이동통신 환경에서의 사용자 익명성을 보장하는 AKA 프로토콜

이동규*, 황성민*, 최영근*, 김순자*

*경북대학교, 전자공학과

AKA protocol assuring anonymity of user in mobile communications

Dong-kyu Lee*, Sung-min Hwang*, Young-geun Choe*, Soon-ja Kim*

*Department of Electronics Engineering, Kyungpook National Univ.

요 약

본 논문에서는 이동통신 환경에서 signcryption 기법을 적용하여 연산량과 통신 오버헤드를 개선한 공개키 기반의 인증 및 키 합의 프로토콜을 제안한다. 제안된 프로토콜에서는 사용자와 서비스를 제공하는 네트워크간 사용자 익명성을 보장하고, 사용자와 네트워크가 상대 개체를 안전하게 상호 인증한다. 또한 보안 요구 조건들을 제시하고 기존의 익명성을 제공하는 프로토콜들에 대한 간략한 소개와 문제점들을 살펴본 뒤, 제안된 프로토콜과 비교 분석한다.

I. 서론

일반 이동전화 서비스를 비롯한 이동 컴퓨팅, 이동 멀티미디어 서비스 등 이동통신시스템을 통한 응용서비스 개발과 서비스 제공이 증가함에 따라 사용자 신분 및 위치 정보의 노출, 불법적인 서비스 이용, 송수신 데이터의 도청 및 변경 등과 같은 이동통신 환경에서의 보안 문제가 중요하게 되었다. 이에 따라, 이동통신 환경에서의 보안취약점을 방지할 수 있는 안전한 인증 및 키 합의 프로토콜이 필요하다. 지금까지 암호기술을 이용한 여러 AKA(authentication and key agreement) 프로토콜들이 제안되었으나, 최근 강한 보안성을 제공하는 공개키 암호시스템을 이용한 AKA 프로토콜들이 제안되고 있다. 공개키 암호시스템은 대칭키 암호시스템에 비해 계산량이 많고 키 길이가 길어서 효율성은 떨어지지만, 강한 보안성과 키 관리가 용이하다. 그러나 이동통신 환경에서의 AKA 프로토콜 설계 시에 유선 네트워크에 비해 이동통신 환경이 갖는 제약점, 즉 제한된 메모리, 자원, 계산 능력, 대역폭을 고려해야 한다. 따라서 빠른 키 생성과 빠른 계산속도, 적은 양의 메모리를 사용하면서도 강한 보안성을 갖는 공개키 기반의 AKA 프로토콜의 설계가 필요하다.

사용자의 위치가 고정된 유선통신 환경과 달리, 휴대성과 이동성을 특징으로 갖는 이동통신 환경에서는 사용자의 위치 정보 및 사용자의 활동에 대한 보안이 중요하다. 만약 그 정보가 노출되었을 경우, 사용자의 사생활이 침해받을 수 있다. 이것은 사용자에 대한 중대한 보안 위협요소가 되기 때문에, 이동통신 환경에서 사용자 신분 정보의 기밀성, 즉 익명성은 차세대 이동통신시스템 인증 프로토콜의 개체간 상호 인증과 함께 반드시 고려해야 할 중요한 요소 중에 하나이다[1]. 기존의 이동통신 시스템에서 현재 사용중인 인증 프로토콜은 무선접속구간의 사용자 익명성 보장 관점에서 보안상 취약하다고 할 수 있다.

본 논문에서는 차세대 이동통신 시스템의 사용자와 서비스를 제공하는 네트워크간 사용자 익명성을 보장하고, 사용자와 네트워크가 상대 개체를 안전하게 상호 인증할 수 있는 공개키 시스템을 이용한 AKA 프로토콜을 제안한다.

II. 보안특성

이동통신 사용자는 언제 어디서나 보다 편리하고 안전하게 네트워크가 제공하는 서비스를 제공받고 자원을 이용하고자 한다. 이를 위해 무선접속구간의 사용자와 네트워크간 보안 프로토콜 설계에서 평가되어야 할 보안특성은 상호 개체 인증, 개체 상호간 세션 키 합의, 합의된 키의 상호 인증, 키 갱신 보증, 사용자 익명성 보장, 과금 데이터에 대한 부인방지 등이 있다[2, 3].

