이동통신 무선접속구간에서 이용자 익명성을 보장하는 인증 및 키 합의 프로토콜

고재승, 김광조
한국정보통신대학원대학교 공학부
e-mail : jsgo @icu.ac.kr, kkj@icu.ac.kr

Authentication and key exchange protocol assuring user anonymity over wireless link in mobile communications

Jaeseung Go, Kwangjo Kim
Dept. of Engineering, Information and Communications University

요 약

차세대 이동통신 시스템의 이용자와 네트워크간 이용자 익명성을 보장하고, 이용자와 네트워크가 상대 실체를 안전하게 상호 인증할 수 있는 공개키 암호 방식에 기반한 개선된 인증 및 키합의 프로토콜을 제안한다. 이프로토콜은 이용자와 네트워크는 이용자의 고유신분과 세션별로 변하는 랜덤 수를 입력으로 하여 임시신분 정보를 생성 및 상호 공유하고, 네트워크는 초기에 이용자의 신분을 확인하며, 임시신분 정보는 이용자와 네트워크가 상호 선택한 랜덤 수에 따라 세션별로 갱신되므로 무선 접속 구간 상에 익명성을 보장하고 기존의 방식에 비교하여 보다 강화된 안전성을 보장한다.

1. 서론

시간에 따라 이용자의 위치가 변하는 이동통신 시스템에서 이용자는 서비스를 이용하기 위해 네트워크에 연결을 시도한다. 연결 시도의 초기에 이용자와 네트워크는 상대 실체에 대한 상호 인증 및 해당 세션을 위한 안전한 키 합의 프로토콜이 필요하다.

현재 무선 접속 서비스를 제공하는 CDMA 셀룰러 및 GSM 과 같은 2 세대 이동통신 시스템의 인증프로토콜에서는 네트워크와 이용자간의 공유 비밀키과 네트워크측에서 발생한 랜덤 수에 대하여 지정된 인증 알고리즘을 적용하는 도전-응답(challenge-response) 방식을 사용하여 네트워크가 이용자를 인증하는 일방향성 인증 방식을 이용하고 있다. [1, 2, 3].

차세대 이동통신 시스템에서는 네트워크에 의한 이용자 인증과 더불어 이용자가 현재 이동중인 위치에서 연결이 가능한 네트워크를 인증하는 이용자-네트워크간 상호 인증이 필요하다.

무선 접속구간을 통한 호 설정과 연결단계의 초기에 이용자-네트워크간 상호 인증과 해당 연결에서 이용하는 세션 키 합의 과정이 수행된다. 인증과정에서 이용자는 서비스를 제공하는 네트워크에 대하여 자신이 정당한 서비스 가입자임을 증명하는 이용자 신분을 제시하고 네트워크측에서는 이용자의 신분확인이 가능해야 한다. 그러나 무선접속구간에서 고유 신분을 포함한 이용자 관련 정보가 외부에 누설될 경우, 그 이용자의 현재 위치가 노출되고, 이것은 이용자에 대한 중대한 보안 위협요소가 된다. 따라서, 무선접속구간에서 이용자 신분정보의 기밀성, 즉 익명성은 차세대 이동통신 시스템 인증 프로토콜의 실체간 상호 인증과 함께 반드시 고려해야 할 중요한 보안 목표중의 하나이다 [4].

GSM 에서 네트워크는 이용자의 고유신분에 대응하는 임시신분을 이용자에게 부여하며, 이용자의 위치가 변경되어 초기 등록을 할 때에 이용자는 임시신분 및 고유신분을 이용하여 네트워크에 자신의 신분을 확인하는 인증 과정을 수행한다 [2]. 이러한 신분확인 및 실체 인증 과정에서 무선 접속구간에 고유신분과 관련된 이용자 정보가 암호화되지 않은 상태로 노출되었을 경우, 관련 정보를 얻고자 하는 악의의 공격자가 있다면, 이용자에 대한 보안상의 중대한 위협이 된다. 기존의 이동통신 시스템에서 현재 사용중인 인증프로

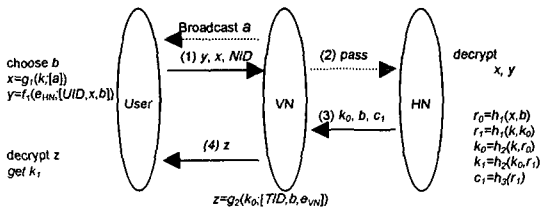
토콜은 무선접속구간의 이용자 익명성 보장 관점에서 보안상 취약하다고 할 수 있다. 이동통신 시스템에서 이용자와 네크워크간 익명성을 보장하면서 실체를 상호 인증하고 안전하게 세션 키를 합의할 수 있는 공개키 암호 방식에 기반한 인증 프로토콜을 제안한다.

