IMT-2000 UPT 서비스의 정보 보안을 위한 연구

최 영준°, 김 명철
한국정보통신대학원대학교 공학부
{cyjnice, mckim}@icu.ac.kr

Research of information security in IMT-2000 UPT service

Young-Joon Choi°, Myung-Chul Kim
Dept. of engineering, Information and Communications University

요약

IMT-2000 은 다양한 이동 전화 시스템의 규격을 통일하여 세계 어느 곳에서도 하나의 단말기 또는 사용자 접속 카드로 서비스를 이용할 수 있도록 하는 글로벌 멀티미디어 서비스이다. 본 논문은 IMT-2000 의 어플리케이션 중 범용 개인 통신 서비스인 UPT 서비스의 정보 보안 방법을 모색하여 본다. 과금 서비스인 UPT 서비스는 malicious person 의 공격에 의한 금전적 손실을 차단하기 위하여 가입자 인증 정보의 보안이 필요하다. 본 논문에서는 ATM 교환기를 사용하는 IMT-2000 시스템에서 지능망 프로토콜로 메시지를 주고 받는 UPT 서비스 시나리오 및 공격 시나리오를 분석하고, RSA 암호 기법을 적용한다.

1. 개요

다양하게 개발된 현재의 이동 통신 서비스는 각각의 서비스마다 구현하는 기술 방식이 다르고, 국가나 지역마다 사용하는 주파수 대역이 달라 이동성을 완벽하게 실현하는데 한계가 있다. 또한 무선 전송 매체를 사용해야 하는 기술적인 제약으로 인해 멀티미디어 서비스 등을 완벽하게 제공하지 못한다. 이러한 기존 이동 통신 서비스의 한계를 극복하고자 등장한 것이 International Mobile Telecommunications-2000 (IMT-2000) 이다. ITU 를 중심으로 추진되고 있는 이 시스템은 2Mbps 급 고속 데이터 통신이 가능한 사양 등을 갖추도록 제안되었다 [3].

본 논문은 IMT-2000 서비스의 하나인 Universal Personal Telecommunication (UPT) 서비스의 정보 보안 방법을 모색한다. UPT 서비스란, 서비스 프로파일을 이용하여 언제, 어디서나, 어떤 단말을 통해서든 원하는 상대에게 전화를 할 수 있고, 또한 받을 수 있는 범용 개인 통신 서비스이다. 서비스 프로파일은 서비스 가입자에게 고유하게 주어지는 개인 UPT 이용 코드와 함께 가입자 별로 제공 가능한 서비스의 범위, 현재 위치 그리고 과금 정보 등을 관리한다. 가령, UPT 서비스 가입자가 다른 단말기에 착신 또는 발신 전환을 하면 그 이후의 요금은 단말기의 소유자가 아닌 UPT 서비스 가입자에게 부과된다. UPT 서비스를 이용하려면 서비스 접근 번호, UPT 이용 코드, 비밀 번호, 기능 선택 번호가 필요하다 [1]. 이 중, 서비스 접근 번호, UPT 이용 코드와 비밀 번호는 UPT 서비스 가입자식별 및 서비스 이용에 대한 과금 정보로 사용되기 때문에 번호의 비밀 보장이 반드시 필요하다. 만일 이 정보들이 malicious person 에 의해 공격 받으면, 권한이 없는 사용자의 Free-Riding 으로 인한 금전적 손실이 발생할 수 있다. 기존 CDMA 이동 통신망에서도 pseudo-random noise sequence 나 hadamad-walsh code 등으로 동일 그룹 사용자의 데이터 보안을 위한 주파수 변조를 사용하였다 [4]. 본 논문은 주파수 변조 이전의 데이터를 공개키 암호 기법의 하나인 RSA 암호 기법으로 암호화함으로써 UPT 서비스의 정보 보안성을 향상시키는 방법을 모색하여 본다.

2. 공개키 암호 기법

기존의 관용 암호 기법에서 발생하는 키 관리의 문제점으로 지적되던 키 분배 방식을 해결한 것이 바로 공개키 암호 기법이다. 공개키 암호 기법은 통신 양자간에 서로 다른 키로 암호화, 복호화를 행하는 것으로, 공개키는 공개 목록에 등록하여 공개하고 비밀키는 개인이 보관한다 [2]. 공개키 암호 기법의 원리는 다음과 같다.

그림 1. 공개키 암호 기법.

