

차별화서비스를 위한 Mobile IPv6에서 AAA인증절차의 성능향상을 위한 Fast Handoff 적용방안 연구

변광호, 문영성
승실대학교 컴퓨터학과

e-mail:mun@computing.ssu.ac.kr

A Study on the Performance Improvement of AAA in Mobile IPv6 using Fast- Handoff for Differentiated Services

Kwang-ho Byun, Young-song Mun
Dept of Computing, Soongsil University

요 약

초고속 인터넷 서비스가 일반화되고, PDA 및 노트북 등의 휴대 이동 컴퓨팅 기기의 사용이 증가하면서 인터넷 환경이 유선망에서 무선망으로 점차 변화하고 있다. 무선 인터넷 제공을 위한 주요 인프라는 이동 통신망이나 무선 랜 망이며, 서비스 가입자들은 무선망에서도 유선망과 같은 높은 품질과 안전한 서비스를 요구하고 있다. 그러나 무선망은 유선망에 비해 외부로부터의 공격에 매우 취약하므로 사용자의 QoS 요구사항 뿐만 아니라 안전한 통신을 보장해야 한다. 현재 표준화 기관인 IETF의 Mobile IPv6 워킹그룹에서도 보안문제를 가장 중요하게 다루고 있으며, 기존의 보안 기법들의 취약성을 극복하기 위한 방안으로 표준작업 그룹에서는 인프라 차원의 AAA인증 절차를 이용한 이동노드의 인증 방안이 연구되고 있다. 본 논문에서는 무선인터넷 가입자의 안전성과 서비스 품질을 보장하기 위해 차별화 서비스를 적용한 Mobile IPv6와 AAA연동 방안을 제안 하였으며, AAA 인증 절차에 따르는 핸드오프 지연을 줄이기 위해 Fast Handoff를 적용한 방안을 제안한다.

1. 서론

1)차세대 정보통신망이 IP기반으로 발전함에 따라 IP망에서의 이동성 지원 기술인 Mobile IP[1]에 대한 관심이 증가하고 있다. 실례로 ALL-IP 기반의 3GPP, 3GPP2에서는 이미 기본 인터넷 프로토콜로 IPv6를 채택하고, Mobile IPv6를 이동성 지원 프로토콜로 채택할 것으로 확실시 되고 있다.

그러나 IETF에서는 Mobile IPv6의 표준화에 있어서 보안은 반드시 고려되어야 할 사항으로 간주하고 있으며, Mobile IPv6에서 바인딩 갱신 및 바인딩 응

답(Binding Acknowledge) 메시지 이전에 수행되는 키 분배를 위한 프로토콜로 AAA[2]인증절차를 이용하여 이동노드를 인증하는 방안이 이슈화 되고 있다.

또한, QoS를 보장하기 위한 차별화 서비스[3]에서는 통합 서비스(Integrated Service)의 확장성 문제를 극복한 모델로 자원관리를 수행하는 대역폭 브로커(Bandwidth Broker)[5]에게는 QoS 정책에 준하는 SLA(Service Level Agreements)와 SLA에 할당된 대역폭을 저장하고 있으나 이동노드가 다른 대역폭 브로커가 관리하는 도메인으로 이동시에는 이동노드가 가지고 있는 SLA 내역이 이동한 도메인의 대역폭 브로커에 존재하지 않는 문제로 인해, 이동노드는 지속적인 차별화 서비스를 받을 수 없는 상황이

1) 본 연구는 한국 과학 재단 목적 기초연구 [R01-2001-000-00362-0]지원으로 수행되었음.

발생하게 된다.

그리고 Mobile IPv6는 3계층에서 이동성을 제공함으로써 하부 기술에 독립적인 이동성을 제공할 수 있기 때문에 IP기반의 차세대 망에서 글로벌 로밍을 쉽게 지원할 수 있을 것으로 예상되나 넓은 지역의 이동성 지원을 위해 설계되었기 때문에 빠른 속도로 이동하는 단말에 대한 실시간 서비스 혹은 저속이라도 끊김 없는 서비스를 지원하기에는 많은 어려움이 있다

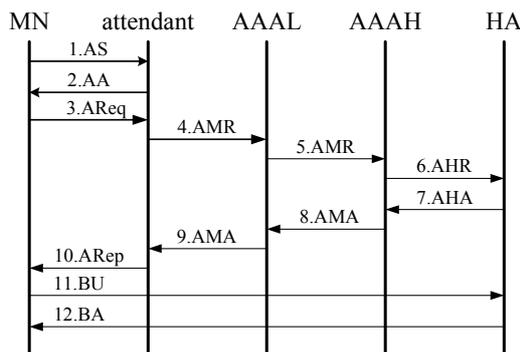
본 논문에서는 QoS 보장을 위하여 차별화 서비스를 위한 Mobile IPv6에서 보안 취약성을 보완하기 위하여 AAA 인증모델을 적용하였으며, 인증 지연 시간과 패킷 손실을 줄이기 위해 Fast Handoff[4]를 연동할 수 있는 방안을 제시한다.

