

가변적인 탐색시간을 이용한 IEEE 802.11 무선랜의 고속 핸드오프 알고리즘

준회원 권경남*, 정회원 이채우**

A Fast Handoff Algorithm for IEEE 802.11 WLANs using Dynamic Scanning Time

Kyoung-nam Kwon* Associate Member, Chae-woo Lee** Regular Member

요 약

인터넷이 성장하면서 사용자들은 이동 중에도 인터넷을 사용하기를 원하고 있다. 이런 요구를 만족시키는 경제적인 한 방법으로 IEEE 802.11 무선랜이 급속히 보급되고 있다. 이동성을 지원하기 위해서는 핸드오프 기능이 필수적이다. 그러나 IEEE 802.11의 핸드오프 지연시간이 최고 300ms가 넘어 실시간 멀티미디어 통신에 적합하지 못하며, 특히 대부분의 지연시간이 기존의 연구와 달리 새로운 Access Point(AP)를 탐색하는 과정에서 발생한다는 것이 최근의 연구에서 밝혀졌다. 본 논문에서는 기존 핸드오프 방식의 문제점을 분석하고, 기존의 IEEE 802.11 무선랜에서 핸드오프 시 새로운 AP를 검색하는 알고리즘을 개선하여 네트워크 상황에 따라 가변적인 시간동안 새로운 AP를 탐색함으로써, 핸드오프에 소요되는 시간을 줄이는 고속 핸드오프 알고리즘을 제안하고, 제안된 알고리즘의 성능이 기존의 방법에 비해 우수함을 시뮬레이션을 통해 보인다.

Key Words : IEEE 802.11, Handoff, Wireless LAN

ABSTRACT

As the Internet usage grows, people want to access the Internet while they are moving. To satisfy this requirement economically, IEEE 802.11 Wireless LANs(WLANs) are rapidly deployed. In order to support mobility, WLANs must provide smooth handoff mechanism. Recent studies show, however, handoff delay of WLANs exceeds 300ms, most of which is due to slow scanning mechanism finding a new AP. With this handoff delay, current WLANs is not suitable to provide seamless realtime interactive services such as VoIP service. In this paper, we analyze the current handoff method of IEEE 802.11 and we propose a new handoff algorithm which can decrease time needed for searching a new AP and thus reduce overall handoff time. We show by simulation that the proposed algorithm has shorter handoff delay than current handoff method.

1. 서론

최근 많은 사용자들이 무선 환경에서 인터넷 사용을 요구하면서 무선 인터넷 환경에 대한 관심이 증폭되고 있다. 무선 인터넷망은 이러한 관심을 받

여하듯 과거 유선망의 발전 속도보다 빠르게 사용 영역을 확대해 나가고 있다. 그러나 현재 서비스되고 있는 이동전화를 이용한 무선인터넷 서비스는 느린 링크속도와 비싼 사용료로 많은 사용자들이 사용을 기피하고 있다. 인터넷에서 이루어지고 있는 서비스들이 점차 멀티미디어 데이터와 같은 대용량

* 아주대학교 전자공학과 멀티미디어 네트워킹 연구실(knkwon@ajou.ac.kr), ** 아주대학교 (cwlee@ajou.ac.kr)

논문번호 : 030304-0722, 접수일자 : 2003년 7월 21일

※ 본 논문은 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초기술연구지원사업(과제번호:03-기초-0078)의 연구결과입니다.

서비스를 중심으로 구성되면서 이동전화를 이용한 무선인터넷은 더욱 외면당하고 있다. 이와 같은 무선인터넷 서비스의 문제를 해결하기 위해 좀더 빠르고 값싼 무선 인터넷 환경을 구축하기 위한 대안으로 떠오른 것이 IEEE 802.11을 기반으로 하는 공중 무선랜이다. IEEE 802.11을 이용한 공중망 서비스는 컨벤션 센터, 공항, 대중 음식점등의 핫스팟(Hot-spot)을 중심으로 그 사용 장소가 빠르게 확산되고 있다.

이처럼 무선을 사용한 인터넷 환경이 점차로 관심을 끌고 있는 것은 이동성을 지원할 수 있다는 무선 환경만의 특성 때문이다. IEEE 802.11에서도 간단한 핸드오프 기능을 통해 어느 정도의 이동성을 보장하고 있다. 그러나 셀룰라 통신과 달리 IEEE 802.11은 하드 핸드오프(hard handoff)방식을 취하고 있다. 하드 핸드오프는 핸드오프를 통해 채널을 변경할 때, 기존의 연결을 끊고 새로운 연결을 생성하는 방법을 사용한다. 따라서 IEEE 802.11에서는 핸드오프 도중에 접속 단절로 인해 데이터의 전송이 끊기는 시간이 존재하게 된다. 이 시간은 핸드오프에 걸리는 시간에 따라서 비례적으로 증가하게 된다. 이처럼 핸드오프 방식으로 인해 IEEE 802.11에서는 셀룰라 통신과 달리 완벽하게 접속 단절이 없는(seamless) 핸드오프를 지원하는 것은 불가능하지만, 핸드오프 지연시간을 단축하여 사용자가 핸드오프 중에 발생하는 지연시간으로 인한 접속 단절을 느끼지 못하게 한다면 셀룰라 통신과 비슷한 수준의 핸드오프 성능을 가지도록 하는 것이 가능하다.

이와 같은 이유로, IEEE 802.11에서 접속 단절이 없는 핸드오프를 지원하기 위해 핸드오프 지연시간을 줄이려는 연구가 최근까지 매우 활발하게 이루어지고 있다^[2-5]. 이 연구들에서는 핸드오프 지연시간을 줄이기 위해 단말기가 AP를 검색한 이후 새로운 네트워크에 접속하기 위한 재접속단계에 초점을 맞추고 있다. 그러나 기존의 연구들은 IEEE 802.11의 핸드오프 과정 중 재접속 단계뿐만 아니라 새로운 AP를 발견하기 위한 스캐닝(Scanning) 단계에서도 지연시간이 나타나는 것을 간과했기 때문에 근본적인 해결점을 제시해주지 못하고 있다. 핸드오프 지연시간을 실제로 측정된 연구에서 스캐닝 단계에서의 지연시간의 비중이 전체 핸드오프 지연시간의 대부분을 차지하고 있음을 보여줌으로써 이러한 사실을 더욱 뒷받침하고 있다^[6].

따라서 본 논문에서는 기존의 논문에서 고려하지

않았던 스캐닝 단계에서의 지연시간의 원인을 알아보고 이를 해결하기 위한 새로운 스캐닝 알고리즘을 제안하고자 한다. 이를 위해 본 논문은 II절에서 핸드오프 지연시간을 핸드오프의 각 단계에 따라 다시 분류하고 스캐닝 단계에서 지연시간이 발생하는 원인을 분석하였다. 다음으로 III절에서 스캐닝 단계에서 발생할 수 있는 지연시간의 원인을 최소화 할 수 있는 새로운 스캐닝 알고리즘을 제안하고, IV절에서 이 방법의 성능을 분석하기 위해 OPNET을 사용하여 실제로 존재할 수 있는 네트워크 상황에서 스캐닝 지연시간의 변화를 기존의 IEEE 802.11의 스캐닝 시간과 비교하였다. V절에서는 본 논문의 내용을 정리하고 결론을 맺는다.

II. MAC 부계층에서 핸드오프 과정

IEEE 802.11에 대한 표준이 제정될 당시에는 건물 내의 사용을 목적으로 개발되었고 비록 사용자가 이동을 하더라도 넓은 지역간의 이동은 고려하지 않았기 때문에, 핸드오프에 대한 연구가 매우 부족했으며 표준도 제정되지 않았다. 따라서 현재 사용되고 있는 핸드오프 방식은 표준에 언급되어 있지는 않지만, 단말기가 처음으로 IEEE 802.11 네트워크에 접속하기 위해 AP를 찾는 과정을 이용하여 핸드오프를 구현하고 있다.

