무선 이동 통신을 위한 보안 프로토콜 설계

강 형우[o*], 이 수연[**], 박 창섭[***]; 이 동훈[*], 윤 이중[****]

[*] 고려대학교 전산학과, [**] 천안외국어대학 사무자동화과,

[***] 단국대학교 전자계산학과, [****] 전자통신 연구소 부호 기술부

Security Protocol Design for Wireless Mobile Communication

Hyung-Woo Kang[o*], Su-Youn Lee[**], Chang-Seop Park[***], Dong-Hoon Lee[*], E-Joong Yoon[****]

[*] Department of Computer Science, Korea Univ., [**] Department of Office Automation, Chonan Foreign College

[***] Department of Computer Science, Dankook Univ., [****] ETRI Coding Technology section

요 약

무선 이동 통신에서는 가입자의 이동성으로 인하여 가입자의 인증 프로토콜을 수행할 때 신원이 노출되기 쉽다. 이러한 가입자의 신원 노출은 제 3자가 이동 가입자의 이동을 추적하거나 위치를 파악할 수 있게 할 수 있다. 또한 이동 가입자가 사용하는 단말기의 낮은 계산능력으로 인하여 가입자의 단말기가 인증 프로트콜을 수행함에 있어서 적은 암호학적 연산이 요구된다. 본 논문에서는 단말기의 계산능력이 낮은 점을 고려하여 단말기에 적은 암호학적 연산이 요구되며 가입자의 위치와 행동의 노출 없이 안전하게 이동 가입자를 인증하는 프로토콜을 제안한다.

1. 서론

전 세계적으로 이동 통신 서비스의 수요가 폭발적으로 증가하는 반면에 무선 통신망을 이용하는 이동 통신의 특성 때문에 불법적인 사용이나 도청 또는 추적을 통한 불법적인 행위, 각종 통신 범죄 행위 등도 늘어나게 된다. 이러한 행위들은 가입자에 대한 서비스의 저하, 그리고 개인의 프라이버시 침해 등의 역기능적인 문제를 기져오게 된다.

최근, 이런 문제들을 해결하기 위하여 각 국의 이동 통신 업무의 표준화에 인증 기능 등을 추가하여 권고하고 있다. 미국의 TIA/EIA(Telecommunications Industry Association/ Electronic Industries Association)에서 무선 인터페이스 표준안으로 권고하고 있는 인증 및 암호화 기능이나, 유럽 국기에서 ETSI(European Telecommunications Standards Institute)의 표준화로 추진하고 있는 GSM(Global System for Mobile Communications)이나 DECT(Digital European Cordless Telecommunications) 표준에서도 인증을 포함한 보안 서비스를 권고하고 있다. 이들 표준들은 인증 및 암호기능을 제공하기 위해서 모두 비밀키 암호 방식을 채택하고 있다. 이는 보안 서비스의 제공으로 인해 시스템에 미치는 부하의 증가, 단말기 소형화에 따른 계산능력의 문제점 등을 고려하여 선정한 것이다 그러나 거대한 데이터베이스의 안전 관리가 문제로 남게 된다. 반면, 비밀키 암호 방식에 의한 보안 서비스의 제공에 대한 취약점을 개선하기 위하여, 공개키 암호 방식을 이용한 각종 방안들이 제시되고 있다. 이들은 비록 비밀키의 단점인 안전한 데이터베이스 관리 문제를 해결할 수 있으나, 시스템의 부하를 증대시키는 등의 문제가 있다.

본 논문에서는 비밀키 암호 방식을 이용하여 시스템 부하와 단말기의 계산 능력을 고려하고, 비밀키 인증서를 사용하여 가입자의 비밀정보를 저장하는 데이터베이스의 안전한 관리 문제를 해결한 새로운 인증 프로토콜을 제안한다. 2장에서는 기존의 연구를 살펴보며, 3장에서는 이동 통신에 적합한 보안 프로토콜을 제안하고, 마지막으로 4장에서는 결론을 논한다.

