시점확인을 위한 PKI 기반 IMT-2000 서비스

이 덕 규, 이 임 영

순천향대학교, 정보기술공학부

A Based on PKI of IMT-2000 for Time Conviction

Deok-Gyu Lee, Im-Yeong Lee

Division of Information Technology Engineering SoonChunHyang Univ.

요 약

무선 이동통신의 발전으로 인해 많은 사용자가 발생하였다. 그러나 1세대나 2세대의 경우 이동통신서비스는 기본적으로 음성을 기반으로 서비스를 하였기 때문에 다른 멀티미디어 서비스와 같은 고속 무선 인터넷 통신 수요자의 요구를 충족시키지 못하고 있다. 향후 무선에서 음성위주의 서비스가 아닌 데이터와 이동 멀티미디어 서비스와 같은 서비스를 통해 얻을 수 있다. 하지만 무선망은 전송로가 노출되어 있어 정당하지 않는 사용자에 의한 불법적인 절취 사용과 도청등에 많은 문제 점이 발생할 수 있다. 악의적인 제 3의 사용자가 공유되어 있는 문서에 대한 문제점뿐만 아니라 양자간의 계약 혹은 과금 정보에 있어 악의적인 목적을 막는 방법이 필요하다. 다음과 같은 방법에 대한 해결책으로써 문서에 대한 내용증명과 시점확인이 바로 그것이다.

본 논문에서는 앞에서 언급한 문제점을 해결하고자 유선에서 사용중에 있는 시점확인 서비스 혹은 내용 증명 서비스를 향후 발전할 IMT-2000에 적용하여 보았다. 제안한 방식은 IMT-2000에서의 개체를 그대로 이용하면서 효율적인 방식을 제안하였다.

I. 서론

이동통신은 1 세대와 2 세대를 거치면서 비약적인 발전을 거듭하였으며 많은 사용자가 발생하였다. 그러나 1 세대와 2세대 이동통신서비스는 기본적으로 음성위주의 서비스를 염두에 두고 개발하였기 때문에 이동 멀티미디어 서비스와 같은 고속 무선 인터넷 통신 수요자의 요구를 충족시키지 못하고 있다. 향후 무선에서는 음성위주의 서비스가 아닌 데이터와 이동 멀티미디어 서비스와 같이 고도화된 서비스를 통하여 얻을 수 있을 것이다. 이러한 이동통신서비스는 시간과 장소의 제약을 받지 않고 음성 및 데이터 서비스를 제공하는 편리함을 가지고 있는 반면에 사용자가 이동성을 가지고 있고 전파를 통신 매개로 이용하는 특성으로 인하여 보안상의 취약점을 가지고 있다.

제 3 세대 이동통신 시스템인 IMT-2000의 특징은 현재 유선망에서 제공하고 있는 서비스의 대부분을 무선망에서도 지원할 수 있게 하면서 유선망에서의 품질을 보장한다는 목표를 가지고 있다. 하지만 무선망은 전송로가 노출되어 있어서 정당한지 않은 사용자에 의한 불법적인 절취사용과 악의를 가진 제 3자가 공유된 전송매체를 통해 전파를 도청하기 쉽다는 문제점을 가지고 있다. 다른 문제점으로는 악의를 가진 제 3자뿐 아니라 양자간에 계약에 있어 한 사용자가 악의적인 목적을 가지고 있을 때 악의적인 목적을 막는 방법이 필요하다 이러한 방법으로는 공증기관을 두어 사용자와 사용자사이의 내용증명과 시점 확인 서비스가 있을 수 있다. 다음과 같은 서비스는 사용자간뿐 아니라 사용자와 서비스 제공 업체와도 연결되어 과금 증명에 사용될 수 있을 것이다.

본 논문에서는 유선에서 제공되고 있는 서비스를 앞으로 사용될 IMT-2000에서 적용하여 내용 증명과 시점확인 서비스를 가능하게 하였다.

하지만 현재 IMT-2000 개발 상황을 고려할 때 시스템이 완벽하게 구축되지 않은 상태에서 전체적인 관점으로 서비스의 체계와 전체적인 서비스를 살펴보는 것은 불가능하다. 하지만 IMT-2000은 전체적으로 유선에서 제공하고 있는 서비스를 제공하고자 하는 것이 목적이다.

