패스워드 기반 프로토콜을 이용한 새로운 위성 한정 수신 시스템

김 영 수[†] · 손 기 욱[††] · 양 형 규[†††] · 원 동 호[††††]

요 약

가입자가 스마트카드를 사용하지 않고, 자신의 ID와 패스워드만으로 유료 방송을 시청할 수 있는 새로운 위성 한정 수신 시스템(Conditional Access System)을 제안한다. 본 시스템을 위해 가입자와 가입자관리시스템간의 세션키 분배 및 상호 인증을 행할 뿐 아니라, 암호화키(authorization key)를 다운로딩하는 두 개의 패스워드 기반 프로토콜을 제안한다. 제안하는 시스템은 몇 가지 장점을 갖는다. 우선, 기존의 시스템과 비교하여 가입자관리시스템의 암호화키-암호화 모듈을 제거하였고, 수신측의 암호화된 난수 발생 초기치-복호화 과정도 간략화하여 계산량을 줄였다. 둘째, 비싼 스마트카드 리더기(Card Adaptive Device)가 필요 없으므로 비용 절감의 효과가 있다. 셋째, 디스크램블러와 스마트카드가 일체형이었던 기존의 방식과는 달리 디스크램블러를 포함한 어떠한 TV 셋탑 박스를 통해서도 이용이 가능한 디스크램블러 독립성을 제공한다.

A new satellite CAS using password-based protocol

Young-Soo Kim[†] · Ki-Wook Sohn[††] · Hyung-Kyu Yang[†††] · Dong-Ho Won[††††]

ABSTRACT

We introduce a new satellite Conditional Access System(CAS) that a subscriber could watch a pay-TV knowing only his or her identity and password, without using a smart card. For this new system, two password-based protocols are presented which not only share a session key and authenticate each other but also download an authorization key. This system has some merits: First, compared with current systems, it reduces the amount of computations by eliminating the AK-encryption module in SMS(Subscriber Management System) and simplifying the receiver's CW-decryption process. Second, since this system does not need an expensive Card Adaptive Device(CAD), it can reduce costs. Finally it provides descrambler independence allowing it to be used through any TV set-top box that includes a descrambler, unlike the current system that a descrambler is linked with a smart card.

1. 서 론

급속한 컴퓨터 및 통신 관련 기술의 발달과 방송 기술 분야의 발달로 인해 멀티미디어 사회가 실현됨에 따라 방송매체 역시 다양해지면서 방송 채널 수 또한 점차 증가하고 있다. 이러한 방송 채널 수의 증가와 함께 전문 방송 채널이 탄생하게 되었으며, 보다 양질의 프로그램 방송을 위해 그 운영의 많은 부분을 시청료에 의존하게 되었다. 따라서, 유료 방송 시스템을 유지하기 위해 가입자들이 모두 시청료를 내고, 비가입자들은 정상적인 방송 신호를 수신할 수 없도록 하는 한정 수신 시스템(Conditional Access System, CAS)

† 준 회 원 : 성균관대학교 대학원 전기·전자 및 컴퓨터 공학부
†† 정 회 원 : 한국전자통신연구원 선임연구원
††† 정 회 원 : 강남대 산업전산전자공학부 교수
†††† 종신회원 : 성균관대학교 전기·전자 및 컴퓨터 공학부 교수
논문접수 : 1999년 9월 2일, 심사완료 : 1999년 11월 12일

이 도입되었다.

과거의 한정 수신 시스템은 TV와 연결된 셋탑 박스(set-top box)에 복호화 알고리즘과 비밀키가 저장되어 있는 구조로 도시청의 발생 가능성을 내포하고 있었다. 여기서, 도시청이란 비가입자가 불법적으로 유료 방송을 시청하는 것을 통칭하는 것으로 가장 널리 알려진 방법으로 TV 셋탑 박스 자체를 하드웨어 복제하는 것을 예로 들 수 있다. 이러한 도시청을 막는 방법 중 하나는 각 가입자 TV의 셋탑 박스를 정기적으로 교체하여 복호화 알고리즘이나 비밀키를 갱신하는 것이다. 그러나, 값비싼 셋탑 박스를 주기적으로 바꾸어 주는 것은 비경제적인 해결책으로, 대신 디스크램블러와 분리가능한 스마트카드를 발급하여 모든 복호화 알고리즘과 비밀키를 스마트카드 내에 저장하는 시스템이 일반화되었다[13, 14].

그러나 이러한 스마트카드를 이용하는 한정 수신 시스템의 경우, 가입자는 값비싼 카드 리더기를 구비해야 하고, 스마트카드 내의 복호화 알고리즘이나 비밀키를 주기적으로 갱신해주어야 한다. 또한 대부분 디스크램블러와 스마트카드가 일체화되어 있는 형태이므로, 자신의 TV 셋탑 박스가 설치되어있지 않은 다른 장소에서는 시청을 할 수 없고, 셋탑 박스를 타인에게 양도시 자격 갱신과 관련된 복잡한 절차를 필요로 하는 등 사용상 많은 제한을 받게 된다[13].[1)]

본 논문에서는 스마트카드를 발급받을 필요없이 가입자가 자신의 ID와 패스워드만을 가지고 디스크램블러가 설치된 어떠한 장소에서도 유료 방송 시청이 가능한 새로운 위성 한정 수신 시스템을 제안한다. 본 시스템을 위해 가입자와 가입자관리시스템간의 인증 및 세션키 분배를 행하고 난수 발생 초기치 암호화에 사용하는 암호화키(authorization key)를 다운로딩하는 두 개의 패스워드 기반 프로토콜을 제안한다. 본 시스템은 비교적 고가인 스마트카드 리더기를 TV 셋탑 박스내에 내장할 필요가 없어 비용 절감의 효과가 있고, 또한 디스크램블러와 스마트카드가 일체형이었던 기존의 방식과는 달리 디스크램블러와 가입자간의 독립성이 유지되므로 자신의 것이 아닌 다른 TV 셋탑 박스로도 원하는 방송을 시청할 수 있어 다양한 유료 방송 서비스 형태에 모두 적용 가능할 것으로 기대된다.