또한 사용자 익명성과 관련하여 임시신분의 일회사용(one-time-use), 생성된 임시신분들간의 무관계성(no direct relationship between *TID*'s), 도메인 분리(domain separation)와 같은 특성들이 고려되어야 한다[4].

III. 기존 프로토콜

표 1은 본 논문에 이용된 기호와 그에 대한 설명을 나타낸다.

기 호	설 명
M, V, H	사용자, 방문네트워크, 홈 네트워크
p	큰 소수
q	$(p-1)$을 나누는 큰 소수 인자
g	위수가 q인 Z_p^*의 원소인 생성원
ID_E	개체 E의 고유신분(식별자)
TID_M	사용자의 초기 임시신분
TID'_M	프로토콜 수행 후 새롭게 생성된 임시신분
$h()$	일방향 해쉬함수
$KH()$	keyed 일방향 해쉬함수
x_E, P_E	사용자의 개인키와 공개키 $(P_E = g^{x_E})$
K_{MV}	M과 V 사이에서 계산된 세션키
$Cert_E$	개체 E의 공개키 인증서
$r_E (\in Z_q^*)$	개체 E에 의해 생성된 임의의 수
$E_K\{\}(D_K\{$	대칭키 암호화(복호화)
$PE_K\{\}$	공개키 암호화

표 1: 사용된 기호와 그에 대한 설명

1. SMA95 프로토콜

이 프로토콜은 대칭키 암호시스템에 기반하고 있으며, 사용자 익명성을 위해 TID 계산에서만 공개키 암호시스템을 사용한다[4].

$$AUTH_{AB} = [r_A, T_A, Token\{A, T_A, r_A\}_{K_{AB}}]$$
$$TICK\{A, B, C, K_{BC}\}_{K_{AB}} = Token\{r_A \oplus C, r_B, r_A \oplus A\}_{K_{AB}} \oplus K_{BC}$$
$$Token\{A, T_A, r_A\}_{K_{AB}} = E_{K_{AB}}\{A \oplus E_{K_{AB}}\{T_A \oplus E_{K_{AB}}\{r_A\}\}\}$$

$$M \rightarrow V: H, TID_M, AUTH_{MV}$$
$$V \rightarrow H: TID_M, TID_V, AUTH_{VH}$$
$$V \leftarrow H: PE_V\{r_M\}, TICK\{H, V, TID_M, K_{MV}\}_K$$
$$M \leftarrow V: TICK\{V, TID_M, V, P_V\}_{K_{MV}}$$

$$TID_M = PE_H\{r_M, r_M \oplus ID_M\}$$
$$TID'_M = PE_V\{r'_M, r'_M \oplus TID_M\}$$

그림 1: SMA95 프로토콜.

그림 1에서 알 수 있듯이, 익명성 제공을 위해 각 세션별로 변하는 랜덤 수 r_M과 ID_M(또는 TID_M)을 H(또는 V)의 공개키로 암호화한다. 처음 프로토콜 실행을 통해 TID_M의 설정이 끝난 후에는, M과 V는 다음 세션에 사용될 TID'_M을 각각 계산하여 공유하게 된다. 이 프로토콜은 앞에서 살펴본 익명성 요구사항을 모두 만족하나, 이동통신 환경에서의 AKA 프로토콜의 보안특성을 제공하지 않는다.

2. ASPeCT 프로토콜

이 프로토콜은 공개키 암호시스템을 기반으로 하며, 상호인증과 프로토콜 내에 과금 관련 데이터를 통합하여 서비스 이용에 대한 사용자 검증 및 서비스 부인방지 등의 보안 특성을 더욱 강화하였다[1].

$$M \rightarrow V: g^{r_M}, ID_T$$
$$M \leftarrow V: r_V, h(K_{MV}, r_B), chd, T_V, Cert_V$$
$$M \rightarrow V: E_{K_{MV}}[Sig_M\{h(g^{r_M}, P_V, r_V, ID_V, chd, T_V, Pay)), Cert_M, pay]$$
$$session\ key: K_{MV} = h((P_V)^{r_M}) = h((g^{r_M})^{x_V})$$

그림 2: ASPeCT 프로도콜.

