情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

3G-WLAN Interworking 환경에서의 빠른 채널스위칭 기반의 무선랜 선인증 기법*

백 재 종,[1†] 김 효 진,[2] 송 주 석,[1‡]
[1]연세대학교, [2]한국정보통신기술협회(TTA)

A WLAN Pre-Authentication Scheme Based on Fast Channel Switching for 3G-WLAN Interworking*

JaeJong Baek,[1†] HyoJin Kim,[2] JooSeok Song[1‡]
[1]Yonsei University, [2]Telecommunications Technology Association of Korea

요 약

EAP-AKA를 표준인증 메커니즘으로 사용하는 3G-WLAN 상호연동 망에서는 핸드오버 수행 시 마다 인증백터 생성 및 조회 등의 많은 지연시간을 초래하게 된다. 따라서 핸드오버가 자주 발생하는 네트워크 환경에 적합하도록 상호 인증시간을 최소화하고 끊김없는 서비스를 제공하기 위한 효율적인 인증기법이 요구되고 있다. 제안하는 선인증 기법은 WLAN에서 단말기가 수평 핸드오버할 때 연결계층의 빠른 채널 스위칭을 이용하여 다음 액세스포인트와 직접 EAP 인증을 수행토록 함으로써 인증 지연시간을 최소화하는 기법이다. 핸드오버 이전에 인증을 완료하여 인증 지연시간을 최소화하였으며, 전원 절약모드를 사용하여 패킷 손실을 방지하였다. 또한 사용자 단말기의 디바이스 드라이버 수정만 필요함으로써 실제 적용이 용이하다. 제안하는 기법의 성능 분석 및 평가로써 표준 인증기법을 선정하여 패킷 손실 및 인증지연 시간 등을 비교하였으며, 기존 기법보다 약 10 배 정도의 패킷 손실 방지 효율을 보였고, 인증에 소요되는 평균 지연시간을 0.16 msec으로 최소화하는 효과를 기대할 수 있었다.

ABSTRACT

The current trend of the handover authentication delay time is gradually increased according to the interworking between 3G cellular network and WLANs. Therefore, authentication mechanism minimized in delay is required to perform the seamless handover and support the inter-subnet and inter-domain handover. In this paper, we propose a novel pre-authentication scheme based on the fast channel switching which directly performs the authentication with the next access point in advance. In addition, the proposed scheme is efficient in the inter-domain handover and can be easily implemented in current WLANs since it just modifies the client side of user. To analysis and evaluate our scheme, we compare the packet loss ratio and the delay time with the two standard 802.11 authentication schemes. The analytical results show that our scheme is approximate 10 times more effective than the standard schemes in packet loss and the delay time is minimized down to 0.16 msec.

Keywords: pre-authentication, authentication, handover, channel switching, WLAN

접수일(2010년 10월 25일), 수정일(12011년 3월 25일), 게재확정일(2011년 4월 15일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2010-0016161)

† 주저자, jjb27@emerald.yonsei.ac.kr
‡ 교신저자, jssong@emerald.yonsei.ac.kr

I. 서 론

3GPP(the Third Generation Partnership Project)[1]에서 제안된 3G-WLAN(Wireless Local Area Network) 상호연동 망에서는 보완적인 액세스 망으로서 WLAN이 사용되어진다. 이러한 흐름에서 WLAN의 로밍개념이 연결하기 전에 단절(break before make)되는 속성에서 서비스의 연속성을 지원하는 단절 전에 접속(make before break)하는 핸드오버 개념으로 변화되었다. 이처럼 현재 및 미래 네트워크에서 필요로 하는 기술의 요구사항은 경계없는 단말의 이동성을 지원하며 지연시간에 민감한 어플리케이션의 QoS(Quality of Service)을 보장하고, 상호인증 및 데이터 암호화와 같은 보안성 강화에 초점을 두고 있다. 즉, 경계없는 단말의 이동성을 지원하기 위해서는 서브넷 및 도메인 간 핸드오버가 가능해야 하며, 지연시간에 민감한 어플리케이션의 QoS를 보장하기 위해서는 핸드오버를 수행하는 동안 지연되는 시간이 최소가 되는 기법이 필요하다.

기존 핸드오버 최적화 연구[2,3]는 후보 액세스 포인트를 결정하는 스캐닝 단계의 지연시간 단축에 초점을 두었으나, 최근에는 사용자 및 단말을 인증하는 인증단계에서의 지연시간을 단축해야한다는 주장이 제기되고 있다[11]. 최근 무선 이동통신 인프라는 Wi-Fi, 3G/4G(the Forth Generation) 등의 다양한 접속기술이 혼재되어 있어, 홈 네트워크를 넘어 외부 네트워크 간 상이한 인증기술 및 보안 협상 과정 등을 수행해야 한다. 즉, 수평 및 수직 핸드오버를 위한 인증 지연시간이 점차 증가하고 있음을 알 수 있다[4,5]. 이처럼 동종 혹은 이종의 네트워크가 상호 연동되면서 각 네트워크에 대한 단말 및 서비스 인증시간은 전체 핸드오버 지연시간의 주요인으로 작용한다. 한 예로, [표 1] 은 USIM(Universal Subscriber Identity Module) 기반의 3G-WLAN 연동인증 기술의 유형 및 수행하는데 필요한 시그널링 오버헤드를 비교한 표이다[5]. [표 1]에서 보는 바와 같이 802.11 표준 open 인증을 기준으로 볼 때 EAP (Extensible Authenticati-on Protocol, RFC3748)[6]를 사용하는 각 인증 기법들에 대한 시그널링 오버헤드 비율은 4~7.5 배로 급격히 증가하고 있음을 알 수 있다. 서버 혹은 단말에서의 처리시간이 생략된 점을 감안하면 전체 인증 시간은 더욱 증가되어 끊김 없는 핸드오버의 가장 큰 장애요소임을 알 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 소개하며, 3장에서는 빠른 채널 스위칭을 이용한 선인증 기법을 제안하고, 4장에서는 제안한 기법의 평가 및 분석을 기술한다. 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

