AAA MIP 환경에서 공유영역 기반 세션키 재사용을 통한 고속 핸드오프 방식연구

최 유 미[†] · 정 민 영[††] · 추 현 승[†††]

요 약

현재 무선 네트워크 IP를 위한 이동성 자원의 표준인 Mobile IP는 이동 노드(Mobile Node, MN)의 접속에 관한 사용자 인증이 비효율적이다. 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. AAA 프로토콜은 QoS를 제한하는 비효율적인 인증 절차가 존재하여 MN이 핸드오프를 수행할 때마다 새로운 세션 키를 분배 받아야 한다. 본 논문에서는 MN이 핸드오프를 수행할 때 발생하는 지연 시간과 MN의 인증으로 인한 AAA 서버의 오버헤드를 줄이고자 공유(Overlap, 오버랩) 네트워크 구조 기반의 세션키 재사용 방법을 제안한다. 본 방식에서는 MN의 보안성 향상을 위하여 공유 세션 키를 유선상에서 전달하는 방식에 기반하고, 그에 따라 신속하고 자연스러운 핸드오프 메커니즘을 제공한다. 분석적 모델링결과에 의하면 제안하는 방식은 기존 세션 키 재사용 방식과 비교하여 핸드오프 시간을 고려하는 핸드오프 실패율에 있어서 40%정도의 성능향상을 보인다.

키워드 : Mobile IP, AAA Protocol, Security

Boundary Zone Overlapping Scheme for Fast Handoff Based on Session Key Reuse

Yumi Choi[†] · Min Young Chung[††] · Hyunseung Choo[†††]

ABSTRACT

The Mobile IP provides an efficient and scalable mechanism for host mobility within the Internet. However, the mobility implies higher security risks than static operations in fixed networks. In this paper, the Mobile IP has been adapted to allow AAA protocol that supports authentication, authorization, and accounting(AAA) for security and collection for accounting information of network usage by mobile nodes(MNs). For this goal, we propose the boundary zone overlapped network structure while solidifying the security for the authentication of an MN. That is, the proposed scheme delivers the session keys at the wired link for MN's security instead of the wireless one, so that it provides a fast and seamless handoff mechanism. According to the analysis of modeling result, the proposed mechanism compared to the existing session key reuse method is up to about 40% better in terms of normalized surcharge for the handoff failure rate that considers handoff total time.

Key Words : Mobile IP, AAA Protocol, Security

1. 서 론

최근 무선랜 망의 급속한 진화에 따라 인터넷 사용자가 증가하고 있으며 이동 환경에서의 무선 인터넷 접속과 망간 연동 등이 이슈화 되고 있다. 특히 이동하기 쉬운 PDA (Personal Digital Assistance)와 노트북 등과 같은 이동 컴퓨팅 장비들이 급증하고 그 성능이 주목할 만한 수준으로 발전하면서 무선 인터넷 사용자가 폭발적으로 증가하였다. 이러한 기술 발전은 많은 어플리케이션들에게 실시간으로 무선 연결을 통해서 정보를 전달하게 하였다. 알려진 바와 같이 무선 연결은 유선 연결보다 보안에 취약하기 때문에 무선 상에서의 전송 데이터 보안이 중요한 문제로 인식되었다. 따라서 단순히 통신을 제공하는 것에서 그치는 것이 아니라 불법적인 서비스 사용을 방지하고, 가입자의 권한 레벨을 부여 및 검증하며, 과금 및 자원 계획을 수립하기 위해 네트워크 사용평가가 요구되었다. 더욱이 매우 빠른 증가세를 보이고 있는 로밍 가입자와 이동 가입자를 수용하기 위해 가입자의 사용 빈도, 사용량, 과금 정보를 유지해야 한

† 준 회 원 : (주)벨웨이브 SW그룹
†† 종신회원 : 성균관대학교 정보통신공학부 조교수
††† 종신회원 : 성균관대학교 정보통신공학부 부교수
논문접수 : 2004년 12월 7일, 심사완료 : 2005년 4월 11일

다. 이에 따라 무선 단말기를 통한 전자상거래가 대중화되고, 이를 위한 무선 환경에서의 인증방안 연구가 이 분야에서 활발히 진행되고 있다.

현재 이동 무선 네트워크 IP를 위한 이동성 자원의 표준은 사실상 Mobile IP[1]로서 위치를 이동하여 인터넷 접속점을 변경하는 MN이 인터넷상의 다른 노드들과의 통신을 계속할 수 있도록 지원하는 프로토콜이다. 그러나 Mobile IP는 MN의 접속에 관해서 효율적인 사용자 인증과 같은 보안면에서 취약하다는 문제점을 갖고 있다. 즉, Mobile IP는 이동성을 보장하지만 보안성은 지원하지 않는다. 저자들은 네트워크 구성원들의 상호 인증과 신뢰 관계를 유지하기 위하여 인증, 권한부여 및 과금을 지원하는 AAA 프로토콜[2, 3]의 자원으로 보안성이 강화된 Mobile IP에 근거하여 신속한 핸드오프 방식을 제안한다.

