The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 3, pp.107-112, Jun. 30, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.3.107
JIIBC 2015-3-15

무선랜 환경에서 AP간 전력임계치값을 통한 호 처리 연구

A Study of Call Admission Scheme using Power Strength Threshold value between APs in Wireless LAN Environments

임승철*

Seung-Cheol Lim*

요 약 스마트폰과 많은 무선단말기들이 이동성의 특성상 AP간 이동하게 되어 무선단말들과 AP(Access Point)간 많은 호 절체가 이루어지게 된다. AP에서 각 무선단말기마다 처리되는 호 처리는 상대적으로 많은 무선트랙픽을 유발하여 무선대역의 효율적인 활용을 저해하는 요인이 되고 있다. 따라서 본 논문에서는 무선단말기와 AP간의 트래픽 발생요인이 되고 있는 AP간 호 절체 트래픽양을 줄이기 위해서 무선단말기에 수신되는 AP들의 전력세기임계치와 임계타이머를 사용하여 AP에서 효과적으로 무선트랙픽을 활용할 수 있는 방안을 제안하였다. 제안된 방식과 기존의 방식을 시뮬레이션을 통하여 AP에서 처리하는 무선트래픽 양이 개선되어 전체적으로 무선대역의 활용을 효율적으로 할 수 있었다.

Abstract A smart phone and the number of wireless terminals are mobile-to the nature of the AP mobility are many call transfer between wireless terminals and AP (Access Point). Each wireless terminal that is the call processing process for each is relatively large to cause the wireless traffic, and a factor that inhibits the efficient use of the radio band on the AP. In this paper, we use the power intensity threshold and threshold timer of the AP received by the mobile station to reduce the amount of switching traffic between the AP's cause and traffic generation factors between the wireless device and the AP that can effectively utilize the radio traffic from the AP the measures proposed. The proposed method and the conventional method is improved by simulation to handle the amount of radio traffic from the AP it was confirmed that it is possible to effectively utilize the whole of the radio band.

Key Words : Power Strength Threshold, Call admission Control, Wireless, IEEE802.1x, AP

Ⅰ. 서 론

우리생활에서 스마트폰, 테블렛 등의 무선단말기의 사용시간이 늘면서 AP에서 사용되는 무선트래픽 양이 폭발적으로 늘어나고 있다.

최근 들어 IEEE 802.11 기반의 무선랜 시스템의 편리성, 경제성 및 이동성 지원이란 장점을 기반으로 무선 인터넷의 플랫폼으로 되고 있다. 무선랜 환경에서 인터넷폰과 스마트폰 등과 같은 실시간 음성 및 멀티미디어 서비스를 이용 하려는 사용자의 관심이 날로 증가되고 있는 상황에서 무선트래픽을 효율적으로 관리하고 활용하는 것은 가장 중요하게 고려해야 부분으로 대두되고 있

*정회원, 우송대학교 IT융합학부
접수일: 2015년 4월 9일 , 수정완료일: 2015년 5월 9일
게재확정일: 2015년 6월 12일

Received: 9 April, 2015 / Revised: 9 June, 2015
Accepted: 12 June, 2015
*Corresponding Author: sclim@wsu.ac.kr
Dept. IT Fusion, Woosong University, Korea

다. 무선랜 환경에서 신속한 호 처리는 WLAN 서비스에 있어서 가장 중요하게 고려해야 할 부분으로 대두되고 있다. 이로 인해 무선트래픽을 줄이면서 신속한 무선단말기와 AP간 호 절체는 상호 밀접한 관계를 가지고 있고, 인증과 무선 구간 데이터 보안에 대한 문제는 WLAN 표준화 초기 단계에서부터 현재에 이르기 까지 끊임없이 연구 되고 있다. WLAN 표준화 초기에 인증과 보안을 위해 IEEE 802.11i는 국제 WLAN 보안표준을 제정하였다.[1]

이 표준은 공개키 기반의 상호 인증 프로토콜인 EAP-TLS(Extensible Authentication Protocol-Transport Layer Security) [2] 를 인증 표준으로 채택하고 새로운 형태의 보안 구조인 RSN(Robust Security Network) 보안 구조를 표준에 반영함으로써, WLAN에서의 데이터 프라이버시 기능 을 더욱 강화하였다.

또한 핸드오프 시 단말기가 AP를 검색한 이후 새로운 네트워크에 접속하기 위한 재접속 단계에서의 완전 인증을 수행하기 때문에 많은 오버헤드를 발생한다. 따라서 본 논문에서는 호 절체시 지연 시간을 줄이고 AP간의 상호 인증과 무선전력세기임계치값을 활용하여, 재 인증 과정과 호 절체회수를 줄여서 무선 트래픽양를 감소시키면서 빠른 호 처리 방법을 제안하고자 한다.

