Mobile IPv6에서 Fast Handoff 기법을 이용한 AAA 인증 성능 향상 방안

(A Method of Performance Improvement for AAA Authentication using Fast Handoff Scheme in Mobile IPv6)

김 창 남 † 문 영 성 †† 허 의 남 †††
(Changnam Kim) (Youngsong Mun) (Eui-Nam Huh)

요 약 본 논문에서는 이동노드의 글로벌 이동성을 제공하기 위한 방법으로 AAA(Authentication, Authorization and Account) 서비스 기반의 보안 인증 모델을 정의하고 AAA 인증 절차에서 발생하는 서비스 지연 시간을 최소화하기 위해 Mobile IP 작업 그룹에서 정의하고 있는 Fast Handoff를 적용하였다. 즉, 이동노드의 로밍이 발생하는 경우 Fast Handoff 절차가 진행되면서 동시에 AAA 인증 절차를 수행함으로써 이동노드 인증 시간을 줄이고 신속한 로밍 및 서비스 제공이 가능하도록 하였다. IPsec (Internet Protocol Security), RR(Return Routability), AAA를 기반으로 한 기존의 방식들은 이동노드의 Layer2 Handoff가 성공적으로 처리된 후에 발생하는 인증 절차를 정의하고 있는데 이 절차가 수행되는 동안은 이동 노드의 서비스가 지연되므로 실시간, 고품질의 서비스를 만족하기 위해서는 이를 줄일 수 있는 방안이 연구되어야 한다. 본 논문에서 제안한 방법은 이러한 목적을 만족하기 위한 것으로써 제안된 방식을 사용했을 때 Layer2 Handoff 전에 이동 노드가 FBACK(Fast Binding Acknowledge) 메시지를 받은 경우 최대 55%, 받지 못한 경우 최대 17%의 성능 향상을 보인다.

키워드 : Mobile IPv6, AAA, Fast 핸드오프

Abstract In this paper, we define the secure authentication model to provide a mobile node with global roaming service and integrate the Fast Handoff scheme with our approach to minimize the service latency. By starting the AAA(Authentication, Authorization and Account) procedure with Fast Handoff simultaneously when a roaming occurs, authentication latency is reduced significantly and provision of fast and seamless service is possible. The previous works such as IPsec(Internet Protocol Security), RR (Return Routability) and AAA define the procedures performed after the completion of Layer2 Handoff which leads us to study a way of providing the real time and QoS guaranteed service during this period. The proposed scheme is for this goal and when appling it to roaming environment it shows the cost reduction up to 55% and 17% for the case of the MN receiving the FBACK and not respectively before L2 Handoff occurs.

Key words : Mobile IPv6, AAA, Fast Handoff

1. 서 론

핸드폰, PDA, 노트북 등의 이동 단말의 빠른 발전과 증가로 인해서 무선 상에서의 사용자들이 이동 중에도 안전하게 끊어짐 없이 서비스를 받을 수 있도록 하기 위한 기술이 큰 관건이다[1]. 현재 표준화 기구인 IETF의 mobileip 작업 그룹에서도 가장 중요하게 다루고 있는 문제가 Mobile IPv6에서의 보안이다.

Mobile IPv6에서 보안을 위해 IPsec과 RR 절차가 제안되었다[1]. IPsec만을 사용하는 경우 이동 단말과 홈 도메인의 홈 에이전트 간에 SA(Security Association)를 설정하고 메시지를 인증할 수 있지만, 만일 이동 단말이 로밍을 하고 있는 경우, 즉 방문 망에서 이동 서비스를 받고자 하는 경우 이동 단말은 방문 망에서 네트워크로 접속할 수 있는 권한을 인증 받아야 한다

· 본 논문은 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신 기초기술연구지원사업의 연구결과물입니다(03-기초-0074).
† 정 회 원 : 니츠 연구원
cnkim@nitz.co.kr
†† 종신회원 : 숭실대학교 컴퓨터학부 교수
mun@computing.ssu.ac.kr
††† 비 회 원 : 서울여자대학교 컴퓨터학부 교수
huh@swu.ac.kr
논문접수 : 2004년 1월 27일
심사완료 : 2004년 9월 6일

[2,3]. 그러나 IPsec에서는 홈 망에서 방문 망으로 이동한 이동 단말이 실제로 홈 망에서 등록된 단말 인지를 판단할 수 없다는 단점을 가지고 있다. 또한 IPsec의 사용은 패킷 송수신자 간에 패킷 처리에 관해서 SA Lookup과정, SN(Sequence Number) 생성과정, 페이로드 암호화 과정, ICV(Integrity Check Vector) 계산 과정 등의 추가적인 부담을 요구한다. 하드웨어적으로 성능이 미약한 핸드폰이나 PDA에서 IPsec을 처리하기에는 처리 부담이 클 수 있다는 취약성을 가질 수 있다. 또한 표준 워킹 그룹에서 최종 방안으로 RR절차를 사용하기로 결정 하였는데, RR 절차는 홈 에이전트를 통한 터널링과 직접 전송의 두 가지 경로가 노출되는 경우 쉽게 키를 유출 당할 수가 있어 보안 강도가 낮다는 단점을 가지고 있다.

