휴대인터넷에서 낮은 지연 특성을 가지는 인증유지 핸드오버를 위한 효과적인 트래픽 관리기법

정회원 최 재 우*, 준회원 강 전 일**, 정회원 양 대 헌***

Efficient Traffic Management Scheme for Fast Authenticated Handover in IEEE 802.16e Network

Jae Woo Choi*, Jeon il Kang**, Dae Hun Nyang*** ***Reguler Member***

요 약

현재 표준화 작업이 한창인 휴대인터넷은 무선랜 보다 서비스 범위가 넓으면서 빠른 이동성을 제공하고 있다. 휴대인터넷 환경이 상용화 되면 많은 사용자들이 휴대인터넷을 사용할 것이며 무선 통신량 또한 급증할 것이다. 휴대인터넷에서 핸드오버가 발생했을 때 사용자에게 원활한 서비스를 제공하기위해 핸드오버 지연을 줄이는 것이 중요하다. IEEE 802.16e에서는 핸드오버 지연을 줄이기 위해 이동할 한 개의 기지국에게 단말기가 자신의 인증정보를 전송한다. 그러나 이것은 어느 기지국으로 이동할지 모르는 상황에서 적합하지 않다.

핸드오버 지연을 줄이기 위해 미리 인접한 기지국에 단말기의 인증정보를 보내는 proactive caching 기법은 [4]에 의해서 제안되었고 이 논문에서는 proactive caching 기법에 의해 발생되는 중복되는 네트워크 트래픽을 줄이기 위해 효과적인 트래픽 관리 알고리즘을 제안한다.

Key Words : Handover, Proactive Caching, Traffic Management Algorithm, Cache Hit Ratio, Authentication

ABSTRACT

Recently, Portable Internet being standardized provides fast movement with wider service range than wireless LAN does. If Portable Internet service starts, many people will use Portable Internet and thus wireless traffic is going to increase. In Portable Internet, it is important to reduce handover latency to provide user with satisfactory service when handover occurs. In IEEE 802.16e, MSS sends its own security context information to one Base Station which it will move to reduce handover latency. But this is not suitable in the situation that the BS doesn't know the security context.

To reduce handover latency of proactive caching method that is to send security context information to adjacency Base Stations in advance has been proposed by[4]. In this paper we propose effective traffic management algorithm to reduce signaling network traffic caused by proactive caching method.

Ⅰ. 서 론

휴대인터넷이 등장하게 된 가장 큰 이유는 사용자들이 적은비용으로 무선 서비스가 제공되는 범위에서 장소에 구애받지 않고 빠른 속도로 이동하면서 무선 서비스를 이용할 수 있다는 것이다. 빠른

* 인하대학교 정보보호 연구실(elvin0@seclab.inha.ac.kr), ** 인하대학교 정보보호 연구실(dreamx@seclab.inha.ac.kr),
*** 인하대학교 정보보호 연구실(nyang0@inha.ac.kr)
논문번호 : KICS2004-11-262, 접수일자 : 2004년 11월 9일
※본 연구는 2004년 하나로 텔레콤 2.3GHz 휴대인터넷 연구개발사업의 지원에 의해 연구되었음.

이동에서 많은 데이터량을 요구하지 않는 서비스들(i.e HTTP)은 핸드오버가 발생했을 때 사용자들이 불편함을 느끼지 못하지만 Voice와 기타 Multimedia 서비스는 실시간으로 많은 데이터 량을 요구하므로 핸드오버 지연으로 인한 끊김 현상에 대해 불편함을 느낄 수 있다. 그러므로 기지국(Base Station)들 사이에서의 핸드오버 처리는 빨리 수행되어져야 하며 핸드오버가 일어난 뒤에도 단말기와 관련된 여러 상태 정보들이 핸드오버가 일어나기 이전의 상태 정보와 같아야 한다. 즉, 단말기들의 세션(Session)과 품질(QoS) 그리고 단말기 정보가 핸드오버가 일어나기 전과 동일한 상태로 유지되어야 하는 것이다.

핸드오버의 지연을 줄이기 위해[4]에서는 proactive기법을 이용하여 단말기의 정보를 이동할 인접한 모든 BS들에게 미리 전송하는 것이다. 그러나 이 proactive기법에는 단말기가 어디로 이동할지 모르는 상황이기 때문에 인접한 모든 BS들에게 자신의 정보를 전송하여 전체 네트워크에 불필요한 부하를 초래한다. 이것은 사용자가 많은 휴대인터넷 환경에서 적지 않은 영향을 미치게 된다.