그림 2에서 보는 바와 같이 인증 프로토콜의 세 번째 메시지에서, 사용자는 세션키로 암호화된 증명서와 서명을 전송함으로써 사용자 익명성을 제공한다. 그러나 사용자의 신분을 확인하기 위해서는 프로토콜의 마지막 메시지까지 진행해야 하는 단점이 있다. 또한 forward secrecy를 제공하지 않는다[5].

3. GK01 프로토콜

이 프로토콜은 인증 및 TID 계산 모두 공개키 암호시스템에 기반하고 있으며, SMA95와 ASPeCT 프로토콜에서 지적된 문제점들을 해결하였다[6].

$$session\ keys: K_{MH} = g^{x_M \cdot r_M}$$
$$K_{VH} = h(g^{r_V \cdot r_H}, g^{r_H \cdot x_V})$$
$$K_{MV} = h(g^{r_M \cdot r_V}, g^{x_V \cdot r_M})$$

$$M \rightarrow V: g^{r_M}, TID_M, ID_H$$
$$V \rightarrow H: g^{r_V}, g^{r_M}, TID_M, T_V, Cert_V, sig_V\{h(g^{r_V}, g^{r_M}, TID_M, ID_V)\}$$
$$V \leftarrow H: E_{K_{VH}}[sig_H\{h(g^{r_H}, g^{r_V}, h(ID_M) \oplus g^{r_M}, ID_H)\}, h(ID_M) \oplus g^{r_M}], g^{r_H}, T_H, Cert_H$$
$$M \leftarrow V: g^{r_V}, T'_V, Cert_V, E_{K_{MV}}\{h(g^{r_V}, g^{r_M}, TID'_M, ID_V), T_H\}$$
$$M \rightarrow V: E_{K_{MH}}[sig_M\{h(g^{r_M}, g^{r_V}, T_H, ID_V)\}, T'_V, Cert_M]$$

$$TID_M = \{h(ID_M) \oplus g^{r_M}\}_{K_{MH}}$$
$$TID'_M = h(g^{r_M \cdot r_V}, h(ID_M))$$

그림 3: GK01 프로토콜.

그림 3에서 보는 바와 같이 사용자 익명성을 제공하기 위해서 임시신분을 사용하며, 임시신분은 프로토콜 초기에 사용자에 의해 생성되어 프로토콜 실행동안 사용자와 네트워크에 의해 갱신된다. 이 프로토콜에서는 네트워크가 초기에 사용자의 신분을 확인할 수 있으며, 임시신분 정보는

사용자와 네트워크가 상호 선택한 랜덤 수에 따라 세션별로 갱신되므로 익명성을 보장하고 기존의 방식과 비교하여 보다 강화된 안전성을 보장한다. 그리나 단말장치의 제한된 연산능력에 비해 사용자측에서의 과도한 연산량을 필요로 하는 단점이 있다.

Ⅳ. 제안한 AKA 프로토콜

1. Signcryption

네트워크를 통해 두 사용자가 메시지를 주고받을 때, 전송되는 메시지의 기밀성을 유지하고 당사자간에는 메시지의 출처를 확인할 수 있도록 하는 가장 효과적인 방법은 공개키 암호 방식을 사용하는 것이다. 즉, 전송할 메시지를 송신자의 비밀키로 서명 한 후 수신자의 공개키로 암호화하여 전송하는 것이다. 이러한 방법을 "서명 후 암호화 기법(signature-then -encryption)"이라 하는데, 이 방법은 메시지의 기밀성 유지나 송신자의 인증에는 적합하나 서명 생성 및 암호화 과정에 공개키 암호 방식을 사용하므로 많은 연산량이 요구된다는 단점이 있다.

이러한 문제점을 해결하기 위해 1997년 Y. Zheng은 디지털 서명과 암호 시스템의 기능을 동시에 만족하면서 요구되는 연산량과 통신비용을 줄인 효율적 기법인 signcryption을 제안하였다[7, 8]. signcryption은 기밀성과 인증성을 동시에 제공하므로 키 합의(key agreement)에 사용될 수 있으며, 실제로 Y. Zheng은 signcryption을 키 전송(key transport)과 키 교환(key exchange)에 적용하였다[9].