기존의 보안 기법들의 취약성을 극복하기 위한 방안으로 표준 작업 그룹에서는 인프라 차원에서 AAA 인증 절차를 이용하여 이동 단말을 인증하기 위한 방안이 중요한 이슈가 되고 있다[4,5].

현재 mobileip 작업 그룹에서는 Mobile IPv6에 AAA를 적용한 제안 모델들이 많이 제안되어지고 있는데, AAA는 Diameter기반의 구조로 많은 연구들이 진행되고 있다[6-8]. Diameter는 PPP(Point-to-Point Protocol) 같은 기존의 기술 및 Mobile IP등의 새로운 기술에 대한 AAA 서비스를 제공하기 위한 가벼우면서도 확장이 가능한 peer 기반의 AAA프로토콜이다.

[6]에서 제안한 방법은 바인딩 갱신절차를 인증 과정 안에 포함시키고 인증과 바인딩 등록이 동시에 완료 되도록 함으로써 메시지 교환양을 줄일 수 있지만 인증 진행 중에 이동 노드의 위치정보를 포함시키므로 이는 중요한 보안 위협 요인이 될 수 있다. 따라서 본 연구에서는 Francis Dupont[7]의 모델을 기반으로 Fast Handoff를 적용하여 인증 지연 시간과 패킷 손실을 줄이기 위한 모델을 제안하여 성능 평가를 하였다. 논문의 구성은 다음과 같다. 2장에서는 Mobile IPv6에서의 AAA인증 방법, Fast Handoff 방법을 기술하며, 3장에서는 논문에서 제안하는 모델 및 메시지 절차를 기술한다. 4장에서는 제안된 방식에 대한 비용 분석 및 성능평가를 기술하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 Mobile IPv6를 위한 AAA 인증

본 절에서는 "AAA for Mobile IPv6"[7] 문서를 통해 Francis Dupont이 제안한 AAA 인증 방법에 관해 논의한다.

Mobile IPv6 시그널링(바인딩 갱신 및 바인딩 응답) 이전에 행해지는 키 분배를 위한 프로토콜인 IKE (Internet Key Exchange) 교환 성능이 이동 환경에서 기대에 못 미치는 것으로 실험적으로 보고됨에 따라 Dupont은 AAA 인프라 구조와의 결합된 방법을 통해 해결책을 제시하고 있다. 그림 1은 이동 노드를 위한 AAA 인증 및 바인딩 절차이다.

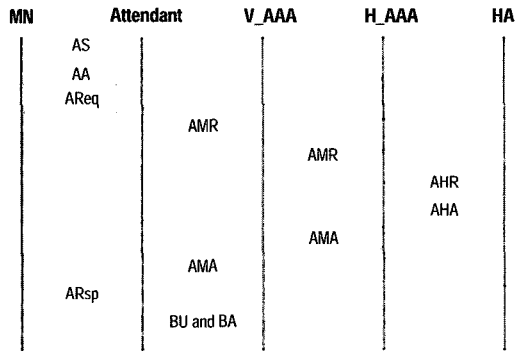

그림 1 AAA인증 및 바인딩 절차

이동 노드가 자신의 IPv6 주소를 설정하고 Attendant를 발견한 후(AS: Attendant Solicitation, AA: Attendant Advertisement) 인증을 요청한다(AReq : Authentication Request). Attendant는 이동노드로부터 수신된 인증 정보를 로컬 AAA 서버로 전달한다(AMR : Authentication MN-Request). 로컬 AAA 서버(V_AAA)는 그 요청 메시지를 AAA 프로토콜로 변환해서 H_AAA 서버로 전달하고, 이때 V_AAA과 H_AAA간에는 사전 협의에 의한 로밍 계약이 체결되어 있어야 한다. H_AAA 서버는 홈 에이전트로 메시지를 전달(AHR : Authentication HA-Request)한 후, 이 메시지를 받은 홈 에이전트는 이동노드로부터 온 메시지임을 인증하고 클라이언트와 홈 에이전트 간에 미리 구성된 키를 바탕으로 이동 노드와 attendant간에 사용될 세션 키를 생성한 후 키 및 키 생성 재료를 리턴(AHA: Authentication HA-ACK)한다. H_AAA 서버는 V_AAA로 응답 메시지를 전달(AMA: Authentication MN- ACK)하고 attendant는 세션 키를 저장하고 키 생성 재료를 이동 노드로 전송(ARsp: Authentication Response)한다. 이 절차가 끝나면 이동 단말은 홈 에이전트에게 홈 등록(BU/BA)을 한다.

