# 강화된 인증 키 동의 프로토콜

이승연°,김영신,허의남
서울여자대학교, 경희대학교
{seungyeon°,youngshin}@swu.ac.kr

# An Enhancement of Authenticated Key Agreement Protocol

Seung-Yeon L.° Kim Y.J. Huh E.N
°Dept of Computer Science, Seoul Women's University
Dept of Computer Engineering, Kyung Hee University

요 약

안전하지 않은 통신망에서 메시지 교환을 통하여 세션키를 공유하고 서로를 인증할 때 공격자는 사용자 간 통신 중에 획득한 메시지를 그대로 사용하거나, 저장된 비밀 정보를 이용하여 정당한 사용자로 위장하여 불법적인 공격을 수행할 수 있다. 본 논문은 SAKA와 Tseng의 프로토콜을 개선 시켜 만든 Kim의 프로토콜을 기반으로 다중채널을 이용하여 공통 세션키를 생성하는 안정성이 강화된 효율적인 프로토콜을 소개 한다.

## 1. 서 론

공개 네트워크를 통하여 안전한 통신을 원하는 사용자는 자신이 정당한 사용자임을 인증하는 절차와 전송될 정보의 암호화가 필수적으로 요구된다. 인증 키 교환 프로토콜은 통신을 원하는 당사자 각각이 제공하는 정보에 의해 상호 인증 및 세션키를 공유하는 과정으로 이때 생성된 세션키는 개체들 사이의 인증, 기밀성, 데이터 무결성 등과 같은 보안 서비스를 제공한다.

인증 키 교환 프로토콜에서 효율적으로 정보를 보호하기 위해서는 안전한 키의 관리가 필요하다. 키 관리는 생성, 보관, 폐기 같은 키 자체의 관리와 분배 및 복구 등의 후 관리로 나눌 수 있는데 그중 가장 중요한 부분은 안전한 키의 분배를 들 수 있다.

Diffie-Hellman 키 교환 프로토콜은 인증된 두 개체간의 안전하지 않은 채널을 사용하여 세션키를 분배하는 방식으로 메시지를 주고받으려는 두 명의 사용자가 서로간의 비밀키를 공유하기 위한 방법이다[1]. 그러나 이 방법은 송수신하는 당사자를 인증하는 내용이 없어서 두 개체 사이에 공격자가 임의의 메시지를 삽입하거나 정당한 사용자로 위장하는 중간자(man-in-the-middle) 공격에 취약하다는 문제가 단점으로 지적되고 있다[1].

이러한 문제점을 해결하기 위하여 여러 가지 키 교환 프로토콜들이 제안되었는데 인증서를 사용하는 방식과 패스워드를 기반으로 하는 방식 등이 그것이다.

인증서를 사용하는 방식은 전송된 메시지의 무결성을 검증하기 위해 신뢰할 수 있는 제 3의 인증기관으로부터 인증서를 발급받아 사용하는 방식이며 패스워드 기반으로 하는 방식은 사용자들이 선택한 패스워드를 사용하여 통신하려는 상대방의 신분을 확인하는 방식이다.

최근 패스워드 기반의 인증 키 교환 프로토콜 방식 중에 하나로 Seo와 Sweeny는 SAKA(Simple Authenticated Key Agreement) 프로토콜을 제안하였다. SAKA 프로토콜은 두 개체가 통신을 시작하기 이전에 공통의 비밀 패스워드를 공유하고 있다는 것을 가정한다. 이러한 특징으로 인해 사용자의 패스워드와 같은 비밀 정보가 노출되거나, 공격자가 과거의 전송정보를 이용하여 패스워드 또는 세션키를 구하려는 공격을 할 경우 안전성에 취약점을 보인다. SAKA 프로토콜에 취약점이 발견된 이후 이를 개선하기 위한 프로토콜들이 제안되어지고 있는데

본 논문에서는 SAKA 프로토콜을 개선한 기존 연구 방식들에 키 설정 및 키 확인 과정을 살펴보고 이를 보완한 보다 안전성이 강화된 세션키를 교환하는 프로토콜을 제시한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 SAKA 프로토콜을 설명하며 3장에서는 새로이 제안하는 프로토콜을 기술하며 마지막 4장에서는 결론을 내린다.

