情報保護學會論文誌
第19卷 第3號, 2009. 6

효율적이고 안전한 SIP 사용자 인증 및 키 교환*

최 재 덕,† 정 수 환‡
숭실대학교 정보통신전자공학부

Efficient and Secure User Authentication and Key Agreement in SIP Networks*

Jaeduck Choi,† Souhwan Jung‡
School of Electronic Engineering, Soongsil University

요 약

본 논문에서는 SIP UA와 서버 사이에서 HTTP Digest 인증과 TLS를 대신하여 효율적이고 안전한 사용자 인증 및 키 교환 기술을 제안한다. 기존에 다양한 SIP 인증 및 키 교환 기술들이 연구되었지만, 이동 단말과 같이 자원 활용이 한정적인 SIP UA에서 암호학적 연산량에 대한 부담이 여전히 존재한다. 제안 기술은 HTTP Digest 인증 기법의 사전 공격 문제를 해결하고 홉 간 보안을 위하여 Diffie-Hellman 키 교환 알고리즘을 사용하여 보안성을 강화하였다. 또한 자원이 충분하지 않은 SIP UA에서 수행해야 하는 Diffie-Hellman 알고리즘의 지수 모듈러 연산을 SIP 서버에게 위임하는 방법을 사용하여 제안 기법이 기존 기법들보다 암호학적 연산량에 대한 에너지 소모량이 적다. 제안 기술은 SIP 표준 인증 절차를 크게 수정하지 않고 필요한 인증 파라미터만을 추가하여 간단하게 구현할 수 있기 때문에 이미 널리 사용되고 있는 SIP 환경에 쉽게 적용할 수 있다.

ABSTRACT

This paper proposes an efficient and secure user authentication and key agreement scheme instead of the HTTP digest and TLS between the SIP UA and server. Although a number of security schemes for authentication and key exchange in SIP network are proposed, they still suffer from heavy computation overhead on the UA's side. The proposed scheme uses the HTTP Digest authentication and employs the Diffie-Hellman algorithm to protect user password against dictionary attacks. For a resource-constrained SIP UA, the proposed scheme delegates cryptographically computational operations like an exponentiation operation to the SIP server so that it is more efficient than the existing schemes in terms of energy consumption on the UA. Furthermore, it allows the proposed scheme to be easily applied to the deployed SIP networks since it does not require major modification to the signaling path associated with current SIP standard.

Keywords: Authentication, Key Agreement, SIP, Diffie-Hellman

I. 서 론

IETF SIP 표준에서는 사용자 인증과 SIP 메시지를 보호하기 위하여 기존에 사용되는 HTTP Digest 인증, TLS, IPSec, S/MIME과 같은 보안 프로토콜들 사용을 정의하고 있다[1]. 사용자 인증을 위한 HTTP Digest 인증 기법이 사전 공격에 취약한 문제점이 있지만, SIP 단말과 서버 사이에서 홉 간 보안 기술인 TLS와 동시에 사용될 경우 안전한 인증 서비스를 제공할 수 있다. SIP 서버 사이에서도 IPSec 또는 TLS와 같은 안전한 보안 프로토콜을 적용하여

접수일(2008년 12월 18일), 수정일(2009년 2월 9일), 게재확정일(2009년 3월 5일)
* 본 연구는 숭실대학교 교내연구비 지원에 의해 이루어진 연구 결과입니다.
† 주저자, cjduck@cns.ssu.ac.kr
‡ 교신저자, souhwanj@ssu.ac.kr

SIP 메시지들을 보호하고, SIP 사용자들 간에도 S/MIME 기술을 사용하여 상호 인증 및 SIP 메시지를 안전하게 보호할 수 있다. 이와 같이 SIP 표준에서 정의하고 있는 보안 프로토콜들은 안전한 VoIP 및 3GPP 네트워크를 구성하는데 크게 기여한다.

그러나 TLS와 S/MIME은 PKI 기반의 보안 프로토콜이기 때문에 PKI 환경이 구축되지 않은 환경에서는 적용하기 어렵다. 게다가 TLS 경우에는 SIP 이동 단말과 서버 사이에서 성능 문제로 실제 네트워크에 적용하기 어려운 문제점이 있다. 예를 들어, VoIP 이동 및 소형 단말 또는 3GPP 휴대 단말과 같이 단말의 성능 및 배터리 사용이 제한적인 경우에, 많은 메시지 교환과 암호학적 연산량을 요구하는 TLS 보안 프로토콜은 이동 단말의 자원을 비효율적으로 사용한다.

이와 같은 SIP 보안 프로토콜의 실질적인 적용 문제를 해결하기 위하여 다양한 연구가 진행되고 있다. SIP 단말과 서버 사이에서 안전한 사용자 인증 및 홉 간 보안을 위하여, 기존의 HTTP Digest 인증 기법과 TLS을 대신하여 DH (Diffie-Hellman) 또는 ECC (Elliptic Curve Cryptography) 기반의 암호 알고리즘을 사용한 기법들이 연구되었다[3-5]. 한편으로 TLS와 같은 PKI 기반의 보안 기술을 대체하기 위하여 IBC (ID-based Cryptosystem)[8] 기반의 공개키 암호 알고리즘을 이용한 인증 및 키 교환 기술이 연구되었다[9-11]. 기존 기술들이 PKI 요구사항 문제를 해결하고 안전한 보안 기술들을 제안하였지만, 자원 사용이 한정적인 이동 단말 및 소형 단말에서 암호학적 연산량에 따른 에너지 소모가 여전히 크기 때문에 전력 사용 측면에서 비효율적이다.

본 논문에서는 HTTP Digest 인증 기법과 경량화한 DH 키 교환 알고리즘을 사용하여 효율적이고 안전한 SIP 인증 및 키 교환 기술을 제안한다. 제안 기법은 보안성이 강한 DH 알고리즘에서 암호학적 연산량이 많은 지수 모듈러 연산을 SIP 단말에서 서버로 위임하는 기법을 사용하여 효율적이고 안전하다. 즉, 제안 기법은 기존 기법보다 SIP 단말에서 수행해야 하는 암호학적 연산량을 줄였기 때문에 기존 기법들보다 에너지 소모량을 최소화할 수 있어 이동 단말의 전력을 효율적으로 사용할 수 있다. 또한 제안 프로토콜은 PKI 환경을 요구하지 않고, SIP 표준 시그널링 절차를 크게 수정하지 않아도 되는 장점 때문에 현재 보급되어 있는 SIP 환경에 쉽게 적용이 가능하다.