본 절에서는 핸드오프 도중에 AP와 단말기가 주고받는 메시지의 전송방식을 알기 위하여 IEEE 802.11 MAC 부계층에서의 DCF(Distributed Coordinator Function) 전송방식을 살펴보고 IEEE 802.11에서 핸드오프를 어떻게 수행하는가를 알아보고자 한다. 앞으로 논의할 핸드오프 지연시간을 분석하기 위하여 우선 핸드오프 과정을 세분화하고 각 단계에서 발생하는 지연시간을 분석하는 과정이 반드시 필요하다.

1. DCF

DCF는 IEEE 802.11의 MAC에서 가장 기본이 되는 경쟁 기반의 서비스를 제공하는 전송방식이다. 이 방식에서는 CSMA/CA를 사용하며 경쟁을 통해 채널의 사용권을 획득한 단말기만이 프레임 전송할 수 있다. 또한 전송하는 프레임의 종류에 따라 채널 사용권의 우선권을 주기 위하여 IEEE 802.11은 IFS (InterFrame Space)라는 시간을 여러 개로 분류하여 사용하고 있다^[1].

그림 1은 RTS/CTS (Request To Send/Clear To

Send)를 사용하는 DCF 전송방식을 보여주고 있다. RTS/CTS는 무선 채널에 잡음(Noise)이 많아 전송 오류가 잦을 때 전송율(throughput)을 높이기 위해 사용하고, 숨겨진 노드 문제 (Hidden Node Problems)를 해결하기 위해서 사용된다. 우선 프레임을 송신하려는 단말기는 RTS 프레임의 수신측에게 전송하며 그 외의 다른 단말기들은 이 RTS의 내용을 참고하여 송신측이 송신한 프레임에 대한 ACK (Acknowledgement)를 받을 때까지의 시간을 의미하는 NAV(Network Allocation Vector)를 설정한다. NAV를 설정한 단말기들은 이 시간동안 채널의 사용권을 획득하려는 시도를 하지 않는다. RTS를 수신한 단말기는 이에 대한 응답으로 SIFS(Short Inter Frame Space)의 시간을 기다린 후 CTS 프레임을 보낸다. 여기서 SIFS는 RTS/CTS 프레임이나 ACK와 같은 가장 높은 우선권을 가진 프레임의 전송을 위하여 사용하는 시간으로 DCF에서 사용하는 IFS중에서 가장 짧은 시간을 가진다. RTS경우와 마찬가지로 그 외의 단말기들은 CTS에 의한 NAV를 설정한다. CTS 프레임을 받은 송신측은 SIFS 시간 후에 데이터 프레임을 전송하고 이를 수신한 수신측은 SIFS시간 이후에 ACK를 송신측에게 전송한다. 이러한 과정으로 하나의 데이터 프레임이 전송되며 전송이 완료된 후 모든 단말기들은 DIFS (Distributed InterFrame Space)시간을 기다린다. DIFS는 SIFS보다 긴 시간을 가지고 있으며 이 시간동안 채널이 사용 중이 아니면 단말기들은 채널을 사용하기 위한 경쟁에 들어간다.

DIFS이후에 모든 단말기들이 전송을 시작하면 충돌(Collision)이 발생하기 때문에 이를 피하기 위해 각 단말기들은 임의의 시간을 더 기다린 후 채널에 대한 사용권을 획득할 수 있다. 이 시간을 백오프(random backoff) 시간이라 하며 DIFS이후에 채널이 사용되지 않는 시간동안 감소한다. 만약 어떤 단말기가 백오프 도중에 다른 단말기의 전송 사실을 알게 되면 이 단말기는 백오프 시간을 중지시키고 전송이 완료된 후 DIFS시간 이후에 중지시켰던 백오프 시간을 다시 감소시킨다. 백오프 시간이 0이 된 단말기는 채널에 대한 사용권을 획득하게 되고 앞서와 같은 RTS/CTS 프레임을 전송하게 된다.

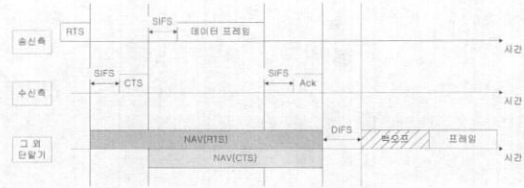


그림 1. RTS/CTS를 사용한 DCF 전송방식.
Fig 1. DCF with RTS/CTS.

2. 스캐닝 단계 (Scanning Phase)

스캐닝이란 IEEE 802.11에서 단말기가 네트워크에 접속하기 위해 AP를 찾는 단계이다. 이 단계를 통해 단말기는 AP에 접속하기 위하여 필요한 모든 정보를 알아낼 수 있다. 그 정보에는 AP의 물리 계층의 전송율이나 동기화정보, AP의 MAC 주소를 나타내는 BSSID(Basic Service Set Identification), 네트워크를 편리하게 구별하기 위해 AP의 MAC주소 대신 문자를 사용하는 SSID(Service Set Identification)등이 있다. 한 네트워크(Basic Service Set, BSS)에 속해있는 단말기가 네트워크 바깥쪽으로 이동을 하면 현재 접속중인 AP로 부터 멀어지면서 AP로부터 받는 신호의 세기(Signal-to-Noise Ratio, SNR)도 점점 약해질 것이다. 이 신호가 일정한 크기의 신호세기(cell search threshold)보다 더 떨어지게 되면 단말기에서는 계속 네트워크와 접속을 하기 위하여 새로운 AP를 찾기 위한 단계를 진행한다. 단말기는 이 스캐닝 단계를 현재 사용하고 있는 전송방식에서 사용할 수 있는 모든 채널에 대해서 순차적으로 진행한다. IEEE 802.11에서 사용가능한 전송 방식은 FHSS(Frequency Hopping Spread Spectrum)와 DSSS(Direct Sequence Spread Spectrum)와 적외선(Infrared)이 있으며 각각의 물리영역의 특성에 따라 사용할 수 있는 채널이 존재한다[1]. 각각의 전송방식을 설명하는 것은 본 논문의 범위를 넘는 것이므로 생략한다.

스캐닝 방법은 수동(passive) 스캐닝 방법과 능동(active) 스캐닝 방법이 있다^[7]. 수동 스캐닝 방식은 AP가 주기적으로 보내는 비콘(beacon) 프레임을 단말기가 단순히 수신함으로써 이루어진다. 단말기는 스캐닝을 해야 하는 상황이 되면 모든 데이터 전송을 중지하고 한 채널에 대해서 정해진 시간동안 AP가 보내는 비콘 프레임을 수신한다. 이 과정을 전송 방식에 따라 사용 가능한 모든 채널에 대해서 수행한 후 수신한 비콘 프레임의 신호 세기를 분석하여 가장 높은 신호 세기를 가진 비콘 프레임을 보낸

AP에게 접속을 시도한다. 수동 스캐닝이 AP에게 비콘을 수동적으로 기다리고 있는 반면, 능동 스캐닝은 단말기가 스캐닝을 진행할 상황이 되면, 직접 AP에게 재접속을 위한 정보를 요청하는 프로브 요청(probe request)을 보내는 것으로 시작된다. 프로브 요청을 보낸 단말기는 다른 단말기들과의 경쟁을 통해서 채널에 접속할 수 있는 권한을 얻게 되고, 그 후 브로드캐스트 메시지로 프로브 요청 프레임 전송한다. 브로드캐스트 메시지로 프로브 요청 프레임이 전송되었기 때문에 단말기와 통신 가능한 모든 AP는 이에 응답을 하게 된다. AP는 일반적인 데이터를 전송하는 방식에 따라 프로브 응답 프레임을 프로브 요청을 보낸 단말기에게 전송하게 된다. 수동 스캐닝과 마찬가지로 단말기는 사용 가능한 모든 채널에 대해 이 작업을 반복 수행하고 수신된 프로브 응답 메시지를 분석하여 전파세가 가장 강한 AP에 접속을 시도한다. 이 과정에서 단말기는 어떠한 데이터 통신도 진행할 수가 없기 때문에 연결이 단절되는 시간이 발생하게 된다. 그러나 핸드오프를 수행하고 있는 단말기를 목적으로 하는 프레임이 계속해서 기존의 AP로 올 수 있기 때문에 AP는 이를 보관하여 재접속단계에서 새로운 AP로 넘겨주는 과정을 진행하게 된다.