[표 1] 3G-WLAN 연동시 인증 시그널링 비교

유형	Cost	시그널링 오버헤드 비율 (b=1/2a, a=b), ※ 802.11 open 인증기준
EAP-AKA	9a + 12b	7.5
SIM-based EAP-AKA	5a + 9b	4.75
EAP-UTLS	10a + 10b	7.5
Robust Authentication Protocol	6a + 8b	5
802.11 open 인증	2a	1

※ a: 단말과 AP 사이의 메시지 수,
b: 네트워크 node 사이의 메시지 수

II. 관련 연구

끊김없는 서비스 연속성과 이동성을 제공하기 위해 핸드오버 단계 중 인증과정에 초점을 두어 연구된 사례는 802.11i, 802.11r 표준기술과 MPA(Media-Independent Pre-Authentication) 등이 있다. 먼저 표준기술을 분석하고 진행 중인 MPA를 간단히 소개한다.

2.1 IEEE 802.11 표준 인증 기법

IEEE 802.11 Open 인증은 실질적인 인증기능이 없으며 단말로부터의 인증 요청에 대해 AP는 무조건 인증하는 방식 이다. 선인증 방식은 지원하지 않으며 BSS(Basic Service Set) 간 이동시에는 무조건 연결단절 후 연결하는 방식으로 로밍하게 된다. 즉, 서비스 연속성이나 이동성을 지원하지 않는 개념으로 기본설계가 된 것이다. 반면 IEEE 802.11i 표준기법은 무선랜 사용자 보호를 위하여 사용자 인증 방식, 키 교환 방식, 무선구간 암호화 알고리즘을 정의하였고 선인증 방식의 마스터키 캐쉬 기능을 이용해서 현재 AP를 경유하여 후보 AP(Access Point)에게 인증 컨텍스트 전송을 통해 간접적으로 수행한다. 이후 핸드오버 시에는 4-Way 핸드셰이크 방식을 사용하여

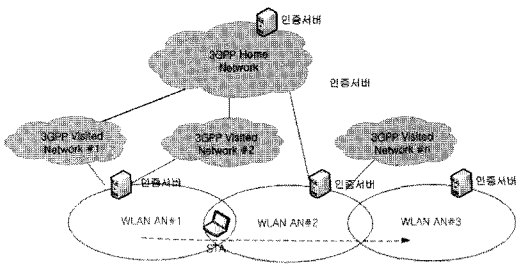
인증시간을 단축하도록 되어 있다. 단점으로는 이러한 선인증을 지원하는 규격의 AP가 필요하며 동일한 서브넷 내에서만 가능하다는 단점이 있다. 즉, ESS (Extended Service Set) 내부에서만 이동성을 지원한다.

802.11r 표준은 모빌리티 도메인 개념을 도입하여 고속 핸드오버 기법을 제공하지만 이동성을 지원하는 도메인, 즉 서브넷 범위를 벗어난 선인증에는 역시 한계가 있어 이종 도메인 및 네트워크 간 선인증을 지원하기 위해서는 추가적인 기법이 필요하다[7].

2.2 MPA

IETF(Internet Engineering Task Force)의 MOBOPTS(Mobility OPTtimizationS) 연구그룹에서 진행 중인 MPA는 현재 Internet-Draft 버전으로 추진되고 있으며 기존 이동성 관리 프로토콜과 이동성 최적화 기법을 동시에 고려하여 도메인 간 핸드오버를 지원한다. MPA는 링크 계층과 독립적으로 동작하며 이동성 관리 프로토콜과 통합되어 지원한다. 즉, 단말의 이동성을 포함하여 어떤 링크 계층(802.11, 802.16 등)에서도 적용될 수 있으며, 다양한 이동성 관리 프로토콜(Mobile IPv4, Mobile IPv6 등)에도 적용될 수 있도록 설계된 핸드오버 최적화 방안으로 제시되었다. 링크 계층(Layer 2 : L2)에서는 선인증(pre-authentication), 네트워크 계층(Layer 3 : L3)에서는 선설정(pre-configuration)을 단계로 구분하고, AA(Authentication Agent), CA(Configuration Agent) 기능을 Access Router에 정의하여 각 계층에서의 지연시간을 최소화하도록 하였다. 또한, PHT(Proactive Handover Tunnel)을 설정으로 핸드오버 중에 발생하는 패킷 손실을 방지하는 방식으로 구성되어 있다. 그러나 현재 표준화가 진행 중인 3GPP-WLAN 구조에 영향을 최소화하는 측면으로 판단해볼 때, MPA 는 기존 시스템에 새로운 구성요소(AA, CA, PHT 등)를 추가하는 비교적 많은 수정이 필요하며, 인증시간을 단축하기 보다는 L2, L3를 모두 고려한 통합 기법 측면에서 의미를 갖는다.

이상의 연구들은 3G-WLAN과 같은 무선 이기종 망에 적용하는데 두 가지 문제점을 가지고 있다. 먼저, 현재의 네트워크나 미래 네트워크 지향적인 측면에서 서브넷, 도메인 간의 선인증을 지원하는데 기존 망에 대한 고려가 없으며, 이는 서브넷 및 도메인 범위를 벗어나는 선인증을 지원하기 위해서는 현재 설치된 장비들을 새로운 것으로 대체해야 하는 비용부담이 있다. 두 번째는, 상기 기법들은 현재 접속하고 있는 AP를 이용하는 간접적인(indirect) 선인증 방식으로 인증 요소를 컨텍스트 전송(context transfer) 하기 때문에 현재 어플리케이션이나 시스템에 패킷 손실 등의 악영향을 줄 수 있는 단점이 있다.



