모바일 IPv6에서 실시간 통신을 위해 해쉬 값을 적용한 빠른 인증 기법

강 형 모[†] · 문 영 성[††]

요 약

모바일 IPv6에서 외부 망을 이동하는 이동노드는 보안의 위협으로부터 올바른 서비스를 제공 받기위해 인증이 필요하다. AAA 는 네트워크에서 서비스를 받는 노드에게 인증 및 권한 부여, 과금 계산을 하는 신뢰적인 기반 구조이며, Mobile IPv6 워킹 그룹은 이동노드의 인증을 위해 AAA 기반 구조의 사용을 권고한다. AAA 기반 구조는 강력한 인증 기능을 제공하지만, 노드가 이동할 때마다 많은 메시지 교환을 통해 이동노드를 인증한다. 이러한 많은 메시지 교환은 지연을 발생시키고, 지연은 실시간 통신에 어려움을 준다. 본 논문에서는 이동노드의 인증 과정으로 발생하는 지연을 줄이기 위해 이동노드의 해쉬 값을 이용한 향상된 인증 기법을 제안한다. 제안 기법을 사용한 이동노드는 이동 직후 일정시간 확장된 기존의 인증협약을 사용하고 새로운 인증협약 설정으로 발생하는 지연을 없앤다. 제안 기법의 성능 평가는 다른 기법들과의 비용 비교 분석을 통해 그 효율성을 검증한다. 그 결과 이동노드가 다른 서브넷으로 이동하는 경우 일반적인의 기법보다 25% 이상의 성능 향상을 보인다.

키워드 : 실시간 통신, 빠른 인증 기법, 모바일 IPv6, FMIPv6, AAA

A Fast Authentication Method using Hash Value for Realtime Communication in Mobile IPv6 network

Hyungmo Kang[†] · Youngsong Mun[††]

ABSTRACT

A node of mobile IPv6 moving foreign networks needs authentication process to support right services against from security threat. AAA is a trust infrastructure that authenticates, authorizes, and accounts nodes receiving a network service. And Mobile IPv6 Working Group recommends use of AAA infrastructure to authenticate mobile nodes. Event though AAA infrastructure provides strong authentication functions, it should exchange a lot of messages to authenticate mobile nodes every movement. The exchange of lots of messages causes latency and it is interfered with realization of real-time communication. This paper proposes an authentication method of improved speed using hash value of mobile node to reduce authentication latency. Directly after movement, a mobile node applying a proposed method uses extended existing security authentication for a while and deletes the establishment latency of new security authentication. Performance evaluation of a proposed method verifies the efficiency through the analysis of cost comparison with other methods. The conclusion of performance evaluation is that the proposed method gets more 25% performance improvement than a general method when a mobile node moves another subnet.

Key Words : Real-time Communication, Fast Authentication, Mobile IPv6, FMIPv6, AAA

1. 서 론

Internet Engineering Task Force(IETF)의 모바일 IPv6 워킹 그룹은 IPv6[1] 노드의 통신 이동성을 지원하기위해 모바일 IPv6[2]를 제안하였다. 외부 망에 있는 모바일 IPv6 환경의 이동노드는 항상 보안의 위협에 노출되어 있기 때문에 올바른 서비스를 위해 서브넷 이동마다 인증 과정을 수행한다. 하지만 인증 과정 완료까지의 지연은 데이터 손실을 야기하고 실시간 통신을 어렵게 한다. 인증 과정의 지연은 IPSec[3]을 통한 인증 협약(Security Association : SA)[4] 설정 시 발생한다. 특히 외부 망에서의 초기 구동시 동적인 인증 협약 설정[5]은 많은 메시지 교환으로 큰 지연을 야기한다. 때문에 모바일 IPv6 워킹 그룹은 신뢰적인 기반 구조를 통한 인증 기법인 인증, 권한, 과금(Authentication,

※ 본 연구는 숭실대학교 교내 연구비지원으로 이루어졌음.
† 준 회 원 : 숭실대학교 대학원 컴퓨터학과 석사과정
†† 종신회원 : 숭실대학교 컴퓨터학부 부교수
논문접수 : 2005년 9월 26일, 심사완료 : 2006년 1월 10일

Authorization, Accounting : AAA)기반 구조[6]의 사용을 권고[7]하였다.

AAA 기반 구조의 적용을 통해 초기구동의 큰 지연 문제는 해결하지만, AAA 인증 과정[8]으로 인한 지연은 여전히 발생한다. 빠른 핸드오버(Fast Handover)[9]와 AAA 인증 과정[8]을 동시에 수행하는 병행 기법[10]은 AAA 인증을 미리 시작하여 인증 지연을 줄인다. 그러나 이동노드의 빠른 이동과 L2 핸드오프의 향상 그리고 빠른 핸드오버의 reactive 모드 같은 상황에서는 비효율적인 메시지 교환과 지연으로 인해 실시간 통신이 어렵다.

본 논문에서는 노드 이동 상황에서 발생하는 인증 과정의 지연을 줄이고 실시간 통신에 적합한 효율적인 인증 기법을 제안한다. 즉, 이동노드는 핸드오버 과정에서 발생하는 정보와 자신의 정보를 통해 해쉬 값을 생성하고, 이 값을 통해 새로운 접속 라우터를 인증한다. 해쉬 값을 통한 인증으로 기존의 인증 협약 범위는 새로운 접속 라우터까지 확장되고, 이동노드는 이동 후에도 기존의 인증협약을 일정 시간 사용할 수 있다. 결과 새로운 인증 협약 설정으로 발생되는 지연이 제거된다.

