논문 2007-44TC-10-23

IEEE 802.11 무선랜에서 고속 이동성 지원을 위한 사용자 사전 인증 기법

(User Pre-Authentication Method for Support of Fast Mobility in IEEE 802.11 Wireless LAN)

권 정 호*, 박 종 태*

(Jung-Ho Kwon and Jong-Tae Park)

요 약

IEEE 802.11 기반의 무선랜 시스템이 초고속 무선 네트워크의 기반구조로 자리 잡아감에 따라 무선단말의 보안성과 이동성에 대한 관심이 날로 증가되고 있다. 그러나 IEEE 802.11i 보안표준을 준수하는 무선단말의 경우 보안성 강화를 위한 IEEE 802.1x 사용자 인증절차를 수행함으로써, 지연이 발생하여 실시간 멀티미디어 서비스에 적합하지 않다. 본 논문에서는 이러한 문제를 해결하기 위한 고속 사용자인증 방법을 제안하고 성능분석을 통해 이를 검증하였다. 무선 단말은 핸드오프 시 사용자 인증을 정상적으로 처리해 줄 수 있는 신뢰성 있는 액세스포인트 정보를 제공하고 이를 기반으로 선택적인 액세스포인트들에 대한 사전인증을 수행함으로써 고속 사용자인증을 가능하게 한다. 또한, 사전인증을 위해 분배된 액세스포인트 내의 단말의 인증정보를 단말의 핸드오프 상황에 따라 효과적으로 관리함으로써 장시간 단말의 인증정보가 노출되는 문제점을 해결하였다.

Abstract

As the IEEE 802.11 WLAN has widely installed as a high-speed wireless network information infrastructure, there has been growing interest in both security and mobility of mobile terminals. However, for the case of mobile terminal employing IEEE 802.11i security standard, it is known that the user authentication procedure of IEEE 802.1x for stronger security enforcement may, due to its large delay, not be suitable for real-time multimedia communication. In this paper, we have proposed fast authentication method to resolve the above authentication delay problem, and verifies its peformance via simulation analysis. Mobile terminals can get AP information reliably, and selectively execute authentication in advance during handover, which results in fast user authentication. In addition, by effectively managing the authentication information in mobile terminal, which are distributed in advance for pre-authentication, the problem of long-time revelation of authentication information has been solved.

Keywords: IEEE 802.11, 무선랜, 고속이동성, 사전인증

I. 서 론

최근 IEEE 802.11 기반의 무선랜 시스템은 단말에 대한 원활한 이동성 지원, 확장성 있는 네트워크 구축 및 유선랜에 버금가는 고속의 전송속도를 지원하여 초고속 무선 네트워크의 기반 구조로 자리 잡아가고 있다[1]. 그러나 이러한 장점에도 불구하고 취약한 보안문제와 이동성으로 인한 문제는 무선랜 시스템의 저변 확대를 가로막고 있다. 무선랜의 모든 데이터는 공중 매체를 통하여 브로드캐스트 되므로 쉽게 도청될 수 있으며 시스템 수준의 취약한 보안인증으로 인해 쉽게 네트워크에 접속할 수 있는 가능성이 있다. 또한 단말의 이동과 핸드오프로 인해 발생하는 지연시간은 VoIP와 같은 실시간 멀티미디어 서비스에 적합하지 않다[2~3].

이러한 무선랜 시스템의 단점을 보완하기 위한 노력

* 정회원, 경북대학교 전자전기컴퓨터학부
(School of Electrical Engineering and Computer Science, Kyungpook National University)
※ 이 논문은 2007년도 경북대학교 연구교수 연구비의 지원을 받아 수행된 연구입니다.
접수일자: 2007년2월6일, 수정완료일: 2007년10월12일

으로 IEEE 802.11i TG는 국제 무선랜 보안표준을 제정하였다[4]. IEEE 802.11i는 IEEE 802.1x 기반의 사용자 인증방식, 동적 키 교환방식 및 단말과 액세스포인트 사이의 무선구간에서의 강력한 암호 알고리즘을 사용함으로써 상위 사용자 레벨의 보안인증 및 사용자 데이터에 대한 안전성을 제공해주고 있다. 하지만 단말의 매 핸드오프 시 마다 IEEE 802.11i 보안 절차에 따라 IEEE 802.1x 사용자 인증절차를 수행하기 때문에, 이로 인한 지연시간은 끊김없는 실시간 멀티미디어 서비스를 제공하는데 문제점으로 여전히 남아 있다. IEEE 802.11i TG에서는 키 캐싱(Key Caching)과 사전인증(Pre-authentication) 기능을 옵션으로 제안하고 있으며, IEEE 802.11f TG에서는 IAPP(Inter Access Point Protocol)을 활용하여 단말의 컨텍스트 정보를 교환함으로써 핸드오프 시 사용자 인증에 걸리는 지연시간을 줄일 수 있는 방법을 제시하고 있다[5]. 이외에도 전 세계적으로 사용자인증에 걸리는 지연시간을 단축시키기 위한 고속 사용자인증 방법에 관한 많은 연구들이 진행되어 오고 있다[6~8]. 하지만 고속의 사용자인증을 제공함에 있어 IEEE 802.11i 표준의 사전인증방법이나 현재 연구되어 온 방법들은 각기 인증서버의 과부하, 제약적 범위에서의 사용, 무선 네트워크 구성요소들 간의 신뢰성 결여 및 사용자 인증정보 관리 등의 부분에 대한 문제점들을 드러내고 있다.

