Mobile IP 및 AAA 프로토콜 기반으로 신속성과 안전성을 고려한 듀얼세션키 핸드오프 방식연구☆

Secure Handoff Based on Dual Session Keys in Mobile IP with AAA

최 유 미* 이 형 민** 추 현 승***
Yumi Choi Hyung-Min Lee Hyunseung Choo

요 약

이동 단말기의 활용이 급증하고 그 성능이 주목할 만한 수준으로 발전하면서 Mobile IP의 사용이 증가되고, 또한 보안성 강화를 목적으로 하는 이동 노드의 인증방식 연구와 데이터의 보안·전송 연구가 이루어지고 있다. 현재 이동 무선 네트워크 IP를 위한 이동성 자원의 표준인 Mobile IP는 이동 노드의 접속에 관해서 효율적인 사용자 인증이 취약하다. 즉, Mobile IP는 이동성을 보장하지만 보안성을 지원하지 않는다. 본 논문에서는 네트워크 구성원들의 상호 인증 및 보안 서비스를 위해서 인증(Authentication), 권한부여(Authorization) 및 과금(Accounting)을 지원하는 AAA 프로토콜에 기반하여 Mobile IP의 보안성을 유지하고 빠른 핸드오프를 수행하는 새로운 보안 핸드오프 방식을 제안한다. 제안된 방식은 AAA 프로토콜을 동작하는 세션 키 목록을 리스트로 유지하는 방법으로 AAAH 서버(Home AAA Server)에서 MN을 인증하는데 필요한 기존의 세션 키와 새로운 세션 키를 리스트로 유지함으로써 재인증 받는 문제점을 해결하고자 한다. 이로써, 이동 노드의 보안성을 유지하면서 핸드오프 수행시간을 충분히 보장한다. 분석적 모델링결과에 의하면 제안하는 방식은 기본적인 Mobile IP와 AAA 프로토콜의 결합방식과 비교하여 핸드오프 시간을 고려하는 핸드오프 실패율에 있어서 60%정도의 성능향상을 보인다.

Abstract

The Mobile IP has evolved from providing mobility support for portable computers to support wireless handheld devices with high mobility patterns. The Mobile IP secures mobility, but does not guarantee security. In this paper, the Mobile IP has been adapted to allow AAA protocol that supports authentication, authorization and accounting for authentication and collection of accounting information of network usage by mobile nodes. For this goal, we propose a new security handoff mechanism to intensify the Mobile IP security and to achieve fast handoff. In the proposed mechanism, we provide enough handoff achievement time to maintain the security of mobile nodes. According to the analysis of modeling result, the proposed mechanism compared the basic Mobile IP along with AAA protocol is up to about 60% better in terms of normalized surcharge for the handoff failure rate that considers handoff time.

☞ Keyword : Mobile IP, Handoff, AAA, and Security

1. 서 론

최근 몇 년간 인터넷 사용의 수는 급속히 증가하였다. 특히 이동하기 쉬운 PDA(Personal Digital Assistance)와 노트북 등과 같은 이동 컴퓨팅 장비들이 급증하고 그 성능이 주목할 만한 수준으로 발전하면서 재택근무를 지원하는 사람이 증가하여 무선 인터넷 사용자가 폭발적으로 증가하였다. 이러한 기술 발전과 작업환경의 변화는 호텔, 공항 그리고 가상 사무실에서 전자우편이나 웹을 안전하고 신뢰성 있게 사용할 수 있도록 요구하게 되었다. 따라서 단순히 통신을 제공하는 것에서 그치는 것이 아니라 불법적으로 서비스를 사용하는 것을 방지해야 하고 가입자의 권한 레벨을 부여하

* 정 회 원 : (주)벨웨이브 SW그룹 연구원
yumi@ece.skku.ac.kr(제 1저자)
** 정 회 원 : 두양상선(주) 전산실장, 동서울대학 겸임교수
hmlee@dooyang.co.kr(공동저자)
*** 정 회 원 : 성균관대학교 정보통신공학부 부교수
choo@ece.skku.ac.kr(책임저자)
☆ 본 연구는 BK21과 정보통신부의 지원을 받았습니다.
[2004/03/16 투고 - 2004/12/03 심사 - 2005/04/20 심사 완료]

고 검증해야 하며, 과금 및 자원 계획을 수립하기 위해 네트워크 사용에 대한 측정이 요구되었다. 더욱이 매우 빠른 증가세를 보이고 있는 로밍 가입자와 이동 가입자를 수용하기 위해 가입자의 사용 횟수, 사용량, 과금 정보를 유지해야 한다. 이에 따라 무선 단말기를 통한 전자상거래가 대중화되고, 무선 환경에서의 인증방안 연구가 전 세계적으로 진행되고 있다. 그러나 이동성이 있는 단말기의 보안을 유지하는 것은 그리 쉬운 문제가 아니다.

현재 이동 무선 네트워크 IP를 위한 이동성 자원의 표준은 Mobile IP[1]로서 인터넷상에서 단말기가 다른 부분 망으로 이동하더라도 단말기에 대한 IP 주소의 재설정 없이도 연속적으로 패킷을 교환할 수 있는 프로토콜이다. 그러나 Mobile IP는 이동 노드(Mobile Node,MN)의 접속에 관해서 효율적인 사용자 인증과 같은 보안에 취약하다는 문제점을 갖고 있다. 즉, Mobile IP는 이동성을 보장하지만 보안성은 지원하지 않는다. 본 논문에서는 네트워크 구성원들의 상호 인증하고 신뢰 관계를 유지하기 위해, 사용자 인증 및 보안서비스를 위해서 인증(Authentication), 권한부여(Authorization) 및 과금(Accounting)을 지원하는 AAA 프로토콜[2,3]을 기반하여 Mobile IP의 보안성을 유지하면서 빠른 핸드오프를 하고자 한다.

기존에 Mobile IP와 AAA 프로토콜이 결합하여 동작하는 방식에 관해서 진행되어 왔다. 특히 Mobile IP와 AAA 프로토콜이 결합시 생기는 지연시간을 감소시키는 연구가 활발하다. 현재 연구 방법에는 Mobile IP와 AAA 프로토콜을 결합하여 MN에 관하여 인증을 받고 서비스 요청 시에 메시지를 전송할 때 필요한 암호화와 복호화 과정에 소요되는 시간을 감소시킨 티켓 기반 방법[4]이 제시되었다. 또 다른 연구 방법으로는 MN이 외부 네트워크로 이동할 때마다 홈 네트워크에 있는 AAA 서버로부터 새로운 세션 키를 생성하여 MN의 CoA 등록 시 발생하는 지연 시간을 줄이기 위해 세션 키를 재사용하되, 제3자를 두어 재사용되는 세션 키를 인증해주는 방법[5]에 관해 연구가 이루어졌다.