본 논문의 구성은 다음과 같다. 2장에서 기존 SIP 보안 기술에 대해서 살펴보고, 3장에서 제안하는 효율적이고 안전한 SIP 인증 및 키 교환 기술을 설명하고, 4장에서 제안 기법의 안전성과 성능을 분석하고 기존 기법들과 비교 분석한다. 마지막으로 5장에서 결론을 맺는다.

II. 관련 기술 및 문제점 분석

SIP 표준에서 정의한 사용자 인증 기술은 사전 공격에 취약하고, 홉 간 보안 기술은 PKI 환경을 요구하거나 이동 단말에 큰 부담을 주어 실질적으로 사용되지 않는 경우가 많다. 이와 같은 문제점을 해결하기 위하여 많은 SIP 인증 및 키 교환 기술들이 연구되고 있다. 다음에서 다양하게 연구되고 있는 SIP 보안 기술들에 대해서 살펴본다.

먼저, HTTP Digest의 사전 공격 문제를 해결하고 PKI를 요구하지 않는 홉 간 보안 기술들에 대해서 살펴본다. 기존 HTTP Digest 인증 기술에 DH 키 교환 암호 알고리즘을 사용하여 SIP 단말과 서버 사이에서 안전한 사용자 인증 및 키 교환 기술이 제안되었다[3]. DH 기반의 SIP 보안 기술이 사전 공격 문제를 해결하고 있지만, DH 알고리즘은 지수 모듈러 연산을 사용하기 때문에 이동 단말에 많은 암호학적 연산량을 요구한다. ECDH 암호 알고리즘을 사용하여 안전성과 효율성을 높인 SIP 보안 기술도 제안되었다[4]. ECDH 방식의 SIP 보안 기법은 작은 키 사이즈로도 높은 안전성을 제공할 수 있는 ECC 알고리즘 사용으로 SIP 단말의 메모리 저장 공간을 적게 사용하고 암호 연산 시간이 빠른 것이 특징이다.

일반적인 SIP 기반의 VoIP 환경이 아닌 3GPP 네트워크에서 SIP 보안 기술을 위하여 ECC 암호 알고리즘과 UICC (Universal Integrated Circuit Card)와 AuC (Authentication Center) 사이에서 공유되어 있는 비밀키를 사용한 기법도 연구되었다[5]. UICC 기반의 SIP 보안 기술은 USIM (Universal Subscriber Identity Module) 카드 기반의 SIP 환경에서 보안 기술을 제안하였기 때문에 현재 일반 VoIP 폰과 같은 비 USIM 환경에서 적용이 제한적이다. 다음으로, SQL 인젝션 공격과 같이 비정상적인 문자가 포함된 SIP 메시지들을 이용한 공격들을 분석하고, IDS (Intrusion Detection System) 시스템을 이용한 해결책과[6] SIP 메시지에 해쉬 함수를 사용하여 무결성을 제공하는 방안도[7] 각각 연구되었다. 그러나 IDS 및 해쉬 함수를 이

용한 보안 기법은 여전히 사용자의 패스워드에 대한 사전 공격에 취약한 문제점이 있다.

PKI 요구 사항을 피하기 위하여, 사용자의 이메일 주소 또는 IP 주소와 같은 식별자 기반의 IBC 솔루션을 이용한 SIP 보안 기술도 연구되었다[9-11]. IBC 공개키 암호 알고리즘에서 사용자는 KGC (Key Generation Center)라는 제 3의 기관을 통해서 자신의 IBC 개인키를 발급 받는다. KGC는 자신의 비밀 마스터 키와 사용자의 ID를 사용하여 IBC 개인키를 사용자에게 발급한다. 사용자들 간에 보안 통신에서 사용자 ID는 메시지를 암호화하는 공개키 또는 서명된 메시지를 검증하는 공개키로 사용되기 때문에 인증서 교환 및 인증서 유효성 검증 절차를 요구하는 PKI 시스템을 대신하여 Ad-hoc 네트워크와 같이 네트워크 기반 구조가 없는 환경에서 많이 사용된다.

먼저, IBC 솔루션을 이용한 최초의 SIP 보안 기술은 SIP REGISTER와 INVITE 과정에서 사용자와 서버 간에 상호 인증을 제공하고, UAC (User Agent Client)와 UAS (User Agent Server) 간에 통화시 SRTP (Secure RTP)에 사용되는 세션키를 생성한다[9]. 이 보안 기법이 PKI 요구사항 없이 높은 보안성을 제공하지만, key escrow 또는 ID revocation 문제점들이 있다. 즉, IBC 솔루션에서는 근본적으로 KGC에서 사용자의 개인키를 생성하기 때문에 KGC에 의해 사용자들의 개인키가 오남용될 수 있는 key escrow 문제점이 있고, IBC 방식에서는 사용자의 ID에 매핑 되는 하나의 개인키만이 존재하기 때문에 사용자의 개인키가 공격자에 의해서 노출될 경우 그에 매핑 되는 ID는 더 이상 사용할 수 없는 문제점이 있다. 처음에 제안된 IBC 방식의 SIP 보안 기술 역시 이 두 가지 문제점을 그대로 안고 있다. 다음으로, IBC 방식 중 일방향 키 교환 기법을 이용한 빠른 SRTP 키 교환 기술이 제안되었다[10]. 일방향 키 교환 기법을 이용한 보안 기술은 SIP UAC가 INVITE 메시지를 전송하고 바로 UAS와 동일한 SRTP 마스터 키를 생성한다. 즉, UAC가 UAS로부터 200 OK 메시지를 수신한 후에 SRTP 비밀키를 생성하는 기존 IBC 방식의 SIP 보안 기법보다[9] SRTP 비밀키 생성에 필요한 시간을 줄인 것이 특징이다. 그러나 일방향 키 교환 방식의 IBC 솔루션 또한 key escrow 및 ID revocation 문제점이 있다.

