논문 2012-50-3-4

영지식 증명을 이용한 가입기간이 정해진 서비스에서 이동 통신 기기간 인증 기법

(Scheme for Verification Between Mobile Devices in a Service with Expiration Time by Using Zero-knowledge Proof)

박 영 훈*, 서 승 우**

(Young-Hoon Park and Seung-Woo Seo)

요 약

이동 통신 기술이 발달함에 따라 통신 기기간의 메시지 교환이 가능한 서비스가 생겨나고, 그 사용 횟수가 폭발적으로 늘고 있다. 기기간의 통신을 위해서는 통신 기기간의 서비스 구성원이라는 인증이 선행되어야 한다. 하지만, 기존 인증 기술은 Trusted party와 같은 제 삼자와의 통신이 수반되는데, 이로 인하여 대역폭이 낭비되거나, 기지국 범위 밖의 이동 통신 기기는 기기간 통신에 참여할 수 없다는 문제점이 발생할 수 있다.

본 논문에서는 제 삼자의 개입이 없는 새로운 이동 통신 기기간 인증 기법을 소개할 것이다. 제안된 기술에 대하여, 서비스의 가입 여부 및 서비스 가입 시간을 모두 검증해야 하므로, 이를 가능하게 하는 새로운 영지식 증명 기법을 개발하여 적용할 것이다. 또한, 이 영지식 증명 기법은 인증정보를 암호화된 그대로 검증하기 때문에 증명 하고자 하는 기기의 프라이버시가 보장이 되며, 질의-응답 방식을 사용하기 때문에 다른 기기의 인증 메시지를 재사용하는 공격으로부터 보호할 수 있다.

Abstract

As the mobile communication technology is developed, the services for communication between the mobile devices are provided, and the amount of usage is increasing tremendously. For the device-to-device communication, the device should be verified if it is a service member. The existing verification schemes include interactions with the third party, while this may cause the problems that the bandwidth is dissipated and the devices which are out of the communication range of the base station cannot communicate with other devices.

To solve such problems, we propose a new scheme for verification between mobile devices without interaction of third party. For the proposed scheme, we develop and employ a new zero-knowledge proof protocol, which verifies the device's membership and its expiration time. Furthermore, the scheme guarantees privacy of the mobile device since it checks the encrypted verification message without decrypting, and protects replaying attack since it uses challenge-response method.

Keywords : device-to-device verification, zero-knowledge proof, strong Diffie-Hellman

Ⅰ. 서 론

통신 기술이 발달함에 따라 이동 통신 기기와 기지국과의 통신은 물론, 이동 통신 기기간의 통신도 가능하게 되었다. 이동 통신 기기간 통신을 통하여 기기간에 유용한 정보를 주고받을 수 있을 뿐 아니라 기지국에서 전달된 정보를 hop-by-hop으로 다른 이동 통신 기기에 전달할 수도 있다.[1] 이에 따라, 기기간 통신(M2M)이나

* 정회원, 삼성전자 소프트웨어 센터
(Software Center, Samsung Electronics)
** 정회원, 서울대학교 전기컴퓨터공학부
(Department of Electrical and Computer Science, Seoul National University)
※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2012-000918).
접수일자: 2013년1월3일, 수정완료일: 2013년2월18일

VANET과 같이, 기지국과 기기간의 통신과 기기간의 통신을 모두 제공하는 서비스가 생겨나고 있고, 이 두 가지 방식을 모두 제공하는 서비스는 점점 확산되어갈 것이다.[2~3] 이러한 서비스는 대부분 전용망을 사용하기 때문에, 유료로 제공되는 경우가 많다(ex. 기기간 통신(M2M)이 3G망 혹은 LTE망을 사용하는 경우,[2] 또는 VANET에서 차량간의 통신이 802.11p 망을 사용하는 경우[3]). 그리고 유료 서비스는 가입 시작 시점과 종료 시점이 명확히 결정되어 있다.

상기 언급한 형태의 기기간의 통신에서 가장 중요한 점은 정보를 주거나 받는 기기가 같은 서비스에 가입되었는지에 관한 여부를 확인하는 것이다.[4] 정보를 제공하는 기기의 경우, 서비스에 가입이 되어 있지 않았다면 잘못된 정보를 제공해 줌으로써 부당한 이득을 취할 수 있다. 또한, 정보를 제공 받는 기기의 경우, 서비스에 가입 되어있지 않은 상태에서 불법으로 정보를 받아볼 수 있다. 따라서 이동 통신 기기간의 통신이 이루어지기 전에는 반드시 상대방 기기에 대한 인증 과정이 필요하다.

기존의 유료 서비스에서의 이동 통신 기기간 통신 기술에서는 기기간 인증 시 제 삼자(예를 들면 서비스 관리자)와의 메시지 교환이 반드시 필요했다.[2] 하지만 서비스에 가입하는 이동 통신 기기의 수가 늘어날 경우, 이동 통신 기기간의 정보 교환의 수가 늘면서 그 인증 요청 메시지도 폭발적으로 늘 것이다. 이렇게 되면 대역폭의 소모가 심해져서 일반적인 통신 활동에 방해가 될 수 있다. 또한, 기지국의 통신 범위 밖에 있는 이동 통신 기기들은 인증 자체를 요청하거나 받을 수 없으므로 이동 통신 기기간의 통신이 제한될 수 있다.

이동 통신 기기간의 통신에서 상대방에 대한 인증 이외에도 프라이버시 문제가 발생할 수 있다. 이동 통신 기기는 인증을 위하여 자기 자신의 정보를 보내주게 되는데, 이 정보를 암호화되지 않은 채로 보낸다면 그 기기의 위치가 그대로 노출되고, 이에 따라 기기 사용자의 위치 프라이버시가 침해될 수 있다.[5] 따라서 인증 메시지는 반드시 암호화된 채로 전송이 되어야 하며, 그 자체로 메시지의 진실성이 증명되어야 한다.

상기 언급한 문제들을 해결하기 위하여, 본 논문에서는 이동 통신 기기간의 제 삼자의 개입이 없는 프라이버시가 보장되는 인증 기법을 제안할 것이다. 제안된 인증 기법의 특징은 다음과 같다.

