OPNET 시뮬레이터의 무선랜 핸드오프 구현과 이를 기반으로 한 TCP 성능 향상 기법에 관한 연구

준회원 정 세 원*, 정회원 이 채 우**

A Study on TCP Performance Improvement Method Using WLAN Handoff Implementation by OPNET Simulator

Se-won Jung* *Associate Member*, Chae-woo Lee** *Regular Member*

요 약

본 논문에서는 OPNET Modeler 9.0을 사용하여 IEEE 802.11b 무선랜을 기반으로 한 핸드오프 시뮬레이터 개발 과정을 설명하고, 이를 이용하여 트랜스포트 계층(TCP, UDP)에 따른 핸드오프 성능을 분석해 본다. 기존의 OPNET Modeler 9.0에 제공되는 IEEE 802.11b 무선랜 모델은 시뮬레이션의 초기에 설정된 하나의 BSS(Basic Service Set)를 기반으로 동작하기 때문에 MS(Mobile Station)가 다른 BSS로 이동할 경우 통신 단절이 발생한다. 따라서 논문에서는 기존의 무선랜 모델에 핸드오프 기능을 추가하고 이를 사용하여 핸드오프에 의한 여러 가지 측면에서 성능 특성을 분석해 본다. 또한 결과를 통해 표준 핸드오프 알고리즘의 문제점을 분석하여 TCP Timeout 방지형 알고리즘을 제안하고 두 알고리즘의 성능을 비교한다.

Key Words : Handoff, Wireless LAN, IEEE 802.11b, OPNET

ABSTRACT

In this paper, we explain the development procedure for a WLAN (IEEE 802.11b Wireless Lan) handoff simulator using OPNET Modeler 9.0 and analyze the handoff performance when TCP and UDP traffic is applied. Because the BSS (Basic Service Set) is set only once at the beginning of a simulation in WLAN model supported by OPNET Modeler 9.0, the discontinuation of the communication between MS (Mobile Station) and AP (Access Point) is occurred by the migration of the MS from one BSS to another. We implement a handoff simulator based on this WLAN model and analyze handoff performance in various scenarios Also, we propose a new handoff algorithm which prevents TCP timeout by analyzing the problems of the handoff using the simulator.

Ⅰ. 서 론

유비쿼터스 시대의 도래가 현실화됨에 따라 블루투스, 휴대인터넷, UWB 등의 각종 무선 접속 기술이 보편화되고 있다. 이들 무선 접속 기술은 실내뿐만 아니라 도로, 공원, 캠퍼스 등의 실외로까지 그 범위가 점차 커지고 있다. 특히, 무선랜은 현재 11Mbps의 전송속도를 지원하는 IEEE 802.11b를 기반으로 실내와 실외의 무선 접속 기술로 자리 매김하고 있으며 비교적 간단한 프로토콜과 낮은 시

* 아주대학교 전자공학과 멀티미디어 네트워킹 연구실(jswhaha@ajou.ac.kr), ** 아주대학교 (cwlee@ajou.ac.kr)
논문번호 : 040047-0202, 접수일자 : 2004년 2월 2일
※ 본 논문은 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초기술연구지원사업(과제번호:03-기초-0078)의 연구결과입니다.

스템 비용, 그리고 최대 54Mbps의 높은 전송률(IEEE 802.11a) 등의 강점으로 공중망 서비스의 후보 기술로까지 기대 받고 있다. 그러나 IEEE 802.11 무선랜은 아직까지 해결되어야 할 많은 문제점을 갖고 있다. ISM 대역사용에 따른 간섭문제와 유선 전송 기술에 뒤떨어지는 전송률, 좁은 범위의 셀에 의한 잦은 핸드오프(Handoff)의 발생, 불완전한 인증 과정과 보안으로 정보의 유출 가능성의 존재 등은 시급히 해결해야할 문제이며 그 해결책을 얻고자 학교와 연구소 그리고 WG(Working Group) 등에서 계속적인 연구가 진행 중에 있다.

그 중 단말의 이동에 의해 발생되는 핸드오프 지연과 그에 따른 패킷 손실 문제 등은 요구되는 QoS(Quality of Service)에 밀접한 영향을 미치는 요소 중 하나이다. 앞에서 언급한 바와 같이 무선랜은 비교적 좁은 범위의 셀로 구성되며, 이는 잦은 핸드오프를 발생시킨다. IEEE 802.11 무선랜에서의 핸드오프는 동일 네트워크 내에서 이루어지는 데이터 링크 계층의 핸드오프(L2 핸드오프)와 타 네트워크로의 이동을 의미하는 네트워크 계층의 핸드오프(L3 핸드오프)로 구분 할 수 있다. L2 핸드오프는 MS(Mobile Station)가 자신이 속한 셀(Basic Service Set, BSS)에서 다른 셀로 이동할 때, 기존 셀에서 통신하던 CAP(Current Access Point)와의 결합을 끊고 새로운 NAP(New Access Point)와 재결합하는 물리적인 이동을 의미한다. L3 핸드오프는 대부분 Mobile IP를 이용하게 되며, L2 핸드오프 이후 외부 네트워크(Foreign Network)에서 부여받은 가상 주소(Care-of-Address, CoA)를 등록하는 등의 절차를 포함한다. 이들 핸드오프 과정은 사용자가 한 지역에서 다른 무선 지역으로 이동할 때 세션의 단절을 예방하여 계속적인 서비스를 받도록 지원한다. 앞서 언급했듯이 L3 핸드오프는 L2 핸드오프가 선행된 후에 네트워크 변동이 있을 경우 진행되는 과정으로, L3 핸드오프 알고리듬의 성능을 말함에 있어서 L2 핸드오프의 정확한 분석이 반드시 요구된다.

본 논문에서는 이동성이 보장되는 IEEE 802.11b에서 높은 QoS를 제공하기 위해 반드시 선행되어야 하는 L2 핸드오프의 성능 분석에 필요한 시뮬레이션 모델을 OPNET Modeler 9.0을 사용하여 개발하고, 개발된 모델을 이용하여 L2 핸드오프 시에 발생하는 지연과 패킷 손실, 그 외 문제점들을 트랜스포트 계층별로 분석한다. 무선랜에서 핸드오프의 지연시간과 그에 따른 영향은 환경에 따라 다양한 특성을 보인다. 그 예로 MS가 탐색(Scanning)하는 지역에 인접한 BSS의 개수에 따라서 IEEE 802.11 무선랜에서의 핸드오프 지연시간은 달라진다. MS가 각각의 채널을 탐색할 때, BSS의 존재 여부에 따라서 해당 채널에 대한 탐색 시간을 달리하기 때문에 핸드오프 지연이 달라진다. 또한 지연시간이 일정할지라도 핸드오프가 미치는 영향은 트랜스포트 계층에 따라서 다르다. UDP(User Datagram Protocol)를 사용하는 응용 프로그램의 경우, 핸드오프 기간 동안 데이터를 계속 내려 보내기 때문에 AP(Access Point)의 버퍼 오버플로우(Buffer Overflow)에 의한 패킷 손실이 발생할 수 있다. 반면, TCP(Transmission Control Protocol)는 네트워크 상황에 맞추어 전송 속도를 조절하기 때문에 핸드오프에 의한 오버플로우가 발생하지 않는다. 결과적으로 핸드오프에 의한 패킷 손실이 UDP보다 작게 발생한다. 하지만 TCP는 패킷 손실을 혼잡(Congestion) 상황이 발생한 것으로 판단하여 전송 속도를 낮추기 때문에 전송률(Throughput)의 저하를 초래한다. 앞에서 살펴본 여러 가지 요소들에 따른 다양한 시나리오를 통해서 무선랜의 핸드오프 성능을 분석한다. 또한 이 분석을 통해 핸드오프가 TCP 성능 저하에 미치는 원인을 분석하여 이를 해결하는 새로운 알고리즘을 제안한다.