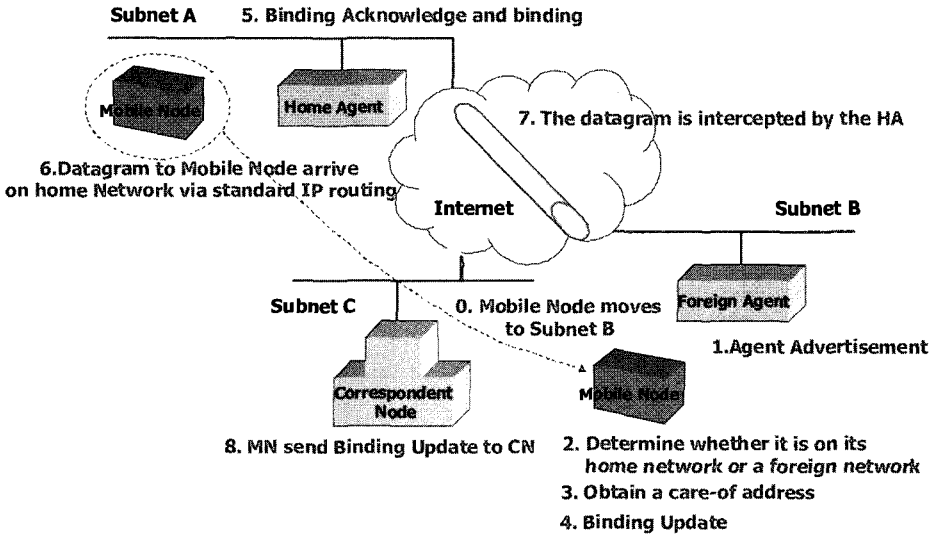
본 논문에서는 MN에 대한 인증을 받는 부분에 관해서 안전성을 강화하는 동시에 미리 인증을 받음으로써 자연스럽게 신속한 핸드오프를 하고자 한다. 즉, Mobile IP의 핸드오프 실패율을 감소시키며 보안을 유지하도록 MN이 에이전트로부터 광고 메시지를 받은 순간부터 핸드오프를 시작하여 빠른 핸드오프를 하고자한다[6]. 본 논문에서 제안하는 방법은 AAA 프로토콜을 동작하는 세션 키 목록을 리스트로 유지하는 방법으로 AAAH 서버(Home AAA Server)에서 MN을 인증하는데 필요한 기존의 세션 키와 새로운 세션 키를 리스트로 유지함으로써 재인증 받는 문제점을 해결하고자 한다. 또한 제안된 방법의 경우 MN이 핸드오프를 준비할 수 있는 시간이 상대적으로 길어져 MN을 인증 할 수 있는 시간이 충분해진다. MN의 보안성을 유지하면서 핸드오프를 수행시간을 충분히 보장한다. 분석적 모델링결과에 의하면 제안하는 방식은 기본적인 Mobile IP와 AAA 프로토콜의 결합방식과 비교하여 핸드오프 시간을 고려하는 핸드오프 실패율에 있어서 60%정도의 성능향상을 보인다.

본 논문은 다음과 같이 구성된다. 제 2장에서는 Mobile IP, AAA 프로토콜에 대한 기본적인 개념, 제 3장에서는 핸드오프의 지연 시간을 단축시키기 위한 방법을 제안하고, 제 4장에서는 이에 대한 성능 평가를 실시한다. 마지막으로 제 5장에서는 결론으로 끝을 맺는다.

2. 관련연구

2.1 Mobile IPv6

Mobile IP는 IETF(Internet Engineering Task Force)에서 표준화한 프로토콜로 IP를 사용하는 노드가 이동함에 따라 자신의 접속점이 변경되더라도 지속적인 통신이 가능하도록 하는 기법이다.



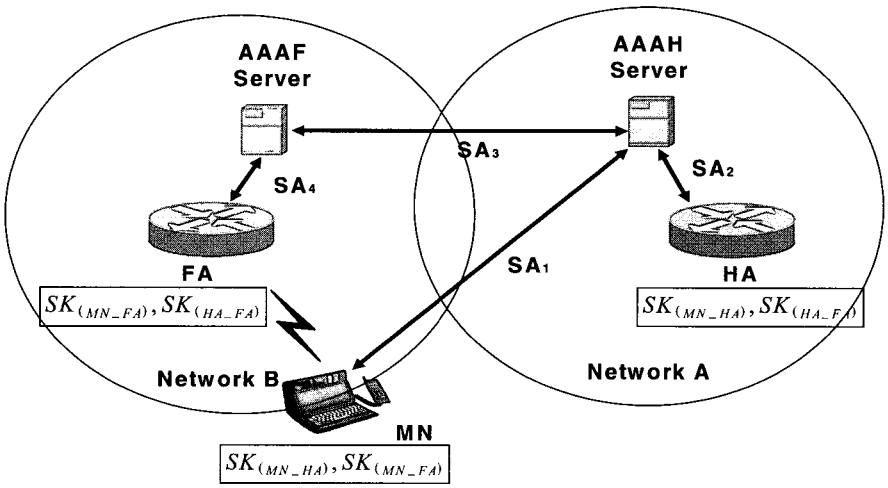
〈그림 1〉 Mobile IP 동작 과정

이를 통해 MN이 네트워크 주소를 바꾸며 이동하여도 자신의 고유 IP 주소를 그대로 사용할 수 있다[7].

Mobile IP 동작 방식은 홈 에이전트(Home Agent, HA) 와 외부 에이전트(Foreign Agent, FA)가 MN의 이동을 확인하기 위해 지속적으로 방송메시지를 보낸다. MN은 이 방송을 통하여 자신이 홈 네트워크에 있는지 외부 네트워크에 있는지 판단할 수 있다. 만약 MN이 외부 네트워크에 있다면 FA를 통해서 CoA(Care of Address)를 얻게 된다. 다음은 Registration request/reply 과정으로 MN의 CoA를 HA에 등록하는 것이다. 등록이란 MN이 자신의 현재 위치를 HA에게 알리는 것으로 이 때 자신의 위치를 대변하는 주소를 CoA라고 한다. 초기 등록 시에 MN은 Mobile IPv4와 같이 CoA를 얻은 후에 FA를 통해 HA로 등록 요청 메시지를 보내게 되며 HA는 MN의 등록 메시지를 받아 MN의 홈 주소 및 CoA 값의 바인딩 정보를 바인딩 테이블에 저장하고 등록 응답 메시지를 보내 MN에게 등록 사실을 알린다. HA에게 CoA가 한 번 등록 된 후에 MN은 CoA 주소를 HA 및 자신이 통신하고 있든 모든 상대노드(Corresponding Node, CN)에게 BU 메시지(Binding Update Message)를 이용하여 알린다. HA는 그 BU 메시지에 대한 응답으로 BA 메시지(Binding Acknowledge Message)를 전송하고 바인딩 정보를 유지한다. CN은 바인딩 정보를 저장하고 다음부터는 그 바인딩 정보를 사용하여 HA를 거치지 않고 통신함으로써 triangular routing 문제를 안정적으로 해결한다[8]. 위의 그림 1은 MN이 Subnet A(홈 네트워크)에 있다가 Subnet B(외부 네트워크)로 이동할 때의 Mobile IP 동작 과정을 보인다.

