한국시뮬레이션학회 '99추계학술대회 논문집 1999.10.9 한양대학교

경로설정 최적화와 바인딩 확장을 이용한 개선된 Mobile IP 핸드오프 기법

오현우, 조영종, 최덕규
아주대학교 컴퓨터공학과

An Enhanced Mobile IP Handoff Mechanism using Routing Optimization and Binding Extension

Hyun Woo Oh, Young Jong Cho, Duk Kyu Choi
Division of Information and Computer Engineering, Ajou University

Abstract

A mobile IP is proposed to support host mobility over the current Internet. One of the most important issues on the host mobility is location and routing schemes that allow mobile hosts to move effectively from one site to another. In a Mobile IP environment, frequent handoffs are likely to degrade the performance of data transport. The proposed method is to enhance the transport performance by minimizing the loss of datagrams during handoffs. The handoff scheme is using routing optimization and binding extension to improve the performance by minimizing the average transfer delay of messages and packet loss. Simulation details show the improvement of transport delays and packet loss rate.

1. 서론

Mobile IP프로토콜은 인터넷 호스트에게 이동성을 지원하기 위한 프로토콜이다. 기본적인 Mobile IP프로토콜을 살펴보면 각각의 이동호스트(MH: Mobile Host)는 단일 홈 주소를 이용하여 어느 지점을 통해서라도 네트워크에 접속할 수 있다. MH와 통신하는 호스트를 Correspondent Host(CH)라 하자. 각각의 MH는 자신의 현 위치를 관리하는 홈 에이전트(HA: Home Agent)를 가지고 있어야 하며 만일 MH가 자신의 HA가 아닌 다른 외부 에이전트(FA: Foreign Agent)가 관리하는 네트워크로 이동했을 경우 MH는 FA에 등록되고 IP상에서 지역적으로 할당된 Care-of-Address(CA)를 HA에 등록하게 된다. 또한 이동의 투명성을 지원하기 위하여

주기적으로 HA에 MH의 위치정보를 갱신한다. HA는 이러한 MH의 현 위치를 나타내는 CA를 유지함으로써 MH로 전송되는 모든 데이터그램을 인터셉트하여 실제 MH가 위치한 FA로 데이터그램을

IP-in-IP 인캡슐레이션(encapsulation)을 사용하여 터널링(tunneling)하게 된다. CA는 FA 자신

의 IP 주소일 수도 있고 DHCP (Dynamic Host Configur- ation Protocol)등을 통해 할당받은 MH의 지역주소일 수도 있다. MH가 데이터그램을 수신한 후 CH에게 응답 메시지를 전송할 때에는 자신의 HA를 경유하지 않고 FA에서 CH로 직접 전송할 수 있다[5].

이곳에서는 핸드오프 방안의 문제점을 보안하기 위해 바인딩 확장에 의한 개선된 핸드오프를 제안한다. 그리고 전송 지연시간(delay time)과 데이터그램 손실(loss)을 기준으로 한 시뮬레이션을 통해 기존의 핸드오프 시 바인딩 캐시와 버퍼링을 이용한 방법보다 바인딩 확장에 의하여 개선시킨 핸드오프 방안이 더 우수함을 보인다.

2. Mobile-IP환경에서의 기존의 핸드오프 기법

2.1 Mobile IP상에서의 핸드오프 기본 모델

그림 1은 Mobile IP상에서 이루어지는 핸드오프의 기본적인 시나리오를 나타낸다.