2. 관련연구

2.1 Mobile IPv6를 위한 AAA 구조[2]

Mobile IPv6의 시그널링 이전에 행하여 지는 키분배를 위한 프로토콜인 IKE(Internet Key Exchange) 교환 성능이 이동환경에서 기대에 못미치는 것으로 보고되었으며, Francis Dupont은 “AAA for Mobile IPv6”문서를 통해 해결점을 제안하였다.

AAA(Authentication, Authorization, Accounting) 구조에서는 도메인 간 인증을 제공하기 위해서 이동노드, 홈 에이전트 등의 Mobile IP 관련 엔티티 이외에 Attendant, 방문 도메인의 AAA 서버, 홈 도메인의 AAA 서버 등의 엔티티가 존재한다.



[그림 1]. AAA 인증 및 바인딩 절차

이동노드가 자신의 IPv6 주소를 설정하고 Attendant를 발견한후 (AS: Attendant Solicitation, AA: Attendant Advertisemen) 인증을 요청하며 (AReq: Authentication Reques), Attendant는 이동노드로부터 수신한 인증 정보를 AAAL 서버로 전달한다. AAAL 서버는 요청 메시지를 AAA 프로토

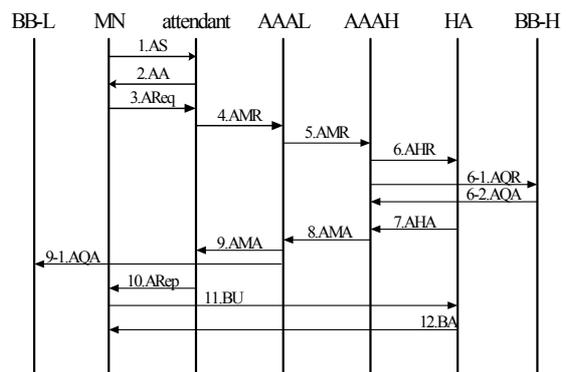
콜로 변환하여 AAAH 서버로 전달하게 되고, 홈 에이전트와 이동노드간의 미리 구성된 키를 바탕으로 이동노드와 Attendant간 사용될 세션 키를 생성한 후 키 및 키 생성 재료를 리턴 한다.

2.2 QoS를 제공하기 위한 AAA구조

QoS를 보장하기 위한 차별화 서비스[4]에는 통합 서비스(Integrated Service)의 확장성 문제를 극복한 모델로 자원관리를 수행하는 대역폭 브로커(Bandwidth Broker)[5]라는 개체가 있다. 대역폭 브로커는 QoS 정책에 준하는 SLA(Service Level Agreements)와 SLA에 할당된 대역폭을 저장하고 있는 소프트웨어 개체이다.

대역폭브로커는 자신의 도메인내의 사용자에게 차별화된 서비스를 제공하여 QoS를 보장할 수 있으며, 정의된 서비스를 위하여 도메인 내부의 라우터를 구성할 책임이 있다. 대역폭브로커는 각각의 SLA를 사용자ID, 패스워드, QoS parameter, source address, destination address, Sorce port, Destination port등의 항목으로 구성하여 저장한다.

QoS를 제공하기 위한 AAA구조에서 이동노드의 사용자 정보는 NAI[3] 또는 Home Address[1]로 구분할 수 있다. 그러므로 대역폭브로커에 저장된 SLA 내역은 사용자의 NAI나 Home Address로 찾아 낼 수 있으며, AAAH와 AAAL 서버간의 안전한 채널로 이동노드의 SLA 내역을 이동할 수 있도록 자신이 속한 도메인의 인증된 사용자가 요구하는 서비스의 SLA 내역이 저장된 데이터베이스를 포함하거나, 대역폭브로커에 접근할 수 있는 인터페이스를 갖는다.