[그림 1] 3G-WLAN 상호연동 망에서의 수평핸드오버 시나리오

이와 달리, 제안하는 선인증 기법은 빠른 채널 스위칭을 통해 연결계층에서 접속할 예정인 후보 AP와 직접(direct) 인증을 수행하는 선인증 방식으로 서브넷 및 도메인간 핸드오버를 지원한다. 또한 선인증 수행 시 패킷 손실을 최소화하기 위해 802.11의 전원절약(PS: power saving) 모드의 버퍼링기능을 이용하여 선인증의 오버헤드를 최소화시켰다.

III. 제안하는 선인증 기법

본 논문에서는 이기종의 네트워크의 모델로 [그림 1]과 같은 3G-WLAN Interworking 참조모델을 고려하였다[2]. 이 모델은 홈 네트워크를 3G 네트워크에 두고 접근 네트워크(Access Network)를 무선랜(IEEE 802.11 WLAN)으로 하는 수평핸드오버 시나리오를 나타낸다. 단말(mobile station : STA)은 이동경로에 따라 인트라(Intra), 인터(Inter) 서브넷, 인터 도메인 핸드오버가 발생하게 되며 각 핸드오버 유형에 따라 로컬 인증서버 또는 홈 네트워크의 인증 서버를 통해 인증되어야 한다. 따라서 핸드오버 유형, 인증 프로토콜 및 인증서버와의 거리 등에 따라 각 인증소요시간은 달라 질 수 있다. 제안하는 선인증 기법은 [그림 1]과 같이, 단말이 AP의 무선전송 범위가 중첩된 지역에 위치하고 다양한 스캐닝 기법을 통해 이미 인접한 AP들에 대한 상태정보(Beacon Interval, Received Signal Strength Indicator, data rate, 채널 등)를 가지고 있으며, 후속 접속에

정인 AP를 최적으로 결정한 상태라고 가정한다. 이해를 돕기 위해 먼저 제안기법에 활용되는 채널 스위칭 및 전원절약모드에 대한 설명을 간단히 하고 세부적인 제안기법에 대해 설명한다.

3.1 제안기법에서의 기본 기술 : 채널 스위칭 및 전원 절약모드 기능

3.1.1 채널 스위칭

무선 랜에서의 채널은 각 하위기술 버전별로 다르며 802.11b의 경우 13개의 채널을 사용할 수 있으며 각각의 채널은 상호 간섭을 방지하기 위해 인접하여 사용하지 않도록 하고 있다[9]. 제안하는 기법은 802.11i 선인증에서의 현재 AP를 경유한 선인증 방식과 다르게 인증을 원하는 AP에 해당하는 채널로 스위칭을 통해 통신가능하게 되며, 후속접속 예정인 AP와 직접 association을 맺어 인증작업을 수행하게 된다. 채널 스위칭에 소요되는 시간은 약 1~5 ms으로 알려져 있다[10]. 제안하는 기법에서의 스위칭 시점은 association에서 결정되는 Listen Interval (Beacon Interval의 배수)에 따라 달라진다. 기본설정으로 100 ms이며, 조정이 필요할 때는 re-association을 수행하여 재조정 한다. 채널 스위칭의 문제점은 채널 스위칭 빈도가 높을 때 이로 인한 수신패킷 손실 또는 현재 사용 중인 서비스에 악영향을 준다는 것이다. 이 문제를 해결하기 위해 제안하는 기법에서는 전원절약 모드의 버퍼링 기능을 활용한다.

3.1.2 전원절약 모드 기능

IEEE 802.11의 전원절약 모드(Poser save Mode : PM)는 단말이 슬립(sleep) 모드 일 때, 수신되는 데이터를 손실되지 않도록 버퍼링(buffering)하는데 사용된다. 본 기법에서는 실제로 슬립 모드로 진입하는 것이 아니라 진입한다는 메시지만을 AP에게 보내고 실제로는 인증 대상 AP의 채널로 스위칭 하여 인증 요청 작업을 수행한 후, 다시 복귀하여 현재의 AP 버퍼에 수신된 데이터가 있다면 이를 수신하고 다시 인증을 요청했던 채널로 재 스위칭 하여 선행 작업의 후속작업(인증 응답 수신 등)을 이어서 하는 방식으로 선인증 작업을 수행하게 된다. 이러한 방식은 패킷 손실을 최소화하고, 현재 사용 중인 서비스에 영향을 최소화 하는 장점이 있다.

3.2 채널스위칭 기반 선인증 기법

3G-WLAN 상호 연동망과 같은 구조에서 단말이 핸드오버를 수행하는 동안 적은 인증 지연시간과 패킷 손실을 보증하는 새로운 선인증 기법을 제안한다. 제안된 기법에서는 채널스위칭을 수행하는 시간 간격을 CSP(Channel Switching Period)라 정의한다. 즉, 채널스위칭의 시작과 끝으로 정의되는 CSP를 할당받아 주어진 시간동안 인증작업을 수행하고 이 시간동안 손실되는 패킷을 AP에서 임시저장하게 함으로써 손실을 방지한다. 제안된 기법의 자세한 선인증 절차는 [그림 1]의 환경을 기반으로 [그림 2]에 도시되어 있다.

제안하는 선인증기법의 절차는 Association, Authentication, Checking의 세 단계로 나누어질 수 있다. 단말의 Active 모드와 PS(Power Saving) 모드가 전환되는 동작은 CSP.BEGIN로 시작되어 CSP.END 메시지로 종료되는 동작이 반복되어 수행된다. 단말의 모드가 이렇게 전환될 때 마다 현재의 AP는 Buffering과 Forwarding을 반복하여 패킷 임시저장 및 전달 역할을 수행함으로써 패킷 손실을 방지한다.