1) 인증 과정에서 인증을 해 주는 기기는 증명을 받고자 하는 기기의 인증 정보를 이용하는데, 인증 정보를 그대로 줄 경우, 그 기기의 소유자에 대한 프라이버시가 침해되게 된다. 또한, 그 기기의 인증 정보를 검증해 줄 제 삼자가 없기 때문에 인증 정보를 위조하여 서비스에 가입된 것처럼 인증을 해 주는 기기를 속일 수 있다. 따라서 제안된 기술은 인증 정보의 기밀성 및 위조 방지성을 보장하기 위하여 영지식 증명 방법을 사용한다.[6]
2) 네트워크에서 기존의 영지식 증명은 사용자의 비밀키와 같은 비밀 정보를 검증하는데 주로 사용된다. 제안하는 기술은 증명을 받고자 하는 이동 통신 기기의 서비스 가입 기간도 한꺼번에 검증해야 하는데, 이는 기존 영지식 증명만으로는 불가능하다. 따라서 본 논문에서는 비밀 정보와 공개 정보의 진실성을 한꺼번에 증명할 수 있는 새로운 영지식 증명을 제안할 것이다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 논문에서 제안되는 기술을 위한 배경 기술을 설명할 것이다. 그리고 Ⅲ장에서는 새로운 영지식 증명의 이론적 배경이 되는 Modified Strong Diffie-Hellman 문제를 정의하고, 이를 바탕으로 Ⅳ장에서 새로운 영지식 증명을 제안할 것이다. Ⅴ장에서는 제안된 영지식 증명을 이용하여 이동 통신 기기간의 인증 프레임워크를 제안하고, Ⅵ장에서는 제안된 프레임워크의 연산 시간과 보안성을 수학적으로 분석할 것이다. 마지막으로 Ⅶ장에서 논문을 마무리할 것이다.

Ⅱ. 배경 설명

1. 네트워크 모델

그림 1은 이 논문에서 가정하고 있는 네트워크 모델을 나타내고 있다. 네트워크를 구성하는 요소는 TA, 기지국, 그리고 이동 통신 기기이다. 각각의 역할은 다음과 같다.

- **TA (Trusted Authority)**: TA는 인증과 관련된 모든 키들을 생성하고 관리한다. 시스템 초기화와 기기의 가입 및 탈퇴를 담당한다. 또한, 인증 과정에서 문제가 발생했을 경우, 그 인증 메시지가 누구로부터 나온 것인 지 추적도 가능하다. TA는 보안성이 완벽하여 외부의 공격 및 침입에 매우 강하며 연산 능력도 충분하다고 가정한다.

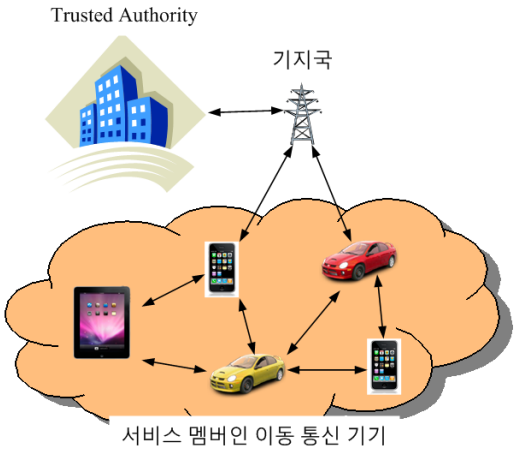


그림 1. 네트워크 모델
Fig. 1. Network model.

- **기지국**: 기지국은 TA와 이동 통신 기기 사이에서 중계를 담당한다. 즉, TA에서 이동 통신 기기로 정보가 전달될 때 기지국을 거치며, 반대로도 마찬가지이다. 단, 이동 통신 기기 사이의 인증 과정에서는 기지국이 전혀 관여되지 않는다. 기지국의 통신 범위에 있지 않는 지역이 존재한다고 가정한다.

- **이동 통신 기기**: 이동 통신 기기는 자유롭게 이동 가능한 기기이며, 기지국 또는 다른 이동 통신 기기와 통신이 가능하다. 이동 통신 기기간의 통신 과정에서 한 쪽이 다른 쪽에게 서비스 가입 구성원이라는 인증을 받게 되는데, 인증을 받는 쪽을 증명자, 인증을 수행하는 쪽을 검증자라고 부른다.

2. Bilinear mapping

최근 들어, 보안이나 프라이버시가 요구되는 네트워크에서 Bilinear mapping은 메시지를 암호화된 채로 인증할 수 있다는 장점 때문에 차세대 인증 기법에 널리 쓰이고 있다.[7~8] 또한, 점차 이동 통신 기기의 성능이 향상되고 있고, Bilinear mapping의 한 기법인 Tate pairing은 연산량과 소요 시간이 다른 Bilinear mapping에 비해 매우 적기 때문에 이동 통신 기기용으로 가능하다고 보고 있다.[9~10]

G_1, G_2, G_T를 각각 소수 p를 기반으로 하는 곱셈 순환군이라 하자. 또한, $g_1 \in G_1$, $g_2 \in G_2$는 생성자이며, 동형 사상 $\psi : G_2 \rightarrow G_1$이 존재하여, $\psi(g_2) = g_1$이라 하자. 이 때, $e : G_1 \times G_2 \rightarrow G_T$가 다음을 만족할 때 e를 bilinear mapping이라 부른다.

a) 이진성: 임의의 $u \in G_1$, $v \in G_2$와 임의의 정수 a, $b \in \mathbb{Z}_p$에 대하여, $e(u^a, v^b) = e(u,v)^{ab}$를 만족한다.
b) 일반성: $e(g_1, g_2) \neq 1$
c) 계산 가능성: $e(u,v)$를 계산할 수 있는 알고리즘이 존재

Ⅲ. p−Modified Strong Diffie−Hellman(MSDH) 문제

이동 통신 기기끼리의 인증 과정에서 제 3자와의 통신이 포함되지는 않는다. 증명자가 검증자에게 자기 자신이 서비스 그룹의 멤버임을 증명하기 위해서는 증명자의 비밀키(x)와 서비스 그룹에 가입한 시간(t_j)과 서비스 그룹을 이탈한 시간(t_d)를 모두 검증 받아야 하고 검증자는 증명자의 이러한 정보들의 진실성을 증명해야 한다. 여기서 x는 검증자에게 공개되면 안 되는 정보이지만 t_j와 t_d는 현재 시각과 비교하여 증명자가 서비스 그룹의 멤버인지 확인해야 하므로 검증자에게 공개되어야 하는 정보이다. 즉, 검증자는 암호화된 x와 암호화되지 않은 t_j t_d의 진실성을 증명해야 한다.