기존에 Mobile IP와 AAA 프로토콜이 결합하여 동작하는 방식에 관한 연구가 진행되어 왔고[4, 5], 특히 결합시 발생하는 지연시간을 감소시키기 위한 연구가 활발하다. 최근 연구에서는 MN이 외부 네트워크로 이동할 때 올바른 MN임을 확인하기 위해 홈 네트워크에 있는 AAA 서버로부터 새로운 세션 키를 발급받는 오버헤드와 지연시간을 줄이기 위해 세션 키를 재사용하되, 제3자를 두어 세션 키를 안전하게 사용하는 방법[4]이 제시되었다. 또 다른 방법으로 MN에 관하여 인증을 받고 서비스 요청 시에 메시지 전송에 필요한 암호화와 복호화 과정에 소요되는 지연시간을 감소시킨 티켓 기반 방식[5]이 있다.

본 논문에서는 MN에 대한 인증을 받는 부분에 관해서 보안성을 강화하는 동시에 영역 오버랩 구조를 제안함으로서 구조적으로 안전하고 신속한 핸드오프 방식을 제안하고자 한다. 즉, Mobile IP의 핸드오프 실패율을 감소시키며 MN을 인증하는 과정에서 세션 키를 재사용하여 빠른 핸드오프를 유도한다. 본 방식은 세션 키를 무선 상에서 전달하여 보안성이 취약하게 되는 문제점을 유선 상에서 세션 키를 전달함으로서 해결하고자 한다. 분석적 모델링[6]결과에 의하면 제안하는 방식은 기존 세션키 재사용 방식과 비교하여 핸드오프 시간을 고려하는 핸드오프 실패율에 있어서 40%정도의 성능향상을 보인다.

본 논문은 다음과 같이 구성된다. 제 2장에서는 기본적인 AAA 프로토콜 기반 Mobile IP 결합 방식과 이전의 관련연구들을 정리하고, 제 3장에서는 핸드오프의 지연시간 단축 및 보안성 강화를 위한 방법을 제안하며, 제 4장에서는 이에 대한 성능 평가를 실시한다. 마지막으로 제 5장에서는 본 논문을 결론 맺고 앞으로의 연구 방향을 논의한다.

2. 관련 연구

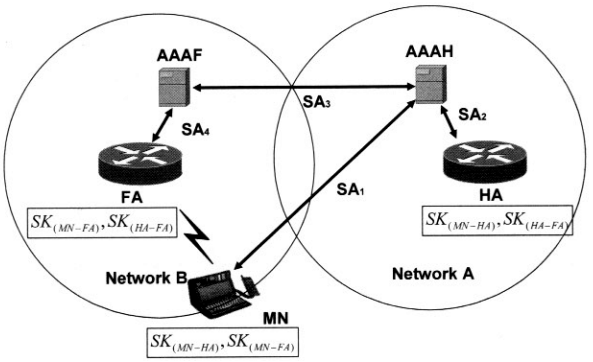
2.1 AAA 프로토콜 기반 Mobile IP

Mobile IP는 IETF(Internet Engineering Task Force)에서 표준화한 프로토콜로 IP를 사용하는 노드가 이동함에 따라 자신의 접속점이 변경되더라도 지속적인 통신이 가능하도록 하는 기법이다. Mobile IPv6는 MN, 홈 에이전트(Home Agent, HA) 와 상대 노드(Correspondent Node, CN)로 동작이 이루어진다. 단말이 외부 네트워크로 이동시에 사용되는 CoA(Care of Address)를 얻기 위해서는 자동으로 주소를 부여 받거나 스스로 주소를 생성하여 주소를 획득한다. MN은 CoA를 통하여 자신이 홈 네트워크에 있는지 외부 네트워크에 있는지 판단할 수 있다. MN이 CoA를 획득하면 이를 HA에 등록한다. 등록이란 MN이 자신의 현재 위치를 HA에게 알리는 것이며 이 때 자신의 위치를 대변하는 주소를 CoA라고 한다. 초기 등록 시에 MN은 Mobile IPv4에서와 같이 CoA를 얻은 후에 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 CN에게 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[7].

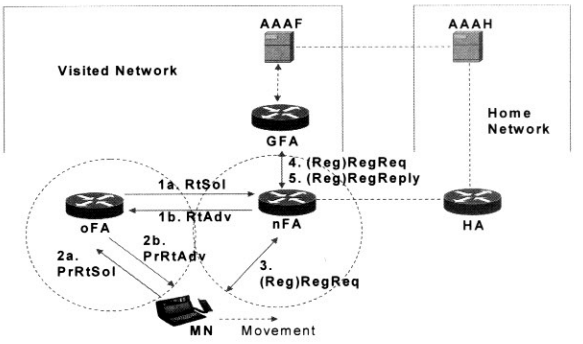
Mobile IP 보안을 위해서 IETF는 Mobile IP와 AAA 프로토콜의 통합을 제시하였다[8, 9]. AAA프로토콜에서 인증이란 망 접근을 허용하기 전에 사용자의 신원을 검증하는 것이고, 권한부여란 망사용이 허락된 사용자에 대해 어떤 권한과 서비스를 허용할 것인지를 정하는 것이며, 과금이란 사용자의 자원 사용에 관한 정보로 적절한 요금을 부과하는 것이다[10, 11].

