이동 무선랜 접속장치의 접속점 보안 천이 메커니즘과 유한상태머신

정회원 정 병 호*, 강 유 성**, 오 경 희***, 김 상 하****

Inter-AP Security Transition Mechanism and Its FSM in WLAN AP Supporting Fast Roaming

ByungHo Chung*, You Sung Kang**, KyungHee Oh***, SangHa Kim**** ***Regular Members***

요 약

무선랜 상에서 실시간 음성 서비스 제공에 대한 기대가 높아지면서 무선랜 접속장치에 빠르고 안전한 이동성 지원 기술을 구현하는 문제는 최근 가장 활발히 연구되고 있는 분야 중 하나이다. 이동 단말이 새로운 접속장치로 이동하더라도 과거 접속장치로부터 제공 받던 보안 강도를 지속적으로 유지하면서 이동 지연시간을 최소화하는 문제는 매우 중요하다. 따라서 본 논문은 IEEE802.11i, 802.1x, 그리고 802.11f를 지원하는 무선랜에서 접속점 보안 천이시간을 시스템 성능 변수로 정의하고, 평균적 천이 지연시간의 최소화를 목적 함수로 하는 보안 메커니즘과 그 실현을 위한 유한 상태 머신을 제안한다. 실험 결과 제안된 보안 메커니즘이 기존의 802.1X인증 방식에 비하여 79% 까지의 성능 이득이 기대됨을 보인다.

Key Words : WLAN security mechanism, Inter-AP security transition latency time, security FSM

ABSTRACT

Recently with the high expectation of voice over WLAN service, to support fast inter-AP security transition in WLAN AP is one of the most actively investigating issues. It is also very important to minimize inter-AP security transition latency, while maintaining constantly the secure association from old AP when a station transits to new AP. Hence, this paper first defines secure transition latency as a primary performance metric of AP system in WLAN supporting IEEE802.11i, 802.1x, and 802.11f, and then presents low latency inter-AP security transition mechanism and its security FSM whose objective is to minimize inter-AP transition latency. Experiment shows that the proposed scheme outperforms the legacy 802.1X AP up to 79% with regard to the transition latency.

Ⅰ. 서 론

최초 실험실 수준에서 등장한 무선랜이 2000년 초고속 무선 인터넷의 유력한 대안으로 선택된 후 급속한 성장과 진화를 거듭해 가고 있다. 무선랜이 무선 액세스 기간망의 역할을 하고, 그 응용 영역 또한 확대되어 가는 만큼 고속화, 품질화, 보안화 관점에서 무선랜에 대한 요구 수준도 높아지고 있다. 무선랜은 단말의 이동성 지원여부에 따라서 고정 접속 무선랜과 이동 접속 무선랜으로 구분할 수 있다. 고정 접속 무선랜은 단말이 최초 접속한 접속장치를 통해서만 단절없는 서비스를 제공 받는 무

* 한국전자통신연구원 정보보호연구단(cbh@etri.re.kr), ** 한국전자통신연구원 정보보호연구단(youskang@etri.re.kr),
*** 한국전자통신연구원 정보보호연구단(khoh@etri.re.kr), **** 충남대학교 컴퓨터공학과(shkim@cnu.ac.kr, 교신저자)
논문번호 : KICS2005-03-127, 접수일자 : 2005년 3월 29일

선랜이다. 단말이 접속장치의 신호 영역을 벗어나면 통신 서비스는 단절된다, 처음부터 다시 인접 접속장치에 접속해야 한다. 반면에 이동접속 무선랜은 단말이 인접 접속장치로 이동할 지라도 단절없는 통신 서비스 품질과 보안 강도를 유지해주는 무선랜이다. 현재 까지는 고정접속 무선랜 환경에서의 통신 서비스 품질 향상 그리고 무선 구간 통신 프라이버시 보장 등의 문제 해결에 집중하여 연구가 진행되어 왔다