공개키 암호 기법으로 가장 널리 사용되는 알고리즘은 1978 년 MIT 의 Rivest, Shamir 와 Adleman 이 처음 제안한 RSA 이다. RSA 암호 기법은 소인수분해의 어려움에 안전도의 근간을 둔다. 즉, 두 소수 p 와 q 의 곱은 계산하기 쉬우나, 주어진 곱 n = pq 로 부터 p 와 q 를 추출하기는 어렵다는 사실에 기초한다. RSA 암호 기법은 모듈러 지수 연산이 주를 이루며 실제 응용에 있어, 작은 암호화 지수를 사용함으로써 복호화보다는 암호화를 더 빠르게 수행할 수 있도록 설계된다. RSA 암호 기법은 다음과 같은 3 단계로 설계된다 [2].

1. key generation

- 소수인 p, q 선택 및 모듈러 연산수 $n = p * q$ 를 구한다.
- 오일러 함수 값 $\phi(n) = (p-1) * (q-1)$을 구한다.
- $\phi(n)$과 서로 소인 공개키 e 를 구한다.
- $ed = 1 \bmod \phi(n)$을 이용하여 비밀키 d 를 구한다.

2. encryption

임의의 문자열 M 을 $C = M^e \bmod n$ 의 식으로 암호화 한다.

3. decryption

암호화된 문자열 C 는 $M = C^d \bmod n$ 의 식으로 복호화 한다.

RSA 암호 기법에서 생성된 비밀키와 공개키를 이용하여 통신망에서 사용자들이 통신을 하는 경우를 도시화하여 보자. 다음 그림 2 는 가입자 A 가 통신망을 통하여 가입자 B 에게 M 이라는 메시지를 전달하는 예이다.

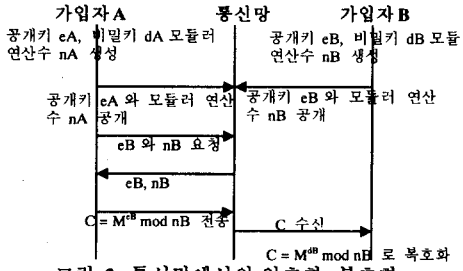

그림 2. 통신망에서의 암호화, 복호화.

그림 2 에서 가입자 A 와 가입자 B 는 통신망의 공개키 등록 디렉토리에 각각 자신들이 생성한 공개키와 모듈러 연산수를 공개한다. 그리고 상대방으로 메시지를 전송하려면 공개키 등록 디렉토리에서 상대방의 공개키와 모듈러 연산수를 가져와서 암호화하여 전송한다.

3. UPT 서비스 시나리오

UPT 서비스는 다음 그림 3 의 개괄적 시나리오로 진행된다.

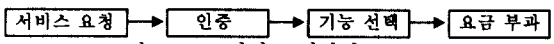

그림 3. UPT 서비스 시나리오.

UPT 가입자가 서비스 접근 번호와 UPT 이용 코드를 입력하여 서비스를 요청한 후, UPT 이용 코드와 비밀 번호의 인증이 성공적으로 수행되면 서비스를 제공 받을 수 있다. 기능 선택 과정에서 UPT 가입자는 등록, 등록 해제, 호 발신 및 착신 절차 중 하나를 선택하여 서비스를 제공 받을 수 있다. 단말기의 호 발신 서비스를 요청하면 발신자는 실제 착신지로의 연결과 서비스 이용에 대한 과금 내역을 안내 받을 수도 있다 [1].

IMT-2000 과 같이 1Kbps 에서 2Mbps 의 이질성을 가지는 트래픽 서비스들을 제공하려면 Variable Bit Rate (VBR) 등의 대역의 효율적인 전송이 가능하고 페이징을 위한 브로드캐스팅이 용이한 ATM 교환기가 IMT-2000 의 교환기로 적절하다. 이동 호 및 지능망 처리를 할 수 있는 ATM 교환기의 내부 블록은 다음과 같다 [1].

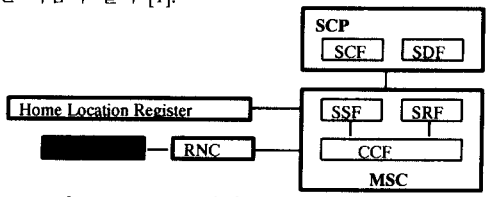

그림 4. IMT-2000 서비스 처리 블록.

지능망 구조의 분산 기능 평면 관점에서 출발한 차세대 이동 통신 시스템인 IMT-2000 의 기능 실체 중 교환기 기능에 속하는 Call Control Function (CCF)는 기본호 처리 기능을 위한 호/접속을 관리하고 지능망 서비스를 위한 스위칭 역할을 한다. Radio Access Network Controller (RNC) 정합부에서 무선 단말의 호가 지능망 서비스임을 감지하면 CCF 는 Service Switching Function (SSF)를 통하여 SCF 로 지능망 서비스를 요청한다. 이때, home Location Register (HLR)을 이용하여 무선 단말의 정보를 참고한다. SSF 는 CCF 와 연결되어 이동 및 지능망 호 처리 기능을 수행하며 Switch Control Function (SCF)와 상호 작용하기 위해 필요한 CCF 의 상태를 관리한다. Specialized Resource Function (SRF)는 SCF 로부터 필요한 자원의 요청을 수신하면 호 발생자에게 안내 방송 등을 발송하는 역할을 하고 Service Data Function (SDF)는 UPT 이용자들의 서비스 프로파일을 관리한다 [1].