Signcryption에서 서명자와 검증자는 미리 서로의 공개키를 알고 있어야 하며 AKA 프로토콜에서 sign -cryption의 사용은 서명 후 암호화기법을 사용하는 것보다 연산량과 통신 오버헤드를 감소시킨다.

2. 새로운 프로토콜 제안

인증 프로토콜의 설계에 있어서 각 개체에 대한 초기 가정은 다음과 같다. 공개키 인증서와 관련하여 사용자와 네트워크는 상대 개체가 신뢰할 수 있는 신뢰기관(TTP)이 발행하는 자신의 공개키 인증서를 가지고 있으며, 각각 상대 개체의 인증서 검증이 가능한 신뢰기관의 공개키를 가지고 있다.

1) 사용자 익명성을 보장하는 AKA 프로토콜

사용자 익명성을 보장하고, 사용자 측에서의 효율적인 연산에 중점을 둔 새로운 인증 및 키 합의 프로토콜을 제안한다. 제안된 프로토콜은 GK01 프로토콜을 개선한 것으로, 같은 보안특성 및 익명성 요구사항을 만족하면서도 [10]에서 제안한 signcryption을 이용하여 사용자 측에서의 연산량과 통신 오버헤드를 감소시켰다.

(1) M : $K_{MH}=(P_H)^{r_M}$, $TID_M=E_{K_{MH}}\{h(ID_M)\oplus g^{r_M}\}$
$M \rightarrow V$: g^{r_M}, TID_M, ID_H
(g^{r_M}, TID'_M ⇒ M과 V사이의 통신시 사용)

(2) $V \rightarrow H$: g^{r_V}, g^{r_M}, TID_M, T_V, $Cert_V$, $sig_V\{h(g^{r_V}, g^{r_M}, TID_M, ID_V)\}$

(3) H : $K_{MH}=(g^{r_M})^{x_H}$, $K_{VH}=h((g^{r_V}P_V)^{r_H})$
$m_H=g^{r_V}\|h(ID_M)\|ID_H$
$r=KH_{g^{r_H}}(m_H)$, $s=r_H/(r+x_H)$,
$c=E_{K_{VH}}\{r, s, h(ID_M)\oplus g^{r_M}\}$
$V \leftarrow H$: g^{r_H}, c, T_H, $Cert_H$

(4) V : $K_{VH}=h((g^{r_H})^{r_V+x_V})$
$D_{K_{VH}}\{c\}$, $g^{r_H}=(P_Hg^r)^s$, $r=KH_{g^{r_H}}(m_H)$
$K_{MV}=h((g^{r_M})^{r_V+x_V})$, $TID'_M=h(K_{MV}, h(ID_M))$
$M \leftarrow V$: g^{r_V}, T'_V, $Cert_V$, $h(g^{r_V}, TID'_M, ID_V)$

(5) M : $K_{MV}=h((g^{r_V}P_V)^{r_M})$
$TID'_M=h(K_{MV}, h(ID_M))$
$m_M=g^{r_V}\|P_V\|ID_V\|T'_V$
$r=KH_{g^{r_M}}(m_M)$, $s=r_M/(r+x_M)$
$c=E_{K_{MV}}\{r, s, Cert_M\}$
$M \rightarrow V$: c

(6) V : $D_{K_{MV}}\{c\}$, $g^{r_M}=(P_Mg^r)^s$, $r=KH_{g^{r_M}}(m_M)$

그림 4: 제안된 AKA 프로토콜.

사용자 M이 새로운 네트워크 V에 처음으로 방문할 경우, M은 그의 홈 네트워크 H의 적법한 가입자임을 밝히기 위해 V와 제안된 프로토콜을 이용하여 등록절차를 시작한다. 그림 4에서 알 수 있듯이, 프로토콜의 실행이 끝난 후에 M과 V는 사용자의 새로운 임시신분 TID'_M을 공유하게 되며, 이는 후에 두 개체사이에 일어나는 통신에 사용자 익명성 보장을 위해 사용되어 진다. M이 V에 등록절차를 걸친 후, 이후의 M과 V의 통신은 이미 공유된 TID'_M을 이용하여 이루어진다.