OPNET은 유연한 시뮬레이션 환경을 제공하며 네트워크 성능을 분석하기 위해 널리 사용되고 있다. 그러나 최근 버전인 OPNET 9.0은 기본적인 무선랜 기능을 제공하지만 핸드오프 메커니즘을 포함하지 않고 있다. OPNET을 사용한 무선랜에서의 핸드오프 성능 분석을 위해서 OPNET에 핸드오프 모듈을 추가하였다. 본 논문에서 개발된 모듈을 설명하고 이를 사용한 시뮬레이션 결과를 살펴볼 것이다. 또한 시뮬레이션 결과를 토대로 핸드오프 성능을 향상시키기 위한 새로운 방법을 제시하고 이에 대한 시뮬레이션 결과를 기존의 알고리즘과 비교한다.

본 논문의 나머지 부분에서는 개발한 핸드오프 모델의 이해를 돕기 위해 2절에서 현재 IEEE 802.11 무선랜의 핸드오프 메커니즘을 설명한다. 3절에서는 기존 OPNET에서 제공하는 무선랜 모델에 핸드오프 메커니즘의 구현 과정을 살펴본 후, 4절에서 개발된 모델을 사용하여 시뮬레이션 환경 설명 및 네트워크 성능 분석을 수행한다. 그리고 5절에서는 4절의 시뮬레이션 결과에서 나타나는 기존 핸드오프 방식의 문제점을 개선하는 새로운 방

법을 제안하고 이에 대한 성능을 검증한다. 마지막으로 6절에서 결론을 맺는다.

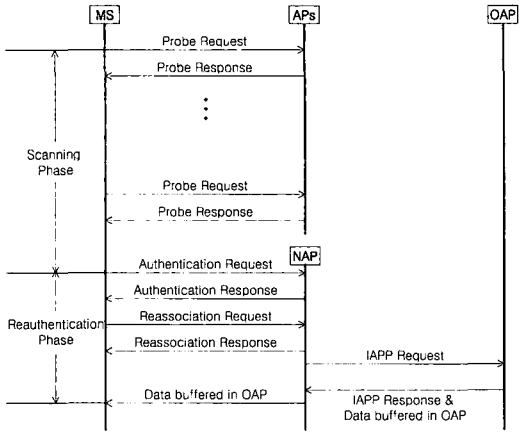


그림 1. IEEE 802.11b 무선랜의 핸드오프 절차.
Fig. 1. Handoff procedure of IEEE 802.11b WLAN.

II. IEEE 802.11b 무선 랜의 핸드오프

IEEE 802.11b에서 현재 지원하는 핸드오프 과정은 핸드오프 할 AP를 찾는 탐색 단계(Scanning Phase)와 NAP와의 재결합을 맺는 재인증 단계(Reauthentication Phase)로 이루어진다. 이번 절에서는 무선랜의 핸드오프에 관한 컨트롤 시그널링을 나타내는 그림 1을 기반으로 핸드오프의 구체적인 동작에 대해 살펴본다.

1. 탐색 단계(Scanning Phase)

탐색 단계란 MS가 CAP의 신호대잡음비가 CST(Cell Search threshold) 이하 일 경우 재결합할 AP를 찾는 단계이다. MS는 CAP와 거리가 멀어지면 CAP와 통신이 두절되기 전에 미리 AP에 관한 정보를 요청하고, 이를 수신한 AP가 이에 응답함으로써 MS에게 자신의 존재를 알린다. MS는 이 단계에서 수집한 AP 정보를 바탕으로 핸드오프를 결정한다. 그림 1에서 보듯이 MS는 AP의 정보를 수집하기 위하여 여러 채널에 대한 탐색을 순차적으로 진행한다. 예를 들어 13개의 채널을 사용하는 무선랜 네트워크의 경우, MS는 13개의 채널을 차례로 탐색한다.

MS는 현재 접속된 AP의 신호대잡음비가 CST 이하로 떨어졌을 경우, 1번 채널로 프로브 요청(Probe Request) 프레임을 브로드캐스트함으로써 탐색 단계를 시작한다. MS는 프로브 요청 프레임을 보낸 후에 최소 채널 시간(Min-Channel-Time) 동안 1번 채널에서의 응답 프레임을 기다린다. 이 시간 동안 프로브 응답 프레임을 받거나 그 채널이 사용되는 경우(BUSY)에는 최대 채널 시간(Max-Channel-Time)까지 연장하여 탐색한다. 반면에 최소 채널 시간 동안 채널이 사용되지 않는 경우(IDLE)에는 인접한 곳에 그 채널을 사용하는 AP가 존재하지 않는 것으로 판단하여 다음 채널에 대한 탐색에 들어간다. 최소 채널 시간은 탐색하는 채널에 AP가 없을 경우 사용되는 탐색 시간이고, 최대 채널 시간은 AP가 존재할 경우 사용되는 탐색 시간이다[1]. 이처럼 무선랜에서 탐색 시간은 채널 상태에 따라 비교적 능동적으로 결정된다. 같은 방법으로 13번 채널까지 탐색을 마친 후, MS는 자신이 접속할 NAP를 결정하고 인증 단계에 돌입하기 위해 대기한다.

2. 재인증 단계(Reauthentication Phase)

CAP와 NAP에서의 신호대잡음비가 어느 일정 이상이 되면 MS는 탐색 단계에서 결정된 NAP에 접속하기 위해 재인증 단계로 들어간다. 재인증 단계는 AP가 자신에게 접속될 수 있는 권한이 있는 MS인지를 검증하는 인증 단계(Authentication)와 물리적인 실제 결합을 의미하는 재결합 단계(Reassociation)로 나눌 수 있다. IEEE 802.11에서 사용되는 기본적인 인증 방법으로 개방-시스템(open-system) 인증과 공유-키(shared-key) 인증[2]이 있으나 본 논문에서는 핸드오프시의 성능에 초점을 맞추고자 간단한 2개의 프레임의 교환으로 이루어지는 개방-시스템 인증을 사용하여 인증 단계를 간단히 구현하였다. 재결합 단계란 인증 받은 MS가 CAP와의 결합을 끊고 NAP와 결합을 맺는 단계이다. 그림 1에서 재결합 요청(Reassociation Request) 프레임과 재결합 응답 프레임을 이용하여 재결합을 완료하고 NAP는 IAPP(Inter Access Point Protocol)를 사용해 재결합 이전에 통신하던 OAP(Old AP)와 통신한다. IAPP는 OAP와 MS 간의 결합을 종료시키고 핸드오프 과정 동안 OAP에 버퍼링된 패킷을 NAP로 포워딩(Forwarding) 시킨다[1].