본 논문에서는 IEEE 802.11 기반 무선랜 시스템에서 보안을 제공하며, 동시에 핸드오프 시 단말의 사용자인증처리로 인한 지연시간을 줄일 수 있는 고속 사용자인증 방법을 제시한다. 구체적으로, 단말의 정상적인 사용자인증 처리를 해줄 수 있는 액세스포인트들이 위치한 도메인에 상호 로밍협약(Roaming Agreement)이 맺어져 있지 않은 RADIUS 인증서버의 관리 도메인이 겹쳐져 있다고 가정할 때, 단말은 주변의 액세스포인트들 중 정상적으로 사용자인증 관련 메시지를 해당 RADIUS 인증서버로 중계해줄 수 있는 신뢰성 있는 액세스포인트들의 정보를 획득하는 과정이 필요하다. 이에 제안된 구조에서는 단말의 추가적인 스캐닝 과정을 통해 얻어진 주변의 액세스포인트 정보를 기반으로 RADIUS 인증서버에서 신뢰성 있는 액세스포인트 정보를 필터링 해주는 방법을 제안한다. 또한 이러한 신뢰성 있는 액세스포인트 정보를 기반으로 해당 액세스포인트들에 대해서만 단말의 사전인증을 수행함으로써 다른 불필요한 액세스포인트들로도 사전인증이 되는 리소스 낭비를 최소화하였다. 이렇게 사전인증을 수행한 액세스포인트로 단말이 접속하게 되면 상호 간 캐쉬되어 있는 단말의 인증정보의 유무만을 체크한 후 완전 사용자인증절차(Full user authentication procedure with IEEE 802.1x)를 생략하게 되므로 사용자인증에 걸리는 시간을 크게 단축시킬 수 있게 된다. 또한 사전인증을 수행하기 위해 액세스포인트에 캐쉬되어 있는 단말의 인증정보를 효과적으로 관리함으로써 단말의 인증정보가 장시간 노출되지 않도록 관리할 수 있는 방법을 제공한다.

본 논문의 Ⅱ장에서는 기존의 관련연구를 살펴보고, 비교 및 분석하였으며 Ⅲ장에서는 고속 사용자인증을 지원함에 있어서의 요구사항을 기술하고 이에 적합한 구조를 제안한다. Ⅳ장에서는 본 논문에서 제안하는 고속 사용자인증 방법에 대한 성능분석 결과를 보여주며 Ⅴ장에서 결론을 맺는다.

Ⅱ. 보안성 있는 고속 핸드오프 기술 비교 분석

무선랜 환경에서 빈번하게 발생하는 핸드오프 때마다 사용자 인증보안을 목적으로 IEEE 802.1x 사용자인증 절차를 수행한다면, 이를 처리하기 위한 지연시간은 실시간 멀티미디어 서비스 제공에 상당한 영향을 끼치게 된다. 이에 본 절에서는 핸드오프 시 사용자인증을 고속으로 지원하기 위한 관련연구를 알아본다.

IEEE 802.11i 보안표준에서는 단말의 고속 로밍지원을 위한 옵션기능으로서 키 캐싱과 사전인증 방법을 제안하고 있다[4]. 키 캐싱이란 단말과 인증서버 간 상호인증으로 생성된 PMK(Pairwise Master Key)를 단말과 액세스포인트가 지속적으로 캐쉬하며 재사용함으로써 향후 단말이 이전 접속했던 경험이 있는 액세스포인트로 다시 재접속을 시도할 경우 캐쉬된 PMK 정보의 유무만을 판단하여 사용자인증 절차를 마무리하는 방법이다. 사전인증은 이러한 키 캐싱을 기반으로 단말이 현재 접속된 액세스포인트를 통해 향후 핸드오프 할 액세스포인트들(Target AP)에 대해 사전에 사용자인증을 시도하는 방법이다. 이렇게 사전인증을 수행하게 되면 단말의 신호 영역(signal coverage) 영역 이외의 액세스포인트에 대해서도 사전인증이 가능한 장점이 있다. 하지만, 현재 접속한 액세스포인트를 통하여 일반 완전인증절차를 수행하게 됨으로 단말의 수, 혹은 단말이 사전인증을 시도할 액세스포인트의 수에 따라 단말, 액세스포인트, 그리고 인증서버에 대량의 부하를 발생시킬 수 있다.

Park 등은 FHR(Frequent Handoff Region)이라 정의하는 단말의 핸드오프 가능 영역을 기반으로 단말의 인증정보를 FHR 영역 내의 모든 액세스포인트들에게 전달하여 사전인증을 수행하는 방법을 제안하였다[6]. 이러한 FHR 영역은 단말의 행동패턴 및 무선 네트워크 환경에 설치되어 있는 액세스포인트들의 물리적 환경요소 등을 기반으로 만들어지며 상시 단말의 핸드오프 이벤트가 발생할 때마다 Event logging 데이터베이스 시스템에서 이를 수집하고 FHR 영역생성에 반영하게 된다. 이렇게 FHR 영역을 기반으로 한 고속 사용자인증 방법은 IEEE 802.11i 사전인증 방법과 비교할 때 단말이나 액세스포인트에 대한 부하가 작고 단말이 향후 핸드오프 할 액세스포인트에 대한 사전인증에 직접적으로 관여하지 않아도 되는 장점이 있다. 하지만 단말의 핸드오프 이벤트가 발생할 때마다 이를 중앙 데이터베이스 시스템에서 매번 수집하고 처리해야 하므로 서버에 대한 부하가 커질 수 있으며 FHR 영역 이외의 액세스포인트에 단말이 핸드오프하게 되면 고속 사용자 인증기능을 제공할 수 없는 단점이 있다.

