무선 랜에서 빠른 재 인증을 이용한 간소화된 키 관리 기법

(A Lightweight Key Management for Wireless LANs with the Fast Re-authentication)

이 재 형 † 김 태 형 †† 한 규 필 †† 김 영 학 †††
(Jae-Hyoung Lee) (Tae-Hyong Kim) (Kyu-Phil Han) (Young-Hak Kim)

요 약 IEEE 802.11 무선 랜이 보안 측면에서 몇 가지 심각한 약점을 가진다는 것이 알려진 후 이러한 무선 랜 보안의 결함을 줄이기 위하여 많은 연구가 수행되어졌다. 그 중 IEEE 802.11i는 새 무선 랜 제품과 함께 새로운 보안 플랫폼을 필요로 하는 궁극적인 장기 해결책이다. 그러나 이 방법은 큰 비용이 들기 때문에 비용이 중요한 작은 기관에게는 적합하지 않을 수 있다. 본 논문은 기존 제품을 조금 변경함으로써 그대로 사용가능한 무선 랜을 위한 간소화된 키 관리 기법으로 FR-WEP을 제안한다. FR-WEP은 최근 제안된 간소화된 키 관리 기법인 WEP*[9]의 확장으로, 호스트 키와 사용자 키를 모두 사용하는 간소화된 상호 인증과 빠른 재 인증을 통해 인증된 사용자들에게 균일한 키 갱신을 제공함으로써 WEP*의 약점을 보완한다. FR-WEP은 특히, 더 나은 보안을 원하는 작은 기관들에게 무선 랜 보안을 위한 무거운 표준안에 대해 좋은 대안이 될 것이다.

키워드 : 무선 랜, 키 관리, 빠른 재 인증

Abstract Since the IEEE 802.11 wireless LANs were known to have several critical weaknesses in the aspect of security, a lot of works have been done to reduce such weaknesses of the wireless LAN security. Among them IEEE 802.11i may be the ultimate long-term solution that requires new security platform with new wireless LAN products. However, it might not be the best solution for small organizations due to its high cost where the cost is a critical issue. This paper proposes FR-WEP, a light-weight key management for wireless LANs that can be used with small changes of the existing products. FR-WEP is an extension to a lightweight key management, WEP*[9], which was proposed lately. It makes up for the weak points of WEP* by providing lightweight mutual authentication with both host keys and user keys, and seamless key-refresh for authenticated users with fast re-authentication. It would be a good alternative to the heavy standards for wireless LAN security, especially to small organizations hoping for better security.

Key words : wireless LANs, key management, fast re-authentication

1. 서 론

현재 무선 네트워크는 데이타 통신을 주도해 가는 핵심 기술로 급격히 성장하고 있다. 그러나 무선 매체의 공개성에 따른 해킹의 용이성과 호스트의 이동에 따른 보안 체계의 복잡성은 무선 네트워크의 성장을 위해 해결해야 할 가장 중요한 영역이 되었다. 무선 네트워크에서 고속 데이타 전송을 위해 가장 널리 사용되고 있는 것은 무선 랜으로 현재 IEEE(Institute of Electrical and Electronics Engineers) 802.11 무선 랜 표준[1]을 따르는 많은 제품이 생산되고 있다. 그러나 이 무선 랜 표준은 공중망에의 도입을 목적으로 설계되지 않았기 때문에 보안에 많은 문제점을 내포하고 있다. IEEE 802.11 무선 랜 표준은 스트림 암호화 방식을 사용하는 WEP(Wired Equivalent Privacy)이라는 암호화 기법을 제공하고 있다.

· 본 연구는 2003년도 금오공과대학교 학술연구비 및 기성회 연구용 기자재 지원비에 의하여 연구된 논문임
† 학생회원 : 금오공과대학교 컴퓨터공학부
zzeng09@kumoh.ac.kr
†† 정 회 원 : 금오공과대학교 컴퓨터공학부 교수
taehyong@kumoh.ac.kr
kphan@kumoh.ac.kr
††† 종신회원 : 금오공과대학교 컴퓨터공학부 교수
kimyh@kumoh.ac.kr
논문접수 : 2004년 11월 26일
심사완료 : 2005년 1월 27일

WEP은 통신의 비밀성을 위해 RC4(Rivest Cipher 4) 스트림 암호[2]로 프레임의 몸체를 암호화 하고, 무결성을 위해 CRC(Cyclic Redundancy Check)-32로 프레임 몸체에 대한 무결성 확인 값(ICV: Integrity Check Value)을 생성하여 첨부하며, 호스트의 인증을 위해 WEP 키를 이용한 공유키 인증을 제공하고 있다. 그러나, 최근 보안이 중요한 문제로 대두되면서 이 WEP 암호화 방식에 많은 약점이 존재한다는 것이 여러 연구들로부터 밝혀졌고[3-5], 이는 보안이 필요한 회사나 은행 등에서의 무선 랜 도입에 가장 큰 걸림돌이 되고 있다. 이에 따라 이러한 약점을 극복하기 위해 WEP 키의 크기를 늘이는 것과 같은 간단한 것에서부터 인증 서버와 인증 프로토콜을 도입하는 것[6]과 같은 구조적인 것에 이르기까지 다양한 연구가 이루어져 왔다.

IEEE 802.11 TGi(Task Group i) 워킹그룹에서는 IEEE 802.11의 이러한 보안 취약점들을 개선하기 위한 새로운 형태의 보안 구조로 RSN(Robust Security Network)을 제안하고 IEEE 802.11i 표준화 작업을 수행하고 있다. IEEE 802.11i는 암호화 방식을 RC4보다 보안성능이 우수한 AES-OCB(Advanced Encryption Standard-Offset CodeBook)[7]로 변경하는 등, 여러 부분에서 많은 개선이 이루어져 높은 보안 성능을 가질 것으로 기대되고 있다. 그러나 이러한 보안 표준을 따르는 제품이 생산되어 안정적으로 사용되기까지는 많은 시간과 비용이 예상되며 이전 제품과의 호환성을 보장하지 못하는 문제점을 가지고 있다. 이러한 상황에 대한 단기적인 대책으로 무선 랜 제품개발자들의 협회인 Wi-Fi(Wireless Fidelity)에서 WPA(Wi-Fi Protected Access) 표준을 제안하였다[8]. 이 표준은 WEP의 키 관리 문제점을 해결하기 프레임별로 키를 변경하는 TKIP(Temporary Key Integrity Protocol)을 제안하였는데, 이는 IEEE 802.11 TGi 워킹그룹에서 제안한 RSN 구조를 이용하면서도 기존 장비의 펌웨어 업그레이드를 통해 구현이 가능하다는 장점을 가지고 있다. 그러나 WPA 표준은 RADIUS(Remote Authentication Dail-In User Service) 인증 서버를 통한 IEEE 802.1X 인증 방식을 채택하고 있어 보안 시스템을 갖추기 위해서는 역시 별도의 추가설비가 필요하다.

본 논문에서는 IEEE 802.11i 보안 표준을 따르는 제품이 기존의 제품을 대체하기 이전의 상황에서 별도의 추가 설비 없이 기존의 무선 랜 제품의 펌웨어 업그레이드 등을 통해 현재의 WEP 암호화 방식의 문제점을 해결하기 위한 간소화된 키 관리 기법을 제안한다. 제안된 기법은 키 갱신과 호스트 폐지를 이용한 간소화된 키 관리 기법인 WEP*[9]에서 고무된 것으로 간소화된 키 관리 기법의 틀 안에서 자동 키 재지정(rekeying) 기법과 기존의 인증 메시지 교환을 통한 AP(Access Point)와 호스트간의 상호 인증 기법을 사용하는 빠른 재인증 기반의 WEP 암호화 기법(FR-WEP: Fast Re-authentication based WEP)이라 할 수 있다. FR-WEP 암호화 기법은 WEP 또는 WEP* 방식보다 우수하고 안정적인 보안 성능과 더불어 기존 제품과 함께 사용가능한 이전 호환성을 제공한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 기존 WEP 암호화 방식의 문제점과 이를 해결하기 위한 관련 연구들을 간략히 소개한 다음 제안하는 기법의 설계 방향과 자세한 동작원리를 3장에서 다룬다. 4장에서는 제안된 기법의 정당성과 이전 장비와의 호환성을 살펴보고 다른 기법과의 성능 비교를 통해 제안된 기법의 평가를 수행한 다음 5장에서 결론을 맺는다.

2. 관련 연구

제안하는 키 관리 기법을 설명하기에 앞서 먼저 IEEE 802.11 표준 WEP 암호화 방식의 문제점과 이를 해결하기 위한 관련 연구들을 간단히 소개한다. 기존의 연구들과의 비교를 통해 본 제안 기법의 동기와 개선점을 명확히 이해할 수 있을 것이다.

