Mobile IP 망에서 지역 등록 기법을 이용한 효율적인 인증 방안

장 성 은[†] · 박 정 민[††] · 채 기 준[†††]

요 약

Mobile IP는 이동 단말기를 통해 인터넷 서비스를 받고자 하는 요구가 늘어남에 따라 기존의 IP 망에서 사용자의 이동성을 지원하기 위한 프로토콜이다. Mobile IP는 이동 노드가 외부 에이전트를 통해서 홈 에이전트에 등록을 시도할 때마다 신원을 확인하기 위하여 안전한 인증 과정을 수행해야 한다. 본 논문에서는 Mobile IP의 등록기법을 기존의 홈 에이전트에서만 수행하는 기법이 아닌 지역등록 기법을 도입하였다. 즉 등록 기법을 홈 등록과 지역등록으로 나누어서 이동 노드가 새로운 외부 네트워크에서 접속할 경우 지역 에이전트를 두어서 지역 에이전트에서 인증 과정을 수행함으로써 홈 에이전트와의 빈번한 인증 등록 과정을 생략하였다. 시뮬레이션 결과를 통해 제안된 인증 메카니즘이 기존의 인증 메카니즘에 비해 전체 등록 시간이 짧다는 것을 확인할 수 있었다.

An Efficient Authentication Mechanism Using Regional Registration in Mobile IP Network

Sung-Eun Jang[†] · Jung-Min Park[††] · Ki-joon Chae[†††]

ABSTRACT

As Internet access through mobile devices is increasing, Mobile IP is the protocol to provide the mobility of a host on the existing IP. It is important to provide secure authentication when mobile node register with home agent through the foreign agent each time it moves. In this paper, we propose the authentication mechanism using a regional registration. The proposed authentication mechanism reduce frequent home registration in regional movement. The simulation results show that the proposed authentication reduces the total registration time and is more efficient than conventional registration mechanism.

키워드 : Mobile IP, 인증(authentication), 지역등록(regional registration)

1. 서 론

노트북, 휴대전화, PDA등과 같은 이동 단말기를 통해 인터넷 서비스를 받고자 하는 요구가 늘어남에 따라 사용자의 이동성을 지원하기 위한 다양한 기술들이 개발되어 왔으며, 특히 이동중인 데이터 서비스 사용자들에게 서비스를 제공하기 위한 연구가 매우 활발히 이루어지고 있다. 시스템의 네트워크 관련 매개변수의 값을 변경하지 않고 지리적인 위치에 상관없이 인터넷 서비스를 이용할 수 있고 다른 라우터나 호스트를 변경하지 않고 계속해서 사용할 수 있는 기술이 필요하게 되었다. IETF의 Mobile IP 프로토콜[1, 2]은 이동성을 제공하는 프로토콜로서 이동 호스트가 자신의 IP 주소를 바꾸지 않고 이동할 수 있으며 이동 중에도 상위 계층의 연결을 유지할 수 있다.

Mobile IP 프로토콜은 이동 호스트가 이동하면 외부 에이전트를 통해서 이동 노드의 새로운 위치 정보를 홈 에이전트에 등록시킨다. 그런데 만약 악의를 가진 사용자가 이동 노드임을 가장하여 등록을 시도할 경우 잘못된 COA(Care of Address)를 홈 에이전트의 라우팅 테이블에 등록시키게 되므로 홈 에이전트는 등록 메시지가 올바른 이동 노드로부터 전송됨을 확신할 수 있도록 홈 네트워크와 이동 노드 사이에 안전한 인증과정을 수행해야 한다. 이러한 Mobile IP 프로토콜은 몇 가지 문제점을 가진다. 첫째, 이동 노드가 현재 속해 있는 네트워크에서 다른 네트워크로 이동할 때마다 홈 에이전트에 저장되어 있는 COA를 변경해야 하므로 홈 에이전트에 이동노드를 빈번하게 등록해야 한다. 둘째, 이동 노드가 홈 네트워크에서 멀리 떨어질수록 홈 에이전트로 등록할 때 발생하는 핸드오프 지연시간이 증가함으로써 패킷

※ 본 연구는 정보통신부의 대학기초연구지원 사업의 결과임.
† 정 회 원 : 이화여자대학교 과학기술대학원 컴퓨터학과
†† 준 회 원 : 이화여자대학교 과학기술대학원 컴퓨터학과
††† 종신회원 : 이화여자대학교 컴퓨터학과 교수
논문접수 : 2002년 7월 29일, 심사완료 : 2002년 8월 21일

손실이 증가하고 처리율이 감소한다. 셋째 이동 노드를 향해 전송한 IP 패킷이 최적의 경로를 따르지 않고 홈 에이전트를 반드시 거쳐가므로 삼각 라우팅 문제가 발생한다.

본 논문에서는 이동 사용자가 새로운 외부 네트워크로 접속했을 경우 지역 등록 기법을 이용하여 홈 등록과 지역 등록으로 나누어 인증 메카니즘을 수행하여 이동 사용자가 빈번하게 홈 에이전트로 인증을 요구하는 시간을 줄임으로써 보다 효율적이고 빠른 인증 메카니즘을 제안하고자 한다.

또한 Mobile IP 망에서 기존의 인증 메카니즘인 비밀키 기반 인증 기법, 공개키 기반 인증 기법 및 최소 공개키 기반 인증 기법의 세 가지 인증 기법을 기존의 Mobile IP 인증과 지역 등록 기법을 이용한 Mobile IP 인증에 각각 적용하여 성능을 평가함으로써 안전하고 효율적인 인증 메카니즘을 제안하고자 한다.