본 논문의 2장에서는 IMT-2000에 대한 개요 및 보안 요구사항에 관하여 설명하고, 3장에서는 공증 서비스 개요에 대하여 살펴본다. 이를 바탕으로 4장에서는 IMT-2000에서 적용될 수 있는 시점 확인 서비스를 제

시한다. 그리고 5장에서는 제안방식 분석에 관하여 간략히 언급하고 결론은 내리도록 한다.

II. IMT-2000 개요 및 보안 요소

1. IMT-2000 개요

GSM이나 IS-95 CDMA 시스템과 같은 2세대 이동통신 시스템과 비교하여, 진보된 3세대 방식인 IMT-2000 시스템은 고속의 멀티미디어 서비스 제공 및 글로벌 로밍을 특징으로 한다.

이러한 이동통신의 환경의 변화는 정보보호에 대한 대책을 절실히 요구하고 있고, 또한 정보보호 기술도 새로운 환경 변화에 맞추어 발전해야 한다. 이에 부합하여 IMT-2000의 발전을 주도하고 있는 지역 그룹인 3GPP(3rd Generation Partnership Project)와 3GPP2(3rd Generation Partnership Project2)에서는 각각 자신들의 기술에 맞는 표준화 작업을 진행 중이다. 특히, 비동기 방식 표준을 제정하고 있는 3GPP는 ETSI, ARIB, TTA, TI, TTC로 구성되어 있고 여러 작업 그룹에서 활발한 활동을 보이고 있다. 보안 아키텍쳐 , 인증 메커니즘, 암호 알고리즘 등과 같은 정보보호와 관련해서는 TSG SA WG3에서 담당하고 있다.

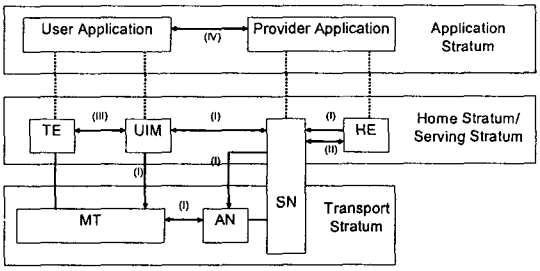

그림 1: 보안 구성도

▷ 네트워크 엑세스 보안 : 3G(3rdGeneration) 서비스에 대한 안전한 access 및 radio link 상에서 제3자의 attack 을 방지하는 기능을 제공한다. (I)

▷ 네트워크 도메인 보안 : 네트워크의 유선구간에서 전송되는 정보의 보호 및 signaling 정보에 대한 보호를 제공한다.(II)

▷ 사용자 도메인 보안 : MS(Mobile Station)에 안전하게 access 하는 부분을 제공한다.(III)

▷ 어플리케이션 도메인 보안 : 사용자와 Service provider domain에서 안전하게 메시지가 전송되도록 하는 기능(IV)

III. 공증 서비스

안전성과 신뢰도는 전자상거래에 있어 필수적인 요소이다. 안전성은 제 3자에 의한 위협요소를 제거함으로써 실현될 수 있지만, 거래 당사자들 간의 신뢰성이 없다면 안전한 전자상거래는 이루어질 수가 없다. 따라서, 전자공증은 거래 당사자들 간의 신뢰성을 형성하는데 있어 핵심적인 역할을 하는 기능이라고 정의할 수 있다.

전자공증의 기능은 인터넷상에서 사용되는 전자공증 시스템은 일반적으로 상용되고 있는 공증의 기본서비스와 PKI와 관련된 인증서 공증 등의 서비스를 제공한다. 전자공증과 관련된 여러 가지 기능들은 다음과 같은 것들이 있을 수 있다. 송신자와 수신자 확인, 배달 증명(Certification of Delivery), 부정조작의 검출(Detection of Tampering), 타임스탬프(Time-Stamp), 접근기록(Recording of Accesses), 절차기록(Recording of Processes), 그리고 디지털 저장(Digital Storage)이 있다.

