논문 2011-48TC-1-13

미래네트워크의 효율적인 모바일 환경 구축을 위한 향상된 Fast Handover for Proxy MIPv6 기법

(An Enhanced Fast Handover for Proxy MIPv6 Scheme for Efficient Mobile Environment of The Future Network)

고 광 섭*, 정 의 석**, 문 영 성***

(Kwangsub Go, Uiseok Jung, and Youngsong Mun)

요 약

휴대 단말장치들의 발전과 새로운 기술적 요구로 인해 새로운 네트워크를 설계하려는 미래네트워크 연구가 진행되고 있다. 미래네트워크는 다양한 네트워크 요구사항을 충족해야하며, 사용자에게 이동 중에도 끊김없는 네트워크 서비스와 높은 보안성을 제공해야 한다. 이로 인해 휴대 단말장치의 이동성을 보장하고 사용 인증을 통해 보안성을 제공하는 프로토콜이 연구되고 있다. 그 중, Fast handovers for proxy MIPv6(PFMIPv6) 프로토콜에서 인증, 권한 검증, 과금을 지원하는 AAA 기법을 사용하여 이동성과 보안성을 제공하는 방법이 제안되었다. 이 방법은 보안성을 제공하고 패킷손실을 줄일 수 있지만 처리할 메시지가 많고 긴 핸드오버 지연시간을 갖는 문제점이 있다. 이를 해결하기 위하여 PFMIPv6 기반에서 인증기법을 이용한 향상된 전송방안을 제안한다. 제안된 방법은 AAA 기법을 사용되는 인증메시지에 등록메시지를 포함시켜 동시에 전송하기 때문에 시그널링 비용과 핸드오버 지연시간이 단축시킬 수 있으며, 사용자 인증을 통해 보안성도 제공할 수 있다. 제안된 방법의 성능평가를 통하여 분석하여 비교하였으며, 제안된 방법이 기존의 PFMIPv6 기반의 인증기법보다 우수한 성능을 제공함을 알 수 있었다.

Abstract

To develop the new network, the future network architecture is studied. Since the mobile devices are also advanced, they need for the mobility protocols. The one of the protocols, Fast handovers for proxy MIPv6(PFMIPv6) has studied by the Internet Engineering Task Force(IETF). Since PFMIPv6 adopts the entities and the concepts of fast handovers for MIPv6(FMIPv6) in proxy MIPv6(PMIPv6), it reduces the packet loss. Although the conventional scheme has proposed that it cooperated with an Authentication, Authorization and Accounting (AAA) infrastructure for authentication of a mobile node in PFMIPv6, it has the drawbacks such as high signaling cost and long handover latency. To reduce the signaling cost and the handover latency, we propose an enhanced authentication scheme in Fast handover for Proxy MIPv6. The proposed scheme reduces the handover latency and the signaling cost because the registration procedure and the authentication procedure are simultaneously performed. We also compare the proposed scheme with the conventional scheme in terms of the signaling cost and the handover latency.

Keywords: Fast handovers for Proxy MIPv6, Proxy MIPv6, AAA infrastructure,

I. 서 론

현재의 인터넷은 많은 연구자들의 기술적 요구를 수용하기 어려운 단계에 이르러 있으며, 많은 요구사항들을 충족할 수 있는 미래네트워크 연구가 진행되고 있다. 또한, 이동성을 제공할 수 있는 기기의 발달로 인해 언제 어디서든지 원하는 장소에서 무선 인터넷을 서비스를 받고자 하는 사용자들의 요구에 이동노드의 이동성을 보장하는 프로토콜에 대한 연구가 진행되고 있다.