신속한 서비스의 생성과 효율적인 서비스 제어를 목적으로 망의 기능이 여러 개의 시스템으로 분산되는 구조를 갖는 지능망에서는 시스템 간에 긴밀한 정보 교환 방안을 고려해야 한다. 이때 사용되는 프로토콜이 Intelligent Network Application Protocol (INAP)이다. INAP 은 물리 실체들 간의 상호 작용을 지원하기 위한 응용 계층의 프로토콜이며 INAP 하부 프로토콜로서는 No. 7 공통선 신호 방식이나 ISDN 신호 방식이 사용된다. 이 INAP 프로토콜을 이용한 UPT 서비스 시나리오는 다음과 같다 [1].

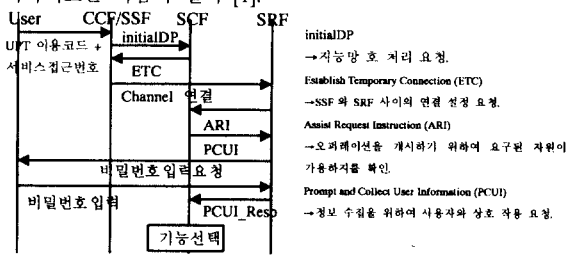

그림 5. UPT 공통 절차.

위의 그림 5 는 UPT 서비스의 공통 절차이다. 이용자들은 UPT 이용 코드 + 서비스 접근 번호를 호 처리 담당 블록인 CCF/SSF 로 전송한다. UPT 와 같은 지능망 서비스인 경우는 SCF 에 지능망 처리 시작을 지시한다. 채널 연결이 된 후에는 비밀 번호를 입력하여 기능 선택 절차에 들어간다. 기능 선택 절차에서 사용자가 착신 전환을 선택하면 그 이후에 UPT 가입자에게 전달되는 호는 착신 전환 단말로 전해진다. 그리고 발신 전환을 선택하면 발신 전환 단말을 UPT 가입자의 단말로 인식한다. 이와 같은 경우 서비스 요금은 서비스 프로파일에 기록된다.

4. 공격 시나리오

UPT 가입자를 인증하는데 사용되는 UPT 이용 코드 + 서비스 접근 번호와 비밀 번호가 malicious person 에 의해서 공격된 상황을 가정하여 보자. 단말기와 교환기 (기지국) 사이의 정보 교환은 공중망을 통한 전파에 의해 형성된다. 따라서 malicious person 의 전파 스캐닝에 의한 정보 유출 위험이 높다. 그림 6 은 malicious person 이 User A 에게 Free-Riding 하여 각종 서비스를 받는 상황이다.

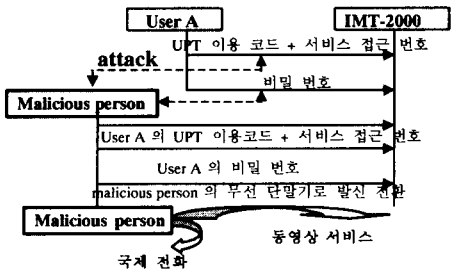

그림 6. 공격 시나리오

Malicious person 은 User A 의 UPT 이용 코드 + 서비스 접근 번호와 비밀 번호를 dropping 한다. 그리고 이 정보를 이용하여 자신의 단말로 발신 전환하고 국제 전화나 동영상 서비스를 제공 받는다. 혹은 User A 의 UPT 비밀 번호나 서비스 프로파일을 변경시킬 수도 있다. 이 경우 User A 는 malicious person 이 서비스 받은 요금까지도 부과 받게 되어 자칫하면 막대한 손해를 입을 수도 있다. 다른 과금 서비스인 경우에도 UPT 서비스와 동일한 문제가 발생할 수 있다. 그러므로 IMT-2000 서비스의 전반에 걸쳐 정보 보안을 위한 연구가 필수적이다.

5. RSA 암호 기법 적용

3 장의 UPT 서비스 시나리오에서 서비스 요청 부분과 비밀 번호 전송 부분에 RSA 암호 기법을 적용하여 보자. 실제 데이터는 디지털화되어 전파로 전송되므로 암호화는 단말기에서, 복호화는 기지국에서 수행된다. 사용자가 단말기의 버튼을 누르고 데이터를 전송하면 단말기 내부에서 아래의 계산으로 암호화하여 디지털 시그널로 변조한다. 본 보고서에서는 서비스 접근 번호를 2 자리, UPT 이용코드와 비밀 번호를 8 자리로 가정하여 암호 체계를 설계한다. 따라서 최대 $10^8 - 1$ 의 UPT 서비스 가입자를 수용할 수 있다. 계산 툴인 mathematica 를 이용하여 RSA 암호 체계를 설계하여 보자.