Strong Diffie-Hellman(SDH) 문제는 Boneh.et.al에 의하여 제안되었고, 비밀 키(x)의 진실성을 검증하기 위한 수단으로 쓰이고 있다.[11] 즉 SDH 문제를 푸는 것은 매우 어렵다는 사실이 진실성을 증명하고자 하는 값이 변조되지 않았음을 증명해 주고 있다. 하지만, 이 논문에서는 x 뿐 아니라 공개된 정보인 t_j, t_d도 검증해야 하므로 세 값을 한꺼번에 검증하기 위한 변형된 SDH 문제인 MSDH 문제를 제안하고자 한다.

표 1. 변수 설명
Table 1. Notations.

값	의미
p	큰 소수
G_1, G_2	곱셈 순환군
g_1, g_2	생성자
t_j	증명자의 서비스 그룹 가입 시간
t_d	증명자의 서비스 그룹 이탈 시간
x	증명자의 비밀 키
k	증명자의 공개 키(g_2^x)
C	증명자의 인증서($g_1^{1/(x+\gamma t_j+\delta t_d)}$)
γ, δ	인증서 검증을 위한 비밀값
J, D	인증서 검증을 위한 도움값(g_2^{γ}, g_2^{δ})

G_1, G_2를 소수 p를 위수로 하는 곱셈 순환군(multiplicative cyclic group) 이라 하고, $g_1 \in G_1$ $g_2 \in G_2$를 각각 생성자(generator)라 하자.

p−Modified Strong Diffie-Hellman 문제:
γ, x, $t \in \mathbb{Z}_p$에 대하여, $(p+2)$개의 값 $(g_1,\ g_2,\ g_2^{\gamma},\ g_2^{\gamma^2},\ g_2^{\gamma^3},\cdots,\ g_2^{\gamma^p})$이 주어져 있을 때, 순서쌍 $(g_1^{\frac{1}{x+\gamma \cdot t}},\ x,\ t)$를 유도해 내는 문제.

p−MSDH 문제를 푸는 것이 충분히 어렵다는 것은 다음으로부터 알 수 있다.

정리 1. p−MSDH를 푸는 것은 p−SDH를 푸는 것 보다 쉽지 않다.

증명: $\Pr[B|A]$를 A가 주어진 상태에서 B를 유도할 확률이라고 하자. 그리고, $g_1' = g_1^{1/t}$, $x' = x/t$라고 하자. t가 공개된 값이기 때문에 g_1'역시 공개된 값이다. 그러면, 다음과 같은 확률 식이 성립한다.

$$\begin{aligned}&\Pr\left[\left(g_1,\ g_2,\ g_2^{\gamma},\ g_2^{\gamma^2},\cdots,\ g_2^{\gamma^p}\right)\middle|\left(g_1^{\frac{1}{x+\gamma\cdot t}},x,t\right)\right]\\ =\ &\Pr\left[\left(g_1^{1/t},\ g_2,\ g_2^{\gamma},\ g_2^{\gamma^2},\cdots,\ g_2^{\gamma^p}\right)\middle|\left(g_1^{\frac{1}{t}\cdot\frac{1}{x'+\gamma}},x,t\right)\right]\\ =\ &\Pr\left[\left(g_1',\ g_2,\ g_2^{\gamma},\ g_2^{\gamma^2},\cdots,\ g_2^{\gamma^p}\right)\middle|\left(g_1'^{\frac{1}{x'+\gamma}},x'\right)\right]\end{aligned}$$

상기 확률 식에서 마지막 식은 p−SDH 문제이다. 즉, p−MSDH 문제가 풀릴 필요충분조건이 바로 p−SDH 문제가 풀리는 것이다. 따라서 p−MSDH를 푸는 것은 p−SDH를 푸는 것 보다 쉽지 않다. ■

위의 p−MSDH 문제를 일반화하면 다음과 같다.

일반화된 p−MSDH 문제:
m, x, γ_1, γ_2, $\cdots$, γ_m, t_1, t_2, $\cdots$, $t_m \in \mathbb{Z}_p$에 대하여, $(g_1, g_2, g_2^{\gamma_1}, g_2^{\gamma_2}, \cdots, g_2^{\gamma_m})$이 주어져 있을 때, $(g_1^{\frac{1}{x+\gamma_1 t_1+\gamma_2 t_2+\cdots+\gamma_m t_m}}, x, t_1, t_2, \cdots, t_m)$을 유도해 내는 문제.

정리 2. 일반화된 p−MSDH 문제는 p−SDH 문제보다 쉽지 않다.

증명: 수학적 귀납법으로 증명한다.

$m=1$이면 정리 1에 의해 자명.

$m=m_0$일 때 성립 가정하고, $m=m_0+1$일 때를 살펴보자.

$x+\gamma_{m_0+1}t_{m_0+1}=x'$라 하자. 그러면, $m=m_0+1$일 때 일반화된 p−MSDH문제는 다음과 같은 2단계로 풀 수 있다.

a) $(g_1, g_2, g_2^{\gamma_1}, g_2^{\gamma_2}, \cdots, g_2^{\gamma_{m_0}}, g_2^{\gamma_{m_0+1}})$에서 마지막 한 인자를 제외한 나머지 인자들로 다음을 유도

$$(g_1^{\frac{1}{x'+\gamma_1 t_1+\gamma_2 t_2+\cdots+\gamma_{m_0} t_{m_0}}}, x', t_1, t_2, \cdots, t_{m_0})$$

b) $x'=x+\gamma_{m_0+1}t_{m_0+1}$을 만족하는 x와 t_{m_0+1}을 찾기 위하여, $(g_1^{\frac{1}{x+\gamma_{m_0+1}t_{m_0+1}}}, x, t_{m_0+1})$를 유도.