2. 기 제안된 인증프로토콜

이동통신 시스템의 인증 및 세션키 합의 프로토콜에서 이용자 신분 기밀성 유지와 관련하여 최근에 제안된 프로토콜의 예로서 비밀키 암호 방식과 공개키 암호 방식을 함께 이용한 혼합형 프로토콜 [5]과 공개키 암호방식에 기반한 ASPeCT 프로토콜 [6]을 기술한다.

2.1 혼합형 프로토콜

혼합형 프로토콜은 로밍 환경에서 이용자 고유신분의 보호를 고려하였으며, 이용자는 서비스 가입시에 홈 네트워크와 공유하는 인증에 필요한 비밀키 값 k와 홈 네트워크의 공개키(e_{HN}) 값을 얻는다. 이후에 두 개의 공유 비밀값은 인증이 필요한 모든 세션에서 동일하게 이용된다. 또한 강화된 보안 특성을 제공하기 위하여 비밀키 암호 방식과 공개키 암호 방식이 함께 이용된다. <그림 1>은 혼합형 프로토콜에서 이용자 초기 등록시 이용자와 홈 네트워크(HN)가 공유한 네트워크의 공개키로 암호화하여 이용자 고유신분(*UID*)을 보호하는 것을 나타낸다. VN 은 방문 네트워크를 나타낸다 [5]. 그러나, 모든 세션에서 동일하게 이용되는 공유 비밀값이 누설되는 경우 이용자 고유신분이 노출될 위험이 있다.

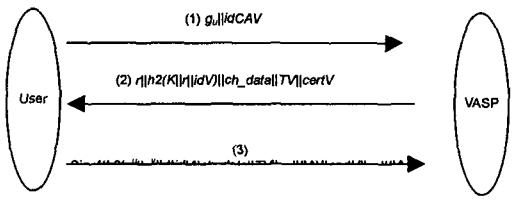


<그림 1> 혼합형 프로토콜 이용자 등록과정

2.2 ASPeCT 프로토콜

공개키 암호방식을 기반으로 하는 ASPeCT 프로토콜은 기존의 2 세대 이동통신 시스템 인증 프로토콜에서 제공하는 기밀성, 시스템의 부정 이용을 방지하는 네트워크에 의한 사용자 인증 외에 공격자의 네트워크 위장을 방지하기 위해 사용자에 의한 네트워크 인증과 프로토콜 내에 과금 관련 데이터를 통합하여 서비스 이용에 대한 이용자 검증 및 서비스 부인방지 등의 보안 특성을 더욱 강화하였다 [6].

ASPeCT 프로토콜은 <그림 2>에서 보는 바와 같이 인증 프로토콜의 세번째 메시지 합의단계에서, 이용자(User)와 네트워크(VASP)가 상호 계산한 세션키를 이용, 이용자의 고유신분을 포함하는 공개키 인증서(*certU*)를 암호화하여 이용자 신분을 확인하는 동시에 이용자의 익명성을 보장한다. 그러나, 이용자의 신분을 확인하기 위해서는 마지막 프로토콜 메시지까지 인증프로토콜을 진행해야 하는 단점이 있다.

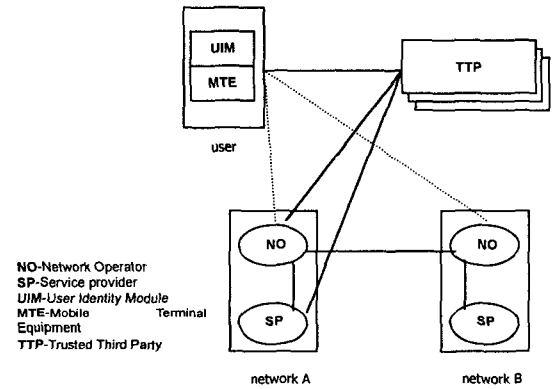


<그림 2> ASPeCT 프로토콜

3. 새로운 인증프로토콜 제안

3.1 시스템 구조 및 키 합의 모델

프로토콜 제안과 관련하여 이동통신 인증 프로토콜 설계시 고려해야 할 시스템 보안 구조에 대한 모델을 가정한다. 여기서는 [7]에서 제시한 차세대 이동통신 시스템 보안 구조에서 스마트 카드로 대표되는 이용자 신분 모듈(UIM)과 이동단말(MTE)을 결합하여 하나의 통신 실체인 이용자(user)로 나타내고, 네트워크 운용자(NO)와 서비스 제공자(SP)를 결합하여 하나의 통신 실체인 네트워크(network)로 나타내어 <그림 3>과 같이 이용자-네트워크 모델을 가정한다.

