Journal of Korea Multimedia Society Vol. 9, No. 10, October 2006(pp. 1314-1321)

강력한 개체인증 특성을 가지는 GSM 사용자 인증 프로토콜

박 미 옥[†], 김 상 근[††]

요 약

GSM(Global System for Mobile Communications)은 전 세계 이동통신 네트워크상의 와이드스프레드 로밍과 개인휴대통신을 지원하는 전 유럽 디지털 셀룰러 모바일 시스템이다. 그러나 보안기능 제공에도 불구하고, GSM에는 사용자인증과 같은 문제점들이 존재한다. 본고에서는 사용자인증문제 해결을 위해 각 네트워크 개체를 강력하게 인증하고 사용자의 프라이버시를 위해 익명성을 제공하는 향상된 사용자인증 메커니즘을 제안한다.

GSM User Authentication Protocol with Property of Strong Entity Authentication

Mi-Og Park[†], Sang-Geun Kim[††]

ABSTRACT

GSM(Global System for Mobile Communications) is a Pan-European digital cellular mobile system supporting widespread roaming and personal communication services in a worldwide wireless communication network. In spite of providing security capability, however, there are some problems like user authentication in GSM. In this paper, we propose the enhanced authentication mechanism to verify strongly each network entity to solve user authentication problem and support anonymity for user privacy.

Key words: Authentication(인증), Anonymity(부분적 익명성), TMSI Allocation(TMSI 할당), GSM, Location Privacy(위치 프라이버시)

1. 서 론

GSM은 가장 대표적인 디지털 이동통신 표준으로서, 전 세계에 수많은 가입자를 보유하고 있다. 또한 GSM은 사용자 인증, 데이터 무결성, 사용자 위치 프라이버시, 그리고 무선상의 시그널 정보 등을 위해 보안기능을 제공한다. 그러나, GSM은 VLR(Visited Location Register)과 VLR간의 통신 그리고 VLR과 HLR(Home Location Register)간의 통신에서는 암호화 방식을 채택하고 있지 않기 때문에, 도청자는 HLR의 물리적 채널을 모니터링하여 임의 정보를 획득할 수 있고, 결국 통화도용이나 사용자프라이버시와 같은 문제에 직면하게 되어 사용자와 서비스 공급자 모두 피해를 입게 된다. 안전한 GSM 사용자인증에 대한 다양한 연구들이 이루어져왔으나[1][2][3], GSM의 비밀키 암호시스템에 기본을 두면서 MS(Mobile Station)와 VLR를 모두 인증하면서 강력한 개체인증방법을 제안한 연구는 매우 드물다. 본고에

※ 교신저자(Corresponding Author) : 박미옥, 주소 : 경기도 안양시 만안구 안양 8동 산147-2(430-742), 전화 : 031-467-8926, FAX : 031-467-8067, E-mail : mopark777@hanmail.net

접수일 : 2006년 5월 2일, 완료일 : 2006년 9월 6일

[†] 정회원, 성결대학교 컴퓨터공학부 전임강사
[††] 정회원, 성결대학교 컴퓨터공학부 부교수
(E-mail : sgkim@sungkyul.edu)

서는 GSM의 비밀키 암호시스템에 기본을 둔 사용자 익명성과 네트워크상의 각 개체를 강력한 인증방법을 사용하여 검증함으로써 기존의 여러 메커니즘들보다 안전한 사용자인증 프로토콜을 제안한다.

본고의 구성은 2장에서 기존의 사용자인증 프로토콜과 문제점을 설명하고, 3장에서 문제해결을 위한 강력한 사용자인증 메커니즘을 제안한다. 4장에서는 제안메커니즘의 암호학적 분석과 기존 메커니즘들과의 비교·분석을 제시하고, 5장에서 결론을 내리고 본고를 마친다.

2. GSM 사용자인증 프로토콜

2.1 사용자인증 프로토콜

GSM 사용자인증 프로토콜은 다음과 같이 동작한다. 먼저, MS는 새로운 VLR에게 TMSI(Temporary Mobile Subscriber Identity)와 LAI(Location Area Identity)를 전송한다. 새로운 VLR은 전송받은 TMSI와 LAI를 이전의 VLR에 전송하고, 이전의 VLR은 TMSI와 LAI에 일치하는 IMSI (International Mobile Subscriber Identity)값을 찾아 새로운 VLR에게 전송한다. 새로운 VLR은 IMSI를 HLR에게 전송하고, HLR은 MS와의 비밀키 Ki와 난수 RAND값을 입력으로 하는 A3를 수행하여 인증서명값 SRES와 암호화키 Kc를 계산한 후, n개의 (RAND, SRES, Kc)를 새로운 VLR에 전송한다. 새로운 VLR은 이 n개 중 선택한 triple에서 RAND값만 MS에게 전송한다. MS는 자신의 비밀키 Ki와 전송받은 RAND를 입력으로하여 A3를 수행하여 SRES를 생성한 후 새로운 VLR에 전송한다. 마지막 단계로, 새로운 VLR은 자신이 계산한 SRES와 MS로부터 전송받은 SRES를 비교하여 두 값이 같으면 MS 인증을 성공시키고, 그렇지 않으면 실패한 것으로 처리하여 세션을 종료한다.