마지막으로, HTTP Digest 인증 기법을 대신하여 CL-PKC (Certificateless Public Key Cryptography)라는 변형된 IBC 방식을 이용한 보안 기술이 제안되었다[11]. CL-PKC는 KGC에서 사용자의 IBC 개인키 일부를 생성하고 사용자에게 분배한다. 사용자는 KGC로부터 받은 IBC의 개인키 일부와 자신이 생성한 나머지 IBC 개인키 일부를 사용하여 완성된 IBC 개인키를 생성한다. 따라서 CL-PKC를 이용한 SIP 보안 기법에서는 사용자가 생성한 IBC 개인키 일부를 KGC가 알 수 없기 때문에 key escrow 문제를 해결하는 특징이 있다. 그러나 IBC 방식을 이용한 기존의 모든 SIP 보안 기술들은 페어링 연산을 사용하기 때문에 많은 암호학적 연산량을 요구하는 단점이 있다.

이와 같이 다양한 방면으로 SIP 보안 기술이 연구되었지만, SIP 단말과 서버 사이에서 사용자 인증과 키 교환 기능을 제공하는 기존 기술들은 암호학적 연산량 때문에 SIP 이동 단말의 배터리 소모와 같은 자원 활용 측면에서 비효율적이다.

III. 제안 기법

〔표 1〕 표기법

표 기	정 의
$H(\ )$	안전한 일방향 해쉬함수
pwd	패스워드
$\|\|$	두 개의 비트열의 연접
p	큰 소수
Z^*_p	모듈러 p로의 곱셈군
N_A, N_S, r, $nonce$	Z^*_p에 속하는 랜덤 값
g	Z^*_p의 생성자
$realm$	SIP 서버의 도메인 정보
$username$	SIP 사용자 ID
$response_x$	노드 x의 인증값
SK	DH 세션키
AK, IK, EK	SK로부터 파생된 SIP UA와 서버 간에 인증키, 무결성키, 암호화키
$Enc_k(\ )$	키 k로 암호화

제안 기법은 DH 암호 알고리즘을 사용하여 높은 보안성을 제공하면서, SIP 단말에서 수행해야 하는 지수 모듈러 연산을 SIP 서버에게 위임하는 기법을 사용하여 기존 기법들보다 배터리 사용 측면에서 효율적인 것이 특징이다. 제안 기법은 두 단계로 나뉜다. 즉, SIP 사용자 인증 및 키 교환 단계와 (단계 1, III 장 1절) SIP 메시지 보호 단계로 (단계 2, III 장 2

절) 나뉜다. 단계 1에서는 새로운 DH 세션키 SK (Session Key)를 생성하는 단계이고, 단계 2에서는 단계 1에서 생성된 DH 세션키 SK로부터 파생된 AK (Authentication Key), IK (Integrity Key), EK (Encryption Key)를 사용하여 SIP 사용자 인증 및 메시지를 보호하는 단계이다. DH 세션키 교환은 단계 1에서만 수행되고 단계 2에서는 수행되지 않는다. 본 논문에서 사용되는 기호들을 〔표 1〕에 정리하였다.

3.1 SIP 인증 및 키 교환 단계 (단계 1)

〔그림 1〕은 초기 SIP 단말과 서버 간에 인증 및 키 교환 과정을 보여준다. 먼저, SIP 서버는 사용자의 패스워드를 $H(pwd)$과 $g^{H(pwd)} \bmod p$형태로 저장한다고 가정한다.

Step 1-1. SIP UA → SIP 서버

SIP UA는 임의의 랜덤 값 $N_{A(1)}$와 r 값을 생성하고, R_1과 R_2 값을 식 (1)과 같이 생성하여 SIP Request 메시지와 함께 SIP 서버에게 전송한다. 또한 SIP UA는 $g^{H(pwd)} \bmod p$를 계산하고 $g^r \bmod p$ 값과 함께 일정 시간 동안 저장한다. 이 두 값들은 다음 단계 1의 DH 키 교환 과정에서 SIP 단말의 지수 모듈러 연산량을 줄이기 위해 재사용된다. 참고로, SIP UA의 DH 개인키인 $N_{A(1)}$는 단계 2에서 DH 세션키 사용에 대한 일정 시간이 만료되어, 단계 1을 통해 새로운 SIP 사용자 인증 및 키 교환 절차가 필요할 때 새롭게 생성된다.

$$\begin{aligned} R_1 &= N_{A(1)} + H(pwd) + r, \\ R_2 &= H(pwd) \oplus g^r \bmod p \end{aligned} \quad (1)$$

Step 1-2. SIP 서버 → SIP UA

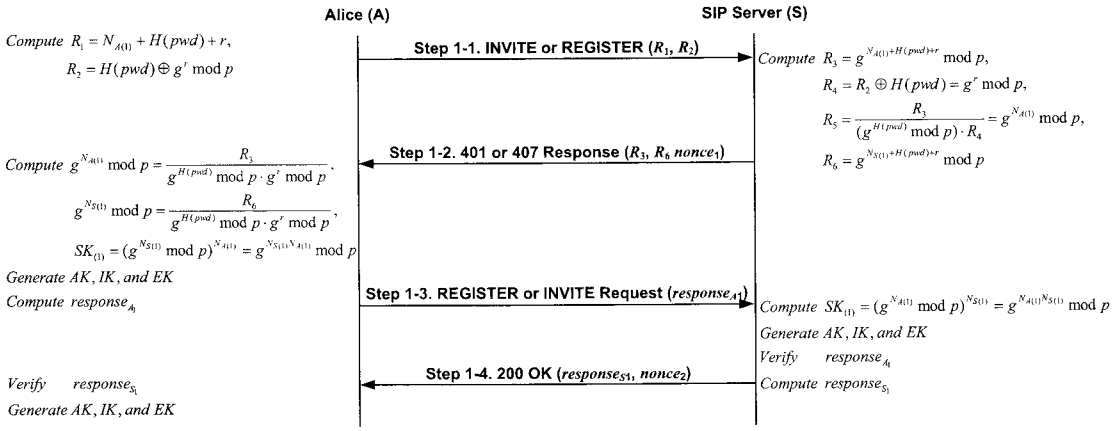
SIP UA로부터 R_1과 R_2 값을 받은 SIP 서버는 R_1에 대한 지수 모듈러 연산 값 R_3와 SIP UA의 패스워드 식별자 $H(pwd)$를 사용하여 $g^r \bmod p$ 값 R_4를 식 (2)와 같이 계산한다. 또한 SIP 서버는 사용자의 $g^{H(pwd)} \bmod p$ 값과 R_3, R_4 값을 이용하여 SIP UA의 DH 공개키 $g^{N_{A(1)}} \bmod p$ 값을 식 (3)과 같이 계산한다. 이와 같은 과정을 통해 SIP UA는 자신의 DH 공개키 $g^{N_{A(1)}} \bmod p$에 대한 지수 모듈러 계산을 SIP 서버에게 위임하여 단말의 배터리 자원을 효율적으로 사용할 수 있다. SIP 서버는 자신의 DH 공개키를 식 (3)과 같이 R_6 값으로 계산하고, R_3, R_6, $nonce_1$ 값과 함께 4XX 메시지로 UA에게 응답한다.