2.2 AAA protocol(Authentication Authorization and Accounting) with Mobile IP

AAA 프로토콜은 IETF내에 AAA 작업 그룹에서 보안을 위해 제정한다. 최근에 AAA 프로토콜은 MN에 관한 인증을 필요로 하는 Mobile IP를 부양하기 위해 채택되었다. 여기서 AAA는 인증(Authentication), 권한부여(Authorization), 과금(Accounting)의 기능을 제공한다[9-11]. 인증(Authentication)은 망 접근을 허용하기 전에 사용자의 신원을 검증하는 것이며, 권한부여(Author



〈그림 2〉 Mobile IP에서 AAA 프로토콜 SA 관계[14]

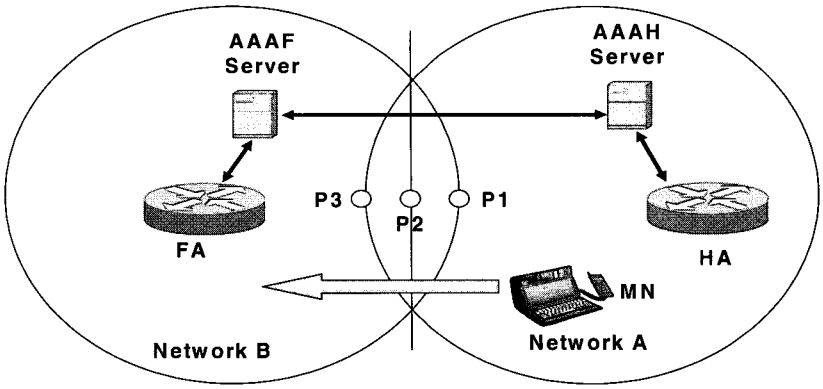
ization)는 망사용이 허락된 사용자에 대해 어떤 권한과 서비스를 허용할 것인지를 정한다. 마지막으로 과금(Accounting)은 사용자의 자원 사용에 관한 정보를 모으는 방법을 제공한다. 그리고 이 정보는 사용요금, 회계 그리고 용량 증설에 사용된다.

AAA 프로토콜 기본 방법은 MN이 핸드오프 이후에 홈 도메인에 위치했던 MN이라는 것을 확인 하기위해 인증서를 보내어 인증하는 것이다. 즉, MN이 홈 도메인에서 외부 도메인으로 이동한 후에 이동한 MN이 홈 도메인에 있었던 MN이라는 것을 증명하기 위해 AAAF 서버(Foreign AAA Server)를 통해 AAAH 서버에게 인증서를 보냄으로써 인증을 받는다. AAA 프로토콜의 동작 과정을 살펴보면 MN이 외부 도메인 지역으로 이동시 자신의 신분을 확인하기 위해 인증서를 AAAF 서버에게 보낸다. AAAF 서버에서는 MN에 관한 정보를 가지고 있지 않으므로 홈 도메인에 있는 AAAH 서버에게 메시지를 전송한다. 그러면 AAAH 서버에서는 MN의 인증서를 받고 인증을 한 후 세션 키를 생성하여 HA에게 CoA 값과 세션 키를 보낸다. HA는 CoA 값을 등록하고 세션 키를 저장한 후 회신 메시지를 보낸다. AAAH 서버는 HA로부터 회신 메시지를 받고 세션 키를 FA와 MN에게 전달함으로써 보안관계를 확립한다[12,13].

AAA 프로토콜은 그림 2와 같이 보안 관계를 맺고 있다. MN은 AAAH 서버와 상호 보안 관계(SA1)를 설립한다. 홈 도메인에서는 AAAH 서버와 HA의 사이에 보안 관계(SA2)를 맺고 있으며, 외부 도메인에서는 AAAH 서버와 AAAF 서버가 보안 관계(SA3)를 맺는다. 그리고 외부 도메인에서는 FA와 AAAF 서버가 보안 관계(SA4)를 정의한다[15,16].

3. 제안하는 방식

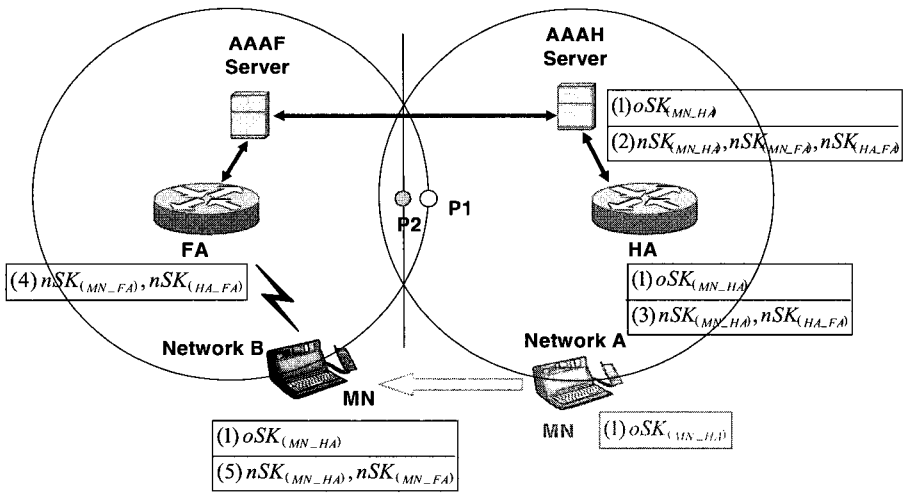
그림 3에서 MN이 Network A에서 Network B로 이동하는 경우를 생각해보자. 일반적인 AAA 프로토콜에서의 Mobile IP 동작은 MN이 P2를 지나면서 Network A와 Network B의 FA로부터 신호 세기를 검사한다. MN이 P2를 지나게 되면 Network B의 신호가 더 세게 되며, 이때 핸드오프를 시작하여 MN의 인증절차를 밟는다. 이러한 핸드오프 방식은 MN이 핸드오프를 수행하면서 인증 할 수 있는 시간이 P2에서 P3을 지나는 시간이다.