## 2. 기존 연구

### 2.1 Seo-Sweeny의 SAKA 프로토콜

Seo-Sweeny는 Diffie-Hellman 방식을 기반으로 패스워드를 사용하여 두 개체들 사이의 인증과 비밀 세션키를 공유하기 위한 SAKA 프로토콜을 제안하였다[2]. SAKA 프로토콜은 사전에 공유된 패스워드 기술을 기반으로 하고 있다. 따라서 프로토콜이 사직되기 전에 사용자는 비밀 패스워드를 공유하고 있고, Diffie-Hellman 방식처럼 공통값 $n$과 $g$를 가지고 있다는 것을 가정한다.

SAKA 프로토콜과 본 논문에서 제시하는 시스템 파라미터는 다음과 같다

"본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2005-(C1090-0502-0009))

[시스템파라미터]

- $Alice, Bob$: 통신 참여자
- $Eve$: 공격자
- $s$: 공통의 비밀 패스워드
- $p$: 큰 소수
- $g$: $Zp$상의 원소 $(ord(g) = p-1)$
- $a$: Alice가 선택한 랜덤 수, $a \in_R Z^*_n$
- $b$: Bob이 선택한 랜덤 수, $b \in_R Z^*_n$
- $SKa, b$: Alice와 Bob의 세션키

SAKA 프로토콜의 키 설정 과정 확인 과정은 다음과 같다.

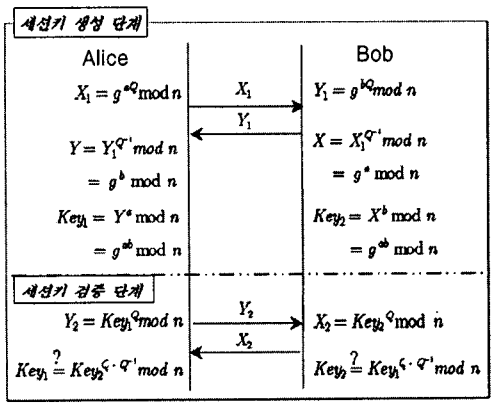


그림 1. SAKA 프로토콜

[세션키 설정과정]

① Alice와 Bob은 각각 패스워드 $P$로부터 두 정수 $Q$와 $Q^{-1} \bmod (n-1)$을 각각 계산한다. 이 때 $Q$의 값은 미리 유도된 값이다.

② Alice는 임의의 정수 $a$를 선택하고 다음 식의 값을 Bob에게 전송한다.

$$X = g^{aQ} \bmod n$$

③ Bob 또한 임의의 정수 $b$를 선택한 후, 다음 식의 값을 Alice에게 전송한다.

$$Y_1 = g^{bQ} \bmod n$$

④ Alice는 세션키인 $Key_1$ 다음을 계산한다.

$$Y = Y_1^{Q^{-1}} \bmod n = g^b \bmod n$$
$$Key_1 = Y^a \bmod n = g^{ab} \bmod n$$

⑤ Bob은 세션키인 $Key_2$를 다음을 계산한다.

$$X = X_1^{Q^{-1}} \bmod n = g^a \bmod n$$
$$Key_2 = X^b \bmod n = g^{ab} \bmod n$$

[세션키 검증 과정 ]

① Alice는 $Key_1^Q \bmod n$을 계산하고, Bob에게 전송한다.

② Bob은 $Key_2^Q \bmod n$을 계산하고 Alice에게 전송한다.

③ Alice와 Bob은 $Q^{-1}$을 이용하여 각각 전송 받은 메시지에서 $Key$를 계산해내고, 자신의 세션키와 계산해 낸 $Key$를 비교한다.