$$\begin{aligned} R_3 &= g^{N_{A(1)} + H(pwd) + r} \bmod p \\ R_4 &= g^r \bmod p = R_2 \oplus H(pwd) \end{aligned} \quad (2)$$

$$\begin{aligned} R_5 &= g^{N_{A(1)}} \bmod p = \frac{R_3}{(g^{H(pwd)} \bmod p) \cdot R_4} \\ R_6 &= g^{N_{S(1)} + H(pwd) + r} \bmod p \end{aligned} \quad (3)$$

Step 1-3. SIP UA → SIP 서버

SIP UA는 서버가 보내준 R_3 값과 UA에 저장되어 있는 $g^{H(pwd)} \bmod p$와 $g^r \bmod p$ 값을 사용하여 자신의 DH 공개키 값을 식 (3)에서 $g^{N_{A(1)}} \bmod p$ 계산과 같이 구한다. 여기서 SIP UA의 DH 공개키는 나눗셈 연산으로만 계산되기 때문에 기존 DH 방식에서 요구되



〔그림 1〕 초기 SIP 사용자 인증 및 키 교환 절차

는 SIP UA 측에서 지수 모듈러 연산 부담을 덜 수 있다. SIP UA는 식 (4)와 같이 SIP 서버의 DH 공개키 $g^{N_{S(1)}} \bmod p$를 계산하고, DH 세션키 SK를 생성한다. 또한 SIP UA는 식 (5)와 같이 사용자 인증키 AK, 메시지 무결성 키 IK, 메시지 암호화 키 EK를 각각의 식별 문자열과 함께 SK로부터 생성한다.

$$g^{N_{S(1)}} \bmod p = \frac{R_6}{(g^{H(pwd)} \bmod p) \cdot g^r \bmod p} \tag{4}$$

$$\begin{aligned} SK &= (g^{N_S} \bmod p)^{N_A} = g^{N_S N_A} \bmod p \\ AK &= H(SK \| "AuthenticationKey") \\ IK &= H(SK \| "IntegrityKey") \\ EK &= H(SK \| "EncryptionKey") \end{aligned} \tag{5}$$

마지막으로, SIP UA는 인증값 $response_{A1}$을 식 (6)과 같이 생성하고, SIP Request 메시지에 포함하여 SIP 서버에게 전달한다.

$$response_{A_1} = H(AK \| g^{H(pwd)} \| nonce_1 \| realm \| username \| g^{N_A} \| g^{N_S}) \tag{6}$$

Step 1-4. SIP 서버 → SIP UA

SIP 서버가 SIP UA로부터 인증값이 포함된 SIP Request 메시지를 수신하면, SIP UA의 DH 공개키 $g^{N_{A(1)}} \bmod p$와 자신의 DH 개인키 $N_{S(1)}$를 사용하여 DH 세션키 SK를 생성하고, SK로부터 AK, IK, EK를 각각 생성한다. 그리고 AK를 사용하여 SIP UA의 인증값 $response_{A1}$을 검증한다. 만약 검증에 실패하면 SIP 서버는 인증 과정을 종료한다. 인증값이 일치하면, 상호 인증을 위하여 SIP 서버도 인증값 $response_{S1}$을 식 (7)과 같이 생성하여 $nonce_2$를 포함한 200 OK 메시지와 함께 SIP UA에게 전송한다. SIP UA도 $response_{S1}$을 성공적으로 검증하면 SIP 인증 및 키 교환 과정을 마친다.

$$response_{S_1} = H(AK \| g^{H(pwd)} \| nonce_1 \| nonce_2 \| realm \| username \| g^{N_A} \| g^{N_S}) \tag{7}$$

3.2 SIP 재등록 또는 다음 콜 설정에서 보안 단계(단계 2)

앞서 설명한 초기 SIP 인증 및 키 교환 과정이 (단계 1) 끝나면, SIP UA와 서버는 생성된 AK, IK, EK를 일정 시간 동안 저장한다. 그리고 SIP UA의 재등록 과정 또는 다른 콜 설정 과정이 시작되면 이 세 키들을 사용하여 사용자 인증 및 SIP 메시지를 보호한다. 그림 2는 SIP 재등록 또는 다른 콜 설정 과정시 흡 간 보안을 보여준다.