〈그림 3〉 MN의 이동에 의한 핸드오프

만약 시간 내에 핸드오프를 완료하지 못하면 핸드오프의 실패로 인해 통화의 단절이나 패킷의 손실이 발생한다. 또한 핸드오프 실패로 MN을 인증하지 못한다. 사용자의 증가로 인해 셀의 크기는 점점 작아지고 있다. 셀의 크기가 작아짐에 따라서 MN의 핸드오프 수는 증가하게 되며, 또한 P2와 P3의 거리는 점점 작아지고 있다. 따라서 MN을 인증하면서 핸드오프를 완료해야 하는 시간도 그 만큼 줄어들고 있으며, 핸드오프 실패 확률은 증가한다. 또한 MN이 외부 도메인으로 이동하는 경우 망의 경계 지역에서는 두 망사이의 신호의 세기가 명확하게 차이가 나지 않아 어느 네트워크로 등록할지 모호한 경우가 발생한다. 이 경우 MN의 핸드오프 메시지는 계속 증가하게 되며, 두 네트워크의 FA 모두 상당한 양의 작업을 처리해야 한다. 이런 일련의 과정은 FA와 네트워크에게 과중한 오버헤드를 발생하여, 핸드오프 시에 실패할 확률은 높아지고, 비효율적인 처리가 발생한다.

본 논문에서는 AAA 프로토콜로 Mobile IP 보안을 유지하면서 핸드오프의 실패율을 감소하기 위해 Dual Session Keys (DSK) 방법을 제안한



〈그림 4〉 Dual Session Keys (DSK) 방법

다. 즉, AAA에서 Mobile IP의 보안성을 위해 MN이 P1 지점에 도착할 때 핸드오프를 시작한다. 따라서 MN의 보안성을 유지하기 위해 충분한 핸드오프 시간을 유지한다. 그래서 핸드오프 실패율이 감소한다.

그림 4에서 MN이 Network A에서 Network B로 이동하는 경우를 생각해보자.

단계 1: MN이 P1에 도달하는 경우 Network B의 FA로부터 최초로 광고 메시지를 받는다. 광고 메시지에는 MN 이 Network B로 이동시에 사용할 새로운 CoA 값을 포함한다.

단계 2: 광고 메시지를 받자마자 MN은 핸드오프를 준비하여 시작하고, 인증을 요청한다.

단계 3: MN은 새로운 CoA 값과 $oSK_{(MN-HA)}$로 암호화 된 인증 정보를 AAAF 서버를 통해 AAAH 서버에게 보낸다.

단계 4: AAAH 서버는 이미 존재하는 $oSK_{(MN-HA)}$로 MN에 관하여 인증한다.
(그림 4 (1) 참조)

단계 5: 그리고 새로운 세션 키 $nSK_{(MN-HA)}$, $nSK_{(MN-FA)}$, $nSK_{(HA-FA)}$를 생성한다.

여기서 'o'는 기존 세션 키를 의미하고 'n'은 새로운 세션 키를 의미한다. 일반적으로 AAA 서버는 새로운 세션 키를 생성하면 기존의 세션 키를 대체하여 새로운 세션 키로 써 넣게 된다. 이전의 방법과는 달리 제안된 DSK 방법은 동시에 새로운 세션 키와 기존 의 세션 키를 유지한다.

단계 6: AAAH 서버는 HA에 해당하는 세션 키($nSK_{(MN-HA)}$, $nSK_{(HA-FA)}$)를 포함하여 등 록 요청 메시지를 보낸다.

단계 7: HA는 CoA 값을 등록한 후에 그림 4에서 보이는 것처럼 세션 키($nSK_{(MN-HA)}$, $nSK_{(HA-FA)}$)를 유지한다.

단계 8: 그리고 회신 메시지를 AAAH 서버에게 보낸다.

단계 9: AAAH 서버는 HA로부터 회신 메시지를 받은 후 FA($nSK_{(MN-FA)}$, $nSK_{(HA-FA)}$)와 MN($nSK_{(MN-HA)}$, $nSK_{(MN-FA)}$)에게 각각 AAAF 서버를 거쳐 세션 키를 전달한다.

동시에 기존의 세션 키와 새로운 세션 키를 유지함으로써 양쪽의 네트워크 간에 보안 관계가 확립된다.

여기에서 AAAH 서버가 인증정보를 받고 세션 키를 분배해야 할 시점에 기존의 세션 키와 새로운 세션 키를 유지하면서 새로운 세션 키에 대해서 분배하지 않는다. MN이 HA에 연결하다가 신호의 세기에 따라 새로운 지역 Network B의 신호 세기가 더 강해질 때 MN이 HA에게 이동을 알려 AAAH 서버로 메시지를 보낸다. 메시지를 받았을 때 AAAH 서버는 새로운 세션 키를 분배한다. 서버와 에이전트들은 새로운 세션 키를 받아 기존의 세션 키와 함께 저장한다. DSK 방법을 적용함으로써 MN이 Network A에 있는 P1지점에서 핸드오프를 시작하여 P2지역까지 이동하다가 다시 Network A지역으로 이동하여도 AAAH 서버에서는 기존의 세션 키 값을 가지고 있으므로 기존의 세션 키로 사용할 수 있어 다시 보안관계를 확립해야 하는 오버헤드가 없어지게 된다. 또한 MN이 외부 도메인으로 이동하는 경우 망의 경계 지역에서는 두 망사이의 신호의 세기가 명확하게 차이가 나지 않아 어느 네트워크로 등록할지 모호한 경우가 발생한다. 따라서 기존의 세션 키와 새로운 세션 키를 동시에 유지하는 DSK 방식은 신호의 세기에 따라 각 Network에 맞는 세션 키를 사용함으로써 오버헤드를 줄인다. MN은 광고메시지를 통하여 네트워크를 인식함으로써 알맞은 세션 키를 선택한다. 기존의 Mobile IP와 AAA 프로토콜을 결합하여 동작하는 방식과 비교하여 볼 때, 핸드오프를 미리 시작함으로써 핸드오프가 빨라지고 실패율이 감소하여 보안측면에서 안정적이다.