2장에서는 기존 무선 랜의 핸드오프 인증, 세션키 도출과정 대하여 살펴보고 무선단말기에서 전력세기임계치 적용을 통한 호 저리방안을 제안한다. 3장에서는 제안한 호 처리 방식의 성능을 분석하고 4장에서는 결론을 맺는다.

II. 제안한 호 처리방식

본 논문에서는 기존의 무선랜 환경에서 무선단말기의 중첨지역에서 전력세기 임계치와 임계타이머를 사용하는 mobile assist 핸드오프를 적용하여 기존의 호 처리 방식에서 호 절체시간을 개선하고자 한다.

1. 기존의 무선랜 호 처리방식

IEEE802.11에서 사용하는 호 처리 과정은 탐색 과정과 재인증 과정으로 이루어진다.

이동 단말기는 이전 AP에서 수신하는 신호세기를 체크하여 정해진 수준 이하로 내려가거나 링크가 단절되었을 때 핸드오프의 첫 단계로서 자신이 접속할 새로운 AP를 찾기 시작한다. 이 과정이 탐색과정이다. 탐색과정에서 이동 호스트는 자신이 발견할 수 있는 모든 이웃 AP들을 유일하게 식별하게 하는 BSSID(Basic Service Set Identification) 및 해당 AP의 물리 계층 파라미터 등을 수집하고, 이 정보를 이용하여 AP들의 리스트를 만든다. 이 모든 정보는 AP에서 주기적으로 보내지는 비콘 프레임에 의해 얻어진다.

이전 AP와 새로운 AP에서의 전파특성 차가 어느 일정 이상이 되면 이동 호스트는 이전 AP에 접속하기 위해 재인증 단계로 들어간다. 이동 호스트는 탐색 과정에서 만들어진 AP의 리스트를 보고 선택된 새로운 AP에게 재인증을 시도한다. 재인증 과정은 AP가 적합한 이동 호스트임을 확인하는 인증과정과 이동 호스트가 자신의 MAC주소를 등록하는 재결합과정으로 나눌 수 잇다. 핸드오프는 이동 호스트가 AP로부터 재결합 응답 메시지를 받음으로써 끝나게 된다.

802.1X 인증 모델은 네트워크 서비스를 제공받으려는 인증 요구자와 인증절차를 수행하는 인증자 , 인증서버로 구성된다. 이때 인증 요구자와 인증자를 PAE(port access entity)라고도 한다.[3] 802.1X에서는 포트 기반 접근제어를 사용하는데 이를 위하여 비 제어 포트와 제어 포트의 개념이 사용된다. 비 제어 포트는 인증 요구자가 네트워크의 인증 서버와 같이 인증에 필요한 인증 관련 자원만을 사용할 수 있는 포트로써, 인증이 성공적으로 이루어지면 제어 포트를 이용하여 네트워크 자원을 자유롭게 사용할 수 있게 된다. 802.1X는 전송 프로토콜로 EAP(extensivle authentication protocol)를 이용한다. 인증 요구자와 인증자 사이의 통신은 EAPOW(EAP over WLAN)를 사용하고, 인증자와 인증 서버 사이의 통신은 EAPOL(EAP over LAN)을 사용한다.[4]

EAP-TLS는 인증 단계와 세션키 확립 단계로 구성된다. 인증단계에서 AS와 MS은 자신의 공개키 인증서를 서로 교환하여 서로를 인증한다.

그림 1은 MS와 AP를 경유한 AS(Authentication Server)사이의 인증 및 세션 키 생성을 보여주는 예로써 802.1x EAP-TLS Authentication 과정을 통해 MS와 AS 사이의 상호인증 및 PMK(Pairwise Master Key) 도출을 진행한다. [5][6]