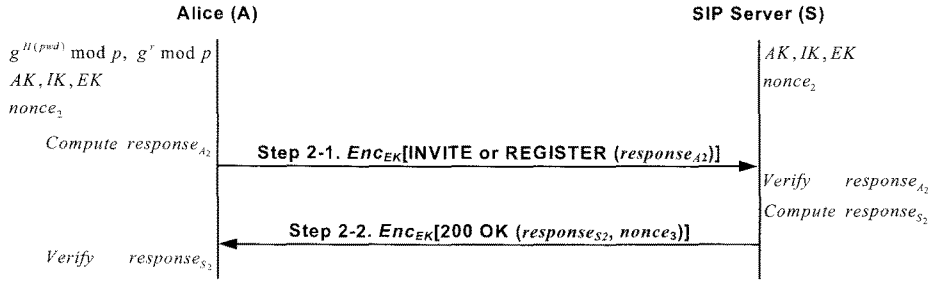
Step 2-1. SIP UA → SIP 서버

AK와 $nonce_2$를 저장하고 있는 SIP UA는 식 (8)과 같이 $response_{A2}$를 생성한다. 즉, challenge-response 구조와 같이 초기 SIP 인증에서 4번의 메시지를 교환할 필요 없이, 이전 세션에서 저장하고 있는 AK와 $nonce_2$를 사용하여 2번의 메시지 교환으로 재인증 과정을 마칠 수 있다. SIP Request 메시지를 서버에게 전송할 때는 무결성 키 IK를 사용하여 MAC (Message Authentication Code)을 생성하고 EK를 사용하여 SIP 메시지 전체를 암호한다.

$$response_{A_2} = H(AK \| g^{H(pwd)} \| nonce_2 \| realm \| username) \tag{8}$$

Step 2-2. SIP UA → SIP 서버

SIP 서버는 해당 SIP UA의 AK와 IK, EK를 사용하여 메시지를 복호화하고, MAC 값 및 $response_{A2}$ 값을 검증한다. 검증이 성공적으로 이루어지면, SIP 서버는 식 (9)와 같이 $response_{S2}$를 생성하여 $nonce_3$ 값과 함께 SIP UA에게 200 OK 메



〔그림 2〕 SIP 재등록 및 다른 콜 설정 단계에서 보안

시지를 전달한다. 마찬가지로 200 OK 메시지도 IK와 EK를 사용하여 무결성 및 기밀성이 제공된다. SIP UA는 $response_{S2}$를 검증하고 인증 절차를 마친다. 이후에 모든 SIP 메시지들은 SIP UA와 서버 사이에서 IK와 EK를 사용하여 메시지에 대한 무결성과 기밀성이 제공된다.

$$response_{S_2} = H(AK \| g^{H(pwd)} \| nonce_2 \| nonce_3 \| realm \| username) \quad (9)$$

SIP UA는 초기 인증 과정을 통해서 생성한 SK 및 AK, IK, EK의 유효 시간이 지나면 III장 1절과 같이 초기 인증 및 DH 키 교환 과정을 수행한다. 이 과정에서 SIP UA는 DH 개인키 $N_{A(2)}$ 만을 새롭게 생성하고, UA에서 저장하고 있던 $g^{H(pwd)} \bmod p$과 $g^r \bmod p$ 값들을 재사용하여 식 (3)과 같이 SIP UA에서 DH 공개키 계산을 위한 지수 모듈러 계산을 수행할 필요 없이 효율적인 인증 및 DH 키 교환 과정을 수행한다.

IV. 안전성, 성능, 비교 분석

이 장에서는 제안 기법의 안전성과 성능을 분석한다. 안전성 분석을 위하여, 다양한 공격 모델을 정의하고 제안 기법이 어떻게 대응하는지 살펴본다. 효율성 분석을 위하여 SIP UA에서 암호학적 연산량에 따른 에너지 소비량을 분석한다. 마지막으로 제안 기법과 기존 기법들과 비교 분석한다.

4.1 안전성 분석

• 사전 공격 (Dictionary attacks)

공격자는 SIP 메시지를 스니핑 한 후 사전 공격을 통해 사용자의 패스워드를 알아낼 수 있다.

패스워드를 사용하는 인증 및 키 교환 기법에서 가장 취약한 공격이 사전 공격이다. DH 기반의 제안 기법은 패스워드와 함께 DH 알고리즘을 사용하였기 때문에 사전 공격에 안전하다. 공격자가 패스워드를 포함하고 있는 R_1, R_2, R_3, R_6 메시지들을 스니핑 한다고 하더라도, 공격자는 임의의 랜덤한 N_A와 N_S, r 값들을 모르기 때문에 사용자의 패스워드를 추측할 수 없다. 여기서 r 값은 R_2에 포함되어 있지만, DLP (Discrete Logarithm Problem)에 의해서 안전하다. 공격자가 $response_A$와 $response_S$를 스닝핑 한 경우에도, DH 세션키에서 유도된 AK를 모르기 때문에 사전 공격을 수행할 수 없다. SIP 초기 인증 및 키 교환 과정 이후에는 모든 SIP 메시지들이 EK로 암호화되어 있기 때문에 공격자들이 SIP 메시지들을 스니핑 한다고 하더라도, 복호화가 어렵기 때문에 사전 공격을 수행할 수 없다.

• 중간자 공격 (MITM attacks)

SIP UA와 서버 사이에서 SIP 세션을 제어할 수 있는 공격자가 DH 키 교환으로 생성되는 세션키에 대해서 중간자 공격을 수행하여 SIP 사용자의 중요 정보를 알아낼 수 있다.

제안 기법은 DH 공개키 교환시 SIP UA와 서버 사이에서 공유된 사용자의 패스워드 식별자 $H(pwd)$를 사용하기 때문에, 공격자가 DH 공개키를 변경할 경우 SIP UA와 서버는 잘못된 인증값을 감지하고 인증 과정을 종료한다. 공격자가 SIP UA와 서버의 DH 개인키를 각각 N_A'과 N_S'로 생성하고 임의의 패스워드 pwd'를 사용하여 중간자 공격을 시도할 경우, SIP 서버는 공격자가 Step 1-3에서 보내온 인증값 $response_{A1}'$을 SIP UA는 공격자가 Step 1-4에서 보내온 인증값 $response_{S1}'$을 각각 검증하는데 실패한다. 따라서 SIP UA와 서버는 인증 및 키 교환 과정을 중단하기 때문에 공격자가 중간자 공격을 통해 사용자의 중요 정보를 알아낼 수 없다.

• 위장 공격 (Impersonation attacks)

공격자가 정당한 SIP UA 또는 서버로 위장하여 인증을 시도하거나 패스워드를 알아내기 위한 공격을 수행할 수 있다.

