무선 통신에서의 키 분배 및 인증에 관한 연구

박 희 운† · 이 임 영††

요 약

최근 무선 이동 통신의 발전을 기반으로 향후 이동 통신 시스템은 많은 사용자들에게 현재보다 더 나은 고품질의 멀티미디어 서비스를 제공할 것으로 기대된다. 따라서 이와 관련된 많은 기술적 부분들이 고려되고 있으며, 특히 보안 관련 분야의 도입을 통해 기밀성 및 인전성을 획득하려 하고 있다

본 논문에서는 이와 관련하여 이동 통신상에서 발생 가능한 취약성들 및 요구사항들을 제시한다 동시에 이들 요구 사항에 근거하여 상호 인증 및 키 분배를 위한 call set-up 및 hand-off 프로토콜을 제안하고, 기존 방식들과 제안 방식을 비교 분석한다

A Study of Key Distribution and Authentication for Mobile Communication

Hee-Un Park† · Im-Yeong Lee††

ABSTRACT

Base on the development of mobile communication, the future mobile communication systems are expected to provide higher quality of multimedia services for users than today's systems Therefore, many technical factors are needed in this systems Especially the secrecy and the safety would be obtained through the introduction of the security for mobile communication.

In this paper, we presents weaknesses and propose required properties in mobile communication. Based on those proposed properties, we propose a new 'call set-up' and 'hand-off' protocol for authentication and key distribution Also we compare between the proposed scheme and conventional schemes

1. 서 론

정보화 사회의 발전을 통해 인간 문명 전반에 획기적인 변환의 시대가 도래하고 있다. 현대 사회의 정보화 현상은 산업 구조 및 사회 일반에 광범위한 컴퓨터의 보급 확산과 통신 서비스의 발전을 통해 확대되고 있다.

이 중에서 이동 통신 분야는 IT(International Telecommunication) 산업계에서 가장 빨리 성장하는 분야 중에 하나로서, 많은 사람들이 이동 통신 서비스를 통해 그 편리성과 유용성을 인지하고 있다. 일 예로, 1995년 유럽에서 이동 통신 사용자 수가 2,200만 명에서 2000년에는 11,000만 명에 이를 전망이다 기존의 2세대 이동 통신인 GSM과 DECT는 계속적으로 사용될 전망이며, 제 3세대 이동 통신인 UMTS는 2002년부터 유럽에서 상용화 될 전망이다. 이와 함께 세계 각국의 이동 통신 서비스의 발전을 바탕으로 그 수요는 계속 늘어날 전망이다[1-5]

이러한 이동 통신 발전의 이면에는 가입자들의 다양한 서비스가 요구되고 있다. 즉, 단순한 의사 교환의 범위를 넘어서 음성과 동영상 그리고 이들을 포괄해 인터넷과 같은 서비스까지 포괄적으로 요구되고 있다. 향후 멀티미디어 이동 통신 서비스가 제공된다면, 우

† 준 회 원 : 순천향대학교 대학원 전산학과
†† 정 회 원 : 순천향대학교 정보기술공학부 교수
논문접수 2000년 1월 25일, 심사완료 : 2000년 3월 16일

리는 단순 통화에서 전세계의 모든 정보를 값싸고 편리하게 이용하는 시대로 도약하게 될 것이다.

그러나 무선 이동 통신상에서 이와 같은 서비스들은 많은 문제점에 노출될 수 있다. 이동 통신에서 신호 교환은 무선 채널을 통해 대기 중에서 수행되므로, 도청자나 그 밖의 신뢰되지 못한 요소들로부터 위조나 불법적 변경 등과 같은 위협들에 대해서는 취약성을 지니고 있다. 이러한 위협의 범주에는 가입자 정보 수집 및 불법적 시스템 사용 등이 있다. 따라서 가입자를 제외한 다른 불법적 가입자들로부터 기밀성과 안전성을 확보하기 위해 암호 시스템의 연구가 활발히 진행되고 있다.

2 세대 이동 통신 시스템에서는 공중파 상에서의 기밀성, 사용자 익명성, 불법적인 단말기 사용을 방지하기 위한 대칭키 암호 기법들이 도입되어 사용되고 있다. 차세대 이동 통신으로 주목받고 있는 3세대 이동 통신의 경우 전일보하여 불법적인 제 3자의 도청 및 위조 방지를 수행하고 데이터의 무결성을 보장하기 위하여 인증성을 필수 요소로 삼고 있다. 이를 위해 현재는 공개키 암호화 기법을 자연스럽게 적용시키고 있는 추세이다.

이러한 암호 시스템에서 핵심적인 부분이 바로 '키 관리' 및 '인증' 분야이다. 즉, 아무리 암호화 시스템이 훌륭하다 하더라도 키가 노출되거나 교환이 정확하고 안전하게 수행될 수 없다면, 시스템은 불안전할 수밖에 없다. 또한 통신의 주체가 되는 사용자 및 단말기와 기지국이 불법적인 제 3자의 위법 행위로 인해 정당한 사용이 불가능하게 되는 것을 막기 위해 사용자 인증은 필수적일 것이다. 현재 이를 위한 많은 연구가 진행중이지만 아직 완벽한 해결책은 제시되고 있지 못한 상황이다.