2.2 Fast Handoff

Mobile IPv6에서 Fast Handoff는 핸드오프 시 발생할 수 있는 지연이 실시간 또는 지연에 민감한 트래픽에서 받아들일 수 없는 상황인 경우 이러한 지연을 최소화 시킬 수 있는 방법을 제시한다. 그림 2는 Fast Handoff의 메시지 절차를 나타낸다[9].

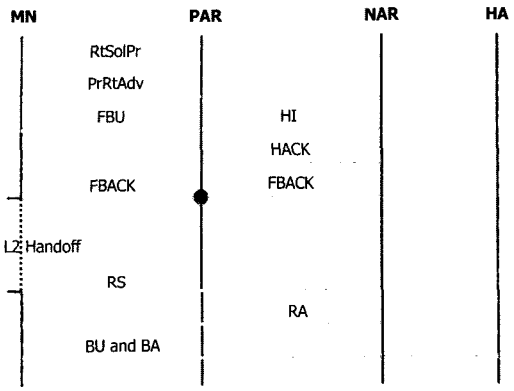

그림 2 Fast Handoff 메시지 절차

이동 단말이 새로이 이동할 AR(Access Router)에 대한 정보를 가지고 있거나 또는 새로운 서브넷으로 핸드오프 할 것을 결정하였다면 Previous AR로 RtSolPr (Router Solicitation for Proxy) 메시지를 보내고 이에 대한 응답으로 PrRtAdv(Proxy Router Advertisement) 메시지를 받는다. 이 메시지는 새로운 서브넷에서 new CoA(Care of Address)를 구성하기 위해 이동 단말에 필요한 서브넷 프리픽스와 같은 3계층 정보를 이동 노드에게 제공한다. PrRtAdv 메시지를 받은 이동 단말은 NAR에게 L2 Handoff가 발생하기 전에 PAR에게 FBU(Fast Binding Update) 메시지를 보낸다.

FBU 메시지를 받은 PAR은 터널 설정을 하기 위해서 HI(Handover Initiate) 메시지를 NAR에게 보내는데, 이때 HI 메시지는 두 가지 의미를 포함한다. 첫째는 두 AR 사이에 터널을 설정하기 위한 초기 메시지이고, 둘째는 이동 단말이 PAR로부터 받은 new CoA가 정당한 것인지를 검사하는 메시지이다. HI 메시지가 NAR에서 처리 되면 NAR은 HACK(Handover Acknowledge) 메시지로 응답하게 된다. PAR이 HACK 메시지를 받은 후에 이동 단말에게 FBACK(Fast Binding Acknowledge) 메시지를 보내게 된다. FBACK 메시지를 받은 이동 단말은 new COA를 사용하게 된다. 이동 단말이 NAR의 링크로 이동하게 되면 RS(Router Solicitation) 메시지와 RA(Router Advertisement) 메시지를 주고받은 후에 바인딩 갱신이 이루어지고 NAR에 버퍼링 되었던 패킷들을 전달하게 된다.

3. Fast Handoff를 이용한 모델 제안

3.1 Fast Handoff가 적용된 시스템 모델

AAA의 인증 절차로 인한 처리 부하를 줄이기 위한 방안으로 Fast Handoff를 적용한 방식을 제안 하였다. 모델 제안을 위해서 모든 Access Router들은 Attendant의 역할을 지원해야 하고, AAA와 Fast Handoff의

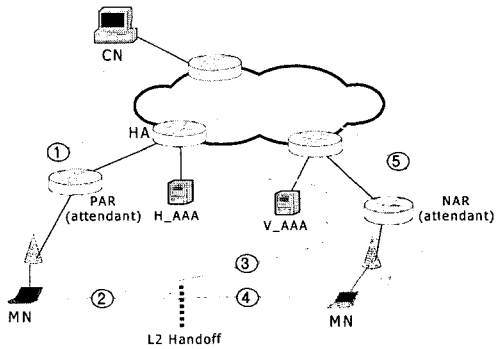

그림 3 제안된 시스템 모델의 동작 절차

표준 문서의 역할을 따른다. 제안된 모델은 Fast Handoff를 적용함으로써 패킷 손실을 줄일 수 있고, 인증 지연 시간을 줄일 수 있다는 장점이 있다. 그림 3은 Fast Handoff가 적용된 제안된 모델의 동작 절차를 위한 시스템 모델이다.

