혼합모드 무선랜에서의 동적 키 관리 방식 연구

정회원 강 유 성*, 오 경 희**, 정 병 호***, 정 교 일****, 양 대 헌*****

A Study on Dynamic Key Management in Mixed-Mode Wireless LAN

You Sung Kang*, KyungHee Oh**, ByungHo Chung***, Kyo-il Chung****,
DaeHun Nyang***** *Regular Members*

요 약

무선랜 시스템이 초고속 무선인터넷의 인프라로 자리 잡으면서 무선랜 보안에 관한 관심이 급속히 커가고 있다. 기존의 IEEE 802.11 기반의 무선랜 보안 요소라 할 수 있는 WEP 알고리즘의 취약점을 극복하기 위한 노력의 일환으로 Wi-Fi에서는 WPA 보안규격을 발표하였다. WEP 알고리즘을 사용하는 단말기와 WPA 지원 단말기가 동시에 존재하는 혼합모드 무선랜 환경에서는 각 단말기별 unicast용 pairwise 키 관리와 전체 단말기에 대한 broadcast용 group 키 관리가 훨씬 복잡하다. 본 논문에서는 pairwise 키와 group 키 관리를 위한 WPA authenticator 키 관리 상태머신의 취약점을 분석하고, 분석된 각각의 취약점을 극복할 수 있는 대응방안을 제시한다. 또한, 제시된 해결방안이 적용된 WPA authenticator 키 관리 상태머신의 재구성된 형태를 보인다. 본 논문에서 재구성한 키 관리 방식은 혼합모드 무선랜 환경에서 다양한 접속 방식의 단말기들에 대해서 group 키 교환과 group 키 업데이트 수행을 효과적으로 처리할 수 있는 토대를 제공한다.

Key Words : mixed-mode wireless LAN; key management; wireless LAN security; WPA.

ABSTRACT

The interest in wireless LAN security is on the increase owing to a role of high-speed wireless Internet infrastructure of wireless LAN. Wi-Fi has released WPA standard in order to overcome drawbacks of WEP algorithm that is security element of current IEEE 802.11-based wireless LAN system. Pairwise key management and group key management in a mixed-mode which supports both terminals running WPA and terminals running original WEP security are very complicate. In this paper, we analyze flaws in WPA authenticator key management state machine for key distribution and propose the countermeasures to overcome the analyzed problems. Additionally, WPA authenticator key management state machine to which the solutions are applied is described. The reconstructed WPA authenticator key management state machine helps the AP perform efficiently group key exchange and group key update in the mixed-mode.

Ⅰ. 서 론

무선랜 기술은 초고속 무선인터넷 환경의 인프라를 구축하기 위한 매력적인 기술로 인식되고 있다. 최근 들어 선이 없는 자유로운 통신환경을 추구하면서 무선랜 시스템의 구축이 기업체 내부망을 비롯해 공중망 서비스를 위한 형태로 활발히 전개되고 있다. 대부분의 무선랜 제품은 Wi-Fi 인증된

* 한국전자통신연구원 정보보호연구단(youskang@etri.re.kr), ** 한국전자통신연구원 정보보호연구단(khoh@etri.re.kr),
*** 한국전자통신연구원 정보보호연구단(cbh@etri.re.kr), **** 한국전자통신연구원 정보보호연구단(kyoil@etri.re.kr),
***** 인하대학교 정보통신대학원(nyang@inha.ac.kr),
논문번호 : 030422-0926, 접수일자 : 2003년 9월 23일

IEEE 802.11 규격에 기반한 제품이 주류를 이루고 있다[1]. 현재 IEEE 802.11b 규격 제품은 2.4GHz 대역에서 최대 11Mbps 전송속도의 서비스를 제공하고 있으며, 최근 출시되고 있는 5GHz 대역의 IEEE 802.11a 규격 제품과 2.4GHz 대역의 IEEE 802.11g 규격 제품은 최대 54Mbps 전송속도를 지원한다. 그러나 이러한 전송속도 향상에도 불구하고 무선구간을 보호하기 위한 암호 알고리즘이나 사용자 인증 등의 보안 서비스 제공을 위한 기능은 여전히 기존의 WEP(Wired Equivalent Privacy) 알고리즘에 의존하고 있는 실정이다. WEP 알고리즘은 IV(Initialization Vector)의 평문 전송, 키 스트림의 단순성, 고정 키 사용에 따른 RC4 키 업데이트 부재 등의 취약점으로 인해 WEP 키 길이에 상관없이 보안 서비스 제공에 적합하지 않을뿐더러 공격자에 의해 WEP 암호문은 평문으로 유도될 수 있다고 판명되었다[2][3].

이에 따라 무선랜 시스템의 보안성을 높이기 위한 노력의 결과로써 IEEE 802.11 TGi(Task Group i)에서는 RSN(Robust Security Network)으로 명명한 새로운 보안구조를 제시하여 IEEE 802.1X 사용자 인증 및 4-way handshake 키 관리 등으로 접근제어를 강화하고, TKIP(Temporal Key Integrity Protocol), CCMP 알고리즘의 사용으로 무선구간 데이터 기밀성 강화를 추구하고 있다[4]. 또한 Wi-Fi에서는 IEEE 802.11i Draft 3.0 문서의 내용을 중심으로 WPA(Wi-Fi Protected Access) 규격을 제정, 발표함으로써 무선랜 보안기술의 활용을 적극적으로 장려하고 있다[5]. Wi-Fi는 IEEE 802.11 규격에 기반한 무선랜 제품의 상호호환성을 인증해 주는 무선랜 산업체의 비영리 연합으로써 사실상의 상용화 제품 표준을 주도하고 있으며, IEEE 802.11b 규격 인증, IEEE 802.11a 규격 인증에 이어 WPA 인증을 위한 테스트베드를 구축해 놓고 있다.

현재의 모든 액세스포인트와 무선랜 카드가 전체적으로 WPA 제품으로 교체된다면 그동안 무선랜 시스템이 취약했던 보안 문제를 해결할 수 있을 것으로 기대된다. 그러나 일부 액세스포인트가 WPA 제품으로 교체되어 운용된다 하더라도 무선랜 단말기에서는 기존의 WEP 방식 무선랜 카드와 새로운 WPA 방식의 무선랜 카드가 다양하게 공존하는 기간이 상당기간 지속될 것이다.

이렇듯, 기존의 WEP 방식 단말기와 새로운 WPA 지원 단말기가 공존하는 상황을 혼합모드 무선랜 환경으로 정의할 수 있다[6]. 혼합모드 무선랜 환경에서는 다수의 무선랜 단말기들이 하나의 액세스포인트에 접속을 시도하는 경우에 액세스포인트는 각각의 단말기에 대해 인증을 실시하고, 키 교환 및 암호 알고리즘의 적용을 수행해야 한다. 이 때의 키 교환 및 암호 알고리즘의 적용은 pairwise 키와 group 키를 각각 고려해야 하며, 특히 group 키는 하나의 액세스포인트가 다수의 무선랜 단말기에게 동시에 데이터 전송을 시도하는 broadcast 암복호용 키이기 때문에 키 관리에 있어서 키 교환이 요구되는 단말기의 수와 키 교환 완료 여부 및 사용되는 암호 알고리즘에 대한 정보를 관리해야 하는 복잡성이 존재한다.