1) 김경신 등은 이에 대한 해결책으로 디스크램블러와 스마트카드 간의 상호 인증 주체를 스마트카드가 아닌 디스크램블러로 변경함으로써 디스크램블러의 독립성을 확보하기도 하였다[12, 13].

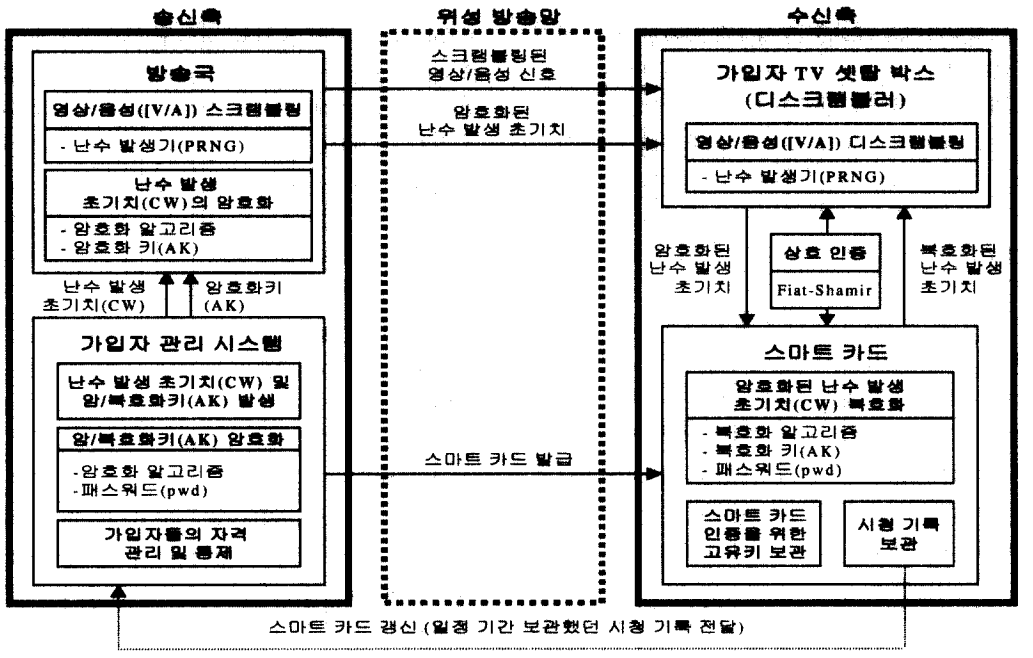
본 논문의 구성은 다음과 같다. 2장에서는 기존의 스마트카드를 이용하는 위성 한정 수신 시스템에 대하여 살펴본다. 3장에서는 최근까지 제안된 패스워드 기반 프로토콜들에 대하여 살펴보고, 제안하는 시스템의 전체적 구성 및 필요한 모듈, 그리고 본 시스템에 적합한 두 개의 패스워드 기반 프로토콜을 소개한다. 마지막으로 4장은 결론부이다.

2. 스마트카드를 이용하는 기존의 위성 한정 수신 시스템

기존의 위성 한정 수신 시스템은 (그림 1)과 같이 송신측, 위성 방송망, 수신측 등 크게 세 부분으로 구성되며, 송신측은 방송국과 가입자관리시스템으로 구성된다. CAS 동작을 위해 사용되는 표기는 다음과 같다.

- CW : 난수 발생 초기치 (Control Word)
- AK : CW에 대한 암호화키
- pwd : 가입자의 패스워드
- PRNG(CW) : CW를 초기치로 하여 발생한 난수 (Pseudo-Random Number)
- SCR(x) : x를 스크램블링한 값
- $SCR^{-1}(y)$: y를 디스크램블링한 값
- $E_{AK}(CW)$: AK를 키로 하여 CW를 암호화한 값
- $D_{AK}(F)$: AK를 키로 하여 F를 복호화한 값
- [V/A] : 영상/음성 신호
- h : 해쉬 함수

방송국에서는 전송될 영상/음성 신호([V/A])를 제작하고, 제작된 신호를 난수 발생기(Pseudo-Random Number Generator, PRNG)에서 발생된 난수(I)로 스크램블링한다. 이때 사용된 난수 발생기의 초기치(CW)는 가입자관리시스템의 컴퓨터에서 제공되며, 역시 컴퓨터에서 발생된 키(AK)로 암호화되어 스크램블링된 [V/A]와 함께 방송국으로부터 방송위성을 통해 각 가입자의 TV 셋탑 박스에 전달된다. 디스크램블링에 필요한 CW의 복호화는 그것을 암호화할 때 사용된 키를 얻으면 가능하다. 가입자관리시스템의 컴퓨터에서 발생된 이 키는 다시 각 가입자의 패스워드(pwd)로 암호화되어, 스마트카드에 저장되어 계약 갱신 주기마다 가입자들에게 전달된다. 이때 CW를 암호화했던 키(AK)도 계약 갱신 주기마다 바뀔 수 있다. 가입자의 TV