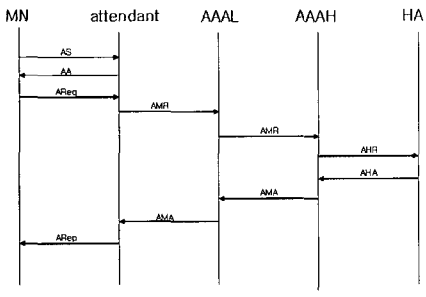
본 논문의 2장은 관련연구로서, Dupont AAA 기법[8]과 빠른 핸드오버에 Dupont AAA를 병행한 기법[10]을 분석한다. 3장에서는 제안 기법과 그 절차를 보여주며, 4장에서는 제안기법과 기존 연구 [10]의 인증 과정 동안 소요되는 시간 비용을 비교 분석하여 성능 평가를 수행한다. 마지막으로 5장에서는 결론을 나타낸다.

2. 관련 연구

2.1 Dupont AAA 기법

Dupont AAA 기법은 이동노드와 홈 에이전트 그리고 AAA 사이에 정보 메시지 교환을 통해 모바일 IPv6가 AAA를 이용하도록 한 것이다.

AAA 클라이언트인 attendant는 로컬 AAA 시스템에 접속할 수 있는 접점이며 동시에 로컬 주소 제공 및 등록의 역할을 한다. 홈 AAA 서버(AAAH)는 홈 도메인의 인증 서버이다. 로컬 AAA 서버(AAAL)는 외부 망의 인증 서버로서. AAA 클라이언트와 홈 AAA 서버 사이에 위치하며 정보를 전달하는 역할을 한다.



(그림 1) Dupont AAA 과정을 통해 이동노드를 인증하는 것을 나타내고 있다.

이동노드는 attendant의 발견을 위해 AS(Attendant Solicitation) 메시지를 보내고, attendant는 이에 대한 응답으로 AA(Attendant Advertisement)를 보낸다. 이동노드는 로컬 주소의 할당 및 등록을 요청을 위해 AReq(Authentication Request) 메시지를 attendant에게 보낸다. 첫 번째 AAA 메시지, AMR(Authentication MN-Request)은 attendant에서 AReq 내에 있는 인증 요청 정보를 로컬 AAA 서버(AAAL)와 홈 AAA 서버로 보낸다. 두 번째 AAA 메시지, AHR (Authentication HA-Request)은 홈 AAA 서버에서 홈 에이전트로 이동노드의 홈 주소와 SecuParam_I[5]정보를 보낸다. AHR의 정보를 통해 홈 에이전트는 SecuParam_R(이동노드와의 인증협약을 위한 재료)을 생성하고 홈 AAA 서버에 세 번째 AAA 메시지인 AHA(Authentication HA-ACK)를 보낸다. AMA(Authentication MN-ACK)는 AHA의 정보를 홈 AAA 서버에서 attendant까지 전달한다. AMA는 RC(Result Code)값을 통해 AAA 결과를 알린다. attendant는 SecuParam_R를 포함한 응답 메시지 ARsp(Authentication Response)를 이동노드로 전달하면서 Dupont AAA 과정을 통한 이동노드의 인증 절차를 마친다.

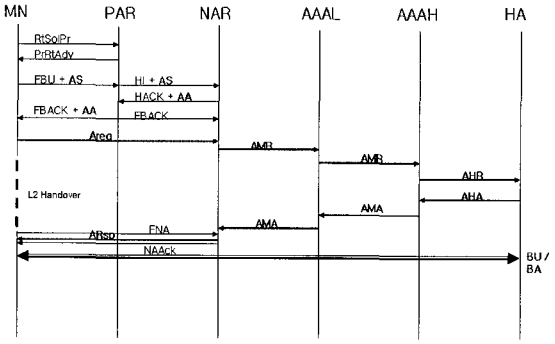
2.2 빠른 핸드오버와 Dupont AAA 기법의 병행

빠른 핸드오버에 AAA 인증 절차를 적용하면, 모든 핸드오버과정의 수행 후에 AAA 절차가 수행된다. 결국 인증 과정으로 지연이 발생한다. 이 문제를 해결하기 위해 참고문헌 [10]은 이동노드가 빠른 핸드오버를 수행함과 동시에 AAA 인증 절차도 수행하도록 하였다.

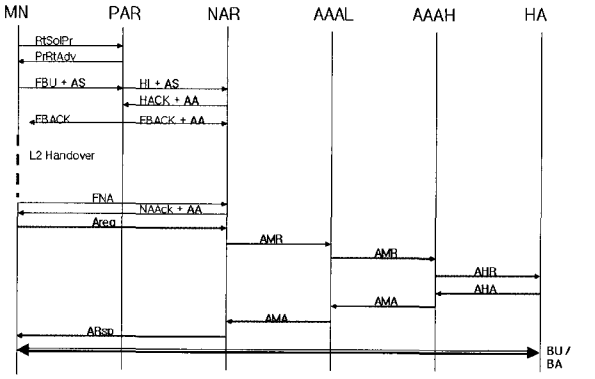
(그림 2)와 (그림 3)은 참고문헌 [10]의 두 가지 상황에서의 절차를 나타내며, 표시된 부분은 제안사항이다. 빠른 핸드오버의 Fast Binding Update(FBU) 메시지에 Dupont AAA의 AS 메시지를 포함해 보냄으로서, AAA 인증을 미리 시작한다. AS 메시지는 이전 접속 라우터에서 새로운 접속 라우터로 전달되고, 새로운 접속 라우터는 이에 대한 응답으로 이전 접속 라우터에게 AA 메시지가 포함된 Handover ACK (HACK) 메시지를 전송한다. 터널이 생성되고, HACK메시지를 받은 이전 접속 라우터는 AA 메시지를 Fast Binding ACK (FBACK) 메시지에 포함시켜 이동노드와 새로운 접속 라우터로 보낸다. 만일 이동노드가 새로운 서브넷으로 이동하기 전에 FBACK메시지를 받게 되면, L2 핸드오프 시간 동안에도 일련의 AAA 인증 절차가 수행되고, 인증 절차로 인한 지연이 줄어든다. 그리고 만약 이동노드가 FBACK 메시지를 받지 못한 경우에는 빠른 핸드오프 후에 나머지 인증 절차를 수행한다. 하지만 이 경우는 Dupont AAA 과정의 대부분이 FNA 메시지 전송 후 수행되기 때문에 지연을 줄이는 효과가 적다.