전자 공증에 대한 요구사항으로 책임성을 들 수 있다. 책임성의 가장 중요한 요소는 안전성 추구이다. 보안관련 요구사항으로는 데이터에 대한 불법적인 변조나 파괴에 강해야 한다.

IV. 제안방식

다음에서는 IMT-2000환경에서 적용 가능한 PKI기반에서의 시점확인 서비스 구조를 제안한다.

1. 구성요소

다음은 본 방식에서 사용되는 구성요소를 기술하고 있다. 그림 2에서는 전체 구성도를 도식하고 있다.

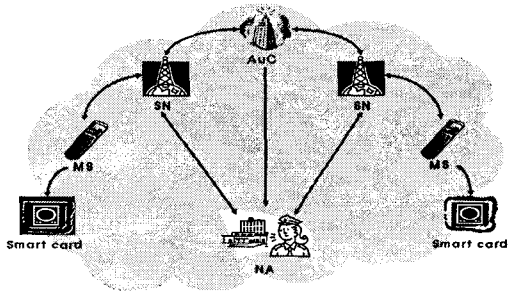

그림 2: 전체 구성도

· AuC : Authentication Center로써 사용자에 공개키 인증서를 송신한다.

· NA : Notary Authority로써 AuC로부터 통신 요청이 완료되면 NA는 AuC로부터 키를 받게되며 이를 바탕으로 세션키를 생성하게 된다.

· SN : Service Network으로써 MS_0와 MS_1이 암호화 통신을 할 때 SN에 암호화된 내용이 저장된다

· MS : Mobile Station으로 다른 MS에 통신을 요청하며 NA로부터 받은 Key를 USIM에 저장하는 역할을 한다.

· USIM : User Subscriber Identity Module으로 Key를 저장한다.

2. 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술하고 있다.

- CKey : AuC에서 생성하는 Key
- NKey : NA에서 생성하는 Key
- E_{Key} : MS간에서 사용될 세션키
- ID : Identity
  - MS : Mobile Station
  - AuC : Authentication Center
  - NA : Notary Authority
- H() : 해쉬 함수
- PK_{MS0}, PK_{MS1} : MS_0의 공개키 및 MS_1의 공개키
- PK_{AuC} : AuC의 공개키
- SK_{AuC}, SK_{NA} : AuC의 비밀키 및 NA의 비밀키
- Sig_{AuC}, Sig_{MS0}, Sig_{MS1} : AuC의 서명 및 MS_0, MS_1의 서명
- TS_{MS0}, TSL_{AuC} : MS_0의 공개키 및 AuC의 공개키
- Res : Response 값

3. System Protocol

다음은 개괄적인 프로토콜에 대하여 도식한 것이다.

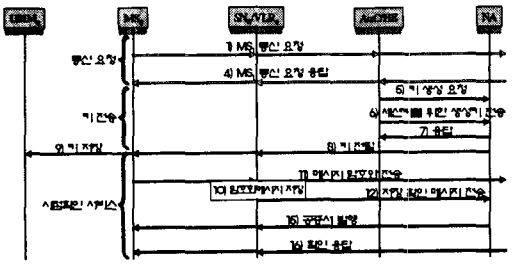

그림 3: MS_0에서의 개략적 Protocol

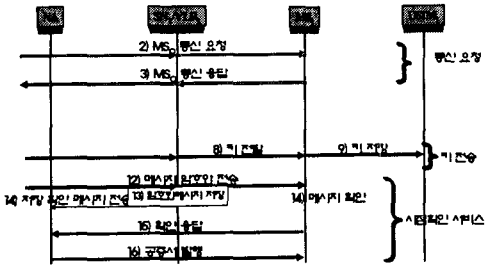

그림 4: MS_1에서의 개략적인 Protocol

그림 3은 MS0에서의 개략적인 Protocol이며 그림 4는 MS1에서의 개략적인 Protocol이다. 그림 3과 그림 4를 붙여놓았을 때 전체적인 Protocol로써 완성된다.

다음은 위의 그림을 바탕으로 자세한 프로토콜을 기술한다.