2.1 RC4 암호화의 문제

WEP은 가변 키를 사용하는 스트림 암호화 기법인 RC4 암호화를 사용한다[2]. WEP은 24비트 크기의 IV(Intialization Vector)와 40비트 크기의, WEP 키라 불리는 네 개의 공유키 중 하나로 구성된 총 64비트의 키를 이용해 RC4 키스트림을 생성한다. 그러나 IV는 IEEE 802.11의 프레임에서 암호화되지 않기 때문에 WEP 키가 갱신되지 않는다면 그리 길지 않은 시간 안에 동일한 키스트림을 사용하는 프레임들을 찾아낼 수 있다.

WEP에서 사용하는 RC4 암호화의 가장 큰 문제점은 IEEE 802.11이 LLC(Logical Link Control) 캡슐화를 사용하기 때문에 암호화할 데이타의 첫 바이트가 노출된다는 점이다[4]. 이로 인해 충분한 양의 프레임을 캡처할 경우 동일한 WEP 키와 IV 중 몇 개의 취약키를 갖는 프레임들을 이용해 비밀 키를 쉽게 계산해 낼 수 있다는 심각한 문제를 낳는다[4]. 이를 이용해 실제 Wepcrack이나 Airsnort와 같은 WEP 키 크래킹 소프트웨어가 개발되어 있는 실정이다.

이 문제의 해결을 위해 크게 두 가지의 접근 방법이 존재하는데 하나는 RC4 대신 다른 암호화 기법을 사용하는 것이고 다른 하나는 RC4를 그대로 사용하고 WEP 키의 해독을 보다 어렵게 만드는 것이다. WEP 키를 40비트에서 104비트로 확장하는 것은 무선 랜 제품의 개발 시 실제 많이 쓰이고 있으나 WEP 키의 해독 시간

을 약간 연장 시켜줄 뿐 근본적인 해결 방법은 되지 못한다. 가장 주목받는 해결 방법은 WEP 해독에 필요한 충분한 데이타를 갖지 못하도록 WEP 키를 자주 갱신하는 기법이다[9,10]. 이러한 기법은 AP와 호스트가 장기 마스터 비밀 키를 공유하고 이를 통해 주기적으로 WEP 키를 생성해내는 방법을 이용한다. WPA의 TKIP 메커니즘도 이러한 키 재사용 기법을 기반으로 하고 있다. 한편 IEEE 802.11i는 이 문제에 대한 궁극적인 해결방법으로 RC4 암호화 대신에 CCM(Counter Mode Encryption with CBC-MAC) 모드의 AES(Advanced Encryption Standard) 암호화를 사용한다[11].

2.2 인증 프레임을 이용한 인증의 문제

IEEE 802.11은 호스트의 무선랜 서비스를 위한 인증을 위해 다음과 같은 4개의 인증 프레임(authenticaton frame) 교환에 의한 인증 프로토콜을 사용한다.

표 1 LKM에서의 인증 메시지

순서번호	전송방향	Payload 내용	WEP	메시지번호
1 :	host → AP :	없음	사용안함	1
2 :	AP → host :	N(도전문)	사용안함	2
3 :	host → AP :	WEP[N]	사용	3
4 :	AP → host :	successful/fail	사용안함	4

이 인증 과정의 문제점 중 가장 심각한 것은 RC4 스트림 암호를 사용하기 때문에 암호화되지 않은 도전문을 포함하는 2번 메시지와 공유키로 암호화된 도전문을 포함하고 있는 3번 메시지의 캡쳐를 통해 RC4 키스트림을 생성해 낼 수 있다는 것이다[3]. 이 RC4 키스트림과 이미 알고 있는 IV를 이용하면 무선 랜 상의 데이타를 위조할 수 있게 된다. 만약 MAC(Med ium Access Control) 기반의 접근 제어를 사용하지 않는다면 2번 인증 메시지에 대해 올바른 3번 메시지를 생성할 수 있게 되어 불법 인증이 가능하게 된다.

이 문제를 해결하기 위한 일반적인 접근 방법은 외부에 AP와는 별도로 RADIUS 서버와 같은 인증 서버를 두는 것이다[6]. 이때 인증 프로토콜은 802.1X 인증 구조를 사용하게 되며 인증 서버로부터 인증키를 안전하게 전송받기 위해 키 전송 프로토콜이 요구된다. 그러나 이러한 별도의 설비 도입은 무선 랜 시스템의 광범위한 도입에 장애가 될 수 있다는 문제점을 갖는다.

2.3 MAC 기반 접근제어 및 호스트 폐지 문제

IEEE 802.11 무선 랜은 WEP 키를 이용해 호스트의 인증을 수행하지만 WEP 키가 보안상 안전하지 못하기 때문에 현재 많은 무선 랜 제품들이 선택 항목으로 MAC 기반의 접근 제어 기능을 제공하고 있다. 즉, 인증 시에 MAC 주소를 확인하여 미리 입력된 결합 허용 주소 목록에 들어있는 경우에만 인증을 허용하는 것이다. 이 방법은 유용하게 사용될 수 있지만 보안 측면에서 역시 문제점을 가지고 있다. 즉, MAC 주소는 IEEE 802.11 프레임에 암호화되지 않고 그대로 노출되어 전송되기 때문에 결합 허용 주소를 쉽게 알 수 있고, 이에 따라 공격자에 의해 MAC 주소가 쉽게 변경될 수 있어 사칭(spoofing) 공격이 가능하다.

또 하나의 문제점은, 이러한 MAC 기반 접근 제어가 성공한다 하더라도 WEP 키가 알려졌을 경우에는 데이타를 전송하는 것은 불가능하지만 무선 데이타를 캡쳐하여 그 내용을 확인하는 스니퍼링은 여전히 가능하다는 점이다. 예를 들어 어느 회사의 직원이 회사를 퇴사했을 경우, 회사의 네트워크 관리자가 그 사원이 사용하던 호스트의 MAC 주소를 접근 허용 주소 목록에서 삭제하더라도 WEP 키가 변경되지 않는 한 그 사원은 WEP 키를 이용해 회사 주변에서 회사 네트워크의 무선 데이타 도청이 가능하다. 이 문제를 방지하기 위해서는 사원의 퇴사에 맞추어 WEP 키를 갱신해야 하는데 자동 키 갱신 메커니즘이 없다면 상당히 번거로운 일이 될 것이다. 이러한 호스트의 폐지 문제를 해결하기 위해서 몇 가지 키 갱신 기법이 제시되었는데 [9,10] 그 중 WEP* 기법을 2.5절에서 자세히 다룰 것이다.

2.4 데이타 무결성을 위한 CRC-32 사용 문제

WEP 암호화 기법은 데이타의 무결성 검사를 위해 CRC-32를 이용한다. CRC는 우수한 버스트 오류 검출 성능을 가지기 때문에 많은 프로토콜의 데이타 오류 검출에 사용되지만 암호학적으로는 전혀 안전하지 않다[12]. 암호학적으로 안전한 무결성 검사 코드는 예측 불가능한 해쉬 함수에 의해 생성되어서 공격자가 데이타를 수정하였을 때 예측 불가능하도록 변경되어야 한다. 그러나 CRC 코드는 키를 갖지 않는 선형 함수에 의해 생성되며 WEP의 RC4 암호화도 역시 선형함수인 XOR 연산을 사용하기 때문에 데이타 수정 시에 변경되는 값을 쉽게 예측할 수 있다[5].

WPA 표준의 TKIP은 이러한 WEP의 데이타 무결성에 대한 취약점을 해결하기 위해 CRC-32 대신 암호학적으로 보다 안전한, 키 기반의 해쉬 함수인 Michael[13]을 사용하며, IEEE 802.11i 표준에서는 인증과 암호화에 사용되는 CCM 프로토콜을 통해 데이타의 무결성도 함께 보장한다.

2.5 WEP*: 간소화된 키 갱신 기법

IEEE 802.11 무선 랜의 WEP은 네 개의 장기(long-term) 공유키 중 정적으로 한 개를 선택하여 암호화 및 인증에 사용한다. 이러한 정적 키 갱신 방법으로는 2.3절에서 설명한 것과 같이 호스트 폐지 문제에 효과적으로 대처할 수 없다. WEP*[9]는 이 문제를 해결

하기 위해 제안된 간소화된 키 관리 기법으로 이전 호환성을 최대한 유지하도록 하여 현재의 무선 랜 장비에 대한 최소한의 수정으로 사용이 가능하도록 고안되었다.

WEP*는 AP에서 호스트의 인증 시에 네 개의 WEP 키 셋을 생성하고 두 번째 인증 메시지를 이용하여 도전문 영역에 키 셋과 키 갱신을 위한 정보를 실어 각 호스트에게 분배한다. 이 때 키를 허가된 사용자에게 안전하게 분배하기 위해 위 정보를 각 호스트와 AP 간에 사전 공유된 장기 대응키로 RC4 암호화하여 보낸다. 이 장기 대응키를 사원이 퇴사했을 때 말소시킴으로써 호스트 폐지 문제를 해결할 수 있다. 키 셋을 받은 호스트는 기존의 인증과 결합 과정을 통해 AP에 결합된 후 키 셋의 첫 번째 키를 이용해 암호화된 데이타를 주고받는다. 이때 키 셋과 함께 받은 정보 중 키 재지정 시간이 지나면 AP와 각 호스트는 자동적으로 키 셋 내의 그 다음 키로 사용키를 변경한다. 이 과정을 세 번 반복하여 키 셋 내의 모든 키를 다 사용한 후에는 인증 해제를 수행하고 다시 인증-결합 과정을 통해 새로운 키 셋을 AP로부터 할당받게 된다.

