GSM 시스템에서 부분적 익명성을 위한 사용자인증 프로토콜의 변형

정회원 박 미 옥*, 김 상 근*

Modification of User Authentication Protocol for Partial Anonymity in the GSM System

Mi-og Park*, Sang-geun Kim* ***Regular Members***

요 약

GSM(Global System for Mobile communications)은 전 세계에서 가장 대표적인 이동통신 표준으로서, 모바일 사용자들에게 이동성과 함께 편리성을 제공한다. 그러나 GSM 시스템은 사용자인증과정 중 MS(Mobile Station)의 IMSI(International Mobile Subscriber Identity)값이 노출되어 사용자를 정상적으로 인증할 수 없는 문제를 가지고 있다. 본고에서는 이러한 인증문제를 해결하기 위해 기존의 GSM 사용자인증 프로토콜에 기본을 둔 변형 메커니즘으로서, IMSI 값을 HLR(Home Location Register)로부터 암호화하여 전송함으로써 IMSI값의 노출을 막고, HLR에 의해 검증된 네트워크 개체만이 IMSI값을 사용하도록 하여 안전한 사용자인증을 제공한다. 또한 제안 메커니즘에서는 임시 아이디를 이용하여 사용자의 익명성을 제공할 뿐만 아니라, 기존의 GSM 사용자인증 프로토콜의 새로운 VLR과 이전의 VLR 간의 구조를 변경하지 않고 단계를 축소하여 빠른 사용자인증을 제공한다.

Key Words : user authentication, partial anonymity, TMSI allocation, GSM

ABSTRACT

GSM(Global System for Mobile communications) provides mobile users with portability and convenience as the most popular standard for mobile phones in the world. However, GSM system has the problem that can't normally authenticate a user by the exposure of IMSI(International Mobile Subscriber Identity) of Ms(Mobile station) during the user authentication procedure. In this paper, we propose secure user authentication by preventing the exposure if IMSI via transfer the encrypted IMSI from the HLR(Home Location Register) and making the only network entities verified from the HLR use the IMSI value, as the modified mechanism based on the original user authentication protocol to solve this authentication problem. Also the proposed mechanism provides fast user authentication without changing the architecture between new VLR and old VLR in the original GSM user authentication protocol as well as user's anonymity by using a temporary ID.

Ⅰ. 서 론

디지털 이동통신은 시간과 장소의 제약을 받지 않고 음성 및 데이터 서비스를 제공하여 모바일 사용자에게 많은 편리함을 제공한다. 그러나 전파를 통신매체로 사용하기 때문에 통화도용과 같은 문제점을 가지고 있으며, 이러한 통화도용은 요금징수와 관련하여 통신 사업자에게는 수익의 감소와 서비스

* 성결대학교 컴퓨터공학과 (mopark777@hanmail.net, sgkim@sungkyul.edu)
논문번호 : KICS2005-10-438, 접수일자 : 2005년 10월 27일, 최종논문접수일자 : 2006년 5월 8일

제공에 대한 불안을 주고, 사용자에게는 요금체계와 통화에 대한 불신감을 초래하며 더 나아가 사용자의 프라이버시에 심각한 피해를 줄 수 있다. 그러므로 이를 방지하기 위한 보안서비스의 제공은 필수적 사항이 되었다. GSM 보안기능은 크게 두 가지 목적을 가지고 있다. 하나는 인증되지 않은 접근으로부터 네트워크를 보호하는 것이고, 다른 하나는 사용자의 프라이버시를 보호하는 것이다. 그래서 GSM의 보안특성은 사용자인증, 사용자 위치 프라이버시(location privacy), 그리고 무선상의 시그널정보(signal information)로 구성된다. 그러나, GSM 시스템은 VLR(Visited Location Register)과 VLR 간의 통신 그리고 VLR과 HLR간의 통신에 암호화 방식을 사용하지 않기 때문에, 도청자는 HLR에 연결된 채널을 모니터링하여 IMSI와 같은 인증정보를 획득함으로써 사용자인증 문제가 발생한다.