3.2.1 CSP 메시지 구성

CSP.BEGIN 메시지와 동작은 다음과 같다.

① Null frame을 serving AP에게 PM bit = 1 (buffering)로 세팅하여 전송

② Target AP 채널로 스위칭 수행

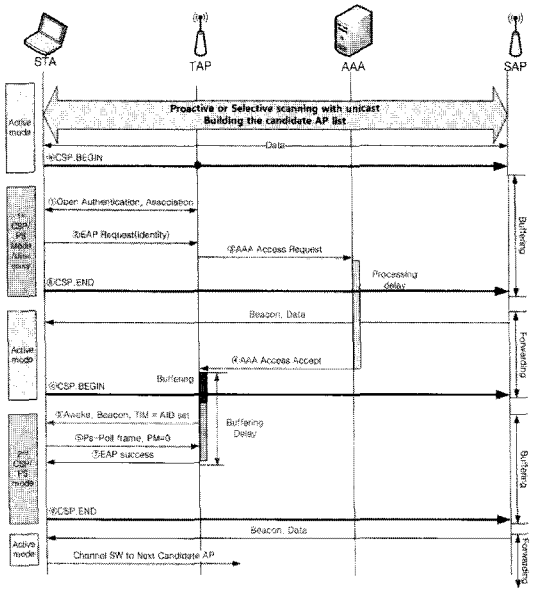
CSP.END 메시지와 동작은 다음과 같다.

① Null frame을 target AP에 PM bit = 1 (buffering)로 세팅하여 전송

② Serving AP 채널로 스위칭 수행

③ Null frame을 serving AP에 PM bit = 0 (forwarding)으로 세팅하여 전송

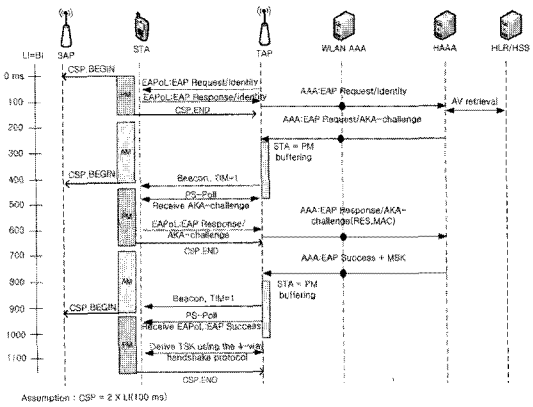
단말은 serving AP로부터 수신되는 beacon을 통해 자신에게 도착한 데이터의 유무를 확인한다. 인증서버로부터 도착한 인증결과가 target AP에 수신된 경우, 802.11 PS 모드에 의해 AP 버퍼에 먼저 임시저장한 후 LI 시간에 맞춰 beacon 신호(메시지 ⑤)를 통해 단말에 알려 awake mode로 활성화 되도록 한다. 이후 단말은 PS-poll frame 및 PM=0



〔그림 2〕 제안하는 기법의 선인증 절차

메시지(메시지 ⑥)를 AP로 전송하여 응답데이터를 수신하게 된다. 이 때 발생되는 target AP에서의 버퍼저장 지연시간과 단말의 응답대기 시간을 줄이기 위해 LI(Listen Interval)를 조정하여 re-association을 맺는 방안도 활용할 수 있다. 그러나 그 감소하는 시간 량이 근소하여 효율성은 그리 크지 않는 것으로 나타났다.

〔그림 3〕는 제안한 기법을 EAP-AKA 프로토콜에 적용하였을 경우, CSP를 2 X LI, 즉 200 msec 로 설정했을 때를 적용한 메시지 흐름도이다. EAP-AKA는 3G-WLAN 상호연동망에서 표준으로 권고하는 인증 프로토콜이며 사전공유 비밀방식이다. 첫 번째 CSP 에서는 단말(STA)이 로컬 인증서버(WLAN AAA)를 경유하여 홈 네트워크에 있는 인증서버(HAAA)에게 인증요청하고, 가입자 정보 서버(HSS : Home Subscriber Server)로부터 인증벡터(AV : Authentication Vector)를 얻어서 다시 TAP (Target AP)에게 응답해준다. 이 시점에서 현재 STA 는 TAP 관점에서 PM이므로 임시로 버퍼링을 하고 있다가 두 번째 CSP가 시작될 때, STA은 PS-Poll 메시지로 해당 응답프레임을 수신한 후, 다시 이에 대한 EAP Response/AKA challenge 메시지를 전송한 후 다시 PM 에 진입한다. 세 번째, CSP 가 시작되면 전과 동일하게 응답프레임을 수신하여 보안 협상을 완료한다. 본 예에서는 약 1.1 sec 소요되는 인증시간을 3회의 CSP(200 msec)를 통해



〔그림 3〕 제안기법을 EAP-AKA 에 적용한 메시지 시그널링

미리 수행하게 된다. 이 후 TAP에 핸드오버 한 경우에는 단말과 AP간의 association 및 4-way handshaking 과정을 통해 간단히 인증을 완료한다.

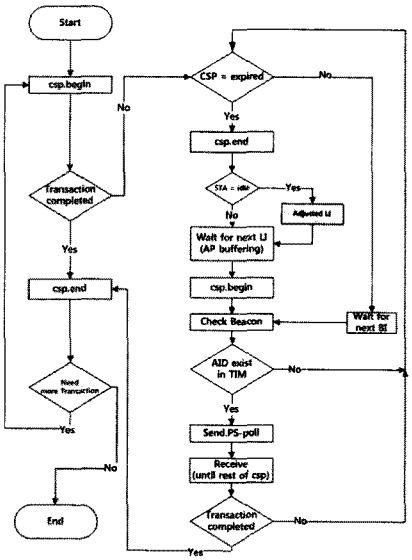
3.2.2 CSP 할당 알고리즘

CSP 시간(duration)을 결정하는 문제는 선인증의 성능에 중요한 영향을 미친다. 너무 짧게 할 경우, 자주 채널스위칭을 수행함으로 에너지 소모 및 성능에 저하가 발생하고, 너무 길게 할 경우 AP의 저장 공간 소모 및 단말의 이동성에 제한을 주게 된다. CSP의 할당 단위는 AP의 beacon 신호를 통해 데이터의 유무를 확인하는 방식에 기반을 두게 되므로 beacon의 배수로 결정되는 LI 시간 간격으로 할당한다.