III. OPNET을 이용한 핸드오프 시뮬레이터 제작

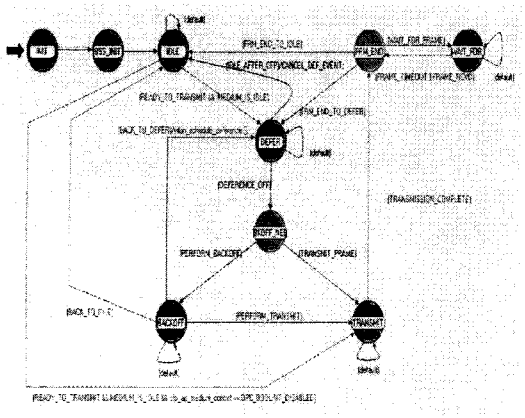


그림 2. OPNET Modeler 9.0에서의 IEEE 802.11b 무선랜 모델.
Fig. 2. IEEE 802.11b WLAN model supported in OPNET Modeler 9.0.

IEEE 802.11b의 완전한 핸드오프 시뮬레이터 구현을 위해서 무선 링크를 사용한 AP와 단말기의 통신 지원, 셀 내 단말의 이동성 지원과 세션의 유지, 셀 간 단말의 이동과 세션의 유지, IAPP을 위한 AP 간 통신 기능 및 버퍼링된 패킷의 전송 등의 기능들이 요구된다. 하지만 현재 OPNET Modeler 9.0에서 지원하는 무선랜 시뮬레이터는 셀 내 단말의 이동과 데이터 전송만을 위한 기능만을 제공한다. 3절에서는 구현 과정의 이해를 돕기 위해 현재 OPNET Modeler 9.0에서 제공하는 무선랜의 데이터 전송 모델을 간단히 살펴본 후, 새롭게 구현된 무선랜 핸드오프 모델의 개발 과정을 살펴본다.

1. OPNETv9.0에 구현된 IEEE 802.11b 무선랜 모델

OPNET Modeler 9.0에 구현된 기존의 무선랜 모델에서 모든 노드는 설정된 채널 주파수와 BSSID(Basic Service Set IDentification)에 따른 등록 과정을 거치게 된다. 이 과정은 BSS 설정 단계로써 시뮬레이션을 초기화하는 과정에서 오직 한번만 수행되며 시뮬레이션 과정 중 변경되지 않는다. 이러한 제약으로 인해 현재 OPNET에서 제공하는 무선랜 모델을 이용했을 경우 핸드오프에 대한 시뮬레이션은 불가능하다.

그림 2는 OPNET Library로 제공되는 802.11b 무선랜 모델의 상태 전이 그림(State Transition Diagram)을 보여준다. 그림 2에서의 각 상태(State)에 관한 설명을 표 1에 나타냈다. INIT과 BSS_INIT 상태는 시뮬레이션 실행 초기에 오직 한번만 수행되는 상태로써 시뮬레이션 환경을 초기화한다. IDLE, DFFER, BKOFF_NEED, BACKOFF, 그리고 TRANMIT 상태는 802.11b 무선랜에서 액세스 기술로써 사용되는 CSMA/CA(Carrier Sense Multiple Access/Collision Avoidance)를 수행하는 상태들이다. 프로세스는 프레임을 전송한 후, FRM_END 상태로 이동하고 전송한 프레임에 따라서 다음 상태를 결정한다. 만약 전송된 프레임이 ACK(Acknowledgement)나 CTS(Clear-To-Send)와 같은 응답을 필요로 한다면 WAIT_FOR 상태로 이동하여 응답을 기다리게 된다. 응답이 필요 없다면 프로세스는 IDLE 상태로 바로 이동한다. 그림 2에 나타난 모든 상태들은 프레임 송신과 관련된 역할을 분담한다. 반면, 프레임의 수신은 그림 2의 어느 상태에서든지 인터럽트 루틴(Interrupt Routine)을 통해서 처리된다. 다음은 각 상태에 대한 구체적인 설명이다.

- INIT:시뮬레이션 초기화
- BSS_INIT:모든 노드에 대한 BSS의 설정
- IDLE:보낼 프레임이 없을 경우 대기 상태
- DFFER:프레임 전송 이전에 각 ISF 시간 대기 상태
- BKOFF_NEED:백오프(Backoff)과정의 수행 여부 결정
- BACKOFF:랜덤(Random)하게 결정된 백오프 슬럿(Slot) 동안을 대기하는 상태
- TRANSMIT:프레임을 전송하는 상태
- FRM_END:프레임 전송 완료 후, 다음 상태 결정
- WAIT_FOR:전송한 프레임에 대한 응답을 기다리는 상태

그림 2의 무선랜 모델에서 BSS에 관한 설정은 시뮬레이션 초기에 BSS_INIT 상태에서 단 한번만 수행되며 시뮬레이션 동안 이 설정이 계속 유지되기 때문에 MS가 한 BSS로부터 다른 BSS로 이동하여 통신하는 것이 불가능하다. 그렇기 때문에 핸드오프가 가능하기 위해서는 핸드오프의 발생시 BSS 설정이 다시 이루어져야 한다. 그림 3은 IEEE802.11b를 바탕으로 핸드오프 지원 모델이 갖추어야 할 과정과 이를 위해 새롭게 추가된 기능들을 나타낸다. 앞에서 살펴본 바와 같이 그림 2의 무선랜 모델은 이동성을 지원하는데 한계를 가지고 있기 때문에, MS의 이동은 MS와 AP간의 통신 단절을 유발한다. 그러나 개발된 핸드오프 지원 모델

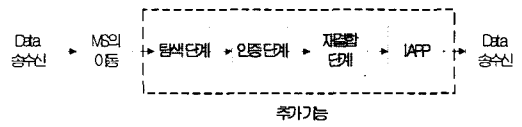


그림 3. 개발된 핸드오프 지원 모델에서 추가된 기능.
Fig. 3. new functions of the developed handoff module.

에서는 그림 3에서와 같이 표준에 기반을 둔 추가된 기능에 의해 계속적인 통신이 가능하다. 추가된 기능은 MS의 이동에 따른 탐색단계와 NAP로부터의 인증 및 재결합 단계를 거쳐 IAPP를 이용한 패킷 포워딩(Forwarding) 과정을 지원한다.

2. 핸드오프 알고리즘의 구현

앞 절에서 살펴본 핸드오프 알고리즘의 구현은 그림 1에 나타난 컨트롤 시그널의 교환, BSS의 변경, 그리고 IAPP의 구현 세 과정으로 진행되었다. 알고리즘의 구현 설명에 있어서 지면 관계상 세부적인 코딩은 생략하고 기능 및 상태 이동 중심으로 설명한다.