사용자인증에 대한 많은 연구들이 이루어져왔으며, Harn과 Lin[1]은 GSM 시스템에서 VLR에 저장되는 민감한(sensitive) 정보의 양을 축소하기 위한 메커니즘을 제안했고, Lee[2]는 GSM 시스템의 전반적(global) 구조를 위한 보안 메커니즘을 제안하였다. 여기서 전반적 구조란 임의의 HLR과 다른 HLR간의 보안 메커니즘을 의미하는 것으로서, 그는 HLR들간의 네트워크상의 기밀성과 키생성 메커니즘을 제안하였다. 그러나, 대부분의 논문들은 전반적 구조가 아닌 MS와 HLR간의 보안 메커니즘만을 다루고 있으며, 본고에서도 MS와 HLR간의 메커니즘만을 다룰 것이다. [1, 3]에서는 빠른 사용자 인증을 위해 인증프로토콜의 절차를 축소했지만, 기존의 GSM 인증프로토콜의 구조를 변경해야 하는 단점이 존재한다. 또한 사용자인증 문제를 해결하기 위한 대부분의 논문에서는 안전한 인증을 위한 다양한 해결책들이 제안되고 있는 반면 날로 증가하는 중요한 개념인 사용자 프라이버시를 위한 익명성(anonymity)에 대한 해결책은 거의 제안되고 있지 않다. Molva, Samfta, 그리고 Tsudik[4]가 익명성을 위한 사용자인증 메커니즘을 제안하였지만, KryptoKnight에 기본을 두고 있기 때문에 GSM에서 사용하는 기존의 알고리즘과 구조에 많은 변화의 오버헤드를 요구한다. 본고에서는 기존의 GSM 비밀키 암호시스템에 기본을 둔 부분적(partial) 익명성, VLR 인증 등의 장점을 제공하는 메커니즘을 제안할 것이다.

본고의 구성은 다음과 같다. 2장에서 GSM의 사용자인증 프로토콜을 설명하고, 그에 대한 문제점을 제시한다. 3장에서는 사용자인증 문제해결을 위해 임시 아이디(Temporary Identity, TID)에 기본을 둔 변형된 사용자인증 프로토콜을 제안한다. 4장과 5장에서는 기존의 메커니즘들과의 비교·분석을 통해 제안 메커니즘의 효율성을 보이고 결론을 내린다.

Ⅱ. 관련 연구

2.1 사용자인증 프로토콜

GSM에서 사용자인증은 암호화키 분배과정과 함께 수행되며 IMSI가 네트워크에 알려지고, 채널이 암호화되기 전에 수행된다. 사용자인증 과정은 그림 1과 같으며, 그림 1에서 VLRn은 MS가 새롭게 방문한 VLR을 의미하고, VLRo는 이전에 방문한 VLR을 의미한다. AuC(Authentication Center)는 HLR안에 포함되어 있다고 가정한다.

MS는 새로운 VLR에게 TMSI(Temporary Mobile Subscriber Identity)와 LAI(Location Area Identity)를 전송하여 자신의 존재를 알린다. 새로운 VLR은 이전의 VLR에게 MS가 전송해온 TMSI와 LAI를 전송하여 MS의 IMSI값을 되돌려 받는다. 새로운 VLR은 MS의 신원을 인증받기 위해 IMSI를 HLR에게 전송한다. HLR은 자신의 비밀키(subscriber authentication key) Ki와 128비트의 난수 RAND값을 입력으로 하는 A3알고리즘을 수행하여 인증 서명값 SRES와 암호화키 Kc를 계산한 후 인증 파라미터 (RAND, SRES, Kc)를 새로운 VLR에 전송한다. 이 때, 전송되는 세 개의 파라미터 (RAND, SRES, Kc)는 triple이라고 하며 n개의 복사본이 전송된다. 새로운 VLR은 이 n개 중에서 한 쌍의 triple을 선택하고, 선택된 triple에서 RAND값만 MS에게 전송한다. 새로운 VLR로부터 RAND값을 전송받은 MS는 자신의 비밀키 Ki와 전송받은 RAND을 입력하여 A3알고리즘을 수행한 후, SRES를 생성하여 새로운 VLR에 전송한다. 새로운 VLR은 자신이 저장하고 있는 SRES와 MS로부터 전송받은

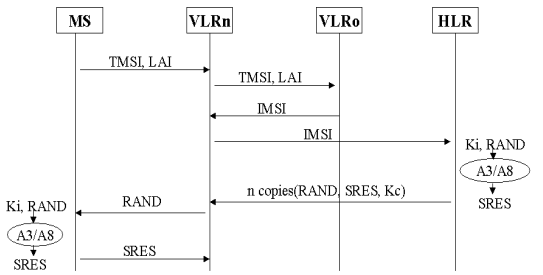

그림 1. GSM의 사용자인증 프로토콜

SRES를 비교하여 두 개의 값이 동일하면 MS를 정당한 개체로 인증하여 다음 서비스를 계속한다. 만약 값이 동일하지 않으면, MS의 인증은 실패한 것으로서 세션은 종료된다[5, 6].

