# 재인증주기를 통한 IEEE 802.11 무선랜 환경에서의 안전하고 효율적인 재인증과 키교환 프로토콜

김 세 진(金 世 珍), 안 재 영(安 宰 瑩), 박 세 현(朴 世 炫)
중앙대학교 전자전기공학부
전화 : (02) 820-5338 / 팩스 : (02) 825-1584

# An efficient and security-enhanced Re-authentication and Key exchange protocol for IEEE 802.11 Wireless LANs using Re-authentication Period

Se Jin Kim, Jae Young Ahn, Se Hyun Park
School of Electrical and Electronic Engineering, Chung Ang University
E-mail : shpark@cau.ac.kr

## Abstract

In this paper, we introduce an efficient and security-enhanced re-authentication and key exchange protocol for IEEE 802.11 Wireless LANs using Re-authentication Period. We introduce a low computational complexity re-authentication and key exchange procedure that provides robustness in face of cryptographic attacks. This procedure accounts for the wireless media limitations, e.g. limited bandwidth and noise. We introduce the Re-authentication Period that reflects the frequency that the re-authentication procedure should be executed. We provide the user with suitable guidelines that will help in the determination of the re-authentication period.

## I. 서론

무선통신의 기술의 발전을 따라 무선랜 분야도 많은 변화와 발전을 거듭하였다. 전파무선랜(Radio Wireless LANs)도 그 중 대표적인 예로 여러 상황에서 유선랜을 구축하는 경우보다 효과적으로 망을 구축할 수 있다. 1997년에 무선랜의 표준인 IEEE 802.11[5]이 승인되었다. 이 표준은 지원되는 두가지 물리계층(infra red와 radio)의 통신 원리에 대해 자세히 기술하고 있다. 본 논문에서는 이 중에서 대역확산기술을 사용하는 전파무선랜만을 고려한다. 대역확산방식 통신의 보안측면에 대해서는 [7]에서 연구되었다. [7]에서 저자들은 대역확산방식만을 유일한 보안 방어책으로 삼는 것은 불충분하다고 결론지었다. 같은 서비스 지역내에 있는 적극적인 침입자는 초기확산코드를 쉽게 알아낼 수 있다. 따라서 무선망환경에서 보안이 보장되는 안전한 통신망의 설계와 구현은 아주 중요하고도 어려운 일이다. 이러한 무선통신망 설계에서 무선매개물(wireless medium)은 그 자체로 본질적인 문제점(ISM 내에서의 제한된 대역폭, 노이즈에 의한 채널간섭, 이동터미널의 제한된 파워 등)을 안고있다[3].

본 논문은 위에서 언급한 문제점을 안고 있는 무선랜 환경에서의 재인증과 키교환에 대해 다루고자 한다. 이는 [1, 2]에서 제안되었던 인증 프로토콜에 기반을 둔 프로토콜로서, 암호화 공격에 강력한 대응을 하고 시스템 자원을 많이 소모하는 복잡한 계산을 줄인 안전하고 효율적인 재인증과 키교환 프로토콜이다. 이를 위해 재인증주기(Re-authentication Period)란 개념을 도입하였다. 무선랜환경에서 대역폭은 제한된 자원이므로, 재인증과 키교환을 위해 사용되는 대역폭에 대해서 알아본다. 이는 재인증주기, 시스템구성, 어플리케이션에 할당된 대역폭, 무선랜 데이터 전송률 등의 함수로 계산된다.

본 논문의 구성은 다음과 같다. 서론에 이어 II장에서는 재인증과 키교환 프로토콜을 제안한다. III장에서는 제안된 프로토콜의 성능을 분석하고, IV장에서는 이 논문의 결론을 맺는다.

## II. 재인증과 키교환 프로토콜

제안된 재인증과 키교환 프로토콜은 다음과 같은 무선랜의 고유한 특성을 고려하였다.

• 제한된 대역폭 : 무선랜은 특성상 제한된 대역폭을 갖고 있다. 이런 대역폭의 제한은 초기 인증 절차에서 널리 사용되고 있는 3단계 핸드쉐이크(three-way handshake) 과정을 사용하기 어렵게 한다.

• 노이즈에 노출된 무선채널환경 : 따라서, 보안 메시지가 목적지에 제대로 도착하지 못했을 때는 재전송이 준비되어야 한다. 만약에 TCP와 같은 신뢰할 수 있는 전송 프로토콜이 사용되었을 때는, 재전송은 이 전송 프로토콜에 의해 행해진다. 하지만, UDP와 같은 신뢰할 수 없는 전송 프로토콜이 사용되었을때는, 제안된 재인증 프로토콜이 재전송을 담당하게 된다.