AP에서 비콘 프레임을 주기적으로 보내는 간격은 일반적으로 100ms이상의 시간을 사용하기 때문에 같은 시간동안 스캐닝을 진행했을 때 수동 스캐닝은 능동 스캐닝에 비해 정확한 네트워크 정보를 알아내기가 어렵다. 그러므로 수동 스캐닝은 한 채널에 대한 스캐닝 시간이 능동 스캐닝보다 더 길어야 한다. 이런 이유로 인하여 현재 대부분의 IEEE 802.11 장비들은 핸드오프 지연시간을 줄이기 위해 능동 스캐닝 방식을 사용하고 있다^{[6][7]}. 본 논문에서 제안하는 핸드오프 방식도 능동 스캐닝 방식을 사용한다.

3. 재접속 단계 (Reassociation Phase)

스캐닝이 네트워크에 대한 정보를 얻는 단계라면 재접속 단계는 네트워크에 접속하기 위해 AP에게 접속을 요청하는 단계라 할 수 있다. 단말기는 스캐닝 단계를 통해 인접한 AP에 대한 정보를 알아내면 그 중에서 가장 강한 신호를 보낸 AP에 접속하기 위한 과정을 진행한다.

재접속 단계는 인증(authentication)단계와 재접속(re-association)단계로 세분할 수 있다. 인증단계는 유선 네트워크처럼 물리적인 접근에 의해 내재적으

로 보안성을 제공할 수 없는 무선 네트워크에 보안성을 강화하기 위한 과정이다. 인증은 언제나 단말기에서 AP로의 단방향으로 진행되며, 단말기가 AP에 인증 요청 메시지(Authentication request message)를 보내는 것으로 시작된다. 이 메시지를 인증하기 위하여 개방-시스템 인증(Open-System Authentication)과 공유키 인증(Shared-Key Authentication)방법을 사용한다. 개방-시스템 인증의 경우는 단순히 단말기가 인증을 요청하게 되면 AP는 이를 받아들이는 방법으로 보안의 의미는 들어있지 않다. 공유키 인증방식은 WEP(Wired Equivalent Privacy)표준에 따라 인증하는 방식이며 이를 위해 단말기와 AP에 WEP이 모두 구현되고 같은 공유키를 모두 가지고 있어야 한다.

각 인증방식에 따라 인증이 완료되면 단말기는 네트워크에 접근을 획득할 수 있도록 AP와 재접속할 수 있다. 인증과 마찬가지로 재접속 단계도 단말기가 재결합 요청 메시지를 보내는 것으로 시작된다. 이 재결합 메시지에는 단말기가 기존에 연결되어 있던 현재 AP의 주소가 들어있다. 이미 인증단계를 거친 새로운 AP는 새로운 결합ID(Association ID, AID)와 함께 결합 응답 메시지를 단말기에게 전송한다. 앞부분에서 설명한바와 같이 기존의 AP는 핸드오프를 진행하고 있는 단말기로 전달되는 프레임을 보관하고 있다. 이를 전송받기 위해 새로운 AP는 기존의 AP에게 재결합을 요청한 단말기가 받아야할 프레임을 IAPP(Inter-Access Point Protocol)을 통해 요청하게 되고 기존의 AP는 그 단말기와의 연결을 종료하고 보관하고 있던 프레임을 새 AP에게 전달하게 된다. 이를 받은 새 AP는 재결합 된 단말기에게 전달받은 프레임을 전송하면서 재결합 단계가 종료된다.

4. IEEE 802.11 핸드오프 지연시간 분석

최근의 연구에 따르면 IEEE 802.11에서 발생하는 전체 핸드오프는 장비 구성에 따라서 최고 300ms가 넘는 시간이 걸린다^[6]. 음성 통신을 위한 지연시간이 30ms가 넘으면 음성에 열화가 발생하며 최소한의 원활한 음성 통신을 위한 최대 지연시간을 ITU(International Telecommunication Union)에서 150ms로 권고하고 있기 때문에 300ms가 넘는 핸드오프 지연시간은 IEEE 802.11이 VoIP(Voice over IP)와 같은 실시간 서비스를 지원하는데 커다란 문제점으로 나타날 수 있다^[8].

이와 같은 문제점을 해결하기 위해 지금까지 수

행된 연구에서는 핸드오프 지연 문제를 재접속 단계 중 인증단계에서의 지연을 최소화하는데 중점을 두고 있었다²⁻⁵⁾. 그러나 이러한 접근 방법은 단말기가 AP를 찾는 과정에서 발생할 수 있는 지연시간을 간과하고 있었으며 이러한 연구가 전체 핸드오프 지연시간을 단축하는데 부족하다는 것이 최근에 실측을 통하여 핸드오프를 분석한 연구 결과에서 밝혀졌다. 이 연구에서는 핸드오프 지연시간의 90% 정도가 스캐닝 단계에서 발생하고 있다는 것을 보여주고 있다⁶⁾. 따라서 본 논문에서는 기존의 연구 결과와는 달리 핸드오프 지연시간을 최소화하기 위해 스캐닝 단계에서의 지연시간을 최소화하는 것에 초점을 맞추고자 한다. 우선 새로운 스캐닝 방법을 설명하기에 앞서 스캐닝 단계에서 지연시간이 발생하는 원인을 좀더 분석해 볼 필요가 있다. 핸드오프를 하기 위한 과정은 앞 절에서 밝힌바와 같이 능동 스캐닝에서 일어나는 과정을 사용할 것이다.

능동 스캐닝 방식을 다시 살펴보면 단말기가 일정한 신호세기보다 낮은 신호를 수신했을 때 프로브 요청 프레임을 보내는 것으로 핸드오프 과정을 시작한다. 단말기는 브로드캐스트 주소를 사용하여 한 채널에 프로브 요청 프레임 전송한다. 그 후 단말기는 현재 채널을 사용하는 AP가 실제로 존재하는가를 결정하기 위해 정해진 최소 탐색시간(MinChannelTime)동안 채널의 신호를 감지하는 동작을 취한다. 이 시간 안에 채널이 사용 중이라는 것을 감지하게 되면 단말기는 현재 채널에 AP가 존재한다고 판단하게 된다. AP가 존재한다고 판단하면 다시 정해진 최대 탐색시간(MaxChannelTime) 동안 해당 채널을 사용하는 모든 AP에서 보내는 프로브 응답 프레임을 수신하는 것으로 하나의 채널에 대한 스캐닝을 완료한다. 이 과정은 현재 IEEE 802.11 네트워크를 구성하는 물리 매체의 전송방식에 따라 사용할 수 있는 모든 채널에 대해 모두 수행된다. 스캐닝이 완료되면 프로브 응답을 분석하여 가장 강한 신호를 보낸 AP에 재접속을 시도한다¹¹⁾⁷⁾.