2.2 사용자인증 프로토콜의 문제점

MS를 인증하기 위한 GSM의 사용자인증 프로토콜은 다음과 같은 문제점들이 존재하여[7, 8], 정당한 사용자를 안전하게 인증할 수 없다.

- VLR과 VLR간 그리고 VLR과 HLR간의 통신에 암호화 방식을 사용하지 않기 때문에, 인증정보인 IMSI가 노출되어 사용자인증 문제를 초래한다.
- GSM은 시도-응답 메커니즘을 사용하여 MS만을 인증하는 단일인증(unilateral authentication) 방식을 제공한다. 그래서 VLR의 신분이 검증되지 않아 제 3자가 합법적인 네트워크 개체로 가장할 수 있다.
- VLR은 MS를 인증할 때마다 MS의 HLR에게 n개의 새로운 인증 파라미터 (RAND, SRES, Kc)를 요청해야한다. 하나의 VLR안에 존재하는 모든 MS들은 n개의 인증 파라미터를 가지고 있고, 이 인증 파라미터들은 VLR의 데이터베이스에 저장되기 때문에 n개의 인증 파라미터를 저장하기 위한 공간 오버헤드가 발생한다.
- VLR은 MS를 인증할 때마다 n개의 인증 파라미터를 전송하기 때문에 VLR과 HLR간의 대역폭 소비가 발생한다.

Ⅲ. 변형된 사용자인증 프로토콜

3.1 부분적 익명성을 위한 제안 메커니즘

제안 메커니즘은 부분적 익명성과 안전한 사용자 인증을 위해 TID를 사용한다. 본고에서, 부분적 익명성이란 제안된 사용자인증 프로토콜의 모든 절차의 7단계에서 익명성이 보장되는 것이 아니라 IMSI를 사용하기 위한 네트워크 개체가 인증되기 전까지만 사용자의 익명성이 보장되는 것을 의미한다. TID는 IMSI 대신에 사용자를 인증할 수 있는 부가적인 인증 파라미터로서, IMSI와 일대일로 매핑되며 MS의 HLR에서 유일한 값이어야 한다. TID와 IMSI값의 관계는 HLR만 알고 있는 비밀정보이어야 한다. 그러나, 파라미터 TID 자체는 공개정보이다. TID의 생성은 MS의 HLR만이 가능하며, 사용자는 등록과정에서 비밀키 Ki, IMSI, 그리고 TID를 함께 제공받는다.

제안 메커니즘은 A3, A5, A8알고리즘을 기본으로 하며 수행절차는 다음과 같다.

1단계. MS는 TMSI, LAI, 타임스탬프 T를 새로운VLR에게 전송한다.

2단계. 새로운 VLR은 MS의 TID를 얻기 위해 TMSI와 LAI를 이전의 VLR에게 전송한다.

3단계. 이전의 VLR은 자신의 데이터베이스에서 TMSI와 LAI에 일치하는 TID를 탐색한 후, 일치하는 TID가 존재하면 그 값을 새로운 VLR에게 전송한다. 만약, 일치하는 TID가 존재하지 않으면 세션은 이 단계에서 종료된다.

4단계. 새로운 VLR은 TID, T, VLR의 아이디 VLR_ID, SRES1을 HLR에게 전송한다. SRES1는 VLR과 HLR간에 공유하는 비밀키 K_{VH}와 T를 A3의 입력으로 사용하여 계산된다.