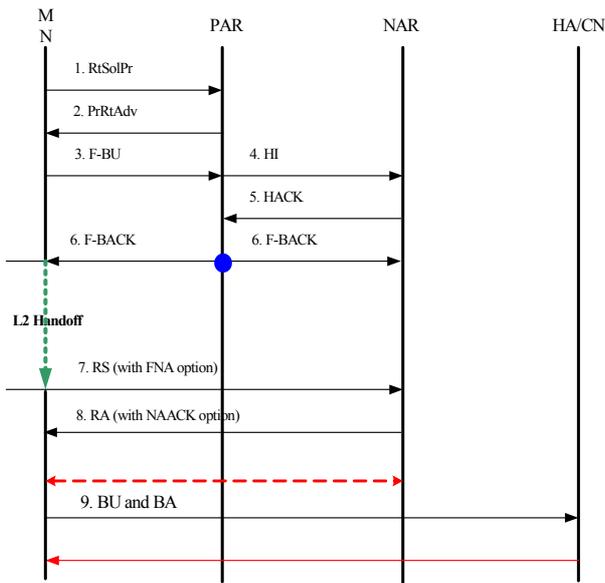


[그림 2]. 차별화서비스를 위한 AAA 절차

이동노드의 차별화서비스를 위한 AAA 절차는 [그림 2]와 같다. 이동노드가 데이터 전송중에 이동을 한다면 인증절차에 따르는 지연시간만큼의 패킷 손실 및 차별화 서비스를 받을 수 없다.

2.3 Layer3 Mobile IPv6 핸드오프[3]

Mobile IPv6는 IP 기반 3계층에서 하부 기술에 독립적으로 이동성을 제공함으로써 차세대 망에서 글로벌 로밍을 쉽게 지원할 수 있다. 그러나 핸드오프 과정 중에 2 계층과 3 계층 핸드오프 시간이 각기 분리되어 있어서 재등록까지 지연이 생기게 되므로 빠른 속도로 이동하는 이동노드와 실시간 서비스를 제공하는데 어려움이 있다. 이러한 문제점을 보완하기 위해 Fast Handoff에서는 미리 CoA를 설정하는 방법과 양방향 터널을 설립하는 방법을 통해 해결점에 접근하고 있다.



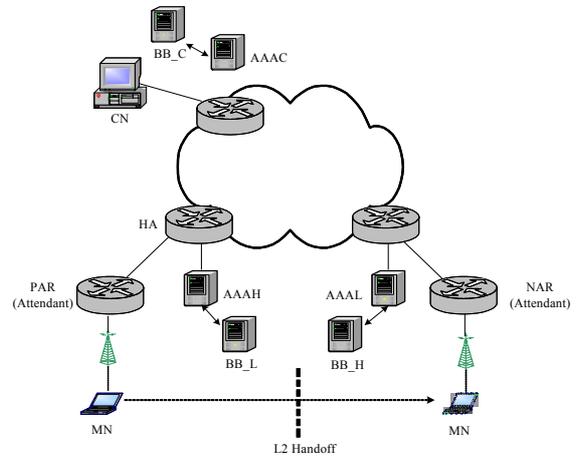
[그림 3]. Layer 3 Mobile IPv6 핸드오프

[그림 3]에서 Fast Handoff 1에서 6 과정은 셀 간의 중첩된 부분에서 이루어진다. 이동노드가 새로운 AR로 접근하여 2계층 정보를 받기 시작할 때 전파 세기를 비교해서 중첩된 부분임을 인식하고, 핸드오프시에 연결지속을 위해 nCoA(new CoA)를 미리 생성해야 한다. 이동노드는 PAR(Previous AR)에 RtSolPr/PrRTAdv 메시지를주고 받음으로써 NAR에서 사용될 nCoA 주소를 획득한다. 그리고 이동노드는 F-BU메시지를 통해서 핸드오프 전에 미리 nCoA를 PAR에 등록한다. PAR은 HI/HACK메시지를 주고 받음으로써 PAR과 NAR 사이에 터널을 설립하고 이동노드의 nCoA의 사용 가능여부를 검사한다. PAR은 F-BACK메시지를 통하여 NAR에게 터널 설립 완료 메시지를 MN에게 터널 설립 완료 및 nCoA의 검증 결과를 전송한다. 이동 단말이 NAR로 2계층 핸드오프를 하는 동안에 PAR에서 설립된 터널을 통해 이동 단말의 oCoA (old CoA)로 도착한

패킷을 NAR로 전달한다. NAR은 이 패킷을 detunneling하여 버퍼링을 하고 있다가 이동노드가 NAR에 접근하여 RS/RA 메시지 과정을 통하여 3계층 등록을 완료하면 전달된다. 핸드오프 과정이 완료되면 이동노드는 홈 에이전트 및 상대노드에게 nCoA를 사용함을 알린다. 이후 상대노드는 이동노드의 nCoA로 패킷을 전송한다.