AAA 프로토콜의 기본 방법은 MN이 홈 도메인에서 외부 도메인으로 이동한 후에 이동한 MN이 홈 도메인에 있었다는 것을 증명하기 위해 AAAF(Foreign AAA Server)를 통해 AAAH(Home AAA Server)에게 인증서를 보냄으로써 인증을 받는다. AAA 프로토콜의 동작 과정을 살펴보면 MN이 외부 도메인 지역으로 이동시 자신의 신분을 확인하기 위해 인증서를 AAAF에게 보낸다. AAAF에서는 MN에 관한 정보를 가지고 있지 않으므로 홈 도메인에 있는 AAAH에게 메시지를 전송한다. 그러면 AAAH에서는 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. AAAH는 HA로부터 회신 메시지를 받고 세션 키를 외부 에이전트(Foreign Agent, FA)와 MN에게 전달함으로써 보안관계를 확립한다[12, 13].

AAA 프로토콜은 (그림 1)과 같이 보안 관계를 맺고 있다. MN은 AAAH와 상호 보안 관계(SA1)를 유지한다. 홈 도메인에서는 AAAH와 HA의 사이에 보안 관계(SA2)를 맺고 있으며, MN이 외부로 이동할 경우 이를 인증하기 위하여 AAAH는 AAAF와 보안 관계(SA3)를 맺는다. 그리고 외부 도메인에서는 FA와 AAAF가 보안 관계(SA4)를 정의한다[15, 16].



(그림 1) Mobile IP에서 AAA 프로토콜 SA 관계[14]



(그림 2) AAA 기반에서의 사전 등록 핸드오프 동작

2.2 이전의 연구 방식들

기존에 Mobile IP와 AAA 프로토콜이 결합하여 동작하는 방식에 관한 연구가 진행되어 왔고, 특히 결합시 생기는 지연시간을 감소시키기 위한 연구가 활발하다. 그 중에 핸드오프 시간이 감소된다는 측면에서 좋은 성능을 갖는 사전등록 핸드오프 방법[17]과 세션키 재사용 방법[4]에 관하여 논의한다.

현재 무선 인터넷에서 사용되는 Mobile IP는 서로 다른 FA에 의해서 서비스 되는 서브넷 간의 IP 계층 핸드오프 절차를 규정하고 있다. 그러나 Mobile IP는 넓은 지역의 느린 이동성 지원을 위해 설계되었기 때문에 빠른 속도로 이동하는 단말에 대한 실시간 서비스 제공에는 어려움이 있다. 따라서 MN이 외부 네트워크로 이동하는 경우 지연시간을 줄여 동작하는 사전등록 핸드오프 방법(Low Latency Handoff, LLH)을 제시한다. LLH는 MN이 네트워크의 도움을 받아 2계층(데이타 링크 계층) 핸드오프 완료 이전에 3계층(IP 계층) 핸드오프를 수행하는 방법으로 (그림 2)에서 핸드오프 절차를 보여준다.

메시지 1a와 1b는 각각 oFA에서 nFA로의 Route Solicitation(RtSol), nFA에서 oFA로의 Route(또는 Agent) Advertisement(RtAdv)를 나타내며 이 과정은 사전 등록 핸드오프가 수행되기 전에 이루어진다. 여기서 oFA는 현재 MN이 머무르고 있는 영역의 에이전트이고, nFA는 새로 이동할 영역의 에이전트를 의미한다. oFA는 이 과정에서 이웃하는 nFA에게 광고를 요청하여 nFA 영역에서 사용가능한 CoA 값을 캐시한다. 이를 통해 사전 등록 핸드오프 시 발생하는 지연을 제거할 수 있다. 메시지 2a는 Proxy Route Solicitation(ProxyRtSol)로 새로운 nFA에서 사용할 CoA를 요청하는 메시지이다. 이에 대한 응답으로 Porxy Route Advertisement(PrRtAdv) 메시지(2b)에 CoA를 포함하여 MN에게 보낸다. MN이 PrRtdv를 받으면 nFA로 등록 요청 메시지 3(Registration Request, RegReq)을 보내게 된다. 메시지 4와 5는 Mobile IP의 표준 등록 과정을 나타낸다[17]. 이로써 MN의 핸드오프시 이전 네트워크에서 새로운 네트워크로 등록 완료되기 전까지 상대노드에 대한 연결성을 잃어버리지 않게 되어 패킷 손실을 최소화하고 지연시간을 감소시킬 수 있다. 또한 MN이 oFA에서 nFA로 이동시에 미리 CoA를 받음으로서 MN의 등록시간에 대한 시그널링 지연시간을 감소시킨다. 또한 oFA에서 nFA로 MN이 이동시에 미리 CoA를 받음으로써 MN의 등록시간에 대한 시그널링 지연시간을 감소시킨다.