5단계. 새로운 VLR로부터 파라미터를 전송받은 HLR은 VLR_ID가 합법적인 VLR인지 그리고 T가 변경되었는지를 조사한다. VLR_ID가 합법적이면, HLR은 VLR_ID에 해당하는 비밀키 K_{VH}를 알고있기 때문에 새로운 VLR을 인증하기 위해 A3알고리즘을 사용하여 SRES1'를 계산한다. 만약 전송받은 SRES1과 자신이 계산한 SRES1'이 동일하면, HLR은 새로운 VLR을 정당한 개체로 믿고, VLR의 인증서 Auth_VLR과 임시키 TKi를 계산한다. TKi는 (Ki, RAND)와 (Ki, T)를 A3에 각각 입력하여 출력된 두 결과 값을 XOR하여 계산한다. Auth_VLR는 A3의 입력으로 Ki와 RAND를 사용하여 Auth_VLR를 계산한다. TKi를 생성한 후에, HLR은 전송받은 TID에 매핑되는 IMSI값과 TKi를 사용하여 E_{VH}(IMSI, TKi)를 계산한다. E_{VH}는 VLR과 HLR간에 공유되는 비밀키를 사용하여 암호화함

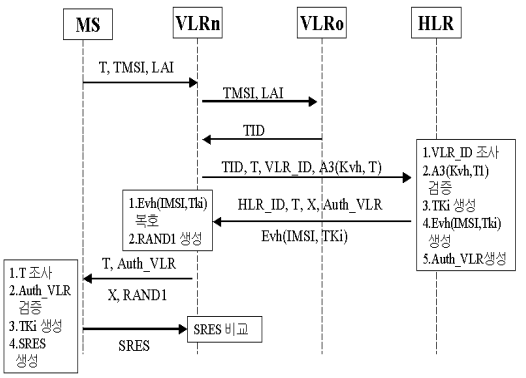

그림 2. 제안된 사용자인증 프로토콜의 절차

을 의미한다. HLR은 HLR의 아이디 HLR_ID, T, X, Auth_VLR, 그리고 E_{VH}(IMSI, TKi)를 새로운 VLR에게 전송한다.

6단계. 새로운 VLR은 HLR_ID를 확인하여 이 아이디에 해당하는 비밀키 K_{VH}를 찾아낸 후, E_{VH}(IMSI, TKi)를 복호화하여 IMSI와 TKi값을 추출한다. VLR은 다음 호의 인증을 위해 새로운 난수 RANDj만을 생성한다. 다시 말하면 MS가 동일한 VLR의 영역에 있는 동안, VLR은 MS를 인증하기 위한 새로운 인증 파라미터를 HLR에게 요청할 필요 없이 VLR 자신이 각 j번째 호를 위한 새로운 RANDj를 생성하여 MS를 인증한다. 그래서, 새로운 VLR은 자신이 생성한 새로운 난수 RAND1과 HLR로부터 전송받은 T, X, Auth_VLR를 MS에게 전송한다.

7단계. MS는 T값의 변경여부를 조사하여 값이 변경되지 않고 자신이 보낸 이전의 T값과 동일하면, VLR의 정당성 검증을 위해 X와 T를 XOR하여 RAND값을 계산한 후, Auth_VLR'를 HLR에서 계산한 것과 동일한 방식으로 계산한다. MS가 계산한 Auth_VLR'과 전송받은 Auth_VLR값이 동일하면, VLR을 정당한 개체로 믿고 TKi를 생성한다. MS와 새로운 VLR간의 임시키 TKi가 생성되면, 새로운 VLR에서 전송받은 RAND1을 A3알고리즘의 입력으로 사용하여 계산된 결과값 SRES를 새로운 VLR에게 전송한다. 새로운 VLR은 MS로부터 전송받은 SRES와 자신이 계산한 SRES'값을 비교하여, 두 값이 동일하면 MS를 정당한 개체로 인증하고, 그렇지 않으면 MS의 인증은 실패하여 세션을 종료한다.

3.2 절차가 축소된 제안 메커니즘

제안 메커니즘은 절차를 축소한 기존의 다른 메커니즘들처럼 인증절차를 축소할 수 있다. 절차를 축소한 두 번째 메커니즘은 3.1절에서 제안된 메커니즘에 기본을 두고 있다. 이 메커니즘의 기본개념은 대부분 첫 번째 제안 메커니즘과 동일하나, 그림 3에서 보듯이 크게 두 가지 다른 점이 있다. 하나는 첫 번째 단계에서 MS의 전송 파라미터에 TID가 첨가되는 것이고, 두 번째 다른 점은 첫 번째 제안 메커니즘의 2와 4번째 단계를 두 번째 제안 메커니즘에서는 동시에 수행하는 것이다. 그래서 두 번째 제안 메커니즘의 3과 5번째 단계는 2와 4번째