1) 핸드오프 컨트롤 시그널의 교환

그림 1은 핸드오프 과정에 따른 컨트롤 시그널의 발생 순서를 보여준다. 그림에서의 순서와 동일하게 MS과 AP가 컨트롤 시그널을 교환하도록 구현하였다. MS는 프로브 요청 프레임, 인증 요청 프레임, 그리고 재결합 요청 프레임을 전송하며, AP는 프로브 응답 프레임, 인증 응답 프레임, 재결합 응답 프레임, 그리고 IAPP 요청 및 응답 프레임을 보낸다. 이 때, MS와 AP는 CSMA/CA에 따라 컨트롤 시그널들을 전송하게 된다. 따라서 표준에 따른 각 프레임의 포맷[3]이 무선랜 모델에 새롭게 추가되었고, 이 프레임들의 전송은 데이터 프레임과 동일하게 그림 2의 TRANSMIT 상태에서 처리하도록 구현되었다.

본 논문에서 구현된 무선랜 모델에서는 유럽(ETSI)의 규정에 따른 2.4Ghz~2.5Ghz 대역의 13개 채널을 사용하여[1] 핸드오프 발생 시 MS가 여러 개의 채널을 변경하면서 통신할 수 있도록 하였다. 또한 최소 채널 시간과 최대 채널 시간으로써 현재 사용되는 상용 제품에서 사용되는 값을 토대로 각각 3ms와 30ms로 설정하였다[1][4].

2) BSS의 변경

기존의 무선랜 모델에서 BSS에 관한 설정은 그림 2의 BSS_INIT 상태에서 시뮬레이션의 처음 한 번만 일어난다. 일단 시뮬레이션이 시작되면 시나리오 내에 존재하는 모든 MS와 AP는 자신의 BSSID와 다른 설정값들을 글로벌 리스트(Global List)에 등록한다. 여기서 글로벌 리스트는 프로그램 상에서 동일한 BSS내에 존재하는 모든 MS와 AP를 연결시키기 위해 사용된다. 등록된 BSSID를 바탕으로 AP는 자신의 BSS에 속하는 MS에 대한 테이블을 구성한다. 그렇기 때문에 핸드오프가 일어날 때 MS는 BSS 설정에 필요한 모든 설정값들을 새로운 값으로 재등록하고 AP는 재등록된 값들을 바탕으로 테이블을 수정한다.

3) IAPP의 구현

그림 1에서 보듯이 NAP는 MS에게 재결합 응답 프레임을 보냄과 동시에 IAPP를 통해 OAP에게 버퍼링된 패킷을 요청한다. NAP가 IAPP 요청 프레임을 보낼 때, NAP는 핸드오프 중인 MS의 주소를 IAPP 요청 프레임의 소스 주소로 사용하여 OAP로 보내기 때문에 OAP에서 NAP사이의 경로 상의 모든 브릿지들의 테이블을 수정하여 MS가 이동했음을 알림으로써 이동한 MS로 보내지는 패킷들이 NAP로 전송될 수 있도록 구현하였다. IAPP 요청 프레임을 받은 OAP는 IAPP 응답으로써 버퍼링된 프레임을 NAP로 보냄과 동시에 MS와의 결합을 종료한다.

IV. 시뮬레이션을 통한 IEEE 802.11 핸드오프 성능 분석

이번 절에서는 개발된 핸드오프 시뮬레이션 모델을 이용하여 무선랜에서 핸드오프가 발생할 때 나타나는 각 프로토콜 성능의 변화를 고찰하고자 한다. 이를 위해 본 논문에서 사용되는 여러 가지 시나리오를 살펴본 후, 각각의 시나리오에 대한 시뮬레이션 결과를 분석한다.

1. 시뮬레이션 환경 및 시나리오

시뮬레이션을 위한 데이터 링크 계층의 파라미터는 표 1과 같다. 시뮬레이션은 무선랜의 물리 계층 기술로 11Mbps의 DSSS(Direct Sequence Spread Spectrum)를 사용한다[5]. 또한 무선랜은 CSMA/CA로 알려진 액세스 방식을 사용하는 DCF(Distributed Coordination Function) 모드만으로 동작하도록 설정하였다[3]. 재전송 한계(Retry Limit)는 AP에서 MS로의 패킷 전송이 실패했을 경

표 1. 데이터링크 계층의 파라미터 설정.
Table 1. Parameters of Data Link layer.

데이터링크 계층 파라미터	Value
전송 속도	11 Mbps
물리적 전송 방식	DSSS
PCF 모드	사용안함
RTS/CTS	사용안함
재전송 한계 (Retry Limit)	7번
데이터링크 계층의 버퍼 크기	256kbit

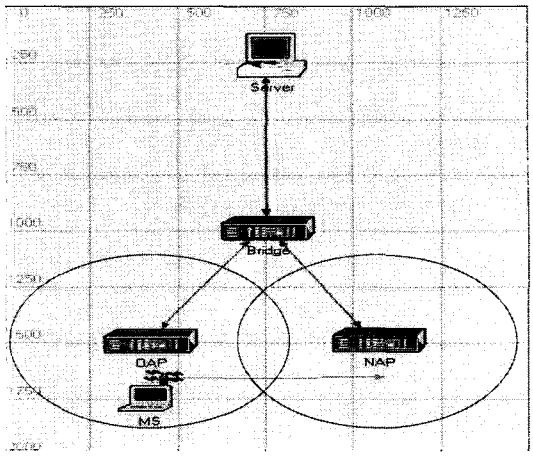
우 반복해서 전송할 수 있는 최대의 횟수이다. 즉, AP가 패킷을 재전송 한계만큼 재전송하고도 Ack를 받지 못하면 패킷을 버린다. 또한 CST로써 Orinoco 기술 보고서의 권고 사항에 따라 23dB를 사용한다 [6].

본 논문에서는 크게 두 가지 트랜스포트 계층에 따라 시나리오를 분류한다. UDP는 하위 계층에서의 패킷 손실에 상관없이 데이터를 내려 보낸다. 또한 UDP을 사용하는 경우에는 패킷 손실과 지연에 영향을 미치는 전송 속도와 버퍼 크기를 고려하여야 한다. 반면에 TCP는 Ack를 받지 못하면 CWND(Congestion Window) 이상의 데이터를 보내지 않는다[7]. 그렇기 때문에 TCP는 UDP와 달리 핸드오프 동안에 통신이 단절되더라도 패킷 손실이 많이 발생하지 않는다. 이번 절에서는 앞에서 언급한 요소들에 따라 분류된 여러 시나리오를 설명하고 다음 절에서 그에 따른 결과를 분석하고자 한다.