이 논문에서는 [4]의 핸드오버 지연을 줄이는 기법에 효과적인 트래픽 관리 알고리즘을 적용하여 네트워크의 부하를 줄이는 기법을 제안한다. 2장에서는 IEEE 802.16e에서 사용하는 핸드오버 기술을 설명하고 3장에서는 IEEE C802.16e-04/50에서 사용하는 proactive기법을 설명한다. 4장에서는 효과적인 트래픽 관리 알고리즘으로 전체 네트워크의 부하를 줄이는 방법을 설명하며 마지막 5장에서는 4장의 효과적인 트래픽 관리 알고리즘을 시뮬레이션 결과 보여준다.

Ⅱ. 배 경

2.1 IEEE 802.16e 핸드오버

이 논문에서는 다음과 같은 용어를 사용한다.

1) MSS(Mobile Subscriber Station) : 휴대인터넷 단말기
2) serving BS : MSS의 가장 최근 기록을 가지고 있는 기지국
3) target BS : MSS가 serving BS에서 다른 곳으로 이동할 기지국
4) neighbor BS : MSS에 인접한 target BS들
5) HO : 핸드오버

현재 표준화 작업 중인 IEEE 802.16e에서는 무선 랜과 달리 핸드오버가 일어나기 전에 항상 인접한 기지국(neighbor BS)들에 대한 상태를 MSS에게 알려주며 핸드오버가 일어나는 상황은 다음 세 가지가 있다. 첫 번째는 MSS가 현재 서비스를 받고 있는 기지국(serving BS)에게 핸드오버 요청을 하면 serving BS는 target BS들의 상태를 확인하여 가장 적합한 target BS를 MSS에게 알려주는 방식이고 두 번째는 serving BS가 target BS들의 상태를 체크하고 MSS에게 핸드오버 요청을 하면서 적합한 target BS를 MSS에게 알려주는 방식이다. 그리고 마지막은 두 번째와 비슷하지만 serving BS가 적합한 target BS를 알려주는 것이 아니라 MSS가 적합한 target BS를 serving BS에게 알려주는 방식이다.

이러한 세 가지 방식은 핸드오버가 발생하기 전에 MSS가 serving BS로부터 제공받은 target BS의 상태를 보고 가장 적합한 target BS로 핸드오버를 할 것이라는 것을 알고 있다는 가정 하에 proactive 기법을 사용한다. 즉, MSS가 어디로 이동할지 아는 하나의 target BS와만 pre-authentication request/response 메시지를 통해 pre-authentication 과정을 수행하여 핸드오버 지연을 줄이고 있다. 하지만 만약 단말기가 pre-authentication을 수행하지 않은 기지국으로 이동할 경우 핸드오버 지연이 발생된다. 다음절에서는 pre-authentication 메시지를 이용하는 것과는 달리 인접한 모든 target BS들에게 MSS의 security context information을 HO-pre-notification에 포함하여 전송하는 proactive기법을 설명한다. [4]에서 사용하는 이 메시지는 기존 IEEE 802.16e에서 정의한 HO-pre-notification 메시지를 이용한다.

Ⅲ. IEEE C802.16e-04/50의 Proactive Caching

현재 표준화 작업이 진행 중인 IEEE 802.16e에서는 핸드오버를 위해 MSS가 serving BS로 RNG_REQ(Ranging Request) 메시지에 HMAC Tuple를 포함하여 전송하며 이것은 MSS의 인증을 빨리 처리하기 위해 사용된다. IEEE 802.16e는 MSS와 BS 사이의 무선 메시지에 관련해서 표준화작업 중이며 BS와 BS사이의 백본 메시지는 IEEE 802.16g에서 표준화 작업 중이다. 하지만 IEEE 802.16g의 표준화 작업은 아직 시작단계라 어떤 메시지도 정의하고 있지 않은 상태이다.

이렇게 BS와 BS사이의 메시지가 정의되지 않은

상태에서 [4]에서는 빠른 인증을 위해서 HO-pre-notification 메시지를 이용하여 MSS가 target BS들에게 security context information을 전송하는 방법을 기술했다. serving BS가 target BS들에게 HO-pre-notification을 통해서 security context information을 전송함으로써 MSS가 핸드오버를 위한 target BS들에게 암시적으로 인증되는 것이다. 그리고 이 메시지를 받은 target BS들은 전송받은 security context information을 HMAC Tuple을 적용하여 핸드오버 이후의 빠른 인증을 위한 MSS와 target BS 사이의 새로운 인증키를 생성한다.