참고문헌 [10]은 인증과정을 핸드오버 과정과 병행하여 수행하기 때문에 인증으로 인한 지연을 줄인다. 특히 (그림 2)의 경우는 많은 지연 단축의 효과를 얻을 수 있다. 하지만 이동노드가 빠른 속도로 자주 이동하게 되면 계속적인 인증으로 인한 인증지연이 발생하고 이는 비효율성의 문제가 된

다. 또한 L2 계층의 성능 향상으로 인한 L2 핸드오프 지연의 감소나 홈 AAA 서버가 먼 거리에 위치한 것도 인증으로 인한 지연의 영향을 받게 된다. 결국 이러한 지연 문제들은 실시간 통신에 큰 어려움을 준다.



(그림 2) 참고문헌 [10]에서 이동노드가 FBACK 메시지를 받고 이동한 경우를 나타내고 있다.

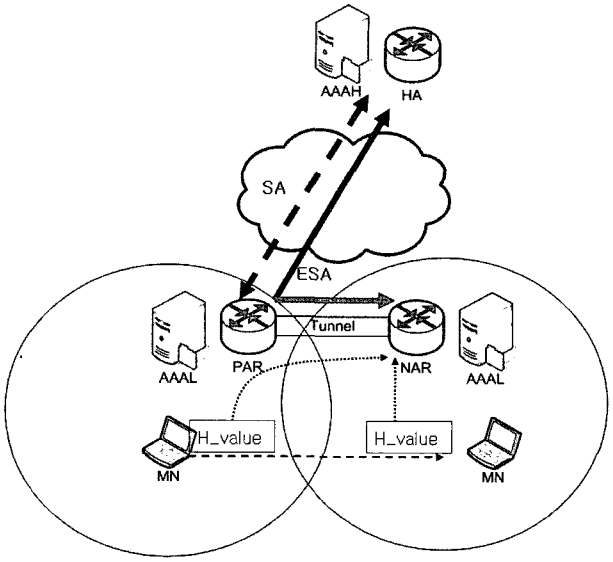


(그림 3) 참고문헌 [10]에서 이동노드가 FBACK 메시지를 받지 못하고 이동한 경우를 나타내고 있다.

3. 제안 방안

3.1 제안 기법의 구조

모바일 IPv6 노드는 서브넷 이동마다 새로운 인증 협약을 맺어야 한다. 인증 협약은 여러 메시지 교환을 필요하기 때문에 이동마다의 인증 절차는 노드가 서브넷을 빠른 속도로 자주 이동하는 경우 비효율성과 지연의 문제를 야기한다. 본 논문은 인증지연 문제를 해결하며 동시에 실시간 통신을 제공하기 위해 임의의 해쉬 값을 통한 인증으로, 서브넷 이동 시 발생하는 많은 메시지 교환의 인증 과정 대신에 단순한 인증과정을 수행한다. 이를 위해 이동노드는 이전의 접속 라우터와 새로운 접속 라우터를 통해서만 얻을 수 있는 고유한 정보를 바탕으로 임의의 해쉬 값을 생성한다. 그리고 이 값을 통해 새로운 접속 라우터를 인증하고 그 결과 인증 구간을 확장한다. 즉, 홈 에이전트에서 이전 접속 라우터를 거쳐 이동노드로 정해져 있던 신뢰구간을 홈 에이전트에서 이전 접속 라우터와 새로운 접속 라우터를 거쳐 이동노드로 그 범위를 확장한다. 인증구간의 확장으로 인해 이동노드는 서브넷 이동 후에도 일정시간 기존의 인증 협약을 사용한다.



(그림 4) 인증 값 H_value를 적용하여 빠른 인증을 수행하는 제안 기법의 수행과정을 나타내고 있다. 그림에서 기존의 인증협약을 Security Association (SA)라 하고, 제안 기법을 통해 확장된 인증협약을 Extended Security Association (ESA)로 정의한다.

[정의 1] H_value = First(64,HMAC_SHA1(NAI,(HoA|OCoA|NCoA|HA|aaa_key)))

"H_value = First(64,HMAC_SHA1(NAI,(HoA|OCoA|NCoA|HA|aaa_key)))는 이동노드가 가지고 있는 NAI, HoA, HA, Old CoA, New CoA, aaa_key 를 HMAC_SHA1 해쉬 함수를 이용하여 얻은 해쉬 값이다."

본 논문에서는 빠른 인증을 위해 임의의 해쉬 값 H_alue를 정의 및 사용한다. 제안된 인증 값은 정의 1의 식을 통해 얻어진다. 각 재료들은 이동노드의 식별자(NAI), 이동노드의 홈 주소(HoA), 홈 에이전트 주소(HA), 빠른 핸드오버의 RtSolPr와 PrRtAdv메시지 교환을 통해 얻은 New CoA와 기존에 가지고 있던 Old CoA, AAA 기반의 사용을 위해 이동노드가 생성하는 키잉 재료인 aaa_key이다.