* 정회원, ** 학생회원, *** 평생회원-교신저자,
숭실대학교
(Soongsil University)
접수일자: 2010년9월2일, 수정완료일: 2011년1월14일

최근 네트워크에서의 이동성 지원을 위한 연구가 진행되고 있으며, Internet Engineering Task Force(IETF)에서 Proxy Mobile IPv6(MIPv6)[1]가 표준화되었다. PMIPv6는 Mobile Access Gateway(MAG)가 이동노드의 이동성 관리를 대신해주기 때문에, 이동노드가 새로운 네트워크로 이동하였을 때 이동노드의 부담을 줄이고 핸드오버 지연시간을 줄일 수 있다. 그러나 PMIPv6는 기본적으로 Mobile IPv6(MIPv6)[2]의 동작을 따르기 때문에 이동노드의 핸드오버 동안 패킷손실이 일어나는 문제점이 있다. PMIPv6의 문제점을 해결하기 위해서, IETF의 MIPSHOP 워킹그룹에서는 PMIPv6의 네트워크 기반의 이동성 관리 프로토콜 기반에서 Fast handovers for MIPv6(FMIPv6)[3]의 빠른 핸드오버 기법을 접목한 Fast handovers for proxy MIPv6 (PFMIPv6)[4]를 제안하였으며, 개선방안을 연구중에 있다. PFMIPv6는 기존의 FMIPv6에서 사용하는 빠른 핸드오버 기법을 수행함으로써, 두 가지의 모드가 존재한다. 첫 번째는 Predictive 모드로써, 이동노드가 NMAG로 이동하기 전에 PMAG와 NMAG 사이에 양방향 터널이 설립되는 모드이다. 두 번째 Reactive 모드는 이동노드가 NMAG로 이동한 후에 PMAG와 NMAG 사이에 양방향 터널이 설립되는 모드이다. 이러한 PFMIPv6는 네트워크 기반의 이동성 관리와 빠른 핸드오버 기법을 사용함으로써 패킷손실을 줄일 수 있다.

한편, 관리상의 도메인 사이를 이동할 때 이동노드의 인증을 위한 AAA(Authentication, Authorization and Accounting) 기법[6~8]이 필요하다. AAA 기법은 다양한 유무선 서비스에 대하여 인증, 권한 검증, 과금을 수행한다. 현재 여러 프로토콜에서 AAA 기법을 연동하여 이동노드의 인증, 권한검증, 과금, 노드간 인증 등의 기능을 수행하는 연구가 진행 중이다. 이 연구들 중, Zhou et al.[5]은 PFMIPv6 기반의 인증기법을 제안하였다. 이 기법은 이동노드가 새로운 네트워크에 진입할 때, 인증을 통해서 이동노드를 Replay Attack과 Key Exposure 같은 보안위협으로부터 보호할 수 있다. 그러나 이 기법은 핸드오버 과정 동안 높은 수준의 보안성을 제공하였지만, AAA 기법과 등록메시지 등 많은 메시지를 포함하고 있어서 시그널 메시지와 핸드오버 지연시간이 증가하는 문제점이 있다.

본 논문에서 이러한 문제점을 해결하기 위하여, PFMIPv6 기반에서 Proxy Binding Update(PBU) 메시지와 Proxy Binding Acknowledgement(PBA) 메시지를 AAA 인증메시지에 담아서 2계층 핸드오버 이전에 전송하는 기법을 제안한다. 이 방법은 인증메시지에 등록메시지를 포함하여 동시에 전송하기 때문에 시그널링 비용과 핸드오버 지연시간을 줄일 수 있다. 또한, AAA 기법을 사용하여 이동노드를 인증함으로써 높은 보안성을 얻을 수 있게 된다.

본 논문의 구성은 Ⅱ장에서 제안 방안과의 비교 대상인 Zhou의 방법을 분석하였고, Ⅲ장에서 본 논문이 제안하는 방법에 관하여 설명하였다. Ⅳ장에서는 제안하는 방법의 성능평가에 대하여 살펴보고, 마지막 Ⅴ장에서는 결론 및 향후 연구 방향을 제시한다.