본 논문에서는 무선 이동 통신 시스템 상에서 정보 보호를 위한 고려 사항을 살펴보고, 기존의 방식들이 이에 대해 어떻게 대처하는지 살펴볼 것이다. 또한 제시된 고려 사항들을 기초로 무선 이동 통신 인증 및 키 분배 메커니즘을 위해 Call Set-Up 프로토콜을 제시하고 안전한 Hand-Off 프로토콜을 제안할 것이다. 마지막으로 각 제안 방식에 대한 분석을 통해 안전성을 확인해 볼 것이다.

2. 고려 사항

2.1 정보 송/수신시 고려 사항

무선 통신상의 정보교환을 위해서 키 분배 및 인증, 사용자 인증 등이 필요하며 송/수신된 메시지에 대해 부인봉쇄를 수행할 수 있어야 한다. 또한 각 메시지는 제 3자의 불법적 도청을 방지하기 위하여 비밀성을 확보해야 한다. 다음은 이들에 대한 고려사항을 기술한 것이다.

(1) 인증성
- 사용자와 기지국 사이의 실체 및 세션키 인증이 필요하다.
- 메시지 인증을 통해 전송 정보의 불법적인 변경을 확인할 수 있어야 한다.

(2) 비밀성
- 통신시 송/수신되는 Call Set-Up 정보는 제 3자로부터 안전해야 한다.
- 송/수신 메시지는 불법적인 제 3자로부터 안전해야 한다.

(3) 부인 봉쇄
- 디지털 서명을 통하여 사용자가 전송한 메시지에 대한 부인 행위를 막을 수 있어야 한다.

2.2 무선 이동 통신상에서의 구성 요소에 대한 고려 사항

무선 이동 통신상에서 각 통신 주체의 역할 및 환경 구성에 있어 발생할 수 있는 위협에 대해 다음과 같은 보안 요소가 고려되어야 한다

(1) 안전성
- 각 가입자의 등록 정보가 MSC(Mobile Switching Center)의 DB에 저장되어 있을 경우, 제 3자의 가입자 정보에 대한 불법적 접속 및 유출이 방지되어야 한다

(2) 효율성
- 사용자 단말기의 한계를 고려하여 정보 계산량 및 패스의 수는 가능한 최소화되어야 한다.
- 공개키 사용시 기존의 유선에서 제공되는 X.509 인증서의 형식을 간소화함으로서 단말기의 부담을 줄여야 한다.

(3) 익명성
- 가입자의 위치는 허가된 실체 외에는 확인할 수 없어야 한다

2.3 키 생성 관련 요소에 대한 고려 사항

유선 통신과 마찬가지로 무선 통신상에서 메시지 안전성과 비밀성을 보장하기 위해서 키 생성을 위한 세심한 배려가 필요하다. 특히 이 부분은 인증 부분과 관련하여 무선 이동 통신 상에서 중요한 부분을 차지

하게 된다. 다음은 이에 관한 고려 사항을 기술한 것이다.

(1) 일회성(freshness)
- 사용되는 세션키는 매 통화시 각각 새로이 구성하여 인증을 수행함으로서 제 3자의 불법적 행위로부터 안전성을 획득해야 한다.

(2) 선택성
- 사용자가 키 생성 함수를 임의로 선택하게 함으로서 안전성을 높일 수 있어야 한다.

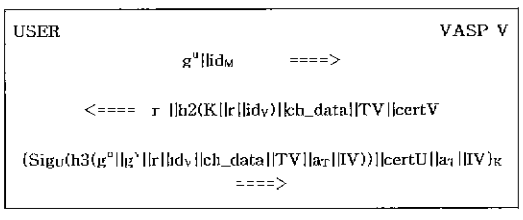
(3) Hand-Off 허용
- 이동 통신 가입자는 통화중 이동성을 가지고 있다는 특성을 가지고 있다. 이때 가입자가 새로운 셀(Cell) 범위로 진입할 경우, 새로운 기지국과 새로운 세션키를 통해 메시지를 송/수신해야 한다. 이를 위한 인증은 필수적이며 사용자 및 메시지에 대한 안전성 또한 확보되어야 하는데, 이러한 일련의 과정을 Hand-Off 과정이라 한다. 무선 통신에 있어 Hand-Off 허용 여부는 중요한 의미를 갖는다.

3. 기존 방식 분석

다음에서는 기존에 제시되고 있는 무선 이동 통신 키 분배 및 인증 방식에 대해 살펴본다. 키 분배에 있어 크게 3-way 방식 및 2-way 방식으로 구분될 수 있으며, 안전성 및 효율성 면에서 몇 가지 차이를 보이고 있다[6-9]

3.1 Hom & Preneel(H-P) 방식

이 방식은 3-way 방식을 이용하고 있다. 사용자가 최초 메시지를 전송하는 과정에서 암호화 과정이 없고, 기지국에서 이를 직접적으로 인증할 방법이 없다는 문제점을 안고 있는 방식이다. 또한, 사용자가 통신을 위해 2번의 통신 회수를 가지게 됨으로서 비효율적이다. 그러나 마지막으로 수신된 서명 메시지를 통해 인증을 수행하고 있다[6].