다음 그림들은 IEEE 802.16e에서 기술한 세 가지 핸드오버 방법들이다. 그림 1은 MSS가 serving BS에게 핸드오버 요청메시지(MOB_MSSHO_REQ)를 전송하고 serving BS가 MSS에게 적절한 target BS를 추천하는 메시지(MOB_HO_RSP)를 통하여 핸드오버를 처리하는 과정이며 그림 2는 serving BS가 target BS들에게 핸드오버를 알리는 메시지(HO-pre-notification)을 전송한 다음에 MSS에게 핸드오버 요청메시지(MOB_BSHO_REQ)를 전송하고 핸드오버를 위해 적절한 target BS를 추천한 메시지(MOB_BSHO_RSP)도 전송하여 핸드오버를 처리하는 과정이다. 마지막 그림 3은 그림 2와 비슷하지만 핸드오버를 위한 target BS를 결정한 메시지(MOB_MSSHO_RSP)를 MSS가 serving BS에게 전송하는 과정이다. 핸드오버를 시작하기 전에 serving BS는

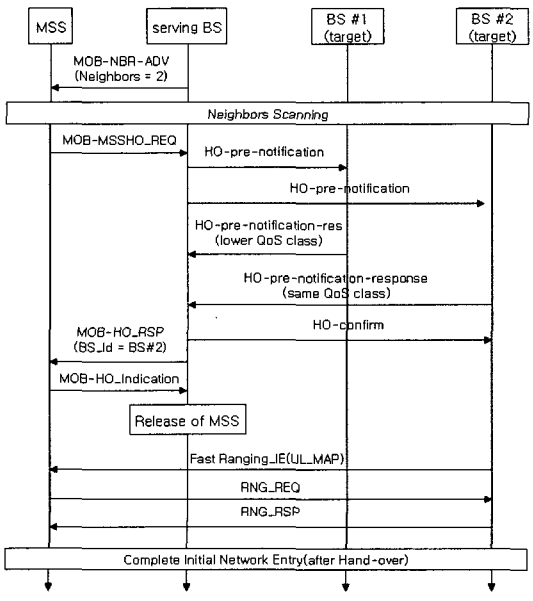


그림 1. MSS 요청에 의한 핸드오버처리

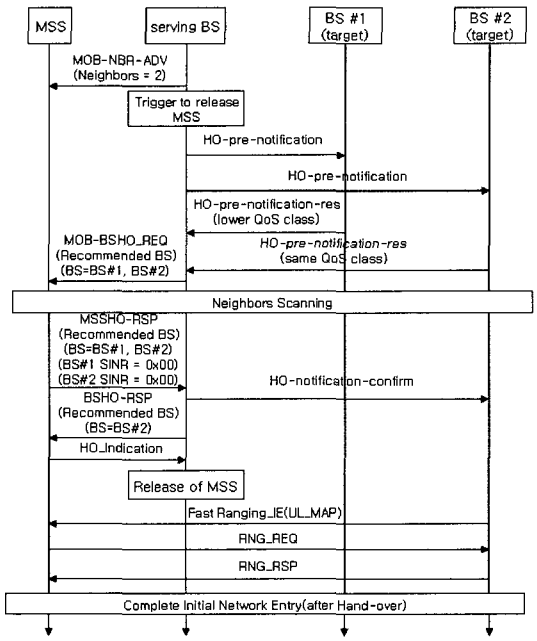


그림 2. BS 요청에 의한 핸드오버 처리

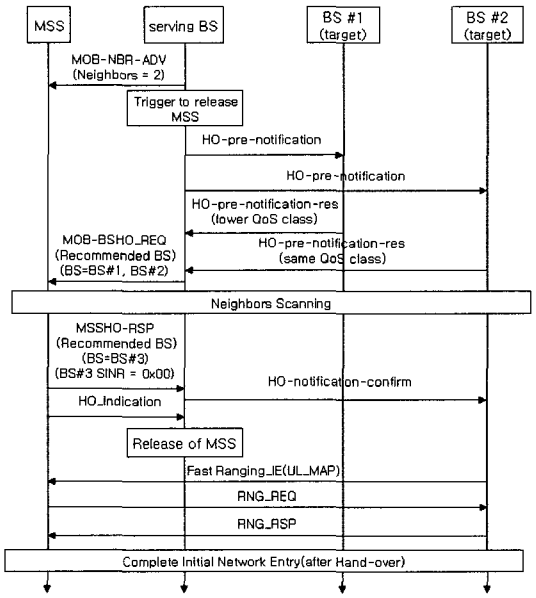


그림 3. BS 요청과 target BS의 MSS결정에 의한 핸드오버 처리

주기적으로 MSS에게 NBR-ADV 메시지를 전송하여 target BS들의 정보들을 알려준다.