WEP*는 기존의 인증 메시지 교환을 이용하여 키 분배를 수행하기 때문에 일반 WEP을 지원하는 무선 랜 제품과 함께 사용할 수 있고 간단한 업그레이드를 통해 무선 랜 제품의 WEP을 WEP*로 변경할 수 있다는 장점을 갖는다. 그러나 AP와 호스트간의 장기 대응키만으로는 사용자 인증을 완벽히 수행하기 어렵고, 키 갱신 시 각 호스트 간에 타이밍 문제가 발생하며, 키 셋에 있는 네 개의 키를 모두 사용한 후에는 인증해제와 새 인증 과정을 통해 키를 다시 받아야하는 문제가 존재한다.

한편, WEP*는 IEEE 802.11 인증 과정을 그대로 사용하기 때문에 도전문과 이에 대한 RC4 암호문이 함께 노출되어 키스트림을 추출할 수 있는 문제가 여전히 존재한다. 이 문제를 해결하기 위하여 WEP* 저자는 WEP**도 함께 제안하고 있는데 이는 호스트에서 3번 인증 메시지 전송 시 도전문이 아닌 호스트의 정보에 대해 RC4 암호문을 구성하는 것이다. 이때 전송되는 호스트의 정보는 호스트의 인증에 사용할 수 있어 보이지만 이 경우 호스트의 인증 이전에 2번 인증 메시지를 통하여 WEP 키 셋이 호스트에게 전송되기 때문에 실제 호스트 인증의 의미를 부여하기는 어렵다는 단점을 갖는다[9].

3. 제안하는 키 관리 기법

3.1 설계 방향(design approach)

제안하는 키 관리기법 FR-WEP은 기본적으로 WEP*의 간소화된 키 관리기법과 동일한 출발점을 갖는다. 즉, 기존의 IEEE 802.11 표준을 최대한 유지하여 하위 호환성을 제공하고, 기존의 인증 메시지 교환을 이용하여 키 셋을 분배하는 간소화된 키 관리를 수행하는 것이다. 그러나 FR-WEP은 2.5절에서 언급한 WEP*의 문제점들을 상당 부분 해결한 것으로, 보다 체계적인 키 관리 기법이라 할 수 있다. FR-WEP의 설계 방향은 다음과 같다.

첫째, 이동 호스트의 다양한 사용 환경을 만족시킬 수 있는 사용자 인증 기법을 구현하고 호스트 폐지 문제에 보다 효과적으로 대응하도록 한다.

둘째, 인증 메시지 교환 시, 호스트와 AP간에 간소화된 상호 인증이 이루어지도록 하며 상호 인증이 성공한 후에 WEP 키 셋이 호스트에게 전송되도록 한다.

셋째, 인증 메시지를 통해 받은 키 셋 내의 각 키 갱신 시 각 호스트 간에 타이밍 문제가 발생하지 않도록 한다.

넷째, 키 셋 내의 키를 다 사용한 후에 새로운 키 셋을 다시 전송 받기 위해 인증 해제를 거치지 않고 신속하게 재 인증을 수행하여 네트워크 서비스 이용에 지장을 주지 않도록 한다.

본 장에서는 이러한 목적을 이루기 위하여 FR-WEP이 어떻게 구현되고 동작하는가를 단계적으로 자세히 설명한다.

3.2 용어 정의

먼저 제안하는 키 관리 기법의 명확한 기술을 위해 본 논문에서 사용되는 용어를 다음과 같이 정의한다.

- 현 WEP 키 셋(K_{curr}) : 무선 랜에서 WEP 암호화를 제공하기 위해 AP와 이동 호스트간에 현재 공유되는 WEP 키 셋 ($K_{curr}.k[0]$, ..., $K_{curr}.k[3]$)
- 사용자 키(K_{user}) : 사용자를 인증을 위한 인증키로 각 사원에게 부여되는 64비트의 비밀 키이다. 사용자에 의한 접근 제어를 위해 AP에서도 각 호스트에 대응하는 사용자 키 목록 $K_{user}.k[i]$을 MAC 주소 테이블에서 관리 한다 (단, $1 \le i \le N$ 이고, N은 한 호스트의 최대 사용자 수).
- 호스트 키(k_{host}) : 이동 호스트의 인증을 위한 인증키로 각 이동 호스트에게 부여되는 64비트의 비밀 키이다. 호스트에 의한 접근 제어를 위해 AP에서도 각 호스트 ID에 대응하는 호스트 키를 MAC 주소 테이블에서 관리 한다.
- 활성화된 사용자 키($K_{user}.defkey$) : 특정 호스트에 대응된 사용자 중에 현재 네트워크 사용이 허가되어 사용 중인 사용자 키의 인덱스.
- 기본 키 지정자($K_{curr}.defkey$) : 현재 AP와 이동 호스트에서 사용되고 있는 기본 키를 지정하기 위해 사용되고 있는 인덱스(index), $0 \le K_{curr}.defkey \le 3$.

- 키 갱신 : 현 WEP 키 셋 K_{curr} 중에서 현재 기본 키로 사용되고 있는 키를 키 갱신 기간(T_{rekey})에 따라 키를 갱신해 줌으로 AP와 이동 호스트 간의 키 동기화를 제공한다. (K_{curr}에서 최대 3번 갱신; IEEE 802.11에서는 4개의 WEP 키를 가짐)
- 키셋 갱신 : 이동 호스트의 키 갱신이 모두 이루어지고 나면 새로운 키 셋을 받기위해 AP에서 현재 사용하고 있는 키 셋의 만료 전에 새롭게 생성한 키 셋을 현재 AP와 결합되어 있는 모든 이동 호스트에게 전송한다.

제안하는 FR-WEP은 기존 WEP 키의 보안 취약점을 극복하기 위하여 주기적인 WEP 키 갱신과 함께 주기적인 WEP 키 셋 갱신을 수행한다. 이 과정은 3.5절과 3.6절에서 자세히 다룰 것이다.

3.3 호스트 키 및 사용자 키 관리

실제적인 업무 환경에서는 각각의 호스트마다 여러 명의 사용자가 있을 수 있고, 반대로 하나의 사용자가 여러 개의 호스트를 사용할 수 있다. 이런 상황에서 AP와 호스트 간의 대응키 즉, 호스트 키만으로는 사용자 인증을 효과적으로 수행하기 어렵다. 이러한 환경에 효과적으로 대처하기 위해서 각 호스트에 대해 호스트 키(k_{host})와 더불어 사용자에 대한 비밀 키인 사용자 키(K_{user})를 둔다. 대부분의 AP는 MAC 주소 기반의 접근 제어를 제공하기 위해 MAC 주소 테이블을 가지고 있다. 표 2는 사용자 인증을 위해서 AP의 MAC 주소 테이블에 호스트 키(k_{host})와 사용자 키(K_{user}) 필드를 추가한, 확장된 MAC 주소 테이블 구조이다.

표 2 AP의 확장된 MAC 주소 테이블

(단, $1 \le i_n \le N$, $n=1,2,\cdots$, N은 한 호스트의 최대 사용자 수)

호스트 ID	k_{host}	K_{user}	$K_{user}.defkey$
MAC 주소$_1$	$k_{host.1}$	$K_{user.1}.k[N]$	i_1
MAC 주소$_2$	$k_{host.2}$	$K_{user.2}.k[N]$	i_2
MAC 주소$_3$	$k_{host.3}$	$K_{user.3}.k[N]$	i_3
...	...	...	...

표 2의 $K_{user}.defkey$는 각 호스트에 대해 현재 사용이 허가되어 활성화된 사용자의 인덱스를 나타내는 필드로 만약 어느 호스트에 대해 활성화된 사용자가 없을 경우에는 -1값을 갖는다. AP는 'MAC 주소$_j$'을 호스트 ID로 갖는 각 호스트에 대해 호스트 키 $k_{host.j}$와 호스트의 사용 권한을 갖는 사용자들의 사용자 키 $K_{user.j}.k[N]$ 및 현재 활성화된 사용자 정보 i_j를 가진다. 각 호스트에 대해 해당 호스트를 사용할 수 있는 권한이 있는 사용자는 여러 명일 수 있으나 특정 시간에는 한 사람 만이 사용하게 되므로 AP는 그 사용자에 대해서만 인증을 수행하게 된다.