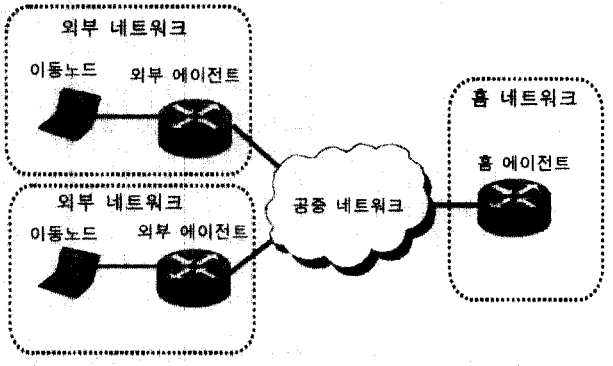
본 논문의 구성은 다음과 같다. 2장에서 Mobile IP 동작 및 지역 등록 기법에 대해 알아보고 3장에서는 제안하는 지역 등록 기법을 이용한 인증 기법에 대해서 설명한다. 4장에서는 다양한 시나리오의 시뮬레이션을 통해 제안한 인증 방법의 성능을 비교·분석하고 5장에서 결론을 맺는다.

2. Mobile IP 인증 서비스 구조

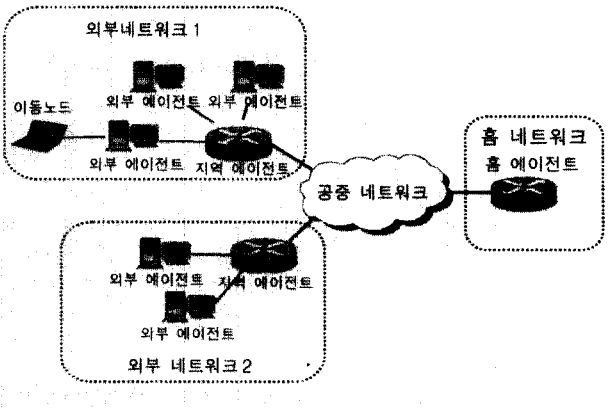
Mobile IP는 기존의 IP 상에서 호스트에게 이동성을 제공하기 위한 프로토콜이다. 호스트의 이동성을 제공하기 위해 홈 네트워크와 외부 네트워크에 이동 에이전트를 둔다. 에이전트는 자신의 존재를 알리기 위해 주기적으로 이동 에이전트 광고 메시지를 네트워크에 전송한다. 이동 노드가 홈 네트워크에서 외부 네트워크로 이동하면 이동 노드는 이동 에이전트 광고 메시지를 통해서 외부 에이전트를 발견하고 외부 에이전트에서 새로운 COA를 받는다. 이동 노드는 새로운 COA를 홈 에이전트에게 등록 요청하고, 홈 에이전트는 COA까지 터널을 생성하여 이동 노드로 전송되는 패킷을 가로채서 터널링의 방법으로 이동노드에게 전달한다.

등록 정보를 인증하는 것은 Mobile IP에서 모든 데이터그램이 이동하는 통로를 결정하기 때문에 매우 중요하다. 인증 메커니즘은 합법적으로 통신하는 이동 노드와 홈 에이전트 사이에 인증 메시지의 안전성을 보장하기 위한 것으로 중간에 메시지가 변조되지 않도록 하며 이전에 사용되었던 인증 메시지가 잘못 재사용되는 것을 막기 위해서이다. (그림 1)은 기존의 Mobile IP 메커니즘을 보여준다. 기존의 Mobile IP 메커니즘 동작을 살펴보면 몇 가지 문제점이 나타난다. 첫째, 이동 노드가 현재 속해있는 네트워크에서 다른 네트워크로 이동할 때마다 홈 에이전트에 저장되어있는 COA를 변경해야 한다. 이 때문에 이동 노드는 홈 에이전트로 빈번하게 등록을 해야한다. 둘째, 이동 노드가 홈 네트워크에서 멀리 떨어질수록 홈 에이전트로 등록할 때 발생하는 핸드오프 지연 시간이 증가한다. 또한 핸드오프 지연시간 증가로 인하여 패킷 손실이 증가하고 처리율이 감소한다.

셋째, 이동 노드를 향해 전송한 IP 패킷이 최적 경로를 따르지 않고 홈 에이전트를 반드시 거쳐가므로 발생하는 삼각 라우팅 문제가 있다.



(그림 1) Mobile-IP 메커니즘



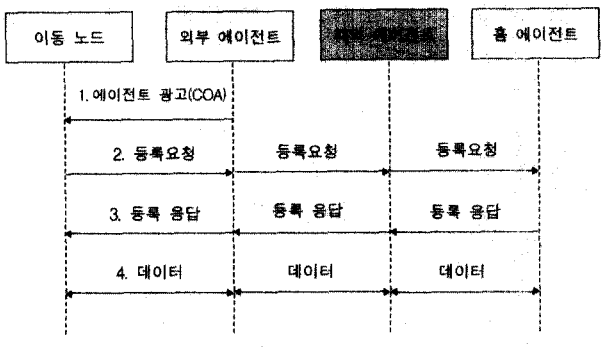
(그림 2) Mobile-IP의 지역 등록 메커니즘

Mobile IP 지역 등록 기법은 지역성을 높이기 위해서 이동 노드의 홈 에이전트와 현재 외부 에이전트 사이에 지역 에이전트를 위치시킴으로써 기존의 Mobile IP 확장하였다. 지역 에이전트(regional agent)는 지역 내에서 마치 이동 노드의 홈 에이전트처럼 동작한다. (그림 2)는 Mobile IP의 지역 등록 기법을 이용한 메커니즘을 나타낸다[3]. 이동 노드가 다른 셀로 이동할 때, 이동 노드의 지역 에이전트에 지역 등록을 통해 등록을 수행함으로써 홈 에이전트는 지역적 이동에 관여하지 않는다. 홈 등록은 네트워크 접속점에 관여하지 않으므로 최대 핸드오프 지연을 이동 노드와 홈 에이전트 거리에 관계없이 일정 수준으로 제한할 수 있다.