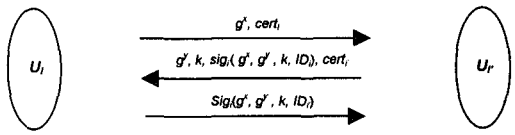


<그림 3> 인증 관련 이동통신 시스템 보안 구조

차세대 이동통신 시스템에서 일부 보안 서비스 제공 및 초기화는 제 3 의 신뢰기관(TTP)에 의존한다고 가정한다. TTP 는 상호 인증이 필요한 실체들에 대한 공개키 인증서 발급 및 검증에 관여하지만, 인증프로토콜에 직접 참여하지 않는다. 통신에 참여하는 개별 실체들과 관련된 각각의 실체가 신뢰하는 TTP 는 다수가 존재할 수 있으나, TTP 의 계층구조를 고려하지 않는다.

실체들간의 상호 인증과 세션 키 합의 설정은 대부

분 동일한 프로토콜에서 동시에 논의된다. 최근의 연구에서 안전한 인증 및 키 설정과 관련하여 정형적인 보안 모델이 제안되었다 [8, 9, 10]. [10]에서는 실제 시스템과 이상적인 시스템간의 시뮬레이션 관계를 기본으로 안전한 세션 키 합의에 대한 정형 보안 모델을 정의하고, 시스템에 대한 공격자의 시뮬레이션 능력(simulatability)에 의하여 키 합의 프로토콜의 안전성을 정의하였다. 제안된 프로토콜은 [10]에서 제시한 모델 중 Diffie-Hellman 기반 키 합의 프로토콜인 <그림 4>의 DHKE-2 모델을 기반으로 하고, 이동통신 시스템의 인증과 익명성 보장이라는 시스템 보안 특성을 고려한 서비스 제공에 중점을 두고 구성되었다.



<그림 4> DHKE-2 키 합의 프로토콜 모델

3.2 새로운 프로토콜 제안

앞에서 고려한 이동통신 시스템 보안 구조와 키 합의 프로토콜 모델을 기반으로 익명성을 고려한 인증 프로토콜을 제안한다.

이용자(U,user)와 네트워크(N,network)는 상대 실체가 신뢰할 수 있는 신뢰기관(TTP)이 발행하는 공개키 인증서($cert_U$, $cert_N$)와 상대 실체의 인증서를 검증할 수 있는 TTP 의 공개키를 가지고 있다. 네트워크(N)는 서비스 가입시에 이용자(U)에게 초기 임시 신분(TID)를 부여하고, 이용자와 네트워크는 고유신분(UID)과 초기 임시신분을 저장한다.

다음은 제안된 인증 프로토콜 구성에 이용한 기호와 그에 대한 설명을 나타낸다.

U, N : 통신 실체인 이용자(U), 네트워크(N)

G : 큰 소수의 위수 q 인 군(group)

$g \in G$: 군 G 에서 랜덤하게 선택한 생성원

$x, y \in Z_q$: 랜덤하게 선택한 비트 스트링

u, g^u {n, g^n}: U{N}의 인증된 서명용 비밀 및 공개키

$cert_U, cert_N$: U, N 의 공개키 인증서

UID, NID : U, N 의 고유신분(식별자)

TID : 이전 세션에서 생성된 U 의 임시신분

$TID' = H_j(UID, g^{xy})$: 현재 세션에서 변경된 U 의 임시신분

H_j, H_k, H_l : 쌍으로 존재하는 독립 해쉬함수

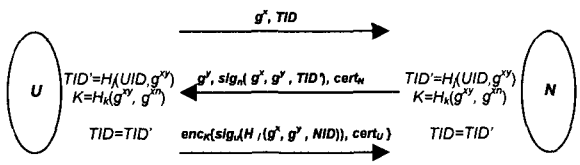
j, k, l : 해쉬함수 지수, 특정 길이의 비트 스트링

$K = H_k(g^{xy}, g^{xn})$: 합의된 세션 키

$sig_u(msg), sig_n(msg)$: 메시지에 대한 U, N 의 서명값

키 합의 프로토콜 DHKE-2 모델을 기반으로 위에서 제시한 이동통신 시스템의 보안구조와 통신 실체간 상호 인증 및 안전한 키 합의, 이용자 익명성의 보안 서비스 제공에 중점을 둔 새로운 인증 프로토콜을 <그림 5>에 나타내었다.