2. 기존의 연구

GSM(Global System for Mobile)[1]은 가입자의 프라이버시를 제공하기 위한 최초의 디지털 셀룰라 네트웍이다 GSM에서 프리이버시는 TMSI(Temporary Mobile Subscriber Identifiers)로 알려진 가명을 이용하여 제공되는데, 가입자의 단말기에 전원이 들어갈 때 IMSI(International Mobile Subscriber Identifier)로 알려진 가입자의 ID가 전송되고. 그 다음 단계부터는 TMSI가 가입자의 가명으로 전송된다. 이 때 도청자기 계속 사용되는 TMSI를 이용하여 IMSI를 추적할 수 있으므로 가입자의 ID를 알아 낼 수 있다 또한 가입자와 홈 도메인 사이에 TMSI의 동기화가 끊어졌을 경우에는 가입자는 다시 홈 도메인에게 IMSI를 보내야 한다. GSM의 또 다른 문제점은 홈 도메인과 방문 도메인사이의 네트웍은 안전하다고 가정을 하였기 때문에 방문 도메인이 홈 도메인에게 가입자의 IMSI와 위치정보를 평문 상태로 보내게 된다. 하지만 이런 일들은 가입자의 프라이버시를 해치기 쉬운 일들이다.

GSM과는 달리 CDPD(Cellular Digital Packet Data)[4]는 좀 더 안전한 방법을 취한다. CDPD는 인증 과정이 일어나기 전에 먼저 가입자와 방문 도메인사이의 Diffie-Hellman 키 교환 프로토콜[3]을 이용하여 세션키를 공유하고 그 다음에 가입지는 자신의 ID를 세션키로 암호화하여 방문 도메인에게 전송한다. 이 방법에서 첫 번째 문제점은 방문 도메인이 가입자의 ID를 알 수 있다는 것이다. 두 번째 문제점은 Diffie-Hellman 키 교환 프로토콜 자체에 "man-in-the-middle attack"이 존재하므로 권한이 없는 제 3자가 방문 도메인을 가장할 수 있고 그 결과는 제 3자가 가입자의 ID를 알아내고 여러 비밀정보를 알아 낼 수 있다.

그 밖에 가입자의 신원을 감추기 위하여 공개키 암호방식의 가명을 사용한 가입자 인증 프로토콜이 Samfat, Molva 그리고 Asokan[7]에 의해 제안되었다. 그들이 제안한 인증 프로토콜은 인증과 가입자의 익명성과 추적 불가능성 문제를 해결하지만 단말기의 낮은 계산능력과 적은 배터리 용량 때문에 공개키 방식은 이동 통신에서 인증과정으로 사용하기에는 적절하지 않다.

3. 제안된 이동 통신 환경에서의 인증 프로토콜

본 장에서는 Park[5]이 제안한 오류수정부호를 이용하여

이동 통신 환경에서 가입자의 익명성과 추적 불가능성을 제공하는 가입자 인증 프로토콜을 제안한다.

3.1 가입자 익명성과 추적 불가능성을 제공하는 인증 프로토콜

Park[5]은 오류수정부호와 비밀키 인증서를 이용하여 이동 가입자 MU(Mobile User)를 인증서버 AS(Authentication Server)가 인증하는 시도/응답(Challenge/Response) 인증 프로토콜을 제안하였다.