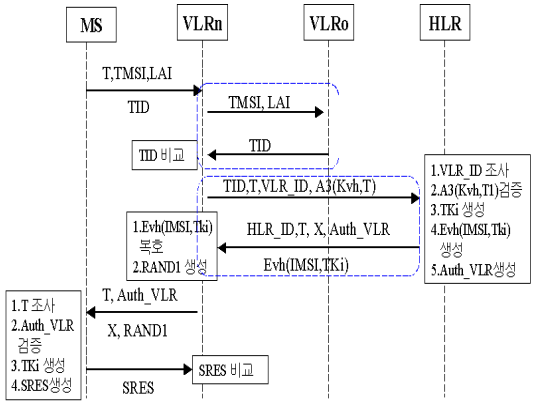

그림 3. 절차축소된 사용자인증 프로토콜의 절차

단계가 완료되면 곧바로 동시에 수행된다. 다시 말하면, 새로운 VLR은 3단계에서 이전의 VLR로부터 TID값이 전송되는 것을 기다릴 필요 없이 1단계가 끝난 후에, MS가 새로운 VLR에게 보낸 TID를 HLR에게 곧바로 전송한다. 이러한 처리가 가능한 이유는 새로운 VLR이 1단계에서 MS가 보낸 TID를 이미 가지고 있기 때문에, 이전의 VLR이 MS의 TID를 전송할 때까지 기다릴 필요가 없게 된다. 그림 3의 박스 처리된 부분은 동시 수행되는 과정을 나타낸 것으로, 위의 박스는 첫 번째 제안 메커니즘의 2와 3번째 단계를 아래 박스는 첫 번째 제안 메커니즘의 4와 5번째 단계를 나타낸다.

두 번째 제안 메커니즘의 절차는 다음과 같다.

1단계. MS는 TID, TMSI, LAI, T를 새로운 VLR 에 전송한다.

2단계. 2-1단계와 2-2단계는 동시에 수행된다. 여기서, 2-1단계와 2-2단계는 첫 번째 제안 메커니즘의 2단계 그리고 4단계와 각각 동일하다.

3단계. 3-1단계와 3-2단계는 동시에 수행된다. 여기서, 3-1단계와 3-2단계는 첫 번째 제안 메커니즘의 3단계 그리고 5단계와 각각 동일하다.

4단계. 첫 번째 제안 메커니즘의 6단계와 동일하다.

5단계. 첫 번째 제안 메커니즘의 7단계와 동일하다.

Ⅳ. 비교분석

4.1 암호학적 분석

제안 메커니즘은 GSM의 알고리즘에 기본을 두고 있기 때문에, 제안 메커니즘의 비도는 GSM의 A3, A5, A8알고리즘의 비도에 의존한다.

• 재생(replay) 공격

MS와 VLR은 타임스탬프 T와 T1을 사용하였기 때문에, 제 3자가 재사용한다 할지라도 값이 올바르지 않기 때문에 재생공격은 성공할 수 없다. 그러므로 제안 메커니즘은 재송공격에 안전하다.

• 안전한 사용자인증

첫 번째 제안 메커니즘의 3단계와 두 번째 제안 메커니즘의 3-1단계에서 TID를 전송하기 때문에, IMSI값 노출은 전혀 없으며, 5단계와 3-2단계에서는 IMSI를 암호화하여 전송하므로 IMSI값이 노출되는 문제를 해결하여 안전하게 사용자를 인증한다.

• TID의 안전성

HLR만이 TID와 IMSI값의 일대일 매핑관계를 알고 있고, TID값 자체는 공개정보이기 때문에 TID를 이용한 IMSI값의 유추공격에 안전하다.

• HLR에 의한 VLR의 인증

GSM과 대부분의 기존 메커니즘들은 VLR을 인증하지 않고 MS의 인증권한을 부여했기 때문에 안전성에 큰 문제점을 야기할 수 있다. 제안 메커니즘에서 새로운 VLR은 HLR로부터 검증받은 후, 인증이 성공하면 IMSI값을 사용할 수 있다. 그러므로 검증받지 않은 아무 개체에게나 IMSI값과 같은 중요정보가 그대로 노출되는 문제점을 해결할 수 있다. 또한, 제안 메커니즘에서 VLR은 검증받은 후에만 다음 서비스를 제공받을 수 있어 비밀키 Ki의 노출 위험성은 그만큼 낮아지게 된다.