본 논문에서는 혼합모드 무선랜 환경의 키 관리를 책임지는 IEEE 802.1X authenticator 키 전송 상태머신과 WPA authenticator 키 관리 상태머신을 분석하며, 분석 결과로써 현재의 WPA authenticator 키 관리 상태머신이 group 키 분배와 설정에 취약하다는 것을 밝힌다. 또한 분석된 취약점을 극복할 수 있는 해결책을 제시하고, 재구성된 WPA authenticator 키 관리 상태머신을 보인다.

본 논문의 구성은 다음과 같다. II장에서는 혼합모드 무선랜 시스템에서 공존할 수 있는 동적 키 교환 방식인 IEEE 802.1X 키 전송 방식과 IEEE 802.11i 키 교환 방식을 설명하며, 더불어 키 교환보다 선행되어야 하는 사용자 인증 및 PMK 획득 절차에 대해 설명한다. III장에서 본 논문이 분석하고 해결책을 제시하는 혼합모드 무선랜에서의 키 관리 방식을 상세히 묘사한다. 본 논문에서 고려하는 혼합모드 무선랜 시스템에 대한 예시와 키 생성 및 설정에 관하여 설명하고, IEEE 802.1X 키 전송 상태머신을 보인다. 그리고 WPA 키 관리 상태머신의 취약점 분석과 해결책 제시를 상세하게 설명한다. 끝으로 IV장에서 본 논문의 결론을 맺는다.

II. 동적 키 교환

무선랜 시스템에서의 동적인 키 교환 방식은 크게 두 가지 방식으로 구분할 수 있다. 첫 번째 방식은 IEEE 802.1X authenticator 키 전송 상태머신([7]의 8.5.5절 Authenticator Key Transmission State Machine 참조)을 사용하는 IEEE 802.1X 키 전송 방식이며, 또 다른 하나는 IEEE 802.11i authenticator 키 관리 상태머신([4]의 8.5.6절 Authenticator Key Management State Machine 참

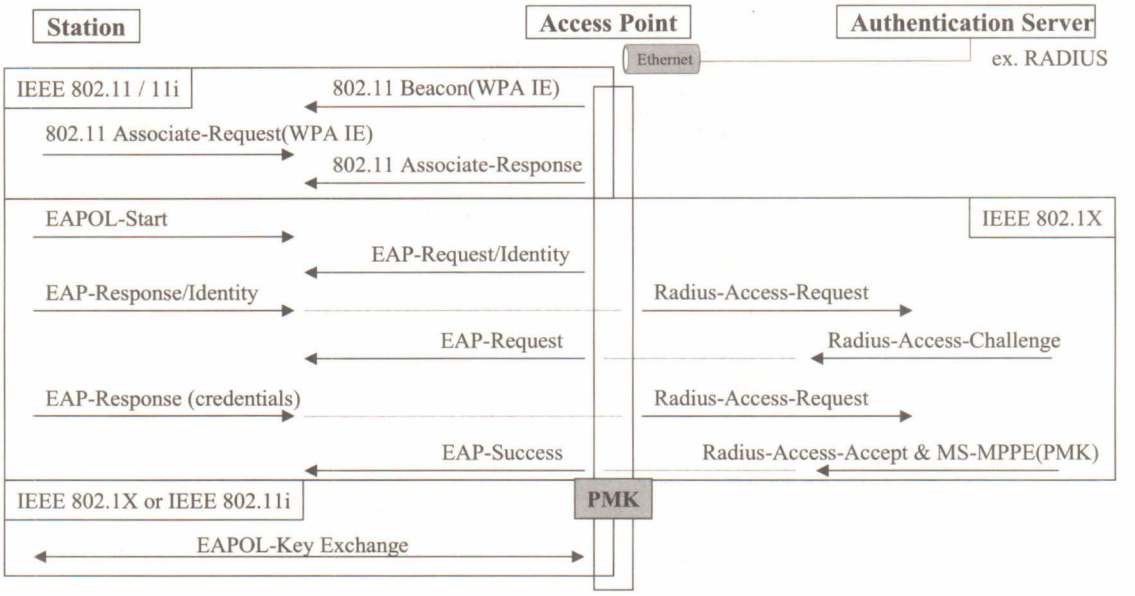


그림 1. EAP 방식의 IEEE 802.1X 인증에 기반한 PMK 획득 흐름도
Figure 1. PMK acquisition using IEEE 802.1X with EAP authentication

조)을 사용하는 IEEE 802.11i 키 교환 방식이다. 후자인 IEEE 802.11i 키 교환 방식은 WPA 규격에서 그대로 차용하고 있으므로 본 논문에서는 IEEE 802.11i 규격과 WPA 규격을 동일하게 취급한다.

1. PMK 획득

동적인 키 교환을 수행하는 주체는 무선랜 단말기와 액세스포인트이다. 따라서 액세스포인트와 무선랜 단말기는 동적 키 교환 프레임의 안정성을 보장하기 위한 마스터 세션 키를 공유해야 한다. 무선랜 시스템에서는 키 교환 당사자 사이의 마스터 세션 키를 PMK(Pairwise Master Key)라 하며, 키 교환은 PMK 획득 이후에 진행되어야 한다. PMK를 획득하는 방식은 두 가지 방법이 있는데, 하나는 인증서버로부터 받아오는 방법이고, 또 다른 하나는 PSK(Pre-Shared Key)로부터 유추하는 방법이다. 그림 1은 인증서버로부터 PMK를 받아오는 절차이다.

인증서버로부터 PMK를 받아오기 위해서는 우선 인증서버가 무선랜 단말기에 대한 인증 및 마스터 세션 키 확보를 위한 인증 프로토콜을 수행해야 한다. 인증 프로토콜은 IEEE 802.1X 규격에서 정의하고 있으며, 인증 메시지를 전달하는 프레임은 EAP(Extensible Authentication Protocol) 패킷이다[7][8]. 또한 대표적인 인증서버는 RADIUS(Remote Authentication Dial In User Service) 서버이며, 인증서버가 무선랜 단말기와 상호 인증 및 마스터 세션 키 생성을 위해서 사용하는 EAP 방식으로는 EAP-TLS(EAP-Transport Layer Security) 방식이 널리 알려진 방식이다[9][10].

그림 1에서 보이듯이 액세스포인트는 무선랜 단말기의 접속 이후에, 단말기와 인증서버 사이의 IEEE 802.1X 인증 메시지를 중계하고, 최종적인 인증 결과를 인증서버로부터 받음(Radius-Access-Accept)과 동시에 PMK도 받아온다(MS-MPPE)[11].

PMK를 획득한 액세스포인트는 단말기와 협상된 메커니즘에 따라 IEEE 802.1X 키 전송 또는 IEEE 802.11i 키 교환을 수행하는데, 본 논문에서는 WEP 암호 알고리즘을 사용하는 단말기에게는 IEEE 802.1X 키 전송을 수행하고, WPA 규격에서 정의한 TKIP 암호 알고리즘을 사용하는 단말기에게는 IEEE 802.11i 키 교환을 수행하는 혼합모드 무선랜 환경을 가정한다.

2. IEEE 802.1X 키 전송

IEEE 802.1X 규격에 따르면, 키 전송을 위한 상태머신인 IEEE 802.1X authenticator 키 전송 상태머신을 구현상의 선택항목으로 규정하고 있다[7]. IEEE 802.1X authenticator 키 전송 상태머신은 III장 그림 5에서 상세히 묘사하고 있으며, 그림 2는 IEEE 802.1X 키 전송 절차를 나타내는 흐름도이다.