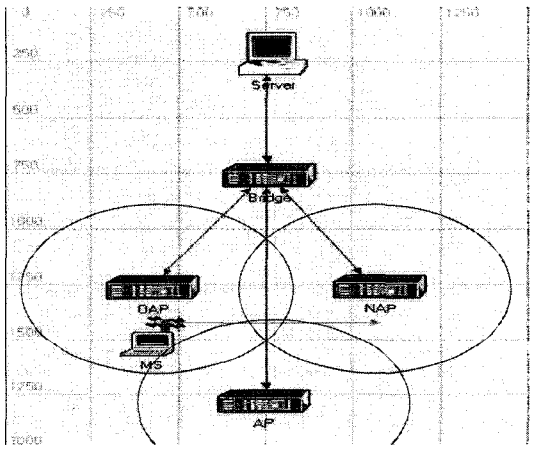
1) TCP 성능 분석을 위한 시나리오

이 시나리오에서는 응용 프로그램으로 FTP를 사용하여 파일 서버가 MS로 18Mbyte의 파일을 전송하는 중에 핸드오프가 일어나도록 한다. 그림 4-(a)는 시뮬레이션 환경과 MS의 이동 경로를 보여준다. 파일을 전송하는 동안 CWND의 크기를 측정함으로써 핸드오프에 의한 전송률의 저하를 분석한다.

TCP의 파라미터 설정은 다음과 같다. TCP의 MSS(Maximum Segment Size)는 1460byte, AP의 버퍼 크기는 256kbit, TCP 수신 버퍼 크기(Receive Buffer Size)는 64kbyte로 설정하였다. 또한 TCP 버전은 Reno를 사용하며, 손실된 패킷은 3개의 중복된 Ack를 받은 경우 이를 패킷 손실로 간주하여 바로 재전송을 하는 Fast Retransmit과 보낸 패킷에 대한 Ack를 일정 시간 동안 받지 못하는 경우 이



(a) 2개의 BSS가 중복되는 경우.



(b) 3개의 BSS가 중복되는 경우.

그림 4. 시뮬레이션 환경과 MS의 이동 경로.
Fig. 4. Simulation environment and movement of MS.

를 패킷 손실로 간주하여 재전송을 하는 Retransmit Timeout을 통하여 복구된다.

2) UDP 성능 분석을 위한 시나리오

이 시나리오에서는 응용 프로그램으로 VOD(Video On Demand)를 사용하여 서버가 MS로 시뮬레이션 동안 계속해서 보내준다. 시나리오는 크게 MS가 핸드오프하는 지역에 중복되는 BSS가 2개(그림 4-(a))인 경우와 3개(그림 4-(b))인 경우 두 가지로 나눈다. UDP의 경우, 패킷 손실이 지연 시간에 민감하기 때문에 중복되는 BSS의수가 3개인 경우도 시나리오에 추가시킴으로써 지연 시간에 따른 패킷 손실의 증가를 분석한다.

전송 속도는 17280byte 크기의 프레임을 사용하여 시나리오별로 10frame/sec에서 40frame/sec까지

5frame/sec 단위로 달리하고, AP의 버퍼 크기는 시나리오별로 256kbit, 512kbit, 1024kbit 세 가지로 달리하여 시뮬레이션 한다. 이 외의 데이터 링크 계층 파라미터는 AP의 버퍼 크기를 제외하고 표 2와 동일하게 설정하였다.

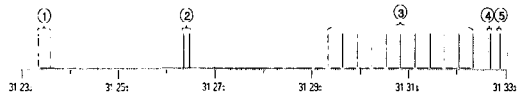


그림 5. MS에서 측정한 Handoff Signaling.
Fig. 5. Handoff signaling captured at MS.

2. 결과 분석

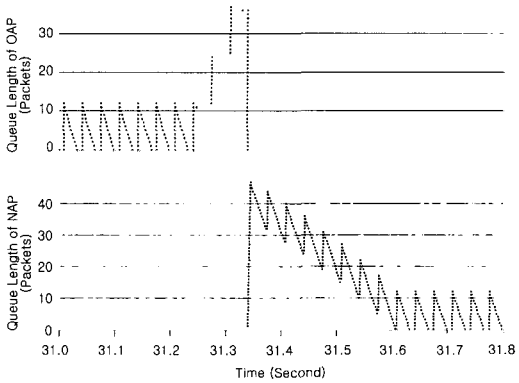
시뮬레이션에서 측정된 핸드오프의 지연은 중복되는 BSS가 2개인 경우에는 평균 99.26msec, 중복되는 BSS가 3개인 경우에는 평균 126.37msec로 나타났다. 이번 절에서는 우리가 구현한 핸드오프 모델이 잘 동작하는지 확인한 후, TCP와 UDP를 사용하는 시나리오에서 핸드오프의 지연이 각각 어떤 결과를 야기하는지 고찰해본다.

1) 구현된 핸드오프 모듈 동작 검증

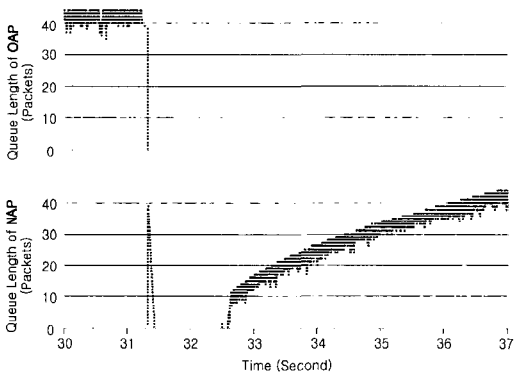
3절에서는 무선랜 모델에 핸드오프 기능을 구현하는 방법에 대해서 살펴보았고, 이번 소절에서는 3절에서 구현한 핸드오프 시뮬레이터가 어떻게 동작하는지 그림 5와 그림 6을 통해서 살펴본다.

그림 5에서는 MS가 핸드오프하는 지역에 중복되는 BSS의 개수가 2개인 네트워크에서 핸드오프 발생 시 MS과 AP사이에 교환되는 컨트롤 시그널(Control Signal)을 보여준다. 그림 5의 X축은 핸드오프가 일어날 무렵의 시간이며 ①,②,③에 나타나는 이벤트는 탐색 단계에서 사용되는 컨트롤 시그널인 프로브 요청 프레임과 응답 프레임이다. ①,②에 나타나는 바와 같이 1번과 2번 채널에서는 AP가 존재하기 때문에 프로브 응답 프레임을 수신하여 최대 채널 시간에 해당하는 30msec 동안 해당 채널을 탐색하고 있지만 ③에 나타나는 나머지 채널들에서는 AP가 존재하지 않기 때문에 각각의 채널을 최소 채널 시간에 해당하는 3msec 동안만 탐색한다. 또한 ④와 ⑤에 나타나는 이벤트는 인증 단계와 재결합 단계에 교환되는 컨트롤 시그널을 보여준다. 위의 그림을 통해 탐색 단계, 인증 단계, 그리고 재결합 단계가 올바르게 동작함을 확인할 수 있다.

IAPP의 동작을 증명하기 위하여 그림 6은 핸드오프 동안 버퍼 크기가 512kbit인 OAP와 NAP에 버퍼링된 패킷 수(Queue Length)를 보여준다. 그림 6-(a)는 30frame/sec의 전송 속도를 갖는 UDP에서, 그림 6-(b)는 TCP 시나리오에서의 결과이다. 각 그래프에서 약 31.33초에 OAP에 버퍼링된 패킷이 순간적으로 급격하게 줄어들고, 곧바로 NAP의 버퍼 내 패킷이 급격하게 증가하는 것을 볼 수 있다. IAPP에 의해 OAP에 버퍼링된 패킷이 NAP로 100Mb의 이더넷망을 통해 빠르게 전달되기 때문에 NAP의 큐 길이가 빠른 속도로 증가하기 때문에 그림 6에서는 수직으로 증가하는 것처럼 나타난다. 이를 통해 IAPP 또한 잘 구현되었음을 확인할 수 있다.