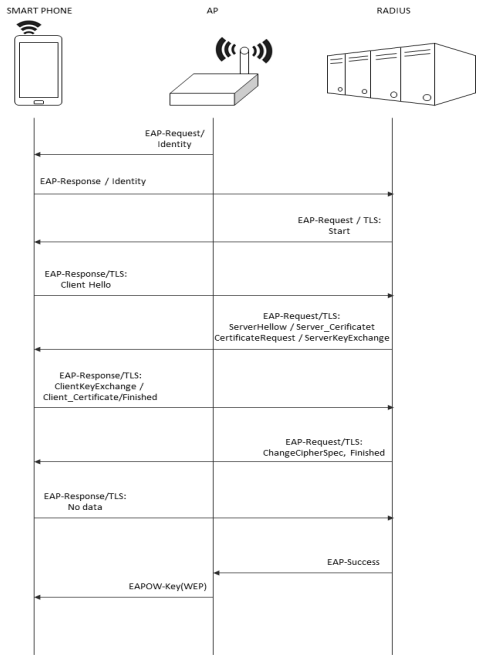

그림 1. EAP-TLS 인증 과정
Fig. 1. EAP-TLS authentication process

2. 제안한 호 처리 방식

이동 단말기는 그림 2와 같이 이전 AP에서 수신하는 신호세기를 체크하여 정해진 수준 이하로 내려가거나 링크가 단절되었을 때 핸드오프의 첫 단계로서 자신이 접속할 새로운 AP를 찾기 시작한다. 이 과정에서 이동 호스트에서 주변의 AP의 전력세기를 측정한 후 임계치 이상의 AP기와 핸드오프타이머가 만료시 RADIOUS 서버에 핸드오프를 요청한다.

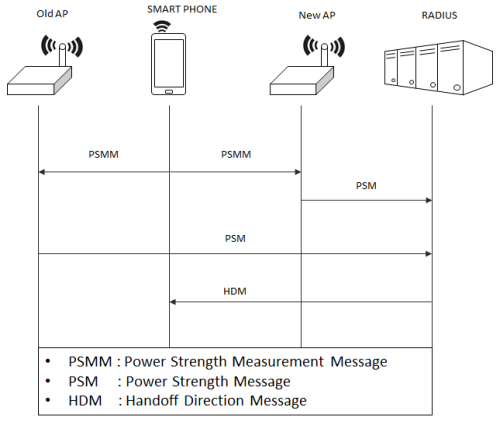

그림 2. 제안방식의 이동단말기도움 핸드오프처리 과정
Fig. 2. Proposed Mobile Assist Handoff process

그림 3과 같이 무선 단말기가 이동시에 핸드오프처리를 위해 주변에 있는 AP의 전력세기를 측정한 후 수신된 전력세기가 임계치값 이하가 되고, 핸드오프 타이머값이 만료될 때 주변의 검색된 AP에서 가장 높은 세기의 AP로 핸드오프 할 수 있도록 RADIUS 서버에 요청한다.

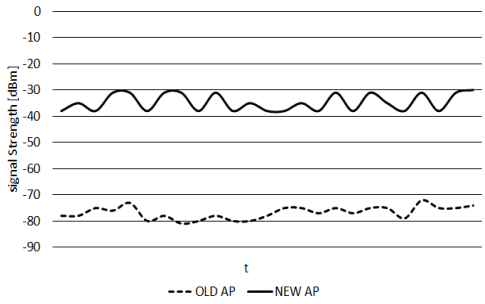

그림 3. AP의 전력세기
Fig. 3. Power Strength of APs

핸드오프를 요청 받은 AP가 무선 네트워크를 이용하여 무선 단말기에게 서비스를 제공 하던 이전 AP의 정보를 요구하면 새로운 AP에 접속을 하고 무선 단말기는 이전 AP와의 연결을 해지한다. 이와 같이 중접지역에서 핸드오프처리는 전력임계치값과 핸드오프 타이머를 적용하여 빈번한 횟수의 핸드오프 처리횟수를 줄이도록 제안하였다.

그림 4와 같이 AP는 자신의 주변에 위치한 AP들과 미리 완전 인증을 통해서 상호 인증 과정을 수행해야 한다. 이 과정을 통해서 각 AP는 인접한 AP에 대한 정보와 공개키를 획득하고 이를 테이블로 저장하게 된다.

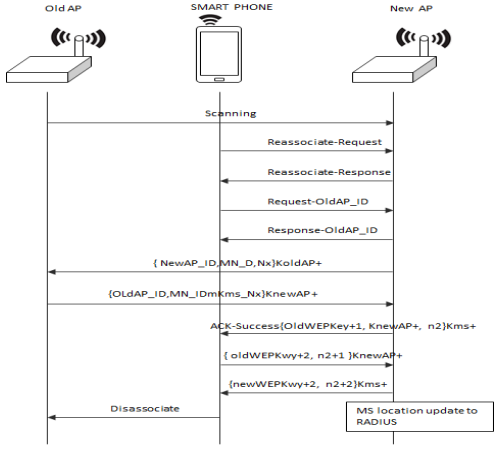

그림 4. 인증 과정
Fig. 4. Authentication process

무선 단말기의 초기 인증 과정에서는 AP가 단말기의 인증서와 CRL을 모두 확인해야 하지만, 핸드오프 시 인증에서는 각 AP간의 상호 인증을 통해 CRL 확인 과정을 생략하게 되고 RADIUS 서버에는 생략된 무선 단말기 인증서의 CRL 정보를 주기적으로 확인하고 CRL 변경사항이 생기면 해당 무선 단말기에게 서비스를 제공하고 있는 AP에게 사용자 인증 무효를 통보하게 된다.