• 보안을 위한 하드웨어를 무선랜카드에 추가하는 것은 많은 비용의 부담이 있고, 시스템의 유연성을 저해한다. : 그러므로, 재인증과 키교환은 소프트웨어로 구현하는 것이 바람직하다. 이를 위해 재인증 절차에서는 많은 복잡한 계산량을 필요로 하는 공개키 암호화 기술을 사용하지 않는다.

본 논문에서는 다음과 같은 표현들이 사용되었다.

- $L_i$ : nonce i의 생존기간
- $T$ : nonce가 발행된 시간
- $SK_i$ : i번째 세션키
- $MD(Z)$ : Z를 hash 한 값
- $E(X, <Y>)$ : 키 X를 사용한 Y의 암호화

제안된 재인증 프로토콜은 단방향 핸드쉐이크(one-way handshake)를 사용한다. 두 스테이션 ST1과 ST2의 세션에서, 재인증은 PC(Point Coordinator) 없이 두 스테이션 사이에서 행하여진다. 초기 인증 절차 후, ST1과 ST2는 위에서 언급한 $L_1$, $T$, $SK_1$ 등을 공유한다. ST1과 ST2 사이 세션에서 제안된 재인증과 키교환 프로토콜은 다음과 같다.

1. $i = 1$
2. 재인증을 요청할 때까지 기다린다.(재인증주기가 되었거나 공격받을 가능성이 있을 때 요구된다.)
3. i번째 재인증을 시작한다.(ST1 → ST2)
   a. $L_{i+1}$을 생성한다.
   b. ST1이 ST2에게 재인증 메시지를 보낸다. : $E(SK_i, <MD(L_i) \text{ xor } L_{i+1}>)$
   c. ST2는 재인증 메시지를 받는다.
      c.a. 재인증 메시지로부터 $L_{i+1}$을 구해낸다.
      c.b. $T$, $SK_i$, $L_{i+1}$을 이용해서 새로운 세션키를 만들어낸다. : $SK_{i+1} = MD(L_{i+1}+T) \text{ xor } SK_i$
      c.c. ST2에서 ST1으로 보내어진 데이터 패킷은 새로운 세션키 $SK_{i+1}$로 암호화된다.
4. 3의 과정을 마친 후 다음의 2가지 경우를 볼 수 있다.

• 재인증 메시지의 전송이 성공했을때(ST2로부터 새로운 키 $SK_{i+1}$로 암호화된 데이터를 받았을때) : $i = i+1$, *goto 2*

• 재인증 메시지의 전송이 실패했을때(ST2로부터 이전키 $SK_i$로 암호화된 데이터를 받았을 때) : *goto 3*(재인증 메시지를 재전송한다.)

그림 1은 이 프로토콜의 흐름도를 보여준다.

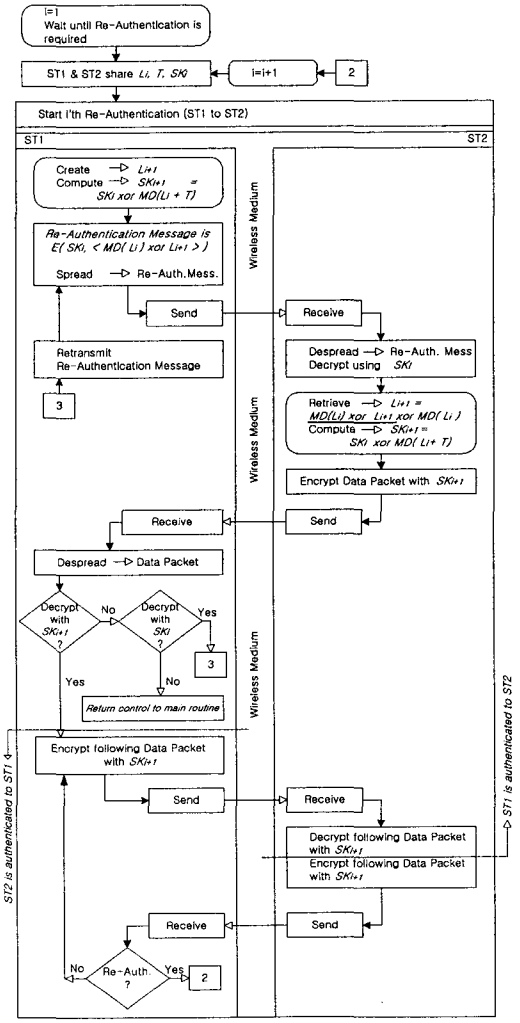


그림 1 재인증 프로토콜 흐름도

제안된 프로토콜은 다음과 같은 장점을 가지고 있다.