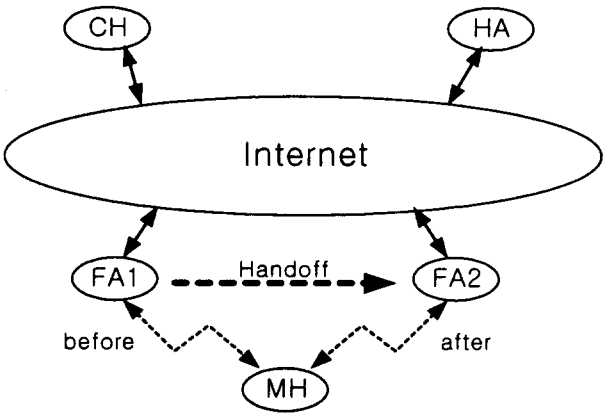

그림 1 기본적인 핸드오프 시나리오

핸드오프 중에 발생되는 문제는 MH에게 서비스를 제공해야 하는 FA2가 MH의 인증 및 등록절차가 완료되기 전에는 FA2로 향하는 메시지 터널링이 불가능하게 된다는 것이다. 따라서 MH의 인증 및 등록절차가 완료되기 전에 CH로부터 전송된 데이터그램은 손실되게 된다. 데이터그램이 손실되는 이 구간을 취약구간(Vulnerable Period)이라고 한다. 기본적인 Mobile-IP에서는 MH에 대한 위치정보가 HA에 기록되므로 CH가 MH로 데이터그램을 전송할 때는 반드시 HA를 통해 전송된다. 즉 CH에서 전송된 데이터그램을 HA가 인터셉트한 후, HA는 MH가 존재하는 FA1의 CA로 이 데이터그램을 터널링한다[4]. 따라서 패킷의 지연과 취약구간에 전송되는 패킷의 손실이 크게 된다. 이러한 문제점을 해결하기 위한 방법으로 경로설정 최적화 기법 중 하나인 바인딩 캐시(Binding Cache) 방법이 있다[1],[4],[6].

2.2 바인딩 캐시 방법에 의한 핸드오프

기본적인 Mobile IP에서는 비효율적인 라우팅이 존재하기 때문에 대용량의 빠른 전송을 요구하는 환경에서는 적합하지 못하다. MH의 홈 주소와 FA의 IP주소(CA)의 조합인 바인딩(binding) 정보를 저장하는 바인딩 캐시 방법은 종전에 Mobile IP 상에서 HA를 반드시 경유해야 하던 경로설정을 보완한 경로설정 최적화의 기법이다[6],[9]. 바인딩 캐시 방법을 이용한 경로설정 최적화는 네트워크에 걸리는 부하를 줄일 뿐 아니라 보다 빠른 데이터그램 전송이 가능하다[2],[3]. 각 노드는 바인딩 정보를 저장할 수 있지만 편의상 데이터그램을 전송하는 CH가 MH에 대한 바인딩 정보를 저장하는 것으로 가정한다. 만일 CH가 MH에 대한 바인딩 정보를 저장하고 있다면 HA를 경유하지 않고도 목적지 IP 주소로 데이터그램을 터널링할 수 있다[8]. 전송할 메시지를 갖는 CH는 HA에게 바인딩 요구 메시지를 보내고 HA는 MH의 IP 주소(현 FA의 IP 주소)가 포함된 응답 메시지를 리턴하게 되고 CH에서 바인딩 캐시가 이루어진다. 바인딩 캐시 방법을 이용한 핸드오프 기법은 경로설정 최적화에 따라 패킷의 지연이 현저히 줄어들 수 있다. 하지만 핸드오프 동안에 발생하는 취약구간

은 아직도 존재하게 되고 바인딩 정보를 저장하기 위한 제어 메시지가 추가됨으로써 취약구간이 길어질 수 있다. 따라서 고속의 대용량 전송이 요구되는 환경에는 적합하지 않다.