(그림 1) H-P 방식 흐름도

3.1 1 시스템 계수

본 방식은 다음과 같은 시스템 계수를 정의하고 있으며, 프로토콜 수행에 있어 필수적인 요소들을 설명한다.
- g : 생성지
- g^u : 랜덤한 u를 생성하여 계산된 사용자의 공개키
- id_M, id_V : 사용자와 기지국의 ID
- v : 기지국에서 생성하는 랜덤 값
- hx : 일방향 해쉬 함수 (x=1(부분 일방향 MAC 의사 랜덤 함수), 2(부분 일방향 MAC 함수), 3(충돌 회피성 함수))
- K = h1($(g^u)^v$||r) : 사용자와 기지국간에 생성되는 세션키(단, r은 기지국에서 생성하는 랜덤 값)
- ch_data : 지불 스킴 상의 입력에 필요한 부가 정보
- certy : 사용자 및 기지국의 공개키 인증서 (y = U, V)
- SigU 사용자의 서명
- TV : 사용자의 통신 요청이 접수된 시간
- a_T : 현재 사용자가 지불 가능한 과금의 총 범위
- IV : 사용자가 선택한 해쉬 함수의 종류

3 1.2 프로토콜

본 방식은 다음과 같이 수행된다. 사용자 각각은 두 번씩의 통신 접속을 수행하며, 기지국은 한 번의 통신 회수를 가지는 3-way 방식이다.

(1) 사용자
- 랜덤 수 u를 생성해 $g^u||id_M$을 V에게 전송한다. .

(2) 기지국
- 랜덤 수 r을 생성해 $(g^u)^v$를 계산하여, 다음과 같이 세션키를 생성한다.

$$K = h1((g^u)^v||r)$$

- 세션키 보유 확인을 위해 h2(K||r||id_V)를 계산
- 랜덤 값 r과 함께 자신의 공개키 인증서 certV. 지불 스킴 상에 필요한 부가 정보인 타임 스탬프(TV) 및 요금 관련 데이터 ch_data를 인접해 전송한다.

(3) 사용자
- 수신된 정보를 통해 세션키 K를 생성한다

$$K = h1((g^u)^v||r)$$

- 수신된 정보를 가지고 다음과 같이 해쉬를 수행함으로서 V가 세션키를 가지고 있음을 확인한다.

$$h2(K||r||idv)$$

- 지불 스킴과 관련된 정보를 생성한다.

$$a_T, IV$$

- 수신된 정보, 자신의 공개키, 지불 관련 정보에대해 해쉬 및 서명을 수행한 다음, 공개키 인증서 및 지불 정보를 연접해 K로 암호화하여 전송한다.

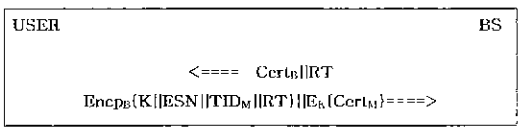
$$\{Sig_U(h3(g^u||g^v||r||idv||ch\_data||TV||a_T||IV)) ||certU||ar||IV\}_K$$

(4) 기지국

- certU를 확인한 다음, 사용자의 서명을 확인한다.
- 서명 및 향후 지불 스킴에 사용할 정보를 저장한다.

3.2 PACS 방식

이 방식은 2-way 방식을 적용하고 있다. 이 방식은 기지국에서 암호화 및 서명 없이 메시지가 전송되므로 인증, 비밀성 및 부인봉쇄가 불가능하게 된다. 동시에 기지국에서 암호화된 메시지 정보를 받는다 하더라도, 별도의 랜덤 값을 사용하지 않으므로 키 일회성은 획득할 수 없다는 단점을 가지고 있다. 다음은 이 방식에 대한 프로토콜을 기술한 것이다[8].



(그림 2) PACS 방식 흐름도

3.2.1 시스템 계수

본 방식에서 사용하는 시스템 계수는 다음과 같다

- $Cert_B$, $Cert_M$: 기지국 B 및 가입자 M의 공개키 인증서
- TID_M : 개체 M의 가명 식별자
- ID_B : 기지국 B의 식별자
- Enc_{PB} : B의 공개키
- RT : 기지국에서 생성하는 TimeStamp
- ESN : 사용자 단말기의 serial 번호
- $K = Sig_M\{RT||ID_B||TID_M||ESN\}$: 세션키

3.2.2 프로토콜

본 방식은 다음과 같이 수행된다 사용자 및 기지국 각각은 한 번씩의 통신 접속을 수행하므로 2-way 방식이다.