- 복잡한 계산량을 줄였다. : 공개키 암호화방식 대신에 공통키 암호화방식을 사용하여서, 프로토콜 계산의 복잡도를 줄였다.[4]
- 적은 대역폭을 사용한다. : 단방향 핸드쉐이크를 사용함으로써 사용되는 대역폭을 줄였다.
- 효율적인 보안방안을 제공한다. : 주기적으로 새로운 키를 만들어내어 재인증한다.
- 채널의 오류에 효율적으로 대응한다. : 재인증 메시지의 전송오류시, 재인증 메시지를 재전송한다.
- IEEE 802.11 PCF로 구현가능하다. : ST2에게 보낼 데이터가 있는 ST1이 PC에게 폴(poll)되고 재인증이 필요한 경우, ST1은 ST2로 데이터 패킷 대신에 재인증 메시지를 보내준다. 이는 [1]의 인증 절차를 보완해준다.(그림 2 참조)

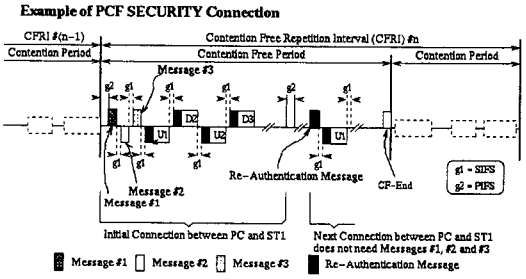


그림 2 PCF 보안 프로토콜

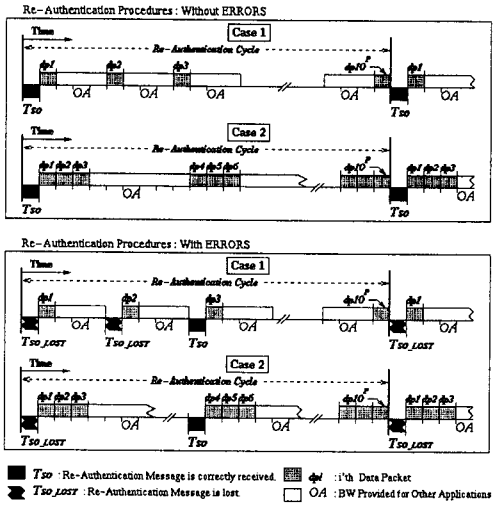


그림 3 재인증 간격의 예

## III. 성능 분석

이 장에서는 재인증주기(P)를 소개한다. 재인증은 ST1에서 ST2로 $10^P$개의 데이터가 전송될 때 마다 이루어진다. 재인증간격(re-authentication cycle)은 연속된 두 재인증 실행의 시간 간격 또는 연속된 두번의 세션키의 변화를 겪을 때의 시간 간격으로 볼 수 있다.(그림 3 참조) 재인증 간격은 ST1에서 ST2로의 $10^P$개의 데이터 전송과 재인증 오버헤드로 결정된다. 재인증 절차에 소요되는 대역폭은 어플리케이션에 할당된 대역폭과의 비로 나타낼 수 있다. 이는 무선랜에서의 데이터 전송율, 재인증 메시지의 손실확률, 보안측면의 오버헤드(재인증 메시지의 계산 시간과 전송시간, 목적지에서 새로운 키를 만드는데 걸리는 시간 등으로 구성되어 있다.), 재전송주기 등의 함수로서 표현될 수 있다.

이를 위해 다음의 변수들이 정의되었다.

- $T_{SO}$는 재인증 메시지의 계산시간과 전송시간, 목적지에서 새로운 키를 만드는데 걸리는 시간 등 보안에 관련된 재인증 오버헤드를 나타낸 값이다.
- $T_D$는 데이터 패킷의 전송시간을 나타내었다.
- A는 특정 어플리케이션에 할당된 대역폭을 무선랜의 총대역폭과의 비로 나타낸 것이다.
- P는 재인증주기를 나타낸다.
- $\rho$는 재인증 메시지에 에러가 발생하여 재전송이 필요하게 될 확률이다. 이때, 재인증 메시지의 평균 전송량은 $1/(1-\rho)$이다.

F라고 표기되는 재인증 절차에 사용되는 대역폭의 비는 다음과 같다.

$$F = \frac{T_{SO} * \frac{1}{1-\rho}}{T_{SO} * \frac{1}{1-\rho} + T_D * 10^P * A}$$

분자는 재인증 절차에 소모된 시간을 나타내며, 분모는 재인증 시간과 데이터 패킷의 전송 시간을 포함하는 재인증 간격을 나타낸다.