(그림 1) 스마트 카드를 이용하는 기존의 위성 CAS

셋탑 박스에서는 수신된 신호 중 암호화된 CW를 디스크램블러에 보내고 디스크램블러의 스마트 카드는 저장된 가입자의 패스워드로 AK를 복호화하고, 복호화된 키로 다시 CW를 복호화하여 이 값을 디스크램블러로 보내 [V/A]를 디스크램블링하는데 사용한다. 지금까지의 동작 과정을 나타내면 (그림 2)와 같다. 이때

방송국 (가입자관리시스템)		가입자 TV 셋탑 박스 (디스크램블러)
		(가입 신청)
가입자의 패스워드 pwd 생성 AK 생성, $G=E_{pwd}(AK)$	G, pwd (스마트카드에 저장) →	
① CW 생성 [V/A] 제작 I=PRNG(CW) $J=SCR_I([V/A])$ $F=E_{AK}(CW)$	② J, F →	(디스크램블러에 스마트카드 삽입) ③ $AK=D_{pwd}(G)$ $CW=D_{AK}(F)$ I=PRNG(CW) $[V/A]=SCR^{-1}_I(J)$

(그림 2) 스마트카드를 이용하는 위성 CAS의 동작 과정

스마트카드와 디스크램블러는 Fiat-Shamir의 영지식인증[4]을 이용하여 서로 합법적인 상대임을 확인한다.

3. 제안하는 새로운 위성 한정 수신 시스템

본 장에서는 스마트카드 대신 안전한 패스워드 기반 프로토콜을 이용하는 새로운 위성 한정 수신 시스템을 제안한다. 우선 최근까지 제안된 패스워드 기반 프로토콜들을 살펴본 후, 새로운 시스템의 구성과 필요한 모듈들을 설명하고, 끝으로 두 개의 패스워드 기반 프로토콜을 제안한다.

3.1 패스워드 기반 프로토콜

1992년에, Bellovin과 Merritt은 Encrypted Key Exchange (EKE)라는 새로운 프로토콜을 제안하였다[1]. 대칭키 암호방식과 공개키 암호 방식을 함께 사용하는 EKE는 수동적 공격자가 자신이 추측한 패스워드의 검증을 위한 정보를 충분히 얻지 못하도록 함으로써 사전 공격(dictionary attack)을 막는다. ElGamal 공개키 암호 방식을 사용하는 일반적인 EKE 형태에서, 두 통신 당사자들은 분배된 패스워드를 대칭키 암호 방식의 키로

하여 키재료(key material)를 암호화한다. EKE 이후, 안전성을 강화하거나 새로운 특성들을 추가한 많은 변형들이 제안되었다. 예를 들어, DH-EKE[10]와 SPEKE[5]는 공격자가 패스워드를 알아내어도 이전 세션의 세션키들을 얻는 것에는 도움이 되지 않는다는 전향적 안전성(forward secrecy)을 추가하였다. 이 성질은 일반적으로 세션키를 얻는 것이 패스워드에 대한 전사적(brute-force) 추측 공격에 전혀 도움을 주지 않는다는 의미이기도 하다.

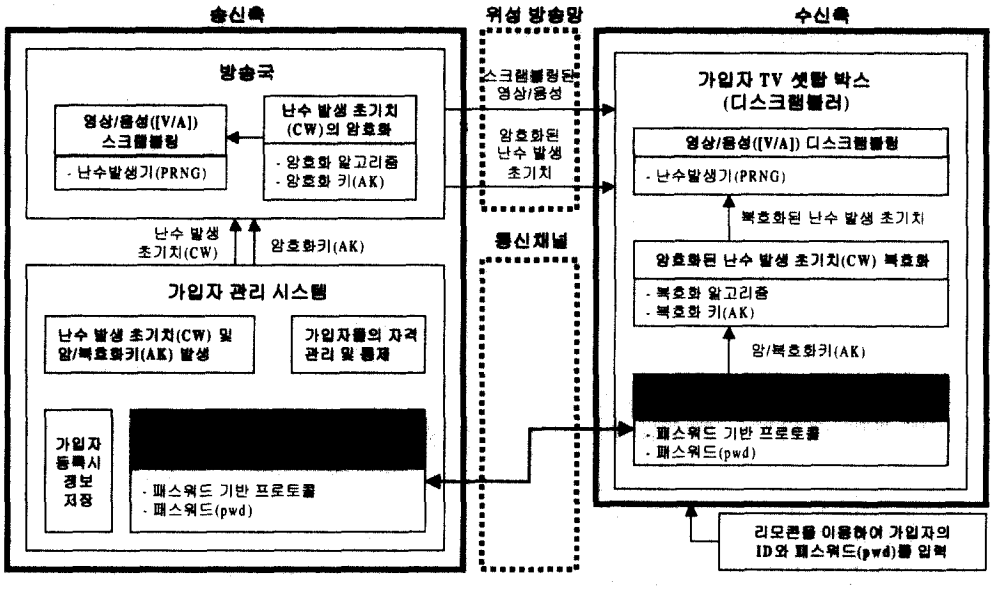
한편, EKE의 가장 큰 단점은 평문-상응(plaintext-equivalent) 메카니즘[11]을 사용한다는 것으로 클라이언트나 서버가 동일한 비밀 패스워드나 해쉬값에 접근한다. 이에 대한 해결책으로 디지털 서명을 사용하는 검증자(verifier) 기반 프로토콜인 Augmented EKE(A-EKE)가 제안[2]되었으나 이러한 변형은 완전 전향적 안전성(perfect forward secrecy)을 보장하지 못하는 결과를 초래하였다[10].