• MS와 VLR간의 상호인증

MS 인증은 기존의 단일 인증방식을 활용하고, VLR 인증은 HLR로부터 전송된 Auth_VLR를 검증하여 수행된다. Auth_VLR은 A3를 사용하기 때문에 VLR 인증을 위한 새로운 알고리즘이 필요 없어 인증수행의 오버헤드는 아주 작다. 또한, 제 3자가 Auth_VLR에 대한 공격에 성공하려면, HLR과 MS간의 비밀키 Ki를 분석해야만 한다.

• VLR의 인증권한에 의한 Ki값의 안전성

VLR은 HLR로부터 부여받은 인증권한을 위해 HLR로부터 전송받은 TKi를 MS와 VLR간의 공유키로 사용한다. TKi값의 생성은 비밀키 Ki로부터 유도되고, VLR은 Ki값을 모른 상태에서 MS의 인증이 가능하여 Ki값의 노출위험은 없다.

4.2 기존 메커니즘들과의 비교분석

• 부분적 익명성

대부분의 메커니즘들은 익명성을 거의 제공하지 않고 있다. 그러나 제안 메커니즘은 TID를 사용하여 VLR이 HLR에게 인증되기 전 단계까지 IMSI값이 노출되지 않기 때문에, 부분적 익명성이 제공된다. 또한, TID는 공개정보이기 때문에 새로운 VLR과 이전의 VLR간에 암호화를 했던 기존 메커니즘들과 달리 제안 메커니즘은 VLR간의 통신에 암호화가 필요 없는 장점을 제공한다.

• 일차적 인증과 이차적 인증

첫 번째와 두 번째 제안 메커니즘의 3단계와 3-1단계는 TID에 의해 MS를 일차적으로 인증하고, 4단계와 3-2단계는 T와 MS의 인증서에 의해 이차적 인증을 수행한다. 일차적 인증은 이전의 VLR에 의해 자신의 데이터베이스에 저장된 TMSI와 LAI에 일치하는 TID의 존재여부에 따라, 존재하면 정당한 MS라고 인증하게 된다. 인증이 실패하면 세션은 이 단계에서 종료되어 다음 단계까지 계속 처리되는 부담을 줄일 수 있고, 공격을 더 빨리 차단할 수 있다. 그러나 일차적 인증은 모두 공개정보와 암호화 과정을 사용하지 않기 때문에 불안전하며 이차적 인증과정에 의해 안전한 MS의 인증이 수행된다.

• 구조변경 없는 절차축소

절차를 축소한 기존의 메커니즘들은 대부분 GSM 인증절차의 3단계인 새로운 VLR에서 이전의 VLR간의 절차를 없애고 새로운 VLR에서 곧바로 HLR로 IMSI값을 전송하여 기존의 7단계를 5단계로 축소하였다. 그래서 3단계의 절차변경에 의해 기존의 GSM 인증프로토콜의 구조가 변경된다. 그러나 두 번째 제안 메커니즘은 2와 4단계, 3과 5단계를 동시에 수행함으로써, 기존 프로토콜의 구조변경 없이 절차수를 감소하여 빠른 인증뿐만 아니라 다음 서비스도 빠르게 제공할 수 있는 장점을 가진다.

• VLR에 의한 MS의 인증

HLR 대신에 VLR이 MS 인증을 수행하는 과정은 매번 HLR에 의해 수행되는 MS의 인증부담을 줄일 수 있다. 또한, 제안 메커니즘에서는 기존 메커니즘들과는 달리 VLR이 MS의 인증권한을 부여받기전에 HLR로부터 검증받기 때문에 VLR에 의한 인증권한의 남용 위험성은 아주 작다.

• 대역폭 소비의 감소

MS가 임의의 한 VLR의 영역에 계속 머무르는 동안, VLR은 MS를 인증하기 위해 새로운 인증 파라미터를 HLR에 다시 요청할 필요가 없다. 기존의 메커니즘에서는 MS를 인증하기 위해 각 호마다 n개의 새로운 인증 파라미터를 HLR에 요청하여 다시 전송받는다. 그러므로 기존 메커니즘들과 비교할 때, VLR과 HLR 사이의 시그널 처리량이 축소된다.