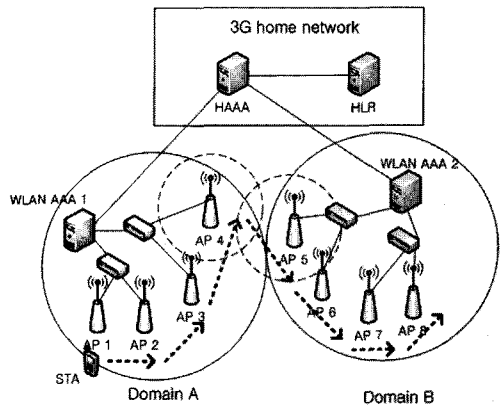
〔그림 4〕은 CSP의 할당 흐름도이다. CSP 개시부터 종료까지 아직 완료되지 않았다면 추가적인 CSP를 할당하며, 이후부터 LI 마다 인증응답의 유무를 확인하여 인증응답을 수신 완료할 때까지 반복적으로 Wait 과 Checking 단계를 수행한다. 응답이 AP에 도착된 것을 확인 되면 이후에 다시 CSP를 할당하여 수신한다. 이렇게 처리되는 한 건의 인증작업을 트랜잭션(transaction)으로 명명하여 CSP 기간 내에 처리되는 작업단위로 나타낸다. 각 CSP의 기간은 인증 프로토콜에 따라 다르게 된다.

IV. 분석 및 평가

본 장에서는 제안된 기법의 성능을 분석 및 평가하기 위하여 네트워크 모델을 제시하고, 패킷 손실, 지연시간 단축 관점에서 기존의 802.11 인증기법과 비



〔그림 4〕 CSP 할당 흐름도



〔그림 5〕 평가 네트워크 모델

교분석한다. 현재 제안하는 기법처럼 후속 AP와 직접 선인증을 수행 하는 유사기법의 비교대상은 찾지 못했다. 따라서 선인증을 지원하지 않거나 현재 AP를 경유하여 지원하는 기존의 표준 인증 기법을 선택하여 핸드오버 할 때 발생되는 각 손실 패킷의 양와 지연시간으로 비교하여 분석하였다. 핸드오버 성능의 정확한 측정은 동적인 네트워크 구조와 노드 위치 변화와 같은 다양한 요소에 의해 영향을 받기 때문에 어려운 작업이다. 기존의 802.11 핸드오버는 단말이 현재 AP와 접속을 끊고 새 AP와 다시 접속을 수행하는 "break-before-make" 방식이며 제안하는 기법은 "make-before-break" 방식으로 기존 방식과 비교하여 패킷 손실 및 성능저하에 대한 비교분석을 수행한다. 〔그림 4〕와 같은 3G-WLAN 연동망 환경에서 인증작업 수행 시 소요되는 지연시간을 각 단계별 수식 화하여 핸드오버를 반복적으로 수행하였을 때 발생되는 총 지연시간으로 성능을 평가한다.

〔그림 5〕는 평가 네트워크 모델로서 8개의 AP가 4개의 서브넷 및 2개의 도메인 A, B로 각각 동일하게 구성되어 로컬 AAA 서버 및 홈 AAA 서버를 사용하는 인증구조를 사용하고 있다. 평가하기 위한 가정 사항은 다음과 같다. 각 도메인은 사전에 미리 보안협약(security association)을 체결한 것으로 가정한다. 단말은 AP 1번 영역에서 AP 8번 영역으로 걷는 속도로 이동하고 있다고 가정한다. 각 AP는 802.11i RSN(Robust Security Network)을 지원하나 서브넷 및 도메인 간 RSN 로밍은 허용되지 않는다〔10〕. 또한 단말은 핸드오버 이전에 후속 AP를 미리 정해놓은 상태라고 가정한다.

〔그림 5〕와 같은 환경에서는 단말의 인증방식에 따라 현재 AP에서 연결이 해제될 때, 서비스가 단절되는 경우도 있고, 끊김없이 부드럽게 서비스의 연결성을 유지할 수도 있다. 본 분석 및 평가에서는 기본 802.11 인증, 802.11i 선인증, 그리고 제안하는 선인증 기법 등의 세 가지 기법을 상호 비교하여 분석을 수행하였다.

4.1 총 패킷 손실 분석

먼저 단말이 각 핸드오버 기법에서 인증을 수행할 때 발생하는 패킷 손실의 양을 분석한다. 총 패킷 손실은 단말이 핸드오버를 수행할 때 손실된 패킷의 합을 의미한다. 기본적인 IEEE 802.11에서는 핸드오버 도중 발생되는 손실 패킷에 대한 처리기능이 없어 모두 손실된다. 그러나 제안하는 기법에서는 손실되는 패킷을 최소화하기 위해 전원절약모드를 통해 AP에 임시 저장한다. 핸드오버를 수행하기 위해 초기 환경변수 값을 설정하여 패킷 손실 및 핸드오버 회수에 따른 제안하는 기법의 효율성을 나타낸다.