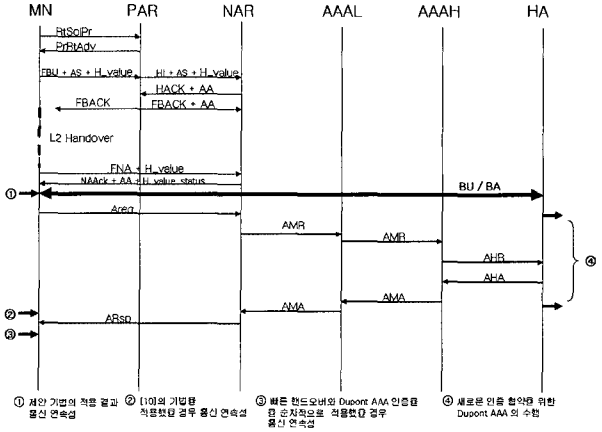
제안 기법의 구조는 (그림 4)와 같다. 먼저 이동노드는 서브넷 이동전에 H_value를 생성한다. 그리고 Fast Binding Update (FBU) 와 Handover Initiate (HI) 메시지를 통해 H_value를 새로운 접속 라우터로 전달한다. 이때, 새로운 접속 라우터는 받은 메시지 내에 포함된 H_value와 이동노드의 NAI를 저장한다. 이동노드가 새로운 접속 라우터로 이동하게 되면, 이동노드는 H_value를 재생성 및 새로운 접속 라우터에 전송하고, 새로운 접속 라우터는 해당 노드의 이동전 H_value와 이동 후 H_value의 비교하여 이동노드의 인증을 수행한다. 이동노드가 같은 H_value를 보낸 것이 확인되면 인증이 완료되고, 결과 이전의 접속 라우터와 새로

운 접속 라우터 사이를 신뢰구간으로 추가한다. (그림 4)에서 점선은 노드의 이동전 서브넷에서 사용한 인증 협약(Security Association : SA) 범위이고, 실선은 이전 접속 라우터와 새로운 접속 라우터까지의 신뢰구간을 추가한 확장 인증 협약(Extended Security Association : ESA)이다. 제안 기법은 노드가 서브넷 이동 후에 바로 새로운 인증 협약(New Security Association : NSA)을 설정하는 것이 아니라 기존의 인증협약 구간과 H_value를 통해 인증된 구간을 추가한 확장 인증협약을 일정시간 사용함으로서 인증지연을 줄이는 것이다. 새로운 인증협약 설정은 통신 중에 수행되며, 인증 협약의 응답(ARep)이 오면, 사용 중인 확장 인증 협약을 새로운 인증 협약으로 교체한다.

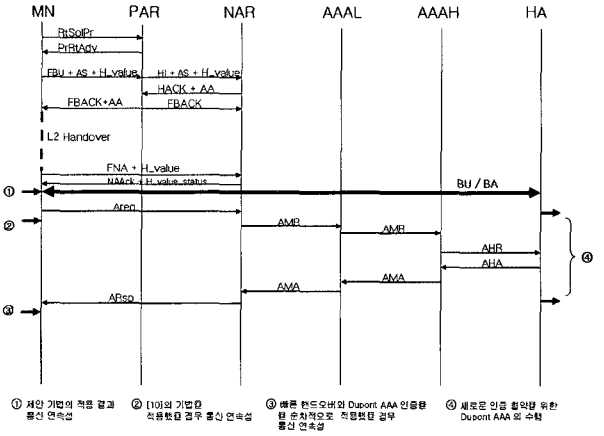
제안 기법은 새로운 인증 협약을 설정하는 동안 확장 인증 협약을 사용하기 때문에, 지연이 없고, 실시간 및 연속적인 통신이 가능하다. 만약 새로운 인증 협약이 실패하거나, 인증 협약의 교체 시간이 만기되면 이동노드는 통신을 멈추고 재 인증을 요청한다. 제안기법은 또한 이전 접속 라우터와 새로운 접속 라우터 그리고 이동노드사이의 인증과정을 통해 접속 라우터들 사이의 터널 내 정보에 신뢰성을 준다. H_value를 통한 인증이 완료되면, 기존의 인증 협약 시간은 재설정 되며, 이 시간은 새로운 인증 협약의 설정시간과 같다. 인증 재전송으로 발생하는 지연손실을 막기 위해 재설정 시간은 라우터들 사이를 이동하는 운송수단의 평균시간으로 정한다. 또한 Replay attack을 방지하기위해, 새로운 접속 라우터는 H_value에 의한 인증을 마친 후 등록된 이동노드의 H_value를 지운다. 제안 기법에서 이전 접속 라우터는 자신의 서브넷에서 이동하려는 노드에 대해서만 해쉬 값을 전송하고, 새로운 라우터는 전송 받은 해쉬 값이 이전 라우터로부터 온 정보임을 확인하는 기능이 있어야 한다.

3.2 제안 기법의 절차

(그림 5), (그림 6)은 제안 기법의 절차들을 나타내며, 절차 중 표시된 부분이 제안 기법인 H_value를 통한 빠른 인증 과정에 해당한다. 핸드오버 과정의 Router Solicitation for Proxy (RtSolPr)와 Proxy Router Advertisement (PrRtAdv) 메시지 교환 후 이동노드는 NCoA를 생성함과 동시에 인증 값인 H_value를 만들어 FBU 메시지 내에 Dupont AAA의 AS와 함께 보낸다. FBU 메시지를 받은 이전 접속라우터는 HI 메시지 내에 AS와 H_value를 역시 포함시켜 새로운 접속 라우터로 보낸다. 새로운 접속 라우터는 HI 메시지를 통해 H_value를 얻고, 이동노드의 NAI와 인증 값을 저장한다. L2 핸드오버 후에, 새로운 접속 라우터에 도착한 이동노드는 자신이 가진 정보를 통해 H_value를 재생성하고, Fast Neighbor Advertisement (FNA) 메시지에 인증 값을 포함시켜 보낸다. 이때, 새로운 접속 라우터는 FNA 메시지를 통해 얻은 H_value와 해당 NAI로 저장된 이동노드의 H_value를 비교 한다. 비교 결과 값이 동일하면 이전 접속 라우터와 새로운 접속 라우터 사이의 구간 인증이 완성되고 이를 신뢰구간으로 하며, 기존의 인증 협약 범위를 새로운 접속 라우터까지 연장한다. 제안 기법은 기존의 인증 협약을 재사용하지만 보안을 위해 새로운 인증 협약을 설정한다. 이는 (그림 5)와 (그림 6)의 ④번 절차이다. 새로운 인증 협약은 핸드오버 후 AAA 절차에 의해 별도로 수행되고, 인증이 완료되면 기존의 인증 협약과 교체한 뒤, 통신을 계속한다.