2.3 버퍼링을 이용한 개선된 핸드오프

기본적인 Mobile IP상에서의 핸드오프와 바인딩 캐시 방법에 의한 핸드오프는 취약구간이 존재하며 이 기간 동안에 전송된 데이터그램은 손실된다. 또한 손실된 메시지가 재전송 되기까지 많은 지연시간이 요구된다. 따라서 인터넷망에서 가장 중요한 특징인 대용량의 고속전송을 요구하는 환경에서는 데이터그램이 손실되는 취약구간이 가장 큰 문제점이다. 버퍼링을 이용한 핸드오프 기법은 취약구간에 전송된 데이터그램을 이전에 서비스를 제공하던 FA1에서 버퍼링을 한다. 핸드오프가 완료되고 등록절차가 완벽하게 이루어진 뒤에 버퍼링된 데이터그램을 MH에게 전송하면 메시지의 손실을 막을 수 있다. 즉 취약구간으로 인한 문제를 해결할 수 있다. MH가 FA2로 이동할 때 FA2에게 등록요구 메시지를 전송하게 되고 또한 동시에 FA1에게도 등록요구 메시지를 전송한다. FA1이 등록요구 메시지 사본을 수신하게 되면 MH가 자신의 서비스 영역을 벗어났다고 간주하고 그 시점으로 CH로부터 터널링되어 수신되는 모든 메시지를 버퍼링한다. 그 후 등록절차가 완료되어 HA로부터 등록승인 응답을 수신한 MH는 FA1에게 등록삭제 요구 메시지를 전송한다. 이 메시지를 FA1이 수신하면 그 동안 버퍼링하고 있던 모든 메시지를 MH로 전송하게 되고 데이터그램이 손실되는 취약구간을 갖지 않는다. 그러나 이 방안은 두 가지 문제점을 안고 있다. FA1에서 MH로의 데이터그램을 저장하는 일시적인 버퍼의 용량은 유한한데 비해 등록절차의 지연이 무한히 길어지게 되면 버퍼의 오버플로우가 초래된다. 일반적으로 IP프로토콜의 상위 계층에서는 TCP프로토콜이 사용된다. TCP프로토콜 상에서 데이터그램이 전송될 때 전송된 데이터그램에 대한 타이머가 설정된다. TCP 계층에서 전송된 데이터그램이 Mobile IP상의 취약구간동안 FA1에 버퍼링이 되고 TCP 계층에서는 전송된 데이터그램에 대한 TCP 전송 타이머가 정지(off)된다. 이때 TCP프로토콜은 재전송 알고리즘(Binary Backoff Algorithm)을 동작시키고 데이터그램을 재전송하게 된다[7]. CH에서는 TCP프로토콜에 의해 데이터그램의 재전송이 이루어지고 Mobile IP상의 FA1은 동일 데이터그램을 수신하여 버퍼링하게 된다. 비록 기본적인 Mobile IP와 바인딩 캐시 방법에서의 데이터그램이 손실될 수 있는 취약구간은 제거됐지만 FA1은 불필요하게 재전송된 데이터그램을 처리해야 하고 유한 버퍼의 오버플로우로 인한 네트워크의 과부하가 발생할 수 있다. 3장에서는 이러한 문제점을 해결하고 고속의 대용량 실시간 서비스를 지원하는 바인딩 확장에 의한 개선된 핸드오프 기법를 제안하고 있다.

3. 바인딩 확장에 의한 핸드오프 성능의 개선

지금까지 제시한 핸드오프 기법들은 메시지가 손실되는 취약구간으로 인한 불필요한 메시지 재전송과 버퍼의 오버플로우로 인한 자원 낭비의 문제점이 발생하였다. 이곳에서 제안하는 바인딩 확장에 의하여 성능을 개선시키는 핸드오프 기법은 취약구간에서 발생하는 문제와 버퍼의 오버플로우 문제를 해결한다. 그림 2는 바인딩 확장에 의하여 인증절차를 간소화하는 타이밍 다이어그램을 나타낸다.