이 호스트 키와 사용자 키는 다음 절에서 설명할 AP와 호스트 간의 간소화된 상호 인증에 사용된다. 2.3절에서 언급한 것처럼 호스트의 MAC 주소는 암호화되지 않고 전송되기 때문에 이를 호스트 인증에 사용하여 접근 제어를 수행하는 것은 안전하지 않다. 따라서 FR-WEP은 WEP*의 경우와 같이 호스트 키를 통해 호스트 인증을 수행하게 된다. 그러나 일반적으로 어느 호스트를 사용하는 사용자가 항상 동일한 사람이 아닐 수도 있기 때문에 사용자 키를 통한 사용자 인증을 함께 수행한다면 보다 높은 보안 성능을 얻을 수 있을 것이다. 이 경우 사용자가 이동 호스트에 로그인할 때 해당 사용자의 사용자 키가 호스트의 무선 랜 장치에 설정되도록 하는 사용자 세션 관리 소프트웨어가 이동 호스트 내에 운용되어야 한다.

사용자 키를 통해 인증을 수행할 경우, 호스트 폐지 문제, 보다 정확히는 사용자 폐지 문제에도 보다 효과적으로 대처할 수 있다. 즉, 회사에서는 사원의 입사 시에 그 사원에 대한 사용자 키를 생성하고 퇴사 시에는 그 사용자 키만 말소시키면 된다. 나아가 각 사용자의 인증 시간을 저장할 수 있으므로, 근무 외 시간의 사내 무선 네트워크 서비스 사용 여부를 확인할 수 있는 등의 추가적인 보안 관리가 가능하다.

3.4 간소화된 상호 인증

IEEE 802.11의 인증 메커니즘은 AP와 호스트 간의 공유키를 통해 호스트를 인증하는 형식이다. 그러나 계속 살펴본 바와 같이 공유키의 비밀 보장이 이루어지지 않기 때문에 위장된 호스트에 의한 인증 사칭의 위협이 존재하며 호스트에게는 AP의 인증이 이루어지지 않기 때문에 위장된 AP에 의해 정보가 노출될 수 있는 문제가 있다. 이러한 문제에 대처하기 위해 제안하는 FR-WEP에서는 AP와 호스트 간에 간단한 상호인증을 제공한다. 즉, 기존의 인증 메시지 교환 과정에서 호스트 및 사용자의 인증을 가장 먼저 수행하기 위해서 1번 인증 메시지(표 1 참조) 대신 사용할 5번 인증 메시지를 새로 설계하였고, AP의 인증을 위해서는 WEP*의 2번 인증 메시지와 유사한 방식으로 2번 인증 메시지를 수정하였다. 이 때 WEP*와 같이 2번 메시지를 통해 WEP 키 셋 K_{curr}이 주어진다. 따라서 상호인증이 성공적으로 수행된 경우에만 호스트는 AP로부터 주어진 WEP 키를 사용하게 된다.

3.4.1 호스트 및 사용자 인증

5번 인증 메시지는 인증 메시지의 인증처리 순서번호 필드에 5 값을 넣어 구별하며 1번 인증 메시지에서는 사용하지 않는 도전문 부분을 추가하고 도전문 영역(M_5)에 표 3과 같은 정보를 실어 AP에게 전송한다.

표 3 5번 인증 메시지의 도전문 영역 M_5 (암호화 전)

Field	h	t_{host}	MAC_{AP}	MAC_{host}
Bytes	20	8	6	6

표 3에서 MAC_{host}와 MAC_{AP}는 각각 host와 AP의 MAC 주소를 저장하기 위한 필드이고, t_{host}는 호스트에서의 5번 메시지 전송 시각을 저장하기 위한 필드이다. h는 암호화 해쉬 함수의 출력 값을 저장하는 필드로 호스트에서 5번 메시지 도전문 영역 M_5 내의 모든 필드를 채운 후에 M_5에 대해 암호화 해쉬 함수 $H(M_5)$를 계산하여 그 값을 h에 기록한다. 해쉬 함수로는 CRC보다 우수한 보안 성능을 가진, 20 바이트의 출력을 갖는 SHA-1(US Secure Hash Algorithm 1)을 사용한다 [14]. 5번 인증 메시지를 이용한 호스트와 사용자의 인증 절차는 다음과 같다.

(1) 호스트는 비컨 메시지나 프로브 응답 메시지를 통해 얻은 무선 랜의 정보를 바탕으로 5번 메시지를 구성한다. 이 때 도전문 영역 M_5의 각 필드를 표 3과 같이 채운다.

(2) M_5의 모든 필드를 채우게 되면, 사용자 키 k_{user}와 호스트 키 k_{host}를 합한 128비트의 키를 이용하여 암호화된 도전문 $C_5 = E_{k_{user}, k_{host}}(M_5)$을 생성한다.

(3) 생성된 암호화된 도전문 C_5는 5번 인증 메시지의 AP에게 전달된다.

(4) AP에서는 5번 인증 메시지 MAC 주소를 통해 자신의 MAC 주소 테이블에 등록된 호스트의 MAC 주소$_j$를 찾는다.

(5) AP의 MAC 주소 테이블에 등록된 호스트의 $k_{host,j}$와 $K_{user,j}.k[i]$에 대해 (초기값 i=0) 5번 인증 메시지의 도전문 C를 복호화하여 원문 M을 얻는다. 즉, $M = E^{-1}_{K_{user,j}.k[i], k_{host,j}}(C)$. 여기서 메시지 M 내의 필드 F의 값은 F^M으로 표기한다.

(6) AP는 $H(M) = h^M$ 인지를 검증함으로 메시지의 무결성을 검사한다.

(7) $MAC_{host}{}^M = MAC_{host}$, $MAC_{AP}{}^M = MAC_{AP}$ 인지와 $|t_{AP} - t_{host}{}^M| \leq \Delta$ 가 만족하는지를 검증하여 재연(replay) 공격을 방지한다. 여기서 Δ는 호스트와 AP사이의 허용 메시지 전파 시간의 최대값이다.

(8) 만일 하나라도 검증에 실패하면, AP는 i를 하나 증가시켜 (5)~(7)번 과정을 반복한다. 모든 등록된 사용자에 대해 검증이 실패하면 인증 실패로 판단하고 인증 실패를 나타내는 4번 인증 메시지를 호스트에게 보낸다.

(9) 검증에 성공하면 AP는 $K_{user,j}.defkey$ 필드를 현재 i 값으로 저장한다.

등록된 각 사용자에 대해 인증과정을 반복함으로써 발생하는 지연 시간을 최소화하기 위해서 $K_{user,j}.k[i]$ 값을 등록할 때 사용자의 사용 빈도 순서에 따라 사용자 키를 저장한다.

3.4.2 AP 인증

AP는 5번 인증 메시지를 통해 호스트 및 사용자의 인증에 성공하면 2번 인증 메시지를 생성하여 해당 호스트에게 전송한다. 이 때 2번 메시지의 도전문 생성 시 IEEE 802.11 표준에 따라 RC4 암호화기법으로 얻어진 도전문을 생성하지 않고 표 4와 같이 WEP 키 셋과 AP의 인증을 위한 정보로 구성된 메시지 M_2로부터 도전문을 생성한다.

표 4 수정된 2번 인증 메시지의 도전문 영역 M_2 (암호화 전)

Field	h	t_{AP}	MAC_{AP}	MAC_{host}	T_{rekey}
Bytes	20	8	6	6	8

Field	*keylen*	*defkey*	*k*[0]	*k*[1]	*k*[2]	*k*[3]
Bytes	1	1	13	13	13	13

M_2의 각 필드 중 M5에 존재하는 h, MAC_{host}, MAC_{AP}와 t_{AP}는 AP의 인증을 위한 것으로 t_{AP}는 2번 메시지의 전송시각이 저장된다. M_2의 나머지 필드들은 WEP 키 분배와 갱신을 위한 것으로 3.5절에서 자세히 다룰 것이다.

2번 인증 메시지를 이용한 AP의 인증 절차는 다음과 같이 호스트 및 사용자의 인증절차와 같은 방식으로 이루어진다. 여기서 AP의 인증절차는 WEP*의 AP 인증 방법과 같다.

(1) AP는 M_2의 각 필드를 표 4와 같이 채우고 인증된 호스트/사용자의 키 $K_{user,j}.k[i_j]$와 $k_{host,j}$를 합한 128 비트의 키를 이용하여 2번 인증 메시지의 암호화된 도전문 C_2를 다음과 같이 생성한다.

$$C_2 = E_{K_{user,j}.k[i_j], k_{host,j}}(M_2), *, *, \ldots, *$$

여기서 *는 도전문이 IEEE 802.11 표준에 맞추어 128 바이트가 되도록 추가되는 문자로 총 26 바이트가 추가된다.

(2) 생성된 암호화된 도전문 C_2는 2번 인증 메시지의 M_2에 담겨 해당 호스트에게 전달된다.

(3) 호스트에서는 2번 인증 메시지를 받으면 자신의 호스트 키 k_{host} 및 사용자 키 k_{user}를 이용해 2번 인증 메시지의 도전문 C를 복호화하여 원문 M을 얻는다. 즉, $M = E^{-1}_{k_{user}, k_{host}}(C)$. 여기서 메시지 M 내의 필드 F의 값은 F_M으로 표기한다.