Mishra 등은 NG(Neighbor Graph)라 불리는 단말이 향후 접속을 시도할 가능성이 있는 후보 액세스포인트들을 선정하여 단말의 인증정보를 분배하는 사전 키 분배(Proactive Key Distribution) 방법을 제안하였다[7]. 이는 FHR 기법과 유사한 방법이기는 하지만 NG 영역 내의 액세스포인트들은 한 단말의 사전인증을 위해 분배된 키를 서로 다른 형태로 보유하고 있으므로 동일한 인증정보를 가지는 위험성을 제거하였다. 하지만 사용자의 인증정보를 한 홉 단위 거리의 액세스포인트들에 대해서만 분배되며 FHR 기법과 동일하게 NG 영역 이외의 액세스포인트로 단말이 핸드오프하게 되면 고속 사용자 인증기능을 제공할 수 없는 단점이 있다.

Mishra 등은 IEEE 802.11f에서 정의하는 기존의 IAPP 프로토콜을 확장시켜 액세스포인트들 간에 사용자의 인증정보가 담긴 컨텍스트 정보를 교환하고 캐쉬함으로써 고속 사용자인증을 지원하는 방법을 제안하였다[8]. 기존의 방법과는 달리 액세스포인트를 중심으로 인증정보가 분배되고 관리되므로 기존의 인증서버에 걸리는 과부하를 막을 수 있는 장점이 있다. 하지만 액세스포인트들 간의 인증정보의 분배가 이루어지므로 Layer 3 핸드오프에서는 사용할 수 없으며 사전 키 분배 방법과 동일하게 한 홉 단위의 모든 액세스포인트들에 대해 인증정보가 분배되어지므로 불필요한 시그널링 오버헤드가 발생할 수 있는 단점이 있다.

다음의 표 1은 앞서 언급한 관련연구에 대한 비교분석표이다. 관련연구 분석을 통하여 모든 방법(Approach)들은 사전인증을 통하여 단말에 대한 고속

표 1. 보안성 있는 고속 사전 인증 방법 비교
Table 1. Comparison of fast pre-authentication method.

특징	802.11i 사전인증	FHR	PKD	PNC
단말인증 정보전달	인증서버	인증서버	AP	AP
인증정보 관리	No	Weak (Timer)	No	Yes (Message)
L3 핸드오프	Yes	Yes	Yes	No
단말의 사전인증 AP인지	Yes	No	No	No
장점	표준프로토콜 사용 사전 인증 AP 임의선택 가능	단말 핸드오프 지역에 대한 사전인지 시그널링 오버헤드 적음	단말 핸드오프 지역에 대한 사전인지 동일 인증정보 보유하지 않음	핸드오프 지역에 대한 사전 인지 인증서버 부하적음 효율적 단말 인증 정보 관리
단점	완전인증을 통한 사전인증 방식 단말, AP, AS 부하증가 인증정보관리 기능 없음	서버 부담증가 인증정보관리 기능 약함 단말에서 사전 인증된 AP정보 없음	사전인증을 현재 AP기준의 한 홉 단위 수행 인증정보관리 기능 없음 단말에서 사전 인증된 AP정보 없음	시그널링 오버헤드 큼 사전인증을 현재 AP 기준의 한 홉 단위 수행 단말에서 사전 인증된 AP정보 없음

사용자인증을 지원할 수 있다는 것을 알았다. 고속 사용자인증 지원에 있어 단말에 대해 사전 인증된 확실한 액세스포인트 정보를 제공한다면 그렇지 않은 액세스포인트들로 핸드오프 할 문제점을 해결할 수 있으며, Layer 3 핸드오프를 고려하여 RADIUS 인증서버 기반의 사전인증 방식을 수행해야 한다. 마지막으로 사전인증을 위해 분배된 단말의 인증정보를 지속적으로 노출시키는 문제점을 해결하기 위해 단말의 핸드오프 상황에 맞게 인증정보를 효과적으로 관리할 수 있는 방법이 제시되어야 한다.

Ⅲ. 고속 사용자인증 지원을 위한 요구사항 분석

일반적으로 단말은 현재 접속되어 있는 액세스포인트와의 신호강도가 일정 이하로 떨어지게 되면 다음 액세스포인트로의 핸드오프 과정을 준비하게 된다. 이 때 단말은 향후 핸드오프 할 대상의 액세스포인트를 선택하기 위하여 스캐닝 과정을 통해 주변의 액세스포인트 정보를 수집하고 이들 중 적합한 액세스포인트를 선택하여 접속을 시도하게 된다. 단말의 스캐닝 과정을 통해 얻어진 액세스포인트의 정보들은 무선랜 환경에서 액세스포인트가 설치된 물리적 환경이나 액세스포인트의 신호강도 등의 외부적인 요인에 영향을 끼치게 된다[9]. 단말이 현재 접속한 액세스포인트를 기준으로 주위에 다른 인증서버가 관리하는 영역의 액세스포인트들이 해당 영역에 물리적으로 인접해 있거나 거리 상 충분히 떨어져 있지만 이들 액세스포인트들의 신호강도가 상대적으로 세다고 가정한다. 이 경우에는 단말이 자신의 사용자인증을 정상적으로 처리할 수 있는 영역의 올바른 액세스포인트로 핸드오프 하는데 영향을 끼칠 수 있다. 또한 불법 액세스포인트(Rouge AP)들은 굉장히 센 신호를 송출하여 단말에 대해 가장 인접한 액세스포인트로 착각을 일으켜 단말의 접속을 유도시키고 사용자의 데이터를 해킹할 수 있는 상황이 벌어질 수도 있다. 그림 1은 이러한 상황에 대한 문제점을 나타내고 있다.

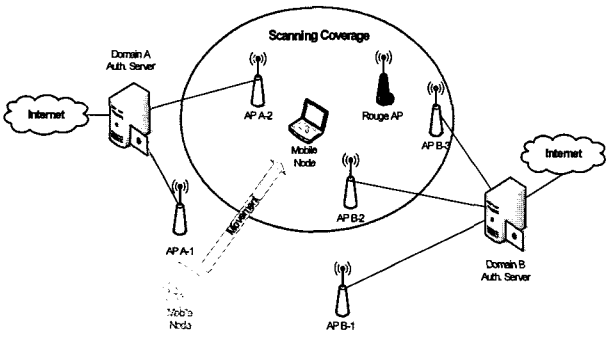


그림 1. 스캐닝 과정의 문제점
Fig. 1. Problem in scanning procedure.