2.2 Tseng 프로토콜

Tseng[3]은 SAKA 프로토콜이 올바른 키 확인 과정을 수행하지 못함을 지적하고 이를 개선하기 위한 SAKA 프로토콜의 키 인증 과정을 보완한 프로토콜을 제안하였다. Tseng의 프로토콜은 중간자 공격과 패스워드 추측 공격에 강인한 개선된 SAKA 프로토콜을 제공한다.

Tseng은 Seo-Sweeny 프로토콜의 약점을 극복하기 위해 세션키 확인 과정을 다음과 같이 개선된 프로토콜을 제안하였다.

[세션키 확인과정]

① Alice는 Bob으로부터 수신한 $Y_1$ 정보를 이용하여 다음식과 같이 계산하여 Bob에게 전송한다.

$$Y = (Y_1)^{Q-1} = g^b mod\, n$$

② Bob은 Alice부터 수신한 $X_1$을 이용하여 다음과 같이 계산하여 Alice에게 전송한다.

$$X = (X)^{Q-1} = g^b mod\, n$$

③ Alice와 Bob이 각각 수신한 값과 자신이 계산한 값을 비교하여 올바른 사용자 인지 검증한다.

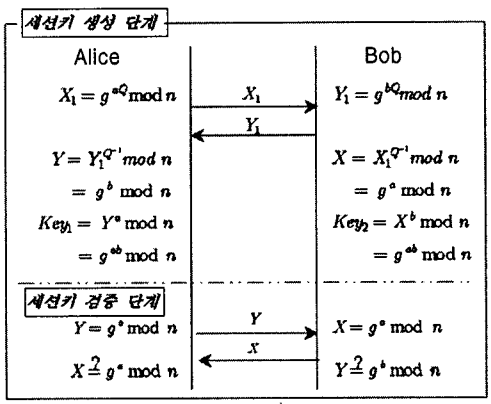


그림2. Tseng 프로토콜

Tseng의 개선된 프로토콜을 사용할 경우 공격자가 세션키 검증 과정에서 Alice를 속이기 위해서는 반드시 Alice로부터 $X_1$값을 수신한 후 $X$를 계산한 다음 Alice에게 전송해야 한다. 그러나 공격자가 $g^q mod\, n$ 과 $Q$값을

정확히 얻는다는 불가능 하므로 공격자는 $X_1$과 $Y_1$만을 가지고 정확한 $X$을 계산할 수 없다[4].

### 3. 제안하는 프로토콜

본 장에서는 SAKA의 키 인증 단계에서의 취약점과 Tseng의 재전송 공격에 대한 단점을 보완하고자 좀 더 강화된 인증키 프로토콜을 기술한다.

안전하지 않은 통신망에서 메시지 교환을 통하여 세션키를 공유하고 서로를 인증할 때 공격자는 사용자간 통신 중에 획득한 메시지를 그대로 사용하거나, 저장된 비밀 정보를 이용하여 정당한 사용자로 위장하여 불법적인 공격을 수행할 수 있다. [5]에서 제안한 간단한 인증키 동의 프로토콜은 위의 관련연구의 단점들을 보완하고 안전하면서도 수행성능이 개선된 프로토콜이다. 하지만 이러한 프로토콜들은 단지 단일 채널에서만 보안사항을 고려하기 때문에 공격자는 임의의 채널만 고려하여 공격을 진행한다. 이를 막기 위해 채널에 변화를 주어 단순한 경로로써 패킷이 오가는 것을 막기 위한 프로토콜을 소개하고자 한다.