이동 단말과 상대 노드가 통신 중에 이동 단말이 이동을 시작하게 되면 Fast Handoff의 동작이 수행된다. 이때 Fast Handoff 동작 절차가 시작되면 AAA 인증 절차도 수행 할 수 있도록 제안한 방식이다. L2 Handoff가 발생하기 전에 몇몇 AAA 인증 절차가 수행되었기 때문에 이동 단말이 이동을 마치면 나머지 AAA 인증 절차만을 수행함으로써 인증 절차로 인한 지연시간을 줄일 수 있다.

이렇게 인증을 마치게 되면 이동 단말은 홈 에이전트에게 BU(Binding Update) 메시지를 보냄으로써 홈 에이전트의 바인딩을 갱신 할 수 있다.

3.2 제안된 모델의 메시지 절차

제안된 메시지 절차는 FBACK 메시지를 MN이 받을 경우와 받지 못할 경우로 나누어서 제안 하였다. 그림 4는 FBACK 메시지를 MN이 받을 경우의 메시지 절차이다.

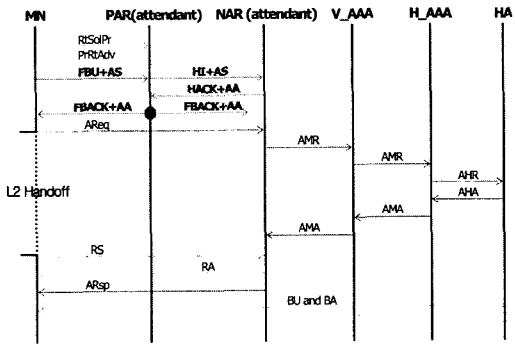

그림 4 MN이 FBACK 메시지를 수신한 경우

MN이 이동을 시작하면 Fast Handoff 동작이 수행되는데, 터널설정과 MN이 획득한 new CoA를 확인하기 위해 FBU 메시지를 PAR(Previous Access Router)에게 보내게 된다. 이때 제안된 방법으로 FBU 메시지에 AAA 메시지 절차인 AS 메시지를 포함해서 보냄으로써 AAA 인증 절차를 Handoff가 발생하기 전에 시작할 수 있다. AS 메시지가 포함된 FBU 메시지를 받은 PAR은 HI 메시지에 AS 메시지를 포함해서 보내는 기능을 수행할 수 있어야한다. HI 메시지를 받은 NAR (New Access Router)은 HI 메시지와 AS 메시지를 처리한 후, HI의 응답 메시지인 HACK 메시지에 AA 메시지를 포함해서 보내게 된다. 이때 터널 설정이 이루어지고 HACK 메시지를 받은 PAR은 FBACK 메시지에 AA 메시지를 포함해서 보내는 기능을 수행할 수 있어야한다. FBACK 메시지를 받은 MN은 AAA 인증 요청 메시지인 AReq 메시지를 보냄으로써 AAA 인증절차를 수행시킬 수 있다. 즉, L2 Handoff와 RS, RA 메시지가 수행되는 동안에 AAA 인증 절차가 수행됨으로써 MN이 이동한 후에 나머지 AAA 인증 절차만 수행함으로써 인증 절차로 인한 지연 시간을 줄일 수 있다.

그림 5는 FBACK 메시지를 MN이 받지 못했을 경우에 대한 제안 절차이다. 이 경우에 FBACK 메시지를 보낼 때까지의 절차는 그림 4의 절차와 같다. 하지만 FBACK 메시지를 MN이 받지 못했을 경우에 MN이 AA 메시지를 받을 수 없게 되고 L2 Handoff가 발생하기 전에 AReq 메시지를 보낼 수 없게 된다. 그러므로 L2 Handoff가 발생한 후 RS 메시지를 MN에게 보내고 이에 대한 응답 메시지인 RA 메시지에 AA 메시지를 포함해서 보냄으로써 AAA 인증 요청 메시지인 AReq 메시지를 보내게 된다. 이동 단말에 대한 인증 절차가 끝나면 바인딩 갱신 메시지를 보냄으로써 홈 에이전트의 바인딩을 갱신할 수 있다.