1997년에, Jablon은 패스워드 파일내에 검증자를 저장하도록 하는 방법으로 EKE를 확장하였다[6]. 이러한 B-SPEKE는 클라이언트가 실제 패스워드를 알고 있는지 여부를 검증하기 위해 추가적인 키 교환 라운드가 필요하므로 수행 시간과 계산 복잡도가 상대적으로 높다. 권태경[7] 등은 이러한 통신량과 계산량을 줄이기 위해, 키분배를 위한 암호화 방법으로는, 일회용 패드를 사용하고 키의 무결성 검사를 위해서는 강한 해쉬함수를 사용하는 방법을 제안하기도 하였다. SRP[11] 역시 검증자 기반 프로토콜로서, 검증자를 획득한 공격자라 하더라도 그것을 호스트 접속에 직접 이용할 수 없다. SRP는 영지식 증명 방식과 비대칭 키 교환 프로토콜을 함께 사용하며 A-EKE나 B-SPEKE 같은 검증자 기반 프로토콜들에 비하여 효율이 매우 뛰어나다.

최근에 권태경[8] 등은 SRP와 유사하지만 지수의 형태가 Diffie-Hellman 지수[3]인 g^{xy} (여기서 g는 갈로아체(p)상의 원시원소, p는 소수, x와 y는 랜덤수)와 동일한 스킴을 제안하였는데, 이는 A-EKE나 B-SPEKE에 비하여 상대적으로 적은 라운드 수와 실행 시간을 갖는다. 한편, 안전한 패스워드 기반 프로토콜을 이용하여 가입자의 비밀 정보(security context)를 다운로딩할 수 있는 새로운 스킴이 Perlman과 Kaufman[9]에 의해 제안되었는데, 이 스킴에서는 EKE나 SPEKE의 핸드셰이킹(handshaking) 부분을 생략하고 분배된 세션키로 비밀키나 인증서 등 가입자 관련 정보들을 암호화하여 전송한다.

3.2 제안하는 새로운 위성 한정 수신 시스템

제안하는 새로운 위성 한정 수신 시스템은 안전한



(그림 3) 제안하는 시스템의 전체적 구성

패스워드 기반 프로토콜을 이용하여 가입자와 가입자 관리시스템간의 인증 및 세션키 분배, 그리고 정상적인 방송 시청을 위해 가장 중요한 암/복호화키(AK)를 다운로딩한다. 기존의 시스템과 비교하여 가입자관리 시스템의 암/복호화키 암호화 모듈을 제거하였고, 수신측의 암호화된 난수 발생 초기치 복호화 과정도 간략화하여 계산량을 줄였다. 송신측, 위성 방송망, 수신측 등 크게 세 부분으로 구성되며, 송신측은 방송국과 가입자관리시스템으로 구성된다. (그림 3)은 그 구성과 필요한 모듈들을 나타낸다.

비교적 고가인 스마트카드 리더기를 가입자 TV 셋탑 박스내에 내장할 필요가 없어 비용절감의 효과가 있고, 또한 디스크램블러와 스마트카드가 일체형이었던 기존의 방식과는 달리 디스크램블러의 독립성이 유지되므로 장소에 구애받지 않고 원하는 방송을 시청할 수 있는 장점이 있다. (그림 4)는 본 시스템의 동작과정이다.

방송국 (가입자관리시스템)		가입자 TV 셋탑 박스 (디스크램블러)
	ID, pwd (가입신청시 가입자에게 전달) →	(가입 신청)
① CW, AK 생성 ② [V/A] 제작 I=PRNG(CW) J=SCR$_I$([V/A]) ③ F=E_{AK}(CW)	④ J, F (자격통제메시지에 저장) →	
	⑥ AK (by 패스워드 기반 프로토콜) →	(프로그램 시청시) ⑤ ID, pwd 입력 (by 리모콘) ⑦ CW=D_{AK}(F) ⑧ I=PRNG(CW) [V/A] = SCR$^{-1}{}_I$(J)

(그림 4) 제안하는 시스템의 동작 과정

① 가입자가 가입 신청을 하면, 가입자관리시스템은 가입자에게 ID와 패스워드 pwd를 발급한다. 가입자관리시스템은 난수 발생 초기치 CW와 이에 대한 암호화키 AK를 생성하여 방송국에 전송한다.

② 방송국은 전송 받은 CW를 사용하여 난수 I를 발생시킨다. 또한, 방송국은 전송될 영상/음성 신호 [V/A]를 제작하고 제작된 신호를 I로 스크램블링한 값 J를 생성한다.

$$I = PRNG(CW)$$
$$J=SCR_I([V/A])$$

③ 방송국은 가입자관리시스템으로부터 받은 AK로 CW를 암호화한 값 F를 계산한다.

$$F=E_{AK}(CW)$$

④ 방송국은 위성 방송망을 통하여 J와 F(여기서 F는 자격통제메시지(Entitlement Control Message, ECM)내에 담겨 있음)를 브로드캐스팅하고 각 수신측의 가입자 TV 셋탑 박스는 이것을 수신한다.