위의 과정에서 a)는 $m=m_0$일 때의 일반화된 p−MSDH 문제를 푸는 과정이다. 즉, $m=m_0+1$일 때의 일반화된 p−MSDH 문제를 풀기 위해서는 $m=m_0$일 때의 문제를 우선 풀어야 하므로 $m=m_0+1$일 때의 문제가 $m=m_0$일 때의 문제보다 쉽지 않다. 이 때, $m=m_0$일 때의 문제는 귀납 가정에서 p−SDH를 푸는 것 보다 쉽지 않다고 했으므로 결론은 성립한다. ■

본 논문에서 제안하는 기술은 공개된 정보가 서비스 그룹 가입시각과 탈퇴시각과 같이 두 개이므로 $m=2$일 때의 p−MSDH 문제를 이용할 것이다.

Ⅳ. p−MSDH를 이용한 영지식 증명 기법

이 절에서는 Ⅲ에서 제안했던 p−MSDH를 이용하여 증명자가 보낸 값들을 검증자가 검증하는 기법을 제안할 것이다. 제안하는 기법의 목표는 1) 증명자의 정보의 진실 여부를 검증자가 파악할 수 있어야 하고 2) 증명자의 비밀키(x)의 값은 검증자가 알 수 없어야 하며 3) 증명자의 프라이버시를 위하여 검증자는 증명자가 누구인지조차 몰라야 한다는 것이다. 제안 기법을 위하여 믿을 수 있는 기관 TA (Trusted Authority)를 추가로 둘 것이다.

두 개의 소수 p를 위수로 하는 곱셈 순환군 G_1, G_2와 생성자 $g_1 \in G_1$, $g_2 \in G_2$, 그리고 임의의 두 정수 γ, $\delta \in \mathbb{Z}_p$를 생각하자. 여기서 g_1, g_2, γ, δ는 모두 TA에

의해 생성된 값들이며, 특히 γ, δ는 TA 이외의 다른 사용자들에게는 비공개 처리 된다. TA는 두 개의 도움 값 $J=g_2^{\gamma}$, $D=g_2^{\delta}$를 계산하고, J, D는 검증자 증명자 모두에게 공개한다. 참고로, J는 t_j를 검증하기 위한, 그리고 D는 t_d를 검증하기 위한 값들이다.

x, t_j, t_d를 각각 증명자의 비밀키, 서비스 그룹에 가입한 시간, 서비스 그룹을 이탈한 시간이라고 하자. 이제, 증명자는 검증자에게 이 세 값의 진실성을 증명할 것이다. 하지만 비밀키 그 자체는 보안이 유지되어야 하므로 x 대신 증명자의 공개키인 $k=g_2^x$를 검증받는다. 이 때 세 값의 위조를 방지하기 위하여 증명자의 인증서인 $C=g_1^{\frac{1}{x+\gamma t_j+\delta t_d}}$를 도입한다. 인증서는 TA에 의해 만들어지며, $p-$MSDH 문제를 푸는 것이 어렵다는 것에 근거하여 C를 증명자가 만들어낼 수는 없다. 인증서 C는 다음 수식을 만족한다.

$$e(C,k\cdot J^{t_j}\cdot D^{t_d})=e(g_1,g_2)$$

즉, 검증자는 증명자의 인증서(C), 공개키 (k), 그리고 시간 정보(t_j, t_d)의 진실성을 위의 수식이 성립하는지 여부를 통하여 알아낼 수 있다. 하지만, C, k를 그대로 검증자에게 보여줄 경우 증명자가 누구인지 알 수 있게 되기 때문에 위 3)에 어긋난다. 따라서 인증서와 공개키 자체도 암호화하여 보낸다.

우선 μ, $\nu\in\mathbb{Z}_p$를 도입하자. 여기서 μ, ν는 TA에 의해 만들어지고, TA 외에 다른 개체에는 공개되지 않는 값들이다. 그리고 TA는 $u=g_1^{\mu}$, $v=g_1^{\nu}$, $h=g_1^{\mu\nu}$를 계산하여 이 값들을 검증자, 증명자에게 나누어준다. 이제 증명 및 검증 방식은 다음과 같다.

1) 증명자는 α, $\beta\in\mathbb{Z}_p$를 임의로 선택한다. 이 때, α, β는 증명자만이 알고 있는 값이다.
2) 증명자는 다음과 같은 세 값을 계산한다.

$$T_1=u^{\alpha},\ T_2=v^{\beta},\ T_3=C\cdot h^{\alpha+\beta}$$

3) 증명자는 r_{α}, r_{β}, r_x, r_{χ_1}, $r_{\chi_2}\in\mathbb{Z}_p$를 임의로 선택한다. 이 다섯 개의 값 역시 증명자만이 알고 있는 값들이다.
증명자는 다음과 같은 다섯 개의 값을 계산한다.

$$R_1=u^{r_{\alpha}},\ R_2=v^{r_{\beta}}$$

$$R_3=\frac{e(T_3,g_2)^{r_x}}{e(h,g_2)^{r_{\chi_1}+r_{\chi_2}}\cdot e(h,J^{t_j}D^{t_d})^{r_{\alpha}+r_{\beta}}}$$

$$R_4=T_1^{r_x}\cdot u^{-r_{\chi_1}},\ R_5=T_2^{r_x}v^{-r_{\chi_2}}$$

증명자는 다음 값을 검증자에게 보낸다.

