

무선 이기종망에서 무선랜의 선인증 최적화 기법

서성훈, 백재중, 이종협, 송주석
연세대학교 컴퓨터과학과

e-mail : {hoon, jib27, jhlee, jssong}@emerald.yonsei.ac.kr

An Optimized Pre-authentication Mechanism in WLAN-enabled Heterogeneous Wireless Networks

SungHoon Seo, JaeJong Back, JongHyup Lee, and JooSeok Song
Department of Computer Science, Yonsei University

요 약

본 연구에서는 무선 이기종망 환경에서 운용되는 듀얼모드 단말이 현재의 연결을 무선랜으로 변경하는 경우에 필요한 선인증 과정의 최적화 기법을 제안한다. 제안된 인증 기법은 빠른 채널 변경 기술을 MAC(Media Access Control) 기능에 적용하여 현재 활성화된 패킷 데이터 통신에 손실을 최소화 하고 핸드오프 과정에서 발생할 수 있는 인증 과정에 필요한 지연시간을 단축한다. 또한 시뮬레이션 실험을 통하여, 기존에 제안된 전통적인 인증 방법을 사용하는 일반적인 방식 보다 빠른 핸드오프를 수행하여 끊김없는 연결성을 보장함을 보인다.

1. 서론

최근 다양한 형태의 무선 접속망의 발전에 힘입어 다양한 형태의 듀얼모드 단말이 출현되고 있다. 일반적인 형태의 듀얼모드 단말은 현재 망 상황에 따라서 접속망을 선택하고 이를 통하여 끊김없는 데이터 통신을 가능하게 한다. 이와 같이 무선 이기종망 사이에서 연속적인 통신을 가능하게 하는 기술을 수직적 핸드오프(Vertical Handoff)라 칭한다.

수직적 핸드오프를 지원하기 위한 표준화를 위하여 IEEE 802.21 Media Independent Handoff (MIH)와 3GPP 진영의 UMA (Unlicensed Mobile Access)/VCC (Voice Call Continuity)와 같은 기술들을 선보이고 있다[1][2][3]. 한편 언급된 기술들을 기반으로 한 실제 상품화를 통해 이미 다양한 서비스를 제공하고 있다.

수직적 핸드오프를 수행하는 경우 반드시 수반되어야 하는 과정중에서 인증 과정은 이종망 사이에서 합법적인 사용자를 판단하기 위한 중요한 단계이다. 특히 듀얼모드 단말이 IEEE 802.11 무선랜 (WLAN: Wireless Local Area Network)의 핫스팟 영역으로 핸드오프를 수행하는 경우, 전체 핸드오프 수행 단계의 부분으로서 인증 처리에 소요되는 시간은 탐색 및 스캔 과정과 비교하여 미묘할 정도로 적게 걸린다. 하지만 인증 과정은 반드시 현재 활성화된 연결을 끊고 새로 수행(break-before-make)되어야 하므로 제공받고 있는 서비스에 대한 단절이 발생할 수 있다.

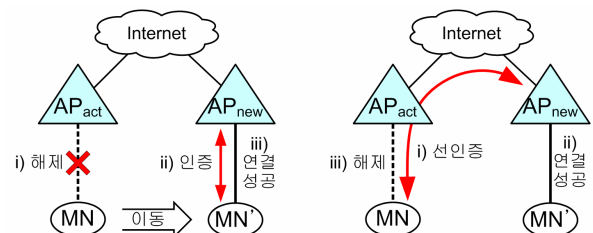
본 연구에서는 현재 활성화된 연결의 서비스 단절을 최소화 할 수 있는 최적화된 선인증 기법(OPA: Optimized Pre-Authentication)을 제안한다. 제안된 OPA

기법은 무선랜 네트워크 인터페이스 카드에 적용되는 MAC(Media Access Control) 기능의 수정을 통하여 빠른 채널 변경이 가능토록 하여 현재 활성화된 연결중에 다른 AP(Access Point)로의 선인증이 가능하도록 한다. 특히 제안된 기법은 듀얼모드 단말 상의 MAC 만을 수정하여 운용이 가능하므로 AP 에 탑재되어야 하는 소프트웨어 변경없이 운용이 가능하므로, 이미 전세계적으로 많은수가 배치된 AP 를 그대로 사용할 수 있는 기술이다. 또한, 수직적 핸드오프를 위한 기술로 제안하고 있으나, 동일한 망에서 수행되는 수평적 핸드오프를 위한 기술로서 활용할 수 있고, 인증 메커니즘에 투명성을 제공할 수 있다.