오류수정부호는 채널오류나 잡음을 가진 통신망 내에서 신뢰성을 제공하기 위해 사용되어진다. 암호학에 적용 된 오류수정부호의 응용은 McEliece[2]에 의해 처음 소개되었다. 이것은 Berlekamp, McEliece, Van Tilborg에 의해 작성된 선형블록코드의 일반적인 복호화 문제가 NP-complete라는 초기 논문의 결과이다 길이가 N, 차원이 K 그리고, 최소거리가 D인 선형 오류수정부호는 (N,K,D)로 표기되어진다. 이진 k-tuple의 메시지 m은 $c = m \cdot G$에 의해 N 비트의 코드워드로 부호화 되어지고 오류벡터 e 가 추가되어 $c' = c + e$ 벡터의 결과가 되어진다. 여기서, G는 K x N의 생성행렬이다. 만약, e의 해밍 가중치가 $t = \lfloor (D-1)/2 \rfloor$보다 작거나 같다면 c'는 신드롬 벡터 $s = c' \cdot H^T$를 사용하여 c로 복호화 할 수 있다. 여기서, H는 $G \cdot H^T=0$가 되는 $(N-K)$ x N 패리티 검사행렬이다.

사전 단계로 AS는 적합한 가입자로써 MU를 등록시키고 비밀키 k와 부호화된 비밀키 인증서 $c = m \cdot G$를 제공한다. 여기서, 메시지 $m = f(k_{AS}, [id, k])$는 실제 신분 id와 MU의 비밀키 k를 AS 자신만이 알고 있는 비밀키 k_{AS}를 사용하여 암호화한 비밀키 인증서이다 여기서 $f()$는 대칭형 암호 알고리즘이다 다음은 Park[5]의 인증 프로토콜을 나타내고 있다.

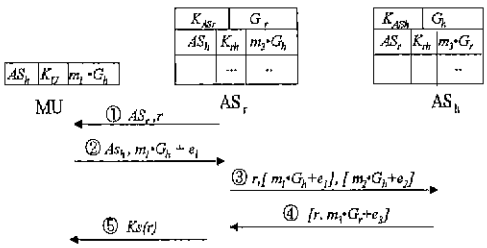
[프로토콜]
MU ← AS : r
MU → AS : $m \cdot G + e$

AS에 의해 생성되어진 난수(challenge) r을 이용하여 MU는 응답으로 $h(k,[r, id])$를 계산한다, 여기서, $h()$는 키를 이용하는 해쉬 함수이고 k는 MU의 비밀키이다. 다음으로 s-비트의 해쉬 값 $h(k,[r, id])$를 길이 N, 해밍가중치 $t = \lfloor (D-1)/2 \rfloor$ 인 오류 벡터 e로 변형시키고 이 오류 벡터 e를 추가한 부호화 된 비밀키 인증서 $c = m \cdot G + e$를 AS에게 보낸다. 여기서 해쉬 값 $h(k,[r, id])$는 [8]의 알고리즘을 이용하여 오류 벡터 e로 변형시킬 수 있다.

$m \cdot G + e$를 수신한 후 AS는 복호화 과정을 수행하고 m과 마찬가지로 오류벡터 e를 식별한다. 이동 가입자의 실제 신분 id와 대응되는 비밀키 k는 $m = f(k_{AS}, [id, k])$를 AS의 비밀키 k_{AS}로 복호화하여 얻을 수 있다. 그 후 s-비트의 해쉬 값 $h(k,[r, id])$는 AS에 의해 계산된다 만약, 계산된 s-비트 해쉬 값이 e로부터 유도된 값과 같다면 AS는 MU를 합법적인 가입자로 인증한다.