2.2 사용자인증 프로토콜의 문제점

GSM 사용자인증 프로토콜에는 다음과 같은 문제점들이 존재한다[4,5].

- 새로운 VLR과 이전의 VLR간의 통신 그리고 VLR/HLR간의 통신에 암호화방식을 사용하지 않기 때문에, 도청자는 HLR의 채널을 통해 MS의 IMSI나 위치갱신 정보와 같은 중요한 정보를 쉽게 획득할 수 있다.

- 사용자인증 프로토콜은 MS 단일인증만 지원할 뿐 VLR인증은 지원하지 않기 때문에, 제 3자가 합법적인 네트워크 개체로 가장하는 것이 가능하다.

- 새로운 VLR은 n개의 인증파라미터를 모두 소비할 경우, n개의 새로운 인증파라미터를 HLR에 다시 요청하기 때문에 VLR/HLR간의 대역폭이 소비된다.

- VLR은 하나의 MS당 n개의 인증파라미터를 저장하기 때문에 VLR의 저장공간 오버헤드가 발생한다.

- VLR은 모든 인증파라미터 소비시, HLR에 새로운 인증파라미터를 요구하기 때문에, VLR은 MS를 인증할 때 항상 HLR의 도움을 필요로 한다.

- IMSI값의 노출로 인해 제 3자는 정당한 사용자의 프라이버시, 통화도용, 더 나아가 서비스 공급자 모두에게 피해를 줄 수 있다.

3. 제안된 사용자인증 메커니즘

3.1 강력한 사용자인증 메커니즘

• 익명성

제안메커니즘은 사용자 프라이버시를 위해 TID (Temporary Identity)를 사용한다. TID의 사용은 기존의 사용자인증 프로토콜의 단계3에서 IMSI를 전송하는데 반해, 제안 메커니즘의 단계3에서는 TID를 전송하며, 새로운 VLR이 IMSI를 획득하기 위해 자신의 신분이 HLR에 의해 인증된 후에만 사용가능하다. TID는 IMSI대신에 MS를 인증할 수 있는 부가적인 인증파라미터로서, HLR안에서 유일한 값이어야 한다. 또한, TID 생성은 MS가 새로운 VLR에 방문시 처음 한번만 생성되며, TID 자체는 공개정보이다. 사용자는 첫 번째 등록과정에서 Ki, IMSI, 그리고 TID를 할당받으며, 그 다음의 새로운 TID값들은 제안메커니즘의 사용자인증 과정을 통해 할당받는다. MS가 최초로 방문하는 VLR은 초기 TID를 가지고 있지 않기 때문에, MS로부터 인증요청을 받으면 곧바로 HLR과 통신하는 것으로 가정한다.

• 강력한 개체인증

본고에서 인증권한부여란 VLR이 HLR대신 MS를 인증하는 기능을 의미하는 것으로서, 이 기능을

위해 새로운 VLR은 HLR로부터 공유비밀키 TKi를 전송받는다. TKi는 HLR이 생성된 난수 $RAND_H$와 MS가 생성한 타임스탬프 T1, 그리고 MS의 새로운 임시아이디 TIDn을 XOR한 후, 그 결과값을 HLR/MS간의 비밀키 Ki와 함께 A3로 입력함으로써 계산된다. 또한 인증권한을 부여받은 VLR은 MS가 동일한 VLR의 영역에 계속 머무르는 동안, MS인증을 위해 각각의 j번째 호를 위한 하나의 RANDj만을 생성한다. 난수생성은 안전한 난수생성기를 사용한다고 가정한다.

제안메커니즘은 세 개의 인증서를 사용해 각 개체의 강력한 인증기능을 제공한다.

- $AUTH_M$

MS는 HLR에게 자신이 정당한 개체임을 증명하기 위해 MS인증서 $AUTH_M$을 사용한다. $AUTH_M$은 MS에서 생성한 T1과 HLR로부터 전송받은 $RAND_M$, 자신의 임시아이디 TIDo, 그리고 IMSI를 XOR한 후, 그 결과값을 자신의 비밀키 Ki와 함께 A3에 입력함으로써 생성된다.