위 과정에서 주목할 만한 부분은 어떤 채널에 네트워크가 존재한다고 판단했을 때 단말기가 그 채널에서 MaxChannelTime까지 프로브 응답 프레임을 계속 수신하는 동작을 취하고 있는 점이다. 이러한 과정을 진행하는 이유는 프로브 응답 프레임이 일반적인 데이터 프레임과 동일한 방법으로 전송되기 때문에 충분한 시간을 두고 AP에 대한 정확한 정보를 단말기에게 알려주기 위해서이다. 같은 채널

을 사용하는 AP가 여러 개 존재하는 네트워크에서 DCF 방식을 따라 전송되는 각 AP의 프로브 응답 프레임은 MinChannelTime 시간 안에 모두 전송되지 못한다. 그러므로 단말기가 MaxChannelTime까지 계속해서 프로브 응답을 기다리는 것은 정확한 네트워크 정보를 얻을 수 있는 합리적인 방법이라 할 수 있다. 그러나 프로브 응답 프레임은 MaxChannelTime이 되기 전에 모두 전송되는 경우도 존재할 수 있다. 이러한 경우 단말기는 프로브 응답 메시지가 더 이상 전송되지 않는 경우에도 MaxChannelTime까지 계속 스캐닝을 진행해야하기 때문에 불필요한 시간을 낭비하게 된다.

III. 가변적인 검색 시간을 이용한 스캐닝 방법 (Dynamic Scanning Phase)

IEEE 802.11에서 단말기는 네트워크 상에 존재하는 AP의 위치나 개수를 알지 못한다. 그렇기 때문에 단말기는 핸드오프를 하기 위하여 어떤 한 채널에서 네트워크가 존재한다고 판단되었을 때 그 채널에서 MaxChannelTime까지 스캐닝을 진행하여 그 채널을 사용하는 AP들에 대한 정보를 가능한 많이 수집해야 하고, 사용 가능한 모든 채널에 대해서 같은 방식으로 전체 네트워크에 대한 정보를 얻어야 한다. 그러나 단말기가 MaxChannelTime까지 프로브 응답을 수집하는 기존의 방법은 정확한 네트워크에 대한 정보를 알 수는 있지만, MaxChannelTime 이전에 모든 AP에 대해서 프로브 응답을 전송받은 이후에도 불필요한 시간을 계속해서 프로브 응답 수신에 소비하게 되는 문제점이 있다는 것을 앞 절에서 설명하였다.

본 논문에서는 단말기가 AP를 찾는 과정에서 수신이 가능한 모든 프로브 응답을 받은 상황에서는 스캐닝을 MaxChannelTime 이전에도 끝마칠 수 있도록 하는 알고리즘을 제안하여 이와 같이 불필요한 시간낭비를 피하는 방법을 모색하고자 한다. 이 방법은 단말기가 프로브 요청 프레임 보낸 이후 이를 수신한 AP는 이에 대해서 반드시 응답해야 하며 프로브 응답 프레임은 DCF 방식에 따라 일반적인 데이터 프레임과 같은 방식으로 전송한다는 것을 이용한다. 앞서 밝힌바와 같이 프로브 응답을 보내야 하는 AP가 다수일 때, 각각의 AP들은 다른 AP가 존재한다는 것을 알지 못한다. 따라서 AP들은 서로의 전송 상태와 무관하게 프로브 응답 프레임이나 데이터 프레임을 전송하게 될 것이다. 그러

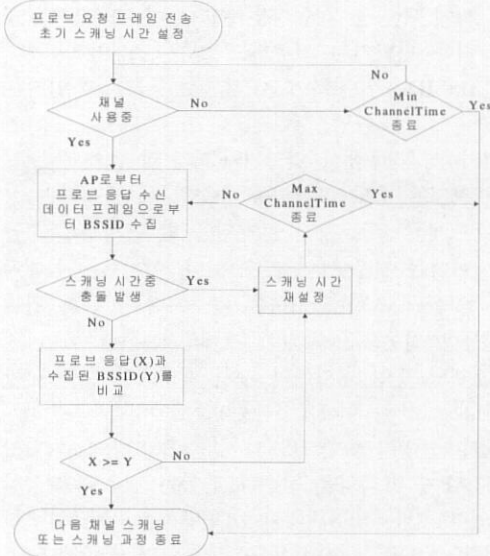


그림 2. 가변적인 스캐닝 시간을 사용하는 알고리즘.
Fig. 2. Proposed algorithm using dynamic scanning interval.

므로 스캐닝 단계에서 충돌이 발생하지 않았다면, 현재 프로브 응답 프레임을 보낸 AP가 1대라고 판단할 수 있다. 단말기는 이러한 점을 이용하여 충돌이 발생했다면 1대 이상의 AP가 있다고 판단한다. 이에 대한 자세한 설명은 아래 부분에서 다시 할 것이다. 채널상의 충돌은 단말기의 수신부에서 잡작스런 신호 레벨의 변화를 살펴봄으로써 판별할 수 있다.

가변적인 스캐닝 시간을 적용하기 위해서는 현재 IEEE 802.11에서 지원하는 기능만으로는 부족한 점이 있기 때문에 새로운 기능의 추가가 필요하다. 이를 위하여 다음과 같은 가정을 바탕으로 알고리즘을 설명하고자 한다.

- AP는 자신에게 버퍼링된 데이터보다 우선적으로 프로브 응답 프레임을 전송한다. 이것은 AP에서 프레임 응답이 다른 데이터 프레임의 전송보다 우선적으로 처리되도록 하기 위해서이다. 현재 AP에서 데이터 프레임이 전송되기 위해 대기 중이라 하더라도 프로브 요청 프레임을 받으면 우선적으로 프로브 응답 프레임을 전송하도록 한다.
- 단말기는 BSSID를 포함하고 있는 모든 프레임에서 BSSID의 확인이 가능케 한다. IEEE 802.11의 대부분의 프레임에는 프레임이 AP로

전송되거나 단말기로 전송되느냐에 따라 이를 구분하는 필드가 있으며, 이에 따라 BSSID가 주소 필드에 반드시 존재한다. 그러므로 프레임 헤더 정보와 주소 필드들의 정보를 사용하여 BSSID만을 확인할 수 있다.

그림 2는 가변적인 스캐닝 시간을 사용한 스캐닝 알고리즘을 설명한 순서도이다. 단말기는 프레임 요청 프레임을 보낸 후 네트워크의 존재 유무를 판단하기 위해서 MinChannelTime동안 무선 채널의 상태를 감지한다. MinChannelTime까지 무선 채널이 사용 중(busy)이 아니면 단말기는 현재 채널에서 네트워크가 존재하지 않는다고 판단하고 다음 채널의 스캐닝을 시작하거나 종료한다. MinChannelTime이 끝나기 전에 네트워크가 존재한다고 판단되면, 단말기는 MaxChannelTime까지 프로브 응답 프레임을 기다린다. 단말기가 기다리는 시간은 하나 이상의 프로브 응답 프레임을 수신할 수 있는 시간이다. 이 시간은 다음과 같은 과정을 통해 구할 수 있다.