제안 기법은 SIP UA와 서버 사이에서 공유된 패스워드 식별자를 사용하고 DH 알고리즘의 DLP 문제 때문에 위장 공격으로부터 안전하다. 공격자가 임의의 패스워드 pwd'를 사용하여 SIP UA로 위장한 경우, 공격자는 Step 1-2 과정을 통해 SIP 서버로부터 받는 R_3와 R_6 메시지만으로 패스워드를 추출할 수 없다. 공격자는 수신한 R_3와 R_6 값을 이용하여 DH 세션키를 생성하고 임의의 패스워드 pwd'를 사용하여 $response_{A1}'$ 값을 계산한 후, Step 1-3 과정을 통해 SIP 서버에게 인증 값을 전달해야 한다. 그러나 SIP 서버는 정당한 패스워드 pwd를 모르는 공격자가 생성한 $response_{A1}'$ 값을 검증하는데 실패하고 인증 과정을 종료한다. SIP UA로 위장한 공격자는

SIP 서버로부터 Step 1-4 과정을 통해 인증이 실패했다는 메시지만 수신하고 더 이상 인증과 관련된 어떠한 정보도 받지 못하기 때문에 공격자가 SIP 서버로부터 추가 정보를 받아 패스워드를 알아내는 것이 어렵다.

공격자가 SIP 서버로 위장한 경우에, 공격자는 Step 1-3 과정에서 SIP UA로부터 수신한 인증값 $response_{A1}'$을 사용하여 사전 공격을 수행할 수 있지만, SIP 서버로 위장한 공격자는 DLP 때문에 SIP UA의 랜덤 값 N_A와 r 값을 모르기 때문에 사전 공격을 수행할 수 없다.

• 재전송 공격 (Replay attacks)

공격자가 이전에 정당한 SIP 사용자와 서버 사이에서 교환된 인증 파라미터들을 재사용하여 인증을 받을 수 있다.

재전송 공격은 *nonce* 값을 사용하기 때문에 SIP 서버에서 쉽게 차단될 수 있다. 공격자가 수집한 R_1, R_2 메시지를 재전송 하면, SIP 서버는 새로운 *nonce* 값을 포함한 4XX 메시지를 공격자에게 전달한다. 공격자는 4XX 메시지를 무시하고, 이미 수집한 $response_{A1}$ 값을 SIP 서버에게 전달하여 인증을 시도한다. 그러나 SIP 서버는 새로운 *nonce* 값으로 $response_{A1}$ 값을 검증하기 때문에 공격자가 보내온 인증값을 검증하는데 실패한다.

• DoS 공격

공격자가 대량의 SIP 인증 요청 메시지를 서버에게 전송하여 암호학적 연산량 부하를 통한 DoS 공격을 수행할 수 있다.

제안 기법은 SIP 단말의 지수 모듈러 연산을 SIP 서버에게 위임시켰기 때문에 기존 DH 암호 알고리즘을 이용한 기법보다 SIP 서버에서 수행해야 하는 지수 모듈러 연산 횟수가 많다. 그러나 3번의 지수 모듈러 연산을 실시간으로 동시에 수행하지 않기 때문에 암호학적 연산량 부하를 줄일 수 있다. 즉, R_3 계산을 위한 지수 모듈러 연산 1회는 SIP 인증 요청 메시지를 수신한 후에 실시간으로 수행하지만, SIP 서버의 DH 공개키 값인 $g^{N_S} \bmod p$는 미리 생성해 놓고 사용할 수 있다. DH 세션키 생성은 SIP 서버가 SIP UA의 인증값 $response_{A1}$을 수신한 다음에 수행하기 때문에 제안 기법은 계산량이 많은 암호학적 연산을 분산 실행함으로써 DoS 공격에 효과적으로 대응할 수 있다.

4.2 성능 분석

제안 기법을 포함한 SIP 보안 기술들의 암호학적 연산량에 따른 이동 단말의 에너지 소비량을 측정하여 효율성을 비교하였다. 실험 환경 및 내용은 다음과 같다.

• 실험 환경
- 이동 단말 : Mobile 733MHz CPU 기반의 Intel Pentium III 노트북
- 암호 라이브러리 : MIRACL[13] (지수 모듈러, 포인트 곱셈, 페어링 연산)

• 실험 내용
- 동일한 보안 강도를 갖는 각 암호 알고리즘에서 수행되는 지수 모듈러, 포인트 곱셈, 페어링 연산의 단위 수행 시간을 측정 (T_E, T_M, T_P) (해쉬 함수와 같이 수행 단위 시간이 작은 연산은 제외) [표 2]
- SIP UA와 SIP 서버 간에 INVITE, 407, INVITE, 200 OK 메시지들을 교환하는 콜 설정 과정을 가정하고, 각 보안 기법들이 적용되었을 때 SIP UA에서 수행되어야 하는 암호학적 총 연산량을 (T_{total}) 분석 [표 3]
- CPU 최대 전력 (Power) 9.3W를 이용하여 한 번의 SIP 콜 설정 단계에서 각 보안 기법이 수행될 때 소요되는 에너지양을 식 (10)과 같이 계산하고, 총 10회의 SIP 콜 설정 과정이 이루어진다고 가정하였을 때 각 SIP 보안 기법들의 누적 에너지 소모량을 비교 [그림 3]

$$Energy = T_{total} \times Power \tag{10}$$

위 실험 환경과 실험 내용을 바탕으로 Mobile 733MHz CPU 기반의 Intel Pentium III 노트북에서 MIRACL 암호 라이브러리를[13] 사용하여 지수 모듈러, 포인트 곱셈, 페어링 연산의 단위 수행 시간을 측정하여 [표 2]에 정리하였다. [표 3]은 SIP UA에서 매번 SIP 등록 또는 콜 설정 단계에서 인증 및 키 교환 과정을 수행한다고 가정할 경우, n 번을 수행할 때 요구되는 암호학적 총 연산량을 정리한 것이다. 참고로, 제안 기법은 초기 SIP 인증 및 키 교환 과정 이후에 생성된 AK, IK, EK를 사용하여 다음 SIP 등록 또는 콜 설정 단계부터는 새로운 키 교환 과정 수행 없이 생성된 세 개의 키들을 이용하여 SIP

메시지를 보호하지만, 기존 기법과의 연산량 비교를 위하여 매번 SIP 등록 또는 콜 설정 때마다 초기 사용자 인증과 키 교환 과정을 수행하는 것으로 가정하였다. 또한 IBC 솔루션 중 일방향 키 교환 방식의 보안 기법은[6] SIP 사용자 간에 SRTP 키 교환 기법이지만 SIP UA와 서버 간에 인증 및 키 교환 기법을 수행한다고 가정하고, 다른 기법들과 같이 암호학적 연산량을 계산하였다.