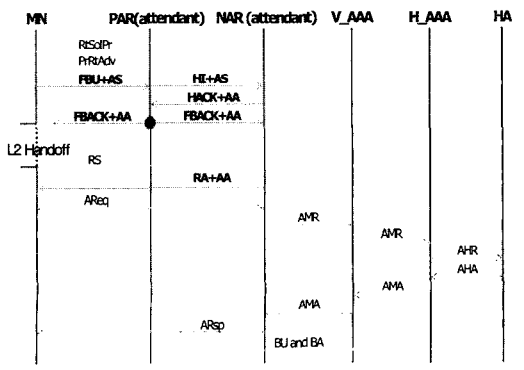

그림 5 MN이 FBACK 메시지를 받지 못했을 경우

4. 성능평가

제안된 구조의 성능 분석을 위한 모델은 그림 6과 같으며 이는 MN이 새로운 도메인으로 이동시에 Fast Handoff방법을 적용해서 AAA인증을 완료하기 위한 각 엔티티 및 엔티티 간의 거리를 보여 준다. 네모 상자로 표시된 것은 제안 인증 방식에 참여하는 엔티티를 나타내며 각 엔티티들은 메시지 흐름 절차에 의해 실선으로 연결되고 각 엔티티 간 연결에 대해서는 링크상의 거리를 나타내는 가중치 값을 표시한다.

λ와 μ를 각각 데이타 패킷의 평균 수신율과 노드의 이동 비율로 정의하며 이때 CN은 λ 비율로 MN에게 데이타 패킷을 전송하고, MN은 μ 비율로 다른 도메인으로 이동한다고 가정한다. 본 논문에서는 MN이 이동할 때마다 CN으로부터 수신되는 평균 패킷 수를 Packet to Mobility Ratio (PMR), $\rho=\lambda/\mu$로 정의한다. 제어 패킷의 평균 길이를 l_c라 하고, 데이타 패킷의 평균 길이를 l_d라고 정의하며, 비율은 $l = l_d / l_c$ 라고 정의한다. 이때 제어 패킷을 전송하는 비용은 송신자와 수신자의 거리에 의해 주어지며 데이타 패킷의 전송 비용은 제어 패킷에 비해 평균 l 배 크다고 정의한다. 그리고 한 호스트에서 제어 패킷을 처리하는 평균 비용은 γ 이라고 가정한다.

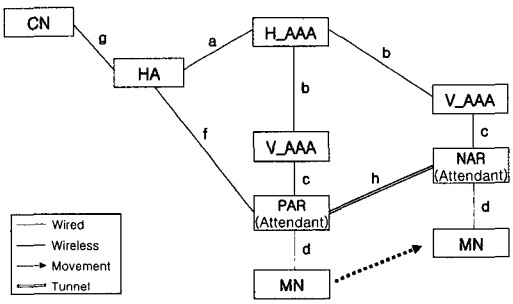

그림 6 비용 분석을 위한 시스템 모델

4.1 성능분석

다음은 본 연구에서 제안된 메시지 절차에 대한 전체 비용을 계산하기 위한 과정으로 FBACK 메시지를 MN이 받았을 경우와 MN이 L2 Handoff 전에 받지 못했을 경우로 나누어서 분석 하였다. Fast Handoff가 적용된 Mobile IPv6에서 MN이 새로운 도메인으로 이동시 발생하는 전체 비용은 (1)에 의해서 C_{total} 로 정의한다.

$$C_{total} = C_{signal} + C_{delivery} \quad (1)$$

MN이 새로운 도메인으로 이동을 시작 했을 때 MN이 등록 메시지를 보낼 때까지의 시그널링 비용은 (2)에 의해서 C_{signal}로 정의한다.

$$C_{signal} = 11a + 2(b + c + d + m) + 17r \quad (2)$$

제안된 절차에서 Packet Delivery Cost는 MN이 FBACK 메시지를 받았을 경우 $C_{delivery-FM}$으로 (3)에 의해서 주어진다.

$$C_{delivery-FM} = (\lambda \times t_{delay-FM} \times C_{dt-FM}) + C_{loss-FM} \quad (3)$$

본 연구에서는 Fast Handoff가 적용된 Mobile IPv6에서 AAA 인증 절차를 적용해서 지연을 줄이기 위함이 목적이므로 Fast Handoff의 실패율은 고려하지 않았다. 그 외에 패킷 손실 부분은 NAR(New Access Router)에서 터널링된 패킷을 버퍼링 하지 않을 경우에 발생할 수 있다. 이 경우를 위해서 NAR은 HI 메시지를 받으면 버퍼링 기능을 지원하도록 가정한다. 패킷이 포워딩 될 때까지의 지연시간은 (4)에 의해 나타낼 수 있다.

$$t_{delay-FM} = 5t_a + 2t_m + \max\{2(t_b + t_c + t_d) + 6t_r, (t_{L2} + 2t_a + 2t_r)\} + 6t_r \quad (4)$$

식 (4)에서 FBACK 메시지를 받은 MN은 인증요청을 위해 AReq(Authentication Request) 메시지를 NAR에게 보낸 후부터 ARsp(Authentication Response)메시지를 받을 때까지의 지연시간은 AAA 인증 절차 $(2(t_b + t_c + t_d) + 6t_r)$와 L2 Handoff 에 RA와 RS메시지의 지연시간$(t_{L2} + 2t_a + 2t_r)$이 중첩 되므로 지연이 큰 시간을 계산 하였다.