(4) 호스트는 $H(M) = h^M$ 인지를 검증함으로 메시지의

무결성을 검사한다.

(5) $MAC_{host}{}^{M}$ = MAC_{host}, $MAC_{AP}{}^{M}$ = MAC_{AP} 인지와 $|t_{host}-t_{AP}{}^{M}| \le \Delta$ 가 만족하는지를 검증하여 재연(replay) 공격을 방지한다. 여기서 Δ는 AP와 호스트 사이의 허용 메시지 전파 시간의 최대값이다.

(6) 만일 하나라도 검증에 실패하면, 호스트는 인증 실패로 판단하고 인증 과정을 종료한다.

(7) AP의 인증에 성공하면 M의 $k[0]^{M}$, ..., $k[3]^{M}$ 값을 $keylen^{M}$에 저장된 키 길이를 참고하여 자신의 WEP 키 셋 K_{curr}에 저장하고, $K_{curr}.defkey$는 $defkey^{M}$ 값으로 설정한다. 또한, $T_{rekey}{}^{M}$의 값을 키 재지정 시간 상태 변수에 할당한다.

(8) 이후의 인증 과정은 IEEE 802.11의 표준 인증과정과 동일하게 3번과 4번 인증 메시지를 주고받음으로써 인증 과정을 종료한다. 단, 3번 인증 메시지 전송 시 도전문은 2번 인증 메시지의 도전문을 $k[defkey^{M}]^{M}$의 키로 RC4 암호화 하여 전송한다.

위 상호 인증 과정이 성공적으로 종료되면 호스트는 2번 인증 메시지로부터 저장된 각 값을 통해 자신의 WEP 키를 관리한다.

3.5 초기 WEP 키 설정 및 주기적 키 갱신

FR-WEP에서 AP는 현재 WEP 키 셋인 K_{curr}을 생성하고 전달해 주는 역할을 한다. 이때 AP에서는 현재 자신이 사용하고 있는 WEP 키를 기본 키로 지정하여 전달하게 되고 이동 호스트는 AP의 기본 키를 자신의 기본 키로 설정한 후에 AP와 동일하게 T_{rekey}에 맞추어서 키를 갱신한다. 이동 호스트에서 주어진 키 셋이 만료가 되면 인증 해제 후 다시 인증 과정을 수행하여 새로운 K_{curr}를 받아야 하는데 FR-WEP은 빠른 재인증을 제공하여 인증 해제 없이 키 셋의 만료 전에 AP로부터 새로운 키 셋을 제공받는다. 빠른 재인증 기법은 3.6절에서 자세히 다룰 것이다.

3.5.1 AP에서의 키 생성

AP는 현재 WEP 키 셋인 K_{curr} 생성을 위해 임의의 네 개의 WEP 키 w_0, w_1, w_2, w_3를 생성한다. 임의의 키를 생성하기 위해서 그림 1과 같이 AP에 비밀 마스터 키 z를 설정하고 이 키를 사용하는 키 기반 해쉬 함수 F_z를 사용한다. 새로운 키의 생성은 항상 키 셋 단위로 이루어지며 사용이 현재 키 셋 K_{curr}와 현재시간을 나타내는 시간 변수 T_{curr}를 이용하여 완전 난수에 가까운 키를 생성한다.

전원 연결 시 AP는 4개의 WEP 키 w_i, $0 \le i \le 3$를 생성하고 이를 현재 WEP 키 셋 K_{curr}에 할당한다. 즉, $K_{curr}.k[i] \leftarrow w_i$, $0 \le i \le 3$. 이 때 네 키 중 처음 키가 최초 기본 키가 된다. 즉, $K_{curr}.defkey \leftarrow 0$ 이다.

WEP*가 첫 키 셋 이 후의 키 생성을 위해 키를 하

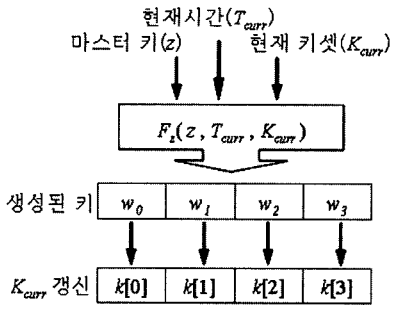

그림 1 AP의 키 셋 Kcurr 갱신 과정

나씩 순차적으로 생성하여 키 셋을 관리하는 것과는 달리 FR-WEP은 키 셋 전체의 일괄 갱신을 수행하여 빠른 재인증 시 사용한다. 이 때 AP는 호스트에서 전송되는 이전 키로 암호화된 메시지를 처리하기 위하여 세 번의 키 셋 만료 시간($3T_{rekey}$)마다 네 개의 키 중 가장 최근에 사용된 키를 제외한 나머지 세 개의 키 갱신만을 수행한다. 이를 통한 키 셋 배분 과정은 3.6절에서 자세히 설명된다. 키가 생성되고 관리되는 자세한 과정은 다음과 같다.

(1) 첫 번째 키 셋 만료 시간인 $4T_{rekey}$ 후에 첫 키 셋 생성과 마찬가지로 키 기반 해쉬 함수 F_z를 사용하여 새로운 키 w_i, $0 \le i \le 3$를 생성한다.

(2) 다음과 같이 생성된 키를 현재 WEP 키 셋 K_{curr}에 할당한다. 단 마지막 키는 할당하지 않는다. 즉, $n \leftarrow 3$; $K_{curr}.k[i] \leftarrow w_i$, $0 \le i \le 3$, $i \ne n$.

(3) 현재 키 셋 중 갱신된 세 개의 키가 만료되는 '이전 키셋 갱신 시간+$3T_{rekey}$' 후에 다음 키 w_i, $0 \le i \le 3$를 생성한다.

(4) 다음과 같이 생성된 키를 현재 WEP 키 셋 K_{curr}에 할당한다. 이 때 n 값을 갱신하고 n번째 키는 할당되지 않는다. 즉, $n \leftarrow (n-1) \bmod 4$ (단, $0 \le n \le 3$); $K_{curr}.k[i] \leftarrow w_i$, $0 \le i \le 3$, $i \ne n$.

(5) 이후의 계속적인 키 갱신을 위해 과정 (3)과 (4)를 반복한다.

3.5.2 AP와 호스트에서의 주기적 키 갱신

AP는 호스트를 인증하는 과정에서 2번 인증 메시지를 통해 키의 재지정 시간 T_{rekey}를 전송한다. AP와 호스트에는 키 갱신을 위해 키 재지정 시간을 관리하는 타이머가 존재하여 키의 할당과 함께 T_{rekey} 값이 이 타이머에 이 할당된다. 이 타이머가 만료되면 기본 키는 그 다음 키로 변경된다. 즉, $K_{curr}.defkey \leftarrow K_{curr}.(defkey+1 \bmod 4)$. 이 과정은 WEP*의 주기적 키 갱신 과정과 동일하다.

3.6 빠른 재 인증을 위한 키 셋 배분

이동 호스트의 키 셋이 만료가 되면 이동 호스트는

더 이상 AP로부터 전달되어지는 메시지를 해독할 수 없게 된다. 따라서 이동 호스트는 키 셋의 만료 전에 AP로부터 새로운 키 셋을 받아서 현재 키 셋을 새로운 키 셋으로 갱신시켜줘야 한다. 이때 WEP*와 같이 새로운 키 셋을 전송받기 위해 인증해제와 재 인증과정을 거칠 수 있다. 그러나 이 과정은 이동 호스트가 핸드오프 되었다가 다시 재접속될 때와 동일한 인증-결합 과정을 거치게 되고 재 인증과정에 따르는 시간 지연과 전송 중인 데이타가 손실될 위험이 있는 문제를 가지고 있다. FR-WEP은 이 문제를 해결하기 위해 인증 해제를 거치지 않고 새로운 인증 메시지를 사용하는 빠른 재 인증을 사용한다.

새로운 WEP 키 셋을 부여 받기 위해서는 호스트 및 사용자의 인증이 요구되지만 현재 AP와 통신을 수행하고 있는 호스트 및 사용자는 이미 인증을 받은 상태이므로 이에 대한 인증은 생략한다. 즉, 빠른 재 인증은 호스트로부터 AP에게 보내는 5번 인증 메시지 없이 현재 WEP 키 셋 K_{curr}이 만료되기 전에 AP에서 생성된 키 셋을 기존 2번 인증 메시지와 동일한 필드를 갖는 6번 인증 메시지를 이용해 각 이동 호스트에게 미리 분배하는 것이다. 빠른 재 인증을 위해 새롭게 정의한 6번 인증 메시지는 5번 인증 메시지와 같이 인증 처리 순서 번호를 6번으로 하여 구별한다. 다음은 AP에서 호스트로의 각 키 셋 분배와 호스트의 키 셋 갱신의 과정이다.