보안관점에서 살펴보면, 무선랜의 WEP 프라이버시 메커니즘이 취약한 것으로 알려졌고[2], 이를 해결하는 새로운 보안 아키텍쳐와 통신 프라이버시 보호 프로토콜이 IEEE 802.11i 작업반에 의하여 개발되었다[3]. 또한 비인가자의 무단 접속으로부터 통신망을 보호하기 위한 표준이 IEEE 802.1x[5] 규격으로 정리되었다. 그리고 무선랜 접속장치(AP) 상호간의 연동 보안망 구성과 정보 전달을 위한 프로토콜 즉, Inter-Access Point Protocol(IAPP)가 IEEE 802.11f 워킹그룹에 의하여 마무리되었다[4]. 전술한 표준들은 모두 개별 기술이 아니라 하나의 통합된 기술로 접속장치에 구현되어야한다. 현재 상기 보안 기능의 일부를 개별적으로 지원하는 제품이 출시되고 있다. 예를 들면, 802.1x + 802.11i TKIP 지원 AP를 들 수 있다. 최근, Wi-Fi폰을 이용한 무선랜 음성 서비스 제공 (VoWLAN)에 대한 기대가 높아지면서, 무선랜 환경에서 빠르고 안전한 이동 멀티미디어 서비스를 실현하는 메카니즘은 가장 활발한 연구 분야로 인식되고 있다. 이동 단말이 새로운 접속장치로 이동하더라도 과거 접속장치로부터 제공 받던 보안 강도를 지속적으로 유지하는 가운데 접속점 천이에 따른 지연시간을 최소화하는 문제는 매우 중요하다. 이러한 관점에서, 본 논문은 기존에 연구된 IEEE 802.11i, 802.1x 및 802.11f 기능을 통합하여 이동 접속 무선랜 보안 서비스를 제공하고자 할 때, 접속장치가 접속점 보안 천이에 따른 지연 시간을 최소화하는 방향으로 보안메커니즘이 재구성되어야 한다는 점을 직시한다. 이를 위하여, 본 논문은 먼저 접속점 보안 천이시간을 성능 변수로 정의하였다. 그리고 평균적 보안천이 지연시간의 최소화를 목적 함수로 하는 저지연 보안 메커니즘과 접속장치에서 그 메커니즘을 제어하기 위한 유한 상태 머신을 제안하고 성능이득을 분석한다.

Ⅱ. 접속점 보안 천이문제 정의

접속점 보안 천이 문제는 이동접속 무선랜에서 단말이 AP 사이를 로밍 할 때 이전 접속장치 (이하 oAP로 칭함)에서 제공받던 IEEE 802.11i의 보안 강도를 새로운 접속장치 (이하 nAP로 칭함)로 단절없이 그리고 지연시간이 최소화되도록 천이시키는 문제로 정의된다. 고정 접속점에서 단말의 보안 서비스를 결정하는 요소는 1) 인증 (공유키, 8021x) 및 키관리 (공유키, 802.11i 동적키교환) 방식 2) 프라이버시 보호 방식(WEP, TKIP, CCMP)의 취사선택에 의해서 결정된다. 이 때 단말의 보안 강도는 최초 AP와의 보안 연관 협상 과정을 거치면서 실현된다.

802.11i[3]에서는 두가지 형태의 프라이버시 보호키를 제공한다. 하나는 특정 AP에 접속된 모든 단말 상호간에 그룹통신 보호를 위한 그룹키이고, 다른 하나는 (단말, AP) 쌍 간의 비밀통신에 사용되는 비밀키이다. 비밀키와 그룹키를 동적으로 생성하기 위해서는 먼저 1단계로, 단말이 특정 AP에 접속을 시도하면 접속장치는 802.1x인증 프로토콜을 이용하여 단말과 802.1x인증서버 간에 상호 인증을 수행하고, 상호인증을 전제로 유도된 마스터키(PMK)를 인증서버가 AP로 전달한다. 이 과정에 의해서 단말과 AP가 동일한 PMK를 공유하게 된다. 다음 2단계에서, 단말과 AP가 둘만의 통신 프라이버시 보호에 필요한 비밀키(PTK)를 PMK와 둘만이 아는 난수를 이용하여 교환한다(802.11i는 이 과정을 4-단계 키협상 과정 이라고 칭함). 이렇게 PTK 협상이 종료된 후, AP는 PTK를 이용하여 단말에게 그룹통신키 (GTK)를 분배해준다. 전술한 바와 같이 단말이 nAP 에서도 oAP에서와 동일한 강도의 통신 서비스를 제공 받는데 필요한 접속점 보안 천이의 소요 시간을 최소화하기 위해서는1) 802.1x를 통한 단말 재인증 시간, t_{1X} 2) 마스터 키(PMK) 분배 시간, t_M 3) 프라이버시 보호 키(PTK, GTK) 협상 시간, t_{4W} 을 어떻게 축소할 것인가의 문제로 귀결된다.