2. OPA (Optimized Pre-Authentication) 기법

가. 기존 연구

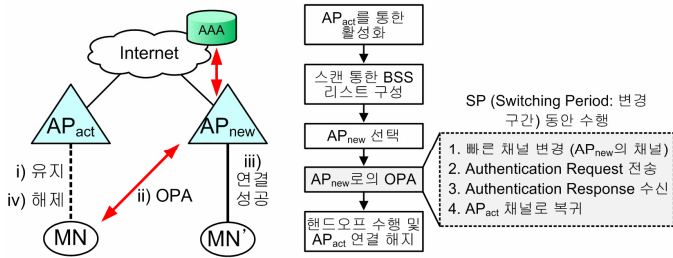
그림 1-(가)는 무선랜 환경에서 일반적인 사용되는 인증방식에 대한 도식이다. 단말(MN: Mobile Node)은 현재 AP_{act} 를 통해 활성화 되어있는 상황이고 AP_{new} 로 접속점 변경을 시도한다. 인증 시도는 AP_{act} 를 통해 활성화 되어 있는 연결을 해지하고 시도를 해야한다. 인증이 완료된 후 새로운 위치의 단말(MN')은 연결에 성공한다. 이 방식은 인증 수행에 앞서 반드시



(가) 일반적 인증 과정

(나) 선인증 과정

(그림 1) 기존 인증 방식



(그림 2) 제안된 OPA 기법의 인증 과정 및 흐름도

수행하여야 하는 탐색 과정으로 인해 핸드오프 지연 시간 측면에서 비효율적이다. 반면 IEEE 802.11i의 선인증 기법[4]은 활성화된 연결을 통하여 핸드오프로 이동하게 될 AP_{new}에 대한 인증을 수행한다(그림 1-(나)). 이 방식은 일반적인 방식에 비해 높은 연결성을 보장할 수 있으나 모든 AP들에 대한 프로토콜을 수정해야 하므로 비용측면에서 비효율적이다.

나. 제안된 기법의 동작

OPA는 선인증 과정의 최적화를 통해 빠른 수직적 핸드오프 지원은 물론 현재 활성화된 연결에 대한 서비스 단절을 최소화 할 수 있다. 그림 2에서와 같이 OPA의 수행 과정은 다음과 같이 요약된다. i) AP_{act}를 통해 활성화된 모든 연결을 그대로 유지된다. 그와 동시에 단말은 주변 AP에 대한 BSS (Basic Service Set) 리스트를 탐색에 의해 구성하고, 핸드오프를 통해 이동하게 될 AP_{new}를 결정한다. ii) OPA를 수행한다. OPA 과정은 빠른 채널 변경 기법을 통해 현재 채널을 AP_{new}에 설정된 채널로 전환하여 인증 요청 프레임(Authentication Request)을 전송한다. AP_{new}로부터 인증 응답(Authentication Response) 관리 프레임을 수신하고 다시 이전의 채널(AP_{act})로 복귀한다. 이때 OPA는 SP(Switching Period) 동안 지속되는데 그동안에 인증 응답을 받지 못하는 경우 OPA를 위한 채널 변경 및 복귀 과정을 여러번에 걸쳐 수행하도록 확장 가능하다. iii) 최종적으로 인증에 성공하고, iv) 기존 연결을 해제함으로써 수직적 핸드오프 과정이 완료된다.