(1) AP에서 키 셋 갱신을 위해 생성한 키 셋 K_{curr}를 6번 인증 메시지의 키 셋 필드에 복사하여 전송한다. 즉, $k[i] \leftarrow K_{curr}.k[i]$, $0 \le i \le 3$.

(2) 호스트에서 6번 인증 메시지를 받으면 키 셋 필드의 키를 자신의 현재 키로 복사한다. 즉, $K_{curr}.k[i] \leftarrow k[i]$, $0 \le i \le 3$.

그림 2는 빠른 재 인증을 위한 각 호스트들의 키 셋 갱신의 과정을 보여주고 있다. 네 개의 숫자는 AP와 각 호스트에 사용하는 WEP 키의 일련번호를 나타내고 네모로 표시된 숫자는 현재 암호화에 사용하는 기본키를 나타낸다. 각 호스트는 시간 t_0, t_1, t_2 에 AP에 참여하여 인증을 거쳐 결합되었고, 이때 현재의 키 셋을 부여받게 된다. AP에서는 첫 번째 키 갱신 시간 $4T_{rekey}$에 새로운 키 셋을 생성하여 자신의 키 셋을 먼저 갱신한 후에 이를 각 호스트에게 전달한다. 이 때 마지막 4번 키는 갱신되지 않음을 유의한다. 호스트에서는 AP로부터 새로운 키 셋을 받은 직후 키 셋 갱신을 수행하게 된다. AP에서 마지막 4번 키를 갱신하지 않고 유지하도록 하는 이유는 각 호스트에서 현재 사용하고 있는 최근 키로 암호화하여 보내는 메시지의 해독을 위해서이다. 호스트 1과 호스트 2는 정상적으로 4번 키를 암호화에 사용한 후 5번 키를 사용할 수 있다. 동일한 방법으로 AP에서는 $7T_{rekey}$ 시간과, $10T_{rekey}$ 시간에 키 셋을 갱신하고 이를 각 호스트에게 분배한다.

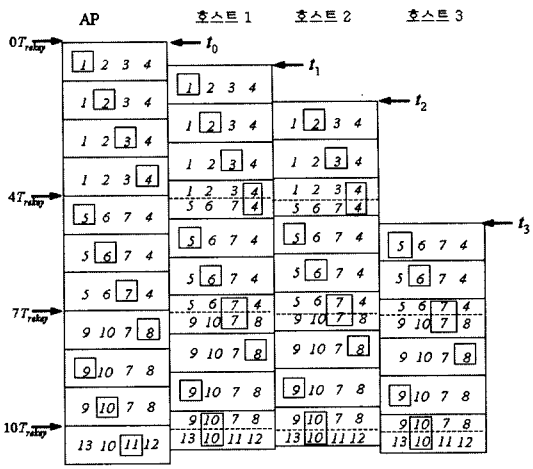

그림 2 빠른 재 인증을 위한 키 및 키 셋 갱신

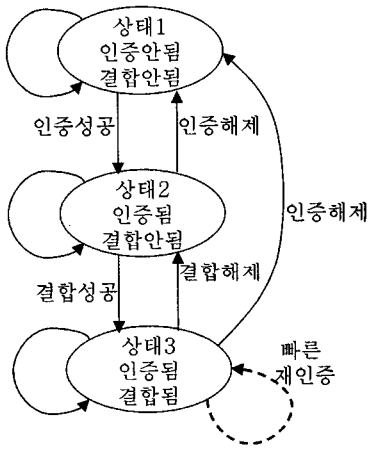

그림 3 수정된 IEEE 802.11 상태도

6번 인증 메시지를 통한 새로운 키 셋 K_{new}의 전송 방법 및 절차는 2번 인증 메시지에서의 키 셋 전송 방법 및 절차와 동일하다. 6번 인증 메시지의 도전문도 2번 인증 메시지의 M_2와 동일한 필드를 갖는 평문 M_6를 해당 호스트 키와 사용자 키로 RC4 암호화하여 생성된다. 단, 이 때 AP는 현재 결합된 각각의 호스트에게 해당 호스트 키와 기본 사용자 키로 암호화된 6번 인증 메시지를 개별적으로 전송한다.

각 이동 호스트에서는 6번 인증 메시지를 받으면 2번 인증 메시지에서와 같이 자신의 호스트 키와 기본 사용자 키로 복호화 하고, 새로운 키 셋을 현재 키 셋 K_{curr}에 복사한다. 그림 3은 빠른 재 인증 사용 시 변경되는 IEEE 802.11의 상태도를 보여 준다.

4. 평가

제안된 FR-WEP을 평가하기 위해서는 제안된 기법의 하드웨어 구현을 통한 실험이 가장 정확할 것이다. 먼저 연구용 AP 개발도구[15]를 이용하여 직접 구현하는 방법을 시도하였으나 FR-WEP을 구현하기에는 구현의 유연성이 부족하였다. 다음으로 OPNET[16]을 통한 모의실험을 시도하였으나 구현 중 다음과 같은 문제에 부딪히게 되었다. 먼저 OPNET은 이벤트 기반의 모의실험 도구로 실제 암호화된 메시지의 전송을 모의실험하는 것이 아니라 암호화되는 시점의 이벤트를 통해 암호화 과정에 대한 통계적 성능을 분석한다. 또한, FR-WEP에서 이루어지는 동기화나 키 갱신을 수행하기에는 기존모듈에 대한 방대한 수정이 이루어져야할 뿐 아니라 수정된 후에도 기존 모듈과의 호환성문제로 동기화에 대한 정확성에 대해 보장할 수 없게 된다. 따라서 본 논문에서는 무선 랜 보안 시스템을 이용한 실험을 토대로 FR-WEP의 실제적인 구현 시 고려되어지는 부분에 대한 논리적인 입증을 이용하여 제안한 FR-WEP의 보안성능을 평가하였다. 먼저 FR-WEP의 구현시 부가적으로 요구되는 공간 및 시간 비용, 기존 장비와의 호환성을 살펴봄으로써 그 정당성을 입증하고 FR-WEP의 보안 성능 및 인증 처리시간을 기존의 방법들과 비교한다.

4.1 FR-WEP의 정당성

FR-WEP의 정당성 평가에 있어서 중요하게 고려되어야할 것에는 다음과 같은 것들이 있다. 첫째, 사용자와 호스트의 인증을 위해 필요한 사용자 키와 호스트 키의 보관을 위한 메모리 공간 및 추가적으로 요구되는 관리 소프트웨어 문제와, 둘째, 제안한 FR-WEP을 동작시키는데 필요한 부가적인 작업으로 인한 시간 지연의 문제, 셋째 기존 장비들과의 이전호환성 문제이다.

4.1.1 공간 요구사항

FR-WEP 사용 시 사용자 및 호스트 키에 대한 보관을 위해 AP에서는 표 2와 같은 확장된 MAC 주소 테이블을 가져야 한다. 이때 요구되는 추가 메모리 요구량은 AP가 관리하는 호스트 수와 한 호스트의 최대 사용자 수가 각각 H와 N이고 사용자 및 호스트 키의 길이가 L 바이트일 때 다음과 같다.

$$H \times N \times L \text{ 바이트}$$

여기서 FR-WEP구현 시 AP에서의 메모리 요구량은 그리 크지 않음을 알 수 있다. 각 호스트에서는 해당 호스트를 이용하는 최대 사용자 수만큼의 메모리 공간만이 추가적으로 요구되므로 AP에 비해 상대적으로 적은 메모리 공간으로 구현이 가능하다. 한편 각 호스트에서는 3.3절에서 설명한 사용자 세션 소프트웨어가 추가로 운용되어져야하는데 이는 해당 호스트 운영체제에서 장치 드라이버를 이용한 응용 프로그램의 구현을 통해 가능하기 때문에 FR-WEP 구현 시 장치 내에 추가적인 메모리 공간을 요구하지 않는다.

4.1.2 시간 요구사항

FR-WEP에서는 호스트 및 사용자와 AP 사이의 상호인증을 위해 기존 WEP에서의 1번 인증메시지 대신 5번 인증메시지를 사용한다. 이때 5번 메시지의 도전문 영역(M_5)에는 사용자 키 k_{user}와 호스트 키 k_{host}를 합한 128비트의 키를 갖는 암호문 $C_5 = E_{k_{user}, k_{host}}(M_5)$가 들어간다. 여기서 5번 메시지 생성시간은 기존 WEP의 1번 인증 메시지 생성시간에 추가로 암호문 C_5를 생성하기 위한 k_{host}와 k_{host}의 메모리 탐색시간과 이 키를 이용한 암호화 시간이 요구된다. 또한 AP에서는 5번 인증메시지를 받고 AP의 MAC 주소 테이블에 등록된 호스트의 $k_{host,j}$와 $k_{host,j}.k[i]$를 찾는데 소요되는 메모리 탐색시간과 이 키를 이용한 5번 인증 메시지의 도전문 C에 대한 복호화시간 및 복호화된 메시지 M 내의 필드의 값을 비교하는 메시지의 검증 시간이 추가로 요구된다. 이때 AP에서 추가로 소요되는 시간을 $t_{AP(5)}$라고 하자.