1) 통신 요구 단계

다음은 본 방식에서 처음으로 통신하기 위해 필요한 요청과 응답에 대하여 기술하고 있다.

① MS_0는 MS_1과의 통신을 SN_0에 요청한다.

② SN_0는 AuC에 MS_1의 위치를 요청한다.

③ AuC는 SN_1에게 SN_0의 정보와 MS_1의 통신을 요청한다.

④ SN_1은 MS_1에게 MS_0의 통신을 요청을 확인한다.

⑤ MS_1은 통신 확인에 대한 응답을 한다.

⑥ SN_1은 응답에 대한 결과를 AuC에 전송한다.

⑦ AuC는 요청에 대한 응답을 SN_0에 전송하면 마지막으로 SN_0는 MS_0에 응답을 전송한다.

2) 키 분배 단계

다음은 본 방식에서 메시지 암호화를 위해 필요한 키 분배에 대하여 기술하고 있다.

① 통신 요구 단계에서 ⑥의 단계가 완료되면MS_0와 MS_1과의 통신 요청이 올바르게 되었음을 알리고 키 생성 요청을 한다.

② AuC는 CKey (1)을 생성하여 메시지 (2)를 NA에 전송한다.

$$CKey = H(ID_{AuC} || ID_{MS_0} || ID_{MS_1} SK_{AuC}) \quad (1)$$

$$PK_{NA}(CKey || Sig_{AuC}(H(CKey))) \quad (2)$$

③ CKey 전송에 대한 응답을 한다.

이로써 통신 요구 단계에 키 분배 단계까지 완료한다.

3) 메시지 전송 단계

다음은 본 방식에서는 키 분배 단계를 거쳐 메시지 전송 단계에 대하여 기술하고 있다

① NA는 다음의 Key를 생성한다.

$$NKey = H(ID_{NA} || SK_{NA}) \quad (3)$$

$$Key = H(ID_{MS_0} || ID_{MS_1} || CKey || NKey) \quad (4)$$

② 생성된 Key를 SN_0와 SN_1에 다음의 (5), (6)으로 전송한다.

$$PK_{MS_0}(ID_{MS_0} || Key || Sig_{AuC}(ID_{MS_0} || Key)) \quad (5)$$

$$PK_{MS_1}(ID_{MS_1} || Key || Sig_{AuC}(ID_{MS_1} || Key)) \quad (6)$$

③ 다시 SN_0와 SN_1는 (5), (6)을 MS_0와 MS_1에 전송한다.

④ MS_0와 MS_1는 받은 Key를 USIM에 저장한다.

⑤ MS_0는 메시지 M을 Key로 암호화하여 다음을 전송한다.

$$E_{Key}(ID_{MS_0}||M||TS_{MS_0}Sig_{MS_0}(H(ID_{MS_0}||M||TS_{MS_0}))) \quad (7)$$

⑥ SN_0는 전송받은 (7)을 저장한 후, SN_1에 전송한다. SN_0는 저장할 때 자신의 비밀키로 타임스템프를 첨부하여 보관한다.

$$Sig_{SN_0}(E_{Key}(ID_{MS_0}||M||TS_{MS_0}Sig_{MS_0}(H(ID_{MS_0}||M||TS_{MS_0})||TS_{SN_0}) \quad (8)$$

⑦ SN_1 또한 전송받은 (7)을 저장한 후, MS_1에 전송한다. SN_1 또한 타임스템프를 첨부하여 보관한다.

$$Sig_{SN_1}(E_{Key}(ID_{MS_0}||M||TS_{MS_0}Sig_{MS_0}(H(ID_{MS_0}||M||TS_{MS_0})||TS_{SN_1}) \quad (9)$$

⑧ SN_1은 저장 후 확인 메시지를 NA에 발송한다.

⑨ MS_1은 전송받은 (7)을 확인한 후 SN_1에 확인 응답을 발송한다.

$$E_{Key}(ID_{MS_0}||RES, Sig_{MS_1}(ID_{MS_0}||RES)) \quad (10)$$

⑩ SN1은 SN0에 발송하고 다시 SN0는 MS0에 응답 메시지를 발송한다.