그러므로 Fast Handoff가 적용된 Mobile IPv6에서 AAA인증시 MN이 새로운 도메인으로 이동했을 때 FBack메시지를 MN이 받았을 경우의 전체 비용은 (5)에 의해 나타낼 수 있다.

$$C_{total-FM} = 11a + 2(b + c + d + m) + 17r + (\lambda \times t_{delay-FM} \times C_{dt-FM}) + C_{loss-FM} \quad (5)$$

MN이 FBACK 메시지를 받지 못했을 경우, 제안된 절차에서 Packet Delivery Cost는 $C_{delivery-FP}$으로 (6)에 의해서 주어진다.

$$C_{delivery-FP} = (\lambda \times t_{delay-FP} \times C_{dt-FP}) + C_{loss-FP} \quad (6)$$

패킷이 포워딩 될 때까지의 지연시간은 (7)에 의해 나타낼 수 있다.

$$t_{delay-FP} = 2(3t_a + t_b + t_c + t_d + t_m) + 13t_r + t_{L2} \quad (7)$$

그러므로 Fast Handoff가 적용된 Mobile IPv6에서 AAA 인증시 MN이 새로운 도메인으로 이동했을 때 FBACK 메시지를 MN이 L2 Handoff로 인해서 받지 못했을 경우의 전체 비용은 (8)에 의해 나타낼 수 있다.

$$C_{total-FP} = 11a + 2(b + c + d + m) + 17r + (\lambda \times t_{delay-FP} \times C_{dt-FP}) + C_{loss-FP} \quad (8)$$

4.2 제안된 모델의 성능 평가

모델에 대한 분석을 위해, Fast Handoff가 적용된 Mobile IPv6에서 AAA 인증절차를 이용한 모델에서 일반적인 경우의 모델에 대한 전체 비용과 제안된 절차에 대한 전체 비용을 비율로 나타낼 수 있다. 단일 홉(r=1)에 대한 메시지 처리 비용은 동일하다고 가정하고, 같은 도메인 안에서의 거리 값은 1(a, c, d)이고 두 도메인 간의 거리 값은 2(b, g, f, h, m)으로 가정한다. 그리고 L2 Handoff로 인한 지연시간(t_{L2})은 [10]에 의해서 84 msec로 계산한다. 각 노드에서의 시그널링 메시지 처리 시간(t_r)은 [11]에 의해서 0.5 msec로 처리한다.

새로운 도메인으로 이동시 일반적인 인증절차에 대한 비용과 Fast Handoff가 적용된 인증 절차에 대한 비율은 다음과 같다.

FBACK메시지를 MN이 받았을 경우 :

$$\frac{C_{total-FM}}{C_{total-g}} = \frac{11a + 2(b + c + d + m) + 17r + (\lambda \times t_{delay-FM} \times C_{dt-FM}) + C_{loss-FM}}{13a + 2(b + c + d + m) + 20r + (\lambda \times t_{delay-g} \times C_{dt-g}) + C_{loss-g}} \quad (9)$$

FBACK메시지를 MN이 받지 못했을 경우 :

$$\frac{C_{total-FP}}{C_{total-g}} = \frac{11a + 2(b + c + d + m) + 17r + (\lambda \times t_{delay-FP} \times C_{dt-FP}) + C_{loss-FP}}{13a + 2(b + c + d + m) + 20r + (\lambda \times t_{delay-g} \times C_{dt-g}) + C_{loss-g}} \quad (10)$$

모델 이동성을 나타내기 위해, uniform fluid model을 적용한다. 여기서 서브넷의 평균 크기를 150m로 가정하였을 때 보행 속도(시간당 3마일)로 움직일 때 이동 비율은 μ=0.01 이고 차량의 속도(시간당 60마일)로 움직이는 경우 이동 비율은 μ=0.2 이다[12]. 위의 식에서와 같이 Packet Delivery Cost를 계산할 때 지연시간을 계산하기 위해, 라운드 트립 시간 분석 곡선 결과를 사용한다. 모델의 이동성을 나타내기 위해, Uniform Fluid Model을 적용한다. 이 모델에서 전체 비용 분석을 위해 $C_{total-FM}/C_{total-g}$과 $C_{total-FP}/C_{total-g}$의 비용 율을 도입할 수 있다. PMR이 큰 경우(p>100), 비용 율은 수렴 값에 도달하게 되는데, 이 값은 다음과 같이 얻을 수 있다.