기본적인 Mobile IP의 AAA 방식은 MN이 외부 네트워크로 이동시에 홈에 있는 AAA 서버로부터 인증을 받고 세션 키를 생성하여 에이전트들에게 전달한다. 그러나 MN이 인증받기 위해서 홈 도메인에 있는 AAAH까지 인증 요청 메시지가 전달되어야 하기 때문에, 이에 따른 패킷 전달 지연시간이 발생하여 사용자의 QoS를 제한하는 단점을 가진다. 이런 단점을 보완하기 위해서 세션 키를 재사용 하는 방식이 제시되었다. 세션키 재사용 방식은 LLH에 대한 개념을 도입하여 Mobile IP 등록 과정에서 일어나는 지연시간을 최소화하는 방법이다. 기본적으로 제 3자 역할 기능을 하는 GFA는 FA와 보안관계가 설립되어 있다고 가정한다. 제안된 방법은 이전의 할당된 세션 키를 재사용하며 PKI (Public Key Infrastructure) 방식 대신에 제3자 GFA를 통해 oFA와 nFA 사이에서 세션 키를 안전하게 교환할 수 있도록 하는 방식이다. 세션 키의 비밀성을 보장하기 위해서 oFA와 nFA사이에 생명이 짧은 비밀키를 두어 암호화와 복호화시 사용한다. 세션 키들은 제 3자 GFA의 도움으로 FA들 간에 공유함으로서 안전성을 보장하였다. 따라서, 이 방식은 AAA 구조에서 빠른 핸드오프가 가능하여 홈 네트워크에서 외부 네트워크로 이동시에 생기는 시그널링 지연시간이나 오버헤드가 감소한다. 또한 PKI 방식 대신에 제3자를 통해 세션 키를 교환하기 때문에 비밀성을 제공한다.[4]

3. 제안하는 방식

Mobile IP와 AAA 구조가 결합하여 동작하는 기존 방식은 MN이 새로운 망으로 이동할 때마다 인증과정을 거쳐야 하고 홈 네트워크에 등록 요구 메시지를 전달해야 한다. 이러한 동작은 MN의 인증과정에서 AAAH에 의한 반복적인 세션키 발급과 홈 등록을 위한 많은 양의 시그널링 트래픽을 생성시킴으로서 불필요한 오버헤드가 발생한다. 또한 기존 세션키 재사용 방식에서는 MN이 oFA 영역에서 nFA로 이동하는 경우 재사용되는 세션키가 무선상에서 전달되므로 유선상

의 세션키 전달방식에 비하여 보안성 측면에서 취약하다.

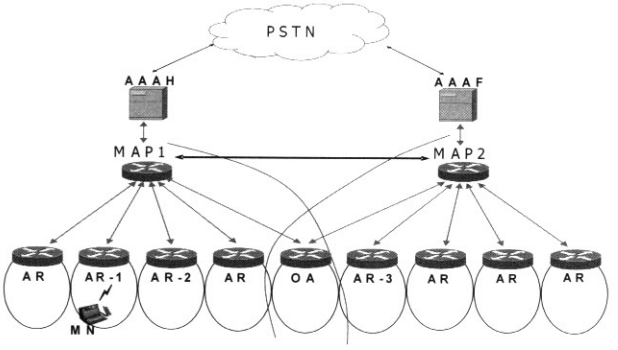
본 논문에서는 MN이 핸드오프 시 발생하는 지연 시간과 MN의 인증으로 인한 AAAH의 오버헤드를 줄이고자 오버랩 네트워크 구조 기반의 세션키 재사용 방법을 제안한다. 본 방식에서는 MN의 보안성 향상을 위하여 공유 세션 키를 유선상에서 전달하는 방식에 기반하고, 그에 따라 신속하고 자연스러운 핸드오프 메커니즘을 제공한다.

오버랩 네트워크 구조 환경에서 세션키 재사용 기법을 위하여 다음과 같이 가정한다.

- 에이전트들과 AAA 서버들 간에 보안 관계가 성립 되어 있다.
- MAP(Mobility Anchor Point)은 여러 개의 에이전트들로 구성된 하나의 클러스터 영역에서 HA의 기능을 수행한다.
- Overlapped Agent(OA)는 다수의 MAP들에 속하며 각 MAP이 속한 영역에 대한 AAA 서버와 보안관계가 성립되어 있는 에이전트이다. MN이 OA 영역으로 이동하게 되면 OA는 해당 AAA 서버에게 MN에 관한 정보를 전달한다.

(그림 3)은 본 논문에서 제안하는 오버랩 네트워크의 구조를 나타내고 있다. 제안하는 구조는 오버랩 지역에 OA를 두고 이웃의 AAA 서버와 보안관계를 맺음으로서 빠른 핸드오프 메커니즘을 제공한다. 제안방식은 클러스터 영역을 관할하는 MAP을 둠으로서 지역 간의 이동성이 신속하게 진행되어 등록에 필요한 시간을 감소시킬 수 있으며, 또한 세션 키를 재사용함으로서 AAAH의 오버헤드를 줄이고 빠른 시간 내에 핸드오프를 완료할 수 있다.