Ⅳ. 효율적인 트래픽 관리 알고리즘

3장에서 IEEE 802.16e HO-pre-notification 메시

지를 이용하여 인접한 target BS들에게 미리 MSS의 정보를 전송하는 proactive caching과정을 보여주었다. 이 과정은 핸드오버가 일어난 후에 다시 핸드오버를 시도할 경우에도 똑같이 반복되는데 이때 중복되는 메시지를 발생시켜 전체 네트워크에 부하를 줄 수 있다. 즉, 중복 메시지가 발생하는 상황은 3개의 기지국이 서로 서비스 범위가 중복 되어 핸드오버가 일어나기전의 target BS와 핸드오버가 일어난 후의 target BS가 동일한 BS가 되는 경우이다. BS의 위치가 그 모양이 트라이앵글과 비슷하여 이 논문에서는 트라이앵글 구조라 부른다. 휴대인터넷 환경에서 트라이앵글 구조는 많이 존재할 것이며 이 장에서는 중복되는 메시지로 인한 네트워크 부하를 해결하고자 다음 두 가지를 정의한다.

3.1 정의

1) Authenticated_BS_List : HO-pre-notification 메시지에 포함되며 MSS가 접속한 serving BS에 인접한 target BS들의 id들이 저장된다. 이 정보는 핸드오버가 발생할 때 Authenticated_BS_Table을 이용하여 데이터 트래픽 재전송을 줄이는데 사용된다.
2) Authenticated_BS_Table : Authenticated_BS_Table에 저장되어있는 id들은 해당 MSS에 대해서 이미 인증이 되었다는 것을 표시하며 Table에 BS들의 id가 저장되는 상태는 다음 세 가지가 있다.
   ① HO-pre-notification 메시지를 보낸 BS의 id를 Table에 기록한다.
   ② HO-pre-notification 메시지를 받으면 Authenticated_BS_List에 인증된 BS들의 id들을 Table에 기록한다.(이때 메시지로부터 받은 id들이 자신의 neighbor BS들 중에 있어야 하고 List중에 자신의 id는 제외한다.)
   ③ serving BS가 인증할 target BS로 HO-pre-notification 메시지를 보내고 target BS의 id를 Table에 기록한다.

3.2 효율적 트래픽 관리 알고리즘을 적용시킨 HO-pre-notification 메시지

각 BS마다 Authenticated_BS_Table을 유지하고 있고 이 Table에 있는 정보는 HO-pre-notification 메시지를 통해 인증된 기지국들의 id를 기록한다. Table에 이러한 target BS들의 id들이 저장됨으로써 메시지 재전송을 줄일 수 있다. 즉, HO-pre-notification 메시지를 받은 target BS들은 MSS가 이동해 왔을 때 Authenticated_BS_Table에서 MSS의 정보가 포함되지 않은 target BS들의 id를 확인하고 메시지를 전송한다.

그림 4는 각 BS가 가지고 있는 Authenticated_BS_Table이며 target BS들에 따라 MSS의 정보를 저장하고 있다. 그림 5는 핸드오버가 일어나기 전 target BS들에게 HO-pre-notification 메시지에 자신의 정보와 Authenticated_BS_List를 전송하는 것을 보여주며 그림 6에서는 핸드오버가 발생한 후에 Table에 이미 인증된 target BS의 id를 확인하고 불필요하게 중복되는 메시지는 보내지 않는 것을 보여준다.

target BSs	MSS IDs
BS #2	1013, 2003 …
BS #3	1013, 3312 …
BS #4	1013, 2003 …
.	.
.	.