Ⅲ. 기존의 보안 메커니즘 분석

이번 장에서는 기존 802.11i와 802.11f에서 접속점 보안 천이와 관련하여 제시된 보안 메커니즘을 분석 한다

3.1 802.11i 천이전 선인증 방식

802.11i 선인증 방식의 기본 아이디어는 단말이 nAP로 천이 할 때, 사전에 단말과 nAP가 상호 공

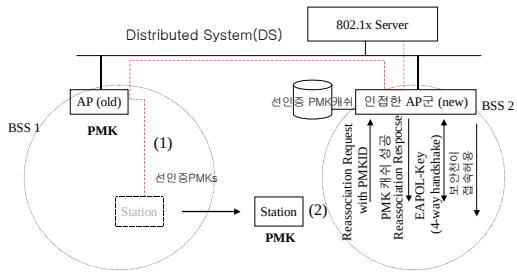

그림 1. IEEE 802.1i 선인증 과정

유된 PMK를 이용해서 (단말, nAP)간 재인증을 수행하고, 프라이버시 보호 키를 분배하겠다는 것이다. 그렇게 함으로써 (t_{1X} - t_M) 만큼의 시간 지연을 축소하는 성능이득을 얻는 것이다. 이를 위해서 단말은 그림 1에서와 같이 nAP로 천이 하기 전에 oAP를 통하여 이동 가능한 후보 접속장치 군(nAP들)에 각각 802.1x인증을 받고, 그렇게 생성된 PMK들을 해당 AP에서 캐쉬한다.

이후 단말이 실제로 nAP로 이동할 때, 선인증 PMK ID 값을 재연결 요청 메시지에 포함시켜 보낸다. 이 때 nAP는 자신이 캐쉬하고 있는 PMKID와 비교하여 그 값이 일치하는 경우, 그 PMK를 이용하여 프라이버시 보호 키 교환 과정을 수행하고 단말의 접속을 허용한다. 이 방법을 선인증 방식이라고 하고 1) 최초 접속장치에서만 802.1x인증을 받고, 그 다음 천이할 때 부터는 재인증에 따른 시간지연을 최소화하는 것2) (단말, nAP) 마다 다른 PMK를 갖는 다는 특징을 갖는다. 선인증 방식의 성능은 선인증 받아야 할 nAP의 수와 단말이 nAP에 재접속시 선인증 PMK의 캐쉬 힛트율에 의해서 영향을 받는다. 만일 단말이 천이한 nAP에서 PMK 캐쉬 실패가 발생하면, 해당 단말에 대해서 802.1x 인증 및 키 협상 전과정을 다시 수행하여야 한다. 이 과정은 보안 천이 지연 시간을 최대로 만드는 문제가 발생한다.

3.2 IEEE 802.1f 천이후 컨텍스트 전송방식

IEEE 802.11f는 그림 2와 같이 인접 AP 상호간에 서비스 컨텍스트를 안전하게 주고받는 전송방식(IAPP)을 제공한다[4]. 보다 구체적으로, 어느 한 단말이 IAPP 지원 AP에 접속이 이루어졌을 때 인접 AP군에 이 사실을 방송하는 Add-notify 패킷, 특정 단말이 nAP로 재접속 시도를 할 때 nAP가 oAP가 제공했던 보안 서비스 컨텍스트 정보를 전달해달라고 요청하고 받는 Move-notify/response 패킷, 그리고 향후 다른 AP로의 로밍에 가능성에 대비하여 단말 정보를 인접 AP에 미리 캐쉬해 놓은 Cache-notify/ response 패킷이 정의되어있다.