FBack메시지를 MN이 받았을 경우 :

$$\lim_{p \to \infty} \frac{C_{total-FM}}{C_{total-g}} = \lim_{p \to \infty} \frac{C_{signal-FM} + (p \times \mu \times t_{delay-FM} \times C_{dt-FM}) + C_{loss-FM}}{C_{signal-g} + (p \times \mu \times t_{delay-g} \times C_{dt-g}) + C_{loss-g}} \quad (11)$$

$$\fallingdotseq 0.45$$

FBack메시지를 MN이 받지 못했을 경우 :

$$\lim_{p\to\infty}\frac{C_{total-FP}}{C_{total-g}} = \lim_{p\to\infty}\frac{C_{signal-PM}+(p\times\mu\times t_{delay-FP}\times C_{dt-FP})+C_{loss-FP}}{C_{signal-g}+(p\times\mu\times t_{delay-g}\times C_{dt-g})+C_{loss-g}} \fallingdotseq 0.83 \quad (12)$$

다음 그림은 제안된 모델과 일반적인 모델의 전체 비용에 대한 비율을 PMR 값의 증가에 따라 나타낸 그래프이다. FBACK메시지를 MN이 받았을 경우와 받지 못했을 경우에 교통수단(μ=0.2)을 이용 했을때와 도보(μ=0.01)를 이용 했을 때의 시스템 파라메터를 이용하여 나타내었다.

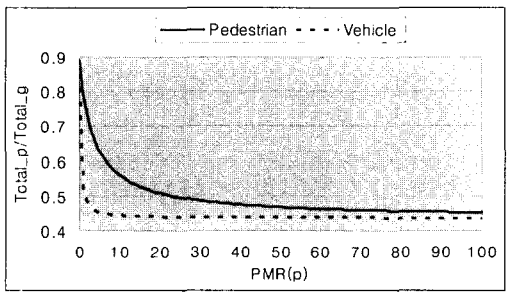

그림 7 FBACK 메시지를 받았을 경우

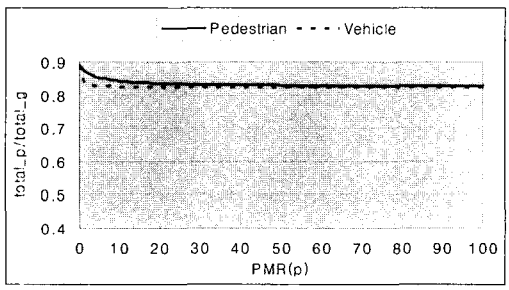

그림 8 FBACK 메시지를 받지 못했을 경우

그림 7에서와 같이 MN이 FBACK 메시지를 받았을 경우에는 PMR 값이 100 이상일 경우에 일정한 값으로 수렴하게 되는데 이때의 값은 0.45의 값에 수렴하게 된다. 따라서 Fast Handoff가 적용된 Mobile IPv6에서의 AAA를 이용한 인증에서 제안된 모델을 사용했을 경우에 55%의 비용 절감을 얻을 수 있다.

다음 그림 8은 MN이 FBACK 메시지를 받지 못했을 경우로서, PMR 값이 100 이상일 경우에 0.83값에 수렴하게 되는 것을 알 수 있다. 따라서 이 경우에는 일반적인 모델에 비해 17%의 비용 절감을 얻을 수 있게 된다.

5. 결 론

현재 무선 환경에서 이동성을 지원하기 위한 대표적인 기술은 2계층(데이타링크 계층)에서 무선 접속을 지원하는 IEEE 802.11의 무선 랜 기술과 3계층(네트워크 계층)에서 이동성을 지원하는 IETF의 Mobile IP 기술이 있다. 무선 랜의 경우 2계층에서 이동성을 지원하기 때문에 하부 기술에 대한 의존성으로 인하여 글로벌 로밍에 어려움이 있다. 이에 반하여 Mobile IP는 3계층에서 이동성을 제공함으로써 하부 기술에 독립적인 이동성을 제공할 수 있기 때문에 IP기반의 차세대 망에서 글로벌 로밍을 쉽게 지원할 수 있을 것으로 예상된다. 그러나 Mobile IP는 이동성 검출, IP 주소 설정, 새로운 도메인에서의 주소 갱신 등을 포함하는 넓은 지역의 이동성 지원을 위해 설계되었기 때문에 빠른 속도로 이동하는 단말에 대한 실시간 서비스 혹은 저속이더라도 끊김없는 서비스를 지원하기에는 많은 어려움이 있다. 특히 차후 무선 인터넷에서는 이러한 실시간 멀티미디어 서비스가 주요 서비스로 등장할 것으로 예상되므로 기존의 Mobile IP 보다 향상된 로밍 기술이 요구되고 있다.