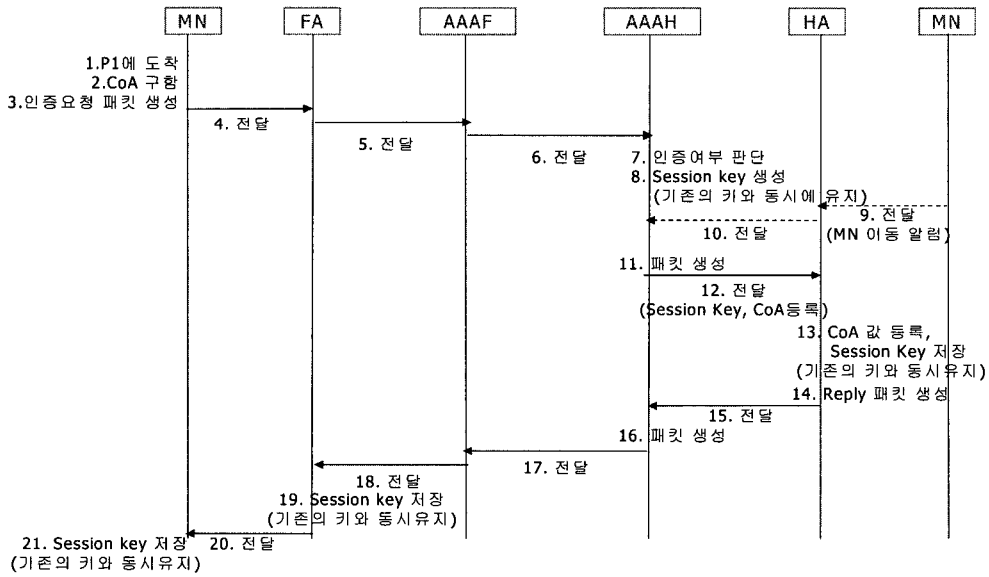
4. 성능평가

4.1 분석적 모델링

그림 5와 같이 데이터 전송 흐름에 따라 메시지를 보내고 처리하는 총 시간을 구하기 위해 분석적 모델링을 한다. 즉, 각 단계별로 핸드오프 동작시 필요한 프로세싱 시간, 메시지를 유·무선으로 처리하여 보내는 시간, MN을 인증하는데 필요한 시간을 통하여 총 핸드오프의 시간을 구한다. 본 모델링의 궁극적인 목표는 총 핸드오프 시간을 고려하여 핸드오프 실패율을 구하는 것이다.

각 단계의 메시지를 보내는 시간 (M_i)은 전송시간(transmission time), 전달시간(propagation time), 처리 시간(processing time)의 합으로 $M_i=\alpha_i+\beta_i+\gamma_i$와 같이 계산한다[17]. 여기서 i는 각 단계를 나타낸다. 전송시간 α_i는 제어 비트로 된 제어 신호를 링크 환경의 메시지 전송률로 나눈 값으로$\alpha_i=\frac{b}{B}$와 같이 표현된다. b는 제어 메시지이며 고정된 크기로 가정한다. B의 경우 유선인 경우에는 B^L 변수를, 무선인 경우에는 B^W를 사용한다.

전달시간 β_i는 전달 매체에 따라서 고정된 값을 갖으며, B^L과 B^W는 유·무선 상의 값을 각각 나타낸다. γ_i는 처리 시간으로 각 에이전트와 AAA 서버 등에서 동일한 값으로 간주한다. 메시지가 전달되는 환경이 유선망인 경우는 매우 안정적이므로 메시지가 손실될 확률이 극히 적으나 무선 환경에서 메시지를 전달하는 경우에는 언제든지 중간에 손실될 수 있다. 따라서 물리적인 전송시간(T_i)을 $M_i(=M_i^L)$로 표현한다. 유선의 경우와 무선을 구분하기 위해 각각의 메시지 전달 시간을 M^L과 M^W로 구분한다. 무선 환경에서 메시지를 전달하며 메시지가 중간에 손실된 경우에는 MN이 이를 판단하여 재전송한다. 따라서 무선 환경에서는 링크 실패 횟수 N_f와 그에 따른 링크 실패율을 고려해야 한다. 링크 실패율을 고려한 메시지 처리 시간을 T_i로 정의하면 유선 상에서는 $T_i=M^L$로 표현되며, 무선 상에서는$T_i=\sum_{N_f=0}^{\infty}(\tilde{T}_i(N_f)\times \Pr ob(N_f$번 실패 후 성공하는 경우)$)$이다. t_W는 메시지가 손실되었음을 인식하는 시간으로 무선 환경에서 요청 신호를 보낸 후 t_W시간 동안 이에 대한 응답



〈그림 5〉 DSK 방식의 데이터 전송 메커니즘

을 받지 못하는 경우 MN은 메시지가 손실되었다고 판단하고 이를 재전송한다. 링크 실패가 N_f번 일어난 경우 이를 재전송하기 위해서는 t_W와 메시지 송신이 N_f번 발생한다. 따라서 $\widetilde{T}_i(N_f)$는 $(N_f+1)M^W+(N_f)t_w = M^W+N_f(t_w+M^W)$과 같이 유도된다. 따라서 재전송을 고려한 메시지 처리시간은 다음과 같다.

$$T_i = \sum_{N_f=0}^{\infty}(M^W+N_f(t_w+M^W)) \times \mathrm{Prob}(N_f\text{번실패후성공하는경우}) = M^W+(t_w+M^W)\times\sum_{N_f=0}^{\infty}N_f \times Porb(N_f\text{번실패하는경우})$$

여기서 $\sum_{N_f=0}^{\infty}(N_f\times\mathrm{Prob}(N_f\text{번실패후성공하는경우}))$는 무한급수로 평균 실패 횟수를 유도할 수 있다. 일반적으로 한 링크의 전송 실패 확률을 q라 한다면 기하분포 랜덤 변수의 기대 값을 $\frac{q}{1-q}$로 표현한다. 여기서 q의 경우 0.5를 일반적으로 가정한다. 그래서 T_i는 $M^W+(t_w+M^W)\times\frac{0.5}{0.5}=2M^W+t_w$와 같이 간단하게 나타낸다. 본 논문에서는 메시지를 생성하는 시간, 에이전트가 메시지를 인식하는 시간과 그에 따른 처리시간을 P로 간주한다.

총 핸드오프 시간을 구하기 위해서 핸드오프 동작 시 필요한 프로세싱 시간, 메시지를 유·무선으로 전달하는 시간과 MN을 인증하는데 필요한 시간의 합으로 표현한다. 각 변수의 값은 [17-20]에 의해 정의된다. 그림 5는 메시지 흐름의 표현을 도식화 하였다. 그림 5에서 보여주고 있는 스킴을 기반으로 총 핸드오프 시간을 구한다.