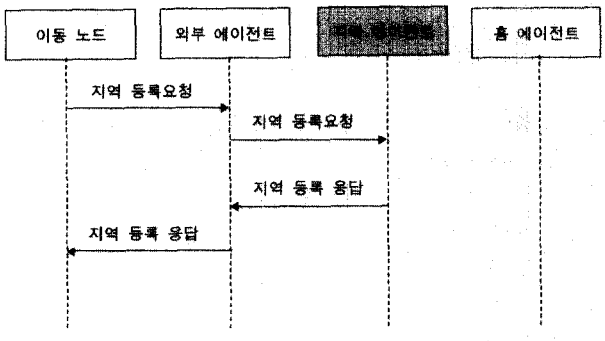
Mobile IP의 지역 등록 기법에서 홈 에이전트는 지역 에이전트를 통해서 COA를 등록한다. 외부 에이전트가 같은 지역에 있는 에이전트일 경우에는 변경되지 않으므로 홈 에이전트는 이동노드가 다른 도메인으로 움직일 때마다 새로운 정보를 요구하지 않는다.

- 홈 등록
  - 초기화를 위해 이동 노드가 홈 에이전트나 외부 에이전트에 지역 에이전트를 설정하거나 새로운 지역 에이전트를 설정할 때 수행한다.
  - 이동 노드 : 새로운 네트워크를 방문했을 때 지역 에이전트 광고 메시지를 통해 COA주소를 받는다. 이동노드는 등록요청 메시지를 생성하여 지역 에이전트 주소의 COA 필드에 넣어서 직접 전송한다.
  - 외부 에이전트 : 외부 에이전트는 등록요청 메시지를 받으면 이동노드에게 지역 에이전트를 할당한다.
  - 지역 에이전트 : 외부 에이전트로부터 받은 캡슐화된 COA주소를 재캡슐화시켜서 홈 에이전트로 전송한다.
- 지역 등록
  - 이동 노드가 지역 에이전트에 등록한 상태에서 이웃하는 셀로 이동할 경우 지역등록만 수행한다[3].

(그림 3)은 홈 등록 과정을 (그림 4)는 지역 등록 과정을 나타낸다.



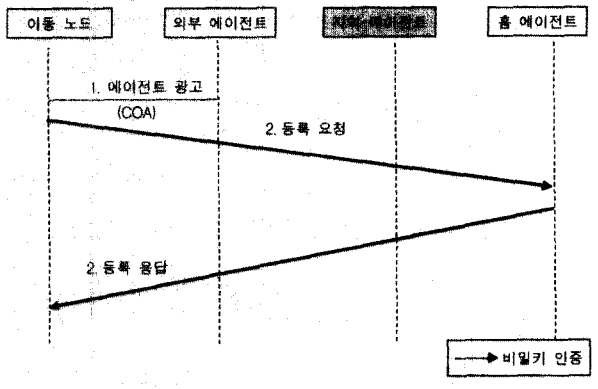
(그림 3) 홈 등록



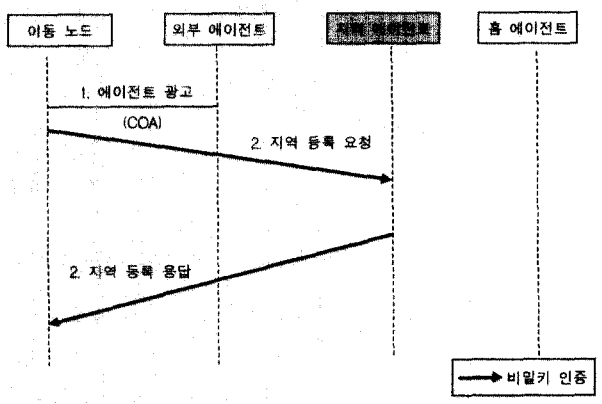
(그림 4) 지역 등록

3. 지역등록 기법을 이용한 인증 메커니즘

기존 Mobile IP의 등록 기법으로 인증 메커니즘을 수행할 경우에는 이동 노드를 홈 에이전트에 빈번하게 등록하게 됨으로써 소비되는 지연 시간이 문제점으로 나타난다. 이것은 Mobile IP 프로토콜을 보안 측면에서 살펴보았을 때, 빠른 인증과정 수행과 안전한 데이터 전송에 효율적이지 못하다. 따라서 본 논문에서는 지역 등록 기법을 이용하여 홈 등록과 지역등록으로 분리하여 인증 메커니즘을 수행하는 방법을 제안하고자 한다. 이 방법은 지역 등록 시에는 홈 에이전트의 역할을 지역 에이전트가 대신하는 것이다. 거리에 따른 제한을 두어 이동 노드가 새로운 네트워크로 들어가서 등록을 요구할 경우 셀의 형태가 마이크로 셀일 경우에는 지역 등록을 수행하여 지역 에이전트에서 인증을 수행하고 이동 노드가 매크로 셀에서 등록을 요구할 경우에는 홈 등록을 수행하여 홈 인증을 하는 방법이다. 이동 노드의 지역 등록 메시지를 처리하는 지역 에이전트는 기존의 Mobile IP에서 홈 에이전트 및 외부 에이전트와 기능이 유사하므로 별도의 시스템을 추가하는 것이 아니라 기존의 외부 에이전트나 홈 에이전트를 모두 지역 에이전트로 사용할 수 있다고 가정한다. 등록 정보를 인증하는데 사용하는 암호 메커니즘으로는 비밀키 기반 인증 메커니즘과 공개키 기반 인증 메커니즘 그리고 최소 공개키 기반 인증 메커니즘을 사용한다. 비밀키 기반 인증 메커니즘에서는 인증은 기본적으로 이동 노드와 홈 에이전트 둘 사이에서 이루어진다. (그림 5)를 보면 이동 노드는 등록 요청에 비밀키와 보호된 필드에 대한 MAC을 첨부시켜 홈 에이전트로부터 인증을 받고, 홈 에이전트도 등록 응답에 동일한 방법으로 이동 노드로부터 인증을 받는다.