- $AUTH_V$

$AUTH_V$는 VLR신분을 검증하기위한 VLR인증서로서, MS가 생성한 T1, VLR이 생성한 T2와 RANDv, 그리고 VLR 아이디 VLR_{ID}를 XOR한 후, 그 결과값을 비밀키 K_{VH}와 함께 A3에 입력함으로써 생성된다.

- $AUTH_{HM}$

HLR은 새로운 VLR이 HLR대신 MS를 인증하는 정당한 개체라는 사실을 MS에게 알리기 위한 방법으로 $AUTH_{HM}$을 사용하며 본고에서 이 $AUTH_{HM}$은 인증권한부여서라고 명한다. $AUTH_{HM}$의 생성은 $RAND_H$와 T1, TIDn, 그리고 HLR 아이디 HLR_{ID}를 XOR한 결과값과 비밀키 Ki를 가지고 A3를 수행함으로써 계산된다.

제안메커니즘의 수행과정은 [그림 1]과 같고, VLRn은 새로운 VLR을, VLRo는 이전의 VLR을 의미하며, VLR/HLR간의 통신은 secure channel로 가정한다.

단계1) MS는 타임스탬프 T1을 생성하고, HLR로부터 전송받아 저장해둔 난수 $RAND_M$, 자신의 임시아이디 TIDo, 그리고 IMSI를 XOR하여 $AUTH_M$을 계산한 후, T1, TIDo, HLR_{ID}, TMSI, LAI, $AUTH_M$을 새로운 VLR에게 전송한다. $RAND_M$은 이전의 MS인증단계에서 HLR이 MS에 전송해 준 파라미터로서, MS에서 저장하고 있는 값이다.

단계2) 새로운 VLR은 이전의 VLR에게 TMSI와 LAI를 전송한다.

단계3) 이전의 VLR은 TMSI와 LAI에 일치하는 TIDo를 자신의 데이터베이스에서 조사한 후, 일치하는 TIDo와 그에 따른 IMSI값이 존재하면, TIDo값을 새로운 VLR에게 전송한다. 만약, 일치하는 TIDo와 그에 따른 IMSI값이 존재하지 않으면 세션은 종료된다.

단계4) 새로운 VLR은 난수 RANDv와 타임스탬프 T2를 생성하여 전송받은 T1, 그리고 자신의 아이디 VLR_{ID}와 XOR연산 후, $AUTH_V$를 생성하여 MS에서 전송받은 TIDo, T1, $AUTH_M$과 함께 VLR_{ID}, T2, RANDv, $AUTH_V$를 HLR에게 전송한다.

단계5) HLR은 전송받은 VLR_{ID}와 TIDo을 사용하여 각각에 일치하는 VLR 아이디와 MS의 현재 TIDo의 존재여부를 조사한 후, 두 파라미터에 각각 일치하는 아이디가 존재하면, VLR과 MS의 검증을 수행한다. 먼저, MS인증을 위해 전송받은 T1, TIDo, 그리고 MS인증서 생성을 위해 이전에 생성·저장해둔 난수 $RAND_M$과 IMSI값을 XOR하여 $AUTH_M$'을 계산한다. 만약 전송받은 $AUTH_M$과 $AUTH_M$'의 값

표 1. 제안메커니즘의 시스템 계수

파라미터	정 의
TIDo, TIDn	MS의 이전 임시아이디와 새로운 임시아이디
T1, T2	MS와 VLR이 생성한 각각의 타임스탬프
$RAND_V$, RAND	VLR이 생성한 난수들
$RAND_M$, $RAND_H$	HLR이 생성한 난수들
K_{VH}	HLR과 VLR간의 비밀키
TKi	MS와 VLR간의 공유비밀키
VLR_{ID}, HLR_{ID}	VLR과 HLR의 각 아이디
X1, X2	X1은T1⊕T2⊕TIDn의 결과값 X2은 T1⊕TIDn의 결과값
$AUTH_M$	MS가 생성하는 MS의 인증서
$AUTH_V$	VLR이 생성하는 VLR의 인증서
$AUTH_{HM}$	HLR이 생성하는 인증권한부여서