5번 인증메시지를 통해 호스트 및 사용자 인증에 성공한 후 AP인증을 위해 AP에서는 2번 인증 메시지를 생성하여 호스트에 전송하게 되는데 이 경우에도 5번 인증메시지와 비슷한 추가 시간이 요구된다. 이때 호스트에서 추가로 소요되는 시간을 $t_{host(2)}$라고 하자. 이후 3번과 4번 메시지의 전송은 기존 WEP 방법과 동일하게 수행된다.

이 같은 고찰을 통해 기존 WEP과 제안된 FR-WEP의 인증에 소요되는 시간의 차는 $t_{AP(5)}+t_{host(2)}$ 임을 알 수 있다. 한편 3.4절에서 설명한 바와 같이 호스트와 AP에서는 메시지 인증 필드를 이용해 상호 시간차, 즉 각각 $|t_{host}-t_{AP}{}^{M}| \le \Delta$와 $|t_{AP}-t_{host}{}^{M}| \le \Delta$를 검증하게 된다. 따라서 FR-WEP 시스템의 처리시간은 호스트에서는 $\max(t_{AP(5)})+T_{prop} < \Delta$, AP에서는 $\max(t_{host(2)})+T_{prop} < \Delta$를 보장할 수 있어야 한다. 그런데 $\max(t_{AP(5)})$와 $\max(t_{host(2)})$는 단지 128 비트의 키로 암호화를 수행하는 과정이므로 기존 WEP의 3번 인증메시지에서 RC4 암호화 처리시간과 비슷하다고 할 수 있다. 따라서 FR-WEP 사용 시 $\max(t_{AP(5)})+T_{prop} < \Delta$와 $\max(t_{host(2)})+T_{prop} < \Delta$를 보장할 수 있도록 Δ값을 선택한다면 운용에 문제가 없게 된다.

4.1.3 IEEE 802.11 장비와의 호환성

FR-WEP에서는 상호 인증 시에 1번 인증 메시지 대신 5번 인증 메시지를 사용하며 빠른 재 인증을 위해서 6번 인증 메시지를 사용한다. 다음 표 5는 FR-WEP의 상호 인증 절차에 사용되는 메시지이다.

표 5 FR-WEP에서의 인증 메시지

순서번호	전송방향	Payload 내용	WEP	메시지번호
1 :	host → AP :	N_5	사용	5
2 :	AP → host :	N_2	사용	2
3 :	host → AP :	WEP[N_2]	사용	3
4 :	AP → host :	successful/fail	사용안함	4
5 :	AP → host :	WEP[N_6]	사용	6
1':	host → AP :	없음	사용안함	1

FR-WEP은 1번 인증 메시지 대신 5번 인증 메시지를 사용하지만 IEEE 802.11 장비와의 호환성을 위해 1번 인증 메시지도 함께 사용한다. FR-WEP을 사용하는 호스트 A가 기존의 IEEE 802.11 표준 AP B에게 인증되어지는 절차는 다음과 같다.

(1) A는 인증 과정을 시작하기 위하여 5번 인증 메시지를 B에게 전달한다.
(2) B가 FR-WEP을 지원한다면 A의 인증에 성공한 경우 인증 메시지 2를 보내주게 된다.
(3) 만일 B로부터 5번 인증 메시지에 대한 응답이 없을 경우 미리 정한 재전송 시간 후에 다시 5번 인증 메시지를 보낸다.
(4) 미리 정한 최대 재전송 횟수 동안 5번 인증 메시지를 보낸 이후에도 B로부터 아무런 응답이 없으면 A는 B를 IEEE 802.11 표준 AP로 판단하고 1번 인증 메시지를 보내어 IEEE 802.11 표준 인증 절차를 통해 인증과정을 거치게 된다.

반대로 IEEE 802.11 표준 만을 지원하는 호스트 A가 FR-WEP을 지원하는 AP B에게 인증되어질 경우, A는 1번 인증 메시지를 보내게 되고 B는 A를 IEEE 802.11 표준 만을 지원하는 호스트라고 판단하여 IEEE 802.11 표준 인증 절차를 통해 인증과정을 거치게 된다. 단 이 때 A는 현재 WEP 키를 알고 있어야 인증이 가능하며 WEP 키 갱신 때마다 수동으로 WEP 키를 받아 설정하여 재인증 받아야 한다.

4.2 FR-WEP의 성능비교

본 절에서는 FR-WEP의 보안성능 비교 및 상호인증과 키 갱신에 소요되는 인증처리 시간에 대한 비교와 기존방법들과의 비교를 통해 FR-WEP을 평가한다.

4.2.1 FR-WEP의 보안성능 비교

기존 WEP의 알려진 보안 취약성 문제들을 FR-WEP에서 어떻게 해결하였는지 살펴보자. 먼저, WEP에서는 RC4 키스트림 암호화의 문제로 인해 키스트림 재생공격을 가능하였다. 이러한 키 스트림 재생공격은 동일한 키와 IV를 사용한 서로 다른 평문에서 가능하게 된다[7]. 이때 동일한 키와 IV를 가지는 메시지는 다음과 같이 약 3시간 만에 획득 가능하게 된다. (단, 패킷크기 : 900바이트, 전송속도 : 11Mbps, IV 길이 2^{24}비트)

$$900 \times 8 \times 2^{24} / 11\times10^{6} \approx 10^{4}\text{초} \approx 3\text{시간}$$

그러나 FR-WEP에서는 키 갱신 시간인 T_{rekey}에 따라 동적 키 갱신을 통해 새로운 키를 가지게 된다. 이 때 동일한 키와 IV가 사용될 가능성은 T_{rekey} 시간의 설정에 따라 달라진다. 따라서 T_{rekey}를 3시간 보다 작게 설정해 주면 이러한 문제를 해결할 수 있게 된다.

또한, FR-WEP은 인증의 문제에도 효과적으로 대응할 수 있다. 기존의 호스트에 대한 일방적 인증이 아닌 AP와 호스트 간의 상호 인증을 수행해 줌으로써 위장 AP나 호스트에 의한 위협을 최소화하였다. 그리고 기존의 MAC 기반 접근 제어 기법의 보완 취약점을 호스트 키 뿐만 아니라 사용자 키를 도입하여 해결하고 있다. 이에 따라 공격자는 호스트 키와 사용자 키를 모두 알아내야만 전송 데이타를 확인할 수 있게 된다. 뿐만 아니라 3.3절에서 살펴본 바와 같이 호스트 키와 사용자 키에 대한 관리를 통해 호스트 폐지의 문제에도 효과적으로 대응할 수 있다.

마지막으로, FR-WEP은 상호 인증시 보내어지는 메시지에 보안에 취약한 CRC 대신 암호화 해쉬 함수 SHA-1를 사용함으로써 데이타 무결성의 측면에서도 보안 성능의 향상을 꾀하고 있다.

4.2.2 인증처리 시간비교

FR-WEP의 인증처리 시간을 평가하기 위해 상호인증과 키 갱신 소요 시간에 대해 기존의 방법과 비교를 수행한다.

먼저 기존 무선랜에서 도입하여 사용하고 있는 802.1X 인증 시스템과 FR-WEP과의 상호인증 시간을 비교한다. 802.1X 인증 시스템에서의 인증 시간은 서로 다른 인증 유형을 고려하여 다음과 같은 식으로 나타낼 수 있다.

$$T_{Auth(802.1X)} \approx T_{min(AAA)} + \triangle T_{EAP}$$

여기서 $T_{min(AAA)}$는 호스트와 외부 인증서버 간의 EAP 인증 메시지 왕복을 통한 최소 인증시간을 나타낸다. $\triangle T_{EAP}(>0)$는 TLS나 PEAP와 같은 EAP 인증 유형에 따라 인증서 교환에 추가로 소요되는 시간을 의미한다. 반면 FR-WEP에서의 상호 인증시간은 4.1.2절에서 살펴보았던 것처럼 다음과 같이 나타낼 수 있다.

$$T_{Auth(FR\text{-}WEP)} \approx T_{Auth(WEP)} + t_{AP}(5) + t_{host}(2)$$

여기서 $T_{Auth(WEP)}$은 AP와 호스트 사이의 인증메시지 왕복에 드는 시간으로 일반적으로 $T_{min(AAA)}$보다 훨씬 작은 값을 갖는다[17]. 또한 $t_{AP(5)}$와 $t_{host(2)}$는 위 시간에 비해 무시할 수 있는 정도이므로 FR-WEP의 상호 인증시간이 802.1X의 상호 인증시간보다 훨씬 작다고 할 수 있다.

다음으로 FR-WEP과 WEP*와의 동적 키 갱신에 소

요되는 시간에 대해 비교한다. WEP*에서 각 호스트는 T_{rekey}에 따라 키 셋 만료 전까지 세 번의 키 갱신을 수행한다. 키 셋 만료 시 WEP*는 인증 해제를 수행하고 다시 인증 및 결합 과정을 통해 새로운 키셋을 AP로부터 다시 할당받게 되는데, 이 시간동안에 호스트는 데이타를 받을 수 없게 된다.