3.2 제안된 인증 프로토콜

본 절에서는 Park[5]이 제안한 오류수정부호를 이용하여 이동 통신 환경에 맞는 가입자 인증 프로토콜을 제안한다. 제안된 인증 프로토콜은 홈 도메인(AS_h)을 제외한 어느 누구도 가입자 MU의 신원(ID)과 방문 도메인(AS_r)의 신원(ID)을 알 수 없게 한 것이다. 이 프로토콜의 기본적인 요구사항은 가입자 MU는 가입 신청시 그의 단말기 안에 홈 도메인이 제공한 비밀키 K_U와 비밀키 인증서($c = m_1 \cdot G_h$)를 저장하고 있고 각각의 인증서버(AS)들은 다른 인증서버에게 발행한 비밀키 인증서를 생성하는 데 사용한 비밀키 K_{AS}와 생성행렬 G를 갖고 있고, 또한 각각의 인증서버들과 공유하는 공유키와 각각의 인증서버들이 발행한 비밀키 인증서를 저장하고 있는 데이터베이스를 가지고 있어야 한다. 하지만 각각의 인증서버들은 자신을 홈 도메인으로 가지고 있는 가입자들의 비밀정보(공유키)에 대한 데이터베이스는 필요로 하지 않는다. 제안된 프로토콜의 수행과정은 다음과 같다 :



[제안된 인증 프로토콜]

1. 이동 통신 가입자가 방문 도메인으로 지역을 이동하였을 경우 AS_r은 먼저 자신의 도메인 내에 있는 단말기에게 메시지①을 시스템 방송한다.
2. 메시지①을 받은 단말기는 자신이 홈 도메인에 있지 않고 외부지역에 있다는 것을 인지하고 방문 도메인(외부지역)에서 이동 통신 서비스를 얻기 위한 인증 프로토콜을 시작한다. 메시지①을 받은 가입자의 단말기는 메시지②에서 자신의 단말기내에 있는 비밀키 K_U와 AS_r로부터 받은 r을 이용하여 s-비트의 해쉬값 $h(K_U,[r,MU])$를 구하고 나중에 AS_r과 통신하기 위한 세션키 Ks를 생성해서 s-비트 해쉬값과 함께 길이 N, 해밍가중치 t인 오류 벡터 e_1으로 변형시켜 오류 벡터 e_1을 추가한 부호화된 비밀키 인증서 $c = m_1 \cdot G_h + e_1$를 AS_h와 함께 ASr에게 보낸다
3. 메시지②를 받은 AS_r은 AS_h가 MU를 인증하기 위한 매시지인 시도(Challenge)값 r에 대한 응답(Response)값 $m_1 \cdot G_h + e_1$과 자신의 신분을 AS_h에게 인증시키기 위하

MU	이동 통신 가입자(Mobile User)의 ID
AS_h	홈 도메인 인증서버의 ID
AS_r	방문 도메인 인증서버의 ID
r	시도(Challenge)로 사용되는 난수열
K_U	가입자 MU와 홈 도메인의 인증서버 AS_h가 공유하는 long-term key
$h(M)$	MAC 해쉬 함수
Ks	가입자 MU가 생성하는 MU와 AS_r사이의 세션키
K_{rh}	AS_r과 AS_h가 공유하는 long-term key
$m_1 = f(K_{ASh}, [MU. K_U])$	$e_1 = Ks, h(K_U, [r, MU])$
$m_2 = f(K_{ASh}, [AS_r, K_{rh}])$	$e_2 = h(K_{rh}, [r, AS_r])$
$m_3 = f(K_{ASr}, [AS_h, K_{rh}])$	$e_3 = Ks, h(K_{rh}, [r, AS_h])$
G_h, G_r	각각 AS_h와 AS_r의 생성행렬

[제안된 프로토콜에서 사용되는 기호]

여 난수열 r을 시도(Challenge)값으로 하는 응답(Response)값 $m_2 \cdot G_h + e_2$를 AS_h에게 보낸다. 여기서 $m_2 \cdot G_h$와 K_{rh}는 AS_r의 데이터베이스에 저장되어있고, e_2는 $h(K_{rh}, [AS_r, r])$이다.