$$(T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5,t_j,t_d)$$

4) 검증자는 우선 현재 시각이 t_j와 t_d 사이에 있는지 확인한다. 만일 현재 시각이 위의 두 값 사이에 있지 않다면 아직 가입이 되지 않았거나 가입 기간이 끝난 사용자이므로 증명자는 서비스 그룹의 가입자가 아닌 것이 된다. 따라서 검증자는 증명자가 서비스 그룹의 가입자가 아닌 것으로 판명하고 검증 절차를 종료한다. 만일 현재 시각이 두 값 사이에 있으면 그 다음 절차로 넘어간다.
5) 검증자는 임의의 질의값 $c\in\mathbb{Z}_p$를 생성하고 증명자에게 c를 보낸다.
6) 증명자는 다음과 같은 응답값들을 계산하고 이를 검증자에게 보낸다.

$$s_{\alpha}=r_{\alpha}+c\alpha,\ s_{\beta}=r_{\beta}+c\beta,\ s_x=r_x+cx$$
$$s_{\chi_1}=r_{\chi_1}+cx\alpha,\ s_{\chi_2}=r_{\chi_2}+cx\beta$$

7) 이제, 검증자는 다음과 같은 다섯 개의 식이 성립함을 증명함으로써 증명자가 보낸 값들의 진실성을 증명한다.

$$\begin{aligned}
u^{s_{\alpha}} &= T_1^c R_1\\
v^{s_{\beta}} &= T_2^c R_2\\
e(T_3,g_2)^{s_x}\cdot e(h,g_2)^{s_{\chi_1}+s_{\chi_2}}\cdot e(h,J^{t_j}D^{t_d})^{s_{\alpha}+s_{\beta}} &= \left(\frac{e(g_1,g_2)}{e(T_3,J^{t_j}D^{t_d})}\right)^c R_3\\
T_1^{s_x}u^{-s_{\chi_1}} &= R_4\\
T_2^{s_x}v^{-s_{\chi_2}} &= R_5
\end{aligned}$$

위의 과정이 과정이 끝나면 증명자는 검증자에 의해 서비스 그룹의 가입자로 확인이 끝난다.

Ⅴ. 제안 프레임워크

이 장에서는 앞 장에서 소개했던 영지식 증명 기법을 기반으로 하여 이동 통신 기기간의 인증 프레임워크를 소개할 것이다. 이 장은 프레임워크 초기화, 새로운 기기 가입, 기기간 인증 과정, 잘못된 사용자 색출로 구성되어 있다.

1. 프레임워크 초기화

이 절에서는 프레임워크를 처음 시작할 때, 혹은 동작 중인 프레임워크를 다시 초기화할 때 TA가 진행하는 순서를 제안할 것이다. 여기서 세 개의 곱셈 순환군 G_1, G_2, G_T와 동형 사상 $\psi : G_2 \rightarrow G_1$, 그리고 bilinear map $e : G_1 \times G_2 \rightarrow G_T$는 주어져 있다고 가정한다.

1) $g_1 \in G_1$, $g_2 \in G_2$를 무작위로 생성한다. 이 때, $\psi(g_2) = g_1$을 만족해야 하며, g_1, g_2는 둘 다 법 p에 대하여 원시근이어야 한다.
2) γ, $\delta \in \mathbb{Z}_p$를 임의로 생성한다. 이 두 값은 다른 기기들에게는 비밀로 한다.
3) 도움값 $J = g_2^{\gamma}$, $D = g_2^{\delta}$을 계산한다.
4) μ, $\nu \in \mathbb{Z}_p$를 임의로 생성한다. 이 두 값 역시 다른 기기들에게는 비밀로 한다.
5) $h = g_1^{\mu\nu}$, $u = g_1^{\mu}$, $v = g_1^{\nu}$, $h_0 = g_2^{1/\mu\nu}$, $u_0 = g_2^{1/\mu}$, $v_0 = g_2^{1/\nu}$를 계산한다.
6) $(g_1, g_2, J, D, h, u, v, h_0, u_0, v_0)$를 모든 서비스 그룹의 사용자들에게 전송한다.
7) 각각의 사용자에 대하여 인증서를 계산하여 보내준다.

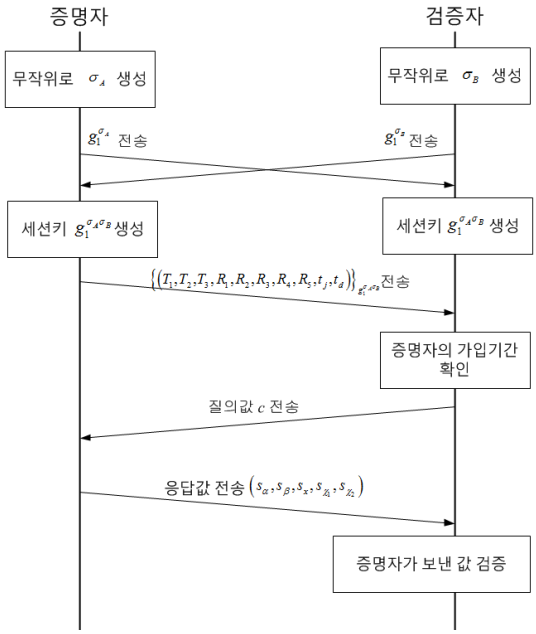


그림 2. 제안된 이동 통신 기기간 인증 과정
Fig. 2. Proposed process for verification between mobile devices.

2. 새로운 기기 가입

이 절에서는 이동 통신 기기가 서비스 그룹에 새로 가입했을 때 진행하는 과정을 소개할 것이다.

1) 이동 통신 기기가 서비스 그룹에 가입하는 시간(t_j)과 서비스 그룹에서 이탈하는 시간(t_d)을 결정하고, 이들을 ID와 함께 TA에게 알려준다.
2) TA가 이동 통신 기기의 유효성을 검사한다.
3) TA가 가입하려는 이동 통신 기기의 비밀키 $x \in \mathbb{Z}_p$를 생성한다. 여기서 $x \notin \{1, p-1\}$이어야 하고, $\gcd(x + \gamma t_j + \delta t_d, p-1) = 1$을 만족해야 한다.
4) TA가 가입하려는 이동 통신 기기의 인증서 C $(g_1^{\frac{1}{x+\gamma t_j+\delta t_d}})$를 계산한다.
5) TA가 비밀키 x와 인증서 C를 가입하려는 이동 통신 기기에 암호화 하여 전달한다.