⑪ MS0는 응답 확인 메시지를 발송하고 모든 과정을 마친다.

4) 시점확인 단계

다음은 본 방식에서 시점에 대한 확인 단계에 대해 기술하고 있다.

① 메시지에 불확실성 확인은 MS의 요청에 의해 이루어진다.

② 사용자로부터 불확실성에 대한 요청이 접수되면 NA는 AuC에게 CKey를 요청한다. AuC로부터 전송되어온 CKey와 NKey를 이용하여 Key를 생성하여 메시지가 저장되어 있는 각 SN에게 전송한다.

③ 각 SN들은 전달되어진 Key를 이용하여 복호화한다. 사용자들은 각 SN에 저장되어진 SN의 TS를 이용하여 전송 시간과 내용 증명 확인을 받을 수 있다.

V. 제안 방식 분석

본 방식에서는 전송로상의 불법적인 도청 및 변조는 각 개체의 공개키 혹은 세션키를 이용하여 문제점을 방지하였다.

또한 이러한 문제점이외에 각 개체들이 악의적인 목적을 가지고 다른 개체에 대해 부정을 저지르지 못하도록 되어있다. 사용자와 서버의 담합의 경우 CKey내에 사용자들의 ID와 AuC의 개인키를 해쉬취한 값이 되므로 서버에서 만들어 낼 수 없다. 따라서 서버와 사용자의 불법적인 담합은 막을 수 있다.

SN이 불법적인 목적을 가지고 있다. NA에게서 사용자에게 전달된 키를 알아낼 수 없으므로 SN은 확인에 대한 요구가 있기 전까지 메시지를 확인할 방법이 없다.

시점확인은 시점에 대한 확인 이외에도 SN에 저장되어있는 암호화된 메시지를 이용하여 사용자들 혹은 법행기관에서 풀어서 내용 증명 서비스를 시행할 수 있다.

VI. 결론

지금까지 무선 이동 통신은 1세대와 2세대를 거쳐오면서 많은 서비스가 제공되고 있다. 향후 서비스를 준비하고 있는 3세대에는 많은 멀티미디어 서비스뿐 아니라 여러 가지 많은 서비스를 준비하고 있다. 그 중에서 사용자와 사용자간의 계약의 문제점, 사용자와 컨텐츠 제공자간의 과금에 대한 시간 및 내용에 대한 증명등 문제점이 발생할 수 있다. 이러한 문제점을 해결하고자 공증기관을 둔 공증서비스를 제안하였다. 이러한 공증서비스는 시점확인 서비스는 물론 내용 증명 서비스를 제공 할 수 있어 사용자가 기록에 대한 불확실성을 제기한다면, 공증기관으로부터 키를 제공받아 증거의 유효성르 증명할 수 있다.

본 논문에서는 향후 발전할 IMT-2000 서비스에서 일부의 서비스를 소개하고 있다. 이러한 여러 서비스들의 개발될 것으로 예상된다. 사용자에게 편리성과 안전성을 제공하는 여러 가지 서비스의 개발되어야 할 것으로 본다.

참고문헌

[1] 3GPP TS 23.002 v3.4.0 3GPP TSG SSA; *Network Architecture* (Relesase 1999) 2000.12.

[2] 3GPP TS 23.003 v3.7.0 3GPP TSG CN; Numbering, addressing and identification (Release 1999) 2000.12.

[3] 3GPP TS 25.413 v3.4.0 3GPP TSG RAN; UTRAN lu Interface RANAP Signaling (Release 1999) 2000.12.1

[4] 3GPP TS 25.921v3.2.0 3GPP TSG RAN; Guidelines and Principles for protocols and error handling (Release 1999) 2000.12.

[5] 3GPP TS 31.102 v3.4.0 3GPP TSG T; Characteristics of the USIM Application (Release 1999) 2000.12.

[6] 3GPP TS 33.102 v3.7.0 3GPP TSG SSA; 3G Security; Security Architecture (Release 1999) 2000.12.

[7] 3GPP TS 33.103 v3.4.0 3GPP TSG SSA; 3G Security; Integration Guidelines (Release 1999) 2000.10.