(1) 기지국

- 자신의 공개키에 대한 인증서와 TimeStamp를 연접해 사용자에게 전송한다.

$$Cert_B||RT$$

(2) 사용자

- 키를 다음과 같이 계산한다.

$$K = Sig_M\{RT||ID_B||TID_M||ESN\}$$

- 자신의 공개키에 대한 인증서에 세션키로 암호화를 수행한다

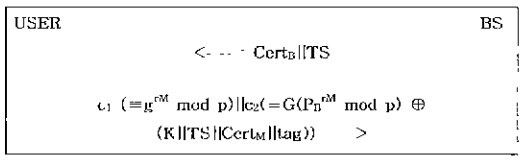
$$E_K\{Cert_M\}$$

- 세션키, 단말기 serial 번호, 가명 식별자 및 Time Stamp를 연접해 이를 기지국의 공개키로 암호화하여 세션키로 암호화한 결과를 연접해 전송한다.

$$Enc_{PB}\{K||ESN||TID_M||RT\}||E_K\{CertM\}$$

3.3 Zheng 방식

본 방식은 상기 방식과 마찬가지로 2-way 방식이다. 이 방식은 메시지 전송시 양자 모두 서명을 수행하지 않기 때문에 부인 봉쇄가 불가능하며, 키 일회성이 없다 또한 기지국에서 메시지 전송시 암호화 수행 과정이 없기 때문에 안전성과 사용자 인증이 불가능하다는 단점을 지니고 있다[9]



(그림 3) Zheng 방식 흐름도

3.3 1 시스템 계수

본 논문에서 제안한 방식은 다음과 같은 시스템 계수를 정의하고 있으며, 프로토콜 수행에 있어 필수적인 요소들을 설명한다.

- rM, xM 가입자가 생성하는 랜덤 수 및 비밀키 생성 요소
- G() 의사 랜덤 생성기
- g : 원시 원소
- $Cert_M$, $Cert_B$: 가입자 M 및 기지국 B의 공개키 인증서
- TS : 기지국에서 제공하는 Time-Stamp
- K : 세션키

- $P_B = g^{yB} \bmod p$ 기지국 B의 공개키
  (단, yB :공개키 구성 요소)
- $tag = hash(K||TS||Cert_M||(P_B^{xM+rM} \bmod p))$

3 3 2 프로토콜

본 방식은 다음과 같이 수행된다. 본 방식은 상기 방식과 마찬가지로 2-way 방식이다. 상기 방식과의 큰 차이점은 메시지 전송시 양자 모두 서명을 수행하지 않기 때문에 부인 봉쇄가 불가능하다는 것이다

(1) 기지국

- 자신의 공개키에 대한 인증서와 TimeStamp를 연접해 사용자에게 전송한다

$$Cert_B||TS$$

(2) 사용자

- 세션키 $K = P_B^{xM} \bmod p$를 생성한다.
- 랜덤 수 rM을 생성해 c_1 및 c_2를 다음과 같이 계산해 낸다.

$$c_1 = g^{rM} \bmod p$$
$$c_2 = G(P_B^{xM} \bmod p) \oplus (K||TS||Cert_M||tag)$$

- c_1 및 c_2를 연접해 기지국에 보냄으로서 키 생성 유무 및 자신을 인증한다.

4. 각 방식별 특성

4.1 특성 비교

상기 처음 방식은 무선 통신상에서 사용 가능한 3-way 방식의 키 분배 및 인증 방식을 제시하고 있다 나머지 두 방식은 2-way 방식의 키 분배 및 인증 방식을 제시하고 있다. 다음은 이들 방식의 특성을 분석한 것이다

4 1 1 H-P 방식

- 본 방식은 3-way 방식을 채택하고 있다. 이는 서명 수행에 따른 계산량의 분산을 통해 단말기의 부담을 줄이기 위해 수행되었으나, 통신 회수 측면에서 사용자의 부담을 가중시키고 있다.
- 본 방식은 (1), (2)에서 별도의 암호화를 수행하지 않기 때문에, 제 3자에 의한 위장이 가능하다.
- 키 생성시 H-P 방식은 Diffee-Hellman 방식을 사용하는 특징을 가지고 있다. 이를 통해 상대방을 인증할 수 있고, 생성된 키에 대해 인증성을 확보할 수 있다

4 1.2 PACS 방식 및 Zheng 방식

- 이들 방식은 2-way 방식을 채택함으로서, 사용자의 통신 회수 측면에 효율성을 높이고는 있지만, 기지국 인증 및 암호화 그리고 부인 봉쇄기 불가능하다는 문제점을 안고 있다.
- 2-way 방식들 모두가 기지국에서 메시지 전송시 암호화 기법을 사용하지 않고 있어 제 3자에 의한 위장을 통해 사용자가 불편을 겪을 수 있다

4.2 각 방식별 문제점

상기 방식들은 비슷한 암호학적 특성을 통해 안전성 및 효율성을 제공하고 있다. 그러나 다음 사항을 미세함으로서 문제점을 발생시키고 있다

4.2 1 H-P 방식

- 키 생성시 별도의 암호화가 수행되지 않으므로, 인증성이 결여되어 있다
- 기지국은 처음 수신된 메시지를 통해 누구와 통신하는지를 알 수 없다는 특징을 가지고 있다
- 본 방식에서 사용자는 수신된 정보를 통해 h2 (K||r||idv)를 계산한다 할지라도 V를 인증할 수 없게 되므로, 제 3자에 의한 위장이 가능하다.
- 본 방식은 사용자의 통신 회수가 2회가 되므로, 통신 이전에 시전 준비를 위한 사용자의 부담이 증가된다. 따라서, 효율성 측면에서 진혀 개선되지 않고 있다.
- 본 방식은 가입자의 식별자를 그대로 사용하고 있다. 이는 익명성을 해칠 수 있는 결과를 낳고 있다.