앞서 기술한 바와 같이 한 지역 내에 영역 A의 액세스포인트들과 영역 B의 액세스포인트들이 산재되어 배치되어 있거나 상호 영역의 중첩영역에 단말이 위치해 있는 경우, 혹은 주변에 불법 액세스포인트가 설치되어 있는 환경이라고 가정한다. 초기 단말은 접속되어 있는 액세스포인트 A-1에서 이동함에 따라 핸드오프의 초기 단계로 스캐닝 과정을 수행하게 된다. 이 때 스캐닝 과정을 통해 얻어진 결과에 영역 B의 액세스포인트들과 불법 액세스포인트의 정보가 포함되어 있다고 가정한다. 영역 A와 영역 B의 인증서버들 간의 로밍 협약이 유효하다면 단말의 영역 B의 액세스포인트로 핸드오프를 하여도 정상적으로 사용자인증을 수행하며 접속이 가능하지만 그렇지 않은 경우에는 접속불가 결과를 통보받고 다음 액세스포인트로 핸드오프를 수행하기 까지는 걸리는 지연시간이 발생하게 된다[10]. 또한 불법 액세스포인트로 핸드오프를 하게 된다면 보안상 큰 문제가 생길 수 있게 된다. 이렇게 액세스포인트로의 핸드오프 시도가 잘못될 경우 인증에 실패하게 되며 최악의 경우 스캐닝 과정을 통해 수집된 영역 B의 인증서버 내 모든 액세스포인트들에 대해 인증을 시도하게 된다면 상당한 지연시간 및 이에 따른 데이터 손실이 발생하게 된다. 만약 단말의 사용자 인증방식에 있어 EAP-TLS 방식을 사용하는 경우 해당 액세스포인트를 통해 인증서버와 상호인증 시도 후 정상적인 결과를 통보 받는데 최대 1초 이상의 시간이 소요된다[11]. 이렇게 단말의 스캐닝 과정을 통해 수집된 액세스포인트 정보들을 기반으로 부적절한 액세스포인트로 핸드오프로 인해 생기는 지연시간과 데이터 손실은 실시간 멀티미디어 서비스를 제공하는데 상당한 문제점을 야기시킬 수 있다. 이에 단말의 스캐닝 과정을 통해 수집된 액세스포인트 정보들 중 단말이 향후 정상적으로 핸드오프를 수행할 수 있는 신뢰성 있는 액세스포인트 정보를 단말에 제공하는 것이 필요하다.

앞서 관련연구의 분석을 통해 대부분의 연구들은 고속 사용자인증 처리를 위해 향후 단말이 핸드오프 할 대상의 액세스포인트들에 미리 사전인증을 수행하여 단말이 접속했을 때 간단한 절차만을 거쳐 사용자 인증절차에 소요되는 지연시간을 줄이는 방식들이라는 것을 알 수 있다. 하지만 IEEE 802.11i 사전인증은 단말이 직접 주체가 되어 현재 접속한 액세스포인트를 통해 다음

액세스포인트에 대한 사전인증을 수행해야 하며 동일한 사용자인증절차를 따르고 있으므로 시그널링 오버헤드가 크다. 이를 개선하기 위해 사전인증 수행에 있어 구성요소들에 대한 부하를 줄이면서 적은 메시지 교환을 통해 동일한 성능을 가지는 여러 가지 연구들이 제안되었다. 이들 연구들은 단말의 핸드오프 가능 액세스포인트들을 단말의 행동패턴이나 액세스포인트의 배치환경 등의 조건들을 수집하고 처리한 후 확률적으로 계산하여 사전인증을 수행하게 된다. 하지만 단말이 예외적으로 사전인증 되지 않은 액세스포인트로 핸드오프를 수행하게 되면 사전인증을 통한 장점을 사릴 수 없게 된다. 이에 단말의 실질적인 핸드오프 정보를 통하여 선택적인 액세스포인트들에 대해서 사전인증을 수행하는 방법이 필요하다.

다른 고려사항은 사전인증을 위해 분배해 놓은 단말의 인증정보를 캐쉬하고 있는 액세스포인트들에 대해서 단말의 인증정보를 지속적으로 가짐으로써 장시간 인증정보를 노출시키는 문제가 발생한다. IEEE 802.11i 사전인증에서는 기본적으로 액세스포인트가 단말의 인증정보를 가지는 규정시간인 PMK Lifetime이라고 부르는 타이머를 동작시켜 만료시간 이후에는 단말의 인증정보를 파기시키는 방법을 활용하고 있다. 하지만 타이머를 활용한 인증정보 관리는 비효율적이므로 단말의 모빌리티 상황에 맞추어 효율적으로 인증정보를 관리하는 방법이 필요하다.