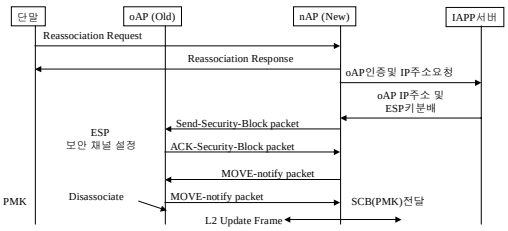

그림 2. IEEE 802.11f IAPP 로밍 과정

그림 2는 단말이 nAP로 재접속이 이루어졌을 때, AP 사이에 주고받는 IAPP 메시지를 보여준다. nAP로부터 Move-notify 패킷을 통하여 단말의 로밍 사실을 통보 받으면, oAP는 Move-response 패킷을 nAP에 반환한다. 이때 (단말, oAP)간에 공유된 PMK 정보를 패킷 내의 포함시켜 전달할 수 있다. 그리고, oAP는 해당 단말의 접속을 해제하고, 접속 관리 테이블에서 제거한다. 또한 nAP는 Move-response 패킷을 수신한 후, 2계층 경로 갱신 프레임을 L2스위치에 방송함으로써 향후 통신 데이터가 nAP로 전달되도록 한다.

보안 관점에서 IAPP는 단말이 최초 접속한 AP에서 생성된 PMK를 AP를 천이해 갈 때 마다 전달해 가거나, 미리 oAP로부터 이동 가능한 인접 nAP군에 캐쉬하는 스킴이다. 따라서 802.11i 선인증 스킴과 달리 재접속을 시도한 단말이 nAP 로 재접속시 단말이 해당 PMK의 소유자인지를 인증하는 절차와 키 분배 절차가 추가적으로 필요하다뿐만 아니라 캐쉬 방법의 경우, 특정 타겟 AP가 결정되지 않은 시점에 인접 AP군이 서브넷에서 통신 서비스를 제공 받고 있는 모든 단말의 프라이버시 키를 알 수 있다는 점에서 보안 취약성이 존재한다. 따라서 이 스킴은 서브넷 안의 모든 AP들은 신뢰할 수 있고, AP사이에는 보안 채널을 통하여 데이터 전달이 수행되며, 캐쉬된 PMK들은 AP 밖으로 노출되지 않는다는 전제 조건이 필요하다.

Ⅳ. 접속점 보안 천이 메카니즘 및 FSM제안

4.1 보안천이 지연시간 분석

표 1은 IEEE802.11i+802.1x+802.11f 지원 무선랜에서 접속점 보안천이를 제공하는 후보 메커니즘들을 지연시간과 제어 메시지 관점에서 분석 결과

표 1. 보안천이 후보 메커니즘의 천이시간 분석

구분	유 형	보안천이시간 분석	제어 트래픽
방법1	802.11i선인증+802.x	$(t_{11i\_cache} \times hit + t_{1X} \times miss) \times t_{11i}$	O(AP수×AP당 접속단말수)
방법2	IAPP 컨텍스트 전달+802.x	$(t_{IAPP} \times ok + t_{1X} \times nok)$	O(이동단말수×2)
방법3	802.11i선인증+IAPP캐쉬+ IAPP컨텍스트전달+802.x	$\min(t_{11i\_cache} \times hit, t_{IAPP\_cache} \times hit, t_{IAPP} \times ok \times miss, t_{1X} \times nok \times miss) \times t_{11i}$	O(AP수×AP당접속단말수×2)

를 정리한 것이다. 표 1에서 t_{11i_cache}와 t_{IAPP_cache}는 nAP에서 802.11i PMKID의 탐색시간과 IAPP PMKID의 탐색시간을 나타내고, *hit*와 *miss*는 PMK 캐쉬 힛트율과 실패율을 나타낸다. t_{11i}는 802.11i의 4단계 키협상에 걸린 시간을 그리고t_{1X}는802.1x를 통한 상호인증 및 AP에 PMK를 분배하는 시간을 의미한다. t_{IAPP}는IAPP를 이용하여 PMK를 oAP로부터 전달해 오는데 소요된 시간을, *ok* 는 PMK의 전달 성공율을 그리고*nok*는 실패율을 의미한다. 평균 천이 지연시간의 최소화를 목적 함수로 표1의 보안 메커니즘을 평가할 때, 방법 3이 가장 지연 시간을 최소화 할 수 있다. 방법 3은 802.11i선인증, IAPP캐쉬, IAPP컨텍스트 전송, 802.1x 중 지연시간이 가장 작은 경우를 선택한다.

4.2 접속점 보안 천이 메카니즘 제안

본 논문에서 표 1의 방법 3을 저지연 보안 천이 메커니즘으로 실현하기 위해서 기존 메커니즘에 추가적으로 고려해야 할 사항을 기술한다.