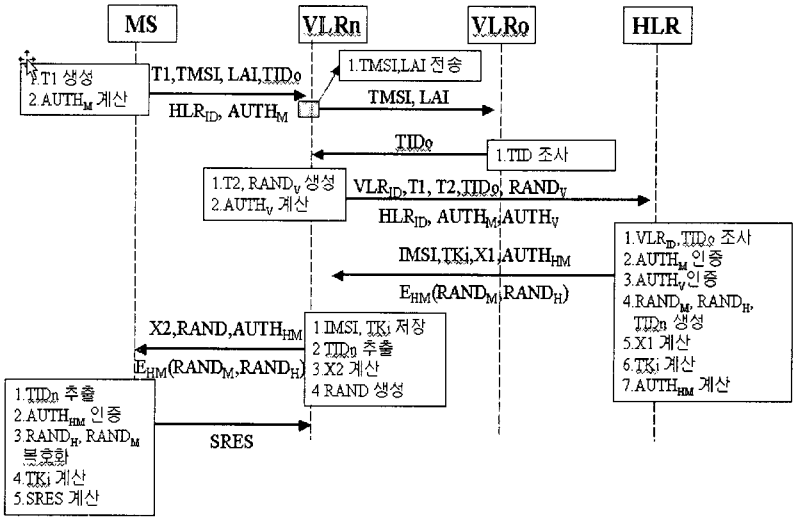

그림 1. 강력한 사용자인증의 수행과정

이 일치하면 MS인증이 성공하여 VLR의 인증을 수행한다. VLR인증은 전송받은 VLR_{ID}에 일치하는 아이디에 의해서 VLR과의 비밀키를 알 수 있기 때문에, 전송받은 T1, T2, RANDv, VLR_{ID}를 XOR한 후, VLR과의 비밀키 K_{VH}를 사용하여 VLR인증서 $AUTH_V'$을 계산한다. 자신이 계산한 $AUTH_V'$값과 전송받은 $AUTH_V$값이 일치하면, HLR은 VLR이 정당한 개체임을 믿고, 새로운 난수 $RAND_H$와 $RAND_M$, 그리고 새로운 TIDn을 각각 생성한 후, 전송받은 T1, T2, TIDn를 XOR하여 X1을 계산한다. 이와 동시에 T1, $RAND_H$, TIDn를 XOR한 후 VLR과의 임시비밀키 TKi를 계산하여, VLR의 인증권한부여서 $AUTH_{HM}$을 계산하고, $RAND_M$과 $RAND_H$를 MS와의 암호화키로 암호화하여, 자신의 아이디 HLR_{ID}, X1, $AUTH_{HM}$, IMSI, TKi, 그리고 E_{HM} ($RAND_M$, $RAND_H$)를 새로운 VLR에게 전송한다.

단계6) 새로운 VLR은 전송받은 IMSI와 TKi를 저장한 후, T2와 T1을 알고 있기 때문에 두 값을 X1과 XOR하여 TIDn을 추출하여 저장하고, T1과 추출한 TIDn을 XOR하여 X2를 계산한다. 그런 다음, 새로운 난수 RAND를 생성하여, X2, $AUTH_{HM}$, E_{HM}($RAND_M$, $RAND_H$)과 함께 MS에게 전송한다.

단계7) MS는 T1과 X2를 XOR하여 새로운 TIDn 값을 추출하여 저장한 후, VLR정당성 확인을 위해 $AUTH_{HM}$를 계산한다. $AUTH_{HM}$의 생성규칙에 의해 자신이 계산한 $AUTH_{HM}'$이 전송받은 $AUTH_{HM}$과 동일하면, MS는 VLR을 정당한 개체로 믿고 $RAND_H$를 복호화하여 T1, TIDn과 XOR하여 TKi를 계산한 후, 전송받은 RAND를 A3의 입력으로 사용하여 SRES를 계산하여 새로운 VLR에 전송한다. 전송받은 $RAND_M$은 HLR과의 다음번의 인증을 위해 저장해둔다. 새로운 VLR은 A3에 TKi와 RAND를 입력한 결과값 SRES'과 전송받은 SRES값을 비교한다. 두 값이 동일하면, MS인증은 성공이고, 그렇지 않으면 MS인증은 실패하여 세션은 종료된다.