(그림 5) 홈 등록 시 비밀키 기반 인증 메커니즘 동작

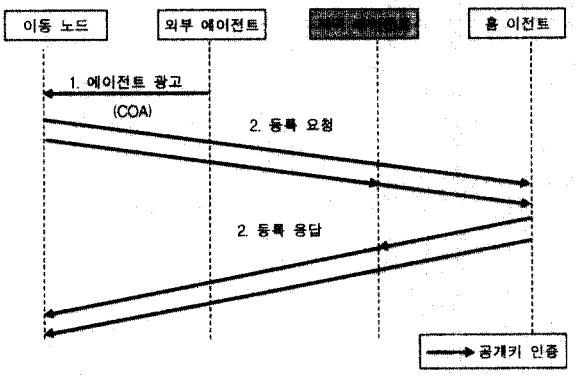


(그림 6) 지역 등록 시 비밀키 기반 인증 메커니즘 동작

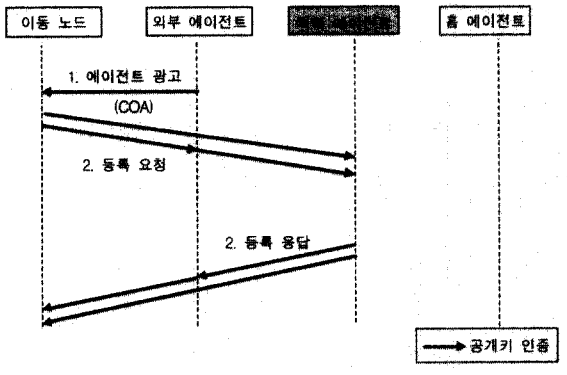
(그림 5)의 회색 화살표는 인증이 이루어지는 시점으로 여기서는 양쪽에서 비밀키 인증이 한 번씩 수행된다. (그림 5)는 홈 등록시 비밀키 기반 인증 메커니즘 동작 절차를 (그림 6)은 지역등록시 비밀키 기반 인증 메커니즘을 수행했을 경우 동작 절차를 나타낸다.

공개키 기반 인증 메커니즘은 세 참여자에 서로에 대한 인증을 메시지를 받고 전달할 때마다 수행한다. (그림 7)을 보면 이동 노드가 보내는 등록 요청에 보호된 필드에 대한 전자서명을 확장으로 덧붙이면 지역 에이전트와 홈 에이전트는 이것을 증명한다. 지역 에이전트도 받은 등록 요청과 등록 응답에 자신의 전자서명을 덧붙여 전달하면 홈 에이전트와 이동 노드는 각각 받을 때마다 증명한다. 홈 에이전트에 대한 인증도 마찬가지이다. 이러한 방법은 등록과정에 참여하는 세 참여자가 모두 서로에 대한 신뢰성 있는 인증을 할 수 있기 때문에 보안면에서 이상적이다.

(그림 7)은 홈 등록시 공개키 기반 인증 메커니즘을 수행했을 경우이고 (그림 8)은 지역등록시 공개키 기반 인증 메커니즘 동작 절차를 나타낸다.

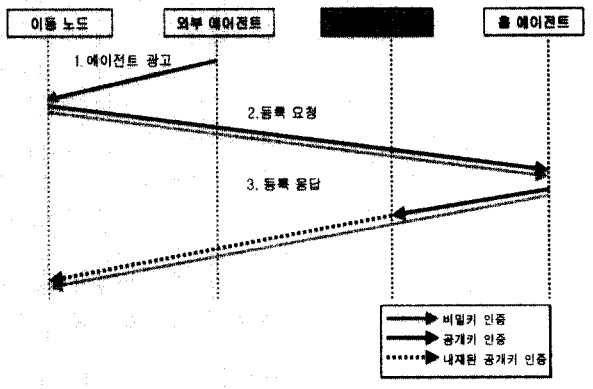


(그림 7) 홈 등록 시 공개키 기반 인증 메커니즘 동작

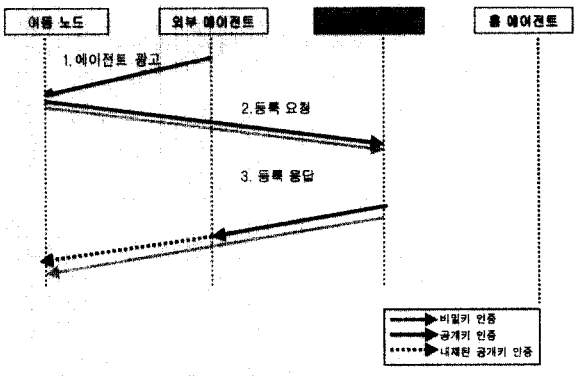


(그림 8) 지역 등록 시 공개키 기반 인증 메커니즘 동작

최소 공개키 기반 인증 메커니즘에서는 지역 에이전트가 이동 노드로부터 등록 요청을 받으면 인증 작업을 수행하지 않고 자신이 보냈던 에이전트 광고의 값이 유효한지만을 검사한다. 이동 노드가 외부 에이전트를 직접 인증하지 않고 홈 에이전트가 인증한 결과를 받음으로써 간접적으로 공개키 인증 효과를 가짐으로써 모든 인증 참여자에 대한 인증이 가능하다. (그림 9)는 홈 등록시 최소 공개키 기반 인증 메커니즘 동작 절차를 나타낸 것이고 (그림 10)은 지역등록시 최소 공개키 기반 인증 메커니즘을 수행했을 경우 동작 절차를 나타낸 것이다.