$$L_g = (T_{auth} + T_{asso} + T_{EAP} + T_{deauth} + T_{deasso}) \times B_{wl} \times N_m + T(s) \quad (2)$$

$$L_p = (T_{auth} + T_{asso} + \lceil n \rceil \times (T_{csp.begin} + T_{csp.end}) + T_{ps-poll}) \times B_{wl} \times N_m + T(s) \quad (3)$$

$$L_r = (T_{auth} + T_{asso} + n \times (T_{csp.begin} + T_{csp.end}) + T_{reasso} + T_{ps-poll}) \times B_{wl} \times N_m + T(s) \quad (4)$$

〔표 2〕 분석 변수 및 의미

변수	의미
s	메시지 크기
tc	평균 세션 연결 시간
tr	평균 3G or WLAN 무선 Cell 체류 시간
Nm	세션 내에 평균 이동횟수, 예) $Nm = \lceil tc / tr \rceil - 1$
LI	AP의 Listen Interval
$T(s)$	단말과 AP에서 메시지를 처리하는 지연시간
B_{wl}	무선링크의 대역폭
T_{EAP}	EAP 인증을 처리하는데 소요되는 시간
n	핸드오버에 할당된 총 CSP 수, $n = T_{EAP} / LI$

〔표 3〕 분석 초기 설정값

변수	값
t_c	1000 sec
t_r	2~40 sec
T_{auth}	80 bytes/B_{wl}
T_{asso}	80 bytes/B_{wl}
T_{deauth}	30 bytes/B_{wl}
T_{asso}	30 bytes/B_{wl}
T_{EAP}	1.568 sec/B_{wl}
B_{wl}	11 Mbps

핸드오버를 수행하기 위해 초기 환경변수 값을 설정하여 패킷 손실 및 핸드오버 회수에 따른 제안하는 기법의 효율성을 나타낸다. 〔표 2〕는 분석을 위한 초기 설정변수에 대한 의미를 나타낸다.

단말기에서 AP로 크기 s인 메시지를 전송하는 지연시간 T(s)는 다음과 같이 정의한다.

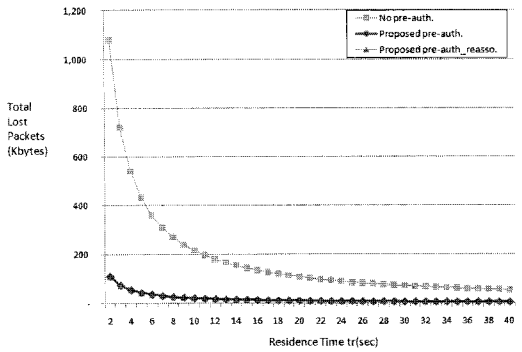
$$T(s) = \frac{s}{B_{wl}} + P_s \qquad (1)$$

단, P_s는 메시지 s에 대한 처리 지연시간을 나타낸다. 총 손실패킷의 양 L 은 인증 조건에 따라 식 (2), (3), (4)와 같이 나타낼 수 있다.

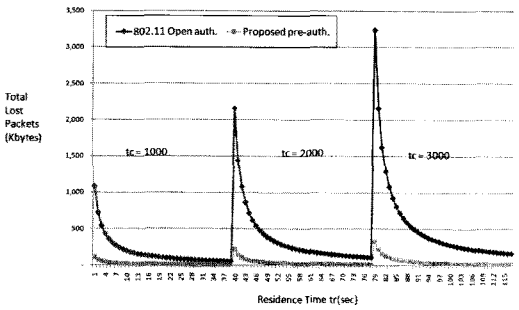
T_{auth}, T_{asso} 는 〔그림 2〕의 메시지 ① open 인증 및 association 과정에 걸리는 소요시간이며 T_{EAP}는 메시지 ②에서 ⑦까지 소요되는 EAP 인증 처리 시간을 나타낸다. $T_{csp.begin}$, $T_{csp.end}$ 는 메시지 ⓐ, ⓑ, ⓒ, ⓓ와 같이 순간 채널 스위칭을 통해 인증작업을 처리하는 메시지처리 시간이며, $T_{ps-poll}$은 메시지 ⑥와 같이 단말이 응답프레임을 수신하기 위해 보내는 메시지 처리 시간이다. 식 (2)는 일반 인증일 때, 식 (3)은 제안하는 기법의 선인증을 적용하였을 경우, 식 (4)는 식 (3)의 경우에서 LI를 재조정하기 위해 re-association 하는 경우의 총 손실되는 패킷의 양을 구하는 수식을 나타낸다. 이 수식에서 사용되는 변수 초기의 설정 값은 〔표 3〕과 같다. 각 설정 초기 값은 H. Choi 등이 〔11〕에서 제시한 초기 값을 사용하였고 T_{EAP}는 실제 실험 결과 평균값을 사용하였다.

측정 시나리오는 다음과 같다. 먼저 단말이 3G 영역이든 WLAN 영역이든 체류하는 시간(residence time)을 증가시킨다. 즉, 핸드오버를 수행하는 횟수가 감소될 때 손실되는 패킷의 양을 측정한다. 〔그림 6〕은 〔표 3〕에서 주어진 설정 값 및 수식 (2), (3), (4)를 통해 분석된 결과를 나타내며, 총 손실 패킷량은 단말의 체류 시간이 증가할수록 점차 감소된다는 것을 보여준다. 또한 제안된 기법이 선인증이 없는 기본 802.11 인증방식 보다 평균 약 10배 정도 패킷 손실을 방지 하는 것으로 나타났다. 따라서 패킷 손실은 핸드오버 동안 연결을 단절하는 구간을 가지고 있는 표준 802.11 핸드오버에서 더 크게 발생함을 알 수 있다. 표준 802.11 WLAN은 단말이 로밍을 수행할 때 현재 세션 패킷이 손실되는 것을 방지하기 위한 메커니즘이 없다. 그러므로 패킷 손실이 많이 발생한다. 한편, 두 가지 제안된 선인증 기법은 유사한 성능을 보여준다.