(그림 4)는 LLH 기법에 기반한 기존 세션키 재사용 방식에서의 핸드오프처리 절차를 보여준다. 세션키 재사용 방법은 AAA 서버의 오버헤드와 Mobile IP 등록 절차 시에 지연 시간을 감소시키는 효과가 있다. 특히 세션키 재사용의 보안을 위해서 제 3자의 역할인 GFA를 통하여 세션 키

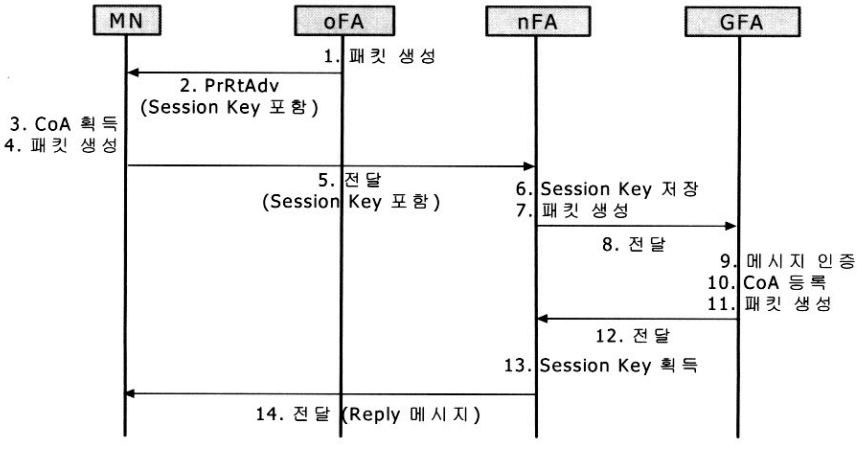


(그림 3) 제안하는 오버랩 네트워크 구조

를 oFA에서 nFA에게 전송한다. 그러나 기존의 세션키 재사용 핸드오프 방식에서는 세션 키를 재사용하기 위하여 세션키 정보를 담은 메시지가 무선상에서 전송되는 것을 알 수 있다(그림 4:2, 5번 단계). 무선 상에서의 메시지 전송은 보안성에 위협요소가 되며, 메시지가 목적지까지 도달하는데 상대적으로 지연시간이 길다는 단점이 있다.

본 논문에서 제안하는 방법에 대한 핸드오프처리 절차는 (그림 5)와 같다. 본 방법에서는 MN의 등록절차 지연시간을 줄이고 세션 키를 재사용하면서 무선상이 아닌 유선상에서 세션 키를 전달하는 것을 핵심으로 한다. 제안방식의 핸드오프 절차는 다음과 같다.

- 단계 1 : MN이 AR-1영역에서 AR-2영역으로 이동시에 MN은 AR-1을 통해 AR-2의 CoA를 얻는다. (AR : Access Router)은 라우터를 의미하며 현재 MN이 머무르고 있는 영역의 라우터를 AR-1, 새로 이동할 영역의 라우터를 AR-2로 놓는다.)
- 단계 2 : MN은 새로운 CoA와 함께 인증요청 패킷을 생성한다.
- 단계 3, 4 : 패킷은 AR-1을 거쳐(단계 3) MAP1에게 전달한다.
- 단계 5 : MAP1은 인증여부를 확인하기 위해 동일 영역



(그림 4) 기존의 세션키 재사용 핸드오프 방식

에 속해 있는 AAAH에게 전달한다.

- 단계 6 : AAAH는 패킷을 확인하여 올바른 사용자의 MN인지 확인한다.
- 단계 7 : 올바른 MN이라면 기존의 세션 키를 포함하여 패킷을 생성한다.
- 단계 8 : 패킷을 MAP1에게 전달한다.
- 단계 9 : MAP1은 AAAH로부터 패킷을 받으면, MAP1은 MN의 CoA를 등록한다.
- 단계 10 : MAP1은 등록 응답 패킷을 생성한다.
- 단계 11 : MAP1은 세션 키를 포함한 등록 응답 패킷을 AR-2에게 전달한다.
- 단계 12 : AR-2는 패킷에 담겨 있는 세션 키를 저장한다.
- 단계 13, 14 : 등록 응답 패킷을 생성하여(단계 13) MN에게 보낸다.

기본적인 방식의 경우 단계 6에서 올바른 MN을 확인하기 위해 AAAH에서 MN을 인증하고 새로운 세션 키를 생성한다. 이에 반해 새롭게 제안하는 방식은 에이전트들과 AAA 서버들 간에 보안관계를 이용하여 AR-2에게 AR-1의 세션 키를 유선으로 전달한다.

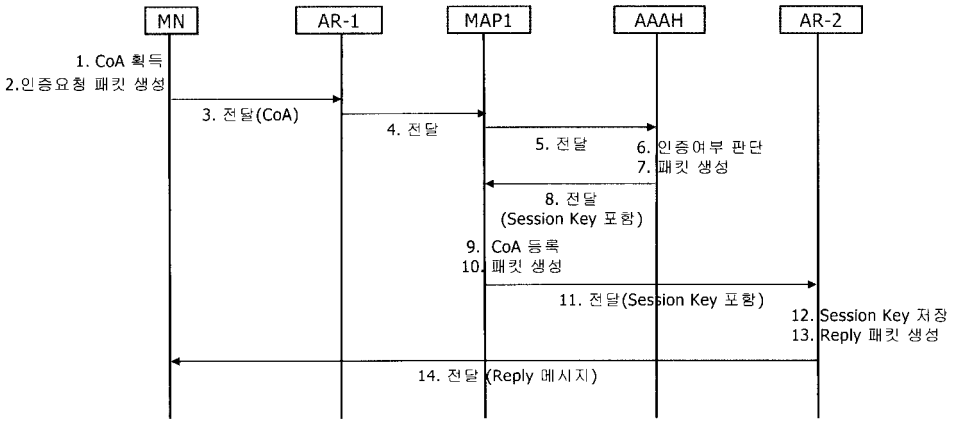
(그림 5) (b)는 MN이 MAP간에 핸드오프 준비 절차를 하기 위한 데이터 흐름도를 보여준다. MN이 다른 영역과의 핸드오프를 신속하게 하기 위하여, MN이 OA 지역으로 이동하면, 미리 MN에 관한 정보를 AAAF에게 전달한다. 즉, OA는 AAAH에게 MN에 관한 정보를 요청하고(1,2,3), 이에 응답으로 AAAH는 MN의 정보를 OA와 연결된 AAAF에게 보안 관계를 통하여 안전하게 전송한다(4,5,6,7). 이로써 AAAF는 기존 세션키를 획득할 수 있다(8). MN이 OA지역에서 AR-3지역으로 이동시에는 단일 클러스터 영역 내에 핸드오프와 같이 동작한다((그림 3) 참조).