(그림 9) 홈 등록 시 최소 공개키 기반 인증 메커니즘 동작



(그림 10) 지역 등록 시 최소 공개키 기반 인증 메커니즘 동작

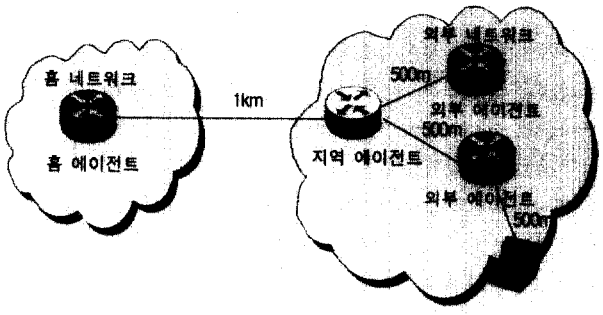
4. 성능 평가

시뮬레이션 도구로는 통신 시스템을 명세화하고 기술하며 SDL(Specification and Description Language)를 사용하였다[4, 5]. SDL은 통신 시스템의 동작을 기술해 주는 사용자와 개발자들의 공통언어로 사용되고 실시간 시스템의 구조, 동작 기능 및 데이터를 표시할 수 있으며 시스템 분석과 설계에 적용할 수 있다.

4.1 시뮬레이션 환경

시뮬레이션 환경은 다음과 같다. 물리적으로 망은 무선랜으로 IEEE 802.11을 따르고 시뮬레이션 망 구성은 (그림 11)과 같다[6].

이동 노드는 홈 네트워크에서 시작하여 홈 에이전트에 고정 IP 주소를 받고 외부 네트워크로 이동하여 외부 에이전트로부터 에이전트 광고를 통해 받은 새로운 COA를 받



(그림 11) 망 구성

아 홈 에이전트에 등록한다. Mobile IP는 매크로 셀에서 작동하기에 알맞으므로 서브 네트워크는 반경 500m로 하며 외부로 이동함에 따라 홈 네트워크와 외부 네트워크 사이의 거리는 1km에서 40km 까지 벌어진다. 새로운 서브 네트워크에 들어가 IP 주소가 바뀔 때마다 홈 에이전트에 새로운 위치 정보를 등록하고 데이터그램을 터널링받는다. 시뮬레이션에 사용된 고정 파라미터는 <표 1>과 같다.

〈표 1〉 시뮬레이션 고정 파라미터

거리	이동노드 : 기지국(무선 링크의 거리)	500m
	외부에이전트 : 지역에이전트(유선 링크의 거리)	500m
	지역에이전트 : 홈 에이전트(유선 링크의 거리)	1km~40km
지연 시간	무선 링크의 지연	7ms/km
	유선 링크의 지연	5ms/km
대역폭	무선 링크 대역폭	2Mbps
	유선 링크 대역폭	10Mbps

4.2 시뮬레이션 내용

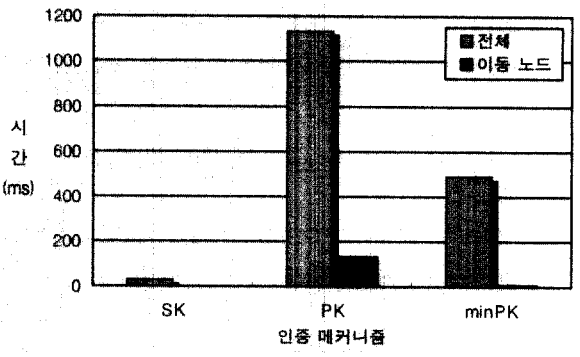
모델링은 이동 노드가 새로운 서브 네트워크로 들어가 에이전트 광고와 같은 특별한 메시지를 받았을 때 새 이동 정보를 홈 에이전트에게 등록하는 과정과 지역 에이전트에게 등록하는 과정에 해당한다[7]. 시뮬레이션은 기존의 등록 기법과 지역 등록 기법을 도입하였을 경우 각각에 대하여 앞서 기술한 세 가지 인증 메커니즘을 적용하여 수행한다. 비밀키 기반 인증 메커니즘(Secret-key Based Authentication)을 SK라고 하고 공개키 기반 인증 메커니즘(Public-key Based Authentication)을 PK라고 하고 최소 공개키 기반 인증 메커니즘(Minimal Public-key Based Authentication)은 minPK라고 표기한다. 기존 Mobile IP 등록 기법을 사용하였을 경우와 지역 등록 기법을 사용하였을 경우 각각에 대해 다음과 같은 측정치를 기준으로 비교하였다.