Re-association 기법을 가진 선인증 기법은 마지막으로 할당된 CSP 구간 내에서의 응답대기시간과 버퍼링 지연시간을 단축시킬 수 있지만 LI가 100 ms와 같이 작은 값이라면 그 효율성은 그리 크지 않다.



〔그림 6〕 체류시간에 따른 패킷 손실량



〔그림 7〕 연결시간(핸드오버 횟수)에 따른 패킷 손실량

〔그림 7〕은 핸드오버가 빈번히 일어날수록(연결시간 t_c = 1000, 2000, 3000 ms) 제안하는 기법의 패킷 손실 방지 효율성이 더욱 높다는 것을 나타낸다. 핸드오버 횟수는 Nm에 의해 구해지며, 연결시간이 길어진다는 것은 핸드오버를 더욱 자주한다는 의미이고, 패킷 손실 량은 더욱 커지게 된다. tr이 증가한다는 것은 핸드오버 횟수가 감소하며 패킷 손실 량도 감소하게 됨을 의미한다.

4.2 총 지연시간 분석

여기서는 비교대상의 각 기법에서 핸드오버를 수행할 때 소요되는 인증 지연시간을 비교한다. 단말이 AP를 사이를 핸드오버할 때, 미리 보안협상이 완료되어 있지 않으면 현재 연결을 끊고(break) 후속 AP와 연결을 수행한다(make). 이런 메커니즘을 〔그림 5〕의 시나리오에 적용할 때, 802.11 open 인증은 7회 이동시 EAP-AKA의 인증시간이 모두 소요되며, 802.11i 인증은 3회의 인트라 핸드오버 선인증, 4회의 인터핸드오버 EAP-AKA 인증이 소요되고, 제안하는 기법은 7회 모두 선인증으로 CSP 할당하는 시간만 소요되어 각 기법들에 대한 1회 이동 시 지연시간(D) 및 각 변수는 다음 식들과 〔표 5〕와 같다.

$$D_g = 7 \times T_b + T(s) \quad (5)$$

$$D_p = 3 \times T_b + 4 \times T_m + \Sigma T_{SA} + T(s) \quad (6)$$

$$D_r = 7 \times T_m + \Sigma T_{csp} + T(s) \quad (7)$$

수식 (5)는 기본 open 인증을 사용할 때 7회에 걸쳐 단절이 발생함을 의미하고, 식 (6)은 802.11i 선인증을 사용시 3회 단절 및 4회 선인증에 키 관리 등의 보안 협상시간이 추가됨을 의미하며, 식 (7)은

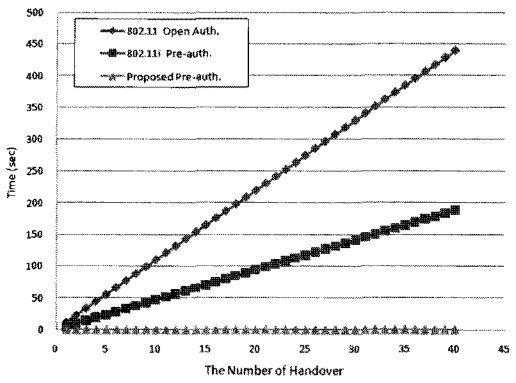
〔표 4〕 분석 변수 및 의미

변수	의미
T_b	핸드오버 시 평균 서비스 단절시간(breaking time)
T_m	선인증 평균 서비스 접속 소요시간(making time)
T_{SA}	802.11i 키 관리 등 보안 협상시간
T_{csp}	채널 스위칭 타임
$T(s)$	크기 s인 메시지를 전송하는 지연시간

제안하는 선인증 기법으로 7회의 선인증 및 할당된 총 CSP 시간으로 표현될 수 있다. T_b는 재접속하는데 소요되는 시간으로 볼 수 있으므로 T_{EAP}와 유사한 시간 값으로 볼 수 있다. T_m은 선인증 시 발생하는 평균 서비스 접속시간으로 EAP 인증작업이 생략된 T_{asso} + T_{auth} 시간으로 계산할 수 있다. T_{SA}, T_{csp} 역시 핸드오버시간에 발생되는 시간이 아닌 선인증시 발생되는 시간이므로 생략 가능하다. 〔그림 8〕은 〔표 3〕의 초기 설정 값을 적용하고, 〔그림 5〕의 네트워크 모델을 적용하여 핸드오버 회수를 40회까지 증가하였을 때 발생되는 총 지연시간(D)을 나타낸다. 핸드오버 횟수가 증가할수록 802.11 기본 인증 및 802.11i 지연시간은 증가하는데 반해 제안하는 기법은 최소치를 유지하고 있어 긴 인증시간이 소요되는 환경에서 더욱 효율성이 높다는 것을 확인할 수 있다.

4.3 분석 요약

〔표 5〕에서 보여주는 결과처럼, 제안하는 선인증 기법이 기존의 802.11 open, 802.11i 인증보다 각각 10 배, 4 배 정도 향상된 평균 패킷 손실량을 보여



〔그림 8〕 핸드오버 횟수에 총 지연시간 비교

〔표 5〕 분석 요약

구 분	802.11 open	802.11i	제안기법
평균 패킷 손실량(Kbytes)	181	78	19
평균 지연시간 (msec)	225	96	0.16

주며 평균 지연시간에 있어서는 두 개의 표준 기법보다 상당한 효율을 보이고 있다. 결과적으로 제안하는 기법은 3G-WLAN 상호연동망에서 단말의 이동성에 따라 발생하는 각 유형의 핸드오버시 인증지연시간을 효과적으로 단축하였으며, 패킷 손실도 방지하고 있음을 알 수 있다.