(a) UDP를 이용할 때의 큐 길이 변화.



(b) TCP를 이용할 때의 큐 길이 변화.

그림 6. 핸드오프 발생 시 OAP와 NAP의 큐 길이(Queue Length) 변화 그래프
Fig. 6. Queue length of OAP and NAP during handoff.

2) TCP 성능 분석

FTP는 TCP를 사용하기 때문에 데이터링크 계층

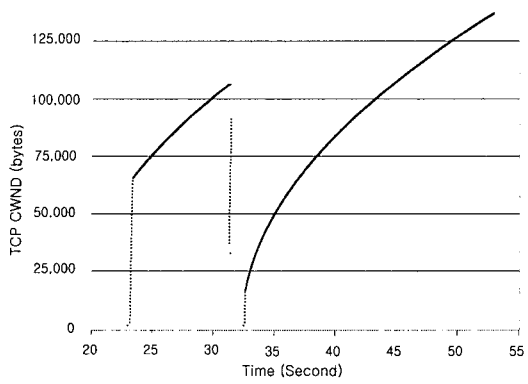


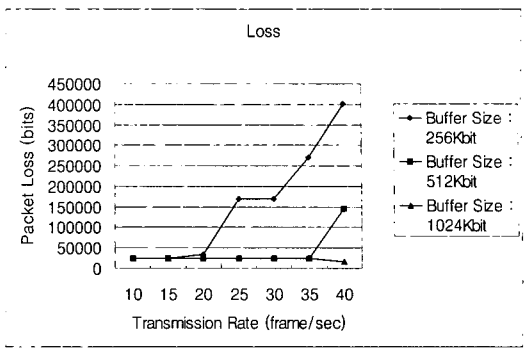
그림 7. IEEE802.11b에서 핸드오프 발생시 송신측 CWND 크기 변화. (단, CST=23dB)
Fig. 7. TCP CWND size of sender during handoff in IEEE802.11b.

에서 AP의 버퍼 오버플로우에 의한 패킷 손실은 발생하지 않았다. 그러나 AP에서 재전송 한계까지 도달하는 연속된 재전송에 의해 3개의 패킷 손실이 발생한다. MS의 핸드오프 과정 동안 OAP는 자신이 전송한 프레임에 대한 Ack를 받지 못했기 때문에 계속해서 재전송을 하게 되고, 재전송 한계인 7번의 재전송 후에도 Ack를 받지 못하면 패킷을 버린다. 설정된 시나리오에서 재전송 한계로 인해 버려진 패킷은 시뮬레이션 결과 평균 3개로 나타났다.

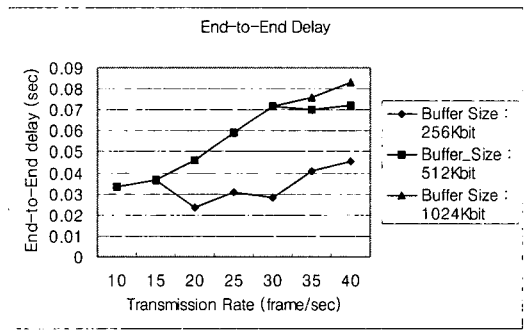
그림 7은 핸드오프 동안 서버의 CWND를 보여준다. 그림의 X축은 시뮬레이션 시간이며, Y축은 CWND의 크기를 byte단위로 측정한 값이다. CWND는 데이터 전송이 시작된 23초부터 증가하기 시작하고, 핸드오프가 일어나는 시점에서 크게 감소하고 있다. 이것은 AP에서 발생된 3개의 패킷 손실에 의한 감소이다. 서버는 첫 번째 패킷 손실에 대한 3개의 중복된 Ack를 받고 재전송을 시작하지만 다음 패킷도 손실되었기 때문에 Fast Recovery 과정으로 들어가지 못하고 Retransmit Timeout이 발생된다. 본 시뮬레이션에서는 TCP-Reno를 사용하기 때문에 Retransmit Timeout 이후의 CWND값은 아래와 같다[7].

$$CWND_{afterRTO} = min(\frac{CWND_{beforeRTO}}{2}, \frac{ReceiveBufferSize}{2}) \quad (1)$$

CWNDafterRTO는 Retransmit Timeout 이후의 CWND이며, CWNDbeforeRTO는 Retransmit Timeout 이전의 CWND이다. 위의 식에 따라서 핸



(a) 핸드오프 동안의 패킷 손실량.



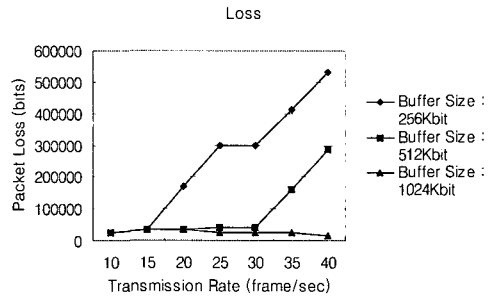
(b) 핸드오프 직후의 종단 간 지연시간.

그림 8. UDP 사용 시 핸드오프에 의한 패킷 손실량과 종단 간 지연시간. (중복되는 BSS:2개)
Fig. 8. Packet Loss and ETE delay during handoff in the case of UDP. (Overlapped BSS:2)

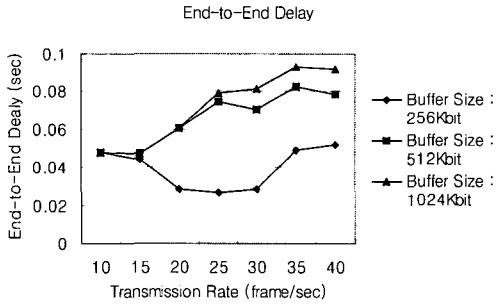
드오프 직후에 CWND가 (Receive Buffer Size/2)인 32kbyte로 줄어든다. 또한 SST(Slow Start Threshold)도 Fast Retransmit과 Retransmit Timeout에 의해 감소한다. 이처럼 핸드오프가 발생할 경우, TCP는 핸드오프에 의한 패킷 손실을 네트워크 혼잡의 신호로 판단하여 불필요하게 전송 속도를 줄이는 혼잡제어(Congestion Control)를 수행함으로써 전송률을 떨어트린다. 시뮬레이션을 통해서 현재의 TCP가 무선 환경에서 좋은 성능을 내지 못하는 이유를 알 수 있었고, 또한 무선 환경에서의 패킷 손실을 네트워크 혼잡 상태와 구별할 수 있는 새로운 TCP의 필요성을 다시 한번 확인할 수 있었다.

3) UDP 성능 분석

그림 8-(a)는 MS의 핸드오프 동안, OAP에서 발생하는 전송 속도에 따른 버퍼 사이즈별 패킷 손실량을 보여주고 있다. 예상했듯이 전송 속도가 빠르고 버퍼 크기가 작을수록, 패킷 손실이 더 많이 나



(a) 핸드오프 동안의 패킷 손실량.