① 전체 등록 시간
② 이동 노드에서의 등록 시간
③ 노드 프로세스 시간
④ 암호화시간

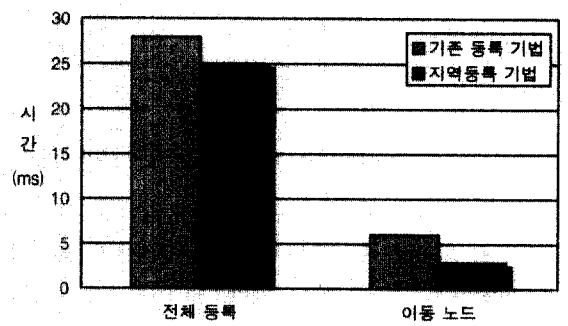
4.3 시뮬레이션 결과 및 분석

4.3.1 전체 등록시간과 이동 노드에서의 등록시간

전체 등록 시간이란 이동 노드가 속해 있던 네트워크를 벗어나서 새로운 네트워크로 들어갔을 때 외부 에이전트를 통해 홈 에이전트에 새로운 위치 정보를 등록시키는 실제 네트워크 계층에 걸리는 시간이다. 전체 등록 시간은 등록 요청 및 등록 응답을 만드는 시간, 각 이동 에이전트들이 자신이 가지고 있는 테이블을 갱신하는 시간을 포함한 노드 프로세스시간, MAC이나 전자 서명을 만드는데 필요한 암복호화 시간, 노드와 에이전트 사이에서 메시지가 전달되는데 걸리는 전달 지연의 세 가지로 구성된다.



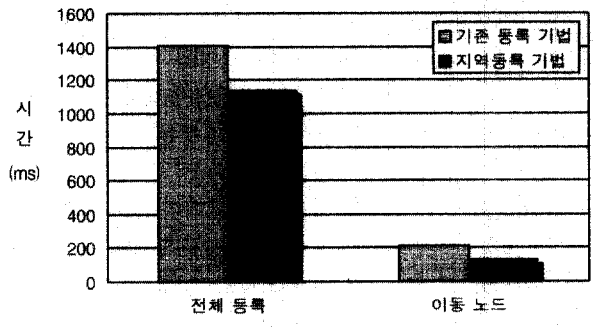
(그림 12) 전체 등록 시간



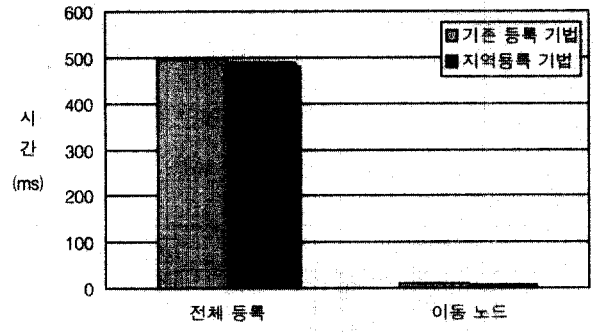
(그림 13) 전체 등록 시간 비교(비밀키 메커니즘)

(그림 12)는 기존의 등록 기법으로 인증 메커니즘을 수행했을 경우 각 인증 메커니즘 별 전체 인증 시간과 이동 노드에서의 인증 시간을 보여준다. 이동 노드에서의 등록시간은 전체 등록시간 중에서 이동 노드에서 수행된 시간만을 계산한 것이다. 이동 노드에서의 시간은 일반적으로 전력의 사용이 제한되어 있다는 점을 생각할 경우, 최소로 유지되어야 한다. 이동 노드에서 이루어지는 계산이 고정 노드에게 넘어갈 경우 고정 노드는 자원이 풍부하므로 더 빠르고 효율적으로 계산할 수 있고 자원이 부족한 이동 노드에게 전력 부담을 줄인다는 면에서 중요한 부분이 아닐 수 없다. (그림 13)과 (그림 14)는 이동 노드가 마이크로 셀로 등록 요청시 기존 Mobile IP의 등록 기법을 사용하여 인증하는 경우와 지역 에이전트를 사용하여 인증 할 경우에 각각 비

밀키 인증 메커니즘과 공개키 인증 메커니즘을 수행하였을 경우 등록 시간을 비교한 것이다. 지역 에이전트를 기법을 이용하여 인증을 할 경우에는 가까운 서브 네트워크로 이동 노드가 이동할 때 지역 에이전트를 통하여 인증 메커니즘을 수행하기 때문에 빈번하게 홈 에이전트로의 등록하는 시간을 줄여주었다.

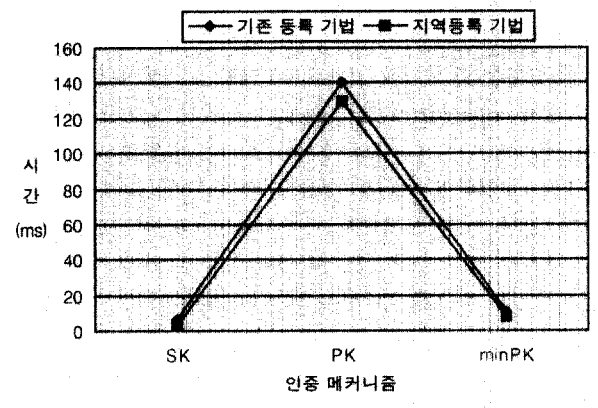


(그림 14) 전체 등록 시간 비교(공개키 메커니즘)



(그림 15) 전체 등록 시간 비교(최소 공개키 메커니즘)

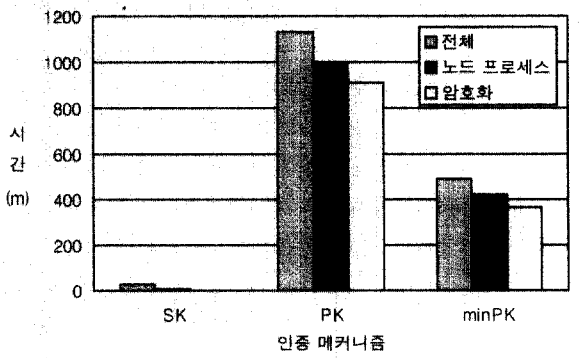
(그림 15)는 이동 노드가 새로운 마이크로 셀로 등록 요청 시 최소 공개키 인증 메커니즘을 수행하였을 경우 기존의 Mobile IP에서 사용하는 등록 기법을 사용하는 경우와 지역 에이전트를 사용하여 인증할 경우 등록 시간을 비교한 것이다.