Ⅰ. 프로세싱 시간의 총 합

프로세싱 시간이 필요한 경우는 2, 3, 11, 13, 14, 16, 19, 21 단계이다. 각 단계 i (P_i)의 프로세싱 시간은 고정된 성능 파라미터 값을 갖는다. 그래서 총 프로세싱 시간은 다음과 같다.

$$P^*_{total} = 8P$$

Ⅱ. 유선상에서 메시지 전송 시간의 합

유선 상에서 메시지가 전송되는 경우는 5, 6, 9, 10, 12, 15, 17, 18 단계이다. 이 경우 메시지가 전송되는데 걸리는 시간의 총 합을 구하면

$$L^*_{total} = L(5)+L(6)\times C_h+L(9)+L(10)+L(12)+L(15)+L(17)\times C_h+L(18)$$

여기서 C_h는 홉 수를 의미하고 $L(i)$는 유선상에서 각 단계 i에서 전송시간을 의미한다. 각각의 $L(i)$ 값은 M^L로 고정된 값으로 표현하면 다음과 같다.

$$L^*_{total} = 2M^L\times C_h+6M^L$$

Ⅲ. 무선상에서 메시지 전송 시간의 합

무선 상에서 메시지를 전송하는 경우는 2, 4, 20 단계이다. 이 경우 메시지 총 전송시간의 합은 $W^*_{total}=3W_i$이다. 여기서 W_i는 무선 상에서 각 단계 i에서의 전송 시간을 의미하며 무선에서의 링크 실패율을 고려하여 표현하면 다음과 같다.

$$W^*_{total} = 3(2M^W+t_w)$$

Ⅳ. 인증하는데 걸리는 시간의 합

인증하는데 걸리는 시간 AU시스템 값으로 7, 8 단계에서 이루어진다. 그래서 총 인증시간은 다음과 같다.

$$AU^{*}_{total} = 2AU$$

따라서 핸드오프를 완료하는데 걸리는 시간의 총합은 다음과 같다.

$$T_{req} = P^{*}_{total} + L^{*}_{total} + W^{*}_{total} + AU^{*}_{total}$$
$$= 8P + 2(3 + C_h) \times M^{L} + (2M^{W} + t_w) \times 3 + 2AU$$

〈표 1〉 성능 파라미터

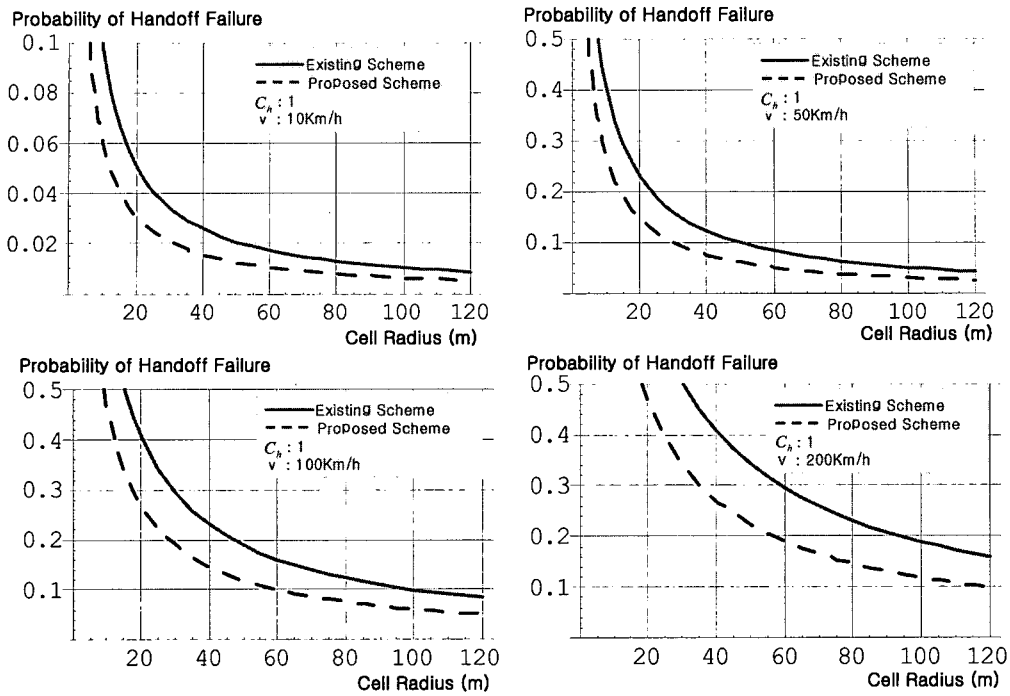
변수	정의	값
P	프로세싱 시간	0.5 msec
B^{L}	유선에서의 전송률	155 Mbps
B^{W}	무선에서의 전송률	144 Mbps
b	제어 메시지 길이	50 byte
β^{L}	유선에서의 메시지 전달시간	0.5 msec
β^{W}	무선에서의 메시지 전달시간	2 msec
t_w	메시지 응답 판단 시간	2 msec
γ	메시지 처리 시간	0.5 msec
AU	인증 시간	6 msec

T는 중복된 경계 지역에서의 MN이 머무르는 시간이며 핸드오프를 완료하는데 요구되는 시간은 T_{req}이다. 그래서 T_{req}시간 전에 MN이 중복된 경계 지역에서 떠나는 확률($\tilde{P}$)은 $P = prob(T < T_{req})$이다. 두 셀의 중복된 경계 지역에서 MN이 머무르는 시간 T가 지수 분포를 따른다고 가정한다. 이때 핸드오프 실패율의 임계 값을 P_f로 놓으면 핸드오프 실패율은 $P = prob(T < T_{req}) = 1 - \exp(-\lambda \times T_{req}) < P_f$이다. 여기서 λ의 값은 MN이 중복된 경계 지역의 도착율을 의미하며 MN이 움직일 수 있는 방향은 $[0,2\pi)$에서 동일한 분포이다. 따라서 λ는 $\lambda = \frac{V \times L}{\pi \times S}$[21]와 같은 값을 갖는다. V의 경우 MN이 움직이는 속도를 의미하는데, 시스템에서 주어진 값에 따라 변하게 된다. L의 경우는 반지름이 l인 원에서 $L = \frac{1}{6} \times 2\pi l \times 2 = \frac{2}{3}\pi l$와 같이 계산 된다. 중복된 지역의 영역 값인 S는 $(\frac{1}{6}\pi l^2 - \frac{\sqrt{3}}{4} l^2) \times 2$ 와 같다. λ의 값은 L과 S 값을 대입하여 $\lambda = \frac{4V}{2l\pi - 3\sqrt{3}\,l}$와 같이 정리된다. 따라서 총 핸드오프 시간 T_{req}값과 λ값을 가지고 우리가 원하는 핸드오프 실패율의 값을 구한다.