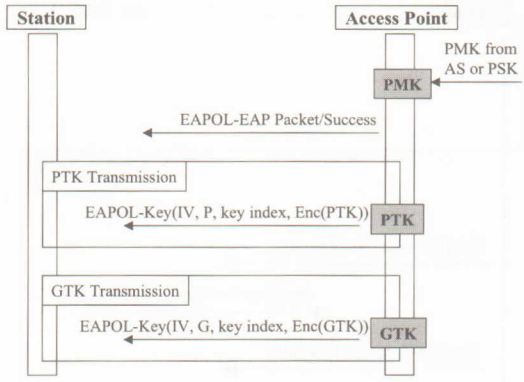


그림 2. IEEE 802.1X 키 전송 흐름도
Figure 2. IEEE 802.1X key transmission procedure

그림 2에서 보이듯이 액세스포인트는 PMK 획득 이후에 단말기에게 unicast용 pairwise 키가 포함된 PTK(Pairwise Transient Key)를 전송한다. 키 전송에서 사용되는 프레임은 EAPOL(EAP Over LAN)-Key 프레임이며, PTK는 IV와 PMK의 연접 스트링을 키로 하여 암호화된다. PTK 전송 직후에 곧바로 broadcast용 group 키가 포함된 GTK(Group Transient Key)를 전송할 수 있다. IEEE 802.1X 규격에서는 무선랜 단말기가 EAPOL-Key 프레임을 수신한 이후에 PTK 또는 GTK를 정상적으로 복원했는지 여부를 확인할 수 있는 ACK 기능에 대한 언급이 없다. 그러므로 본 논문에서는 혼합모드 무선랜 환경에서 IEEE 802.1X 키 전송 방식을 사용하여 WEP 암호 알고리즘을 구동하는 단말기에 대해서는 PTK와 GTK 전송이 항상 정상적으로 수행되었다고 가정한다.

3. IEEE 802.11i 키 교환

IEEE 802.11i 규격은 PTK 교환을 위한 4-way handshake 절차와 GTK 교환을 위한 group key handshake 절차를 정의하고 있다[4]. 그림 3은 WPA 규격이 준용하고 있는 IEEE 802.11i 키 교환 흐름도이며, 이러한 키 교환 절차를 수행하는 상태머신인 WPA authenticator 키 관리 상태머신은 III장의 그림 6에서 묘사하고 있다.

액세스포인트에서 PMK 획득 이후에 진행하는 4-way handshake의 첫 번째 EAPOL-Key 프레임은 액세스포인트에서 생성한 난수인 ANonce (Authenticator Nonce)를 포함하고 있다. 이어서 단말기는 두 번째 EAPOL-Key 프레임을 회신하는데,

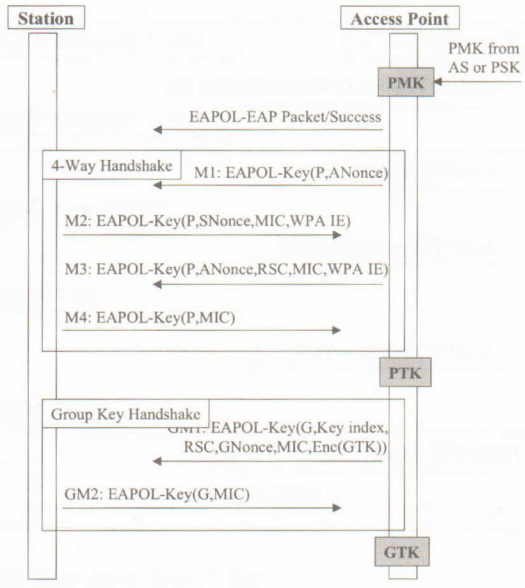


그림 3. IEEE 802.11i 키 교환 흐름도
Figure 3. IEEE 802.11i key exchange procedure

여기에는 단말기가 생성한 난수인 SNonce (Supplicant Nonce)가 포함되어 있으며, 단말기에서 ANonce와 SNonce, 그리고 PMK와 통신 당사자 하드웨어 주소를 파라미터로 하여 생성한 PTK를 이용한 메시지 무결성 체크 값도 포함되어 있다. 두 번째 EAPOL-Key 프레임으로부터 SNonce를 수신한 액세스포인트도 PTK를 생성하고 무결성 체크 검증 후 정상적인 값이면 세 번째 EAPOL-Key 프레임을 전송한다. 네 번째 EAPOL-Key 프레임을 받아서 메시지 무결성 체크가 검증되면 4-way handshake가 마무리되고 통신 당사자인 단말기와 액세스포인트는 동일한 PTK 키 블록을 갖게 된다.

Group key handshake에서는 액세스포인트가 이미 보유하고 있는 GTK를 PTK 키 블록의 일부를 사용하여 암호화한 후에 EAPOL-Key 프레임에 실어 보내고, 단말기에서 메시지 무결성 체크 검증 후에 정상적인 복원이 이루어지면 ACK를 보낸다.

Ⅲ. 혼합모드 무선랜 키 관리

WPA 제품이 개발된다 하더라고 실제 활용되는 상황에 있어서는 전체 무선랜 단말기들이 WPA 제품으로 대체되기에 앞서 액세스포인트가 먼저 WPA 제품으로 대체되어 다양한 무선랜 단말기를 지원해

야 하는 혼합모드 무선랜 환경이 상당기간 지속될 것으로 예견된다. 그림 4는 혼합모드 무선랜 환경을 나타낸 예이다. 무선랜 단말기 중 일부는 기존의 WEP 알고리즘을 사용하고(Station 1, Station 2), 일부는 새로운 암호 알고리즘인 TKIP을 사용하며(Station 3, Station 4), 일부는 암호 기능을 지원하지 않을 수도 있다(Station 5).

1. 혼합모드 무선랜 정의

WPA 규격에서 정의한 혼합모드 무선랜 환경은 기존의 WEP 알고리즘을 사용하는 단말기와 WPA 기능을 지원하는 단말기가 공존하는 환경을 의미한다[6]. 이러한 정의에서 볼 때는 무선구간 암호 알고리즘의 종류에 따른 구분일 뿐이지만 실제 적용되는 상황을 고려하면 훨씬 다양한 경우가 혼재할 수 있다. 예를 들면, 키 교환 기능이 전혀 없는 상태에서 고정 WEP 키를 사용하는 단말기가 존재할 수 있고, IEEE 802.1X 키 전송 방식에 의해 전달된 WEP 키를 사용하는 단말기가 있을 수 있고, WPA 키 교환 방식에 의해 전달된 WEP 키를 사용하는 단말기가 있을 수 있으며, WPA 키 교환 방식에 교환된 TKIP 키를 사용하여 TKIP 암호화 동작을 요구하는 단말기가 존재할 수도 있다. 따라서 액세스포인트가 모든 형태의 다양한 무선랜 단말기를 모두 지원할 수는 없으며, 액세스포인트 자신의 기본 환경 설정 동작에 의해서 자신이 지원할 수 있는 형태의 단말기 범위를 결정하여야 한다.