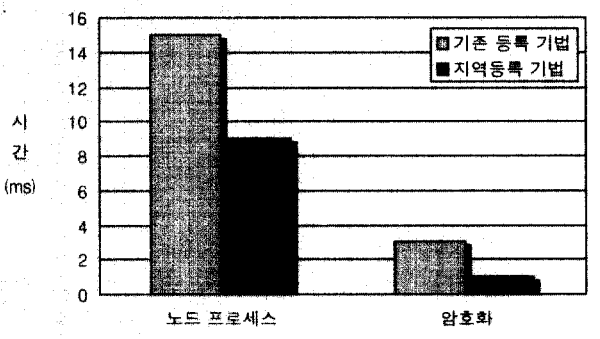
(그림 16) 인증 메커니즘별 지역등록 기법과 기존등록기법의 전체등록시간비교

(그림 16)은 이동 노드가 마이크로 셀로 등록 요청시 지역등록 기법을 사용하였을 경우와 기존의 등록 기법을 사용하였을 경우 각 인증 메커니즘 별 수행시간을 비교하여 보여준다. 이와 같이 이동 노드가 새로운 지역 에이전트를 설정하는 것이 아닌 가까운 외부 에이전트로 이동을 할 경우에는 홈 에이전트에게 광고 메시지를 보내지 않고 지역 에이전트에게 등록 요청을 하여 등록을 수행하는 인증 메커니즘을 사용하는 것이 더 효율적이다.

4.3.2 전체 등록시간, 노드프로세스시간 및 암호화 시간



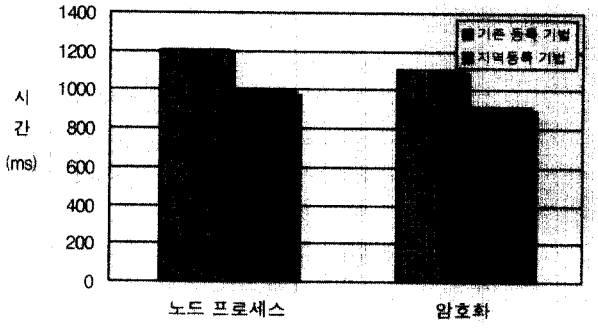
(그림 17) 전체 등록 시간, 노드 프로세스 시간, 암호화 시간



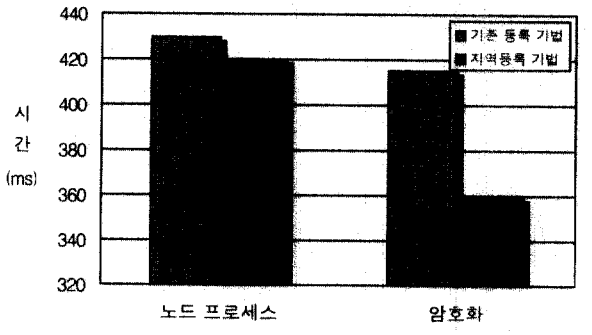
(그림 18) 노드프로세스 시간과 암호화 시간(비밀키 메커니즘)

(그림 17)은 기존의 인증 메커니즘에서 인증 메커니즘별 전체 인증 시간, 노드 프로세스 시간, 암호화 시간을 보인 것이다. SK에서는 대부분의 등록시간은 노드와 에이전트 사이의 전달 지연시간으로 기인한다. 비밀키를 이용한 암·복호화 시간은 매우 적다. 그러나 PK에 오면 공개키를 이용한 암·복호화를 하는 시간이 SK에 비하여 늘어나서 공개키 과정의 비용이 높다는 것을 알 수 있다. 공개키의 과정이 복잡할 뿐 아니라 PK에서는 암·복호화 과정이 여러번 일어나기 때문이다. 공개키 이용이 늘어날수록 전체 등록시간에서 차지하는 암·복호화 과정이 차지하는 비중이 증가한다.

(그림 18), (그림 19), (그림 20)는 비밀키 인증 메커니즘과 공개키 인증 메커니즘 그리고 최소 공개키 인증 메커니즘을 기존의 등록 방법과 지역 등록 방법에 적용했을 경우 나타나는 노드 프로세스와 암호화 시간을 비교하여 보인 것이다.



(그림 19) 노드 프로세스 시간, 암호화 시간(공개키 메커니즘)



(그림 20) 노드 프로세스 시간, 암호화 시간(최소 공개키 메커니즘)

시뮬레이션 결과를 종합해보면 앞에서 분석한 것과 같이 기존의 Mobile IP의 등록 기법으로 인증 메커니즘을 수행할 경우에는 이동 노드와 홈 에이전트와의 빈번한 등록 과정으로 인해 소비되는 지연 시간이 문제점으로 나타난다. 이것은 빠른 인증과정 수행과 안전한 데이터 전송을 중요시하는 Mobile IP 메커니즘에 효율적이지 못하다.