각 노드는 바인딩 정보를 상호 송수신 함으로써 최신의 바인딩 정보를 유지하게 되고 경로설정 최적화가 이루어진다. 바인딩 캐시 방법을

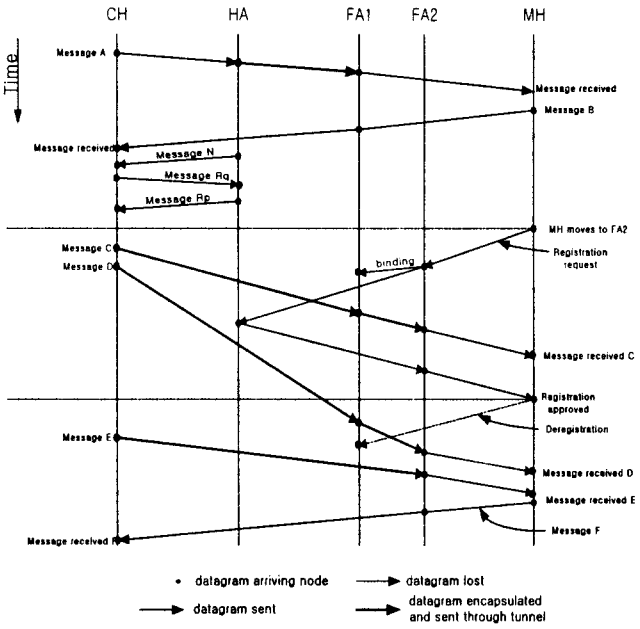

그림 2 바인딩 확장에 의한 개선된 핸드오프 타이밍 다이어그램

이용한 핸드오프에서 발생하는 취약구간은 등록 절차 중 인증절차와 관련된다. 본 논문에서는 인증절차를 간소화하기 위해 바인딩 정보를 확장한다. 확장된 바인딩 정보는 기본적인 바인딩 정보에 SPI(Security Parameter Index)와 인증자(Authenticator)가 추가된다. 등록절차와 함께 이루어지는 인증절차를 위해 각 MH, HA, FA는 그들의 보안 파라미터 색인(SPI: Security Parameter Index)과 IP주소에 의해 색인된 이동 개체들에 대한 이동성 보안 결합 (Mobility Security Association)을 지원해야 한다. 보안 파라미터 색인은 보안 문맥(Security Context)을 구별하는 색인이고, 보안 문맥은 인증 알고리즘(Keyed-MD5)과 인증 모드, 시큐리티, 재사용 방지 스타일등으로 구성된다[5]. 인증자는 키로써 존재하며 이 키값은 HA에 최초로 등록될 때 MH에게 부여되고 이 키값을 알고 있는 에이전트가 MH에 대한 인증절차를 수행할 수 있다. MH가 최초로 HA에 등록될 때 HA와 이동성 보안 결합(Mobility security association)을 맺게 되고 키 값을 할당받는다. FA1에서는 서비스를 제공할 때 CH가 MH에 대한 바인딩 정보를 저장하고 있다면 FA로 직접 터널링하게 되고 데이터그램을 수신한 FA는 MH에 대한 확장된 바인딩 정보를 저장하게 된다. MH가 핸드오프 수행시 FA2로부터 방송되는 신호를 수신한다. MH는 IP 주소, 시스템 ID 등을 비교한 후 FA2에게 등록요구 메시지를 전송하여 등록절차를 수행하게 된다. FA2는 자신의 서비스 영역에 들어온 MH의 확장된 바인딩 정보를 기록하고 HA에게 MH의 등록요구 메시지를 순방향으로 전송함과 동시에 MH의 바인딩 정보를 FA1로 전송한다. 바인딩 확장에 의해 FA1과 FA2 사이에는 인증절차를 위한 관계를 맺고 있기 때문에 FA1은 수신한 바인딩 정보를 통해 MH를 인증하고 위치정보도 알게 된다. 이 시점에서 CH로부터 터널링되는 모든 데이터그램은 FA1에서 FA2로 순방향 전송을 한다. 등록요구 메시지를 수신한 HA는 MH의 위치 정보를 갱신하고 등록확인 메시지를 FA2에게 전송한다. MH가 등록확인 메시지를 수신하게 되면 등록절차가 완료되고 MH는 FA1에게 등록 해제 메시지를 보낸다. 이 동안에 전송해야 할 메시지는 FA1에게 터널링되고 곧바로 FA2에게 순방향으로 전송된다.