4.2 결과 분석 및 비교

본 절에서는 지금까지 유도한 식을 이용하여 기본적인 Mobile IP와 AAA 프로토콜의 결합방식과 본 논문에서 제안하는 DSK 방식을 적용한 Mobile IP와 AAA 프로토콜 결합방식에 관해서 비교한다. 즉, 핸드오프 실패율에 관해서 제안하는 DSK 방식과 기본적인 Mobile IP와 AAA 프로토콜 결합방식에 관하여 비교한다. 제안하는 DSK 방식은 미리 핸드오프를 시작함으로써 핸드오프 준비 하는 시간이 기존의 핸드오프 방법보다 수행할 수 있는 시간이 상대적으로 길어져 핸드오프 실패율이 감소된다.

그림 6은 사용자가 4km/h의 속도로 움직인다고 가정하고, 속도를 변화시키면서 핸드오프 실패율을 측정한다. MN의 이동 속도인 V의 값이 증가하게 되면 핸드오프를 완료해야 하는 시간이 짧아진다. 만일 MN이 일정한 속도 이상으로 움직이게 되면 핸드오프를 완료하는데 필요한 시간을 얻지 못해서 핸드오프 실패가 발생한다. 이에 따라 기존 핸드오프 방법은 지연시간이 증가하게 되어 따라서 핸드오프 실패율이 증가한다. 반지름이 20m를 기준으로 속도의 값이 변함에 따라 기존핸드오프 방식의 실패율은 각각 5.10%, 23.02%, 40.75%, 64.89%의 값을 갖는다. 이에 비해, 본 논문에서 제안하고 있는 방식의 경우 3.10%, 14.58%, 27.04%, 46.76%의 값을 갖는다. 기존 방식과 제안하는 방식과의 차이는 각각 2%, 8.44%, 13.71%, 18.13%로 속도가 증가할수록 점점 더 좋은 성능을 보임으로써 제안하는 방식이 기본적인 Mobile



〈그림 6〉 기존의 방식과 DSK 방식 비교-1

IP와 AAA 프로토콜의 결합방식과 비교하여 성능 향상을 보인다.

더욱이 기본적인 Mobile IP와 AAA 프로토콜 의결합방식보다 제안한 방식이 실패율에 있어서 성능이 우월하다는 것을 보이기 위해 함수 δ를 다음과 같이 정의한다.

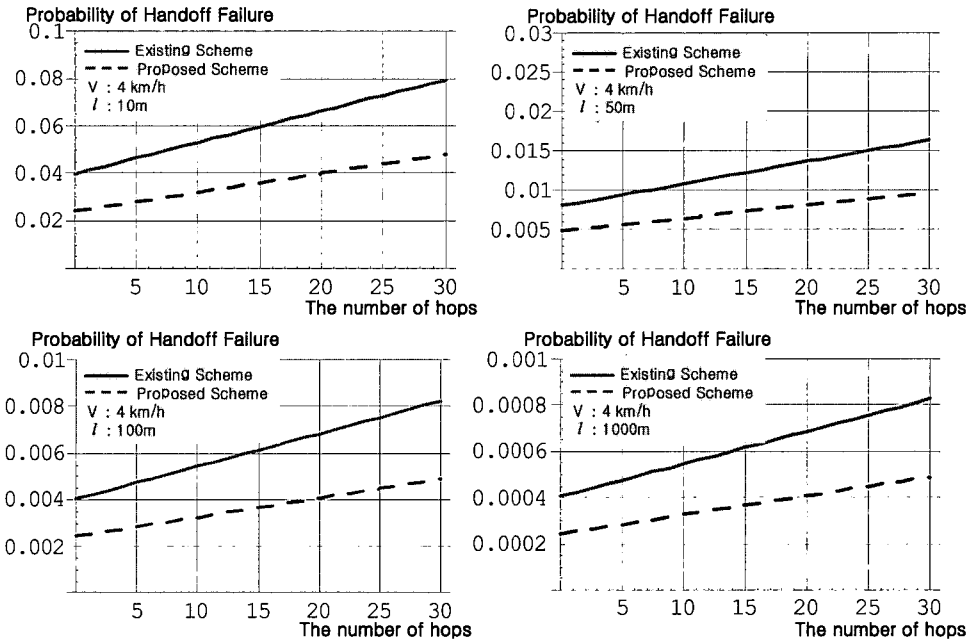
$$\delta = \frac{\widetilde{P_{\exists ing}} - \widetilde{P_{proposed}}}{\widetilde{P_{proposed}}} \times 100\ (\%)$$

제안된 DSK 방식이 기본적인 Mobile IP와 AAA 프로토콜의 결합방식보다 핸드오프 실패율에 있어서 항상 우수하다는 것을 보인다. 즉, 기본적인 Mobile IP와 AAA 프로토콜의 결합방식과 비교하여 핸드오프 시간을 고려하는 핸드오프 실패율에 있어서 60%정도의 성능향상을 보인다.

그림 7에서는 V를 4km/h라 가정하고, l의 값을 변화 시키면서 핸드오프 실패율을 측정한다. l의 길이가 작으면 핸드오프가 빨리 이루어져야 하므로 핸드오프 실패율이 증가한다. 그림 7에서 홉수 10을 기준으로 l의 길이의 변함에 따라 기존 핸드오프 방식의 실패율은 각각 5.30%, 1.08%, 0.54%, 0.054%의 값을 갖는다. 이에 비해, 본 논문에서 제안하는 방식은3.20%, 0.64%, 0.32%, 0.032%의 값을 갖는다. 기존 방식과 제안하는 방식의 차이는 각각 2.1%, 0.44%, 0.22%, 0.024%로 l의 길이가 클수록 핸드오프 실패율이 낮다. 즉, l의 길이가 작으면 핸드오프 실패율이 높고, l의 길이가 크면 핸드오프 실패율이 낮음으로써, 사용자의 증가로 셀의 크기가 작아지는 점에서 제안하는 방식이 기존 방식에 비해 효율적이며 성능이 우수하다.