프로브 요청 프레임을 받은 후에 AP에서는 프로브 응답 프레임을 DCF방식에 따라 전송하려 한다. 이를 위해 우선 AP는 다른 단말기들과 채널을 확보하기 위한 경쟁을 시작한다. 경쟁을 하기 위해서 AP는 다음과 같은 방법으로 백오프 값을 생성한다 [14].

$$\text{backoff window} = \text{random}(0, \text{CW}). \quad (1)$$

여기서 사용하는 random()는 균등 분포(uniform distribution)를 따르는 랜덤 함수이며 결과값으로 정수값을 반환한다. 경쟁윈도우(Contention Window, CW)는 물리 매체에서 사용하는 전송방식에 따라 그 값이 표준에 정의되어 있다. 예를 들어 FHSS를 사용하는 경우 가장 처음 백오프 윈도우를 생성할 때 사용하는 CW인 CWmin는 15, 충돌이 발생하여 2진 지수 백오프(Binary exponential backoff)에 따라 증가할 수 있는 최대 CW는 CWmax=1023, DSSS를 사용하는 경우 CWmin=31, CWmax=1023이다. 이 백오프 윈도우는 한 슬롯시간(Slot_Time, Tslot)마다 하나씩 감소하게 된다. 슬롯시간이란 물리 매체에서 사용하는 전송방식의 특성을 나타내는 시간으로 여기에는 송수신부 전환 시간(RxTxTurn AroundTime), 공기 중에서 전파가 전달되는 시간(AirPropagationTime)등이 포함된다. 슬롯시간은 FHSS에서 50μs, DSSS에서는 20μs로 정의되어 있

다¹¹⁾. 식 (1)을 사용하여 백오프 윈도우를 생성하기 때문에 채널 사용권을 얻는 경쟁을 위해 새롭게 백오프 윈도우를 생성하는 단말기가 가질 수 있는 최대 백오프 윈도우의 크기는 CW_{min}값이 된다.

단말기에서 백오프 시간이 최대로 생성되었을 때를 기준으로 프로브 응답 프레임 기다리고 있으면, 최소한 하나 이상의 프로브 응답을 수신할 수가 있다. 만약 이 시간동안 프로브 응답 프레임이 전송되지 못하고 데이터 프레임이 전송되었다면 단말기가 데이터 프레임으로부터 BSSID를 수집할 수 있으므로 AP가 더 존재하고 있는지에 대한 판단을 내릴 수 있게 된다. 백오프 시간이 지난 후, 단말기가 프로브 응답을 모두 수신하기 위해서는 프로브 응답 프레임의 전송에 걸리는 시간(T_{Probe})을 고려해야 한다. 따라서 단말기가 완전한 프로브 응답 프레임을 수신하기 위해 필요한 최대 시간은 식 (2)와 같이 프로브 응답 프레임이 전송되기 전에 소요될 수 있는 가장 긴 백오프 시간과 프로브 응답 프레임이 전송되는 시간의 합으로 표현될 수 있다. 초기 스캐닝 시간(Initial Scanning Interval, T_{ISI})의 실제에는 시뮬레이션을 설명하는 부분에서 다시 할 것이다.

$$T_{ISI} = CW_{min} \cdot T_{Slot} + T_{probe} \quad (2)$$

여기서 프로브 응답 프레임의 크기가 가변적이기 때문에 이 전송시간은 달라질 수 있다. 그러나 프로브 응답 프레임의 크기를 결정하는 요소인 SSID는 관리자가 임의로 설정할 수 있는 값이기 때문에 일정한 크기를 유지할 수 있다. 이 시간 안에 전송되는 프레임에 따라 스캐닝을 진행하는 단말기에서는 다음의 3가지 경우의 상황이 발생한다.

- 단말기가 보낸 프로브 요청에 응답할 수 있는 AP가 하나인 경우, 첫 번째 스캐닝 시간동안 프로브 응답 프레임은 하나만이 도착한다.
- 같은 채널을 사용하는 다수의 AP가 프로브 요청에 응답하는 경우, 첫 번째 스캐닝 시간동안 여러 개의 프로브 응답 프레임이 도착하여 충돌이 발생한다.
- 현재 무선 채널에 네트워크가 존재한다는 신호는 감지되었으나 프로브 응답 프레임이 도착하지 않는 경우, 이 경우는 프로브 응답을 보내기 위한 채널 확보 경쟁을 하고 있는 AP와 같은 BSS안에 있는 다른 단말기가 채널을 확보

하여 전송을 하는 경우이다. 이 때 스캐닝을 하는 단말기는 전송되고 있는 프레임으로부터 BSSID를 수집하여 AP의 존재를 알 수 있다.

위의 세 경우에서 단말기가 임의의 스캐닝 시간 동안 프로브 응답 프레임을 수신할 때 발생하는 상황은 크게 프로브 응답 프레임을 받는 경우와 충돌이 일어나는 경우로 나눌 수 있다. 여기서 주목해야 하는 것은 충돌이 일어나는 경우이다. 잡음과 같은 채널상의 전송오류에 의한 프레임 손실이 아닌 경우 스캐닝 중인 단말기의 수신 채널에서 충돌이 발생한다는 것은 현재 수신중인 프레임을 전송하는 단말기나 AP가 속한 BSS와 다른 BSS에 속한 단말기나 AP가 프레임을 전송하고 있는 경우로 해석할 수 있다. 같은 BSS내에서 DCF방식을 사용하는 단말기와 AP들은 프레임안의 지속시간 필드(Duration/ID field)를 확인함으로써 지속 시간동안에는 NAV를 설정하여 채널에 접근을 시도하지 않는다. 따라서 같은 BSS내에서 한 단말기가 프레임을 전송중일 때는 다른 단말기들은 프레임을 전송할 수 없다. 이와 같은 사실을 바탕으로 현재 스캐닝 중인 단말기의 수신채널에서의 충돌은 다른 BSS가 존재한다고 판단할 수 있으며 이는 또 다른 AP가 존재한다는 의미로 해석할 수 있다.

일반적으로, 각 BSS안의 AP는 서로의 존재를 알 수 없기 때문에 각각의 AP에서 독립적으로 전송을 하게 된다. 그러므로 앞에서 설정한 초기 시간동안 프로브 응답이 2개 이상 도착한다면 두 프로브 응답 프레임은 이 시간동안에 충돌을 발생시킨다. 그러나 프로브 응답 프레임을 보내는 AP가 하나만 존재하는 경우 이 시간 안에 프로브 응답 프레임이 충돌을 발생시키지 않고 도착할 확률이 높기 때문에 매우 빠른 시간 안에 스캐닝을 종료할 수 있다.

단말기에서 충돌이 발생하면 프로브 응답에 해당하는 ACK를 받지 못하기 때문에 DCF 방법에 따라 이를 전송한 AP는 재전송을 시도하게 된다. 이 때 CW는 2진 지수 증가에 의해 2배로 증가하게 된다. 단말기가 백오프를 하기 위한 시간이 증가하기 때문에 스캐닝을 위한 시간의 재설정성이 필요하다. 재설정된 시간(2nd Scanning Interval, T_{2nd_SI})은 식 (3)과 같다.

$$T_{2nd_SI} = \{2 \cdot (CW_{min}+1)-1\} \cdot T_{Slot} + T_{probe} \quad (3)$$

이 시간동안 충돌이 발생하게 되면 계속 CW값이

증가하기 때문에 단말기가 프로브 응답을 기다리는 시간을 이에 맞추어 재설정해야 한다. 단말기에서 $n-1$ 번째 스캐닝 구간에서 충돌을 감지했을 때 프로브 응답을 기다리는 시간(n th Scanning Interval, T_{nth_SI})은 식 (4)로 표현할 수 있다.

$$T_{nth_SI} = \{2^{n-1} \cdot (CW_{min}+1)-1\} \cdot T_{Slot} + T_{probe}. \quad (4)$$