(그림 5) 제안 기법의 절차 중 이동노드가 이동전에 FBACK 메시지를 받지 못한 경우를 나타내고 있다.



(그림 6) 제안 기법의 절차 중 이동노드가 이동전에 FBACK 메시지를 받은 경우를 나타내고 있다.

(그림 5), (그림 6)에 적용된 번호(①~③)는 빠른 핸드오버 및 인증의 완료 시간을 나타낸 것이다. 완료시간을 통해 제안 기법의 절차가 지연을 줄이는 것을 알 수 있다. 특히, 그림 6 빠른 핸드오버에서의 reactive 모드의 경우로서, 제안 기법은 비교모델들보다 더 빠른 인증 완료를 수행하기 때문에 통신 연속성이 유지된다.

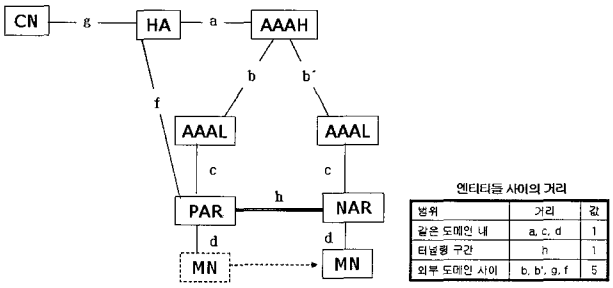
4. 성능 평가

4.1 제안 모델의 비용 분석 및 비교

본 논문은 성능 평가를 위해 참조문헌 [11]의 접근 방법을 참조하였다.

〈표 1〉 성능평가의 수식 계산을 위해 정의한 변수들이다. 참고문헌 [11]을 참조

λ	MN에게 전송되는 데이터 패킷비율
μ	MN이 다른 서브네트워크로 이동할 비율
p	(Packet to mobility ratio: $p=\lambda/\mu$) MN이이동할 때마다 CN으로부터 수신하는 평균 패킷 수
l_c	제어 패킷의 평균길이(200 byte)
l_d	데이터 패킷의 평균길이(1024 byte)
l	$l=l_d/l_c$
r	한 노드에서 제어패킷을 처리하는데 드는 평균 비용



(그림 7) 비용 분석을 위한 시스템 모델을 나타내고 있다.

<표 1>은 본 논문의 성능평가를 위해 정의한 변수들을 나타내었다[11]. (그림 7)에서는 각 엔티티 사이의 거리 값을 나타내었다. 또한 각 홉에서의 메시지 처리 비용은 동일하다고 가정한다.

본 연구에서는 두 가지의 비교 대상 모델들과 제안모델의 비용 분석을 통해 성능평가를 실시한다. 성능 평가 과정에서 빠른 핸드오버·실패는 고려하지 않는다. 두 가지 비교 대상 중 첫 번째는 빠른 핸드오버와 Dupont AAA 기법을 순차적으로 수행한 것이고, 두 번째는 참고문헌 [10]에서 제안한 형태이다.

첫 번째 비교대상(순차적 수행)의 비용 분석:

노드가 서브넷을 이동할 때, 전체 비용을 (수식 1)에 의해서 C_{total}로 정의한다.

$$C_{total} = C_{signal} + C_{packet} \qquad \text{(수식 1)}$$

(수식 2)는 노드가 이동 했을 때, 이동노드가 등록메시지를 보낼 때까지의 시그널링 비용이며 C_{signal}로 정의한다.

$$C_{signal} = M_{fast} + M_{AAA} + m = 2(a+b'+c)+10d+3h+m+18r \qquad \text{(수식 2)}$$

(수식 2)에서 M_{fast}와 M_{AAA}는 빠른 핸드오버와 AAA 인증 절차로 인한 시그널링 비용이다. 그리고 m은 이동노드가 홈 에이전트에 등록하기 위해 수행하는 메시지 절차 비용이다. 패킷 비용은 (수식 3)에 정의되어 있고, C_{packet}으로 정의한다. (수식 3)의 패킷 비용은 손실 비용(C_{loss})과 포워딩 비용(C_{fwd})의 합으로 나타낸다. 본 연구는 빠른 핸드오버의 실패를 고려하지 않으므로, 손실비용은 계산과정에서 제외한다. 포워딩 비용을 계산하기 위해서, 지연 시간인 t_{delay}와 단일 데이터 패킷 비용 C_{dt}를 고려한다.

$$C_{packet} = C_{fwd} + C_{loss} = (\lambda \times t_{delay} \times C_{dt}) + C_{loss} \qquad \text{(수식 3)}$$

(수식 4)의 t_{delay}는 이전 접속 라우터가 FBU 메시지를 받은 시점부터 인증 완료까지의 포워딩 지연시간이다. 이 값은 패킷의 지연시간이므로 이 값의 비교를 통해 인증 완료까지 지연 차이를 알 수 있다.

$$t_{delay} = 2(t_a + t_{b'} + t_c) + 7t_d + 3t_h + 15t_r + t_{L2} + t_m \qquad \text{(수식 4)}$$

(수식 4)의 t_{delay}는 L2 핸드오버의 지연 시간(t_{L2})와 홉 간의 이동시간(t_x) 그리고 호스트에서의 패킷 처리시간(t_r)로 계산한다. (홉 간의 이동시간 t_x에서 χ는 홉 간의 거리 변수를 의미한다.)