(b) 핸드오프 직후의 종단 간 지연시간.

그림 9. UDP 사용 시 핸드오프에 의한 패킷 손실량과 종단 간 지연시간. (중복되는 BSS:3개)
Fig. 9. Packet Loss and ETE delay during handoff in the case of UDP. (Overlapped BSS:3)

타나고 있다. 이것은 UDP에서 발생되는 패킷 손실의 대부분이 버퍼 오버플로우에 의한 것이기 때문이다. 그림 8-(b)는 MS가 핸드오프 한 직후, 전송 속도에 따른 버퍼 사이즈별 종단 간 지연시간에 대해 단위 시간당 평균을 취한 값이다. 그림 8-(a)에서는 버퍼 크기가 클수록 패킷 손실이 감소한다. 하지만 큰 버퍼를 사용하더라도 무선 링크에서 약간의 패킷 손실이 여전히 발생된다. 또한 그림 8-(b)에서는 버퍼 크기가 큰 경우 핸드오프 동안 버퍼에 쌓인 패킷이 많아져서 종단 간 지연이 증가함을 보여준다. 이를 통해 큰 버퍼를 사용하면 패킷 손실을 어느 정도 줄일 수 있지만 종단 간 지연이 커지기 때문에 핸드오프 동안 VOD 응용 프로그램의 QoS는 여전히 보장되지 않음을 알 수 있다.

그림 9는 MS의 핸드오프 구간에 인접 AP의 개수가 3개인 시나리오에서 보여주는 패킷 손실량과 종단 간 지연 시간을 나타낸다. AP가 2개일 경우에는 2개의 채널에서 각각 최대 채널 시간인 30msec를 탐색하게 되고 나머지 모든 채널에서는 각각 3msec만을 탐색한다. 반면 AP가 3개인 경우에는 3개의 채널에서 각각 30msec를 탐색하기 때문에 전체적인 탐색 시간이 27msec만큼 늘어난다. 그렇기 때문에 이 시나리오에서 패킷 손실과 종단 간 지연을 측정한 결과가 그림 8에서보다 증가하는 것을 볼 수 있다. 이를 통해 이웃한 BSS의 수가 많을수록 패킷 손실과 종단 간 지연이 증가한다는 것을 예측할 수 있다.

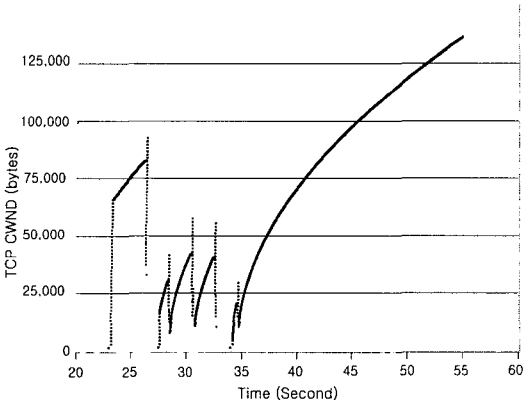
V. TCP Timeout 방지형 핸드오프 기법

4절에서 핸드오프 발생시 3개의 연속된 패킷 손실에 의해서 Retransmit Timeout이 발생하는 것을 확인하였다. TCP는 핸드오프에 의한 Retransmit Timeout을 혼잡 상황이 발생한 것으로 판단하기 때문에 CWND의 크기를 줄임으로써 전송 속도를 제어하게 된다. 따라서 MS와 통신 중인 단말기는 핸드오프의 발생을 혼잡 상황으로 판단하여 전송 속도를 불필요하게 줄이게 된다. 본 논문에서는 이러한 잘못된 혼잡 제어를 방지하기 위해 핸드오프 동안에 AP에서 발생하는 패킷 손실을 방지하는 알고리즘을 제안하고 이에 대한 성능을 검증한다.

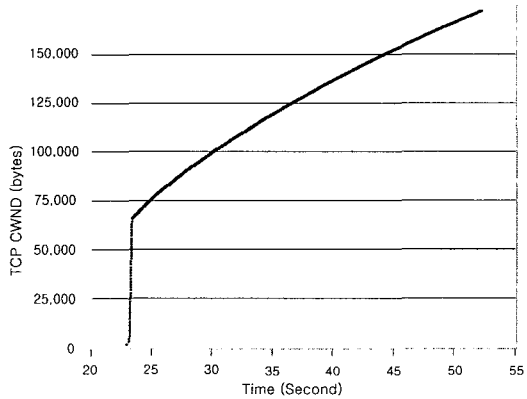
1. 핸드오프 인식에 의한 전송 중단 알고리즘

기존의 핸드오프 메커니즘에서 CAP는 MS의 핸드오프와 상관없이 전송할 데이터가 있으면 계속해서 데이터 전송을 시도하기 때문에 패킷 손실이 발생하게 된다. 따라서 본 논문에서는 CAP가 MS의 핸드오프를 인식하고 이에 따라 데이터 전송을 잠시 중단함으로써 패킷 손실을 방지하는 알고리즘을 제안한다. 제안한 알고리즘에서 변경된 핸드오프 절차는 다음과 같다. 우선, MS가 핸드오프 과정을 시작하게 되면 CAP는 이를 인식하여 데이터 전송을 중단한다. 그리고 핸드오프의 종료를 판단하는 순간, CAP는 MS으로의 데이터 전송을 재개한다. 이 때, CAP가 MS의 핸드오프 시작과 종료를 판단하기 위한 방법은 다음과 같다.

우선 핸드오프 시작의 인식을 위해 본 논문에서는 MS가 13개의 채널 중에 CAP가 속한 채널을 가장 먼저 탐색한다고 가정한다. 핸드오프의 첫 단계로 수행되는 탐색 단계는 여러 채널에서 순차적으로 진행되기 때문에, MS가 CAP가 속한 채널을 처음으로 탐색한다면 CAP는 MS가 보내는 프로브 요청 프레임을 받는 순간 이를 핸드오프의 시작으로 판단할 수 있다. 또한 재인증 단계에서 NAP는



(a) IEEE802.11b



(b) TCP Timeout 방지형 핸드오프 기법

그림 10. 핸드오프 발생시 송신측 CWND 크기 변화. (단, CST=24dB)

IAPP를 사용하여 CAP와 통신하게 된다. 그렇기 때문에 CAP는 IAPP 요청 프레임을 받았을 때 핸드오프가 끝난 것을 알 수 있다.