4 2 2 PACS 방식

- 본 방식은 키 생성시 랜덤 값을 사용하지 않으므로서 일회성이 없으며, 최초 정보 전송시 암호화 및 서명을 수행하지 않으므로서 기지국 인증 및 부인 봉쇄가 미흡한 단점을 가지고 있다 또한 사용자가 자신이 원하는 통신 함수를 선택할 수 없다는 문제점을 가지고 있다
- 본 방식은 가입자의 식별자를 그대로 사용하고 있다. 이는 익명성을 해칠 수 있는 문제점이 가지고 있다.

4.2 3 Zheng 방식

- 본 방식은 최초 정보 전송시 암호 및 서명 수행 과정이 없으므로, 기지국 인증 및 부인 봉쇄가 불

가능하다. 또한 키 생성시 랜덤 값 사용 부재로 일회성이 없으며, 사용자가 함수 선택권이 없다는 문제점이 있다.

- 본 방식은 가입 식별자를 그대로 사용하므로 익명성을 획득하지 못하고 있다.

또한 상기 세 가지 방식은 Hand-Off에 대해 고려하지 않음으로서 가입자의 이동성을 매제하고 있다.

5. 제안 방식

본 제안 방식은 사용자의 통신 효율성을 획득하기 위해 2-way 방식을 적용한다. 또한 상기 2장에서 고려되었던 사항들에 대해 만족할 수 있도록 하기 위해 각 메시지는 암호화되어 전송되며, 무인 봉쇄를 막고 인증성을 획득하기 위해 수신자 지정 서명을 수행한다[10]. 동시에 사용자의 이동성을 고려하여 Hand-Off 프로토콜을 별도로 제안한다. 이를 통해 통화 중에 새로운 셀(Cell)로 범위를 빗어날 경우, 새로운 기지국과 인증을 수행하고 새로운 키를 생성함으로서 지속적으로 안전한 통화를 보장받게 된다.

5.1 시스템 계수

본 방식에서 사용되는 시스템 계수는 다음과 같다.

- $ES_{ig_{BS\_M}}()$: 가입자(사용자)가 기지국에 전송하는 수신자 지정 서명
- SID_M : 가입자의 가명 식별 ID
- r_M : 세션키 생성을 위해 가입자가 생성하는 랜덤 값
- r_{Bi} : 세션키 생성을 위해 기지국이 생성하는 랜덤 값
- hash() : 160비트 출력을 내는 안전한 일방향 해쉬 함수
- T_i (i = 1, 2, ..., n) : 각 기지국 i에서 발행하는 Time-Stamp
- M : 가입자
- Bsi : i 기지국들
- SK : 가입자와 기지국에서 공동으로 생성하는 이동 통신 세션키
- DB_{otp} : 기지국만이 접근 가능한 2중 구조 One-Time Password DB 시스템
- OTP_{i1}, OTP_{i2} : DB_{otp} 접근 패스워드 및 세션키 복구 패스워드
- P_{BSi} : 각 기지국 i의 공개키
- P_{SIDM} : 가입자의 공개키
- E : *를 통해 암호화 수행
- $Sig_{BS}()$: 기지국에서 수행하는 서명
- CF(Choosing Function) 가입자가 선택 가능한 통신 함수

5.2 키 분배 및 Call-Set-Up 인증 단계

이 단계는 임의 지점 i에서 무선 이동 통신을 수행하기 위해 가입자(사용자)와 기지국 사이에 키 분배 및 인증을 수행하는 단계이다. 이 단계에서 가입자는 수신자 지정 서명 방식을 통하여 제 3자로부터 메시지의 비밀성을 제공하고, 오직 기지국만이 자신을 확인하게 함으로서 부인 봉쇄를 방지하고 있다[10]. 동시에 기지국은 MSC/AC(Mobile Switching Center/Authentication Center)와 실 시간적인 가입자 인증과 공개키 인증서를 교환한다. 또한 제안 방식은 2-way 방식을 사용하되 가입자가 먼저 자신의 정보를 제공함으로서 기지국 및 가입자 자신을 모두 인증할 수 있는 효율적인 방식이라 하겠다. 다음은 제안 방식에 대한 프로토콜을 기술한 것이다.

5.2.1 가입자의 통신 요청 및 인증 정보 전송

- 통신을 위한 인증 정보인 랜덤 수 r_M을 생성하여 자신의 가명 식별자 SID_M 및 가입자 함수 선택 값 CF를 연접(concatenation)한다. 이때 가명 식별자를 사용하는 이유는, 혹 불법적인 제 3자에게 자신의 정보가 노출된다 할지라도 자신의 개별 정보 및 위치 정보에 대한 안전성을 유지하기 위해서 사용된다.
- 연접된 정보를 기지국만이 수신 가능하도록 수신자 지정 서명을 수행한다. 여기서 사용되는 수신자 지정 서명 방식은 가입자 정보를 안전하게 기지국에 전달하는 역할을 할뿐 아니라, 기지국으로 하여금 수신된 정보의 정당한 가입자임을 기지국에 인증하고 부인봉쇄 역할을 담당한다.

$$ES_{ig_{BS\_M}}(SID_M||r_M||CF)$$

- 생성된 인증 정보를 전송함으로서 통신 요청이 발생한다.