$t_x \le t_r$로 가정한다.

(수식 5)의 C_{dt}는 CN에서 이동노드로 전달되는 단일 데이터의 패킷 비용을 의미한다.

$$C_{dt} = l(g+f+h+d)+3r \qquad \text{(수식 5)}$$

따라서 이동노드가 빠른 핸드오버와 Dupont AAA를 순차적으로 수행한 경우의 전체 비용은 아래와 같다.

$$C_{total} = 2(a+b'+c)+10d+3h+m+18r + (\lambda \times t_{delay} \times C_{dt}) + C_{loss} \qquad \text{(수식 6)}$$

두 번째 비교대상(참고문헌 [10])의 비용 분석 및 첫 번째 대상과의 비용 비교:

비용분석 과정에서 본 논문은 전체 비용 패킷 전송비용과 시그널링 비용으로 나눈다. 특히 참고문헌 [12]를 통해 시그널링 비용은 패킷 전송비용에 비해 매우 작다고 정하고, 전체 패킷 비용의 비교는 패킷 전송의 지연시간을 중심으로 수행한다.

노드가 새로운 서브넷으로 이동전에 FBACK 메시지를 받았을 경우와 받지 못했을 경우로 나뉜다.

참고문헌 [10]에서 제안한 형태로서, 크게 두 가지로 나뉜다.

-FBACK 메시지를 받았을 경우(predictive),

$$t_{delay-p} = 2t_d + 3t_h + 4t_r + \mathrm{MAX}\{\, 2(t_a + t_{b'} + t_c) + t_d + 7t_r), \; (t_{L2} + 2t_d + 2t_r)\,\} + t_m \qquad \text{(수식 7)}$$

(수식 7)에서 지연시간은 상황에 따라 두 값 중 선택한다. 즉, AReq 전송부터 ARsp 수신까지의 지연을 AAA 인증 절차 $2(t_a + t_{b'} + t_c) + t_d + 7t_r$와 L2 Handoff시간 $(t_{L2} + 2t_d + 2t_r)$ 중 큰 값으로 한다.

-FBACK메시지를 못 받았을 경우(reactive),

$$t_{delay-a} = 2(t_a + t_{b'} + t_c + 2t_d) + 3t_h + 13t_r + t_{L2} + t_m \quad \text{(수식 8)}$$

(수식 8)은 빠른 핸드오버의 reactive 모드 일 경우에서의 지연시간이다.

따라서 참고문헌 [10]의 기법과 순차 수행시의 전체 패킷 비용 비교는 (수식 9)와 (수식 10)으로 나타낸다.

비교 대상간의 인증 완료까지의 지연 시간 비교

$$\text{Predictive}: t_{delay} - t_{delay-p} = 4t_d + 4t_r + t_{L2} \quad \text{(수식 9)}$$

$$\text{Reactive}: t_{delay} - t_{delay-a} = 3t_d + 2t_r \quad \text{(수식 10)}$$

비교 결과 참고문헌 [10]의 기법이 (수식 9)와 (수식 10)과 같이 지연을 줄인다.

제안 기법의 비용 분석 및 두 번째 대상과의 비용 비교: 제안 기법에서는 이동노드가 생성하는 H_value 인증 값에 대해 이전 접속 라우터와 새로운 접속 라우터에서의 별도의 비용이 필요하다. 본 논문에서는 이 비용 역시 r로 정의한다. 따라서 제안 기법에서는 패킷 처리 비용을 $2r$로 한다. 제안 기법의 비용 분석도 이동노드에 대해 FBACK 메시지를 받은 경우인 (수식 11)과 받지 못한 경우인 (수식 12)로 나뉜다.

-FBACK 메시지를 받았을 경우(predictive),

$$t_{delay-p-sug} = 3t_d + 2t_h + 7t_r + t_{L2} + t_m \quad \text{(수식 11)}$$

-FBACK메시지를 받지 못했을 경우(reactive),

$$t_{delay-a-sug} = 2t_d + 3t_h + 7t_r + t_{L2} + t_m \quad \text{(수식 12)}$$

제안 기법과 참고문헌 [10]의 기법의 전체 패킷 비용 비교는 (수식 13)과 (수식 14)로 나타낸다.

참고문헌 [10]의 기법과 제안 기법과의 지연 비교

$$\text{Predictive}: t_{delay-p} - t_{delay-p-sug} = t_d + t_h - t_r \quad \text{(수식 13)}$$

$$\text{Reactive}: t_{delay-a} - t_{delay-a-sug} = 2(t_a + t_{b'} + t_c + t_d) + 6t_r \quad \text{(수식 14)}$$

비교 결과 제안 기법이 참고문헌 [10]의 기법보다 지연을 줄인다.

4.2 제안 기법의 성능 평가

제안 기법의 성능평가를 위해 참조문헌 [11]을 통해 얻은 4.1의 파라미터들과 참조문헌 [12]를 통해 얻은 L2 핸드오버로 인한 지연시간(t_{L2}=84 msec) 및 각 노드에서의 시그널링 메시지 처리시간(t_r=0.5 msec)을 사용한다.

성능평가는 핸드오버시, 일반적인 방법의 전체 비용에 대해 제안 기법의 전체 비용 비율로 구한다. (수식 15)와 (수식 16)은 빠른 핸드오버의 두 가지 모드에 따라 비율을 구한 것이다.