그림 4. Authenticated_BS_Table

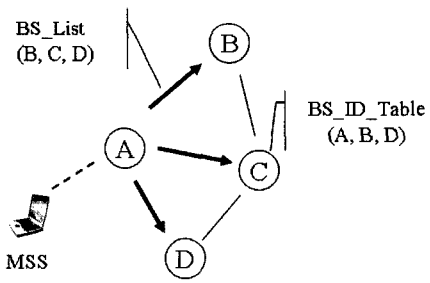


그림 5. 핸드오버가 일어나기 전

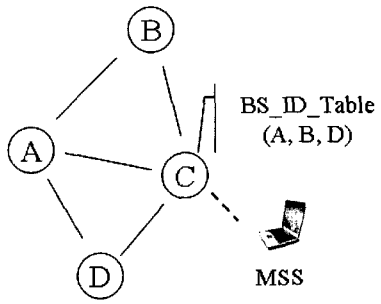


그림 6. 핸드오버가 일어난 후

3.3 BS의 캐쉬 관리를 위한 HO-invalidation* 메시지

이 논문에서는 IEEE 802.16e에서 정의하는 HO-

pre-notification, HO-pre-notification-response, HO-notification-confirm 메시지를 제외하고 기지국의 효과적인 캐쉬 관리를 위해 HO-invalidation 메시지를 정의했다. MSS가 target BS로 이동한 후 기존 서비스를 제공해 주던 serving BS는 MSS와 인접하지 않은 BS들에게 HO-invalidation 메시지를 전송하여 MSS의 정보를 삭제하도록 요청한다. 이것은 BS들이 캐쉬를 효율적으로 관리하기 위해 사용된다.

3.4 Proactive Caching을 위한 효율적인 트래픽 알고리즘

기지국 사이의 메시지 전달 프로토콜은 IEEE 802.16g에서 다루고 있고 시작단계라서 proactive caching기법을 다루는 메시지가 아직 정의 되지 않았으므로 앞서 언급한 메시지들을 이용해 기지국간에 메시지를 전달한다. 다음 함수들은 효율적인 트래픽 관리 알고리즘을 설명하기위해 사용한다.

1) MSS_Context(s) : MSS에 대한 security context information
2) BS_Cache(BSk) : BSk에서 저장하고 있는 캐쉬 데이터구조
3) BS_Table(BSk) : BSk에서 저장하고 있는 테이블 데이터구조
4) Pre_Notification(BSi, s, Authenticated_BS_List, BSj) : HO-pre-notification 메시지를 통해 MSS에 대한 정보와 neighbor BS의 id를 담은 Authenticated_BS_List를 BSi에서 BSj로 전달, Authenticated_BS_List는 효율적인 트래픽 관리를 위해 사용하며 4장에서 언급하고 있다.
5) Delete_MSS_Context_BS_Table(BSold, s, BSnghbr) : BSold는 BS_Cache(BSnghbr)로부터 MSS_Context(s)와 BS_Table(BSnghbr)를 제거하기위해 BSnghbr로 HO-invalidation 메시지를 전송, 이것은 기지국의 효과적인 캐쉬 관리를 위해 사용된다.
6) Delete_BS_ID(BSold, BSnghbr) : BSold는 BSnghbr로 HO-invalidation 메시지를 전송한 BS의 id를 Table에서 제거. 만약 제거하지 않으면 target BS에 자신의 정보가 있다고 판단하고 HO-pre-notification 메시지에 MSS의 정보를 포함하지 않는다. 핸드오버 지연이 발생할 수 있다.
7) Insert_BS_Cache(BSj, Context(s), Authenticated_BS_List) : BSj의 캐쉬에 MSS의 security context information과 Authenticated_BS_List를 저장. 캐쉬 알고리즘은 LRU(Least Recently Used)를 사용한다.

다음 그림 7은 proactive caching을 이용하여 효율적으로 트래픽을 관리하는 알고리즘을 나타낸다.

```
알고리즘은 BSj 혹은 BSk에서 실행된다.
BSi는 old-BS, s는 MSS이다.

 1: if MSS s associates to BSj then
 2:   for all BSi ∈ Neighbor(BSj) do
 3:     Pre_Notification(BSj, s, BS_List, BSi)
 4:   end for
 5: end if
 6: if MSS s reassociates to BSj from BSk then
 7:   if BSi ∉ BS_Table(BSj) then
 8:     for all BSi ∈ Neighbor(BSj) do
 9:       Pre_Notification(BSj, s, BS_List, BSi)
10:     end for
11:   end if
12: end if
13: if MSS s reassociates to BSk from BSj then
14:   for all BSi ∈ Neighbor(BSj) do
15:     Delete_MSS_Context_BS_Table(BSj, s, BSi)
16:   end for
17:   if BSi ∈ BS_Table(BSj) then
18:     Delete_BS_ID(BSj, BSi)
19:   end if
20: end if
21: if BSj received Context(s) from BSi then
22:   Insert_BS_Cache(BSj, Context(s), BS_List)
23: end if
```