5.2.2 기지국 i의 가입자 인증

- 기지국 i는 자신의 비밀키 또는 랜덤 수를 통해 서명 정보를 복호화 한 다음 등록된 가입자의 가명 식별자를 MSC/AC에게 의뢰하고 CF를 전송한다. 이때 CF를 MSC/AC에게 전송하는 이유는 사용자 이동성을 고려하여, Hand-Off시 새로운 기지국이 정확한 통신 함수를 선택하도록 도움을

주기 위해서이다.

$SID_M||r_M||CF$ => SID_M 및 CF를 MSC/AC에게 전송

- MSC/AC에서는 각 가입자의 신원 정보를 DB로 저장하고 있으며, 전송된 가명 식별자와 가입된 실명 확인을 통해 정당한 통신 주체임을 확인하게 된다

SID_M과 DB상의 ID_M 비교 확인

5.2.3 기지국 i의 인증서 확인 및 통신 세션키 생성

- 기지국 i에서는 MSC/AC로부터 전송된 가입자의 공개키 인증서를 수신 및 확인한다.

$Cert(P_{SIDM})$

- 수신된 정보 r_M과 Time-Stamp T_i 및 자신이 생성한 랜덤수와 공개키의 곱을 연접한다.

$r_M||T_i||(r_{Bi}*P_{BS_i})$

- 생성된 정보에 해쉬를 취하여 통신 세션키 SK_i를 생성한다.

$SK_i = hash(r_M||T_i||(r_{Bi}*P_{BS_i}))$

- 기지국 i에서는 OTP_{i1}로 DB_{otp}에 접속한 다음, SK_i를 OTP_{i2}로 암호화하여 저장한다. 이때 Hand-Off를 위하여 OTP_{i2}를 MSC/AC에 전송한다

5.2.4 기지국 i의 인증 정보 전송 및 무선 이동 통신 허가

- 기지국에서는 자신이 생성한 랜덤값 r_{Bi}와 Time-Stamp T_i 및 세션키 SK_i를 연접하여 자신의 서명을 수행한다.

$Sig_{BS_i}(r_{Bi}||T_i||SK_i)$

- 서명 정보와 자신의 공개키 인증서를 연접해 가입자의 공개키로 암호화해 전송한다. 이를 통해 가입자는 통신 허가를 받게 된다.

$EP_{SIDM}(Sig_{BS_i}(r_{Bi}||T_i||SK_i)||Cert(P_{BS_i}))$

5.2.5 가입자에 의한 기지국 인증 및 세션키 생성

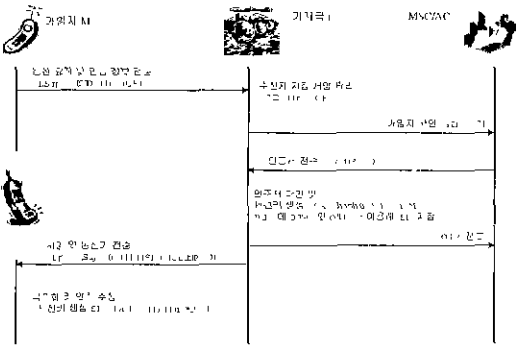
- 가입자는 자신의 개인키로 수신된 메시지를 복호화 한다. 그런 다음 기지국의 공개키 인증서 확인을 통해 정당성을 확보한다.

$Sig_{BS_i}(r_{Bi}||T_i||SK_i)||Cert(P_{BS_i})$

- 서명 확인을 통해 기지국을 인증하고 세션키를 생성한다

$SK_i' = hash(r_M||T_i||(r_{Bi}*P_{BS_i}))$

- 생성된 SK_i'과 SK_i가 동일하다면, 키 분배 및 Call-Set-Up 인증 과정은 끝난다.



(그림 4) 제안 방식 Call-Set-Up 흐름도

5.3 Hand-Off 인증 단계

무선 이동 통신의 특성 중에 하나가 이동 가능하다는 것이다. 이는 통화중에 가입자가 현재 기지국 셀의 범위를 벗어날 수 있음을 의미한다 따라서, 가입자가 새로운 셀로 범위를 이동할 경우, 새로운 기지국과 인증을 수행하고 새로운 키를 생성하기 위한 Hand-Off 인증 단계는 필수적이다. 이렇게 함으로서 새로운 기지국과의 키 분배 및 인증이 수행되고, 지속적으로 안전한 통화를 보장받게 된다. 다음은 Hand-Off 인증 단계에 대한 프로토콜을 기술한 것이다.