3.2 빠른 사용자인증 메커니즘

본 절에서는 제안 메커니즘의 단계를 변형한 빠른 사용자인증 메커니즘을 제안한다. 빠른 사용자인증 메커니즘은 첫 번째 제안메커니즘의 단계의 일부를 동시에 수행함으로써 인증단계를 축소한다. 이 메커니즘의 근본적 원리는 첫 번째 제안메커니즘과 모두 동일하며, 단계축소 방법은 다음과 같다. 두 번째 제안메커니즘은 첫 번째 제안메커니즘의 단계2와 4를 동시에 수행한다. 그러므로 두 번째 제안메커니즘의 단계3과 5는 단계2와 4가 완료되면 곧바로 동시에 수행가능하다. 다시 말하면, 새로운 VLR은 단계3에서 이전의 VLR로부터 TIDo값이 전송되는 것을 기다릴 필요 없이 단계1이 끝난 후에, MS가 새로운 VLR에게 보낸 TIDo를 HLR에게 곧바로 전송한다. 이러한 처리가 가능한 이유는 새로운 VLR이 단계1에서 MS가 보낸 TIDo를 이미 가지고 있기 때문에,

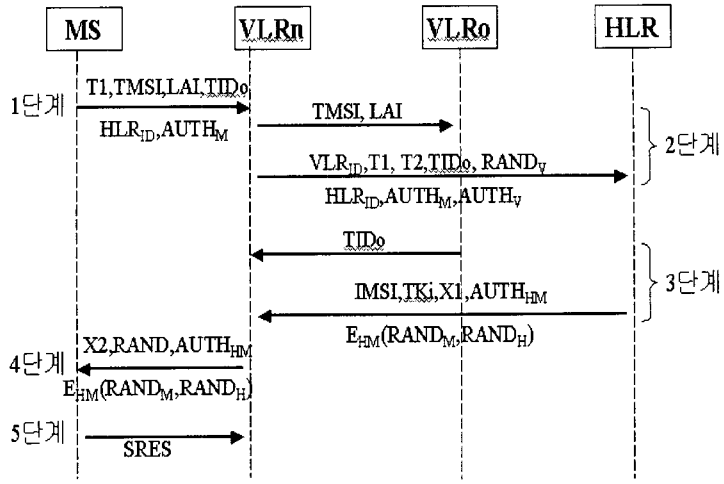

그림 2. 빠른 사용자인증의 수행과정

이전의 VLR이 MS의 TIDo를 전송할 때까지 기다릴 필요가 없게 되기 때문이다. 그러므로 빠른 사용자인증 메커니즘의 동작원리는 [그림 2]와 같이 나타낼 수 있으며, [그림 2]에서 2와 3단계의 표시 부분은 첫 번째 메커니즘의 두 단계가 동시에 수행됨을 의미한다.

4. 제안메커니즘의 분석

4.1 암호학적 분석

제안메커니즘의 비도는 A3, A8, 그리고 A5 알고리즘의 비도에 의존한다.

- 안전한 사용자 인증

IMSI값이 전송되는 두 제안메커니즘의 단계5와 3은 VLR/HLR간의 secure channel를 통해 전송되기 때문에, GSM의 단계3에서 IMSI 노출에 의한 사용자 인증문제를 해결할 수 있다. 더욱이 제안메커니즘에서는 인증받은 개체만이 HLR로부터 IMSI값을 전송받기 때문에, 임의 개체에게 IMSI값이 노출되는 것을 막을 수 있다.

- TID로부터의 IMSI의 안전성

TID는 비도가 안전한 난수생성기를 사용하여 HLR에 의해 랜덤하게 생성되고 IMSI값과 어떤 관계도 존재하지 때문에, TID에 의한 IMSI값의 유추공격에 안전하다. 또한 TID 생성은 MS가 새로운 VLR을 방문할 때마다 새롭게 생성되기 때문에, TID와 IMSI값간의 매핑관계는 MS가 새로운 VLR에 머무르는 동안만 안전하게 유지하면 되기 때문에, 매핑관계의 비밀유지에 대한 많은 부담을 줄일 수 있다.

- 재생(replay) 공격

제안메커니즘에서 MS와 VLR은 각각 타임스탬프 T1과 T2를 사용하고, 이 타임스탬프들은 각 인증서생성을 위해 사용한다. 그러므로 제 3자가 T1, T2, $AUTH_M$, $AUTH_V$값을 획득한다할지라도, 현재 값과 획득한 값은 동일한 값이 아니기 때문에 재생공격을 막을 수 있다.

- MS와 VLR의 상호인증

제안메커니즘의 단계6과 7에서 VLR과 MS는 동일한 비밀키 TKi를 사용해 동일한 SRES를 생성함으로써, MS와 VLR인증을 수행한다.

- TKi로부터 Ki의 안전성

VLR은 MS의 인증권한을 위해 HLR로부터 전송받은 TKi를 MS와 VLR간의 공유키로 사용한다. TKi는 비밀키 Ki로부터 유도되고, VLR은 Ki값을 모른 상태에서 MS의 인증이 가능하기 때문에 제 3자로부터 Ki값의 노출위험은 아주 작다고 할 수 있다.