그림 7. Proactive Caching을 위한 효율적인 트래픽 관리 알고리즘

V. 시뮬레이션

C++로 구현된 시뮬레이션에서, BS는 제한된 캐쉬 사이즈를 가지며 MSS들은 시뮬레이션 동안 자신의 mobility에 따라서 핸드오버를 한다.

5.1 시뮬레이션 목적

기지국(BS)의 수, 이동통신 단말기(MSS)의 수, MSS의 이동성(Mobility)에 따른 전체 토폴로지의 트래픽 량을 관찰하고, 불필요한 트래픽을 줄이는 알고리즘이 기존 proactive caching 기법의 Cache Hit Ratio에 얼마나 영향을 미치는지 관찰한다.

시뮬레이션 모델과 가정

1) 네트워크 토폴로지 : 초기 BS의 위치는 랜덤하게 설정되며 이 토폴로지는 시뮬레이션이 끝날 때 까지 변하지 않는다.
2) 초기 MSS 위치 : MSS들은 전체 토폴로지에 고루 분산되어 있다.
3) MSS Mobility : 시뮬레이션 동안 주어진 시간에 MSS가 이동하는 횟수로서 한 개의 MSS 이동성을 정의한다. Mobility 표시는 1부터 100까지 모든 MSS들에 대해서 균등하게 분포되어 있다[8]. 예를 들어 100초 동안에 Mobility가 1이면 1에서 100초 사이에 한 번 핸드오버가 발생하며 100이면 매 초마다 발생한다.

5.2 시뮬레이션 환경

1) 시뮬레이션은 초기 BS를 랜덤하게 위치하였다.
2) 시뮬레이션 기간 : Mobility가 100인 MSS를 기준으로 3만 번의 재협상 과정을 세 번 실행하여 평균한 것이며 이것은 결과 값이 만족스러운 신뢰성을 줄 만큼의 충분한 기간이다.

5.3 시뮬레이션 결과

시뮬레이션 1 :

MSS(100), BS(20)의 환경에서 전체 네트워크 트래픽량 비교 : 기존 proactive caching과 효율적인 트래픽 관리 알고리즘을 적용시킨 proactive caching을 비교하였다. HO-pre-notification에 MSS의 정보만 전송시키는 알고리즘보다 효율적인 트래픽 알고리즘과 함께 적용시킨 것이 약 40만개의 트래픽 이득이 있다는 것을 보여준다.

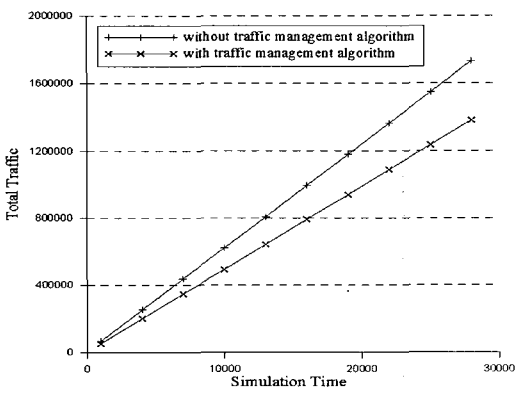


그림 8. MSS(100), BS(20) 환경에서의 전체 네트워크 트래픽량 비교

시뮬레이션 2 :

시뮬레이션 1의 환경에서 Cache Hit Ratio 비교 : 기존 proactive caching의 Cache Hit Ratio와 효율적인 트래픽 관리 알고리즘을 적용시킨 proactive caching을 비교하였다. 각 BS는 MSS의 정보를 저장하기 위해 제한된 캐쉬 20을 가지고 있다. 효율적 트래픽 관리 알고리즘이 기존 proactive caching기법에 크게 영향을 미치지 않으면서 트래픽을 줄이고 있다는 것을 보여준다. 시뮬레이션마다 평균 캐쉬 이득은 0~1% 사이였다.