[표 2] 단위 암호 알고리즘 수행 시간

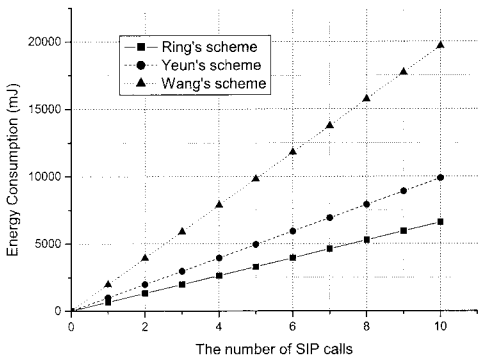
	Security size	Execution Time
T_E	1024 bit	1.121 *ms*
T_M		1.064 *ms*
T_P		34.360 *ms*

T_E: modular exponentiations
T_M: EC point multiplication
T^P: tate pairing

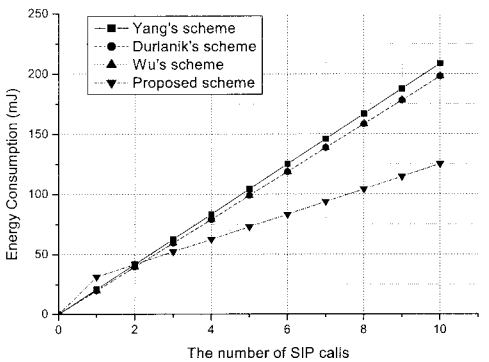
[표 3] SIP UA에서 암호학적 총 연산량 비교

Scheme	Time cost (T_{total})
Proposed scheme	$(3T_E+\sum_{i=2}^{n}1T_E)$
Yang *et al.* [3]	$\sum_{i=1}^{n}2T_E$
Durlanik *et al.* [4]	$\sum_{i=1}^{n}2T_M$
Wu *et al.* [5]	$\sum_{i=1}^{n}2T_M$
Geneiatakis *et al.* [6]	Negligible (hash function)
Ring *et al.* [9]	$\sum_{i=1}^{n}2(T_P+T_M)$
Yeun *et al.* [10]	$\sum_{i=1}^{n}3(T_P+T_M)$
Wang *et al.* [11]	$\sum_{i=1}^{n}(6T_P+5T_M)$

각 기법들의 에너지 소모량을 [그림 3]에서 비교하였다. 페어링 연산을 사용하는 IBC 방식의 기법들은 [9-11] [그림 3(a)] 기존의 다른 기법들과 제안 기법보다 [그림 3(b)] 많은 에너지 소모량을 보여준다. [그림 3(b)]에서 제안 기법은 첫 번째 SIP 인증 및 키 교환 과정에서 SIP UA가 $g^{H(pwd)}\mathrm{mod}p$와 $g^r\mathrm{mod}p$, $(g^{N_S}\mathrm{mod}p)^{N_A}$를 계산하기 때문에 3번의 지수 모듈러 연산으로 기존의 비 IBC 방식보다 비교적 많은 에너지 소모량을 보인다. 그러나 두 번째 SIP 인증 및 키 교환 과정부터는 SIP UA에서 저장하고 있는 $g^{H(pwd)}\mathrm{mod}p$와 $g^r\mathrm{mod}p$ 값들을 이용하여 DH 세션키 $(g^{N_S}\mathrm{mod}p)^{N_A}$ 생성을 위해 단 1회의 지수 모듈러 계산만을 수행하기 때문에 기본 DH 과 ECDH 기반의 기존 기법보다 암호학적 연산량에 따른 에너지 소모량이 줄어드는 것을 확인할 수 있다.



(a) IBC 기반의 SIP 보안 기술 에너지 소모량



(b) 비 IBC 기반의 SIP 보안 기술 에너지 소모량

[그림 3] SIP 단말에서 암호학적 연산량에 따른 에너지 소비량 비교

4.3 비교 분석

SIP 표준에서 정의한 보안 기술을 보완하기 위하여 많은 SIP 인증 및 키 교환 기술들이 연구되었다. 표 4에서 제안 기술을 포함한 SIP 인증 및 키 교환 기술들을 비교하였다. TLS 처럼 PKI를 요구하는 보안 기술을 대체하고 HTTP Digest의 사전 공격 문제를 해결하기 위하여 DH, ECC, IBC 등을 사용한 SIP 보안 기술들이 제안되었다. 변형된 형태의 DH 방식을 이용한 제안 기법이 기존 DH 방식을 이용한

〔표 4〕 SIP 인증 및 키 교환 기술 비교

	암호 방식	제3자 유무	보안 취약성		SRTP를 위한 키 교환	기타
Proposed scheme	변형된 DH	필요 없음	-		지원안함	효율적인 에너지 소모
Yang *et al.* [3]	DH					-
Durlanik *et al.* [4]	ECC	필요 없음	-		지원안함	효율적인 메모리 사용
Wu *et al.* [5]	ECC, secret k	필요함 (AuC)	-			3GPP 환경에서 SIP 보안 기술
Geneiatakis *et al.* [6]	Hash 함수, IDS	필요 없음	사전 공격에 취약함		지원안함	홉 간 키 교환 제공이 안 됨
Ring *et al.* [9]	IBC	필요함 (KGC)	Key escrow 문제가 있음	ID revocation 문제가 있음	지원함	-
Yeun *et al.* [10]						Secure retargeting과 forking 지원 안 됨
Wang *et al.* [11]					지원안함	-