본 논문에서는 고정 WEP 키를 사용하는 단말기는 다수의 사용자가 동일한 키를 공유하여 사용자 데이터 보호라는 보안 취지에 어긋나므로 제외하기로 하며, II장 1절에서 언급하였듯이 IEEE 802.1X 키 전송 방식을 사용하여 전달된 키를 WEP 알고리즘에 적용하는 단말기와 WPA 키 교환 방식을 사용하여 교환된 키를 TKIP 알고리즘에 사용하는 단말기가 공존하는 혼합모드 무선랜 환경을 고려대상으로 한다. 따라서 그림 4에서 볼 때, 키 교환과 암호 알고리즘을 사용하지 않는 단말기(Station 5)는 액세스포인트에서 접속을 허락하지 않을 것이며, 어떠한 자원도 할당하지 않을 것이다.

2. Group 키 생성 및 설정 시점

혼합모드 무선랜 환경에서 무선구간 암호화 기능을 위해서는 반드시 키 교환이 수행되어야 함은 자명한 사실이다. 액세스포인트에서 unicast-용 pairwise 키는 각각의 단말기에 대해 서로 다르게 생성되어 설정되지만, broadcast-용 group 키는 접속된 모든 단말기가 동일한 값을 유지해야 한다. 그러므로 액세스포인트는 자신의 기본 환경 설정에 따라 group 키 생성 및 설정 시점을 결정해야 한다. 여기서 group 키 생성은 액세스포인트 내부의 전역변수로 관리되는 키 값을 만드는 동작을 의미하며, group 키 설정이라 함은 암호 알고리즘에서 사용할 수 있도록 생성된 group 키를 설정해 주는 동작을 의미한다. Pairwise 키는 일대일 관계에서 사용되기

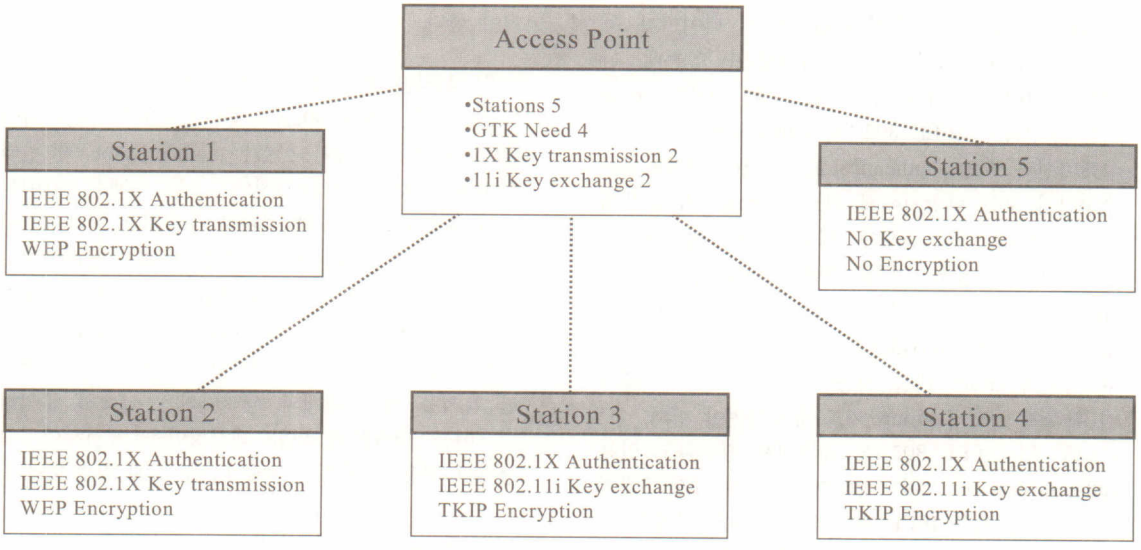


그림 4. 혼합모드 무선랜 시스템
Figure 4. Mixe-mode wireless LAN system

때문에 업데이트 요청이 있더라도 생성 즉시 설정해도 되지만, group 키는 일대다 관계이기 때문에 만일 group 키 업데이트 요청을 처리하기 위해서는 액세스포인트에서 새로운 group 키를 생성한 이후에 전체 단말기에게 새로운 group 키가 분배되었음을 확인하기 전에는 새로운 group 키를 설정하지 않아야 한다.

WPA 규격에 따르면, group 키 생성 및 설정 시점은 최초 액세스포인트 부팅 이후에 가장 먼저 접속을 시도하는 단말기와 group key handshake를 수행한 직후이다. Group 키는 전역변수로 관리되기 때문에 이후에 접속하는 단말기에게는 저장되어 있는 group 키를 전달하면 된다. 그리고 외부적인 요청 또는 일정 주기 타이머에 의하여 group 키 업데이트가 요구될 때 group 키는 새롭게 생성될 수 있는 구조를 지니고 있다.

그러나 혼합모드 무선랜 환경에서 액세스포인트 부팅 직후에 가장 먼저 접속하는 단말기가 WPA 키 교환 방식을 지원하지 못하고 IEEE 802.1X 키 전송 방식만을 지원하는 단말기라면 최초 group 키 생성과 설정 과정이 존재하지 않게 된다. 따라서 본 논문에서 고려하는 혼합모드 무선랜 환경을 지원하는 액세스포인트는 초기 부팅 과정에서 반드시 최초 group 키 생성과 설정 동작을 수행하여야 한다.

키 관리의 한 측면인 키 업데이트 처리를 위해서 group 키 생성은 키 분배 동작 이전에 이루어 져야 하며 모든 단말기에게 group 키 분배가 완료되었음을 확인한 후에 group 키 설정이 수행되어야 한다. Group 키 업데이트 요청은 group 키 타이머가 동작되었거나 외부적인 요청에 기인할 수 있는데, 이러한 요청이 인지되면 액세스포인트는 새로운 group 키를 생성하고, IEEE 802.1X authenticator 키 전송 상태머신과 WPA authenticator 키 관리 상태머신을 구동시켜 모든 단말기에게 새로운 group 키를 분배한다. Group 키 분배가 완료된 이후에 새로운 group 키를 암호 알고리즘에 설정하며, 새로운 group 키를 설정하더라도 액세스포인트는 group 키 업데이트 이전에 broadcast 데이터를 보내는 단말기와 이전의 group 키를 이용한 암호 통신을 수행하기 위하여 이전의 group 키도 유지하여야 한다.

그림 5는 IEEE 802.1X 규격에서 정의하고 있는 authenticator 키 전송 상태머신으로써 II장 2절의 그림 2에서 보인 IEEE 802.1X 키 전송 절차를 수행하는 상태머신이다. 그림 5에서 보이듯이 전송해야 할 키가 존재한다고 인식하면(keyAvailable) 키 전송 함수(txKey())를 구동시켜 EAPOL-Key 프레임을 전송하는 구조이다.

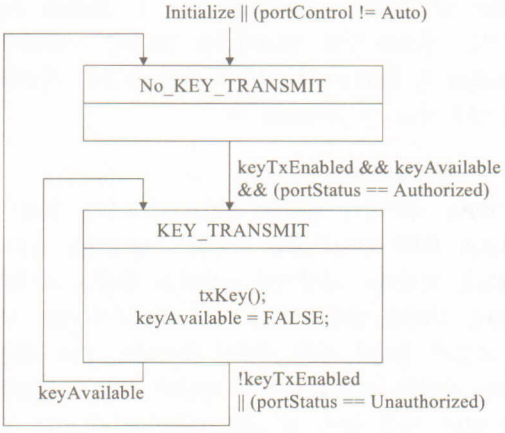


그림 5. IEEE 802.1X authenticator 키 전송 상태머신
Figure 5. IEEE 802.1X authenticator key transmission state machine

IEEE 802.1X 규격은 무선랜 시스템에서 사용하기 위한 특정 목적을 지닌 것이 아니라 일반적인 포트 기반 접근 제어를 위한 범용 규격을 지향하고 있기 때문에 다수의 단말기를 관리하기 위한 변수 또는 상태 천이가 별도로 정의되어 있지 않다. 따라서 액세스포인트에서 키 관리에 영향을 끼치는 전역변수들은 무선랜 보안이라는 특정 목적을 위해 정의된 WPA 또는 IEEE 802.11i 규격에서 관리되어야 한다.