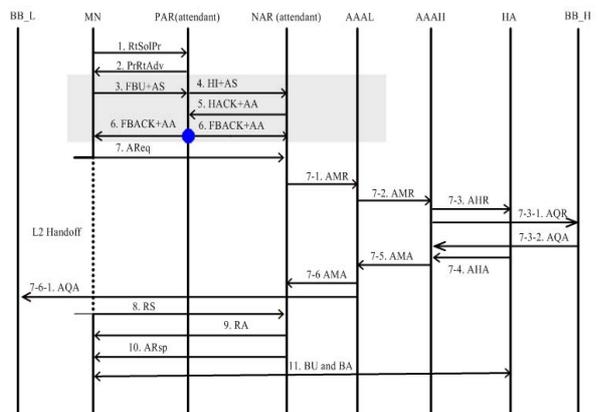
3. 연구내용

관련연구에서 분석한 차별화 서비스를 위한 Mobile IPv6 와 AAA 연동방안 그리고 Fast 핸드오버를 적용한 AAA 인증절차를 통하여 [그림 4]는 최적화된 네트워크 구조를 나타낸다.



[그림 4]. 제안된 시스템 모델

제안하는 모델은 Fast Handoff동작 절차와 AAA 인증 절차가 수행될 수 있도록 제안하였으며 QoS를 위한 SLA 내역의 이동이 AAA 인증 절차와 동시에 수행하여, 인증절차와 SLA 내역의 이동에서 발생하는 지연 시간을 줄일 수 있도록 제안하였다.



[그림 5]. 제안된 시스템 모델의 메시지 절차

본 논문에서 제안한 모델은 [그림 5]의 메시지 절차를 따른다. 이동노드가 이동을 시작하면 Fast handoff 동작이 수행되며, 터널 설립과 이동 노드의 nCoA를 확인 하기 위해 FBU 메시지를 PAR에게 보낸다. 이때 FBU 메시지에 AAA 인증 절차 메시지인 AS 메시지를 포함해서 보냄으로써 AAA 인증 절차를 Handoff 발생전에 시작할 수 있다.

QoS보장을 위한 차별화서비스의 SLA 내역 이동은 AAAH가 이동노드의 NAI나 Home Address로 구분하여 [그림 5]의 7-3-1 AQR와 7-3-2 AQA 메시지 절차를 통하여 획득하고, 홈 에이전트로부터 받은 7-4 AHA 메시지와 SLA내역을 같이 AAAL로 보내는 것으로 이루어진다. 이것을 받은 AAAL은 이동노드의 SLA 내역을 7-6-1 메시지 절차를 통하여 BB_L의 데이터베이스에 저장한다. BB_L은 이동노드의 SLA에 준하여 라우터들을 조정하며, 이로써 이동노드는 이동한 도메인에서 지속적인 QoS를 보장받을 수 있다.

제안하는 모델과 메시지 절차는 AAA 인증 절차와 QoS 보장 절차가 수행되며, AAA 인증 절차와 Fast Handoff의 연동을 통하여 지속적인 차별화 서비스의 보장과 핸드오프 지연 및 패킷 손실을 감소의 이점을 얻을 수 있다.

3. 결론

본 논문에서는 이동노드의 보안성이 보장되는 차별화 서비스를 위하여 Mobile IPv6와 AAA 기법을 이용한 모델을 적용하였고, 이러한 AAA 인증으로 인한 지연을 줄이기 위해 Fast Handoff를 적용한 방안을 제안 하였다.

최근, 무선 인터넷 서비스가 보편화됨에 따라 각 사업자들은 고속 무선 데이터를 보다 저렴하고 효과적으로 서비스하기 위한 방안을 찾고자 노력하고 있으며, 따라서 본 논문에서 제안하는 방안은 이런 요구사항을 충족시켜 줄 것으로 예상된다. 향후 과제로는 홈 에이전트와 상대노드간의 시그널링 처리의 경로를 줄이는 방안과 현재 제안된 보안 기법들과 수식적인 비교 분석을 진행하고자 한다.

참고문헌

- [1] D. Johnson, C. Perkins and J. Arkko. Mobility Support in IPv6, Draft-ietf-mobileip-ipv6-24, Dec. 29, 2003..
- [2] F. Dupont, J. Bournelle: AAA for Mobile

IPv6, draft-dupont-mipv6-aaa-01.txt, Internet Draft, IETF, Nov, 2001.

- [3] P. Calhoun, C. Perkins. Mobile IP Network Access Identifier Extension for IPv4 RFC 2794, March 2000.
- [4] Koodli, R. (editor), "Fast Handovers for Mobile IPv6", draft-ietf-mipshop-fast-mipv6-01.txt, February 2004. Work In Progress.
- [5] S. Blake, D. Black, M. Carlson, Z. Wang, W. Weiss. An Architecture for Differentiated Services RFC 2475, December 1998.
- [6] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence. AAA Authorization Application Examples. RFC2905, August 2000
- [7] Charles E. Perkins, Pat R. Calhoun. AAA Registration Keys for Mobile IP, draft-ietf-mobileip-aaa-key-09.txt, Internet Draft, IETF, Feb 2002..