- 강력한 개체인증

제안메커니즘의 강력한 개체인증은 각 인증서의 생성방법과 각 개체의 인증방법의 두 가지 측면으로 구별할 수 있다. 먼저 각 인증서의 생성방법을 살펴보면 다음과 같다. 대부분의 기존 메커니즘에서 MS와 VLR을 인증할 경우 또는 VLR에게 MS의 인증권한을 부여할 경우, VLR인증서는 A3(K_{VH}, T)나

	GSM	기존 메커니즘들		제안메커니즘
MS인증	-	A3(Ki, RAND)		A3(Ki, T1⊕$RAND_M$⊕TIDo⊕IMSI)
VLR인증	-	인증서 비사용시 의 전송파라미터	-.VLR_{ID}, T, IMSI -.VLR_{ID},E_{VH}(IMSI),T	A3(Kvh, T1⊕T2⊕RANDv⊕VLR_{ID})
		인증서 사용시 인증서 생성방법	-.A3(Kvh, T) -.A3(Kvh, RANDv)	
인증권한 부여	-	A3(Ki, RAND)		A3(Ki, T1⊕$RAND_H$⊕TIDn⊕HLR_{ID})

A3(K_{VH}, $RAND_V$)의 형태로 생성하거나, 단순히 VLR을 신뢰하는 개체로 가정만하고 인증하지 않는 메커니즘들도 다수이다. 그러나 제안메커니즘에서는 각 인증서 $AUTH_M$과 $AUTH_V$, 그리고 인증권한 부여서 $AUTH_{HM}$의 생성에서 보듯이, 각 개체가 생성한 타임스탬프, 각 개체의 아이디, 그리고 각 개체에 의해 생성된 난수들이 포함되어 계산된다. 그러므로 이 3가지 종류의 파라미터의 값들에 대해 각 개체가 동일한 값을 가지고 있는지, 그리고 이 값들을 이용한 각각의 인증서계산 결과가 동일한지를 비교함으로써 보다 강력한 개체인증을 제공한다. 또한 인증서에 사용된 각각의 난수와 아이디는 생성개체가 각각 다르기 때문에 부인봉쇄를 제공할 수 있다. VLR 인증서는 $AUTH_V$에서 자신이 생성한 타임스탬프 T2와 MS가 생성한 T1까지 사용하기 때문에, MS와 VLR까지도 모두 정당한 경우에만 올바른 인증서를 생성할 수 있어 보다 안전한 인증기능을 제공해 준다. 제 3자가 현재의 인증단계에서 사용하는 T1값을 획득했다 하더라도 단계1에서 $AUTH_M$의 생성에 $RAND_M$을 사용하기 때문에 Ki값이 노출되지 않는 한 계속해서 새롭게 생성되는 $RAND_M$값을 획득할 수 없어 올바른 MS 인증서를 계산해 낼 수 없다. 그러므로 제안메커니즘에서는 각 개체의 비밀키와 VLR과 HLR에서 사용한 난수생성기를 분석해야만 공격이 가능하다. 그러나 안전한 난수생성기를 깨는 것은 쉽지 않다. 강력한 개체인증의 두 번째 측면인 각 개체의 인증방법은 이차적 인증기능을 의미한다. 제안메커니즘의 각 단계3은 이전의 VLR에 저장된 TMSI와 LAI에 일치하는 TID의 존재여부와 TID에 매핑되는 IMSI값이 저장되어있으면 MS를 일차적으로 인증한다. 두 제안메커니즘의 각각의 단계4와 2는 $AUTH_M$를 통해 MS를 검증함으로써 이차적 인증을 제공한다. 그러나 일차적 인증은 공개정보인 TID만 사용하기 때문에 이차적 인증에 비해 불안전하다. 기존 메커니즘에서는 일차적 인증과정이 없이 IMSI값이 곧바로 노출되지만, 제안메커니즘에서는 TID값만 전송되고 이 TID 파라미터는 공개정보이기 때문에 단계3에서 일차적 인증이 가능하다. 또한 이전의 VLR에 TID값이 존재하지 않으면 정당한 MS가 아니기 때문에 일차적 인증은 실패하여, 그 다음 단계까지 계속 처리되는 부담을 줄이고 공격을 더 빨리 차단할 수 있는 장점을 가진다.