3. 취약점 분석 및 해결방안 제시

그림 6은 IEEE 802.11i Draft 3.0에서 정의하여 WPA 규격이 준용하고 있는 authenticator 키 관리 상태머신으로써 II장 3절의 그림 3에서 보이는 IEEE 802.11i 키 교환 절차를 수행하는 상태머신이다. 그림 6에 표시된 5개의 원은 현재의 상태머신이 가지는 보안상 취약점을 표현한 것으로써 키 생성, 교환 그리고 업데이트와 관련된 취약점이다. 본 장에서는 혼합모드 무선랜 환경에서 키 관리상 취약한 특성을 지닌 현재의 상태머신을 상세히 분석하고, 이를 극복하기 위한 해결방안을 제시하며, 그 결과가 적용된 새로운 상태머신을 그림 7에 보인다.

1) Group 키 교환 대상 관리

첫 번째 취약점은 group 키 교환이 필요한 단말

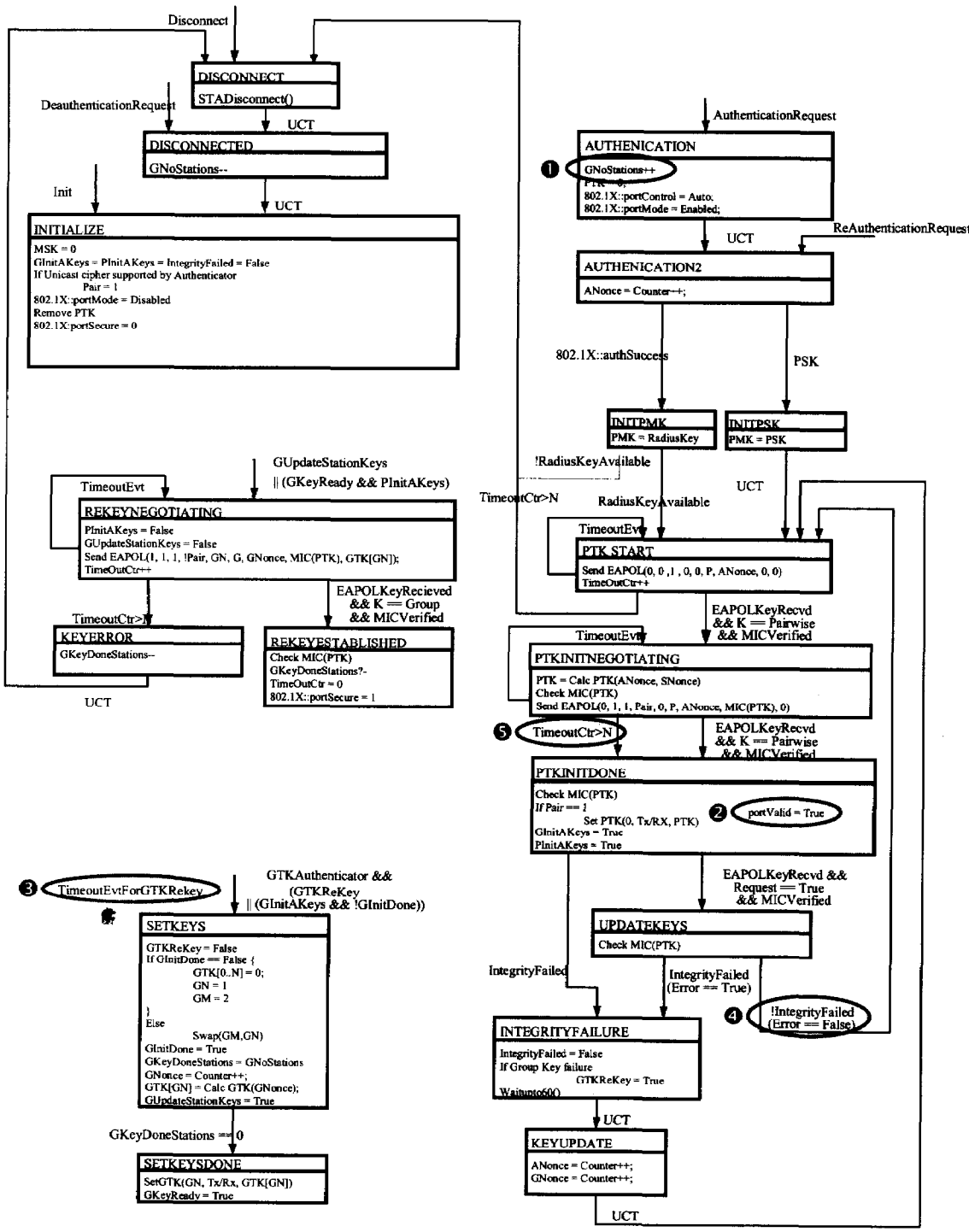


그림 6. WPA authenticator 키 관리 상태머신의 취약점
Figure 6. Week points in WPA authenticator key management state machine

기를 관리하는 전역변수가 부적절한 곳에 위치하여 발생하는 group 키 설정 실패의 가능성이다.

그림 6의 1번 원 내부에 표시된 GNoStations 변수는 group 키 교환 대상의 수를 나타낸다. 현재의 상태머신에서는 인증 요청 초기 동작인 AUTHENTICATION 상태에서 해당 단말기를 추가하여 키 교환 대상의 수를 1만큼 증가시킨다. 그리고 AUTHENTICATION2 상태에서 대기하다가 인증서버로부터 인증 성공 메시지(authSuccess)를 받거나 PSK 방식(PSK)임을 알면 PMK 획득 과정인 INITPMK 또는 INITPSK 상태로 천이한다. GNoStations 변수의 값은 액세스포인트가 group 키를 전달해야 할 전체 단말기의 수로써 항상 유지되는 값이며, SETKEYS 상태에서 GKeyDoneStations 변수로 임시로 저장된다. GKeyDoneStations는 각 단말기에 group 키 교환이 성공적으로 수행되면 REKEYESTABLISHED 상태에서 1만큼 감소하게 되며, 최종적으로 0이 되면 SETKEYDONE 상태로 천이하여 group 키를 설정한다.

만일 가장 먼저 접속을 시도한 단말기와 정상적으로 WPA authenticator 키 관리 상태머신이 구동하였다면 최초 GNoStaitions 값이 1이 되고, 4-way handshake를 수행한 이후에 GKeyDoneStations 변수에 GNoStations 값인 1을 할당하고, group key handshake를 성공하여 GKeyDoneStations 값을 1 감소시킴으로써 group 키를 설정할 수 있다.