Ⅳ. 고속 사용자인증 지원을 위한 제안구조

본 논문에서 제안하는 고속 사용자 인증기법은 위의 요구사항을 해결하기 위해 3가지의 주요기능을 제공한다. 단말에 정상적인 사용자인증을 지원하는 액세스포인트로의 핸드오프를 위한 정보제공, 단말의 실질적인 핸드오프가 가능한 선택적인 액세스포인트들에 대한 사전인증, 마지막으로 단말의 모빌리티 상황에 따른 효율

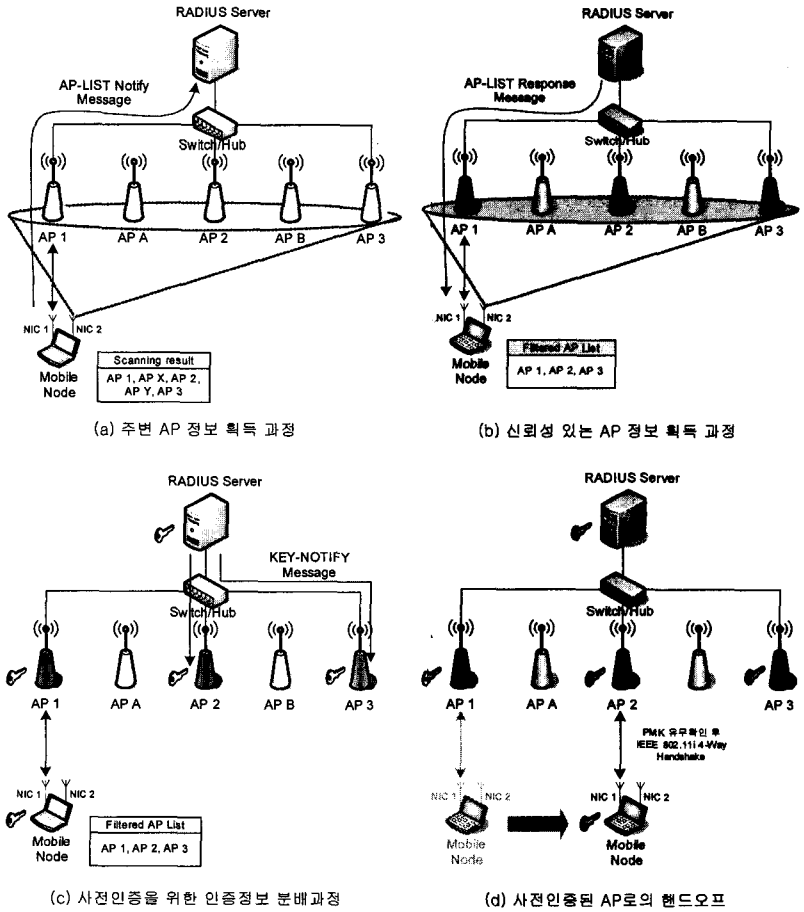
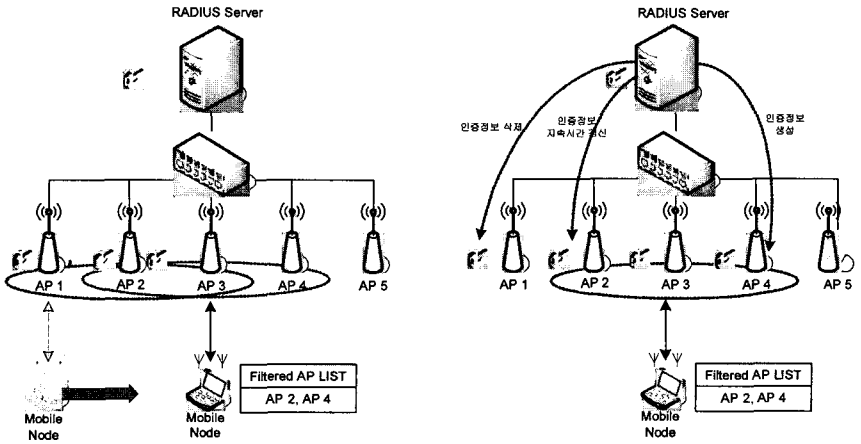


그림 2. 신뢰성 AP 정보기반의 고속 사용자인증 지원과정
Fig. 2. Fast user authentication procedure based on reliable AP information.

적인 단말의 인증정보 관리 기능을 제공한다.

최초 단말은 AP1에 접속되어 있는 상황에서 향후 핸드오프 하여 정상적으로 사용자인증 처리가 가능한 신뢰성 있는 액세스포인트의 정보를 획득하기 위하여 별도의 추가 스캐닝 과정을 수행하기 위하여 별도의 NIC를 동작시킨다. 이렇게 별도의 NIC를 활용하는 이유는 현재 AP1과 접속한 NIC를 통해 스캐닝 과정을 수행하게 되면 이 과정 중에는 정상적인 데이터 통신이 가능하지 않기 때문이다. 이렇게 스캐닝 과정을 통해 얻어진 액세스포인트 정보들은 사전 정의한 AP-LIST Notify 메시지에 담아 RADIUS 인증서버로 전송한다. RADIUS 인증서버는 이 메시지를 수신하여 자신의 관할하는 영역의 액세스포인트 정보들과 비교하여 해당 액세스포인트들만을 필터링하여 사전 정의한 AP-LIST Response 메시지에 담아 전송해 주게 된다. 단말은 이러한 AP-LIST Response 메시지 내의 필터링 된 액세스포인트 정보를 기반으로 핸드오프를 수행하게 되므로 RADIUS 인증서버는 이 정보를 기반으로 해당 액세스포인트들에게만 사전인증을 위한 인증정보를 분배함으로써 불필요한 액세스포인트들로도 사전인증을 수행함으로써 생기는 리소스 낭비를 최소화할 수 있다. 이렇게 사전인증 된 액세스포인트로 단말이 핸드오프하게 되면 IEEE 802.11i 키 캐싱 절차와 같이 단말은 핸드오프 과정상에 association request에 자신이 캐쉬하고 있는 PMK의 고유식별자인 PMKID를 포함하여 전송한다. 액세스포인트는 자신의 PMK Cache Entry내에 동일한 PMKID의 존재유무를 확인한 후 이에 대한 동일한 PMKID가 존재한다면 사용자인증절차를 무시하고 IEEE 802.11i 4-Way Handshake 과정을 바로 수행함으로써 사용자인증절차에 걸리는 시간을 단축시킬 수 있다.