3. 기기간 인증 과정

이 절에서는 이동 통신 기기간의 인증 과정을 설명할 것이다. 이 절에서 사용되는 기호는 Ⅳ장에서 사용된 기호와 동일하게 사용된다. 증명자와 검증자의 메시지를 주고 받는 과정은 다음과 같다.

1) 증명자가 검증자에게 인증 요청을 한다
2) 증명자와 검증자가 각각 무작위로 정수 σ_A, $\sigma_B \in \mathbb{Z}_p$를 생성한다.
3) 증명자가 검증자에게 $g_1^{\sigma_A}$를 전달하고 검증자는 증명자에게 $g_1^{\sigma_B}$를 전달한다.
4) 증명자는 $\left(g_1^{\sigma_B}\right)^{\sigma_A}$를 이용해서, 검증자는 $\left(g_1^{\sigma_A}\right)^{\sigma_B}$를 이용하여 세션 키 $g_1^{\sigma_A\sigma_B}$를 각각 계산한다.
5) 증명자가 Ⅳ장의 영지식 증명방식의 2)와 같이 변수들을 계산하고 이를 다음과 같이 세션 키로 대칭키 암호화 방식으로 암호화 하여 검증자에게 보내준다. $\{(T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5, t_j, t_d)\}_{g_1^{\sigma_A\sigma_B}}$

6) 검증자는 증명자가 보낸 메시지를 세션 키로 복호화 한다.
7) 검증자가 현재 시각이 t_j와 t_d 사이에 있는지 확인 한다. 만일 그렇지 않다면 5)에서 보냈던 증명자의 인증 메시지를 TA에게 보내고, 프로세스를 종료한다.
8) 검증자가 증명자에게 질의값 c를 보낸다.
9) 증명자는 Ⅳ장의 영지식 증명방식의 8)과 같이 응답값을 계산하고, 검증자에게 보내준다.
10) 검증자는 Ⅳ장의 영지식 증명방식의 9)와 같이 값을 검증한다. 만일 검증에 실패하면 5)에서 보냈던 증명자가 인증메시지로 사용되었던 것들을 TA에게 보낸다.

위 검증 방식에서 처음에 세션 키로 암호화한 이유는 증명자의 정보 중 t_j, t_d가 제 3자에게 노출되는 것을 방지하기 위함이다. 이 시간 정보가 노출될 경우 증명자로부터 전송되는 메시지를 엿들음으로써 제 3자의 증명자 추적이 가능하게 된다. 따라서 증명자의 위치 프라이버시가 보장되지 않게 될 수 있기 때문에 t_j, t_d를 암호화하여 전송하게 된다.

4. 잘못 된 사용자 색출

이 장에서는 인증 과정에서 잘못 된 사용자에 대하여 인증 메시지가 누구의 것인지 밝히는 과정을 살펴볼 것이다. 이 과정은 위 3장의 과정 7)과 10)에서 검증 실패로 TA에게 인증 메시지를 보냈을 때 TA가 인증 메시지가 누구로부터 온 것인지를 색출해 낸다. 이 과정으로 불법으로 인증 받으려는 이동 통신 기기가 어떤 것인지 밝힐 수 있을 뿐 아니라 어떤 이동 통신 기기가 다른 기기의 정보를 도용해서 사용하고 있을 때 그 다른 기기가 어떤 것인지 알아내어 도용 당한 기기에게 알려줄 수도 있다.

잘못 된 사용자 색출 과정은 다음과 같다.

1) TA는 검증자로부터 T_1, T_2, T_3를 전송받는다.
2) $C = T_3 \cdot T_1^{-\nu} \cdot T_2^{-\mu}$를 계산한다.
3) C가 누구의 인증서인지 찾아낸다.

위의 과정에서 $T_3 \cdot T_1^{-\nu} \cdot T_2^{-\mu}$의 결과가 인증서가 나오는 이유는 다음과 같다.

$$T_3 = Ch^{\alpha+\beta} = Cg_1^{\mu\nu(\alpha+\beta)}$$

$$T_1^{-\nu} = u^{-\alpha\nu} = g_1^{-\alpha\mu\nu}$$

$$T_2^{-\mu} = v^{-\beta\mu} = g_1^{-\beta\mu\nu}$$

이므로 위와 같이 계산하면 g_1이 포함된 항이 상쇄되고 C가 남기 때문이다.

5. 사용자 탈퇴 및 퇴출

사용자가 서비스 그룹을 이탈하는 경우는 유효기간이 만료되어 탈퇴하는 것과 잘못된 정보 유출이나 보안상의 문제로 서비스 그룹에서 퇴출시키는 것이 있다. 전자의 경우, 인증 과정에서 검증자가 증명자의 탈퇴 시각 t_d를 검사하고, t_d의 진실성까지 검증하는 과정이 있다. 따라서 유효기간 만료에 따른 사용자 탈퇴를 위한 별도의 프로세스는 필요 없다.

사용자가 퇴출되더라도, 사용자가 가지고 있는 인증서를 비롯한 인증 정보는 유효하다. 즉, 퇴출된 사용자가 기존의 인증 정보를 이용하여 서비스 그룹 멤버들에게 인증을 시도할 수 있다. 이를 방지하기 위하여 다음 두 가지 방식이 쓰인다. 하나는 공유하고 있는 값을 바꾸는 것이고, 다른 하나는 CRL (Certificate Revocation List)에 퇴출된 사용자를 올리는 방법이다.

첫 번째 방법은 γ와 δ의 값을 바꾸어 도움값인 J, D를 변경하고 업데이트 된 J와 D를 남아 있는 서비스 그룹 멤버들에게 나누어준다. 또한, 각 서비스 그룹 멤버들의 인증서가 γ와 δ값에 의해 결정되는데, γ와 δ가 바뀌었으므로 인증서 역시 바꾸어서 보내준다. 이렇게 되면, 퇴출된 사용자는 소유하고 있는 인증서를 이용하여 인증 받을 수 없게 된다.