그러나 만일 인증 요청을 인지하여 AUTHENTICATION2 상태에서 대기 중이고, 인증 절차가 진행되다가 인증이 실패하는 경우가 발생하여 인증 성공 메시지(authSuccess)를 수신하지 못하게 되면 현재의 상태머신은 이미 증가시켰던 GNoStations를 감소시키지 않고 그대로 유지하고 있게 된다. 따라서 다시 인증 요청이 시작되면 GNoStations 값은 2가 되고, 이 값은 GKeyDoneStations로 할당되는데, 이 경우에는 group key handshake를 성공하여 GKeyDoneStations 값을 1만큼 감소시킨다 하더라도 최종적으로 0으로 만들 수가 없기 때문에 group 키 설정을 실패하게 된다.

(해결방안)

본 논문에서 제시하는 해결방안은 group 키 교환 대상의 수로 인식하는 부분을 인증 성공 메시지(authSuccess)를 수신한 이후인 INITPMK 또는 INITPSK 상태로 옮기는 방법이다. 그림 7은 본 논문에서 제시하는 해결방안을 적용시켜서 새롭게 구성한 WPA authenticator 키 관리 상태머신이며, 1번으로 표시한 부분이 GNoStations를 1만큼 증가시키는 동작을 옮겨놓은 부분이다. 이렇게 위치를 변경시키면 반드시 인증 성공 이후에 키 교환 대상으로 인식되며, 만일 키 교환 절차가 실패하게 되면 DISCONNECTED 상태로 천이되기 때문에 증가되었던 GNoStation 값을 다시 감소시키는 동작이 수행되어 위에 언급한 GNoStations 값의 유지와 관련된 문제가 해결된다.

그러나 이러한 위치 변경 방법은 재인증 요청이 발생할 경우(ReauthenticationRequest)에 또 다시 GNoStations++ 동작을 수행하기 때문에 여전히 실제 키 교환이 필요한 단말기 수와 내부적으로 유지하는 GNoStations 값이 다르게 되는 문제가 있다. 따라서 INITPMK 또는 INITPSK 상태에서는 재인증 요청의 발생 여부를 확인하여 재인증 요청에 의한 상태 천이라고 판단되면 GNoStations 값을 증가시키지 않도록 해야 한다.

2) Pairwise 키 교환 완료 지시

두 번째 취약점은 포트 기반 접근 제어를 지원하기 위한 pairwise 키 교환 성공을 알려주는 변수가 포함되어 있지 않다는 점이다.

본 논문에서 언급하는 혼합모드 무선랜에서의 액세스포인트는 각각의 단말기에 대하여 인증과 키 교환 결과에 따라 포트 기반 접근 제어를 수행한다. IEEE 802.1X 규격의 추가 및 수정 문서인 IEEE 802.1aa 문서에서는 포트를 통한 접근 허가 여부를 위하여 인증 성공 메시지인 authSuccess 변수와 더불어 키 교환 성공 메시지인 portValid 변수를 참조하도록 정의하고 있다[12]. 따라서 키 교환 동작을 담당하는 WPA authenticator 키 교환 상태머신에서 portValid 변수를 제어함으로써 IEEE 802.1aa 문서의 포트 기반 접근 제어를 명확하게 지원해야 한다.

(해결방안)

본 논문에서는 portValid=TRUE 동작을 PTKINITDONE 상태에 추가시키도록 하였다. PTKINITDONE 상태는 4-way handshake가 성공적으로 완료된 경우에 천이된 상태이므로 IEEE 802.1aa 문서가 요구하는 상황에 가장 적합한 위치이다. 또한 인증 취소 또는 재접속 등의 이유로 초기 동작부터 다시 시작하는 경우(INITIALIZE)에는 portValid 변수를 FALSE로 만드는 동작이 포함되

도록 한다.

그리고 혼합모드 무선랜 환경에서는 WPA authenticator 키 관리 상태머신과 더불어 IEEE 802.1X authenticator 키 전송 상태머신도 존재하므로 후자인 경우에는 그림 5에 보이는 txKey() 함수에서 portValid 변수를 제어해야 할 것이다.

3) Group 키 타이머 동작 처리

세 번째 취약점은 group 키 타이머 동작을 정의하지 않음으로 인하여 한번 설정된 group 키는 액세스포인트의 재부팅 이전에는 바뀌지 않는다는 점이다.

일정 주기 동안 사용한 키는 새롭게 업데이트하는 것이 보안 성능을 향상시키는 방법이다. 현재의 WPA authenticator 키 관리 상태머신은 group 키의 rekey 타이머가 존재하지 않아서 잠재적인 키 노출의 위험을 안고 있다. IEEE 802.11i 규격의 부록 D에 따르면 dot11RSNConfigGroupRekeyTime 이라는 MIB(Management Information Base) 변수가 존재하고 기본 값으로 86400초를 정의하고 있다[4]. 86400초는 하루에 해당하는 값으로써 group 키가 최초 설정된 이후에 매일 group 키를 업데이트 시켜야 됨을 지시하고 있다.

(해결방안)

본 논문에서는 그림 7의 3번으로 표시한 것과 같은 상태 천이를 추가시킨다. Group 키 업데이트는 반드시 group 키가 설정된 이후에 동작되는 것이므로 SETKEYDONE 상태에서 업데이트를 위한 상태 천이가 이루어져야 한다. 최초 group 키가 설정된 이후에 group 키 rekey 타이머가 동작되어 하루가 지나서 타임아웃 이벤트를 인지하면 SETKEYS 상태로 천이하여 새로운 group 키를 생성하고, 모든 단말기에 대해 group key handshake를 수행하여 GKeyDoneStations 값이 0이 되면 SETKEYDONE 상태로 들어가서 group 키를 재설정하게 된다. 혼합모드 무선랜 환경에서는 IEEE 802.1X 키 전송 방식을 사용하는 단말기에게도 새로운 group 키를 전달해야 하는데, 그 역할은 그림 5의 txKey() 함수에서 책임을 질 것이다.

4) Pairwise 키 업데이트 처리

네 번째 취약점은 pairwise 키 업데이트 요청을 인지한 이후에 ANonce를 변경하지 않고 이전의 ANonce를 다시 사용하는 구조를 지닌다는 점이다.

Pairwise 키는 PMK, ANonce, SNonce, 액세스포인트의 하드웨어 주소, 그리고 상대 단말기의 하드웨어 주소를 파라미터로 하여 PRF(Pseudo Random Function) 동작을 통해 생성된다[4]. Pairwise 키 업데이트가 요청되면 4-way handshake를 다시 수행하여 새롭게 pairwise 키를 생성해야 하는데, PMK와 하드웨어 주소가 변경되지 않은 상태이므로 ANonce와 SNonce가 변화해야만 새로운 pairwise 키를 생성할 수 있다. 그러나 그림 6의 4번 원이 지시하는 상태 천이는 UPDATEKEYS 상태에서 PTKSTART로 곧바로 천이하도록 되어있다. 이는 이전에 사용되었던 ANonce를 다시 사용하게 되는 구조로써 일반적인 Nonce의 특징인 단 1회의 사용이라는 근본 취지에 어긋나며, 새로운 pairwise 키 생성을 새로운 SNonce에만 의존해야 하는 취약한 상황이 된다.

(해결방안)

본 논문에서 제시하는 해결방안은 ANonce의 변화를 위해 그림 7의 4번에서 표시하는 것처럼 KEYUPDATE 상태를 거쳐서 PTKSTART 상태로 천이하도록 하는 것이다. KEYUPDATE 상태에서는 ANonce++ 동작을 수행하여 이전에 사용되었던 ANonce와는 다른 값을 지니게 되고, PTKSTART에서는 새로운 ANonce 값을 포함한 EAPOL-Key 프레임을 4-way handshake의 첫 번째 메시지로 전달하여 새로운 pairwise 키로 업데이트할 수 있다.