이곳에서 제시한 바인딩 확장에 의한 방법에서는 FA1에게 바인딩 정보를 전송하는 것으로 인증절차가 간소화되고 등록과 인증절차를 분산시킴으로써 보다 높은 효율을 얻을 수 있다. 따라서 버퍼링을 이용한 개선된 핸드오프에서는 무선환경 하에서 등록요구가 이루어지지만 바인딩 확장에 의한 개선된 핸드오프에서는 유선 환경 하에서 바인딩 정보를 교환함으로써 메시지 손실로 인한 문제를 제거하며 버퍼링으로 인한 자원 낭비를 줄임으로써 핸드오프 시의 성능을 향상시킬 수 있다.

4. 시뮬레이션

이 장에서는 기존의 Mobile IP 핸드오프 기법

들(바인딩 캐시 방법에 의한 핸드오프와 버퍼링을 이용한 개선된 핸드오프)과 제안한 바인딩 확장에 의한 개선된 핸드오프 기법을 메시지 전송의 지연시간과 패킷 단위 데이터그램의 손실을 비교 척도로 하여 시뮬레이션 한다. 시뮬레이션 결과 제안한 바인딩 확장에 의한 개선된 핸드오프 기법이 우수함을 입증한다.

실제적인 시뮬레이션을 위하여 네트워크 모델은 그림 1을 가정한다. CH에서 발생되는 메시지의 발생률은 포아송 분포를 따르고 메시지의 크기는 부정 지수 분포(Negative Exponential Distribution)를 따른다. 시뮬레이션 수행에 사용된 파라미터들은 다음과 같다.

- Simulation time 90000000 *sec*
- Mobile link data network 57.6 *kbps*
- Data rate within local network 10 *Mbps*
- Data rate from local network to Internet sites 256 *Kbps*
- Message generation rate poisson(*mean*=1/)
- Message size negative exponential(*mean*=1/*u*)
- Packet size 60000 *bit*
- Handoff generation rate 1/(i*1000000)

(i=1,2,---,100)(*number/usec*)

생성된 메시지는 패킷 단위로 나뉘어져 송신측 에이전트에서 인터넷을 통하여 목적지 에이전트에게 터널링된다. 시뮬레이션 방식은 이벤트 드리븐(Event-Driven)방식을 이용하며 시뮬레이션을 위해 MH는 FA를 가변적으로 이동하고 HA는 MH의 등록요구 시 무조건 승인해 주는 것으로 가정한다. 한번의 시뮬레이션 전체 시간은 많은 결과 데이터를 산출하기 위하여 충분한 시간을 주었고 핸드오프율(Handoff Rate)은 10E-6 정도로 작게 주어 잦은 핸드오프 중에 패킷 손실과 메시지 지연을 측정한다. 시뮬레이션은 100번을 수행하며 매 시뮬레이션 수행 시마다 핸드오프율을 변화시킨다. 시뮬레이션 초기에는 핸드오프가 많이 일어나고 시뮬레이션이 진행됨에 따라서 적게 일어난다. 그림 3은 시뮬레이션을 수행한 결과의 메시지 평균 지연을 나타낸다.

X축은 핸드오프율이 점점 작아지는 동안 100

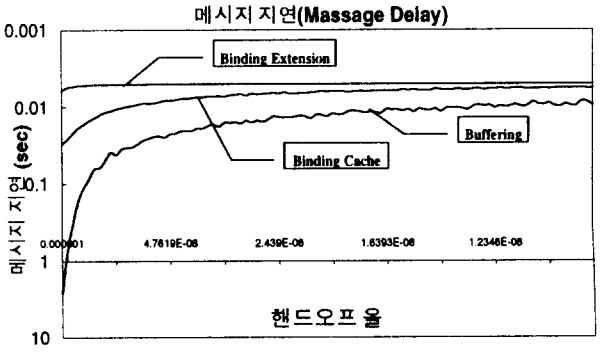

그림 3 메시지의 평균 지연

번의 시뮬레이션이 수행됨을 나타내고 Y축은 부정 지수 분포로 발생된 메시지의 전송 지연을 로그 수치로 나타낸 것이다. 버퍼링을 이용한 핸드오프 기법은 핸드오프가 많이 일어날 때 버퍼링도 많이 하게 되며 이에 따라 메시지의 지연이 크게 나타난다. 이에 비해 바인딩 확장을 이용한 핸드오프 기법은 버퍼링을 하지 않고 새로운 에이전트로 터널링이 됨으로 메시지 지연이 작다.