4 메시지③을 받은 AS_h는 생성행렬(G_h)과 $G_h \cdot H^T=0$의 관계가 있는 패리티-검사 행렬 H를 이용하여 MU와 AS_r 각각의 인증서인 $m_1 \cdot G_h + e_1$과 $m_2 \cdot G_h + e_2$를 복호화하여 m_1, m_2, e_1, e_2를 식별한다. 그 다음 비밀키 인증서 m_1, m_2를 AS_h 자신만이 알고 있는 비밀키인 K_{ASh} 가지고 복호화히므로서 MU와 AS_r의 신원(ID)을 확인하고 가입자 MU의 키인 K_U를 뽑아낸다. 이제, AS_h는 e_1의 해쉬값을 점검하여 가입자 MU가 합법적인 가입자인지를 인증(확인)하고 또한 e_2의 해쉬값을 점검하여 AS_r을 인증한다. 다음 AS_h는 자신의 데이터베이스의 $m_3 \cdot G_r$를 이용하여 AS_r이 생성한 난수열 r을 시도(Challenge) 값으로 하는 응답(Response)값 $m_3 \cdot G_r + e_3$ 쌍을 메시지④로 하여 AS_r에게 보낸다. e_3에는 AS_h가 메시지③의 e_1에서 뽑아낸 가입자 MU와 AS_r의 세션키 Ks가 포함되어 있다. 여기서 세션키 Ks는 가입자 MU와 AS_r이 공유하며 데이터를 암·복호화하는 데 사용하게 될 키이다.

5 메시지④를 받은 AS_r은 AS_h로부터 받은 메시지④안에 포함된 e_3의 해쉬값을 점검하여 AS_h를 인증하고 또한, e_3에서 Ks를 뽑아내어서 MU와의 세션키로 사용한다. 메시지④를 받은 AS_r은 비로소 AS_h를 통해서 가입자 MU를 인증하게 된다. 그리고 AS_r은 MU에게 메시지⑤인 $Ks(r)$을 보낸다. 이 메시지를 받은 MU는 AS_h와 AS_r만이 Ks를 얻을 수 있으므로 AS_r과 AS_h를 인증할 수 있다.

제안된 인증 프로토콜은 시도/응답(Challenge/Response) 메시지를 주고받으면서 가입자의 인증 서비스를 제공하여 부정당한 가입자의 불법 사용 문제를 해결하고 MU와 AS_r이 세션키를 공유하여 메시지 암호를 통한 도청 문제를 해결한다. 그리고 Park[5]이 제안한 오류수정부호를 사용하여 가입자의 익명성을 제공하며 매 세션마다 가변적인 오류벡터로 인한 가입자의 추적 불가능성 서비스를 제공해 준다.

또한, 제안된 인증 프로토콜은 비밀키 방식의 문제점인 방대한 데이터베이스 문제점을 비밀키 인증서를 사용하여 해결하고 인증 프로토콜 수행 시 오류수정부호, 해쉬 함수 그리고 비밀키 암호 알고리즘을 사용하여 공개키 암호 알고리즘을 사용한 프로토콜의 문제점인 단말기에 과중한 계산능력을 요구하는 문제점을 해결하였다. 기존의 프로토콜들에서 단말기가 자신을 인증 서버에 인증 시키기 위해서는 비밀키 알고리즘 연산 또는 공개키 알고리즘 연산 등을 필요로 했는데, 제안된 프로토콜은 빠른 해쉬 알고리즘과 오류수정부호를 사용하고 비밀키 암고리즘 연산의 회수도 최소로 사용하게 된다. 즉, 기존의 어떤 프로토콜보다도 단말기에 가장 적은 암호학적 연산이 요구되는 프로토콜이다.