그림 3은 사전인증 된 액세스포인트의 PMK Cache Entry에 단말의 인증정보를 단말의 핸드오프 상황에 따라 효율적으로 관리하는 시나리오이다. 최초 단말의 신뢰성 있는 액세스포인트 정보를 기반으로 형성된 사전인증 영역이 AP1, AP2, AP3 이라고 가정한다. 이 때 단말이 AP3로 핸드오프하여 본 논문에서 제안하는 구조에 따라 새로 설정된 사전인증 영역이 AP2, AP3, AP4로 형성되었다고 가정한다. 이 때, 새로 설정된 사전인증 영역과 이전 사전인증 영역을 비교해보면 영역 내에 새로 포함된 액세스포인트, 지속적으로 존재하는 액세스포인트, 마지막으로 제외된 액세스포인트로 구분되어 질 수 있다. 이러한 정보를 바탕으로 RADIUS 인증서버는 해당 액세스포인트들에게 상황에 맞는 사전정의된 KEY-NOTIFY 메시지에 적절한 인증정보 관리 메시지를 담아 전송하게 된다. 즉, RADIUS 인증서버는 단말의 매 핸드오프 시 형성된 사전인증 영역을 유지하고 있다가 단말의 다음 핸드오프로 인해 새롭게 형성된 사전인증 지역을 비교하여 새로 포함된 액세스포인트의 경우는 단말의 인증정보를 포함하여 액세스포인트의 PMK Cache Entry에 저장할 수 있도록 하며, 지속적으로 존재하는 액세스포인트의 경우는 단순히 단말의 PMK Lifetime만을 갱신해주도록 한다. 마지막으로 제외된 액세스포인트의 경우는 해당 단말의 PMK를 삭제



(a) 재접속으로 인한 새로운 사전 인증 영역 (b) 단말의 인증 정보의 관리 메시지 송신

그림 3. 인증정보 관리 절차

Fig. 3. Management procedure of authentication information.

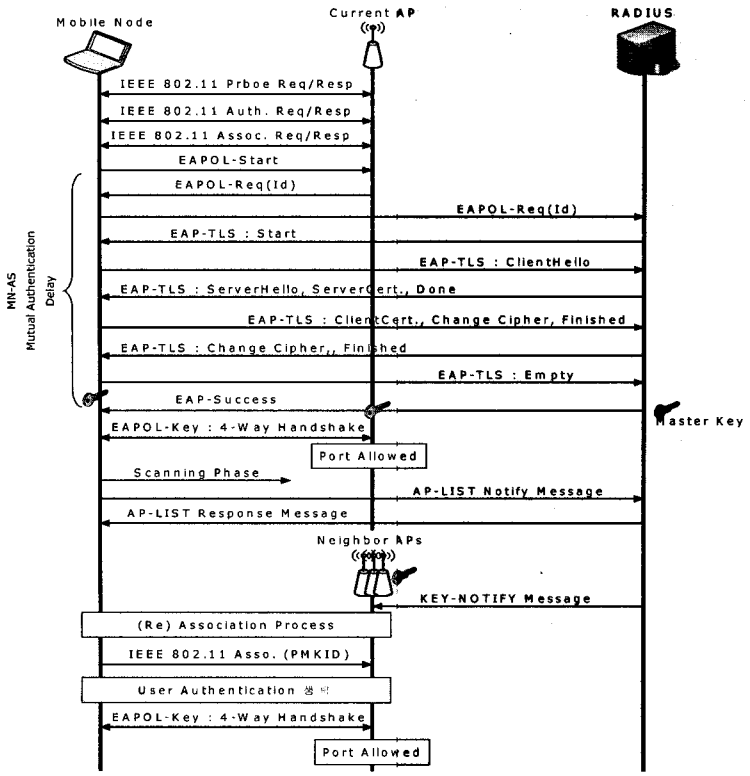


그림 4. 고속 사용자 인증 시스템 전체 메시지 흐름도
Fig. 4. Message flow of fast user authentication system.

시키도록 메시지를 전송하게 된다.

단말이 한 영역 내의 최초 액세스포인트와의 접속은 일반 IEEE 802.11i 보안규정에 따라 IEEE 802.1x 사용자인증절차(일반적으로 EAP-TLS)를 수행한다. 이 때, 단말과 RADIUS 인증서버 간 상호인증을 통하여 인증정보인 마스터 키(Master Key)를 단말, 액세스포인트, 그리고 RADIUS 인증서버가 캐쉬하고 있게 된다. 여기까지는 일반 IEEE 802.11i 기반의 핸드오프 절차를 준수한다. 이 후 단말의 핸드오프의 상황에 신뢰성 있는 액세스포인트의 정보를 단말에게 제공함과 동시에 사전인증을 통해 단말에 고속 사용자인증기능을 지원하기 위한 단계를 수행한다. 단말은 액세스포인트와의 정상적인 접속 이후에 별도의 스캐닝 과정을 거쳐 주변의 액세스포인트 정보를 수집한다. 이러한 액세스포인트 정보는 사전 정의된 AP-LIST Notify 메시지에 담겨 RADIUS 인증서버에 전달되며 RADIUS 인증서버는 자신이 관할하는 영역의 액세스포인트 정보들과 비교하여 필터링 된 정보를 AP-LIST Response 메시지에 포함하여 응답한다. 이 때 필터링 된 액세스포인트 정보들은 단말이 향후 핸드오프 할 대상의 액세스포인트들이 되므로 RADIUS 인증서버는 이러한 정보를 기반으로 해당 액세스포인트들에게 사전인증을 위해 단말의 인증정보인 MK와 기타 단말정보를 포함한 KEY-NOTIFY 메시지를 전송한다. 이를 수신한 액세스포인트들은 MK에서 PMK를 추출하게 되고 추출한 PMK와 자신의 MAC 주소, 그리고 단말의 MAC 주소를 활용하여 단말과 동일한 PMKID를 생성해 낸다.