첫째, 이동 단말이 그림1. (2)와 같이 재접속 메시지에 단말이 보유한 PMKID리스트를 포함하여 재접속을 요구해야 한다[3].

둘째, IAPP를 이용하여 oAP와 nAP 사이에 PMK를 전달하는 자료 구조 정의가 필요하다. IAPP은 AP 사이에 정보를 전달하는 프로토콜은 정의하고 있지만, 프로토콜로 전달될 정보에 대한 세부 컨텍스트는 정의하고 있지 않다. 그림 3은 PMK 전달을 위하여 추가적으로 정의한IAPP 컨텍스트 자료 구조이다. 그림 3에서 PMKID는 단말이 nAP에 재접속을 요청할 때 단말이 PMK를 소유하고 있어서 802.1x인증을 생략하고 곧바로802.11i 키협상을 시작할 수 있음을 알리는 토큰으로 사용되는데 다음 수식과 같은 해쉬 값으로 구성된다[3].

PMKID	PMK	*lifetime*
Octets: 16	32	4

그림 3. 802.11f IAPP PMK 컨텍스트 자료구조

$$PMKID = HMAC\text{-}SHA1\text{-}128(PMK, \text{"PMK Name"} \| BSSID \| STA\text{-}MAC\text{-}Addr) \quad (1)$$

(1)에서 BSSID를 알 수 있다면, PMKID는 PMK로부터 계산해 낼 수 있지만, PMK를 변경하지 않고 단말이 두 번 이상 AP를 로밍 한 경우, nAP는 최초에 PMK가 생성된 액세스포인트의 BSSID를 알 수 없다. 따라서 PMK 뿐만 아니라 PMKID도 함께 nAP로 전달되어야 스테이션이 요청하는 PMKID로부터 PMK를찾을 수 있다. *lifetime*은 PMK가 앞으로 유효한 초 단위의 캐슁시간이다. *lifetime* 이후에는 802.1x재인증을 통하여 PMK를 갱신하여야 한다. 이는 PMK가 802.1x인증서버를 통하여 처음 생성될 때 설정된 유효기간이 로밍 과정에서 의미가 사라지는 것을 막기 위한 것이다. *lifetime*을 0과 같이 특별한 값으로 지정한 경우, nAP의 자체 정책에 따라 유효기간을 지정할 수도 있다.

셋째, 인접 AP에게 802.11i 선인증을 요구하거나 또는 인접 AP에게 IAPP로 PMK를 캐슁할 때, 캐슁해야 할 인접 AP들을 결정해야 한다. 본 논문에서는 PMK를 캐슁 할 인접 AP에 대한 정보가 관리자에 의해서 정책적으로 구성되거나, 단말이 nAP로 재접속을 요청할 때 제시하는oAP의 정보를 학습하면서 인접 AP에 대한 이미지 정보를 구성할 수 있다고 가정한다.

넷째, 이동 단말이 재접속 요청으로 제시한 PMKID들이 802.11i 선인증에 의해서 캐쉬된 PMKID와 IAPP에 의해서 캐쉬된 PMKID가 모두 힛트될 경우, 802.11i 선인증에 의해서 캐쉬된 PMKID에 우선권을 준다. 이는 여러 AP가 PMK를 공유하는 것 보다, AP마다 다른 PMK를 사용하는 것이 키 노출에 대한 위험이 더 낮기 때문이다.

4.3 이동보안 접속장치의 유한상태머신(FSM)

그림 4는 표 1 방법 3의 보안 천이 메커니즘을 제공하는 유한상태머신을 개략적으로 보인 것 이다. 그림의 이벤트 처리기는 단말의 접속 요청이 고정

접속 (Association) 인지 또는 이동접속(Reassociation) 인지를 판별하여 상태 처리머신을 구동시킨다. 단말이 고정 접속 요청인 경우 먼저 서비스 제어용 포트를 생성한 후, 802.1x 인증 및 802.11i 키협상을 진행하고 그 결과가 성공이면 단말에게 포트를 열어준다. 이동 접속 요청인 경우 802.11i선인증으로 캐쉬된 PMK를 최우선적으로 사용한다. 최악의 경우 단말이 요청한 PMKID가 nAP 캐쉬에 없고, IAPP를 이용하여 oAP로부터 PMK를 가져오는 것을 실패한 경우 고정접속 요청에서와 같은 지연시간을 요구하지만, 평균적인 접속점 보안 천이시간은 개선된다.