예제 1. UPT 이용 코드+서비스 접근 번호

1. key generation

p = 48611, q = 48619, n = p * q = 2363418209
$\phi(n) = (p-1) * (q-1) = 2363320980$
$\phi(n)$와 서로 소인 공개키 e = 157
ed = 1 mod $\phi(n)$에서 비밀키 d = 827914993

2. encryption

샘플 데이터 M = 1234567890
C = $(1234567890)^{157}$ mod 2363418209 = 1575054860

3. decryption

C 의 복호화: $(1575054860)^{827914993}$ mod 2363418209 = 1234567890

예제 2. 비밀 번호

1. key generation

p = 7919, q = 7927, n = p * q = 62773913
$\phi(n) = (p-1) * (q-1) = 62758068$
$\phi(n)$과 서로 소인 공개키 e = 157
ed = 1 mod $\phi(n)$에서 비밀키 d = 57961273

2. encryption

샘플 데이터 M = 12345678
C = $(12345678)^{157}$ mod 62773913 = 48223779

3. decryption

C 의 복호화: $(48223779)^{57961273}$ mod 62773913 = 12345678

예제 1 에서 볼 수 있듯이 UPT 이용 코드+서비스 접근 번호의 RSA 암호 체계 설계는 샘플 데이터 M = 1234567890 에 대하여 암호화와 복호화가 성공적으로 수행되었다. 비밀 번호 역시 예제 2 와 같이 암호화, 복호화가 성공적으로 이루어졌다. 암호화 및 복호화된 데이터가 UPT 서비스에서 전송되는 과정을 다음 그림 7 로 살펴보자. 그림 7 에서는 MSC 내부의 블록 CCF, SSF, SRF 를 한 묶음으로 하여 단순 도식화한다. 이 경우 그림 5 와 다르게 CCF/SSF 와 SRF 의 메시지는 고려하지 않는다.

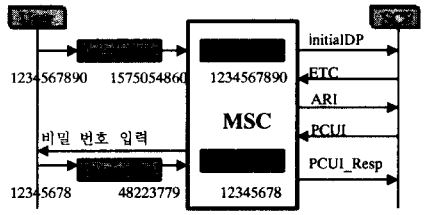

그림 7. RSA 를 이용한 UPT 공통 절차.

암호화된 호 발신 (1575054860) 데이터를 수신한 MSC 는 이것을 복호화하며, 이 호가 지능망 호 임을 인식하여 SCF 로 지능망 서비스 시작 (initialDP)을 요청한다. 그리고 암호화된 비밀 번호 (48223779) 역시 MSC 에서 복호화 되고, MSC 는 비밀 번호를 SCF 에 전송 (PCUI_Resp) 한다. 위와 같은 암호화, 복호화 과정을 통하여 malicious person 의 공격에 의한 금전적인 손실을 최소화 할 수 있다.

6. 결론 및 향후 연구 계획

본 연구에서는 IMT-2000 UPT 서비스의 정보 보안을 위하여 RSA 암호 기법을 적용하여 보았다. UPT 서비스는 단말기의 착신, 발신 전환을 가능하게 하는 것이기에 malicious person 에 의한 공격이 발생하면 금전적인 손실이 발생할 수 있다. 특히 공중 전파를 사용하는 무선 전화망의 경우 정보 유출의 위험도가 높다. 그러므로 과금 서비스인 UPT 서비스에서는 사용자 인증을 위해 사용되는 서비스 접근 번호, UPT 이용 코드, 비밀 번호의 보안이 중요하다.

본 연구에서는 UPT 서비스가 성공적으로 진행되는 경우의 시나리오만 고려하였다. 향후 모든 경우에 있어서의 시나리오를 분석하고, INAP 오퍼레이션의 FSM 을 형성하여 feature interaction 과 같은 프로토콜 시험을 수행할 예정이다. 그리고 키 길이에 제약이 따르는 RSA 를 대체할 수 있는 Elliptic Curve Cryptosystem (ECC) 알고리즘을 적용하여 볼 것이다.

참고 문헌

[1] 최고봉, 김기령, 김태일, 윤병남, "지능망 기술," 홍릉 과학 출판사, 1997.
[2] 이민섭, "현대 암호학," 교우사, 2000.
[3] 한국통신 IMT-2000 홈페이지, http://www.imt2000.co.kr
[4] T. S. Rappaport, "Wireless Communications, Principles and Practice", 1996, Prentice Hall.