단말이 AP-LIST Response 메시지를 수신하면 자신의 스캐닝 한 결과에 대해 향후 핸드오프 할 액세스포인트들 중 인증처리를 올바르게 중계해줄 수 있는 액세스포인트 정보를 획득한 것이다. 고속 사용자인증을 수행하기 위해 KEY-NOTIFY 메시지를 수신한 액세스포인트들이 사전인증을 수행한 것과 마찬가지로 단말도 자신의 PMK와 MAC 주소, 그리고 AP-LIST Response 메시지에 담겨 있는 해당 액세스포인트들에 대한 MAC 주소들을 활용하여 향후 핸드오프 지역 내의 액세스포인트들이 가지고 있는 각각의 PMKID를 동일하게 생성해 낸다. 단말과 접속한 액세스포인트간 신호가 일정 임계치 이하로 떨어지게 되면 다음 액세스포인트로 핸드오프를 수행하게 된다. 이 때 단말은 사전인증을 수행해 놓은 액세스포인트에 대한 정보 및 PMK Cache Entry에 각 해당 액세스포인트들 간 동일한 PMK 및 PMKID를 보유하고 있다. 이에 해당 액세스포인트로 핸드오프하게 되면 단말은 해당 액세스포인

트에 대한 PMKID를 Association Request 메시지에 포함하여 전송하게 된다. 이를 수신한 액세스포인트는 자신의 PMK Cache Entry에서 동일한 PMKID의 유무를 체크하게 되고 만약 동일한 PMKID가 존재한다면 사전인증에 성공했음을 알고 IEEE 802.1x 사용자 인증절차를 생략하고 바로 IEEE 802.11i 4-Way Handshake 과정을 수행하게 되는 것이다.

Ⅳ. 성능 분석

본 절에서는 본 논문에서 제안하는 고속 사용자인증 기법을 통하여 실시간 멀티미디어 서비스에서 요구하는 핸드오프 최소 지연시간을 만족하는 지에 대한 성능분석을 실시하였다. 실험에 대한 환경구성은 그림 5와 같다.

본 논문에서 설계한 고속 사용자인증 기법은 EAP-TLS[12]을 기반으로 하고 있으며 시스템 구현을 위해 RADIUS 인증서버의 경우 freeradius.org에서의 FreeRADIUS Server 프로젝트 소스를 기반으로 하고 있으며 액세스포인트와 단말의 경우 hostap.epitest.fi에서 제공하는 hostAP 및 wpa_supplicant 프로젝트 소스를 기반으로 하고 있다.

사용자 인증과정에 소요되는 지연시간을 측정함에 있어 사전인증 된 액세스포인트로의 핸드오프 시 사용자인증에 대한 시간측정은 IEEE 802.1x 사용자인증과정을 생략하게 되므로 시간측정이 불가능하다. 이에 사용자 인증과정의 소요시간을 측정하기 위하여 단말에서의 Association request 메시지를 송신한 시간 이후부터 최종 IEEE 802.11i EAPOL-Key 메시지의 마지막 패킷을 수신하기까지의 시간을 측정하여 비교하였다. 그림 6은 일반 완전인증을 통한 사용자인증과 본 논문에서 제안하는 사전인증 기반의 사용자인증에 걸리는 지연시간을 비교한 것이다.

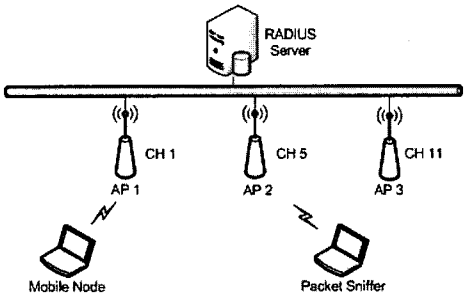


그림 5. 성능 분석을 위한 테스트베드 구축
Fig. 5. Testbed for performance evaluation.

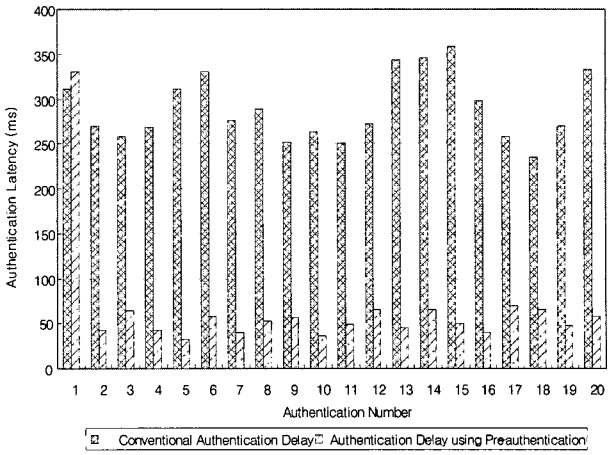


그림 6. 일반 인증과정과 사전인증을 사용한 인증과정 지연시간 비교
Fig. 6. Comparison of latency time between common authentication and pre-authentication procedure.