이와 같이 충돌이 발생했을 때마다 단말기는 스캐닝 시간을 늘려가며 프로브 응답 프레임 수신한다. 그러나 채널상의 충돌 유무로만 AP의 존재를 확인하는 것은 정보가 부족할 수 있다. 예를 들어 초기 스캐닝 시간을 설정한 단말기에서 이 시간동안 충돌이 감지되지 않았지만 프로브 응답이 전송되지 못하고 데이터 프레임이 전송된 경우를 생각해 보자. 충돌이 발생하지 않아 단말기는 스캐닝을 중단할 수 있는 조건이 만족되었지만 실제로 프로브 응답 프레임을 수신하지는 못했다. 이처럼 잘못된 정보로 인한 스캐닝 중단을 방지하기 위해서 단말기는 데이터 프레임으로부터 BSSID를 수집한다. 스캐닝 중에 충돌이 발생하지 않은 경우, 앞서 설명한 바와 같이 단말기에 프로브 응답 프레임외의 다른 데이터 프레임이 전송된다. 단말기는 이 프레임으로부터 수집한 BSSID를 프로브 응답에서 전송된 BSSID와 비교하여 AP의 존재 가능성을 예측할 수 있다. 만약 수집한 BSSID와 수신된 프로브 응답을 통해 수집된 BSSID를 비교하여 더 많은 BSSID를 데이터 프레임으로부터 수집했다면 아직 프로브 응답 프레임을 전송하지 못한 AP가 존재하고 있다는 의미로 해석할 수 있다. 그러므로 이러한 상황에서 단말기는 프로브 응답 프레임을 수신하기 위하여 채널에서 충돌이 발생하지 않았더라도 프로브 응답 프레임을 기다리는 시간을 늘려가며 계속 스캐닝을 진행한다. 수집한 BSSID와 프로브 응답에서 전송된 BSSID가 모두 일치하거나 프로브 응답에 의한 BSSID를 더 많이 수신한 상태에서, 채널 상에서 충돌이 발생하지 않는다면 수집 가능한 프로브 응답 프레임을 모두 수신했다고 판단할 수 있기 때문에 현재 설정된 스캐닝 시간이 완료됨과 동시에 현재 채널의 스캐닝을 종료한다.

겹쳐진 BSS내의 트래픽 부하가 높은 경우 스캐닝 단계에서 다른 데이터 프레임과 프로브 응답 프레임사이의 충돌이 발생할 확률이 높아진다. 그리고 AP가 계속해서 프로브 응답 프레임을 보내기 위한 경쟁에서 채널을 획득하지 못하면 수집한 BSSID와

프로브 응답내의 BSSID가 일치하지 않거나 프로브 응답을 전혀 받지 못하는 경우가 발생할 수 있다. 이때는 기존의 스캐닝 방식과 동일하게 MaxChannel Time까지만 스캐닝을 진행하고 현재 채널에 대한 스캐닝을 중단함으로써 핸드오프 지연시간이 더 발생하는 것을 방지한다.

IV. OPNET을 이용한 시뮬레이션 분석

본 논문에서는 기존의 IEEE 802.11에서 사용하는 스캐닝 방식과 본 논문에서 제안한 스캐닝 방식의 성능을 비교하기 위해 OPNET 시뮬레이터를 이용하여 서로의 스캐닝 시간을 비교하였다^[11]. 본 시뮬레이션에서는 프로브 응답 프레임이 전송되었을 때 충돌이 발생하고 이에 의해 스캐닝 시간이 증가하는 점만을 고려하기 위해 무선 채널 상에서 발생하는 비트 오류에 의한 프레임 손실은 없는 것으로 가정하였다.

일반적으로 사용되는 IEEE 802.11은 대부분 겹쳐진 BSS간에 간섭(interference)이 없도록 채널을 설정하지만 ISM(Industrial Scientific and Medical equipment)대역을 사용하는 IEEE 802.11은 사용할 수 있는 채널 수가 한정되어 있기 때문에 넓은 영역에 네트워크를 구축하기 위해서 불가피하게 같은 채널이 겹쳐진 구간이 존재할 수 있다. 그러나 실제 네트워크를 구축할 때 가능하면 중복되는 채널을 사용하지 않기 때문에 3개 이상의 BSS가 같은 채널을 사용하는 경우는 의미가 없다고 판단하여, 본 논문에서는 모든 BSS가 다른 채널을 사용하는 경우와 두개의 겹쳐진 BSS가 같은 채널을 사용하는 경우의 시나리오를 구성하여 시뮬레이션을 진행하였다. 시뮬레이션에서 사용된 IEEE 802.11의 전송방식은 DSSS를 사용하고 각각의 시뮬레이션에서 사용한 파라미터는 표 1에서 보여주고 있다. 이 파라미터들은 IEEE 802.11의 표준에 제시된 값을 따른다^[11]. 전송방식으로 DSSS를 선택한 것은 DSSS가 현재 IEEE 802.11에서 가장 많이 사용하고 있는 전송방식이므로, 이 같은 설정이 실제 네트워크 상황을 가장 잘 반영할 수 있기 때문이다.

IEEE 802.11은 신호의 세기에 따라서 여러 전송 속도를 지원하는데 신호 세기가 낮을 때는 전송 오류를 줄이기 위하여 1Mbps의 속도만을 사용할 수 있다. 핸드오프 순간에는 신호의 세기가 가장 약하기 때문에 단말기는 1Mbps의 전송속도만을 사용한

표 1. 시뮬레이션 파라미터

항 목	설정값
MinChannelTime	3ms
MaxChannelTime	30ms
CWmin	31
CWmax	1023
SIFS	10 μ s
Slot_Time	20 μ s
DIFS(SIFS+2T _{slot}) ⁽¹⁾	50 μ s
Transmission rate	1Mbps

다. 또한 프로브 메시지와 같은 관리 프레임(Management frame)을 전송할 때 반드시 1Mbps만을 사용하기 때문에 본 시뮬레이션에서도 1Mbps의 전송속도를 사용하였다. 프로브 요청 프레임은 브로드캐스트 BSSID를 사용하여 단말기에서 AP로 전송되고, 프로브 응답 프레임은 단일 주소를 사용하여 일반 데이터 프레임과 같은 DCF방식으로 단말기에게 전송된다. 이때 프로브 응답 프레임의 크기는 50바이트를 고정으로 사용하였으며 데이터 프레임의 크기는 헤더를 포함하여 75.5바이트의 크기를 사용하였으며 데이터의 생성 간격(inter-arrival time)은 지수 분포(exponential distribution)를 사용하였다. DSSS에서는 BSS간의 간섭이 없도록 채널을 사용하기위해 중심주파수가 22MHz이상 떨어지도록 채널을 설정해야 한다. 이를 위해서 IEEE 802.11의 경우 최소 5개의 채널만큼 분리를 하여 채널을 사용해야한다. 따라서 시뮬레이션에서는 1번과 6번, 11번 채널을 사용했다.

본 논문에서는 핸드오프 상황을 시뮬레이션 하기 위해 그림 3과 같은 설정에서 BSS_A는 다른 BSS들과 간섭이 없는 채널을 사용하고 시나리오에 따라 BSS_B와 BSS_C가 동일한 채널을 사용하는 경우와 다른 채널을 사용하는 경우를 설정하였다. 모든 시나리오에서 BSS_A에 속한 단말기는 BSS_B와 BSS_C의 겹쳐진 영역으로 이동하여 핸드오프를 진행하게 된다. 동일한 채널을 사용하는 BSS사이의 겹쳐진 구간에서 단말기가 핸드오프를 진행하는 첫 번째 시나리오를 시뮬레이션 하기위해 그림 3에서 BSS_A에는 채널 1번, BSS_B와 BSS_C에 채널 6번을 설정하였다.

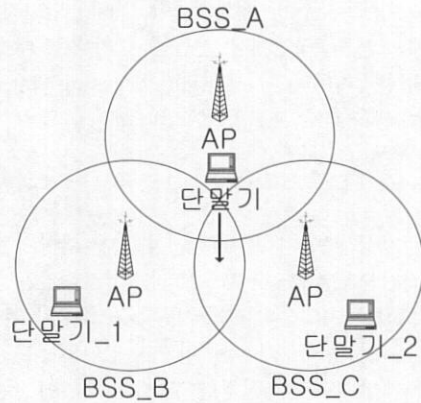


그림 3. 시뮬레이션을 위한 네트워크 구성도
Fig. 3. Simulation topology.