-FBACK 메시지를 받았을 경우 (predictive):

$$\lim_{p\to\infty} \frac{C_{total-sug-p}}{C_{total}} = \lim_{p\to\infty} \frac{C_{signal-sug-p} + (\lambda \times t_{delay-sug-p} \times C_{dt-sug-p}) + C_{loss-sug-p}}{C_{signal} + (\lambda \times t_{delay} \times C_{dt}) + C_{loss}}$$

$$= \lim_{p\to\infty} \frac{C_{signal-sug-p} + (p \times \mu \times t_{delay-sug-p} \times C_{dt-sug-p}) + C_{loss-sug-p}}{C_{signa} + (p \times \mu \times t_{delay} \times C_{dt}) + C_{loss}} \quad \text{(수식 15)}$$

-FBACK 메시지를 받지 못했을 경우 (reactive):

$$\lim_{p\to\infty} \frac{C_{total-sug-a}}{C_{total}} = \lim_{p\to\infty} \frac{C_{signal-sug-a} + (\lambda \times t_{delay-sug-a} \times C_{dt-sug-a}) + C_{loss-sug-a}}{C_{signal} + (\lambda \times t_{delay} \times C_{dt}) + C_{loss}}$$

$$= \lim_{p\to\infty} \frac{C_{signal-sug-a} + (p \times \mu \times t_{delay-sug-a} \times C_{dt-sug-a}) + C_{loss-sug-a}}{C_{signa} + (p \times \mu \times t_{delay} \times C_{dt}) + C_{loss}} \quad \text{(수식 16)}$$

(수식 15)와 (수식 16)에서 $\lambda = p \times \mu$ (표 1. p=λ/μ)이고, μ를 얻기 위해 참고문헌 [11]에서 적용된 uniform fluid model을 사용한다. uniform fluid model은 네트워크 흐름의 평균 지연, 손실률, 처리량 등을 결정 및 분석 하기위해 제안된 빠르고 효율적인 모델이다[13]. 이동성 측정을 위해 제안된 방안으로 모델에서 보행속도는 $\mu = 0.01$(3.6 km/h), 차량속도는 $\mu = 0.2$(72 km/h) 의 비율로 이동한다고 한다. 그리고 지연시간을 계산하기 위해, 라운드 트립 시간 분석 곡선 결과를 사용한다. 즉, 유선 구간에서의 지연은 (수식 17)로, 무선 구간에서는 (수식 18)의 식을 통해 얻는다.

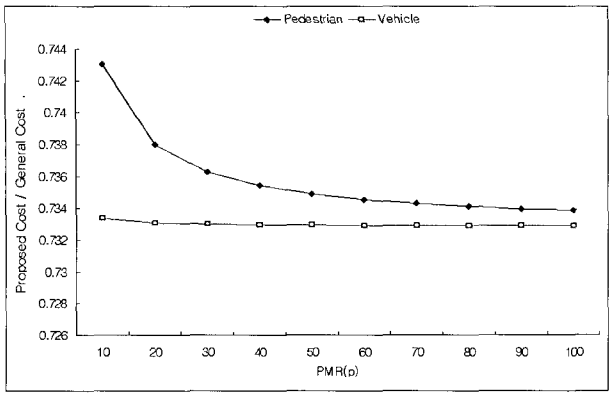
$$t_{RT-wire}(h,k) = 3.63k + 3.21(h-1) \text{ (msec)} \quad \text{(수식 17)}$$

$$t_{RT-wireless}(k) = 17.1k \text{ (msec)} \quad \text{(수식 18)}$$

k는 패킷의 크기(kbyte)를 나타내며, h는 이동한 홉 수를 나타낸다.

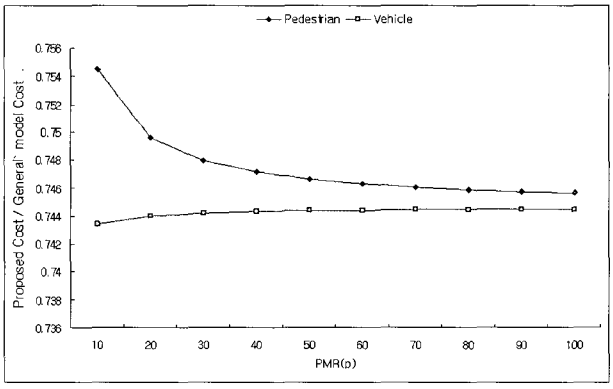
제안된 모델과 일반적인 모델의 전체 비용에 대한 비율을 PMR 값의 증가에 따라 (그림 8), (그림 9), (그림 10)의 그래프로 나타내었다. "x 축 PMR(p)은 Packet to Mobility Ratio: p=λ/μ로 정의[11]."

(그림 8), (그림 9), (그림 10)에서 PMR이 $p > 100$ 인 경우, 비용 비율은 수렴 값에 도달하게 된다.



(그림 8) 빠른 핸드오버의 predictive 모드에서, x 축인 PMR 값의 증가에 따라 (수식 15) 통해 얻은 비율 결과를 나타낸 그래프이다. (보행속도 $\mu = 0.01$, 차량속도 $\mu = 0.2$)

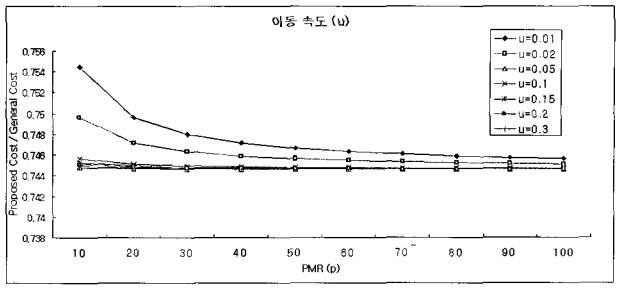
(그림 8) 그래프의 결과로서, 빠른 핸드오버의 predictive 모드에서 보행자와 차량의 이동 속도에 대해 일반적인 방법의 전체 비용 대 제안 기법의 전체 비용 비율은 0.735값에 수렴한다. 즉 제안 기법이 빠른 핸드오버와 Dupont AAA 기법을 순차적으로 수행한 것에 비해 약 27%의 비용절감 효과를 얻는다.