본 테스트의 결과를 얻기 위하여 일반 802.11i 기반의 핸드오프와 본 논문에서 제안하는 사전인증 기반의 핸드오프를 20회 실시하여 각 핸드오프 시 마다 걸리는 사용자인증 소요시간을 측정하였다. 일반 사용자인증에 걸리는 시간은 매회 핸드오프 시 마다 단말과 RADIUS 인증서버와의 상호인증을 수행하게 되므로 평균 290ms 정도의 시간이 소요됨을 알 수 있었다. 하지만 본 논문에서 제안하는 고속 사용자인증 기법을 적용한 네트워크에서의 소요시간에 대한 결과를 살펴보면 첫 단말의 네트워크 진입 시 일반 핸드오프 상황에서 소요되는 시간과는 동일한 결과를 보인다. 이는 RADIUS 인증서버가 단말에 대한 인증정보를 아직 획득하지 않은 상태이기 때문에 일반적인 인증과정을 피할 수 없기 때문이다. 하지만 이 후 단말의 핸드오프 상황에서는 이미 주변의 액세스포인트들에 대해 단말의 인증정보를 전송하여 사전인증이 수행된 상태이기 때문에 이후 단말의 핸드오프 시 사용자인증을 생략함으로써 사용자인증에 걸리는 시간을 절약할 수 있게 된다. 이렇게 사전인증 된 액세스포인트로의 핸드오프 시 인증과정에 소요되는 시간은 평균 51ms로서 VoIP와 같은 실시간 스트리밍 서비스 제공에 있어 적합한 지연시간을 가질 수 있는 것을 확인할 수 있었다.

Ⅵ. 결 론

단말의 핸드오프 시 보안성 강화를 위한 IEEE 802.11i 보안표준에서의 IEEE 802.1x 사용자 인증절차의 처리시간을 줄이기 위한 기존의 관련연구들은 고속

사용자인증 기능을 제공하는데 있어 인증서버의 과부하, 제한적 범위에서의 사용, 단말의 인증정보 관리부족 등에 대한 단점들이 있다. 이에 본 논문에서는 단말에 핸드오프 시 마다 신뢰성 있는 액세스포인트 정보들을 제공함으로써 단말이 향후 사용자 인증처리를 중계해 줄 수 있는 정상적인 액세스포인트로 핸드오프가 가능하게 하며, 단말의 향후 핸드오프 할 수 있는 실질적인 액세스포인트 정보를 기반으로 선택적인 액세스포인트들만 사전인증을 수행함으로써 불필요한 액세스포인트들로 사전인증 수행에 따른 리소스 낭비를 최소화하게 하였다. 마지막으로 사전인증을 위해 액세스포인트들이 캐쉬하고 있는 단말의 인증정보를 단말의 모빌리티 상황에 맞게 효율적으로 관리함으로써 장시간 단말의 인증정보가 노출되는 문제점을 해결하였다.

실질적인 무선랜 환경에서의 고속의 사용자인증 처리를 지원하기 위해서는 RADIUS 인증서버 간의 로밍 협약을 통해 단말이 다른 영역의 어느 액세스포인트들로 핸드오프를 시도하여도 끊김없는 서비스를 제공해주기 위하여 확장성 있는 사전인증 방법의 연구가 필요하다. 또한 Layer 3 핸드오프와 연계되어 Inter-domain 간 핸드오프 시에도 단말에 대해 고속 사용자인증 처리를 지원할 수 있어야 할 것이다. 이에 본 논문에서 제안하는 Layer 2에서의 고속 사용자인증 기법을 Layer 3 핸드오프 시에서도 원활히 제공할 수 있는 구조로 개선 발전시켜야 할 것이다.

참 고 문 헌

[1] 강유성, 오경희, 정병호, 정교일, "무선랜 보안 표준 IEEE 802.11i," TTA 저널, No. 99, pp. 123~130, May 2005.

[2] C. L. Tan, S. Pink and K. M. Lye, "A Fast Handoff Scheme for Wireless Networks," Proceedings of the 2nd ACM International Workshop on Wireless Mobile Multimedia, pp. 83~90, 1999.

[3] T. Moore and B. Aboba, "Pre-authenticated Fast Handoff," Nov. 2001.

[4] IEEE 802.11i, "Amendment 6 : Medium Access control (MAC) Security Enhancement," April 2004.

[5] IEEE 802.11f, "IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," July 2003.

[6] S. Pack and Y. Choi, "Fast Hanodff Scheme Based on Mobility Prediction in Public Wireless LAN Systems," IEEE Proceedings Communications, Vol. 151, No. 5, pp. 489~495, Oct. 2004.

[7] A. Mishra, M. H. Shin, N. L. Petroni, Jr., T. C. Clancy and W. A. Arbaugh, "Proactive Key Distribution Using Neighbor Graphs," IEEE Wireless Communications, Vol. 11, No. 1, pp. 26~36, Feb. 2004.

[8] A. Mishra, M. H. Shin and W. A. Arbaugh, "Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network," IEEE INFOCOM 2004, No. 1, pp. 351~361, Mar. 2004.

[9] Y. Matsunaga, A. S. Merino, T. Suzuki and Randy H. Katz, "Secure Authentication System for Public WLAN Roaming," Mobile Networks and Applications, Vol. 10. pp. 355~370, Sept. 2003.

[10] Chirs Basios, "Defining Architecture and Key Issues towards WLAN Roaming," The 8th International Conference on Telecommunications 2005, pp. 225~230, June 2005.

[11] B. Aboba, "Fast Handoff Issues," IEEE 802.11-03/155r0, Dec. 2004.

[12] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," RFC 2716, Oct. 1999.

저 자 소 개

권 정 호(정회원)

2005년 대구대학교 통신공학과 학사 졸업.
2007년 경북대학교 전자공학과 석사 졸업.
2007년 LG 전자 근무

<주관심분야 : 이동통신, 보안, 모바일>

박 종 태(정회원)

1971년~1978년 경북대학교 전자공학과 공학사
1979년~1981년 서울대학교 전자공학과 공학석사
1981년~1987년 미국 미시건대학교 전기컴퓨터학과 공학박사
1989년~현재 경북대학교 전자공학과 교수
2000년~2003년 IEEE Technical Committee on Information Infrastructure(TCII) 의장
1988년~1989년 삼성전자 컴퓨터시스템 사업부 수석연구원
1987년~1987년 미국 AT&T Bell 연구소 연구위원
1984년~1987년 미국 CITI 연구원

<주관심분야 : 이동통신, 모바일, 차세대 통신망 운용, 네트워크 보안>