앞서 설명한바와 같이 각각의 BSS내의 AP와 마찬가지로 단말기들은 서로의 존재를 알지 못한다. 그러므로 각각의 BSS에 속한 단말기들은 같은 BSS내의 AP가 프로브 응답 프레임을 전송하지 않을 때 데이터 프레임을 보낼 수 있다. 이 때 전송되는 데이터 프레임은 핸드오프를 진행하고 있는 단말기에서 다른 BSS의 AP가 보내는 프로브 응답과 충돌을 발생시킬 수 있다. 이러한 현상이 스캐닝 시간에 미치는 영향을 알아보기 위해 BSS_A와 BSS_B에 각각의 BSS내에 계속 데이터 프레임을 보내는 단말기들(단말기_1, 단말기_2)을 설정하였다. 이 단말기들에서 전송되는 신호는 스캐닝을 진행하는 단말기에서 충분히 감지할 수 있도록 하여 RTS/CTS를 사용하지 않고 숨겨진 노드 문제를 해결할 수 있도록 설정하였다. 스캐닝을 진행하는 단말기는 BSS_A에서 BSS_B, BSS_C가 겹쳐진 영역으로 이동하게 된다. 이렇게 함으로써 단말기는 같은 채널을 사용하는 BSS의 겹쳐진 영역에서 핸드오프를 진행하게 된다.

그 후 스캐닝을 진행하는 단말기에서 프로브 요청 프레임을 보내고 BSS_B, BSS_C의 프로브 응답 프레임을 모두 받을 때까지의 시간을 측정하여 스캐닝 지연시간을 측정하였다. 다른 채널을 사용하는 BSS의 겹쳐진 구간에서의 핸드오프 시나리오에서는 그림 3에서 BSS_A에 채널 1번, BSS_B에 채널 6번, BSS_C에 채널 11번을 설정하였다. 마찬가지로 트래픽 부하를 주기위한 단말기들이 존재하며 BSS_A안에 있는 단말기가 BSS_B와 BSS_C의 겹쳐진 영역으로 이동했을 때 발생하는 스캐닝 지연

시간을 측정하였다. 마찬가지로 스캐닝 지연시간은 한 채널에 대한 지연시간을 알아보기 위해 단말기가 프로브 요청 프레임을 전송한 후 BSS_B에 대한 프로브 응답을 받을 때까지의 소비시간을 측정하였다.

시뮬레이션을 진행하기 위해서는 단말기가 사용할 초기 스캐닝 시간이 필요하다. 초기 스캐닝 시간은 식(1)을 사용하여 계산할 수 있다. 프로브 응답 프레임의 크기를 50바이트로 설정하였기 때문에 프로브 프레임의 전송시간은 다음과 같이 계산할 수 있다.

$$T_{probe} = DIFS + T_{overhead} + T_{Data} + SIFS + ACK = 900(\mu s). \quad (5)$$

$T_{overhead}$ 는 모든 프레임을 보내기 위해 반드시 사용해야하는 시간으로 송신기와 수신기를 동기화하기 위한 프리앰블(preamble)을 전송하는 시간이 이에 해당한다. T_{Data} 은 프로브 응답 프레임의 실질적인 데이터를 전송하는 시간을 뜻한다. 그러므로 초기 스캐닝 시간은 식 (2)에 따라 프로브 응답 프레임의 전송시간에 백오프 시간을 더한 시간이 되며 이를 식 (6)에서 보이고 있다. 이와 같은 방법을 사용하여 시뮬레이션을 위해 초기 스캐닝 시간을 구하기 위한 식 (2)와 충돌이 발생하여 단말기가 다시 설정하는 스캐닝 시간을 구하기 위한 식 (4)에 의해 계산된 스캐닝 시간들을 그림 4에서 그래프로 보여주고 있다.

$$T_{ISI} = CW_{min} \cdot T_{Slot} + T_{probe} = 31 \cdot 20 + 900 = 1520(\mu s). \quad (6)$$

기존의 핸드오프 방식을 그대로 사용하면 단말기가 네트워크가 존재한다고 판단한 후 MaxChannelTime까지 프로브 응답을 기다린다. 그러므로 한 채널을 검색할 때 최소한 MinChannelTime의 시간부터 최대 MaxChannelTime까지 시간을 소비할 것이다. 그러나 본 논문에서 제시하고 있는 방법은 MaxChannelTime에 도달하기 전에 필요한 조건이 만족되면 한 채널의 스캐닝을 중단하기 때문에 그보다 더 짧은 시간 안에 스캐닝을 종료 할 수 있다고 예상할 수 있다. 이것은 다음의 시뮬레이션 결과가 증명해주고 있다.

그림 5는 트래픽 부하를 각각의 BSS에서 동일하게 변화시키면서 부여했을 때, 기존의 스캐닝 방식과 본 논문에서 제안한 알고리즘들의 평균 스캐닝 시

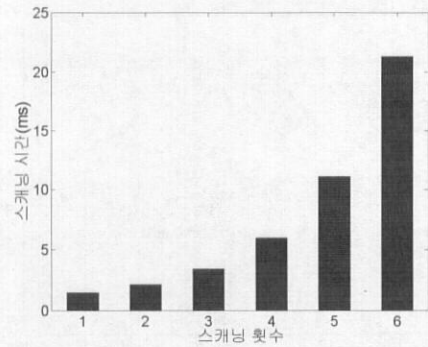


그림 4. 알고리즘을 통해 계산된 스캐닝 시간.
Fig. 4. Scanning interval through proposed algorithm.

간을 보여주는 결과 그래프이다. 시뮬레이션의 결과는 앞서 설명한 바와 같이 같은 채널을 사용하는 BSS들의 겹쳐진 영역에서의 스캐닝 지연시간과 다른 채널을 사용하는 BSS들의 겹쳐진 영역에서의 스캐닝 지연시간을 여러 번 측정하여 평균하였다.

기존의 스캐닝 방식을 쓰면, 단말기는 채널의 신호가 감지되면 무조건 프로브 응답 프레임을 30ms 동안 기다려야 하기 때문에 트래픽 부하와 상관없이 스캐닝 시간은 30ms로 일정하게 나타난다. 그에 비해 본 논문에서 제안하는 가변적인 스캐닝 시간을 사용하면, 시뮬레이션 결과에서 볼 수 있듯이 트래픽 부하에 따라 단말기가 AP의 존재 유무를 판단하여 MaxChannelTime이 되기 전에 스캐닝을 중지할 수 있기 때문에 더 적은 시간만을 소비하고 있음을 알 수 있다. 트래픽 부하가 낮음에도 어느 정도의 지연시간이 발생하는 이유는 한 AP가 프로브 응답 프레임을 전송하고 있을 때 다른 AP가 백오프를 마치고 프로브 응답 프레임을 전송하기 때문이다. 이것은 초기에 생성되는 스캐닝 시간 안에 모든 AP가 프로브 응답 프레임을 전송하기 때문이다. 이것은 같은 채널을 사용하는 AP가 다수 존재할 때 피할 수 없는 상황이다. 그러나 충돌이 발생한 이후 2진 지수 백오프에 의해 각각의 프로브 응답 프레임은 점차로 다른 시간에 전송이 되기 때문에 평균적으로 기존의 방식보다 빠른 시간 내에 스캐닝을 완료할 수 있게 된다.