⑤ 가입자가 프로그램을 시청하고자 할 경우, 가입자는 리모콘을 이용하여 자신의 ID와 pwd를 가입자 TV 셋탑 박스에 입력한다.

⑥ 가입자 TV 셋탑 박스는 일반 통신 채널을 통하여 가입자관리시스템과의 패스워드 기반 프로토콜을 수행(3.2.1과 3.2.2 참조)하고 AK를 다운로딩한다 (여기서, AK는 주기적으로 갱신됨)

⑦ 가입자 TV 셋탑 박스는 위성으로부터 수신한 F를 ⑥에서 다운받은 AK로 복호화하여 CW를 계산하고 이것을 디스크램블러에 보낸다.

$$CW=D_{AK}(F)$$

⑧ 디스크램블러는 CW를 사용하여 난수 I를 얻고, I를 이용하여 위성 수신한 J를 디스크램블링하여 가입자가 시청하고자 하는 [V/A]를 얻는다.

$$I=PRNG(CW)$$
$$[V/A] = SCR^{-1}{}_I(J)$$

다음의 두 절에서는 (그림 4)에서의 세션키 분배 및 가입자 인증, 그리고 AK 다운로드 과정(⑥)을 위해 두 개의 패스워드 기반 프로토콜을 각각 제안한다. 제안하는 프로토콜 I은 방송국이 생성한 랜덤수들($R_{방송국}$, salt)을 이용하여 안전성을 높인 6-메시지 프로토콜이며, 제안하는 프로토콜 II는 실용성을 높이기 위해 통신량과 계산량을 줄인 2-메시지 프로토콜이다.

3.2.1 제안하는 위성 한정 수신 시스템에 적합한 프로토콜 I

제안하는 프로토콜 I은 SPEKE[5]에 기반한 6-메시

지 프로토콜로서 랜덤수들을 이용하여 안전성을 향상시켰다. 방송국이 생성하여 수신측과 주고받는 랜덤수 $R_{방송국}$을 통하여 서비스 거부 공격(denial-of-service attack)을 막는 한편, 랜덤수 salt를 패스워드 함수 W(=h(pwd,salt), 여기서 h는 해쉬함수)에 포함시킴으로써 사전 공격이 어렵도록 설계하였다. 통신량과 계산량이 많은 것은 이러한 랜덤수들을 생성하고 전송하기 위한 계산 과정과 메시지들이 추가되었기 때문이다.

(1) 동작 과정

(그림 5)에서와 같이 가입자가 가입 신청을 하면, 방송국의 가입자관리시스템은 가입자에게 ID와 pwd를 발급하고 이를 저장한다.

① 가입자가 프로그램 시청을 원할 경우 리모콘을 사용하여 자신의 ID와 pwd를 입력하게 되고, 이를 입력받은 가입자 TV 셋탑 박스는 가입자의 ID를 방송국에 전송한다.

② 가입자관리시스템은 ID를 확인하고 랜덤수들인 salt와 $R_{방송국}$을 생성하여 이를 수신측에 전송한다.

③ 수신측의 가입자 TV 셋탑 박스는 전송받은 salt를 포함한 패스워드 함수 W(=h(pwd, salt))를 계산하고 랜덤수 A($1 \le A \le p-2$, p는 1024비트 이상의 큰 소수[2])를 선택하여 $W^A \bmod p$를 $R_{방송국}$과 함께 방송국에 전송한다.

방송국 (가입자관리시스템)		가입자 TV 셋탑 박스 (디스크랩블러)
가입자의 (ID, pwd) 저장	① ID ←	
랜덤수인 salt, $R_{방송국}$ 생성		
($W=h(pwd,salt)$ 계산)	② salt, $R_{방송국}$ →	$W=h(pwd,salt)$ 계산
		랜덤수 A 선택 ($1 \le A \le p-2$)
랜덤수 B 선택 ($1 \le B \le p-2$)	③ $R_{방송국}$, $W^A \bmod p$ ←	
$W^B \bmod p$ 계산	④ $W^B \bmod p$ →	세션키 $SK=W^{AB} \bmod p$ 계산
세션키 $SK=W^{AB} \bmod p$ 계산	⑤ h(SK) ←	h(SK) 계산
$Y=E_W(AK)$, $E_{SK}(Y)$ 계산	⑥ $E_{SK}(Y)$ →	⑦ SK, W를 통하여 AK를 얻음

(그림 5) 제안하는 위성 한정 수신 시스템에 적합한 프로토콜 I

2) p는 전사 공격에 대하여 안전해야 하므로, 현재의 계산능력을 고려하였을 경우, 적어도 1024비트 또는 2048비트 이상 되어야 한다.

④ 방송국은 랜덤수 $B(1 \le B \le p-2)$를 선택하여 $W^B \bmod p$를 가입자측에 전송하고 ③에서 받은 $W^A \bmod p$와 계산한 $W^B \bmod p$를 이용하여 세션키 $SK=W^{AB} \bmod p$를 계산한다.

⑤ 수신측은 세션키 $SK=W^{AB} \bmod p$를 계산하고, 계산된 세션키의 확인을 위해 해쉬값 h(SK)를 구하여 방송국에 보낸다.

⑥ 방송국은 ④에서 계산한 SK에 해쉬값을 구하여 ⑤에서 전송받은 값과 일치하는지를 확인하고, W와 SK를 이용하여 $E_{SK}(Y)$를 계산하여 수신측에 전송한다.