표 1.기존 메커니즘들과의 비교

특성	GSM	Ⅰ	Ⅱ	[2]	[5]	[11]
상호인증	×	○	○		○	×
대역폭 축소	×	○	○	○	×	○
VLR저장공간의 축소	×	○	○	○	×	○
VLR간의 암호화 필요성	×	×	×	○	○	○
부분적 익명성	×	○	○	×	×	×
IMSI 할당주체	VLR	HLR	HLR	VLR	VLR	VLR
인증된 후 IMSI사용	×	○	○	×	×	×
절차수의 감소	-	×	○	○	○	×
구조변경	-	×	×	×	○	×
이차적 사용자인증	-	×	○	×	×	×

• VLR 저장공간의 축소

n개의 인증 파라미터가 하나의 인증 파라미터로 감소되기 때문에 VLR에 저장되는 데이터양도 감소되어 저장공간을 효율적으로 이용할 수 있다.

표 1은 기존 메커니즘들과의 비교결과로서, Ⅰ과 Ⅱ은 제안된 두 개의 각 메커니즘을 나타낸다.

Ⅴ. 결 론

본고에서는 IMSI값의 노출로 인한 GSM의 사용자인증 문제해결을 위해 TID를 사용한 변형된 메커니즘을 제안하였다. 제안 메커니즘은 기존 메커니즘들의 장점뿐만 아니라, 부분적 익명성과 이중의 사용자 인증 등을 제공하여 사용자를 안전하게 인증하였다. 또한, HLR은 VLR을 인증한 후에만 인증권한을 부여하였고 검증받은 VLR만 MS의 IMSI값을 사용할 수 있기 때문에, 검증받지 못한 네트워크 개체들의 정보의 접근이나 사용권한을 제어할 수 있고, 두 번째 제안 메커니즘은 기존의 GSM 인증 프로토콜의 구조를 변경하지 않는 장점을 제공한다.

참 고 문 헌

〔1〕 Harn, L., Lin, H.Y, "Modification to enhance the security of the GSM protocol," *Proceedings of the 5th National Conference on Information security*, Taipei, Taiwan, pp. 416-420, May 1995.

〔2〕 Chii-Hwa Lee, Min-Shiang Hwang, Wei-Pang Yang, "Enhanced privacy and authentication for the global system for mobile communications," *Wireless Networks*, Vol.5, No.4, pp. 231-243, May 1999.

〔3〕 AL-TAWIL, L., AKRAML, A., YOUSSEF, H., "A new authentication protocol for GSM networks," *Proceedings of IEEE 23rd Annual Conference on Local computer networks*(LCN'98) pp. 21-30, 1998.

〔4〕 Molva, R., Samfat, D., Tsudik G., "Authentication of mobile users," *IEEE Network*, Vol. 8, Issue 2, pp. 26-34, 1994.

〔5〕 D.Broron, "Techniques for privacy and authentication in personal communication systems," *IEEE personal communications*, pp. 6-10, August 1995.

〔6〕 J.E. Willas, "Privacy and authentication needs of PCS," *IEEE personal communications*, pp. 11-15, August 1995.

〔7〕 Lee C.C., Hwang M.S., Yang, W.P., "Extension of authentication protocol for GSM," *IEE Proceedings. Communications*, 150(2), pp. 91-95, 2003.

〔8〕 K.Chae, M. Yung, "A Location Privacy Protection Mechanism for Smart Space," *WISA* 2003, LNCS 2908, pp. 162-173, 2004.

박 미 옥 (Mi-og Park) 정회원

1991년 2월 조선대학교 전산 통계학과 졸업

1993년 2월 숭실대학교 컴퓨 터학과 석사

2004년 8월 숭실대학교 컴퓨 터학과 박사

2005년 3월~현재 성결대학 교 컴퓨터공학부 전임강사

<관심분야> 이동통신보안, 전자상거래, RFID

김 상 근 (Sang-geun Kim) 정회원

1987년 2월 중앙대학교 전자 계산학과 졸업

1991년 2월 중앙대학교 전자 계산학과 석사

1996년 2월 중앙대학교 컴퓨 터공학부 박사

1996년 3월~현재 성결대학 교 컴퓨터공학부 부교수

<관심분야> 유비쿼터스 네트워크, 통신 소프트웨어, 인터넷