5) Pairwise 키 교환 메시지 재전송 처리

Pairwise 키 교환을 위한 4-way handshake 동작을 수행하는 상태가 PTKSTART와 PTKINITNEGOTIATING 상태이다. 그림 6의 5번 원 내부에 보이는 TimeoutCtr 변수는 EAPOL-Key 프레임의 송신 횟수를 기록하고 있는 변수이다. 즉, 4-way handshake 메시지를 담고 있는 EAPOL-Key 프레임이 손실되었을 경우를 대비하여 EAPOL-Key 프레임의 재전송을 처리할 수 있는 재전송 카운터이다. 액세스포인트가 보내는 EAPOL-Key 프레임에 대한 응답 EAPOL-Key 프레임이 정해진 시간 안에 도착하지 않으면 이전의 EAPOL-Key 프레임을 재전송하고, 동일한 EAPOL-Key 프레임이 몇 번 전송되었는지를 TimeoutCtr 변수에 기록한다. 따라서 재전송을 시도할 수 있는 최대 횟수(N)가 정해져 있다면 해당 횟수 이내에 응답이 없는 경우에는 키 교환이 실패한 것이므로 접속을 끊고 새롭게 인증 절차 및 키 교환 절차를 진행해야 한다.

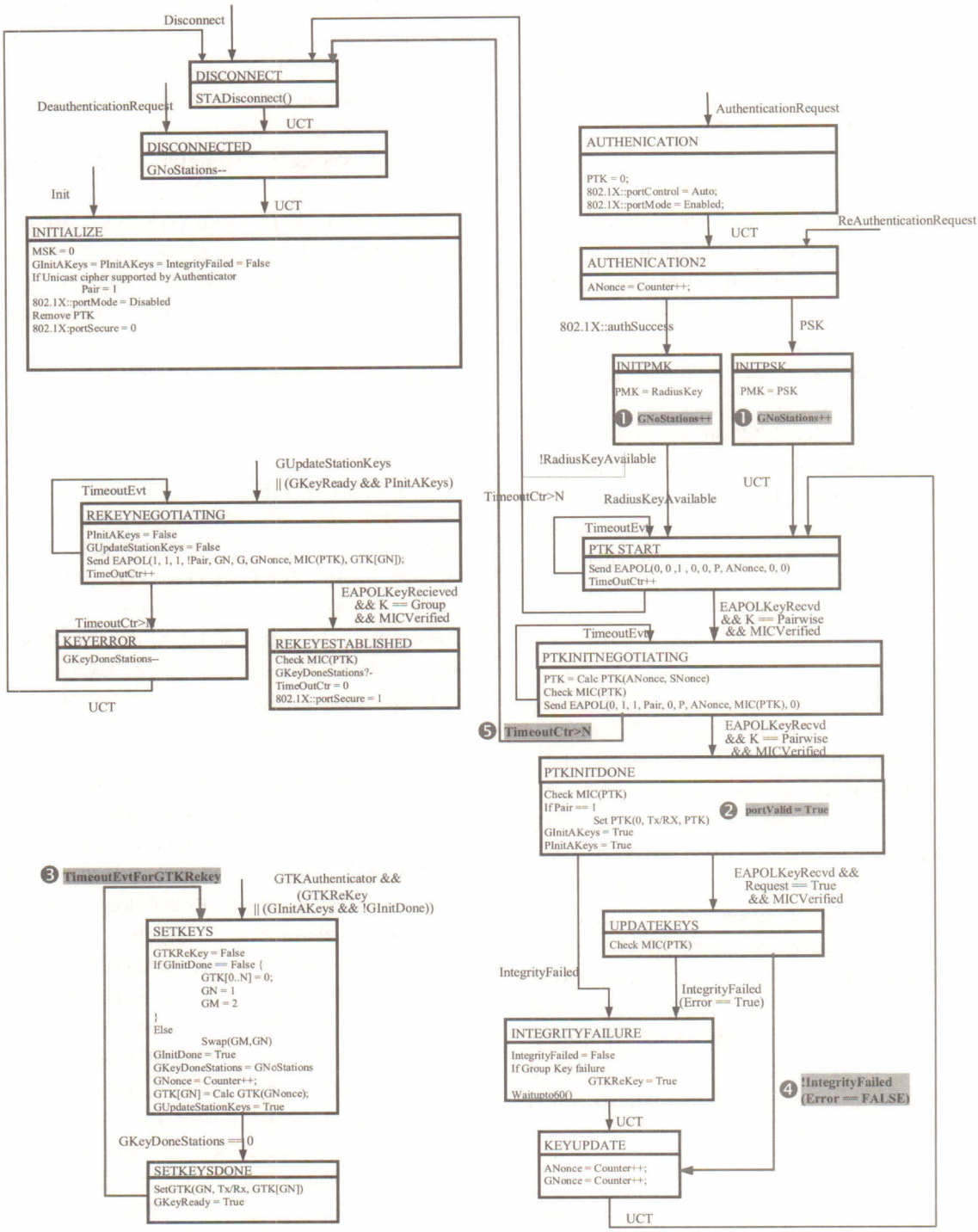


그림 7. 재구성한 WPA authenticator 키 관리 상태머신
Figure 7. Reconstruction of WPA authenticator key management state machine

그러나 그림 6에서 보면, PTKINITNEGOTIATING 상태에서 EAPOL-Key 프레임 전송 이후에 재전송 횟수를 초과한 경우(TimeoutCtr>N)에 PTKINITDONE 상태로 천이하는 오류를 범하고 있다. 이러한 형태의 오류는 전송 프레임이 손실되었음에도 불구하고 정상적인 동작과 동일한 처리과정을 통해 자원을 할당하기 때문에 DoS(Denial of Service) 공격의 원인이 될 수 있다.

(해결방안)

본 논문에서는 그림 7의 5번으로 표시한 것처럼 상태 천이가 PTKINITNEGOTIATING에서 DISCONNECT로 발생하도록 수정하였다. 따라서 액세스포인트에서는 EAPOL-Key 프레임 전송 이후에 정해진 시간 안에 적법한 응답을 수신하지 못하여 재전송을 시도하는 경우에 최대 재전송 횟수를 초과하게 되면 해당 단말기의 접속을 끊고 새롭게 인증 및 키 교환을 수행할 수 있는 구조가 되었다. 따라서 전송 프레임의 손실을 확인하여 정상적인 처리 절차로 진입하지 못하도록 하기 때문에 DoS 공격의 원인을 제거하는 효과가 있다.

Ⅳ. 결 론

본 논문의 연구결과는 WPA 보안 규격에서 정의하고 있는 키 관리 상태머신이 혼합모드 무선랜 환경을 지원하기 위해서는 반드시 수정이 필요함을 보이고 있다. 무선랜 시스템의 상용서비스를 고려하면 기존의 WEP 기반 무선랜 카드의 사용과 새로운 WPA 기능 무선랜 카드를 사용하는 단말기들이 공존하는 혼합모드 무선랜 환경을 지원할 수 있는 액세스포인트의 출현이 기대되는 것은 당연한 이치이다.