무선 단말기는 스캐닝을 통해서 이동할 AP를 선택한 후 재설정을 요청한다. 핸드오프를 요청 받은 새로운 AP는 무선 단말기에게 인증 과정의 시작을 알린다. 새로운 AP는 RADIUS서에 무선단말기가 기존 접속한 AP의 정보를 요청한다. 기존 AP 정보를 새로운 AP에게 전송한다.

Ⅲ. 모의 실험

이 장에서는 제시한 방안의 호 처리 대한 성능과 핸드오프 수행 속도 등을 분석한다.

제안한 호 처리 절차를 사용한 핸드오프와 기존의 핸드오프의 지연시간을 비교하여 핸드오프 수행속도를 분석해 보았다.

$$\text{핸드오프 수행 속도 : } V = C / T_d \qquad (1)$$

여기서 V는 핸드오프 수행속도, C는 중첩된 셀영역의 거리, T_d는 전체핸드오프 수행지연시간이다.

그림 2와 표 1 그리고 수식 (1) 은 각각 핸드오프 수행과정, IEEE의 Latency Scale와 핸드오프 수행속도(Maximum Velocity)이다.[8][9]

일반적인 핸드오프는 EAP-TLS를 이용한 완전 인증을 거친 핸드오프와 지연시간은 수식(2)와 같다.

무선 단말의 핸드오프 속도는 중첩된 셀 영역의 거리(C)를 전체 핸드오프 수행 지연시간으로 나눈 값이다.

$$T_d = T_{scan} + T_{802.1X} + T_{4way} + T_{reassoc} \qquad (2)$$

여기서, T_d는 전체 핸드오프 수행 지연시간, T_{scan}은 단말기가 AP의 신호세기를 주기적으로 스캔하는 시간, $T_{802.1X}$은 802.1X 인증과정을 거치는 시간, T_{4way}은 4-way 핸드쉐이크 수행시간, $T_{reassoc}$는 re-association 시간이다.

표 1. 지연 스케일
Table 1. Latency Scale

Layer	Item	Time(ms)
L2	802.11 scan(passive)	0ms(cached), 1sec(wait for Becon)
L2	802.11 scan(active)	40~300
L2	802.11 assoc/reassoc	2
L2	802.11 authentication (full)	1000
L2	802.11 authentication (fast resume)	250
L2	Fast Handoff (4-way handshake only)	60
L3	MN-HA BU	1RTT(IKE w/HA SA), 4RTT(IKE w/CoA SA)
L3	MN-CN BU	1~1.5RTT(CAM)~2.5RTT(RR)

수식 (2)처럼 일반적인 핸드오프 수행속도는 새로운 AP로 이동할 때마다 IEEE802.1x의 모든 인증을 거치기 때문에 유연한 핸드오프를 제고하기에는 지연시간이 크다.

RADIUS 서버를 이용한 핸드오프는 마스터 키를 RADIUS 서버를 통해 전송받기 때문에 인증과정을 거칠 필요가 없다. 대신 RADIUS 서버를 통해서 마스터키를 주고받기 때문에 2RTT(Round Trip Time)가 필요하다.

$$T_d = T_{scan} + 2RTT + T_{4way} + T_{reassoc} \qquad (3)$$

제안한 핸드오프방식을 사용한 경우는 AP간의 상호 인증을 하기 때문에 키 교환을 위해 1개의 RTT의 시간이 필요하다.

$$T_d = T_{scan} + RTT + T_{4way} + T_{reassoc} \qquad (4)$$

AP간의 제안한 호 처리 방법은 그림 5, 6 에서 성능 분석 결과와 같이 핸드오프 지연이 짧기 때문에 핸드오프 수행시간이 평균 45% 빠르다는 것을 알 수 있다. 각각의 핸드오프 수행 속도를 비교한 것이다.