- HLR의 VLR인증

VLR에게 MS를 인증할 수 있는 인증권한을 부여하는 대부분의 기존 메커니즘들은 VLR을 인증하지 않는다. 그러나 VLR인증없이 곧바로 인증권한을 부여하는 것은 시스템 안전성에 큰 문제를 야기할 수 있다. 제안메커니즘에서는 HLR이 VLR인증을 수행한 후 인증결과에 따라 그 다음 단계를 처리하기 때문에, 비밀키 K_{VH}가 노출되지 않는 한 인증받지 않은 아무 개체에게나 중요정보가 그대로 노출되는 문제점을 해결할 수 있다.

- VLR간의 통신의 안전성

제안메커니즘에서는 VLR간에 공개정보 TID를 전송하기 때문에, 단계2와 3의 VLR간 통신은 암호화 과정없이 안전한 통신을 제공한다.

- 부인봉쇄

MS인증서 $AUTH_M$의 구성요소인 $RAND_M$은 MS가 아니라 HLR에 의해 생성되고 암호화되어 전송되기 때문에, 정당한 MS와 HLR만이 $RAND_M$값을 알 수 있어 MS의 부인봉쇄를 제공한다. 또한 $AUTH_V$과 $AUTH_{HM}$에도 각 인증서생성 개체의 아이디가 모두 포함되어 계산되기 때문에, 다른 개체의 부인봉쇄도 제공할 수 있다.

4.2 기존 메커니즘과의 비교분석

- 익명성

GSM과 기존의 메커니즘에서는 IMSI값이 노출되어 사용자프라이버시에 큰 위험성이 존재할 뿐만 아니라, 비밀키 암호시스템에 기본을 둔 대부분의 기존 메커니즘에서는 프라이버시를 거의 제공하지 않고 있다. 제안메커니즘은 IMSI가 인증받은 개체에게만 안전채널을 통해 전송되고, 안전한 난수생성기를 사용해 IMSI와 TID의 매핑관계도 노출되지 않기 때문에 익명성이 보장된다. 단계4까지 사용자의 유일한 파라미터가 존재하지 않기 때문에 익명성이 보장된다. 단계5에서는 HLR에 의해 새로운 VLR이 인증받은 후, IMSI값을 획득함으로써 새로운 VLR에게 사용자의 익명성이 보장되지 않는다. 그러나 제안메커니즘에서는 MS가 새로운 VLR로 이동할 때마다 새로운 TID값을 HLR로부터 할당받기 때문에, 이전의 VLR은 MS의 IMSI값을 가지고 있다할지라도 IMSI값에 일치하는 TID값이 변경되어 올바른 사용자의 정보를 획득할 수 없기 때문에 이전의 VLR에게는 사용자의 익명성이 보장된다. 단계6 이후부터는 전송 파라미터가 MS자신과 이미 IMSI값을 알고 있는 새로운 VLR이기 때문에 앞 단계까지의 익명성보장과 동일하다. 그러므로 제안메커니즘은 HLR과 인증받은 후의 새로운 VLR만이 MS의 IMSI값을 알기 때문에, 나머지 개체나 제 3자에게 사용자의 익명성이 보장된다.

- 단계축소의 특이성

사용자인증과정을 축소한 기존의 대부분의 메커니즘들은 GSM 사용자인증 구조를 완전히 변경한 것과 달리 제안된 두 번째 메커니즘은 단계2와 4 그리고 단계3과 5를 동시에 수행함으로써 GSM 구조변경 없이 전체 사용자인증 단계를 축소하였다.

- $RAND_M$의 안전성과 오버헤드

제안메커니즘의 단계1에서 $AUTH_M$ 생성에 사용하는 $RAND_M$은 HLR에 의해 생성되므로, MS가 난수를 생성하는 기존 메커니즘에 비해 오버헤드가 작다. 또한 제안메커니즘은 난수를 매번 생성하는 기존 메커니즘들과 달리 MS가 새로운 VLR에 방문한 처음 한번만 HLR에 의해 생성되기 때문에 HLR에서의 난수생성 오버헤드도 줄어든다. 난수생성의 횟수는 MS가 N개의 VLR들을 방문한다고 가정하면 기존 메커니즘에서는 M번의 새로운 호에 의해 인증할 때마다 M×N번이 필요하며, 제안메커니즘은 새로운 VLR을 방문할 때 한번만 필요하기 때문에 N×1번이 필요하다. 또한 $RAND_M$은 암호화되어 전송되기 때문에, MS와 HLR간의 비밀키 Ki를 모르면, $RAND_M$ 값을 유추하기 어렵다.

- 대역폭 소비의 감소

MS가 동일한 VLR에 존재하고, HLR로부터 n개의 인증파라미터를 k번 전송받는다고 가정할 경우, 기존 메커니즘에서는 kn번의 인증파라미터를 전송받고, 제안메커니즘에서는 MS가 새로운 VLR에 방문할 경우, 단계5의 파라미터를 단 한번만 전송받기 때문에 HLR과 VLR간의 대역폭 소비를 줄일 수 있다.