제안된 프로토콜에서 각각의 도메인 인증 서버들은 상대편에 대한 비밀키 인증서를 저장하는 데이터베이스를 갖는 것을 전제로 하고 있다. 인증 서버들간의 인증을 제공하는 기존의 프로토콜들[7]에서도 마찬가지로 인증 서버들간의 인증을 위하여 공유키를 저장하는 데이터베이스를 갖고 있으므로 기존 프로토콜[7]의 데이터베이스에 인증서 필드항목을 하나 추가 시켜서 보관하면 보안상에 문제점이 증가된 것은 없고 단지 이동 통신 사업을 시작할 때 각각의 인증서버들간의 공유키를 생성함과 함께 인증서를 같이 생성해서 각각의 인증서버들의 데이터베이스에 저장하면 된다. 제안된 프로토콜은 인증서버들간의 인증을 제공하는 기존의 프로토콜[7]보다 이동 단말기뿐만이 아니라 인증 서버들(AS_r, AS_h)이 수행해야 하는 암호학적 연산이 줄어들었다. [7]의 프로토콜에서 인증 서버들은 서로 자기자신을 인증시키기 위해서 비밀키 암호 알고리즘과 해쉬 알고리즘을 수행한다. 하지만 제안된 프로토콜에서는 오류수정부호와 해쉬 알고리즘을 사용하므로 인증서버 측면에서 [7]의 프로토콜보다 효율적이다. 또한 일반적인 이동 통신 보안 프로토콜(eg. GSM..)에서는 ASr과 ASh간의 보안 서비스가 불완전하지만 제안된 프로토콜은 MU, ASr 그리고 ASh 모두의 상호 인증을 제공하고 있다. 이런 점은 제안된 프로토콜이 로밍 환경에서의 보안 서비스를 충분히 제공할 수 있음을 나타낸다.

4. 결론

본 논문에서는 Park[5]이 제안한 비밀키 인증서와 오류수정부호의 개념을 이동 통신의 환경에 맞게 설정하여 이동 통신 가입자의 프라이버시를 보장하는 가입자 인증 프로토콜을 제안하였다. 기존의 이동 통신 인증 프로토콜인 GSM과 CDPD의 문제점을 지적하고 그 문제점을 해결하는 새로운 방향을 제시하였다. 제안된 프로토콜은 가입자의 익명성을 제공하기 위하여 비밀키 방식의 인증서를 가입자의 단말기에 저장하여 인증 프로토콜의 수행시 가입자가 자신의 신분확인을 위하여 이 비밀키 인증서를 인증 서버에 전송하는 방식을 채택하여 인증서버들이 가입자들의 비밀정보(공유키)들을 관리하는 방대한 데이터베이스 문제를 해결하였고, 오류 수정부호를 이용하여 가입자의 익명성과 추적 불가능성을 제공하였다. 기존의 프로토콜이 익명성을 제공하기 위하여 공개키 방식의 가명을 사용함으로써 단말기에 과중한 계산능력을 요구하는 반면, 제안된 프로토콜은 비밀키 암호 알고리즘과 오류수정부호 그리고 해쉬 함수만을 사용하여 단말기의 낮은 계산능력을 고려하여 설계하였다.

참고문헌

[1] M. Rahnema, Overview of the GSM System and Protocol Architecture. IEEE Communications Magazine. April 1993

[2] R J. McEliece, A Public-Key Cryptosystem Based on Algebraic Coding Theory, DSN progress Report, Jet Propulsion Lab., Ca., Jan. and Feb. 1978, pp. 42-44

[3] W. Diffie and M Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Novernber 1976.

[4] Cellular Digital Packet Data(CDPD) System Specification, Release 1 0, July 19, 1993.

[5] C. S. Park, Integrating Authentication with Anonymity using Error-Correction Codes, by private communication.

[6] M J. Beller, L F. Chang, Y. Yacobi Security for Personal Communications Services : Public-Key vs Private Key Approaches Proceedings of 2nd International Symposium on Personal, Indoor and Mobile Radio Communications, October 1992.

[7] D. Samfat, R. Molva, N. Asokan. Anonymity and Untraceability in Mobile Networks, Proc. of the ACM International Conference on Mobile Computing and Networking, Nov. 1995, Berkeley, Ca.

[8] C. S. Park, Improving Code Rate of the McEliece Public-Key Cryptosystem, Electronics Letters, vol.25, no.21, pp. 1466-1467, 1989.