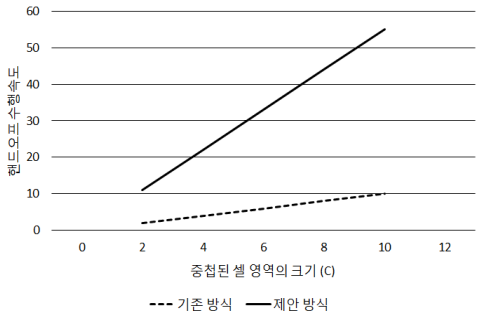

그림 5. 기존 방식과 제안 방식의 핸드오프 수행시간 비교
Fig. 5. Existing methods and proposed method compares the execution time of the handoff

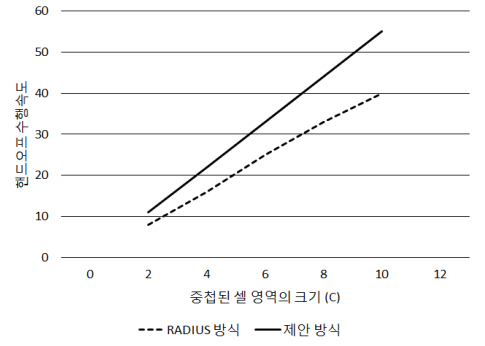

그림 6. RADUIS방식과 제안 방식의 핸드오프 수행시간비교
Fig. 6. RADUIS methods and proposed method compares the execution time of the handoff

Ⅳ. 결 론

무선랜의 보안 문제를 해결하기 위해 등장한 IEEE 802.11i 표준은 무선랜 시스템의 보안을 위해 다양한 기술을 수용할 수 있도록 하고, 새로운 키 교환 방식과 암호 알고리즘을 정의하여 이동하지 않아 핸드오프를 하지 않는 무선 단말기의 통신에 대해서는 효과적인 보안기능을 제공하지만 빈번하게 이동하고, 무선단말기의 특성상 중첩 지역에서 반복적인 핸드오프처리횟수가 발생된다. 이에 따라 AP간의 빠른 핸드오프 기능을 구현하고 중첩 지역에서 불필요한 핸드오프를 줄임으로써 무선자원을 효율적으로 관리할 수 있는 방법이 필요하게 되었다. 또한 무선단말기와 AP간 핸드오프 처리시간의 최소화하는 방안이 요구된다.

본 논문에서는 핸드오프 시 지연 시간 요소로 작용하는 인증 시간을 단축하기 위한 AP간의 상호 인증을 적용하고 중첩지역에서 전력세기임계치를 적용하여 불필요한 핸드오프 횟수를 줄임으로서 향상되는 호 처리성능을 제안하였다. 제안된 호 처리방식을 적용하여 핸드오프지연을 단축하여 핸드오프 수행시간을 향상시킬 수 있었다. 향후 연구 과제로는 다른 통신 사업자간에 AP를 공유하는 방법과 이 경우 호를 효율적으로 처리하는 호 처리 알고리즘에 대한 연구가 필요하다.

References

[1] IEEE Standard 802.11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,” IEEE, IEEE Std 802.11(Revision of IEEE std 802.11-1999), June 2007.

[2] B.Pboba and D.Simon, ″PPP EAP TLS authentication procotol,″ RFC 1510, IETF, 1999.

[3] ″Standard for Port Based Network Access Control″, IEEE Draft P802.1X/D11, March, 2001

[4] L.Blunk ″PPP Extensible Authentication Protocol(EAP)″, IETE RFC 2284, March, 1998

[5] IEEE Standard 802.11i, “″Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,”″ IEEE, July 2004.

[6] IEEE Standard 802.1x, “″IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control,”″ IEEE, IEEE Std 802.1X-2004(Revision of IEEE Std 802.1X-2001), June 2001.

[7] C. He and C. Mitchell, “″Analysis of the 802.11i 4-way handshake,”″ Proceedings of the 3rd ACM workshop on Wireless security(WiSe′04), pp. 43-50, Oct. 2004.

[8] Bernard Aboba, ″Fast Handoff Issues″, IEEE 802.11-03/155r0, December 2004.

[9] M.K., H.J Hwang ″A Low Power Lifelog Mangement Scheme Base on User Movement

Behaviors In Wireless Networks," The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 15, No. 2, pp. 157-165, 2015.

저자 소개

임 승 철(정회원)

- 1985년 : 한양대학교 전자공학과 학사
- 1994년 : 전북대학교 정보통신과 석사
- 2003년 : 전북대학교 영상공학과 박사
- 2006년 ~ 현재 : 우송대학교 컴퓨터정보학과 교수

<주관심분야 : 이동통신, 컴퓨터네트워크, 임베디드시스템소프트웨어>