⑦ 가입자 TV 셋탑 박스는 ⑥에서 전송받은 $E_{SK}(Y)$를 복호하여 AK를 얻는다.

(2) 프로토콜의 안전성

본 프로토콜의 안전성은 SPEKE[5]에 기반한다. 그러므로 여기에서는 SPEKE와 다른 부분, 즉 두 종류의 추가된 랜덤수가 각각 사전 공격과 서비스 거부 공격에 대한 안전성을 제공함을 보이고, SPEKE의 가입자가 방송국을 확인하는 과정을 생략하고 분배된 세션키 SK로 AK를 전송하는 과정을 추가함으로써 안전성에 미치는 영향에 대하여 살펴본다.

- 사전 공격을 막기 위한 랜덤수 salt 사용

공격자가 방송국의 데이터베이스를 읽을 수 있다고 가정할 경우, 공격자는 자신이 추측한 여러 개의 패스워드 후보자들(pwd')에 대한 해쉬값 W'(=h(pwd'))들을 구하여, 이 값들 중 데이터베이스로부터 획득한 패스워드 해쉬값 W(=h(pwd))들과 일치하는 값들만으로 사전을 만들 수 있다. 즉, 추측한 패스워드에 대한 검증을 위해 자신만의 사전을 이용하는 사전 공격(dictionary attack)을 행할 수 있으므로, 이를 어렵게 만들기 위해 W를 고정시키지 않고 프로토콜 수행 중에 전송되는 랜덤수 salt를 포함한 값을 W (=h(pwd,salt))로 사용한다.

- 서비스 거부 공격을 막기 위한 $R_{방송국}$의 사용

방송국의 가입자관리시스템은 횟수의 제한 없이 시청 요청을 받을 수 있는 서버이므로 공격자가 위조한 여러 개의 가입자 위치 정보를 이용하여 방대한 양의 시청 요구를 함으로써 시스템을 마비시키는 일종의 서비스 거부 공격이 가능하다. 즉, (그림 5)에서 $R_{방송국}$의 주고받음이 없다고 가정할 경우, 가입자 TV 셋탑 박

스의 디스크램블러로부터 시청 요청을 받은 가입자관리시스템은 이에 대한 지수 연산(세션키 SK와 W^B mod p 계산)을 수행해야하므로, 짧은 시간 내에 시청 요청이 극도로 많을 경우, 과다한 부하로 인하여 다른 서비스를 제공할 수 없게 되거나 시스템 자체가 마비되는 경우가 발생할 수 있다. $R_{방송국}$은 시청 요청을 한 가입자의 위치 정보 등을 담고 있는 일종의 쿠키(cookie)로서, 추적을 피할 목적으로 위조한 가입자 위치 정보들을 이용하여 방대한 양의 시청 요청을 보내는 이러한 공격을 막을 수 있다.

- 방송국 확인 과정 생략 및 암호화키(AK) 전송 과정 추가가 안전성에 미치는 영향

위의 프로토콜은 EKE[1]나 SPEKE[5]에서 볼 수 있는, 가입자가 방송국을 확인하는 과정을 생략하는 대신 분배된 세션키 SK로 암호화키 AK를 전송하는 과정을 추가하였다. 방송국에 대한 확인 과정이 없으므로 공격자가 가입자의 pwd를 획득할 경우, 방송국을 가장하여 가입자에게 잘못된 AK를 전송할 수 있으나, 가입자의 pwd가 방송국을 확인할 수 있는 유일한 수단이므로 이러한 공격은 불가피한 것이 사실이다. 그러므로 방송국 확인 과정 생략으로 인한 안전성의 저하는 없다고 볼 수 있다.

3.2.2 제안하는 위성 한정 수신 시스템에 적합한 프로토콜 II

제안하는 프로토콜 II는 실용성을 높이기 위해 통신량과 계산량을 줄인 2-메시지 프로토콜이다. 제안하는 프로토콜 I과는 달리 가입 신청시 방송국은 가입자의 ID와 W^B mod p, 그리고 B(B는 랜덤수, $(1 \le B \le p-2)$)를 저장한다. 여기서 W를 직접 저장하지 않는 이유는 공격자가 방송국의 데이터베이스로부터 패스워드를 직접 획득하지 못하도록, 즉 단일 패스워드 추측 공격[1]을 막기 위해서이다. 그리고 방송국은 B를 프로토콜 수행시마다 생성하여 사용하는 것이 아니라 가입 신청시 생성하여 저장함으로써 가입자마다 각기 다른 B를 정해주어 반복하여 사용할 수 있게 함으로써 계산량을 줄였다.

(1) 동작 과정

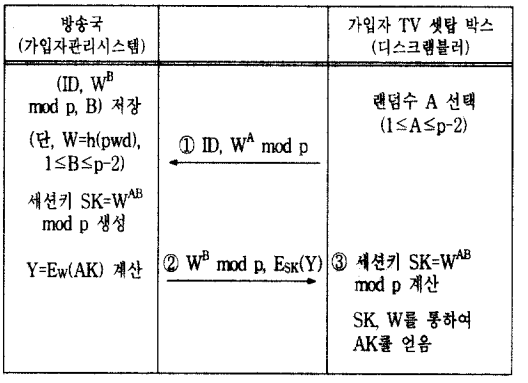
가입자가 가입 신청을 하면, 방송국의 가입자관리시스템은 ID와 pwd를 발급하고 ID와 W^B mod p, 그리고 B를 저장한다(단, W=h(pwd), 여기서 B는 방송국이 정한 가입자 고유의 랜덤수$(1 \le B \le p-2)$).