3. 성능 평가

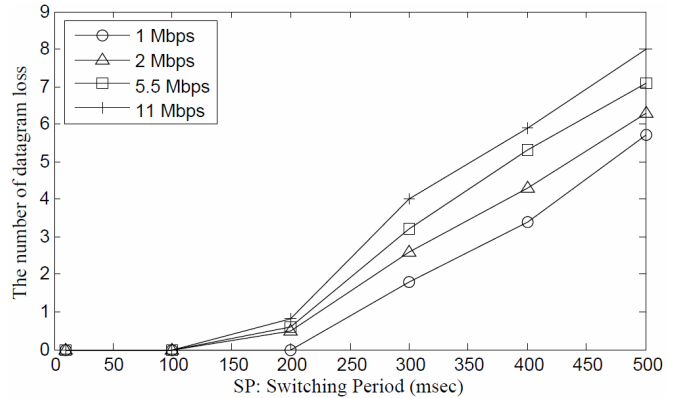
제안한 기법의 성능을 평가하기 위하여 시뮬레이션을 통하여 일반적인 인증 및 선인증 기법과 비교한다. 평가의 지표로서 SP의 영향과 핸드오프 지연시간을 사용한다.

가. 시뮬레이션 환경

802.11b를 지원하는 단말은 새로운 AP로의 핸드오프과정으로써 탐색 및 인증, 그리고 association 과정을 수행하여야 한다. AP에 설정된 채널 간섭은 없고, 설정된 채널 속도는 1, 2, 5.5, 그리고 11 Mbps로 변화시키고 측정을 기반으로 한 인증 시간 및 핸드오프 지연시간[5]을 기반으로 시뮬레이션을 수행한다.

나. 결과

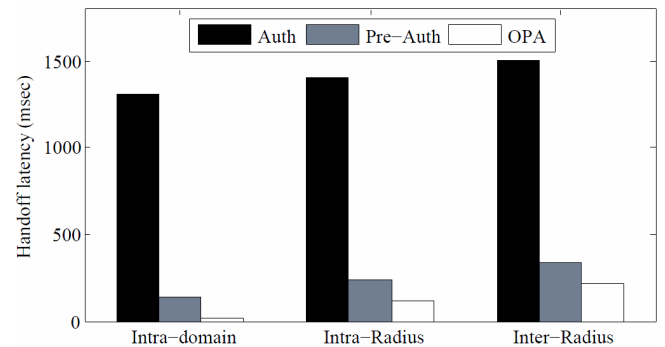
그림 3은 SP의 변화에 따른 데이터 손실량을 나타내고 있다. 모든 AP의 채널 속도에 대하여 SP가 증가할수록 데이터 손실도 증가함을 확인할 수 있다. 100 msec 이하의 SP를 사용하면 현재 활성화된 AP



(그림 3) SP에 따른 데이터 손실량

를 통한 데이터 전송 서비스 단절은 최소화된다.

두번째 시뮬레이션 결과로써 그림 4는 인증서버(Radius)의 위치에 따른 핸드오프 수행에 소요되는 각 기법들의 지연시간을 보인다. 탐색과정을 반드시 수행해야하는 일반적인 인증 방식은 모든 경우에 가장 긴 핸드오프 지연시간을 필요로 한다. 제안한 OPA 기법은 일반적인 인증 및 선인증 기법보다 평균적으로 각각 11.7%와 1.9% 빠른 핸드오프 수행이 가능하다.



(그림 4) 인증서버 위치에 따른 핸드오프 지연시간

4. 결론

본 연구에서 제안된 최적화된 선인증 기법은 활성화된 연결을 통한 서비스 단절을 최소화 하고 빠른 수직적 핸드오프를 가능하게 한다. 제안된 OPA 기법은 일반적인 인증 및 선인증 기법과 비교하여 빠른 핸드오프 수행이 가능함을 시뮬레이션을 통해 보였다.

참고문헌

- [1] Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services, IEEE Std. 802.21, Jun. 2008.
- [2] 3GPP TS 44.318, "Generic Access Network (GAN); Mobile GAN interface layer 3 specification," Dec. 2008.
- [3] 3GPP TS 23.206, "Voice Call Continuity (VCC) between Circuit Switched (CS) and IP Multimedia Subsystem (IMS)," Dec. 2007.
- [4] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: MAC Security Enhancements, IEEE Std 802.11i/D4.1, Jul. 2003.
- [5] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," SIGCOMM, Vol. 33, No. 2, pp. 93-102, 2003.