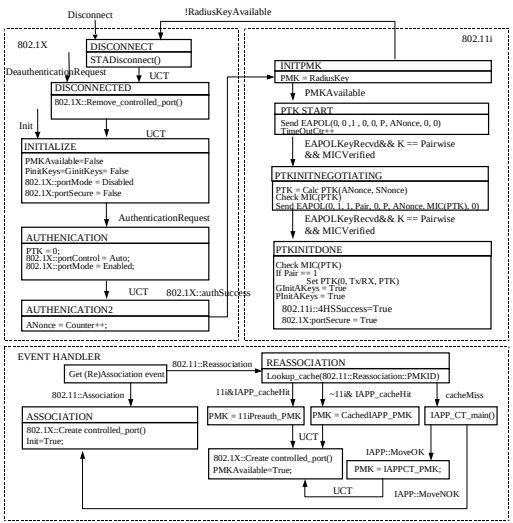

그림 4. 이동보안 접속정치의 개략적인 유한상태머신

그림 5는 그림 4의 FSM을 지원하는 접속장치의 개략적 구조도를 보인 것이다.

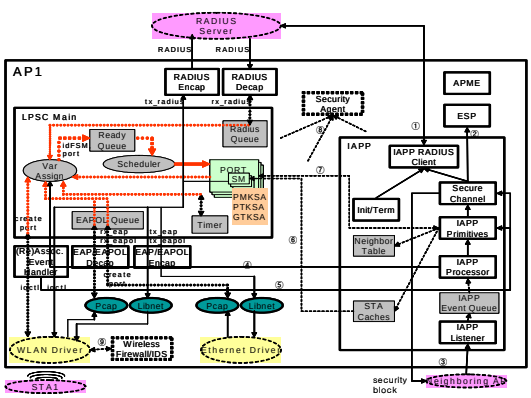

그림 5. 이동보안 접속정치의 개략적인 구조도

V. 실험 및 분석

운영체제로 리눅스 커널 2.4를 사용하는 노트북 컴퓨터를 IEEE802.11i+802.1x+802.11f 지원 접속장치의 개발환경으로 사용하였으며, Prism2 계열의 칩을 사용하고 펌웨어 수정으로WPA 기능이 지원되는 스테이션용 PCMCIA 무선랜 카드를 사용하였다. 해당 무선랜 카드를 사용하여 접속장치로 구동할 수 있는 HostAP 디바이스 드라이버를 수정하여 필요한 기능을 추가하였다. 그리고, 이를 제어하는 보안 모듈 별도로 개발하였다. 보안 모듈에는 802.11i, 802.1x 인증, IAPP, 그리고 고정 및 이동 접속보안 제어를 위한 유한상태머신 등의 기능이 구현되었다.

단말이 AP사이를 천이하는 실험을 위하여 핸드오프 시뮬레이터를 활용하였으며, 그림 6-그림 9와 같이 4가지 케이스 실험으로 측정된 보안 천이 지연시간을 표 2로 정리하여 분석하였다. 표 2에서 성능 이득은 oAP에서 802.1x인증에 소요된 시간을 1로 하였을 때, 접속점 보안 천이 메커니즘을 적용하여 단축된 지연시간을 비교한 상대적인 이득을 말한다.

표 2에서 IAPP를 이용한 PMK 전달 방식은 실제 네트워크 환경의 트래픽 부하에 따라서 성능 변동폭이 달라질 수 있다고 본다. 실험 결과 본 논문이 제안한 저지연 접속점 보안 천이 메커니즘을 적용할 경우, 70%이상의 성능이득이 있음을 알 수 있다.