① 가입자의 ID와 pwd를 리모콘으로 입력받은 가입자 TV 셋탑 박스는 랜덤수 A를 선택$(1 \le A \le p-2)$하고 pwd를 해쉬한 값 W에 A승하여 ID와 함께 방송국에 전송한다.

② 방송국의 가입자관리시스템은 가입자 ID를 확인한 후, 가입자 등록 과정에서 저장해 둔 B$(1 \le B \le p-2)$와 수신측으로부터 전송받은 정보로부터 세션키 $SK=W^{AB}$ mod p를 계산한다. 방송국은 AK를 암호화한 값 Y를 계산한 후 이를 다시 SK로 암호화한 값 $E_{SK}(Y)$를 계산하여, 역시 미리 저장해 두었던 W^B mod p와 함께 수신측에 전송한다.

③ 수신측의 가입자 TV 셋탑 박스는 방송국으로부터 전송받은 W^B mod p에 A승하여 SK를 얻고 이를 이용하여 다시 Y를 복호하여 AK를 얻는다.

(그림 6)은 이러한 동작 과정을 나타낸다.



(그림 6) 제안하는 위성 한정 수신 시스템에 적합한 프로토콜 II

(2) 프로토콜의 안전성

역시 SPEKE[5]에 기반한 위의 프로토콜은 제안하는 프로토콜 I을 최적화한 형태인 2-메시지 프로토콜로서 랜덤수 salt와 $R_{방송국}$, 그리고 수신측(가입자)과 방송국 사이의 상호 인증 과정을 제거하였다(여기서 가입시 방송국이 가입자마다의 고유 B를 저장하게 되고, 이에 따라 W^B mod p 역시 가입자마다 다른 값이 되므로 salt와 같은 랜덤수를 사용할 필요가 없다). 이로 인하

여 발생할 가능성이 있는 안전성 문제에 대하여 다음과 같이 세 가지로 나누어 생각해 보기로 한다:

● 방송국을 가장한 위장(impersonation) 공격

첫 번째 메시지를 가로챈 공격자는 방송국을 위장하여 두 번째 메시지를 획득할 수 있다. 그러나 첫 번째와 두 번째 메시지로부터 얻은 정보인 $W^A \bmod p$, $W^B \bmod p$, $E_{SK}(Y)$를 이용하여 세션키 $SK=W^{AB} \bmod p$값을 얻기 위해서는 A값을 추측해야 한다. 랜덤수 A값을 추측하기 위해서는 $2^{|A|}$의 계산량이 필요한데, A가 갖는 값의 범위는 $1 \le A \le p-2$이므로 A값을 구하는 것은 계산상 불가능하다. (단, 여기서 |x|는 x의 길이를 말하며, 3.2.1절에서 언급하였듯이 p의 크기는 1024비트 이상이다)

● 가입자를 가장한 온라인 패스워드 추측 공격

가입자임을 가장하려는 공격자는 방송국으로부터 발각됨이 없이 자신의 패스워드 추측을 검증할 기회를 가질 수 있다. 공격자가 잘못된 패스워드 추측을 했을 경우, SK 또는 Y에 대한 정보를 얻을 수는 없으나, 자신의 추측이 잘못되었다는 사실만큼은 알 수가 있다. 이때 방송국은 AK를 다운 받으려는 가입자의 요청이 정당한 것인지 아닌지 구별할 수가 없다. 그러나 여기서 중요한 것은 이러한 공격이 단일 온라인 패스워드 추측 공격이라는 점이다. 만일 공격자가 수천 번의 패스워드 추측을 시도한다면 방송국은 이를 의심하게 될 것이다.

● 방송국 데이터베이스 해킹을 통한 공격

공격자가 방송국의 데이터베이스 해킹을 통하여 $W^B \bmod p$값을 얻는다고 하여도 이것으로부터 직접 패스워드(pwd) 또는 패스워드의 해쉬값(W)을 얻기는 어렵다. 이러한 값들을 얻기 위해서는 랜덤수 A값을 추측해야하므로, 역시 $2^{|A|}$의 계산량이 요구된다.

〈표 1〉 제안한 프로토콜 비교

	메시지 수	랜덤값 생성횟수		특 징
제안하는 프로토콜 I	6	방송국	3	안전성 향상을 위해 랜덤수 사용
		가입자	1	
제안하는 프로토콜 II	2	방송국	1*	통신량/계산량을 줄여 실용성을 높임
		가입자	1	

*가입자가 바뀔 때에만 랜덤값 생성

<표 1>은 위의 두 프로토콜을 비교 정리한 것이다. 제안하는 프로토콜 II에서 방송국은 프로토콜 수행시마다 랜덤값을 생성하는 것이 아니라, 가입자가 바뀔 때마다 각각의 고유한 랜덤값을 생성한다.