4. 성능 평가

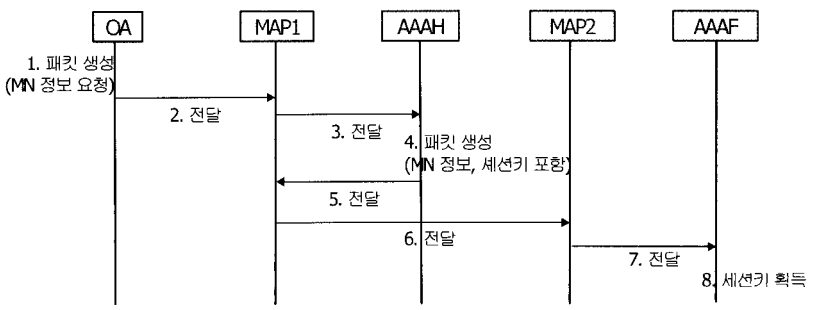
4.1 분석적 모델링

데이터 전송 흐름에 따라 메시지를 보내고 처리하는 총 시간을 구하기 위해 (그림 5) (a)와 같은 핸드오프처리 절차를 고려한다. 즉, 각 단계별로 핸드오프 동작시 필요한 프로세싱 시간, 메시지를 유·무선으로 처리하여 보내는 시간, MN을 인증하는데 필요한 시간을 통하여 총 핸드오프의 시간을 도출하고, 핸드오프 시간에 따른 핸드 실패율을 계산함으로서 제안 방식의 성능을 평가한다.

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[18]. 여기서 i는 각 단계를 나타내며, 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 고



(a) MAP 영역 안에서의 핸드오프 절차



(b) MAP 간의 핸드오프 준비 절차

(그림 5) 제안하는 핸드오프 방식

정된 크기로 가정한다. B의 경우 유선인 경우에는 B^L변수를, 무선인 경우에는 B^W를 사용한다.

전달시간 β_i는 전달 매체에 따라서 고정된 값을 갖으며, β^L과 β^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. 물리적인 전송시간(T_i)을 $M_i(=M_i^L)$로 표현하고 유선의 경우와 무선을 구분하기 위해 각각의 메시지 전달 시간을 M^L과 M^W로 구분한다. 무선 환경에서 메시지 전달시에 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 처리시간을 T_i로 정의하면 유선 상에서는 $T_i = M^L$로 표현되며, 무선 상에서는 $T_i = \sum_{N_f=0}^{\infty}\{\widetilde{T}_i(N_f) \times \text{Prob}(N_f\text{번 실패 후 성공하는 경우})\}$이다. t_W는 메시지가 손실되었음을 인식하는 시간으로 무선 환경에서 요청 신호를 보낸 후 t_W시간 동안 이에 대한 응답을 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 구할 수 있으며, 재전송을 고려한 메시지 처리시간은 다음과 같다.

$$T_i = \sum_{N_f=0}^{\infty}(M^W+N_f(t_w+M^W)) \times \text{Prob}(N_f\text{번 실패 후 성공하는 경우})$$
$$= M^W+(t_w+M^W) \times \sum_{N_f=0}^{\infty}N_f \times \text{Prob}(N_f\text{번 실패 후 성공하는 경우})$$

여기서 $\sum_{N_f=0}^{\infty}(N_f \times \text{Prob}(N_f\text{번 실패 후 성공하는 경우}))$는 무한급수로 평균 실패 횟수를 유도할 수 있다. 한 링크의 전송 실패 확률을 q라 하면, 평균 실패 횟수는 $\frac{q}{1-q}$로 표현된다. q가 0.5인 경우 T_i는 $M^W+(t_w+M^W)\times\frac{0.5}{0.5} = 2M^W+t_w$ 와 같다.