(그림 9) 빠른 핸드오버의 reactive 모드에서, x 축인 PMR 값의 증가에 따라 (수식 16) 통해 얻은 비율 결과를 나타낸 그래프이다. (보행속도 $\mu = 0.01$, 차량속도 $\mu = 0.2$)

(그림 9) 그래프의 결과로서, 빠른 핸드오버의 reactive 모드에서 보행자와 차량의 이동 속도에 대해 일반적인 방법의 전체 비용 대 제안 기법의 전체 비용 비율은 0.746값에 수렴한다. 즉 제안 기법이 빠른 핸드오버와 Dupont AAA 기법을 순차적으로 수행한 것에 비해 약 25%의 비용절감 효과를 얻는다.

(그림 10)은 빠른 핸드오버의 reactive 모드에서 여러 이동 속도에 따른 수렴 값들을 나타내었다. 그래프의 결과로서, 이동 속도에 대해 일반적인 방법의 전체 비용에 대해 제안 기법의 전체 비용 비율은 0.747값에 수렴한다. 즉 제안 기법이 빠른 핸드오버와 Dupont AAA 기법을 순차적으로 수행한 것에 비해 약 25%의 비용절감 효과를 얻는다.



(그림 10) 빠른 핸드오버의 reactive 모드에서, x 축인 PMR 값의 증가에 따라 (수식 16) 통해 얻은 비율 결과들을 나타낸 그래프이다. (이동속도 $\mu = 0.01 \sim 0.3$)

5. 결 론

통신 이용자들은 통신의 안정성 뿐 만아니라 통신의 실시간성까지 요구하고 있다. 하지만 이 두 가지의 특성을 동시에 실현하기는 어렵다. 왜냐하면 노드가 서브넷을 이동할 때, 인증 과정으로 발생하는 지연이 실시간 통신에 부담을 주는 요소이기 때문이다. 지연을 줄이고 실시간 통신을 가능하게 하기 위해, 본 논문에서는 이동노드가 생성하는 해쉬 값을 이용한 효율적인 인증 기법을 제안한다. 제안 기법을 통해 생성된 해쉬 값인 H_value는 인증 키 역할을 하고, H_value를 통한 인증으로 이동노드는 이전 접속 라우터와 맺고 있던 기존 인증 협약을 새로운 접속 라우터까지 연장한다. 결과 새로운 인증 협약 설정 과정에서 발생하는 지연은 사라지고, 새로운 접속 라우터의 신뢰를 보장한다. 성능 평가는 제안 기법의 비용과 빠른 핸드오버에 Dupont AAA 기법을 순차적으로 수행한 것의 비용을 비교함으로써 수행하였다. 성능 평가를 통해, 빠른 핸드오버의 predictive 상황에서는 약 27% reactive 상황에서는 약 25%의 지연 감소를 얻는다.

본 논문의 제안기법은 지연을 줄이지만, 추가적인 처리비용을 야기한다. 하지만 일반 통신에서 지연으로 발생하는 패킷 손실과 그로인한 패킷 재전송의 손실비용이 크기 때문에 라우터에서의 계산 및 비교에 의한 추가적인 처리비용은 손실 비용에 비해 상대적으로 작다. 하지만 제안 기법의 간단한 인증 방식과 이전 인증협약의 재사용은 보안 위협의 원인이 될 수 있으므로 추가적인 보안 관련 연구가 필요하다.

참 고 문 헌

[1] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December, 1998.

[2] Charles E. Perkins and David B. Johnson, "Mobility Support in IPv6", RFC 3775, June, 2004.

[3] J. Arkko, V. Devarapalli, F. Dupont, "Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June, 2004.

[4] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November, 1998.
[5] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November, 1998.
[6] M. Faccin, E. Perkins, and etc. "Mobile IPv6 Authentication, Authorization, and Accounting Requirements", Internet Draft, draft-le-aaa-mipv6-requirements-03.txt, February, 2004.
[7] P. Flykt, C. Perkins, T. Eklund, "AAA for IPv6 Network Access", Internet Draft, draft-perkins-ietf-aaav6-05.txt, May, 2003.
[8] Francis Dupont "AAA for mobile IPv6", Internet Draft, draft-dupont-mipv6-aaa-01.txt, November, 2001.
[9] R. Koodli et al, "Fast Handovers for Mobile IPv6",RFC 4068, July, 2005.
[10] Changnam Kim, Youngsong Mun and etc, "Performance Improvement in Mobile IPv6 Using AAA and Fast Handoff", Lecture Notes in Computer Science 3043, pp. 738-745, June, 2004.
[11] R. Jain, T.Raleigh and C, Graff, M. Bereschinsky, "Mobile Internet Access and Qos Guarantees using Mobile IP and RSVP with Local Register," in Proc. ICC'98 Conf,. pp.690~1695, Atlanta.
[12] Jon-Olov Vatn, "An experimental study of IEEE 802.11b handover performance and its effect on voice traffic", SE Telecommunication Systems Laboratory Department of Microelectronics and Information Technology (IMIT), July, 2003.
[13] http://www-net.cs.umass.edu/fluid

강 형 모

e-mail : kangzzang@sunny.ssu.ac.kr
2005년 숭실대학교 컴퓨터학부(학사)
2005년~현재 숭실대학교 컴퓨터 석사(재학중)
관심분야 : Mobile IPv6, IPv6 Security, Grid networking

문 영 성

e-mail : mun@computing.ssu.ac.kr
1983년 연세대학교 전자공학과(학사)
1986년 알버타대학교 대학원 전자공학과(공학석사)
1987~1994년 한국통신 연구원
1993년 텍사스대학교 대학원 컴퓨터공학과(공학박사)
1994~현재 숭실대학교 컴퓨터학부 부교수
관심분야 : Mobile IPv6, IPv6, IPv6 Security, Grid networking