이에 따라서 본 논문에서는 혼합모드 무선랜 환경을 지원하기 위한 액세스포인트의 키 생성, 교환, 설정과 관련된 키 관리 방식을 분석하여 group 키 생성 시점과 group 키 설정 시점의 결정, 그리고 WPA authenticator 키 관리 상태머신이 지니고 있는 보안상의 취약점을 극복할 수 있는 해결방안을 제시하였다. 본 논문에서 제시하는 최초 group 키 생성 및 설정 시점은 액세스포인트의 초기 부팅 동작이며, 이후의 group 키 업데이트 절차에서는 group 키 생성 시점은 업데이트 요청 직후이고 모든 단말기에게 새로운 group 키 전송이 확인된 시점이 새로운 group 키 설정 시점이다. 그리고 본 논문에서는 WPA authenticator 키 관리 상태머신의 취약점을 극복하기 위하여 group 키 설정에 영향을 주는 키 교환 대상 단말기 수의 증감 처리, portValid 변수의 추가, group 키 rekey 타이머의 추가, pairwise 키 업데이트 시 ANonce 변화 처리, 그리고 pairwise 키 교환 프레임의 재전송 처리 등을 재구성하여 혼합모드 무선랜 환경을 지원할 수 있는 토대를 마련하였다.

혼합모드 무선랜 환경을 지원하기 위하여 본 논문에서 제시하고 있는 키 관리 방식 및 키 교환 상태머신은 주로 WPA authenticator 키 관리 상태머신이 책임지는 부분을 명확하게 재구성하였지만, 상대적으로 IEEE 802.1X authenticator 키 전송 상태머신의 동작은 txKey() 함수에서 전적으로 처리됨을 전제로 하고 있기 때문에 상용화 가치를 극대화하기 위해서는 본 논문에서 제시하는 WPA authenticator 키 관리 상태머신과 더불어 txKey() 함수를 효과적으로 통합하여 설계, 구현하여야 할 것이다.

그리고 무선랜 시스템의 활용 형태를 예측해 볼 때, 향후에는 무선랜 사용자의 안전한 핸드오프 또는 글로벌 로밍과 관련된 기능, 그리고 서비스 사용에 대한 과금 기능의 연구가 필요할 것이다. IEEE 802.11 TGf에서는 무선랜 사용자의 안전한 핸드오프를 지원하기 위하여 액세스포인트 사이에서 사용자의 접속 정보를 전달하는 IAPP(Inter-AP Protocol) 프로토콜을 정의하고 있으며, IEEE 802.11 TGi에서는 신속하고 효율적인 접속 정보 전달을 위한 사전인증 방식에 대한 연구를 진행 중이다[13][14]. 더불어 기존 인증서버의 기능상의 제약점을 극복하고 성능이 향상된 새로운 인증 및 과금 서버의 개발이 IETF를 중심으로 연구되고 있기 때문에 이러한 기술들이 통합 운용된다면 향후 초고속 무선인터넷 환경이 사용자 편의와 보안을 한층 발전시킬 수 있을 것으로 기대된다.

참 고 문 헌

[1] ISO/IEC, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, ISO/IEC 8802-11, ANSI/IEEE Std 802.11, 1999.

[2] J. R. Walker, "Unsafe at any key size; An analysis of the WEP encapsulation", *IEEE 802.11-00/362*, IEEE 802.11 committee,

October 2000.

[3] W. A. Arbaugh, N. Shankar, and Y. C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", *Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks*, December 2001.

[4] IEEE, *LAN/MAN Specific Requirements- Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specification: Specification for Enhanced Security*, IEEE Std 802.11i/D3.0, November 2002.

[5] Wi-Fi Alliance, *Wi-Fi Protected Access (WPA) Version 2.0*, April 2003.

[6] Wi-Fi Protected Access, http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

[7] IEEE, *Standard for Local and metropolitan area networks- Port-Based Network Access Control*, IEEE Std 802.1X, June 2001.

[8] L. Blunk and J. Vollbrecht, *PPP Extensible Authentication Protocol (EAP)*, IETF, RFC 2284, March 1998.

[9] C. Rigney, *Remote Authentication Dial In User Service (RADIUS)*, IETF, RFC 2865, June 2000.

[10] B. Aboba, D. Simon, *PPP EAP TLS Authentication Protocol*, IETF, RFC 2716, October 1999.

[11] G. Pall, G. Zorn, *Microsoft Point-To-Point Encryption (MPPE) Protocol*, IETF, RFC 3078, March 2001.

[12] IEEE, *Standard for Local and metropolitan area networks- Port-Based Network Access Control- Amendment 1: Technical and Editorial Corrections*, IEEE P802.1aa/D6.1, June 2003.

[13] IEEE, *Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation*, IEEE Std 802.11f/D5, January 2003.

[14] B. Aboba, "IEEE 802.1X Pre-Authentication", *IEEE 802.11-02/389r1*, IEEE 802.11 committee, June 2002.

강 유 성(You Sung Kang) 정회원

1997년 2월 : 전남대학교 전자공학과 졸업
1999년 8월 : 전남대학교 전자공학과 석사
1999년 11월 ~ 현재 : 한국전자통신연구원 무선LAN보안연구팀 선임연구원

<관심분야> 무선 네트웍 보안, 암호 프로토콜, 스마트카드

오 경 희(KyungHee Oh) 정회원

1999년 2월 : 연세대학교 컴퓨터과학과 졸업
2001년 2월 : 연세대학교 컴퓨터과학과 석사
2000년 12월 ~ 현재 : 한국전자통신연구원 무선LAN보안연구팀 연구원

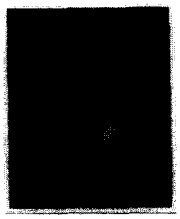
<관심분야> 암호 프로토콜, 무선랜 보안

정 병 호(ByungHo Chung) 정회원

1988년 2월 : 전남대학교 전산통계학과 졸업
2000년 2월 : 충남대학교 컴퓨터과학과 석사
2000년 3월~현재 : 충남대학교 컴퓨터과학과 박사 수료
1998년 2월 ~ 2000년 6월 : 국방과학연구소 선임연구원
2000년 6월 ~ 현재 : 한국전자통신연구원 무선LAN 보안연구팀 팀장

<관심분야> 무선/이동 QoS, MANET Security, 네트웍 보안 프로토콜

정 교 일(Kyo-il Chung) 정회원



1981년 2월 : 한양대학교 전자공학과 졸업
1983년 8월 : 한양대학교 산업대학원 전자계산학과 석사
1997년 8월 : 한양대학교 대학원 전자공학과 박사
1980년 12월 ~ 1981년 11월 : 엠시스템즈 사원
1981년 12월 ~ 1982년 2월 : 한국전기통신연구소 위촉연구원
1982년 3월 ~ 현재 : 한국전자통신연구원 정보보호 기반그룹장/책임연구원
<관심분야> IC Card, Security, Biometrics, 국가기반보호, 신호처리

양 대 헌(DaeHun Nyang) 정회원

1994년 2월 : 한국과학기술원 과학기술대학 전기 및 전자공학과 졸업
1996년 2월 : 연세대학교 컴퓨터과학과 석사
2000년 2월 : 연세대학교 컴퓨터과학과 박사
2000년 9월 ~ 2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 3월 ~ 현재 : 인하대학교 정보통신대학원 전임강사
<관심분야> 암호이론, 암호 프로토콜, 네트워 보안 프로토콜