5.3.1 기지국 i+1의 인증서 확인 및 통신 세션키 생성

- MAC/AC에서는 가입자의 행동 경로에 따라 다음 기지국을 선정한 다음, 가입자의 공개키 인증서와 CF 그리고 OTP_{i2}를 전송한다.
- 기지국 i+1에서는 MSC/AC로부터 전송된 가입자의 공개키 인증서와 CF 및 OTP_{i2}를 수신 및 확인한다. 이를 통해 기지국 i+1에서는 통신 대상이 된 가입자 M을 인증할 수 있게 된다. 동시에 CF를 확인함으로서 통신시 사용될 함수를 확인하고, OTP_{i2} 및 자신의 $OTP_{(i+1)1}$을 통해 세션키 SK_i를 확인하게 된다.

$Cert(P_{SIDM})$, CF, SK_i

- 확인된 세션키 SK_i와 Time-Stamp T_{i+1} 및 자신이 생성한 랜덤수와 공개키의 곱을 연접한다.

$SK_i||T_{i+1}||(r_{Bi+1}*P_{BS_{i+1}})$

- 생성된 정보에 해쉬를 취하여 새로운 세션키 SK_{i-1}를 생성한다.

$$SK_{i+1} = hash(SK_i||T_{i+1}||(r_{Bi+1}*P_{BSi+1}))$$

5.3.2 기지국 i+1의 인증 정보 전송

- 기지국 i+1에서는 자신이 생성한 랜덤값 r_{Bi+1}과 Time-Stamp T_{i+1} 및 새로운 세션키 SK_{i+1}을 연접해 자신의 서명을 수행한다.

$$Sig_{BSi+1}(r_{Bi+1}||T_{i+1}||SK_{i+1})$$

- 서명 정보와 자신의 공개키 인증서를 연접해 가입자의 공개키로 암호화해 전송한다. 이를 통해 가입자는 통신 허가를 받게 된다

$$EP_{SII/M}(Sig_{BSi+1}(r_{Bi+1}||T_{i+1}||SK_{i+1})||Cert(P_{BSi+1}))$$

5.3.3 가입자에 의한 새로운 기지국 인증 및 세션키 생성

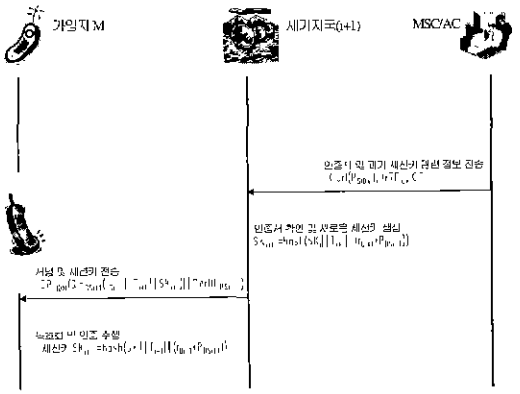
- 가입자는 수신된 정보를 자신의 개인키로 복호화한다. 그런 다음 기지국의 공개키 인증서 확인을 통해 정당성을 확보한다.

$$Sig_{BSi+1}(r_{Bi+1}||T_{i+1}||SK_{i+1})||Cert(P_{BSi+1})$$

- 서명 확인을 통해 기지국을 인증하고 새로운 세션키를 생성한다.

$$SK_{i+1}' = hash(SK_i||T_{i+1}||(r_{Bi+1}*P_{BSi+1}))$$

- 생성된 SK_{i+1}'과 SK_{i+1}이 동일하다면, Hand-Off 인증 과정은 끝나게 된다.



(그림 5) 제안 방식 Hand-Off 흐름도

5.4 제안 방식 분석

본 제안 방식은 수신자 지정 서명 방식을 도입한 2-way 방식을 적용했다. 또한 세션키 보호를 위해 2중 구조 One-Time Password 방식을 적용하였으며, 사용자의 이동성을 고려하여 Hand-Off 프로토콜을 별도로 제안하였다 이를 통해 다음과 같이 2장에서 언급하였던 고려 사항을 만족하고 있다

- 수신자 지정 서명 방식 도입
  이 서명 방식은 오직 지정된 수신자 즉, 기지국만이 전송된 정보를 확인 할 수 있게끔 하고 있다. 이는 기지국에서 정보 수신시 인증성과 비밀성 그리고 부인 봉쇄 특성을 만족하고 있다.

- 2-way 방식 적용
  기존 3-way 방식은 가입자로 하여금 통신 회수에 있어 비효율성을 유발시키고 있다. 이러한 측면에서 제안 방식은 효율성을 확보하고 있다.

- 가입자 가명 식별자 도입
  이 기법을 통해 가입자의 메시지가 불법적 제 3자에 의해 도청되더라도, 자신이 누구이며 어디에 존재하는지를 알 수 없게 함으로서 안전성과 익명성을 제공하고 있다.

- 가입자 및 기지국에서의 랜덤 값 생성
  매 통신시 랜덤 값을 각각 생성하여 세션 키 구성에 적용함으로서 일회성을 확보하고 있다

- CF 선택
  가입자가 자신이 무선 이동 통신시 사용할 통신 함수를 선택함으로서 선택성이 확보되고, 안전성을 높일 수 있다.

- Hand-Off 허용
  가입자가 새로운 셀로 범위를 벗어날 경우, 새로운 기지국과 인증을 수행하고 새로운 키를 생성하기 위한 Hand-Off 수행이 가능하다.