제안된 프로토콜은 Diffie-Hellman 기반 키 합의 프로토콜이다. [10]에서 제시한 바와 같이 DDH(decisional Diffie-Hellman) 가정과 안전한 서명 방식, 암호학적 해쉬 함수와 안전한 비밀키 암호방식 등의 암호 프리미티브 선택시 안전한 키 합의 방식에 의한 인증 프로토콜이다. 프로토콜의 실행이 끝난 후에 세션에 참여하는 통신 실체들은 상호 실체 인증, 상호간 암시적인 키 인증에 의한 안전한 키 합의 및 키 확인, 세션별 키 갱신 보증, 그리고 이용자 익명성 등 이동통신 시스템 인증 프로토콜의 보안목표를 달성할 수 있다 [4].



<그림 5> 새로운 프로토콜

프로토콜의 첫번째 메시지에 임시 신분 TID 를 포함시킴으로써 네트워크(N)는 이용자(U)의 신분을 인증 프로토콜의 초기에 확인한다. 실체 N 은 저장된 데이터베이스를 검색하여 실체 U 가 정당한 가입자인지 확인한 후 서비스 제공 및 프로토콜 계속 여부를 결정한다. 두번째 메시지에서 N 의 g^x, TID' 에 대한 서명은 U 에 대한 암시적인 실체인증을 제공하고, g^x, g^y, k 에 대하여 서명함으로써 암시적인 키 인증 및 키 갱신을 보증한다. 마지막 메시지에서 실체 U 는 NID 에 서명함으로써 N 에 대한 실체 인증을 제공하며, g^x, g^y, k 에 서명함으로써 키 갱신을 보증하고, 키 합의에 의해 설정된 세션 키 K 를 이용하여 전체메시지를 암호화함으로써 명시적인 키 확인을 제공한다. 또한 암호화된 메시지 내에 실체 U 의 공개키 인증서를 포함시킴으로써 이용자 익명성을 보장하고, 실체 N 은 메시지 수신완료 후 실체 U 에 대한 명시적인 신분확인이 가능하다.

3.3 키 합의에 대한 안전성 분석

제안된 프로토콜에서 세션 키 합의 부분의 안전성과 관련하여, 공격자가 프로토콜에 참여하는 실체의 비밀키를 얻을 수 있는 능동적인 경우를 가정하였다. 세션 키 합의와 관련된 프로토콜의 보안특성을 분석하여 공격자의 능동적인 공격방식에 안전할 수 있는지를 기술한다 [11].

- 알려진 키에 대한 안전성(known key security)

제안된 프로토콜은 이전 세션에서 사용되었던 세션키를 알고 있는 공격자에 대하여 현재 세션키의 안전성에 영향을 받지 않는다. 합의된 세션키는 실체가 선택한 랜덤 수를 입력값으로 하며, 세션별로 독립적으로 선택하는 랜덤 수에 따라 세션키 역시 변경된다.

- 전향적 보안성(forward secrecy)

프로토콜에 참여하는 실체의 서명용 비밀키(n 또는 u)가 노출된 경우에도 이전(previous) 세션에 대한 안전성에 영향을 미치지 않는다. 랜덤한 입력값에 의해

계산된 세션키 $K=H_k(g^{xy},g^{xn})$와 임시신분 $TID'=H_f(UID,g^{xy})$에서 DDH 가정과 안전한 해쉬 함수의 사용을 가정하면 세션키 K 와 변경된 임시신분 TID' 의 계산 및 확인이 불가능하다.

- 미지의 키공유(unknown key-share)

제안된 프로토콜의 수행과정에서 공격자 A 가 프로토콜의 중간에서 네트워크(N)의 공개키(g^n)를 알아내어, 신뢰기관에서 공개키 인증서를 발급 받은 후에 이용자(U)와 프로토콜을 수행하며, 동시에 네트워크(N)로 하여금 이용자(U)와 프로토콜을 수행하고 있다고 믿게 만드는 경우를 고려한다.

두번째 메시지에서 N 이 서명문에 $TID'=H_f(UID,g^{xy})$ 을 포함시켜 송신하는 경우, A 가 TID' 를 그대로 중계한다 할지라도 DDH 가정에 의해 TID'에 포함된 N 의 랜덤 입력값(y)을 이용한 세션키의 계산이 불가능하므로, 단지 중계 역할만 가능하며, 프로토콜의 세번째 메시지 내용을 알아낼 수 없으므로 프로토콜을 손상시킬 수 없다.