이상과 같이 제안하는 기법은 기존 표준 기법의 한계였던 Inter subnet 핸드오버를 지원하며 인증지연시간이 긴 구간, 특히 인증 서버가 원거리에 있거나, 많은 계산 량을 요구하는 복잡한 인증절차일 경우 더욱 효과적이며 현재 서비스에 영향을 최소화 하는 하는 장점이 있다. 또한 현재 네트워크 구조에 쉽게 적용될 수 있으며 도메인이 다른 네트워크에서 사업자가 서로 다르며 미리 보안협상이 체결되어 있지 않아도, 해당 도메인에 대한 합법적인 identity 가 있으면 적용이 가능한 선인증 기법이다.

V. 결론 및 향후계획

제안하는 선인증 기법은 WLAN을 접근망으로 사용하는 3G-WLAN 상호연동망에의 연결계층에서 빠른 채널 스위칭을 기반으로 핸드오버 대상 AP로 직접 채널변경을 통해 연결 및 인증을 수행하는 새로운 선인증 방식이며 끊김없는 서브넷 및 도메인 간 핸드오버를 지원한다. 또한 패킷 손실을 최소화하기 위해 IEEE 802.11의 PS 모드를 이용하여 선인증으로 발생하는 패킷손실을 기존기법에 비해 최고 10배까지 최소화하였고 인증에 소요되는 평균 지연시간을 0.16 msec까지 줄임으로 거의 제거하는 효과를 기대할 수 있다. 본 기법을 적용하거나 구현하기 위해서는 단말의 연결계층의 디바이스 드라이버만 수정하면 되기 때문에 현재의 네트워크 구조를 그대로 사용할 수 있는 장점이 있어 실용적이다. 또한 제안하는 기법은 WLAN에만 적용되지만 WLAN을 접속망으로 사용하는 3G-WLAN과 같은 상호연동망에 적용될 수 있으며 상대적으로 더욱 긴 인증시간을 단축시킬 수 있으므로 더욱 효과적이다.

본 연구에서는 제안하는 기법에 대한 효율성 분석 및 평가를 패킷의 손실과 지연시간을 중심으로 수행하였다. 향후 연구 계획으로는 단말의 에너지 소모 관점 및 이동속도에 따른 효율적인 선인증의 수행을 위한 분석 및 평가와 기법에 대한 구현 및 테스트 베드를 통해 실제적인 측정 등에 대한 보완연구를 수행할 것이다.

VI. 참고문헌

〔1〕 3GPP, "3GPP TS 33.234 (v8.1.0), 3G security; WLAN interworking security; System description," vol.V8.1.0, 2008.

〔2〕 3GPP, "3GPP TS 23.234 (v8.0.0), 33GPP system to Wireless Local Area Network (WLAN) interworking" vol.V8.0.0, 2008.

〔3〕 H. Wu, K. Tan, Y. Zhang, and Q. Zhang, "Proactive scan: Fast handover with smart triggers for 802.11 wireless LAN," IEEE INFOCOM, pp.749 - 757, 2007.

〔4〕 I. Ramani and S. Savage, "SyncScan: practical fast handover 802.11 infrastructure networks," IEEE INFOCOM, p.675, 2005.

〔5〕 H. Kwon, K. Cheon, K. Roh, and A. Park, "USIM based authentication test-bed for UMTS-WLAN handover," Proceedings of IEEE INFOCOM, Barcelona, Spain, 2006.

〔6〕 정수환, 안재영, "FMC의 무선 네트워크 환경에서 USIM 기반의 이기종 망간 핸드오버 인증 기술," Telecommunication Review, pp. 35-38, 2008년 8월.

〔7〕 J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," IETF RFC 4187, January 2006.

〔8〕 강유성, 오경희, 정병호, 정교일, 정찬형, "무선랜 보안 표준 IEEE 802.11i,", TTA 저널, 제 99호, pp.123-130, 2005년 5월.

〔9〕 A. Dutta, "A Framework of Media-Independent Pre-Authentication (MPA)

for Inter-domain Handover Optimization," Internet-Draft, Sept. 6, 2010.

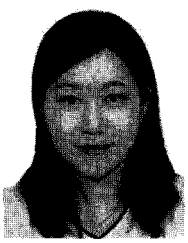
[10] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i-2004, pp.1 - 175, 2004.

[11] H. Choi, O. Song, and D. Cho, "Seamless Handover Scheme Based on Pre-registration and Pre-authentication for UMTS - WLAN Interworking," Wireless Personal Communications, vol. 41, no. 3, pp. 345 - 364, 2007.

[12] Yao, G., J. N. Cao, et al., "Secured Fast handover in 802.11-Based Wireless Mesh Networks for Pervasive Internet Access," IEICE Transactions on Information and Systems, vol. 93D, no. 3, pp. 411-420, 2010.

〈著者紹介〉

백 재 종 (JaeJong Baek) 학생회원
1996년 2월: 한밭대학교 전자계산학과 졸업
2001년 2월: 연세대학교 컴퓨터과학과 석사
2007년 9월~현재: 연세대학교 컴퓨터과학과 박사과정
〈관심분야〉 인증, 스마트폰 보안, MIP 보안, 역공학, 정보전



김 효 진 (HyoJin Kim) 정회원
2002년 2월: 연세대학교 기계전자공학부 정보산업공학과 졸업
2004년 2월: 연세대학교 컴퓨터과학과 석사
2010년 8월: 연세대학교 컴퓨터과학과 박사
2010년 12월~현재: 한국 정보통신기술협회(TTA) 과장
〈관심분야〉 정보보호, 유무선통신 등

송 주 석 (JooSeok Song) 종신회원
1976년 2월: 서울대학교 전기공학과 졸업
1979년 2월: 한국과학기술원 전기전자공학과 석사
1988년 2월: University of California at Berkeley 컴퓨터과학과 박사
1988년~1989년: 미국 Naval Postgraduate School 조교수
1989년 3월~현재: 연세대학교 컴퓨터과학과, 정교수
2006년 한국정보보호학회 회장 역임
〈관심분야〉 정보보호, 유무선통신 등