총 핸드오프 시간을 구하기 위해서 핸드오프 동작시 필요한 프로세싱 시간, 메시지를 유·무선으로 전달하는 시간과 MN을 인증하는데 필요한 시간의 합으로 표현되며, 그림 5(a)의 절차에 따른 총 핸드오프 시간을 구한다. 프로세싱 시간이 필요한 경우는 1, 2, 7, 9, 10, 12, 13 단계이다. 메시지를 생성하는 시간, 에이전트가 메시지를 인식하는 시간과 그에 따른 처리시간을 S로 표현하며, 각 단계의 프로세싱 시간은 동일하다고 가정하였을 때, 총 프로세싱 시간은 다음과 같이 표현된다.

$$S_{total} = 2S_{MN}+S_{AAAH}+2S_{MAP1}+2S_{AR-2} = 7S.$$

유선 상에서 메시지가 전송되는 경우는 4, 5, 8, 11 단계로 메시지가 전송되는데 걸리는 시간의 합을 구하면 다음과 같다.

$$L_{total} = M_{AR-1,MAP1}+M_{MAP1,AAAH}+M_{AAAH,MAP1}+M_{MAP1,AR-2},$$

여기서 각 단계에서의 메시지 전송시간이 M^L로 동일한 경우 $L_{total} = 4M^L$과 같이 정리된다. 무선 상에서 메시지를 전송하는 경우는 3, 14 단계로 무선에서의 링크 실패율을 고려한 메시지 총 전송시간의 합은 다음과 같이 표현된다.

$$W_{total} = W_{MN,AR-1}+W_{AR-2,MN} = 2(2M^W+t_w).$$

인증하는데 걸리는 시간 AU은 6 단계에서 이루어지며, 핸드오프를 완료하는데 걸리는 전체 시간(T_{req})은 위에서 언급한 시간의 합으로 구할 수 있다.

$$T_{req} = S_{total}+L_{total}+W_{total}+AU_{total}$$
$$= 7S+4M^L+(2M^W+t_w)\times 2+AU.$$

T는 핸드오프 시점 지역부터 셀 경계 지역에서 MN이 머무르는 시간이고, 핸드오프를 완료하는데 필요한 시간이 T_{req}이 된다. 따라서 T_{req}시간 전에 MN이 경계 지역 밖으로 이동할 확률은 $\text{Prob}(T < T_{req})$로 계산되며, 경계 셀 안에서 MN이 머무르는 시간 T가 지수 분포를 따른다고 가정하였을 때 핸드오프 실패 확률(P_f)은 다음과 같다.

$$P_f = 1-\exp(-\lambda \times T_{req}).$$

여기서, λ의 값은 MN이 경계 셀 지역에 도착율을 의미한다. MN이 움직이는 방향은 $[0, 2\pi)$에서 균일한 분포를 따른다고 가정하였을 때, MN의 속도 V, 셀 반지름이 r인 경계 셀의 길이 R, 경계 셀의 영역 S에 의해 $\lambda = \frac{V \times R}{\pi \times S}$가 된다[19].

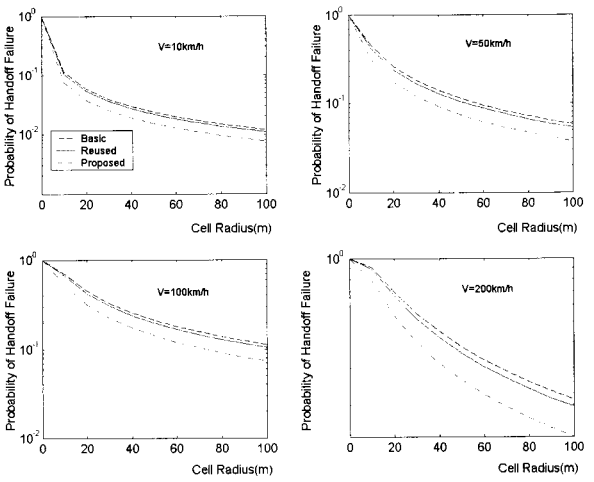
4.2 결과 분석 및 비교

본 절에서는 지금까지 유도한 식을 이용하여 기본적인 Mobile IP와 AAA 프로토콜의 결합방식, 기존 세션 키 재사

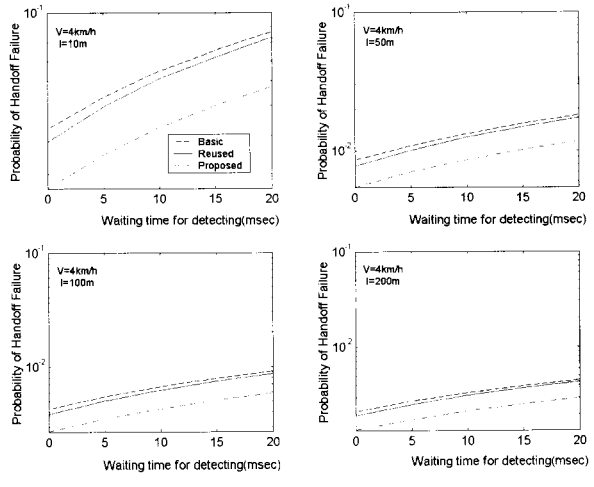
용에 관한 방식과 본 논문에서 제안하는 방식을 핸드오프 실패율에 관하여 비교·분석한다. 비교·분석을 위하여 사용되는 시스템 파라미터 값은 <표 1>과 같다[18, 20-22]. 제안하

〈표 1〉 시스템 파라미터 값

변수	정 의	값
S	프로세싱 시간	0.5 msec
B^L	유선에서의 전송률	155 Mbps
B^W	무선에서의 전송률	144 Kbps
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



(그림 6) 셀의 반경 변화에 따른 핸드오프 실패 확률



(그림 7) 메시지 손실 감지 판단 시간 변화에 따른 핸드오프 실패 확률

는 방식은 오버랩 네트워크 구조를 두고 세션 키를 재사용함으로서 MN의 등록 절차 지연시간과 올바른 MN 판단을 위한 인증시간이 줄어들어 핸드오프 실패율이 감소된다.