4. 결 론

본 논문에서는 가입자 편의를 위하여 스마트카드를 없애고 가입자 자신의 ID와 패스워드만을 가지고 TV 셋탑 박스가 설치된 어떠한 장소에서도 유료 방송 시청이 가능한 새로운 한정 수신 시스템을 제안하였다. 우선 기존의 위성 한정 수신 시스템의 단점들과 제안하는 시스템이 갖는 장점들에 대하여 서술하였다. 또한 본 시스템의 중심 프로토콜인 패스워드 기반 프로토콜에 대한 동향을 살펴보았고 새로운 시스템의 구성과 필요한 모듈들을 설명하였으며, 끝으로 제안하는 시스템에 적용 가능하도록 안전성과 통신량/계산량을 각각 고려한 두 개의 패스워드 기반 프로토콜을 제안하고 안전성을 분석하였다. 본 논문에서 제안한 시스템이 갖는 장점을 정리해 보면 다음과 같다. 우선, 기존의 시스템과 비교하여 가입자관리시스템의 암호화키-암호화 모듈을 제거하였고, 수신측의 암호화된 난수 발생 초기치-복호화 과정도 간략화하여 계산량을 줄였다. 둘째, 비싼 스마트카드 리더기를 TV 셋탑 박스내에 내장할 필요가 없어 비용 절감의 효과가 있다. 셋째, 디스크램블러와 스마트카드가 일체형이었던 기존의 방식과는 달리 디스크램블러와 가입자간의 독립성이 유지되므로 장소에 구애받지 않고 원하는 방송을 시청할 수 있어 다양한 유료 방송 서비스 형태에 모두 적용 가능할 것으로 기대된다.

참 고 문 헌

[1] S.M.Bellovin, M.Merritt, "Encrypted Key Exchange : Password-based protocols secure against dictionary attacks," Proc. of the IEEE Computer Society Conference on Research in Security and Privacy, 1992.

[2] S.M.Bellovin, M.Merritt, "Augmented Encrypted Key Exchange : a Password-Based Protocol secure against dictionary attacks and password file compromise," TR, AT&T Bell Lab, 1994.

[3] W.Diffie, M.E.Hellman, "New directions in cryptography," IEEE Transaction on Information Theory, vol.IT-22, No.6, pp.644-654, 1976.

[4] M.Fiat, A.Shamir, "How to prove yourself : practical solution to identification and signature problems," Advances in Cryptology-Crypto '86, Springer-verlag, Lecture Notes in Computer Science, pp.186-194, 1987.

[5] D.P.Jablon, "Strong Password-only authenticated key exchange," ACM Computer Communications Review, 1996.

[6] D.P.Jablon, "Extended password methods immune to dictionary attack," In WETICE '97 Enterprise Security Workshop, 1997.

[7] T.Kwon, J.Song, "Efficient Key Exchange and Authentication Protocols Protecting Weak Secrets," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E81-A, No.1, pp.156-163, 1998.

[8] T.Kwon, J.Song, "Secure Agreement Scheme for g^xy via Password Authentication," Electronics Letters, vol.35, no.11, pp.892-893, 1999.

[9] R.Perlman, C.Kaufman, "Secure Password-Based Protocol for Downloading a Private Key," Proc. of the 1999 Network and Distributed System Security (NDSS), 1999.

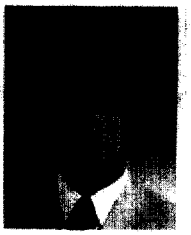
[10] M.Steiner, G.Tsudik, M.Waidner, "Refinement and extension of encrypted key exchange," ACM Operating Systems Review, 1995.

[11] T.Wu, "The Secure Remote Password Protocol," 1998 Internet Society Symposium on Network and Distributed System Security, 1998.

[12] 김경신, "한정 수신 방송 시스템에서의 스마트 카드를 이용한 정보 보호 프로토콜에 관한 연구", 박사학위청구논문, 성균관대학교, 1996. 10.

[13] 김경신, 김승주, 원동호, "스마트카드를 이용한 유료 방송 한정수신 시스템", 제6회 통신정보합동학술대회(JCCI '96) 논문집, pp.180-183, 1996.

[14] 은성경, 조현숙, "유료방송 해킹 방지 기법", NETSEC-KR '99, 1999.

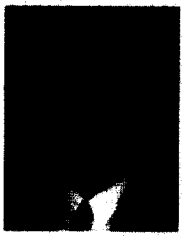


김 영 수

e-mail : yskim@dosan.skku.ac.kr
1998년 성균관대학교 정보공학과(학사)
1998년 현재 성균관대학교 대학원 전기, 전자 및 컴퓨터공학부 석사과정 재학
관심분야 : 한정수신시스템, 스마트카드, 패스워드-기반 프로토콜

손 기 욱

e-mail : kiwook@etri.re.kr
1990년 성균관대학교 정보공학과(학사)
1992년 성균관대학교 정보공학과 (공학석사)
1992년~현재 한국전자통신연구원 선임연구원
관심분야 : 통신망 정보보호, 암호 프로토콜



양 형 규

e-mail : hkyang@kns.kangnam.ac.kr
1983년 성균관대학교 전자공학과(학사)
1985년 성균관대학교 전자공학과 (공학석사)
1994년 성균관대학교 정보공학과 (공학박사)
1984년~1991년 삼성전자 선임연구원
1995년~현재 강남대 산업전산전자공학부 조교수
관심분야 : 통신망 정보보호, 암호 프로토콜

원 동 호

e-mail : dhwon@dosan.skku.ac.kr
1976년 성균관대학교 전자공학과(학사)
1978년 성균관대학교 대학원 전자공학과(공학석사)
1988년 성균관대학교 대학원 전자공학과(공학박사)
1978년~1980년 한국전자통신연구소 연구원
1985년~1986년 일본 동경공대 객원연구원
1996년~현재 성균관대학교 공과대학 전기전자 및 컴퓨터공학부 정교수
관심분야 : 암호이론, 정보이론