첫 번째 방법만 사용할 경우, 모든 서비스 그룹 멤버들과 통신해야 하므로 명백히 통신비용이 많이 발생한다. 이를 보완하기 위한 방법으로 CRL에 퇴출된 사용자를 올리는 방법이 있다[12~13]. CRL은 퇴출된 사용자들의 인증서값으로 구성되어있는 리스트로서, 검증자가 증명자의 보낸 값을 검사할 때, 모든 CRL에 있는 인증서값 C에 대하여, 다음 식이 성립하는지 검사한다.

$$e(T_3/C, h_0) = e(T_1, u_0) \cdot e(T_2, v_0)$$

상기 등식이 성립하는 인증서 C가 존재한다면, 그 증명자는 퇴출된 증명자이다.

CRL의 크기는 시간에 정비례하여 증가하는 속성이

있다[8]. 즉, 시간이 충분히 경과하면 CRL의 크기가 커져서, 매 인증시마다 퇴출된 사용자인지 검사하는 시간이 길어진다. 따라서 CRL의 크기가 정해진 값이 되면 CRL을 비우고 첫 번째 방법인 모든 서비스 그룹 사용자들에게 새로운 공유값 및 업데이트된 인증서를 보내준다.

VI. 제안 프레임워크의 성능 분석

1. 인증 시간 분석

이 절에서는 제안된 이동 통신 기기간의 인증 기술에서 소요되는 시간을 분석할 것이다. 소요되는 시간은 크게 연산시간과 통신시간으로 나눌 수 있다. 연산시간은 연산량과 비례하므로 연산 오버헤드를 분석하는 지표로도 사용될 수 있을 것이다.

연산 과정에서 Bilinear mapping과 대칭키 기반 암호화방식이 가장 많은 시간을 소요한다. 따라서 연산시간은 Bilinear mapping과 대칭키 기반 암호화방식이 사용된 횟수를 알아보면 된다. 증명자의 입장에서는 세 번의 Bilinear mapping이 사용되었고, 검증자의 입장에서는 다섯 번의 Bilinear mapping이 사용되었다. 또한, 증명자는 한 번의 대칭키 기반 암호화 방식의 암호화를, 그리고 검증자는 복호화를 하였다. Bilinear mapping과 대칭키 기반의 암호화방식을 연산하는데 걸리는 시간을 각각 t_B, t_S라 한다면, 증명자와 검증자의 연산 시간은 각각 $3t_B+t_S$, $5t_B+t_S$이다. 또한, 총 다섯 번의 메시지 교환이 있고, 그 중 두 개는 동시에 일어나므로 통신하는데 걸리는 시간을 t_C라 한다면, 발생하는 총 시간은 $8t_B+2t_S+4t_C$가 된다. Y. Kawahara 등의 연구결과[9]와 같이, 1GHz CPU에서 Bilinear mapping을 연산하는 데 수행되는 시간이 32.50ms임과 $t_S \ll t_B$임을 감안하면, 통신 시간을 제외한 연산 시간은 300ms 내외로 걸릴 것이다. 즉, 통신 속도만 보장된다면 실시간 인증이 가능할 것이다.

2. 보안성 분석

이 절에서는 제안한 프레임워크에 발생할 수 있는 공격에 대하여 얼마나 잘 방어할 수 있는지 분석할 것이다.

가. 증명자가 변수들을 위조하여 인증 하려는 경우

해당 공격의 목표는 가입 기간이 끝나거나 아직 가입이 시작되지 않은 이동 통신 기기가 불법적으로 인증을 받고자 하는 것이다. 이를 위하여 증명자는 가입 기간을 변조해야 할 것이다. 증명자의 원래 비밀 키 및 가입 기간을 각각 x, t_j, t_d라 하고, 변조된 가입 기간을 t_j', t_d'라 하자. 이 때 다음과 같은 세 가지의 공격 시나리오가 존재한다.

(1) 가입 기간만 변조할 때

이 경우, 인증자가 인증을 받기 위해서는 다음 식이 성립해야 한다.

$$e(C,k \cdot J^{t_j'} \cdot D^{t_d'}) = e(g_1,g_2)$$

이 식이 성립할 필요충분조건은 다음과 같다.

$$\gamma t_j + \delta t_d \equiv \gamma t_j' + \delta t_d' (\mathrm{mod} p-1) .$$

위 식을 만족하는 t_j'와 t_d'의 쌍의 개수는 $p-1$개다. t_j'와 t_d'를 뽑을 수 있는 전체 경우의 수가 $(p-1)^2$개이므로 인증자가 인증에 성공할 확률은 $\frac{1}{p-1}$이 된다. p는 매우 큰 소수이므로 가입 기간만 변조했을 때 인증에 성공하기는 거의 불가능하다고 볼 수 있다.

(2) 가입 기간과 비밀 키를 변조할 때

변조된 비밀 키를 x'라 하고, $k' = g_2^{x'}$라 하자. 그러면, 인증자가 인증을 받기 위해서는 다음 식이 성립해야 한다.

$$e(C,k' \cdot J^{t_j'} \cdot D^{t_d'}) = e(g_1,g_2)$$

이 식이 성립할 필요충분조건은 다음과 같다.

$$x + \gamma t_j + \delta t_d \equiv x' + \gamma t_j' + \delta t_d' (\mathrm{mod} p-1).$$

t_j', t_d'가 고정되어 있을 경우, 위의 식을 만족하는 x'는 단 하나 존재한다. x'를 뽑을 수 있는 전체 경우의 수가 $p-1$가지이므로 인증에 성공하기 위한 x'를 선택할 확률은 $\frac{1}{p-1}$이다. 역시 p는 매우 큰 소수이므로, 비밀 키까지 변조하더라도 인증 받는 것은 것의 불가능하다고 볼 수 있다.