- 키 위장(key-compromise impersonation)

이용자(U)의 서명용 비밀키(u)가 손상되어 공격자(A)가 네트워크(N)에 대하여 이용자(U)로 위장하거나 U 에 대하여 N 으로 위장하는 경우를 고려한다.

먼저 A 가 N 에 대하여 U 로 위장하는 경우에, A 는 첫번째 메시지에서 유효한 TID 를 제시할 수 없으므로 N 에 의한 신분확인에서 실패한다. 마찬가지로 A 가 U에 대하여 N으로 위장하는 경우, A 는 U에 대한 UID 를 알 수 없으므로 TID'를 계산할 수 없으며, U 의 서명 검증시 실패하게 된다.

위에서 살펴본 바와 같이 제안된 프로토콜은 능동적인 공격자의 이미 알려진 몇 가지 공격방식에 대하여 안전하다.

3.4 인증프로토콜 비교

이동통신 인증 프로토콜의 여러가지 보안 특성중 이용자-네트워크간 상호 신분 확인 및 익명성의 관점에서 GSM 인증 프로토콜, 혼합형 프로토콜, ASPeCT 프로토콜과 제안된 프로토콜에 대한 비교 내용을 <표 1>에 나타내었다.

프로토콜 / 보안특성	GSM	혼합 프로토콜	ASPeCT 프로토콜	제안된 프로토콜
상호 실체인증			o	o
신분확인과 인증 프로토콜의 통합		o	o	o
프로토콜 초기 신분확인		o		o
세션별 임시신분의 상호 생성				o
세션별 임시신분의 갱신				o
이용자 고유 신분정보의 기밀성	o	o	o	o

<표 1> 인증프로토콜 비교

제안된 프로토콜에서 임시 신분의 세션별 갱신은 동일한 서비스 지역에서 세션이 빈번하게 발생하는 이동통신 시스템 환경에서 이용자 익명성의 보안 특성이 더욱 강화된다. 또한, 제안된 프로토콜은 첫번째 프로토콜 메시지에 임시신분을 이용하여, 네트워크가 프로토콜 실행 초기에 이용자의 신분을 잠정적으로 확인할 수 있다는 점에서 프로토콜의 마지막 메시지에서 신분정보를 암호화하여 익명성을 유지하는 ASPeCT 프로토콜과 차이가 있다.

4. 결론

이동통신 시스템의 인증프로토콜과 관련하여 시스템 보안 구조 및 정형적인 키 합의 프로토콜 모델을 설정하고, 설정된 모델을 기반으로 임시신분을 이용하여 통신 실체간 상호 인증 및 신분확인, 안전한 키 합의, 그리고 이용자의 익명성을 보장하는 프로토콜을 제안하고, 세션 키 합의와 관련한 프로토콜의 안전성을 분석하였으며, 상호인증 및 신분확인과 익명성의 관점에서 이전에 제안된 프로토콜과 비교 분석하였다.

참고문헌

1. M. Y. Lee, *CDMA cellular mobile communications network security*, Prentice Hall PTR, 1998.
2. GSM 03.20 version 6.0.1, Digital cellular telecommunications system(Phase 2+); Security related network functions, release 1997.
3. A. Mehrotra, L. S. Golding, "Mobility and security management in the GSM system and some proposed future improvements", Proceedings of the IEEE , Vol: 86 Issue: 7 , pp1480-1497, July 1998.
4. K. M. Martin and C. J. Mitchell, "Evaluation of authentication protocols for mobile environment value added services", draft, 1998.
5. H.Y.Lin and L. Harn, "Authentication protocols for personal communication systems", Proceedings of ACM SIGCOMM'95, pp256-261, August 1995.
6. G. Horn and B. Preneel. "Authentication and payment in future mobile systems", Computer Security – ESORICS'98, Lecture Notes in Computer Science, 1485, pp277-293, Springer Verlag,1998.
7. Gary Gaskell, Mark Looi, Ed Dawson, Colin Boyd and Selwyn Russell, "A proposed security architecture for third generation wireless systems", private communication, 1998.
8. M. Bellare and P. Rogaway, "Provably secure session key distribution - the three party case", In 27th Annual ACM Symposium on Theory of Computing, pp57-66, 1995.
9. M. Bellare, R. Canetti, and H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols", 30th Annual ACM Symposium on Theory of Computing, pp419-428, 1998.
10. Victor Shoup, "On formal models for secure key exchange (version 4)", November 15, 1999 revision of IBM Research Report RZ 3120 (April 1999).
11. S. Blake-Wilson, D. Johnson and A. Menezes, "Key Agreement Protocols and their Security Analysis",: sixth IMA International Conference on Cryptography and Coding, LNCS 1355, pp30-45, 1997.