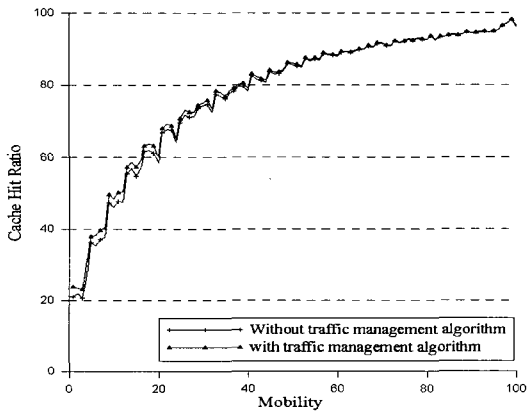


그림 9. MSS(100), BS(20) 환경에서의 Cache Hit Ratio

시뮬레이션 3 :

토폴로지 크기에 따른 트래픽량 : 기존 proactive caching과 효율적인 트래픽 관리 알고리즘을 적용시킨 proactive caching을 비교한다. MSS와 BS가 같은 비율로 증가함에 따라 기존 proactive caching보다 효율적 트래픽 관리 알고리즘을 적용한 proactive caching이 그래프가 완만한 것으로 보아 토폴로지가 커짐에 따라 전체 트래픽량에 많은 이득을 주는 것을 알 수 있다. 가로축 Topology Increasing의 숫자는 토폴로지 크기를 나타내며 다음과 같다.

1=> BS(20), MSS(100)
2=> BS(50), MSS(250)
3=> BS(100), MSS(500)
4=> BS(200), MSS(1000)

시뮬레이션 4 :

MSS 증가에 따른 트래픽량 : BS는 50이고 MSS

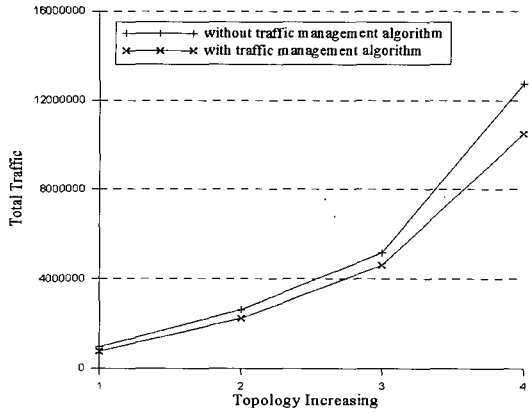


그림 10. 토폴로지 크기에 따른 트래픽량

가 200과 500인 환경에서 proactive caching과 효과적인 트래픽 알고리즘을 적용시킨 proactive caching의 전체 트래픽량의 차이를 비교한다. 그래프를 보면 MSS가 200이였을 때의 차이보다 MSS가 500이였을 때가 차이가 더 크다. 이 그래프는 BS의 개수는 고정이고 MSS가 증가하는 환경에서 그 차이가 점점 커져가는 것으로 보아 MSS가 증가할수록 트래픽 이득률의 차이도 증가하는 것을 보여준다.

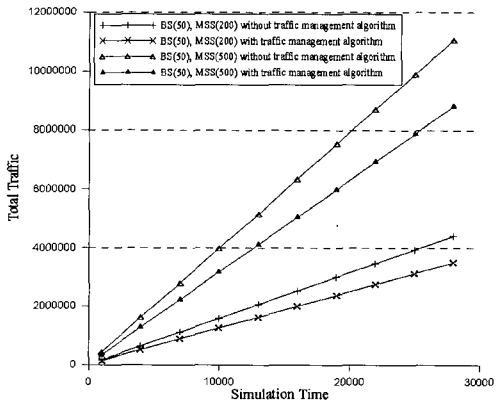


그림 11. MSS 증가에 따른 트래픽량

시뮬레이션 5 :

BS의 위치에 따른 트래픽량 : BS(20), MSS(100)으로 일정하고 토폴로지를 변경하면서 기존 proactive caching과 효과적 트래픽 알고리즘을 적용시킨 proactive caching의 전체 트래픽량을 비교한다. 토폴로지는 랜덤하게 위치하였고 BS의 트라이앵글 구조(3개의 BS 서비스 범위가 서로 겹쳐진 환경)를 증가시켰다. 가로축 The number of overlaped BSs는 다음과 같다.