일반적으로 IEEE 802.11을 사용하여 네트워크를 구축할 때는 각각의 BSS간에 채널이 서로 간섭이 없이 작동할 수 있도록 채널 분배를 잘 해줘야만 한다. 만약, 채널 분배가 제대로 이루어지지 않으면

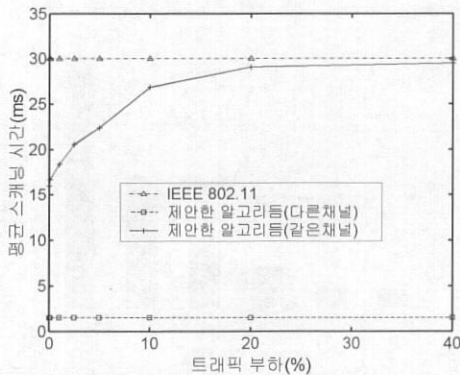


그림 5. 한 채널에서 트래픽 부하에 따른 평균 스캐닝 시간.
Fig. 5. Average scanning time according to traffic load in one channel.

각 BSS간의 프레임 전송이 다른 BSS에 영향을 미칠 수 있기 때문에 네트워크의 데이터 전송 성능이 떨어지게 되는 원인이 된다. 따라서 802.11 네트워크를 구축할 때는 BSS간에 서로 간섭을 일으키지 않는 채널을 사용하는 것이 일반적이다. 이런 환경을 만들기 위해서 본 논문에서는 앞서 설명한 바와 같이 서로 다른 채널을 사용하는 BSS를 구축하였다. 채널 분배가 잘 되어있다면 대부분의 경우 프로브 요청에 응답할 수 있는 AP는 1개일 것이다. 프로브 요청에 응답하는 AP가 하나만 존재하면 다수의 AP가 존재하는 경우와 달리 각 BSS사이에서 프로브 응답이나 다른 데이터 프레임과의 충돌이 존재하지 않기 때문에 트래픽 부하에 관계없이 스캐닝 시간을 더 이상 증가시키지 않고 스캐닝을 종료할 수 있게 된다. 시뮬레이션 결과에서는 이 경우 1.52ms의 초기 스캐닝 시간만이 스캐닝 지연시간으로 나타남을 알 수 있다. 동일한 채널을 사용하는 2개의 AP가 인접한 경우는 BSS간의 채널 분배가 제대로 이루어지지 못한 최악의 상황을 가정한 것이다. 기존 스캐닝 방식과 시뮬레이션 결과를 비교해보면, 본 논문에서 제안하는 방식은 트래픽 부하에 따라 스캐닝 지연시간이 약 15ms까지 떨어지는 것을 볼 수 있다.

시뮬레이션 결과에서 알 수 있듯이, 스캐닝을 진행하는데 기존의 고정적인 시간을 사용하는 것보다 네트워크 상황에 맞추어 가변적인 스캐닝 시간을 사용하는 것이 보다 뛰어난 결과를 보여줌을 알 수 있다. 실측을 통한 핸드오프 지연시간이 스캐닝 단계에서 대부분이 발생한다는 것을 알려주고 있기

때문에, 본 논문의 알고리즘이 보여주는 시뮬레이션 결과는 기존의 핸드오프 방식보다 보다 효과적이면서 지연시간이 짧은 핸드오프 방법을 제공할 수 있다.

IEEE 802.11은 무선 환경을 사용하기 때문에 본 논문에서 시뮬레이션 한 내용과 달리 전송 중에 비트 오류가 발생할 수 있다. 이로 인해 프로브 응답 프레임의 동시 전송뿐만 아니라 일반적인 상황에서도 채널에서의 오류로 인한 프로브 응답 프레임의 손실이 일어날 수 있다. 본 논문에서의 시뮬레이션은 이러한 상황을 가정하지 않았지만, 비트 손실에 의한 프레임 손실은 프로브 응답 프레임을 받지 못한 것과 동일하게 처리할 수 있으므로 본 논문에서 제안하는 알고리즘의 동작에는 영향을 미치지 않는다.

V. 결 론

기존의 핸드오프 방식은 스캐닝 단계에서 많은 지연시간을 보여, 핸드오프 중에 VoIP와 같은 실시간 대화형 서비스를 제공하기 어려운 문제가 있다. 본 논문에서는 이를 해결위해 단말기가 핸드오프시 채널을 검색할 때 고정적인 스캐닝 시간을 사용하는 것에서 벗어나, 네트워크 상황에 따라 가변적인 스캐닝 시간을 사용하게 함으로써 스캐닝 지연시간을 최소화하는 새로운 고속 핸드오프 방법을 제안하였다. 정확한 채널 분배로 인접한 AP가 서로 다른 채널을 사용한다면, 본 논문에서 제안한 방법을 사용했을 때, 스캐닝 지연시간은 무선 네트워크의 트래픽 부하와 관계없이 매우 짧은 시간만이 소요됨을 시뮬레이션을 통하여 알 수 있다. 같은 채널을 사용하는 AP가 두개 이상 인접할 때도 기존의 고정된 시간을 사용하는 스캐닝 단계보다 적은 시간이 소요되며, 특히 트래픽 부하가 낮을 때 짧은 시간만을 스캐닝에 소요함을 시뮬레이션 결과로 알 수 있다. 따라서 본 논문에서 제시한 핸드오프 방법은 기존의 핸드오프 방법에 비해 스캐닝 시간을 감소시킬 수 있으며 이에 따른 전체적인 핸드오프 지연시간도 줄일 수 있다.

본 논문의 시뮬레이션은 DSSS를 사용하여 수행되었지만, IEEE 802.11의 다른 전송방식인 FHSS를 사용한다 하더라도 사용되는 파라미터에 따라 스캐닝 시간을 조절함으로써 같은 방식의 알고리즘을 적용할 수 있다.

참 고 문 헌

- [1] IEEE 802.11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, November, 1999
- [2] S. Pack and Y. Choi, "Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN," *IEEE Networks* 2002, August 2002.
- [3] S. Pack and Y. Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x Model," *IFIP TC6 Personal Communications* 2002, October 2002.
- [4] R. Koodli and Charles E. Perkins, "Fast Handovers and Context Transfers in Mobile Networks," *ACM Computer Communication Review*, September 2001.
- [5] V. Kumar Choyi, B. Sarikaya and S. Gurivreddy, "Fast Handoff Scheme in Wireless LANs For Real-Time Systems," *The Third IEEE WLANs Workshop*, September 2001.
- [6] A. Mishra, M. Shin, and W. A. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," *University of Maryland Technical Report*, UNIMACS-TR-2002-75, 2002
- [7] Matthew S. Gast, *802.11 Wireless Networks-The Definitive Guide*, O'Reilly, 2002.
- [8] International Telecommunication Union, *General Characteristics of International Telephone Connections and International Telephone Circuits*, ITU-TG.114, 1988.
- [9] 김종원, 김대영, "무선 홈네트워킹을 위한 QoS 지원 MAC 기술," *한국통신학회지*, Vol.20, No.6, pp.25-32, 2003년 6월
- [10] 안재영, 오덕길, 김재명, "무선 LAN 기술 동향," *한국통신학회지*, Vol.19, No.5, pp.616-636, 2002년 5월
- [11] OPNET Technologies, <http://www.opnet.com/>

권 경 남(Kyoung-nam Kwon)

준회원



2003년 2월 : 아주대학교 전자공학과 졸업.

2003년 3월-현재 : 아주대학교 대학원 전자공학과 석사과정.

<관심분야> Wireless LAN, Internet QoS.

이 채 우(Chae-woo Lee)

정회원



1985년 : 서울대학교 제어계측학사.

1988년 : 한국과학기술원 전자공학과 석사.

1995년 : University of Iowa 박사.

1985년 1월-1985년 12월 (주) 금성통신 연구원. 1988년 9

월~1999년 3월 한국통신 선임연구원. 1999년 3월~2001년 9월 Lucent Technologies Korea 이사. 2001년 9월-2002년 2월 한양대학교 겸임교수. 2002년 3월-현재 아주대학교 전자공학과 조교수.

<관심분야> 광대역 통신망, Ubiquitous networking, Traffic Engineering.