2) 제안한 프로토콜에 대한 보안특성 분석

① 상호 개체 인증

M에서 V, V에서 H, H에서 V쪽으로 서명과 인증서를 통한 명확한 개체 인증이 제공된다. V에서 M쪽으로는 해쉬값과 인증서를 통한 함축적 개체 인증이 제공된다.

② 상호 키 인증

키 생성에 사용된 랜덤수들(r_M, r_V, r_H)과 비밀키들(x_V, x_H)은 자신이외의 다른 개체들이 알 수 없으므로 각 개체들 사이의 상호 함축적 키 인증이 제공된다. M에서 V, H에서 V쪽으로 세션키로 암호화된 메시지를 보냄으로써 키 확인을

수행한다. 따라서 명확한 키 인증이 제공된다.

③ 상호 키 합의 및 키 신규성

세션키 생성에서 키 생성함수는 랜덤 수 r_M, r_V, r_H을 사용한다.

④ 사용자 익명성

M에 대한 모든 정보가 암호화되어서 전송되므로 익명성이 보장된다.

⑤ 부인방지

M에서 V로 가는 정보에 서명을 하므로 M은 V에 보낸 정보를 부인할 수 없게 된다. 또한 V와 H는 서로에게 보내는 정보에 서명을 하므로 서로가 보낸 정보에 대해 부인할 수 없다.

⑥ Forward secrecy

프로토콜에 참여하는 개체의 비밀키가 노출된 경우에도 이전 세션에 대한 안전성에 영향을 미치지 않는다. 랜덤한 입력값에 의해 계산된 세션키 K_{MV}, K_{VH}와 임시신분 TID'_M에서 DDH가정과 안전한 해쉬 함수의 사용을 가정하면 세션키 K_{MV}, K_{VH}와 임시신분 TID'_M의 계산 및 확인이 불가능하다[8].

⑦ 익명성 요구사항

각 세션마다 변하는 난수 r_M과 r_V를 사용함으로써 대응되는 세션의 임시신분의 신규성을 보장한다. 따라서 임시신분은 그 세션에서만 유일하게 한번 사용된다. 같은 이유로 사용자의 임시신분 사이에 직접적인 관계가 없다. 또한 사용자가 새로운 네트워크를 방문할 때, 신분정보가 암호화되어있는 새로운 TID_M을 보내게 되며 이 때 사용된 암호화키는 M에 의해 생성된 난수 r_M에 따라 변한다. 방문 네트워크 사이의 협정이 있더라도 H로부터 M에 대한 관련 신분정보를 받기 전까지는 새로운 방문 네트워크는 고유신분을 알 수 없으며, V는 H로부터 그런 정보를 얻기 위해서는 먼저 자신의 증명서와 서명을 보내야 한다. 따라서 방문 네트워크 사이에 도메인 분리가 이루어진다.

3) 기존 프로토콜들과의 비교

제안된 프로토콜의 보안 특성 및 익명성, 사용자 측에서의 연산량에 대하여 기존의 이동통신 인증 프로토콜인 SMA95, ASPeCT, GK01 프로토콜과 비교하여 표 2, 표 3에 나타내었다. 표 3에서 ( )는 등록절차 후, M과 V사이의 사용자측에서의 연산량을 나타낸다.

① 보안 특성 및 익명성 비교

	SMA95	ASPeCT	GK01	Proposed protocol
상호개체인증	×	O	O	O
상호 키 인증	×	O	O	O
상호 키 합의	×	O	O	O
Forward secrecy		×	O	O
익명성 요구사항	O		O	O

표2 : 보안 특성 비교.

표 2에서 알 수 있듯이, 제안된 프로토콜은 앞에서 살펴본 ASPeCT 프로토콜의 사용자 신분확인의 지연 문제와 forward secrecy를 해결한 GK01 프로토콜과 같은 보안 특성을 갖는다.

② 사용자 측에서의 연산량 비교

	SMA95	ASPeCT	GK01	Proposed protocol
SKE	6	2	3(2)	2(1)
PKE	1			
Ex.		1	2(1)	1(1)
PreEx.		1	2(2)	2(1)
Sig		1	1(1)	
	△	△	×(△)	∧(O)

표3 : 사용자 측에서의 연산량 비교.