(그림 6)은 MN의 이동 속도(V)를 변화시키면서 핸드오프 실패율을 보여준다. V 값이 증가하게 되면 핸드오프를 완료해야 하는 시간이 짧아진다. 만일 MN이 일정한 속도 이상으로 움직이게 되면 핸드오프를 완료하는데 필요한 시간을 얻지 못하여 핸드오프 실패가 발생한다. 이에 따라 기존 세션키 재사용 방법은 지연시간이 증가하게 되어 핸드오프 실패율이 증가한다. 셀 반경 40m에서 0.80%, 3.68%, 6.55%, 10.41% 차이로 속도가 증가할수록 점점 더 좋은 성능을 보임으로서 제안하는 방식이 기존 세션키 재사용 방식과 비교하여 성능향상을 보인다.

더욱이 기존의 세션키 재사용 방식보다 제안한 방식이 핸드오프 실패율에 있어서 성능이 우월하다는 것을 보이기 위해 함수 δ를 다음과 같이 정의하면[23],

$$\delta = \frac{P_{f\,reused} - P_{f\,proposed}}{P_{f\,proposed}} \times 100\ (\%)$$

제안된 방식이 기존의 세션키 재사용 방식과 비교하여 핸드오프 시간을 고려하는 핸드오프 실패율에 있어서 40%정도의 성능향상을 보인다.

(그림 7)은 세션 키가 포함된 메시지를 무선상에서 전송하는 기존의 세션키 재사용 방식에 비해 유선상에서 메시지 전송하는 제안방식의 우월성을 보여준다. V를 4km/h라 가정하고, l의 값을 변화 시키면서 핸드오프 실패율을 측정한다. 메시지가 전달되는 환경은 유선망인 경우 매우 안정적이지만 불안전한 무선 환경에서는 언제든지 메시지가 중간에 손실 될 염려가 있다. 즉, 무선 환경에서의 메시지 손실은 메시지 응답 판단 시간만큼 지연시간이 생긴다. 따라서 제안된 방식은 유선상으로 세션 키를 전송함으로서 기본 방식들에 비해 현저하게 핸드오프 실패율이 감소한다.

5. 결 론

이동 컴퓨팅 단말기의 급속한 증가로 인하여 Mobile IP에서 보안을 유지하는 문제는 점점 중요해 지고 있다. 본 논문에서는 Mobile IP의 보안을 위하여 AAA 프로토콜을 결합하여 MN이 핸드오프를 수행할 때 발생하는 지연 시간과 MN의 인증으로 인한 AAA 서버의 오버헤드를 줄이고자 오버랩 네트워크 구조 기반의 세션키 재사용 방법을 제안한다. 본 방식에서는 MN의 보안성 향상을 위하여 공유 세션키를 유선상에서 전달하는 방식에 기반하고, 그에 따라 신속하고 자연스러운 핸드오프 메커니즘을 제공한다. 분석적 모델링결과에 의하면 제안하는 방식은 기존 세션키 재사용 방식과 비교하여 핸드오프 시간을 고려하는 핸드오프 실패율에 있어서 40%정도의 성능향상을 보인다.

참 고 문 헌

[1] C.E. Perkins, "IP Mobility Support," IETF RFC 3220

[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] 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.

[5] 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.

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

[8] 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

[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] Karim EI Marki et al., "Low latency handoffs in mobile IPv4," IETF draft-ietf-mobileip-lowlatency-handoffs-v4-03.txt, Nov., 2001.

[18] 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.

[19] 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.

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

[21] 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.

[22] 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.

[23] V. P. Kompella, J. C. Pasquale, and G. C. Polyzos, "Multicast routing for multimedia communication," IEEE/ACM Trans. Networking, Vol. 1, No.3, pp.286-292, June, 1993.

최 유 미

e-mail : yumi@ece.skku.ac.kr

2003년 서울여자대학교 컴퓨터공학과 (공학사)

2005년 성균관대학교 일반대학원, 컴퓨터공학과(공학석사)

2005년~현재 (주)벨웨이브 SW그룹 연구원

관심분야 : Mobile Computing, Security

정 민 영

e-mail : mychung@ece.skku.ac.kr

1990년 KAIST 전자공학과(학사)

1994년 KAIST 전자공학과(석사)

1999년 KAIST 전자공학과(박사)

2002년 ETRI 선임연구원

2002년~현재 성균관대학교 정보통신공학부 조교수

관심분야 : 홈 네트워크, 무선 네트워크, 라우팅 프로토콜, 광 네트워크

추 현 승

e-mail : choo@ece.skku.ac.kr

1988년 성균관대학교 수학과(학사)

1990년 University of Texas at Dallas, 컴퓨터공학(석사)

1996년 University of Texas at Arlington, 컴퓨터공학(박사)

1997년 특허청 심사관(사무관)

1998년~현재 성균관대학교 정보통신공학부 부교수

관심분야 : 광네트워크, 이동컴퓨팅, 라우팅 프로토콜, 그리드 컴퓨팅.