(3) 가입 기간, 비밀 키, 인증서를 모두 변조할 때

변조된 비밀 키, 인증서를 각각 x', C'라 하고,

$k' = g_2^{x'}$라 하자. 인증자가 인증을 받기 위해서는 다음 식이 성립해야 한다.

$$e(C', k' \cdot J^{t_j'} \cdot D^{t_d'}) = e(g_1, g_2)$$

이를 만족하는 x, t_j', t_d', C'을 생성하는 것은 거의 불가능하다. 이는 $p-$MSDH 문제를 푸는 것이 매우 어렵다는 것에 기반 한다. 즉, 인증서를 비롯한 모든 인증 정보를 위조하더라도 불법적으로 인증 받는 것은 거의 불가능함을 알 수 있다.

나. 증명자가 다른 이동 통신 기기의 인증 정보를 도용하는 경우

이동 통신 기기간의 인증 과정에서 Ⅴ.3의 과정 5)와 같이 증명자는 검증자에게 자신의 인증 정보를 보내게 된다. 이 때, 검증자는 그 인증 정보를 저장해 놓고, 검증자 자신이 증명자가 되었을 경우 그 인증 정보를 활용할 수 있다.

하지만, 이 경우 역시 증명자는 자신을 증명할 확률이 매우 낮다. 그 이유는 증명자가 검증자의 질의값에 대한 올바른 응답값을 계산할 수 없기 때문이다. 즉, 질의값에 대한 응답값을 구하기 위해서는 Ⅳ장의 과정 8)과 같이 난수 r_α, r_β, r_x, r_{χ_1}, r_{χ_2}, α, β와 비밀 키 x를 모두 알고 있어야 하는데, 증명자가 알고 있는 값은 오직 $(T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5, t_j, t_d)$ 뿐이기 때문이다. 따라서 증명자가 다른 사용 가능한 이동 통신 기기의 인증 정보를 사용한다고 하더라도 질의-응답 과정에서 제대로 된 응답값을 보내 주지 못 하게 되므로 인증은 실패하게 된다.

Ⅶ. 결 론

본 논문에서는 가입 기간이 정해진 서비스에서 제 삼자의 개입이 없는 이동 통신 기기간의 인증 기술을 제안하였다. 제안된 기술에 적용된 새로운 영지식 증명 기법에 의해 증명자의 서비스 가입 여부 및 가입 기간 확인이 한번에 이루어질 수 있게 되었다. 또한, 제안된 영지식 증명 기법은 인증 정보를 노출시키지 않으므로 사용자의 프라이버시가 보호되며 질의-응답 방식을 사용함으로써 되풀이공격을 방지할 수 있게 되었다.

참 고 문 헌

[1] 류민우, 차시호, 조국현. 2010. “이동하는 차량 간 통신의 신뢰성 향상을 위한 개선된 탐욕 메시지 포워딩 프로토콜.”, *전자공학회논문지-TC*, 제47권, 제4호, 43-50쪽

[2] TR 22.868-800 Study on Facilitating Machine to Machine Communication in 3GPP Systems

[3] A. Sebastian, M. Tang, Y. Feng, and M. Looi, “A multicast routing scheme for ecient safety message dissemination in VANET,” *In Wireless Communications and Networking Conference* (WCNC), 2010 IEEE, pages 1-6, Apr 2010.

[4] 최재덕, 정수환. 2008. “빠른 이동성을 지원하는 VANET 환경의 핸드오버 인증 프로토콜,” *전자공학회논문지-TC*, 제45권, 제5호, 30-39쪽

[5] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. P. Hubaux, “Secure vehicular communication systems: design and architecture,” *Comm. Mag.*, Vol. 46, no. 11, pp. 100-109.

[6] 권창영, 이인숙, 원동호. 1993. “영지식 대화형 증명 방식 및 응용 프로토콜.”, *전자공학회논문지*, 제20권, 제2호, 190-203쪽

[7] D. Boneh, and M. Franklin, “Identity-based encryption from the weil pairing,” *SIAM J. Comput.*, Vol. 32, no. 3, pp. 586-615, Mar 2003.

[8] X. Lin, X. Sun, P. Ho, and X. Shen. “GSIS: A secure and privacy-preserving protocol for vehicular communications,” Vehicular Technology, IEEE Transactions on, Vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[9] Y. Kawahara, T. Takagi, and E. Okamoto. “Efficient Implementation of Tate Pairing on a Mobile Phone Using Java,” In Computational Intelligence and Security, Lecture Notes In Artificial Intelligence, Vol. 4456, 396-405 Springer-Verlag, Berlin, Heidelberg.

[10] S. D. Galbraith, K. Harrison, and D. Soldera. 2002. “Implementing the Tate Pairing,” In Proceedings of the 5th International Symposium on Algorithmic Number Theory (ANTS-V), Claus Fieker and David R. Kohel (Eds.), 324-337 Springer-Verlag, London, UK, UK.

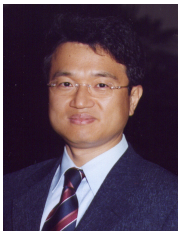
[11] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures, ” In proceedings of CRYPTO 04, pages 41-55, LNCS series, Springer-Verlag, 2004.

[12] G. Atenies, D. Song, and G. Tsudik, “Quasi-efficient revocation of group signatures,” in Proc. Financ. Cryptogr., Southampton, pp. 183-197,

Bermuda, Mar. 2002.
[13] D. Boneh and H. Shacham, “Group signatures with verifier-local revocation,” in Proc. ACM CCS, pp. 166-177, Washington DC, Oct. 2004.

저 자 소 개

박 영 훈(정회원)
2006년 2월 서울대학교 전기공학부 학사
2008년 2월 서울대학교 전기공학부 석사
2013년 2월 서울대학교 전기공학부 박사
2013년 3월～현재 삼성전자 소프트웨어센터 Cloud Computing Lab 책임 연구원
<주관심분야: 네트워크 보안, 암호학, 시스템 최적화>



서 승 우(정회원)
1987년 2월 서울대학교 전기공학과 학사
1989년 2월 서울대학교 전기공학과 석사
1993년 12월 펜실베니아 주립대학 박사
1996년～현재 서울대학교 공과대학 전기컴퓨터공학부 교수
2009년 9월～현재 서울대학교 지능형자동차IT 연구센터 센터장
<주관심분야: 자동차 IT, 유무선 통신망 보안 및 자원 최적화, 스마트그리드>