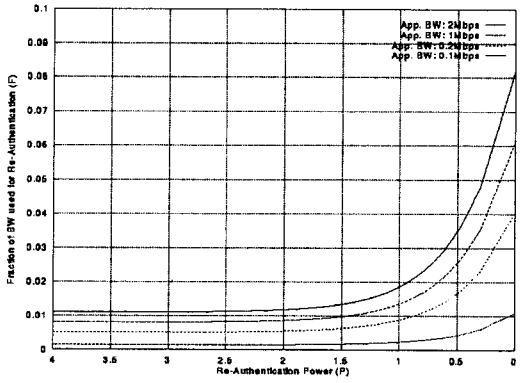


그림 4 재인증에 사용된 대역폭과 재인증주기의 비

그림 4는 재인증에 사용된 대역폭의 비 F를 재인증주기의 함수로서 보여주고 있다($\rho$는 16%로 가정). 이때 F는 여러가지 어플리케이션의 대역폭으로 계산되었다(100Kbps, 200Kbps, 1Mbps, 2Mbps). 참고로 컴퓨터는 Pentium MMX 166MHz, 16M main memory를 사용하였다.

그림 4로부터 다음과 같은 결과를 볼 수 있었다.

- 재인증주기가 증가하면, 대역폭의 비 F가 감소한다.
- 어플리케이션에 할당된 대역폭이 커지면, 대역폭의 비 F도 증가한다.
- 패킷의 손실이 많아지면, 재전송량의 증가로 대역폭의 비 F도 증가한다.

이러한 정보들은 유저에게 어플리케이션에 할당된 대역폭 중 재인증절차가 필요로 하는 대역폭의 비를 시스템 파라미터(시스템 구성, 데이터 전송율, 어플리케이션 대역폭 등)와 재인증주기의 함수로 알려줄 수 있다. 유저는 다음의 두가지 임계값을 제시할 수 있다.

- 첫번째 임계값은 어플리케이션에 필요한 최소의 대역폭이다. 이를 통해 $F_R$로 표기되는 재인증 절차에 이용되는 대역폭의 비를 정할 수 있다. 따라서 재인증에 소요되는 대역폭의 비 F가 $F_R$보다 작은 조건을 만족시키는 어떠한 재인증주기도 재인증절차에 사용될 수 있다.
- 두번째 임계값은 $P_R$로 표기되는 유저가 견딜 수 있는 최대 재인증주기이다. 즉, 재인증은 적어도 $10^{P_R}$개의 패킷이 전송된 후에는 반드시 이루어져야 한다. 이 임계값은 무선 매개물로 전송되는 데이터의 중요성에 따라 보안의 수준을 반영한다.

이러한 두가지 임계값을 만족시키는 값을 찾아서 최적의 재인증 절차를 구현할 수 있다. 하지만 두 임계값 모두를 만족시킬 수는 없는 경우에는, 두 임계값 중 어떤 임계값을 만족시키는 재인증 절차를 구현할지는 유저가 선택한다.

## VI. 결론

본 논문에서는 단방향 핸드쉐이크를 이용한 안전하고 효율적인 재인증과 키교환 프로토콜을 제시하였다. 또한 이를 위해 사용되는 대역폭을 어플리케이션에 할당된 대역폭의 비로 보여주었다. 이는 전체 대역폭과 어플리케이션에 할당된 대역폭의 비, 컴퓨터 구성, 채널의 노이즈로 인한 손실 등의 시스템 파라미터들과 재인증주기의 함수로써 나타낼 수 있다. 유저는 이런 데이터를 근간으로 소요되는 대역폭을 고려해 알맞은 재전송주기등을 선택해 필요한 보안 수준을 구축할 수 있다.

## 참고문헌(또는 Reference)


[1] S.H. Park, A. Ganz, and Z. Ganz, "Security protocol for IEEE 802.11 Wireless Local Area Networks", ACM Mobile Networks Journal Special Issue on Wireless Local Area Networks.

[2] S.H. Park, A. Ganz, and Z. Ganz, "Token-Based Security Protocol for Wireless Local Area Networks", Third Telecommunication R&D Conference in Massachusetts, Lowell, MA, Nov.1997.

[3] A. Aziz and W. Diffie, "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, First Quarter, 1994, pp.25-31.

[4] B. Schneier, "Applied Cryptography", Wiley, 1996.

[5] IEEE Standard 802.11 for Wireless LAN, IEEE P802.11, 1997.

[6] D. Eckhardt and P. Steenkiste, "Measurement and Analysis of the Error Characteristics of an In-Building Wireless Network", SIGCOMM '96, Standford, CA, Aug. 1996, Proceedings, pp. 243-254.

[7] H. Imai, "Information Security Aspects of Spread Spectrum Systems", Proceedings of the Advances in Cryptography - ASIACRYPT '94, 1994, PP. 195-208.