- 2중 구조 One-Time Password 방식 적용
  Hand-Off시 제 3자에게 노출될 위험이 있는 세션키의 안전한 전달이 가능하게 된다.

다음은 기존의 방식들과 제안 방식을 비교 분석한 것이다.

〈표 1〉 각 방식별 고려 사항 만족도 비교 분석표

항목 / 방식	H-P	I-M[K][7]	PACS	Zheng	제안방식
인증성	△/O	△/O	△/O	△/O	O/O
비밀성	△/O	△/O	△/O	△/O	O/O
무인통제	△	△	△	△	O
안전성	O	O	O	O	O
효율성	△(3-way)	O(2-way)	O(2-way)	O(2-way)	O(2-way)
익명성	△	△	O	△	O
일회성	O	O	X	X	O
선택성	O	X	X	X	O
Hand-Off 허용	X	X	X	X	O

주 Weakness, △ : normal, O : Good
인증성 실제 인증키 인증
비밀성 등록 정보 비밀성/메시지 비밀성

6. 결 론

현재 세계적으로 각광을 받고 있는 무선 이동 통신 서비스는 향후 더욱 발전하리라 판단된다. 그러나 무선 이동 통신 환경은 유선 통신 환경과는 매체 및 특성상 제약 사항이 많이 따르게 된다 이에 대해 본 논문에서는 디지털 이동 통신 시스템을 위한 고려 사항을 제시하였고, 이를 기초로 기존에 제시된 몇몇 방식들을 검토해 보았다 기존 방식들 중 몇몇은 실체 인증성이 결여되어 있었고, 서명 방식 도입 부재로 무인 봉쇄가 불가능한 경우가 발생하기도 하였다. 특히 Hand-Off를 고려하고 있지 않기 때문에 부분적으로 문제점을 노출시키고 있다.

본 논문에서는 이에 대해 디지털 이동 통신 시스템을 위한 키 분배 및 인증 방식을 제안하였다. 제안 방식은 2-way 방식을 적용하였으며, 수신자 지정 서명 방식을 도입하였다 그 외에도 가명 식별자 도입, 세션 키 생성을 위한 랜덤 값 생성, 사용자 통신 함수 선택을 위한 CF 전송, Hand-Off 허용 및 2중 구조 One-Time Password 방식 적용 등을 통하여 고려 사항을 충분히 만족하고 있다.

향후 더욱 효율적이고 안전한 무선 이동 통신을 위해 제안 분야의 추가적인 연구가 진행되어야 할 것이며, 특히 각국 및 세계적인 표준화에 적용 가능하도록 확대되어야 할 것이다.

참 고 문 헌

[1] ETSI ETS GSM 02.09. "European Digital Cellular Telecommunications System(Phase 2) ; Security Aspects." Version 4.2.4, September 1994.

[2] ETSI ETS 3000175-7, "DECT Common Interface, Part 7 . Security Features," October 1992

[3] UMTS Forum. "A regulatory framework for UMTS," Report No. 1, 1997.

[4] ETSI ETR 33.20, "Security Principles for the Universal Mobile Telecommunications System (UMTS)." Draft 1, 1997

[5] ITU, "Security Principles for Future Public Land Mobile Telecommunication Systems," Rec ITU-R M 1078.

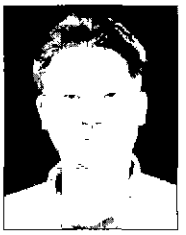
[6] G. Horn and B. Preneel, "Authentication and Payment in Future Mobile Systems," Proceedings ESORICS '98, LNCS 1485, J.-J. Quisquater, Y. Deswarte, C. Meadows, D. Gollmann, Eds, Springer-Verlag, pp.277-293, 1998.

[7] K H. Lee, S. J Moon, W Y. Jeong and T. G Kim, "A 2-pass Authentication and Key Agreement Protocol for Mobile Communications," Pre-Proceedings of ICISC '99, pp 143-155, 1999

[8] JTC(air)/94 12.15-119Rc, "Personal Communications Services," PACS Air Interface Specification, PN3418

[9] Y Zheng, "An authentication and security protocol for mobile computing," proceedings of IFIP, pp.249-257, 1996.

[10] S J Kim, S. J. Park and D. H. Won, "Nominative Signatures," Proc. ICEIC '95, pp.II-68-II-71, 1995.



박 희 운

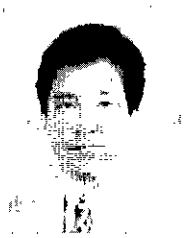
e-mail : hecun@ai-cse.sch.ac.kr

1997년 순천향대학교 전산학과 졸업

1997년~1999년 순천향대학교 전산학과 대학원 졸업 (공학 석사)

1999년~현재 순천향대학교 전산학과 박사과정 재학중

관심분야 : 암호이론, 컴퓨터 보안



이 임 영

e-mail : imylee@asan.sch.ac.kr

1981년 홍익대학교 전자공학과 졸업

1986년 일본 오오사카대학 통신공학과(석사)

1989년 일본 오오사카대학 통신공학과(박사)

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현재 순천향대학교 정보기술공학부 부교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안