** Notation

SKE : 대칭키 암호 방식

PKE : 공개키 암호 방식

Ex. : 모듈라 지수승

PreEx. : 사전 계산된 모듈라 지수승

Sig : 서명에 사용된 모듈라 지수승

일반적으로 공개키 암호시스템은 대칭키 암호시스템보다 1000배 정도의 연산 비용이 들므로, 연산량 비교에서 제안된 프로토콜과 공개키 기반 방식인 ASPeCT, GK01 프로토콜에 대해 살펴본다. 연산량 계산의 대부분은 지수승 연산이라고 가정한다.

표 3에서, 먼저 M이 V에 처음 방문하여 등록절차를 거칠 경우를 살펴보자. M, V, H 사이에 일어나는 등록 프로토콜에 대하여 같은 조건의 GK01 프로토콜보다 적은 연산량을 보이며, ASPeCT 프로토콜과 같은 연산량을 보여준다.

한편 등록절차 후, M과 V 사이의 프로토콜 수행에서는 GK01 프로토콜보다 연산량이 두 배 정도로 줄어들며 ASPeCT 프로토콜보다도 적은 연산량을 보여준다. 사전 계산 단계를 제외한 프

로토콜 실시행 단계만을 고려할 경우, 제안된 프로토콜은 모듈라 지수승 연산을 한번밖에 실행하지 않으며 이는 계산 능력이 적은 단말기를 사용하는 응용에 적합함을 보여준다.

V. 결론

사용자와 서비스를 제공하는 네트워크간 사용자 익명성을 보장하고 사용자와 네트워크가 상대실체를 안전하게 상호 인증할 수 있는 공개키 암호 방식을 기반으로 개선된 AKA 프로토콜을 제안하였다. 또한 제안된 프로토콜의 안전성을 분석하였으며 보안특성 및 익명성, 사용자 측에서의 연산량 관점에서 이전에 제안된 프로토콜과 비교분석하였다.

제안된 프로토콜은 기존의 프로토콜들에 비해 강화된 안전성을 보장하면서도 사용자측에서의 연산량과 통신 오버헤드를 감소시켰다. 또한 방문 네트워크를 서비스 제공자로 홈 네트워크를 TTP로 가정할 경우, 사용자와 부가가치 서비스를 제공하는 서비스 제공자간의 API(authentication and payment initiali- zation) 프로토콜에 적용할 수 있다.

참고문헌

[1] K.M. Martin and C.J. Mitchell, "Evaluation of authentication protocols for mobile environment value-added services", draft, 1998.

[2] G. Horn, K.M. Martin and C.J. Mitchell, "Authentication protocols for mobile network environment value-added services", IEEE Trans. on Vehi. Tech., 51, pp. 383-392, 2002.

[3] G. Horn and B.Preneel, "Authentication and payment in future mobile systems", Computer Security - ESORICS'98, LNCS 1485, pp. 277-293, 1998.

[4] D. Samfat, R. Molva and N. Asokan, " Untraceability in mobile networks", Proceedings of the First Annual International Conference on Mobile Computing and Networking, pp. 26-36, 1995.

[5] D.G. Park, C. Boyd and S.J. Moon, "Forward secrecy and its application to future mobile communications security", Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC2000, LNCS 1751, pp. 433-445, 2000.

[6] J.S. Go, K.J. Kim, "Wireless authentication protocol preserving user anonymity", SCIS2001, vol. 1/2, pp. 159-164, Jan., 2001

[7] Y. Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption)", Advances in Cryptology - CRYPTO'97, Springer-verlag, LNCS 1294, pp. 165-179, 1997.

[8] Y. Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions", Proceedings of 1997 Information Security Workshop (ISW'97), LNCS 1397, pp.291-312, Springer-verlag, 1998.

[9] Y. Zheng, "Compact and unforgeable session key establishment over an ATM network", In Proceedings of IEEE INFOOM'98, pp. 411-418, 1998.

[10] K.H. Lee, S.J. Moon, "AKA protocols for mobile communications", ACISP 2000, LNCS 1841, pp. 400-411, 2000.