1=> 2개의 트라이앵글 구조
2=> 4개의 트라이앵글 구조
3=> 7개의 트라이앵글 구조
4=> 9개의 트라이앵글 구조

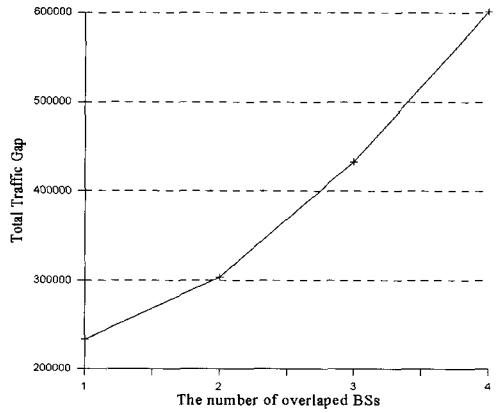


그림 12. BS의 위치에 따른 트래픽량

Ⅵ. 결 론

머지않아 휴대인터넷 환경에 맞는 단말기가 상용화 되면 사용자들은 훨씬 적은 비용으로 높은 수준의 서비스를 받을 수 있을 것으로 기대되며 그로 인해 많은 사용자들이 휴대인터넷을 이용할 것이다. 휴대인터넷 환경에서 사용자들에게 조금 더 나은 서비스를 제공하면서 서비스 기업들에게는 네트워크 부하를 개선시키기 위해 이 논문에서는 핸드오버의 지연을 줄이기 위한 기존 IEEE 802.16e의 proactive caching기법에서 메시지 중복으로 발생하는 불필요한 트래픽량을 줄이는 방법을 제안했다.

현재는 이동성이 빠른 휴대인터넷 환경에서 한 홉 거리에 있는 기지국들에게만 단말기의 정보를 전송하여 핸드오버 지연을 줄이고 있지만 속도가 빠르면 기지국이 단말기의 정보를 전송받기 전에 다른 기지국으로 이동 할 수 있는 상황이 발생하여 핸드오버의 지연이 발생 할 수 있을 것 이다. 향후 이러한 문제를 해결하기 위해 자주 가는 한 홉 이상의 기지국에게 미리 단말기의 정보를 전송하여 핸드오버 지연을 줄이는 방법이 적용 될 수 있을 것이다.

참 고 문 헌

[1] IEEE, "IEEE Standard for Local and metropolitan area networks--Port-Based Network

Access Control", *IEEE Standard 802.1x-2001*, June 2001

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

[3] IEEE, "Draft 5 Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands", *IEEE P802.16e/D5*, September 2004

[4] Dongkie Lee, DongRyul Lee, DongIl Moon, JongKuk Ahn SK Telecom, "Minimization of Handoff interruption time skipping Reauthorization procedure, *IEEE C802.16e-04/50*, May 2004

[5] Sangheon Pack and Yanghee Choi, "Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN," *Networks 2002 (Joint ICN 2002 and ICWLHN 2002)*, August 2002.

[6] Sangheon Pack and Yanghee Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x Model," *IFIP TC6 Personal Wireless Communications 2002(To Appear)*, October 2002.

[7] Arunesh Mishra, Minho Shin, and William Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," *ACM Computer Communications Review*, Apr. 2003.

[8] A. Mishra, M. Shin, and W. A. Arbaugh, "Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network," *IEEE Infocom 2004*, Mar. 2004.

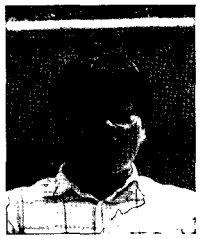
최 재 우(Jae Woo Choi) 정회원

2003년 2월 안동대학교 정보통신공학과 졸업

2003년 9월~현재 인하대학교 정보통신대학원 석사과정

<관심분야> WLAN 보안, 휴대인터넷 보안

강 전 일(Jeon il Kang) 준회원



2003년 2월 인하대학교 컴퓨터공학과 졸업

2004년 3월~현재 인하대학교 정보통신대학원 석사과정

<관심분야> 정보보호, RFID 보안

양 대 헌(Dae Hun Nyang) 정회원

1994년 2월 한국과학기술원 과학기술 대학 전기 및 전자공학과 졸업

1996년 2월 연세대학교 컴퓨터과학과(석사)

2000년 8월 연세대학교 컴퓨터과학과(박사)

2000년 9월~2003년 2월 한국전자통신연구원 정보보호연구본부 선임연구원

2003년 9월~현재 인하대학교 정보통신대학원 교수

<관심분야> 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안, RFID 보안, 휴대인터넷 보안