반면 FR-WEP에서는 키 셋 만료시간인 $4T_{rekey}$가 지나기 전에 6번 인증메시지를 통해 새로운 키 셋 K_{new}를 보내주게 된다. 여기서 $t_{host(6)}$를 6번 인증메시지를 통한 새로운 키 셋 분배 시간이라 할 때 호스트에서 T_{rekey} 값이 $T_{rekey}>t_{host(6)}$를 만족하는 시점에서 AP에서 키 셋을 전송하면 빠른 재인증은 성공적으로 수행될 수 있다. 이 경우 FR-WEP에서는 WEP*와 같은 키 셋 갱신에 소요되는 지연과 그에 따른 데이타의 손실이 발생하지 않는다.

한편, 현재 무선랜의 강화된 보안 구조 표준인 802.11i에서는 802.1X를 통한 다양한 인증 메커니즘을 포함하며 강력한 암호화 메커니즘으로 TKIP이나 AES를 사용하도록 정의하고 있고 동적 키 갱신을 제공하고 있다. 여기서 키 생성 및 재분배에 대한 시점은 IV의 순차 카운트가 한도에 도달할 때 보안 강도를 유지할 수 있도록 결정된다. 이러한 802.11i 표준은 무선랜 보안을 위한 강력하고 효과적인 시스템이지만, 새로운 보안 시스템을 도입하도록 함으로 기존 시스템의 교체가 이루어져야 한다. 이러한 점에서 FR-WEP은 상호인증과 동적 키 분배를 제공하면서 기존 시스템과의 호환성을 가지는 간단하고 효과적인 인증 시스템이라 할 수 있다.

4.2.3 기존방법들과의 비교

FR-WEP은 기존 무선랜의 보안 시스템을 강화를 위해 상호인증 및 사용자인증을 사용하고 시스템의 간소화와 재 인증 시간 단축을 위해 간소화된 키 관리와 빠른 재 인증을 사용한다. 표 6은 기존의 상호 인증을 지원하는 RADIUS 인증 시스템 및 WEP* 기법과 키 관리 방법 및 재 인증 과정을 비교하여 정리한 것이다.

RADIUS 서버를 통한 상호인증 및 사용자 인증을 제공할 수 있다는 점은 무선랜 시스템의 보안 강화에 중요한 요소이지만 장비의 추가 도입으로 인해 비용과 시스템 규모가 크게 증가하는 부담이 있다. 한편 좀 더 간소화된 방식으로 인증을 제공해주는 WEP*는 상호 인증 및 사용자 인증을 지원하지 않으며 기존의 재인증 과정을 그대로 사용한다. 본 논문에서 제안한 FR-WEP은 RADIUS 서버와 같은 별도 인증시스템을 추가로 도입하지 않고도 상호인증과 사용자 인증 및 빠른 재 인증을 지원하므로 중·소규모의 기관에 도입하여 운영하기에 적합한 무선랜 보안 시스템으로 판단된다.

표 6 FR-WEP과 기존 시스템과의 비교

기능	RADIUS + WEP	WEP*	FR-WEP
상호인증	지원	미지원(단방향)	지원
사용자 인증	인증방식에 따라 다름	미지원	지원
재인증	인증 해재후 재인증	인증 해재후 재인증	빠른재인증
키 관리	RADIUS	AP	AP

5. 결 론

바야흐로 무선 랜은 그 편리성과 고속 데이타 전송 속도로 인해 빠르게 그 영역을 넓혀가고 있다. 그러나 IEEE 802.11 무선랜은 많은 보안취약점으로 인해 이러한 성장에 장애물이 되고 있다. 이에 따라 현재 IEEE 802.11i이라는 강력한 보안 성능을 가진 새 표준안이 제정되고 있지만, 이를 위해서는 시스템의 교체와 부대 장치의 설치가 요구되고 있다.

본 논문에서는 이러한 환경에서 기존의 무선 랜 장비들을 최대한 활용하고 이전 호환성을 제공하면서 현재 문제가 되는 보안 취약점을 보완한 간소화된 키 관리 기법인 FR-WEP을 제안하였다. FR-WEP은 호스트 키와 사용자 키를 도입하여 AP와 호스트 및 사용자 간의 간소화된 상호 인증을 제공하고, 사용자의 다양한 상황 변동에 따른 키 관리를 통해 사용자 폐지 문제에 보다 효과적으로 대응할 수 있다. 또한, 주기적인 키 갱신을 통해 RC4 암호화 공격이 성공하지 못하도록 하며 나아가 빠른 재 인증을 통해 인증 해제가 되지 않고 계속 새로운 키로 키 갱신을 할 수 있는 메커니즘을 제공한다. 따라서 보안이 필요한 소규모의 학교 또는 회사에서 무선 랜의 도입을 원할 경우나 기존에 설치 무선 랜 환경에 대해 보안을 강화해야 할 경우에 802.11i를 만족하는 시스템을 새로 도입하기가 여의치 않을 때 FR-WEP은 좋은 대안이 될 것이다.

참 고 문 헌

[1] ANSI/IEEE standard 802.11, "Wireless LAN medium access control(MAC) and physical layer(PHY) specification," 1999.

[2] R. L. Rivest, "The RC4 encryption algorithm," RSA Data Security Inc., (proprietary), 1992.

[3] W.A Arbaugh, "Your 802.11 Wireless Network has No Clothes," In Proc. of *IEEE International Conference on Wireless LAN's and Home Networks*, 2001.

[4] S. Fluhrer et al., "Weaknesses in the key scheduling algorithm of RC4," *LNCS 2259*. Springer-Verlag, 2001.

[5] N Borisov et al., "Intercepting mobile communications: The insecurity of 802.11," In *Proc. 7th ACM*

Conference on Mobile Computing and Networking (MOBICOM'01), Rome, Italy, 2001..
[6] C. Rigney, "Remote Authentication Dial In User Service(RADIUS)," IETF RFC 2865, 2000.
[7] J. Daemen and V. Rijmen, "Advanced Encryption Standard," National Institute of Standards and Technology, NIST FIPS PUB 197, U.S. Department of Commerce, 2001.
[8] The Wi-Fi alliance, "Wi-Fi Protected Access," 2002.
[9] A. Wool, "Lightweight Key Management for IEEE 802.11 Wireless LANs With Key Refresh and Host Revocation," IEEE 802.11-02/411r0, 2002.
[10] N. Shankar et al., "A Transparent Key Management Scheme for Wireless LANs Using DHCP," HP Labs Technical Report HPL-2001-227, 2001.
[11] IEEE Society, IEEE Standard 802.11i/D3.0, "Specification for Enhanced Security," 2002.
[12] Joseph et al., Development of a Transmission Error Model and an Error Control Model," Technical Report, Georgia Institute of Technology, 1975.
[13] N. Ferguson, "Michael: an improved MIC for 802.11 WEP," Document number IEEE 802.11-02/020r0, 2002.
[14] IETF, "US Secure Hash Algorithm 1 (SHA-1)," RFC 3174, 2001.
[15] Intersil Cooperation, ISL36356A AP Development Kit, 2003.
[16] OPNET Technologies Inc., OPNET Modeler V.10.0, 2004.
[17] B. Aboba, "Fast Handoff Issues," doc.:IEEE802.11-03/155r0, 2002.

이 재 형

1993년~2000년 금오공과대학교 컴퓨터공학부(공학사). 2000년~2002년 금오공과대학교 컴퓨터공학과(공학석사). 2002년~현재 금오공과대학교 컴퓨터공학과 박사과정. 관심분야는 무선 네트워크 및 보안, 차세대 통신망

김 태 형

1988년~1992년 연세대학교 전자공학과(공학사). 1992년~연세대학교 전기전자공학과(공학석사). 1996년~2001년 연세대학교 전기전자공학과(공학박사). 2001년~2002년 University of Ottawa(Post-doc.). 2002년~현재 금오공과대학교 컴퓨터공학부 교수. 관심분야는 통신 프로토콜 공학, 무선 네트워크 및 보안, 차세대 통신망

한 규 필

1987년~1993년 경북대학교 전자공학과(공학사). 1993년~1995년 경북대학교 전자공학과(공학석사). 1995년~1999년 경북대학교 전자공학과(공학박사). 2000년~현재 금오공과대학교 컴퓨터공학부 교수. 관심분야는 영상처리, 컴퓨터비전

김 영 학

1980년~1984년 금오공과대학교 전자 공학과(공학사). 1987년~1989년 서강대학교 전자계산학과(공학석사). 1993년~1997년 서강대학교 전자계산학과(공학박사). 1989년~1997년 해군사관학교 전산과학과 교수. 1998년~1999년 여수대학교 멀티미디어학부 교수. 1999년~현재 금오공과대학교 컴퓨터공학부 교수. 관심분야는 병렬 알고리즘, 분산 및 병렬처리