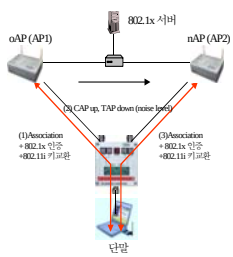

그림 6. 802.1x 이용 접속보안 천이

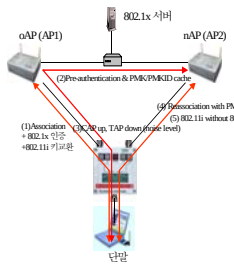

그림 7. 802.11i 선인증 이용 접속보안 천이

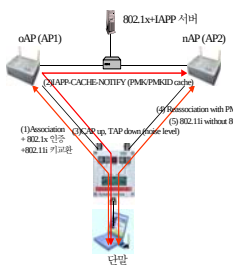

그림 8. IAPP-PMK 캐쉬 이용 접속점보안천이

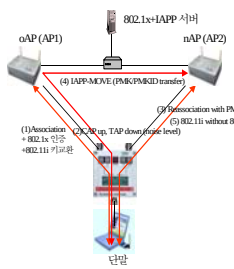

그림 9. IAPP-PMK 컨텍스트 전송이용 보안천이

표 2. Inter-AP 보안지연시간 측정 결과 및 제안 메카니즘의 성능 이득 (단위: 초)

구 분	.1X	.11i 선인증	IAPP.PMK 캐슁	IAPP.PMK 전달
Security(1X+11i)latency time in old AP(A)	2.032	2.055	2.508	2.134
IAPST latency time in new AP(B)	2.675	0.502	0.540	0.617
Performance gain (A-B)(latency reduction)	0%	0.24 (76%)	0.21 (79%)	0.29 (71%)

Ⅳ. 결 론

본 논문은 802.1x, 802.11i, 그리고 802.11f를 지원하는 무선랜 접속장치에서 빠르고 안전한 접속점 보안 천이 메커니즘을 제안하고, 제안 메커니즘을 접속장치에 실현하기 위한 유한상태머신과 접속장치의 개략적 구조도를 제시하였다. 보안천이 지연시간을 성능 변수로 고려할 때 802.11i선인증, IAPP PMK 캐슁, IAPP 보안 컨텍스트 전달 메카니즘을 혼합한 방식이 성능을 최대화 시킬 수 있음을 분석하고, 실험결과 802.1x로 이동 접속한 방식에 비하여 70%이상의 성능 이득을 기대 할 수 있음을 보였다.

무선랜에서 음성 서비스를 제공하기 위해서는 과거 접속점에서 제공 받던 보안 강도를 유지하는 천이 뿐만 아니라, 품질 또한 저하되지 않은 천이가 중요하다. 따라서 단말이 인접 접속장치로 이동하기 전에 재인증, 키분배 뿐만 아니라 QoS를 고려한 자원 선할당 까지를 마치고, 이동 후에는 곧 바로 데이터 서비스를 제공 받을 수 있는 메커니즘에 대해서도 지속적인 연구가 필요하다.

참 고 문 헌

[1] ISO/IEC, *WLAN MAC and PHY*, ISO/IEC 8802-11, ANSI/IEEE Std 802.11, 1999.

[2] W. A. Arbaugh et al., "802.11 Security Vulnerabilities," http://www.cs.umd.edu/~waa/wireless.html.

[3] IEEE, *LAN/MAN Specific Requirements- Part 11: Wireless MAC and PHY: Enhanced Security*, IEEE Std 802.11i/D3.0, November 2002.

[4] IEEE, *Recommended Practice for Multi-Vendor Access Point Interoperability via an IAPP*, IEEE Std 802.11f/D5, 2003.

[5] IEEE, *Standard for Port-Based Network Access Control*, IEEE Std 802.1X, 2001.

정 병 호 (ByungHo Chung) 정회원

1988년 전남대학교 전산통계학과(학사)
2000년 충남대학교 컴퓨터과학과(석사)
2005년 8월 충남대학교 컴퓨터과학과 (박사예정)
1998년 2월~2000년 6월 국방과학연구소
2000년 6월~현재 한국전자통신연구원
<관심분야> 무선/모바일 QoS, 무선 보안

강 유 성 (You Sung Kang) 정회원

한국통신학회 논문지 제 29권 4C 호 참조

오 경 희 (KyungHee Oh) 정회원

한국통신학회 논문지 제 29권 4C 호 참조

김 상 하 (SangHa Kim) 정회원

1980년 서울대학교 화학과(학사)
1984년 University of Huston(석사)
1989년 University of Huston(박사)
1992년~현재 충남대학교 정보통신공학부 교수
<관심분야> 무선/이동 QoS, 무선 멀티케스트