an Enterprise,” *Proc. of the KIISE Korea Computer Congress* 2010, vol.37, no.1(D), pp.42-46, 2010. (in Korean)
[7] H. Mun, K. Han and K. Kim, “3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA,” *Wireless Telecommunications Symposium*, pp.1-8, 2009.
[8] C. Tang and D. Wu, “An Efficient Mobile Authentication Scheme for Wireless Networks,” *IEEE Transactions on Wireless Communications*, vol.7, pp.1408-1416, 2008.
[9] X. Li, J. Ma, Y. Park and L. Wu, “A USIM-Based Uniform Access Authentication Framework in Mobile Communication,” *EURASIP Journal on Wireless Communications and Networking,* vol.2011, pp.1-12, 2011.