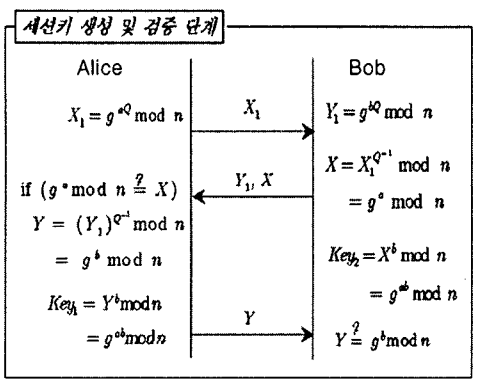


그림3. 강화된 세션키 생성과 검증

그림 3에서는 [5]의 프로토콜 진행과정을 보여준다. 제안하는 프로토콜은 Alice와 Bob이 서로 통신 하고자 할 때 이에 추가하여 사전에 정의된 채널 변경 알고리즘을 사용하는 것이다. 채널 변경 알고리즘은 Alice와 Bob이 서로간의 채널을 정의한 상태에서 프로토콜을 진행하는 것이기 때문에 공격자는 양자간의 통신을 단일 채널이 아닌 모든 채널에 데이터를 모두 분석하여 공격하여야만 한다. 따라서 Alice와 Bob은 사전에 정의된 채널 변경 알고리즘을 이용하여 매번 채널을 변화시켜 공격자의 혼란을 유도한다.

구체적으로 들어가 보면 그림 4와 같이 관련연구의 경우 멀티 채널 로의 다양한 포트 사용은 임의의 포트구간에서 TCP계층에서의 시퀀스 넘버를 기준으로 채널변경 알고리즘을 수행하거나 처음에 보낸 랜덤 넘버를 기준으로 포트 넘버의 변화(1025~65535)를 꾀할 수 있다. 즉, f(a) 와 f(b) 두 병렬 채널을 통해 세션키를 전송하고 검증할 때는 f(a') 와 f(b')를 통해 교환한다.

결론적으로 다른 프로토콜을 모두 개선시킨 [5]의 프로토콜을 기반으로 하여 알고리즘에 의해 채널까지 변경시킨 다면 보다 강화된 보안을 유지할 수 있다. 결국 다중 채널에 의한 프로토콜 진행은 항상 공격자의 혼란을 유도 시킬 수 있으며 단일 채널로 이루어지는 데이터 송수신 보다 효율적인 보안 관계를 수행할 수 있다.

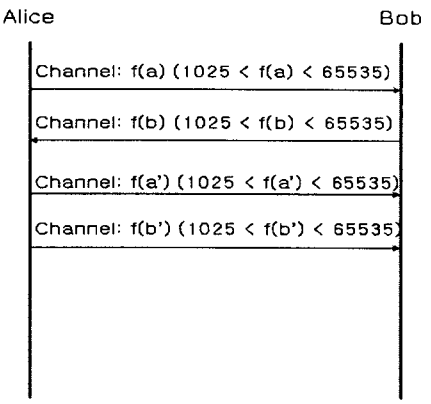


그림 4. 채널 변경 알고리즘을 적용한 플로우

### 4. 결론

본 논문은 두 통신자간에 공통 세션키를 생성하기 위해 보다 효율적인 프로토콜을 소개 하였다. SAKA와 Tseng의 프로토콜을 보다 개선 시켜 만든 Kim의 프로토콜에서 더욱 강화된 보안 세션키를 생성하기 위하여 다중채널을 이용하여 프로토콜을 진행하였다. 이는 단일 채널에 의한 공격을 막을 수 있으며 공격자가 여러 채널을 모두 모니터링 하여야 하는 점에서 고려할 때 효율적이라고 말할 수 있다. 보다 강력하고 안전한 프로토콜이 될 수 있도록 이와 관련된 많은 연구가 이루어지기를 기대한다.

### 참고문헌

[1]W. Diffie, M. Hellman, "New directions in Cryptography", IEEE Trans. on Information Theory, IT-22(6):644-654, November 1976.

[2]Dong Hwi Seo and P. Sweeney, "Simple authenticated key agreement algorithm", Electronics Letters, Vol. 35, No. 13, June, 1999.

[3]Yuh-Min Tseng, "Weakness in simple authenticated key agreement protocol", Electronics Letters, Vol. 36, No. 1, Jan, 2000.

[4]Advanced Modification 공격에 안전한 패스워드 기반 키 동의 프로토콜, 정보처리학회논문지 C 제 11권-C권

[5] 개선된 '간단한 인증키 동의 (Simple Authenticated Key Agreement)' 프로토콜, 한국 인터넷 정보학회 제 4권