- VLR 저장공간의 절약

HLR에서 VLR로 전송되는 파라미터는 n개에서 단지 한번의 인증파라미터로 감소되기 때문에, VLR에 저장해야하는 파라미터의 양도 감소되어 결과적

표 2. 기존 인증 메커니즘들과의 비교

	GSM	제안 I	제안 II	[3]	[4]	[6]	[7]
MS/VLR간 상호인증	×	○	○	○	×	○	×
대역폭 축소	n	1	1	n	1	1	1
VLR 저장공간의 축소	×	○	○	×	○	○	○
기본 암호시스템	비밀키	비밀키	비밀키	비밀키	비밀키	비밀키	공개키
VLR간 암호화과정의 필요성	×	×	×	○	○	○	○
부분적 익명성	×	○	○	×	×	×	×
IMSI 할당의 주체	VLR	HLR	HLR	VLR	VLR	VLR	VLR
인증받은 후에 IMSI 사용	×	○	○	×	×	×	×
사용자 인증단계의 축소	7	7	5	6	7	6	6
GSM 시스템의 구조변경	-	×	×	○	×	×	×
강력한 개체인증	×	○	○	×	×	×	×
인증되는 개체들	MS	MS,VLR	MS,VLR	MS	MS	MS	MS,VLR
부인 봉쇄	×	○	○	×	×	x	×

으로 저장공간이 절약된다.

[표 2]는 앞에서 설명한 제안메커니즘의 여러 특성을 기존 메커니즘들과 비교·정리한 것이다.

5. 결 론

제안메커니즘에서은 MS와 VLR의 각 개체는 강력한 인증서 생성규칙에 따라 HLR로부터 검증받았으며, 빠른 사용자인증을 위해 GSM 구조를 변경한 기존의 다른 메커니즘들과 달리 절차의 특이성에 의해 빠른 사용자인증을 제공하였다. 더욱이 사용자 프라이버시는 날로 중요시되는 반면 이를 지원하는 메커니즘이 거의 드문 현시점에서 제안메커니즘은 TID에 의해 사용자의 익명성을 제공하였다.

참 고 문 헌

[1] C.H. Lee, M.S. Hwang, and W.P. Yang, "Enhanced privacy and authentication for the global system for mobile communications," *Wireless Networks*, Vol. 5, No. 4, pp. 231-243, 1999.

[2] J.F. Stach, E.K. Park, and K. Makki, "Performance of an enhanced GSM protocol supporting non-repudiation of service," *Comput. Commun.*, pp. 675-680, 1999.

[3] R. Molva, D. Samfat, and G. Tsudik, "Authentication of mobile users," *IEEE Network*, Vol. 8, Issue 2, pp. 26-34, 1994.

[4] C.C. Lee, M.S. Hwang, and W.P. Yang, "Extension of authentication protocol for GSM," *IEE Proceedings. Communications*, Vol. 150, No. 2, pp. 91-95, 2003.

[5] Y.S. Cho, S.R. Cho, D.S. Choi, S.H. Jin, K.I. Chung, and C.H. Park, "A Location Privacy Protection Mechanism for Smart Space," *WISA2003*, *LNCS* 2908, pp. 162-173, 2004.

[6] Y.J. Choi and S.J. Kim, "An Improvement on Privacy and Authentication in GSM," *WISA2004*, *LNCS* 3325, pp. 14-26, 2004.

[7] W.B. Lee and C.K. Yeh, "A New Delegation-Based Authentication Protocol for User in Portable Communication Systems," *IEEE Transactions on wireless communications*, Vol. 4, No. 1, pp. 57-64, 2005.

박 미 옥

1991년 2월 : 조선대학교 전산통계학과 졸업
1993년 2월 : 숭실대학교 컴퓨터학과 석사
2001년 1월~11월: 매직캐슬(주) 선임연구원
2004년 8월 : 숭실대학교 컴퓨터학과 박사
2005년 3월~현재:성결대학교 컴퓨터공학부전임강사
관심분야 : 이동통신보안, 전자상거래, RFID

김 상 근

1987년 2월: 중앙대학교 전자계산학과 졸업
1991년 2월:중앙대학교 전자계산학과 석사
1996년 2월 : 중앙대학교 컴퓨터공학부 박사
1996년 3월~현재 : 성결대학교 컴퓨터공학부 부교수
관심분야 : 유비쿼터스 네트워크, 통신 소프트웨어, 인터넷