그림 4는 시뮬레이션을 수행한 결과의 패킷 평균 손실을 나타낸다.

X축은 그림 3과 동일하며 Y축은 부정 지수 분포로 발생하고 부정 지수 분포의 크기를 갖는 메시지가 패킷 단위로 나뉘어져 전송될 때 발생된 패킷 손실을 나타낸다. 바인딩 캐시의 경우 취

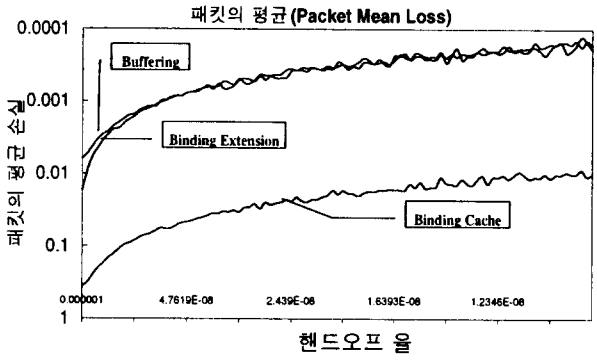

그림 4 패킷의 평균 손실

약구간으로 인한 패킷 손실이 많은 반면, 버퍼링을 이용한 핸드오프 기법과 바인딩 확장을 이용한 핸드오프 기법은 취약구간이 없으므로 패킷 손실이 매우 작다. 하지만 패킷 손실이 전혀 없지 않은 것은 네트워크 자체 손실이며 이는 무시될 수 있는 정도이다.

5. 결론

기존의 Mobile IP 상에서의 핸드오프 기법들은 등록절차 및 인증절차가 완료되기까지 패킷이 손실되는 취약구간이 존재하거나 버퍼의 오버플로우가 발생되었다. 이곳에서 제안한 바인딩 확장을 이용한 핸드오프 기법은 인증절차를 간소화하는 특징이 있고 패킷 손실과 메시지 지연을 줄일 수 있기 때문에 고속의 대용량 실시간 서비스가 요구되는 환경에 사용할 수 있다. 그러나 이 기법은 구현상 기존의 핸드오프 기법보다 더 복잡할 수 있고 인증절차의 신뢰성이 문제점으로 나타날 수 있다.

참고문헌

[1] Myles A., Johnson D.B., and Perkins C., "A Mobile Host Protocol Supporting Routing Optimization and Authentication", *IEEE JSAC*, vol. 13, no. 5, June 1995.

[2] Woo W., Leung V.C.M., "Handoff Enhancement in Mobile-IP Environment", *IEEE ICUPC'96*, 1996.

[3] Tekinay S., Jabbari B., "Handover and channel assignment in mobile cellular networks", *IEEE Communication Magazine*, pp 42-46, November 1991.

[4] Johnson D.B., "Scalable Support for Transparent Mobile Internetworking", Computer Science Department, Carnegie Mellon University.

[5] Perkins C., "IP Mobility Support", RFC 2002, October 1996.

[6] Johnson D.B., "Route Optimization in Mobile IP", Technical report, draft-ietf-mobileip-optim-07.txt, November 1997.

[7] Cáceres R., Iftode L., "Improving the Performance of Reliable Transport Protocol in Mobile Computing Environments", *IEEE Trans. on Selected Areas in Communication*, pp. 850-857, June 1995.

[8] Cho G., Marshall L.F., "An Efficient Location and Routing Scheme for Mobile Computing Environments", *IEEE JSAC*, Vol 13 , NO.5 June 1995.

[9] Simpson W., "IP in IP Tunneling", RFC 1853, October 1995.