기법에[3] 비해 사용자 단말에서 $g^{H(pw\cdot d)} \bmod p$와 $g^r \bmod p$, r과 같은 파라미터들을 저장하기 위해 추가적인 메모리 공간이 요구되지만, 사용자 개인 SIP 단말일 경우 큰 부담이 되지 않는다. 또한, 제안 기법은 한 사용자가 동일한 SIP 단말에서 2번 이상의 SIP 세션 설정을 할 경우 암호학적 연산량 감소를 통해 기존 SIP 보안 기법들보다 SIP 이동 단말의 에너지 소모를 최소화할 수 있는 장점이 있다. 기존의 기법들이 SIP 기반의 VoIP 환경에서 보안 기술들을 제안하였지만, Wu의 기법은 3GPP 네트워크에서 UICC와 AuC 사이에 공유하고 있는 비밀키 k를 기반으로 SIP 인증 및 키 교환 기술을 제안하였다. 해쉬 함수와 IDS를 이용한 보안 기술은[6] 여전히 사전 공격에 취약하다. IBC 방식을 이용한 Ring과 Yeun의 기법들은 KGC와 같이 신뢰할 수 있는 제 3의 노드를 통한 개인키 분배 방식 때문에 key escrow 문제에 취약하다. 즉, 제 3의 노드가 사용자의 개인키를 악용할 경우, 두 사용자의 비밀 통화 내용을 엿들을 수 있는 문제점이 있다. IBC 방식 중 Wang의 기법만이 key escrow 문제를 해결하였지만, IBC 방식의 3가지 기법들은 IBC 개인키와 ID revocation 문제점이 여전히 남아있다. IBC 기법들 중 SRTP 키 교환 기능을 제공하는 기술들도[9-10] 있지만, 일방향 키 교환 기법을 이용한 SIP 보안 기술은[10] IETF SRTP 키 교환 요구사항 문서에서[12] 요구하는 secure retargeting과 forking 기능을 지원하지 못한다.

V. 결 론

본 논문에서는 암호학적 연산량 위임 기법을 이용하여 효율적이고 안전한 SIP 사용자 인증 및 키 교환 기술을 제안하였다. 제안 기술은 높은 보안성을 제공하면서 계산량이 많이 요구되는 암호 알고리즘 연산을 SIP 서버에게 위임하였기 때문에 안전하고 이동 단말의 에너지 소비 측면에서 효율적이다. 또한 제안 기술은 SIP 표준 절차에 따라 DH 파라미터만을 추가하여 간단하게 구현할 수 있기 때문에 이미 널리 사용되고 있는 SIP 환경에 쉽게 적용할 수 있다.

참 고 문 헌

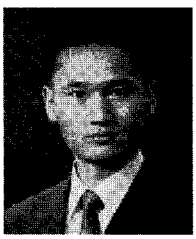
[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, June 2002.

[2] W. Diffie and M. Hellman, "New directions in cryptology," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

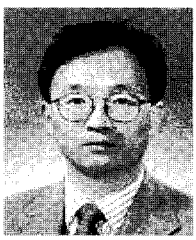
[3] C. Yang, R. Wang, and W. Liu, "Secure authentication scheme for session initiation protocol," Computers & Security, vol. 24, no. 5, pp. 381-386, Aug. 2005.

[4] A. Durlanik and I. Sogukpinar, "SIP authentication scheme using ECDH," Proceedings of World Academy of Science, Engineering and Technology, pp. 350-353, Oct. 2005.
[5] L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," Computer Standards &. Interfaces, vol. 31, no. 2, pp. 286-291, Feb. 2009.
[6] D. Geneiatakis, G. Kambourakis, C. Lambrinoudakis, T. Dagiuklas, and S. Gritzalis, "A framework for protecting a SIP-based infrastructure against malformed message attacks," Computer Networks, vol. 51, no. 10, pp. 2580-2593, July 2007.
[7] D. Geneiatakis and C. Lambrinoudakis, "A lightweight protection mechanism against signaling attacks in a SIP-based VoIP environment," Telecommunication Systems, vol. 36, no. 4, pp. 153-159, Dec. 2007.
[8] A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology, CRYPTO'84, LNCS 196, pp. 47-53, 1984.
[9] J. Ring, K. Choo, E. Foo, and M. Looi, "A new authentication mechanism and key agreement protocol for SIP using Identity-based cryptography," Proceeding of AusCERT Asia Pacific Information Technology Security Conference, pp. 57-72, May 2006.
[10] C. Yeun, K. Han, and K. Kim, "New novel approaches for securing VoIP applications," Proceeding of the Sixth International Workshop for Applied PKC, Dec. 2007.
[11] F. Wang and Y. Zhang, "A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography," Computer Communications, vol. 31, no. 10, pp. 2142-2149, June 2008.
[12] D. Wing, S. Fries, H. Tschofenig, and F. Audet, "Requirements and analysis of media security management protocols," IETF draft-ietf-sip-media-security-requirements-08, Oct. 2008.
[13] MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ library, http://www.shamus.ie

〈著者紹介〉



최 재 덕 (Jaeduck Choi) 정회원
2002년 2월: 숭실대학교 정보통신전자공학부 학사
2004년 2월: 숭실대학교 정보통신공학과 석사
2004년 1월~12월: (주)애드팍테크놀러지 S/W 연구원
2009년 2월: 숭실대학교 전자공학과 박사
2009년 3월~현재: 숭실대학교 전자공학과 박사후 연구원
〈관심분야〉 이동 네트워크 보안, VoIP 보안, 차량 네트워크 보안



정 수 환 (Souhwan Jung) 종신회원
1985년 2월: 서울대학교 전자공학과 학사
1987년 2월: 서울대학교 전자공학과 석사
1988년~1991년: 한국통신 전임 연구원
1996년 6월: University of Washington 박사
1996년~1997년: Stellar One S/W Engineer
1997년~현재: 숭실대학교 정보통신전자공학부 부교수
2009년 3월~현재: 지식경제부 지식정보보안 PD
〈관심분야〉 이동 네트워크 보안, VoIP 보안, 차량 네트워크 보안, RFID/USN 보안