따라서 본 논문 제안한 인증 메커니즘인 홈 등록과 지역 등록으로 나누어서 인증 메커니즘을 수행하는 방법이 더 효율적임을 시뮬레이션을 통하여 입증하였다. 이 방법은 지역 등록 시에는 홈 에이전트의 역할을 지역 에이전트가 대신하는 것으로 거리에 따른 구분을 두어 이동 노드가 새로운 네트워크로 들어가서 등록을 요구할 경우 셀의 형태가 마이크로 셀일 경우에는 지역등록을 수행하여 지역 에이전트에서 인증을 수행하고 이동 노드가 매크로 셀에서 등록을 요구할 경우에는 홈 등록을 수행하여 홈 인증을 하게 하는 것이다.

4. 결 론

본 논문에서는 Mobile IP에서 제공하는 기존 등록 기법으로 인증 메커니즘을 수행할 경우 이동 노드와 홈 에이전트와의 빈번한 등록 과정으로 인해 소비되는 시간 지연으로 빠른 인증 과정 수행과 안전한 데이터 전송을 중요시하는 Mobile IP 메커니즘에 효율적이지 못하다. 이 문제점을 해결하기 위하여 지역등록 기법을 이용한 인증 메커니즘을 제시하였다. 거리에 따른 제한을 두어 이동 노드가 새로운 네트워크로 들어가서 등록을 요구할 경우 셀의 형태가 마이크로 셀일 경우에는 지역등록을 수행하여 지역 에이전트에서 인증을 수행하고 이동 노드가 매크로 셀에서 등록을 요구할 경우에는 홈 등록을 수행하여 홈 인증을 하는 방법이다. 제안한 지역 등록 방법에 대하여 비밀키 인증 메커니즘과 공개키 인증 메커니즘 그리고 최소 공개키 인증 메커니즘의 경우로 시뮬레이션의 성능을 평가하였다. 그 결과, 전체적으로 보았을때 지역등록 기법을 사용하여 인증 메커니즘을 수행하였을 경우 기존의 Mobile IP 등록 기법보다 더 효율적이라는 것을 입증하였다. 또한 기존의 등록 기법은 이동 노드가 외부 에이전트를 통해 홈 에이전트에 등록하는 경우 공중망(public network)을 지나게 되므로 외부 악의의 공격자로부터 쉽게 공격당할 수 있으나 지역 등록 기법을 이용하게 되면 네트워크 도메인 내에서 등록이 이루어지므로 보안의 측면에서 조금 더 안전한 전송이 이루어질 수 있다.

본 논문에서는 지역 등록 기법을 이용하여 효율적인 인증 메커니즘을 수행하는 것만 살펴보았으나 지역 에이전트를 더 확장시켜서 인증뿐만 아니라 다른 보안 기법을 적용시킬 수 있을 것이다.

참 고 문 헌

[1] Charles E. Perkins, "Mobile IP," IEEE Communication Magazine, pp.88-99, May, 1997.

[2] C. Perkins, "IP Mobility Support," RFC2002, http://www.ietf.org/rfc/rfc2002.txt, 1996.

[3] Eva Gustafsson, Annika Jonsson, Charles E. Perkins, "Mobile IPv4 Regional Registration," http://search.ietf.org/internet-drafts/draft-ietf-mobileip-reg-tunnel-06.txt, Mar., 2002.

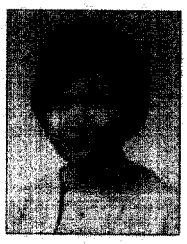
[4] Rolv Break, "SDL Basic," Computer Networks and ISDN System 28, 1996.

[5] SDT Getting Started, "Chapter 1. Introduction to Languages and Notations," SDL 매뉴얼.

[6] William Stallings, Data and Computer Communications, Sixth Edtion, Prentice Hall, 2000.

[7] Vipul Gupta, Abhijit Dixit, "The Design and Development of a Mobility Supporting Network," ISPAN96, 1996.

[8] 한국정보보호센터, 정보보호개론, 교우사, 2000.



장 성 은

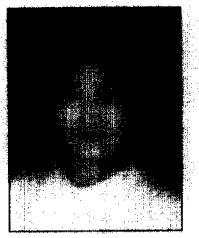
e-mail : sejang@secuve.com

1999년 한신대 수학과 졸업(학사)

2002년 이화여대 과학기술대학원 컴퓨터학과 졸업(석사)

2002년~현재 (주)시큐브

관심분야 : Mobile IP, Secure OS, IDS, IPS, ESM 등



박 정 민

e-mail : pjm@amadeus.kist.re.kr

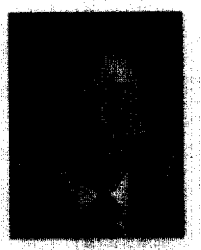
1989년 이화여자대학교 전자계산학과 졸업 (학사)

1991년 이화여자대학교 대학원 전자계산학과 졸업(이학석사)

1999년~현재 이화여자대학교 과학기술대학원 컴퓨터학과 박사과정

1991년~현재 한국과학기술연구원 연구원

관심분야 : Network Security, Mobile IP, Active Network Security, Ad-hoc Network 등



채 기 준

e-mail : kjchae@ewha.ac.kr

1982년 연세대학교 수학과 이학사

1984년 미국 시라큐즈대학교 컴퓨터학과 석사

1990년 미국 노스캐롤라이나 주립대학교 컴퓨터공학과 박사

1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수

1992년~현재 이화여자대학교 컴퓨터학과 교수

관심분야 : 네트워크 보안, 액티브 네트워크 보안 및 관리, 인터넷/무선통신망/고속통신망 프로토콜 설계 및 성능 분석