5. 결 론

이동 컴퓨팅 단말기의 급속한 증가로 인해 Mo



〈그림 7〉 DSK 방식과 기존 방식 비교-2

bile IP에서 보안을 유지하는 문제는 점점 중요해지고 있다. 본 논문에서는 Mobile IP의 보안을 위하여 AAA 프로토콜을 결합하여 신속한 핸드오프를 하면서, 보안을 유지하기 위해 DSK 방식을 제안하였다. 제안된 DSK 방식은 AAA에서 기존의 세션 키와 새로운 세션 키를 유지하는 방식이다. 또한 MN이 외부 도메인에서 광고메시지를 처음으로 받자마자 핸드오프를 시작하는 방식이다. 제안된 방식에서는 MN을 안전성을 유지하기 위해 충분한 핸드오프 시간을 제공한다. 그래서 MN을 인증하면서 핸드오프를 수행하는 영역이 기존의 방식 보다 넓어짐으로 보다 안정적이다. 기본적인 Mobile IP와 AAA 프로토콜의 결합방식과 비교하여 핸드오프 시간을 고려하는 핸드오프 실패율에 있어서 60%정도의 성능향상을 보인다.

참 고 문 헌

[1] C.E. Perkins, "IP Mobility Support," IETF RFC 2002

[2] IETF Authentication, Authorization, and Accounting(AAA) Working Group, http://wwww.itef.ofg/html/charters/aaa-charter.html

[3] S. Farrell, J. Vollbrecht, P. Calhoun, and L. Gommans, "AAA Authorization Requirements," RFC 2906, Aug. 2000.

[4] J. Park, E. Bae, H. Pyeon, and K. Chae "A Ticket-based AAA Security Mechanism in Mobile IPNetwork," ICCSA 2003, vol. 2668, pp.210-219, May 2003.

[5] H. Kim, D. Choi, and D. Kim, "Secure Session Key Exchange for Mobile IP Low Latency Handoffs," Springer-Verlag Lecture Notes in Computer Science, vol. 2668, pp.230-238, Jan. 2003.

[6] D. Choi, H. Choo, "Partial Dual Unicasting Based Handoff for Real-Time Traffic

in MIPv6 Networks," Springer-Verlag Lecture Notes in Computer Science, vol. 2660, pp.443~452, June. 2003.

[7] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. debruijn, C.de Laat, M. Holdrege. D. Spence, "AAA Authorization Application Examples", IETF RFC 2905

[8] B. David, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF draft, Internet Draft draft-ietf-mobileip-ipv6-17. txt, May 2002.

[9] Hasan, J. Jahnert, S. Zander, B. Stiller, "Authentication, Authorization, Accounting and Charging for the Mobile Internet," Mobile Summit, Sep. 2001.

[10] J. Vollbrecht, P. Cahoun, S. Farrell, and L. Gommans, "AAA Authorization Application Examples," RFC 2104, Feb. 1997.

[11] J. Vollbrecht, P. Cahoun, S. Farrell, and L. Gommans, "AAA Authorization Framework," RFC 2904, 2000

[12] S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements," RFC 2977, 2000

[13] M. Laurent-Maknavicius, F. Dupont, "Inter-domain security for Mobile IPv6," ECUMN 2002, pp.238~245, Apr. 2002.

[14] C. Perkins, "Mobile IP Joins Forces with AAA,"IEEE Personal Communications, vol.7, no.4, pp.59~61, Aug. 2000

[15] Tewari, H, O'Mahony, D., "Real-Time Payments for Mobile IP," IEEE, 2003

[16] C. Yang, M. Hwang, J. Li, and T. Chang, "A Solution to Mobile IP Registration for AAA," Springer-Verlag Lecture Notes in Computer Science, vol.2524, pp.329~337, Nov. 2002.

[17] J. McNair, I.F. Akyildiz, and M.D Bender, "An inter-system handoff technique for the IMT-2000 system," INFOCOM 2000, vol.1, pp.203~216, Mar. 2000.

[18] Hess, G. Schafer, "Performance Evaluation of AAA/Mobile IP Authentication," 2nd Polish-German Teletraffic, 2002.

[19] J. McNair, I.F Akyildiz. and M.D Bender, "Handoffs for real-time traffic in mobile IP version 6 networks," GLOBECOM '01.IEEE, vol.6, pp.3463~3467, Nov. 2001.

[20] Jiang Xie, and I.F. Akyildiz, "An optima location management scheme for inimizing signaling cost in mobile IP,"Communications, 2002. ICC 2002. IEEE International Conference on, vol.5, pp. 3313~3317, Apr. 2002

[21] R. Thomas, H. Gilbert, and G. Mazziotto, "Influence of the mobbing of the mobile stations on the performance of a radio mobile cellular network," in Proceedings of the 3rd Nordic Seminar, pp.1-9, Sep. 1998.

[22] R. Caceres and V. N. Padmanabhan, "Fast and scalable handoffs for wireless internetworks," in Proc. ACMMOBICOM96, pp. 56 - 66, 1996.

[23] Pat R. Calhoun: Diameter Base Protocol. draft-ietf-aaa-diameter-17.txt, 2002.

[24] Cappiello, M. Floris, A. Veltri, L., "Mobility amongst Heterogeneous Networks with AAA Support," Communications, 2002. ICC 2002. IEEE International Conference on, Volume: 4,28 pp. 2064 -2069, May 2002.

[25] F. Dupont, M. Laurent-Maknavicius, J. Bournelle, "AAA for mobile IPv6", Internet drfaft-dupont-mipv6,aaa-01.txt, Nov. 2001.

[26] Pat R. Calhoun, Tony Johansson, Charles E. Perkins: Diameter Mobile IPv4 Application. draft-ietf-aaa-diameter- mobileip-13.txt, 2002.

◐ 저 자 소 개 ◑

최 유 미 (Yumi Choi)
2003년 서울여자대학교 컴퓨터공학과 졸업(공학사)
2005년 성균관대학교 일반대학원, 컴퓨터공학과 졸업(공학석사)
2005년~현재 (주)벨웨이브 SW그룹 연구원
관심분야 : Mobile Computing, Security
E-mail : yumi@ece.skku.ac.kr

이 형 민 (Hyung-Min Lee)
1991년 성균관대학교 수학과 졸업(학사)
1994년 성균관대학교 정보처리(석사)
2003년 성균관대학교 정보통신공학부 박사 수료
1990년~현재 두양상선주식회사 전산실장
1998년~ 현재 동서울대학 겸임교수
관심분야 : Mobile Communication, Mobile IP, IPV6
E-mail : hmlee@dooyang.co.kr

추 현 승 (Hyunseung Choo)
1988년 성균관대학교 수학과 졸업(학사)
1990년 University of Texas at Dallas, 컴퓨터공학과 졸업(석사)
1996년 University of Texas at Arlington, 컴퓨터공학과 졸업(박사)
1997년 특허청 심사관(사무관)
1998~현재 성균관대학교 정보통신공학부 부교수
관심분야 : 광네트워크, 이동컴퓨팅, 라우팅 프로토콜, 그리드 컴퓨팅
E-mail : choo@ece.skku.ac.kr