본 논문에서는 2계층 핸드오프 기술인 IEEE 무선 랜 기술과 3계층 핸드오프 기술인 Mobile IPv6 및 Fast Handoff 기술과의 연동을 통해 Mobile IPv6 Fast Handoff가 가지는 핸드오프 지연 감소 및 패킷 손실률 감소의 이점을 유지하고 이동 노드의 글로벌 로밍 지원을 위한 AAA 기반의 인증 구조상에서 Fast Handoff 기법을 적용함으로써 AAA 인증 과정의 지연을 줄이기 위한 개선된 인증 방법을 제시하였다. 기존의 AAA 인증 방식에 비해 본 논문에서 제안한 Fast Handoff 기법을 이용한 AAA 인증 방식은 이동 노드가 2계층 핸드오프 전에 FBACK 메시지를 수신하는 경우 최대 55%, 수신하지 못하는 경우 최대 17%의 비용 감소 결과를 보인다.

참 고 문 헌

[1] Charles E. Perkins and David B. Johnson, "Mobility Support in Mobile IPv6," RFC 3775, Dec. 2003.

[2] S. Glass and C. Perkins, "Mobile IP Authentication, Authorization and Accounting Requirements," RFC 2977, Oct. 2000.

[3] Stefano M. Faccin and Charle E. Perkins, "Mobile IPv6 Authentication, Authorization and Accounting Requirements," IETF Internet Draft, draft-le-aaa-mipv6-requirements-02.txt, Oct. 2003.

[4] Pet. R. Calhoun and Tony Johansson, "Diameter Mobile IPv6 Application," IETF Internet Draft, draft-ietf-aaa-diameter-mobileip-11.txt, Jun. 2002.

[5] Charles E. Perkins, "Diameter Mobile IPv7 Application," IETF Internet Draft, draft-le-aaa-

diameter-mobileipv6-03, Oct. 2003.
[6] Charles E. Perkins and Thomas Eklund, "AAA for IPv6 Network Access," IETF Internet Draft, draft-perkins-aaav6-06.txt, May 2003.
[7] F. Dupont, J. Bournelle, "AAA for Mobile IPv6," IETF Internet Draft, draft-dupont-mipv6-aaa-01.txt, Nov. 2001.
[8] M. Kim and Y. Mun, "Localized Key Management for AAA in Mobile IPv6," IETF internet Draft, draft-mun-aaa-localkm-mobileipv6-01.txt, May 2003.
[9] R. Koodli et al, "Fast Handovers for Mobile IPv6," IETF Internet Draft, draft-ietf-mobileip- fast-mipv6-06.txt, Mar. 2003.
[10] R. Koodli, Charles E. Perkins, "Fast Handovers and Contxt Transfers in Mobile Networks," ACM Computer Communication Review, Vol. 31, No. 5, Oct. 2001.
[11] S. Pack and Y. Choi, "Performance Analysis of Fast Handover in Mobile IPv6 Networks," in Proc. IFIP PWC 2003, Venice, Italy, Sept. 2003.
[12] R. Jain, T.Raleigh, C. Graff and M. Bereschinsky, "Mobile Internet Access and QoS Guarantees using Mobile IP and RSVP with Location Registers," in Proc. ICC'98 Conf,. pp. 1690-1695, Atlanta.

김 창 남
2002년 상명대학교 컴퓨터소프트웨어 졸업(공학사). 2004년 숭실대학교 컴퓨터학과 졸업(공학석사). 2004년 3월~현재 (주)니츠 정보보호기술연구소 연구원. 관심분야는 Mobile IP, Security, IPv6

문 영 성
1993년 연세대학교 전자공학과(학사) 1986년 Unive. of Alberta 전자공학과 졸업(석사). 1993년 Univ. of Texas, Arlington 전산학과 졸업(박사). 1994년~현재 숭실대학교 컴퓨터학부 부교수 관심분야는 Mobile IP, IPv6, Security

허 의 남
1990년 부산대학교 전산통계학과 졸업(학사). 1995년 Univ. of Texas at Arligton 컴퓨터공학 졸업(공학석사). 2003년 Ohio University 컴퓨터공학 졸업(공학박사). 200년 9월~2003년 2월 삼육대학교 컴퓨터학과 조교수. 2003년 3월~현재 서울여자대학교 정보통신 공학부 조교수. 관심분야는 Grid Computing, 유비쿼터스, 임베디드