탐색이 끝난 후, MS는 CAP보다 큰 신호대잡음비를 가지는 AP가 없을 때에는 재인증 단계로 넘어가지 않고 핸 드오프 과정이 종료된다. 이런 경우 IAPP 요청 프레임이 전송되지 않기 때문에, CAP가 중단하였던 데이터 전송을 재개하지 못하는 문제가 발생한다. 본 논문에서는 이를 해결하기 위해 다음의 두 가지 방법을 제시한다. 첫 번째 방법은 타이머를 사용하는 것이다. CAP가 프로브 요청 프레임을 받은 후 타이머를 작동시켜 일정 시간이 지나면 핸드오프의 종료로 판단하여 핸드오프 중이던 MS로 데이터 전송을 다시 시작한다. 이 방법은 추가적인 컨트롤 시그널이 사용되지 않는 장점이 있지만, 핸드오프가 끝나는 시간을 정확히 예측하기 힘들다는 문제점이 있다. 두 번째 방법은 MS가 핸드오프 종료시 추가적인 컨트롤 시그널을 사용하여 CAP에게 종료를 알리는 것이다. 이 방법은 탐색 단계의 종료를 정확히 판단하여 전송을 재개하기 때문에 타이머를 사용하는 방법보다 시간을 좀 더 효율적으로 사용할 수 있다. 하지만 타이머를 사용할 경우, CAP의 타이머 설정값이 실제 핸드오프 시간보다 약간 작다하더라도 이 시간 차이 동안 7번의 재전송에 이르지 않는 한 패킷 손실이 발생하지 않으며, 또한 1개의 패킷 손실이 발생한다 하더라도 이는 Fast Recovery에 의해서 복구될 수 있기 때문에 Retransmit Timeout을 방지할 수 있다. 따라서 본 논문에서는 알고리즘의 변화를 최소화하고자 CAP가 타이머를 사용하여 전송을 재개하도록 한다.

2. 성능 분석

앞서 제안된 알고리즘의 성능을 검증하기 위하여 핸드오프 발생에 의한 CWND의 변화를 통해 기존 알고리즘의 성능과 비교하고자 한다. 그림 10에서는 TCP Timeout 방지형 알고리즘과 기존 IEEE802.11b의 성능 차이를 보여준다. 4장의 그림 7에서는 CST로 23dB를 사용하여 한 번의 탐색에 핸드오프가 완료되도록 시나리오를 구성했다. 하지만 앞서 말했듯이 TCP Timeout 방지형 알고리즘의 동작은 다음의 두 가지 경우에 따라서 달라진다. 우선, 탐색 결과 CAP보다 더 큰 SNR값을 가지는 AP가 존재할 경우, 재인증 단계가 진행되기 때문에 CAP는 IAPP를 통해서 NAP로부터 핸드오프가 완료되는 시점을 알 수 있다. 하지만 탐색 결과 CAP보다 더 큰 SNR값을 가지는 AP가 존재하지 않을 경우, 재인증 단계가 진행되지 않기 때문에 CAP가 타이머를 사용해서 전송을 재개해야만 한다. 따라서 한 시뮬레이션을 통해 TCP 방지형 알고리즘이 위의 두 가지 중 어느 경우에도 잘 동작함을 검증하기 위해 CST를 24dB로 증가시켰다. CST의 증가로 인해 MS는 여러 차례의 사전 탐색 이후 NAP로부터의 SNR값이 CAP로부터의 SNR값보다 커지는 순간 재인증 단계를 수행하게 된다. CST를 변경하지 않더라도 각 노드의 위치 변경을 통해 동일한 상황의 재현이 가능하지만 그림 7에서 사용한 시나리오의 변화를 최소화하기 위해 간단히 CST를 조정하였다. 또한 본 논문에서는 MS가 2초 간격으로 탐색을 수행한다고 가정한다. 따라서 그림 10-(a)에서와 같이 2초 간격으로 Retransmit Timeout 혹은 Fast Retransmit이 발생하여 CWND가 감소한다. 하지만 그림 10-(b)에서 보듯이 제안된 알고리즘을 사

용할 경우, 여러 차례의 탐색에도 불구하고 CWND가 감소되지 않은 채 전송이 계속된다.

VI. 결 론

본 논문에서 OPNET 시뮬레이터에 핸드오프 모듈을 구현하고 이를 사용하여 핸드오프 동안 TCP와 UDP의 성능을 분석하였다. 또한 분석 결과를 토대로 TCP Timeout 방지 기법을 제안하고, 이의 성능이 표준 핸드오프 기법보다 우수함을 증명하였다.

UDP를 사용한 시뮬레이션을 통해서 그것의 성능이 핸드오프 지연, 버퍼 크기, 그리고 전송 속도와 직접적인 연관이 있음을 확인할 수 있었다. 일반적으로 큰 버퍼를 사용할 경우 더 적은 패킷 손실이 발생된다. 그러나 큰 버퍼의 사용은 종단 간 지연을 증가시키는 문제를 야기한다. 또한 버퍼의 크기를 증가시킨다하더라도 무선 링크에서 발생하는 패킷 손실은 여전히 해결되지 않는다. 또한 시뮬레이터를 사용한 TCP의 성능 분석에서 AP의 버퍼 오버플로우에 의한 패킷 손실은 볼 수 없었다. 그러나 핸드오프 동안 무선 링크에서 발생하는 패킷 손실로 인해서 Retransmit Timeout이 발생하고 이에 따라 TCP가 CWND의 크기를 줄임으로써 전송률이 저하된다.

이를 해결하기 위해 본 논문에서는 핸드오프에 의한 TCP Retransmit Timeout 발생 문제를 해결하기 위해 핸드오프 동안 데이터 전송을 중단하는 알고리즘을 제시하였으며, 이 알고리즘이 표준에 따른 핸드오프 방식에 비해 CWND가 더 크게 유지되어 전송 속도가 향상됨을 시뮬레이션 결과를 통해 검증하였다. 또한 제안한 알고리즘은 TCP의 경우 뿐만 아니라, UDP의 경우에도 무선 링크에서 발생하는 패킷 손실을 방지하기 때문에 기존 방식에 비해 향상된 성능을 가질 것이다.

참 고 문 헌

[1] Matthew Gast, "802.11 Wireless Networks : The Definitive Guide", O'REILLY, 2002.

[2] 박애순, 윤미영, 김영진, "802.11b 기반의 무선랜 인증 및 보안 기술", 한국통신학회논문지, Vol. 19, No. 8, pp. 114-127, Aug, 2002.

[3] ANSI/IEEE std. 802.11 ; "Wireless LAN Medium Access Control(MAC)과 Physical Layer(PHY) Specifications", 1999.

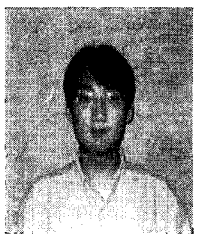
[4] OL-1744-02 ; "Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for MS-DOS", 2002.

[5] OPNET Wireless LAN (IEEE 802.11) http://www.opnet.com/products/library/wlan.html.

[6] ORiNOCO Technical Bulletin 021/A : "roaming with ORiNOCO/IEEE 802.11", December 1998.

[7] W. Stallings, "High-Speed Networks (TCP/IP and ATM design principles)", Computer and Data Communications Technology, January 1998.

정 세 원 (Se-won Jung) 준회원

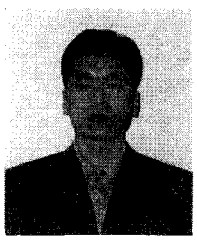


2003년 8월 : 아주대학교 전자공학과 졸업.

2003년 9월-현재 : 아주대학교 대학원 전자공학과 석사과정.

<관심분야> Ad-hoc Network, Ubiquitous networking.

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 9월-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.