Ⅱ. 관련 연구

여러 프로토콜들과 AAA 기법을 연동한 방법들이 연구되고 있다. 그 중, Zhou의 방법은 PFMIPv6 기반으로 AAA 기법을 연동한 방법이다. 이 방법은 이동노드에 대한 보안위협을 극복하는 해결책을 정의하고, AAA 기법과 PFMIPv6의 연동에 대한 방법을 제안하였다.

Zhou의 방법에서 이동노드가 네트워크 자원을 얻기 위해서는 해당 네트워크에 대한 접근 권한을 부여받기 위해서 이동노드는 홈 네트워크로부터 인증을 받아야한다. 이러한 역할을 AAA 서버가 해줌으로써 인증, 권한검증과 이동성 제공을 한 번의 과정으로 수행할 수 있다. Zhou의 방법에서 수행과정은 이동노드의 움직임에 따라 이니셜과 핸드오버 인증과정으로 나눌 수 있다. 이니셜 인증과정은 이동노드가 홈 네트워크의 MAG에 접속하였을 때, 그림 1과 같은 메시지 흐름으로 나타낼 수 있다. 핸드오버 인증과정은 이동노드가 새로운 네트

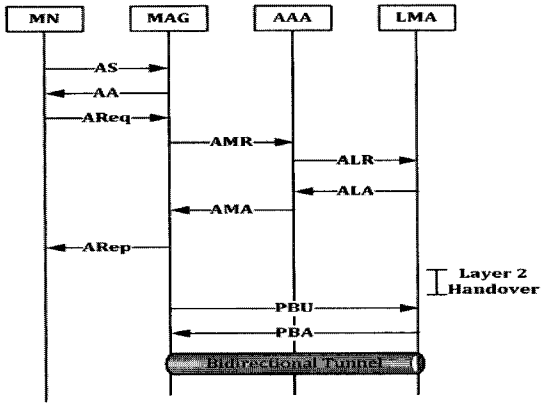


그림 1. 기존 연구의 이니셜 인증과정 메시지흐름
Fig. 1. Message flow of the initial authentication procedure for the conventional scheme.

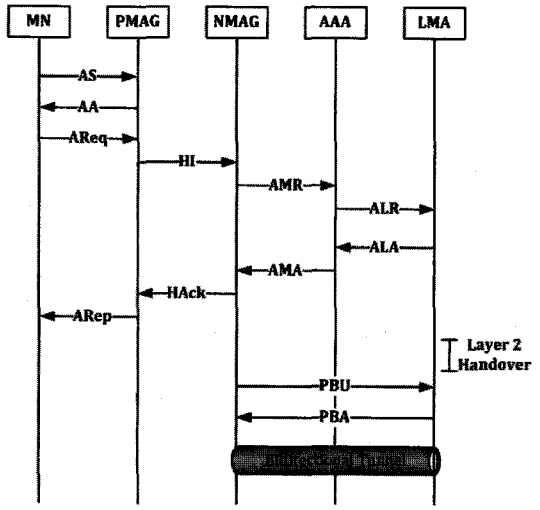


그림 2. 기존 연구의 핸드오버 인증과정 메시지흐름
Fig. 2. Message flow of the handover authentication procedure for the conventional scheme.

워크로 이동하여 해당 네트워크의 새로운 MAG(new MAG: NMAG)에 접근하였을 때, 그림 2와 같은 메시지 흐름으로 나타낼 수 있다. 이니셜 인증과정은 다음 3단계로 나타낼 수 있다.

1 단계: 이동노드가 PFMIPv6 도메인에 들어가서 MAG가 접속되어 있는 액세스 링크에 접속하면, 이동노드는 액세스 링크에 접속된 MAG에게 Attendant Solicit(AS) 메시지를 전송하게 된다. MAG는 AS 메시지를 받은 후, 이동노드에게 Local Challenge(LC) 값을 포함한 Attendant Advertisement(AA) 메시지를 보낸다. 이동노드는 MAG로부터 받은 AA 메시지에 포함된 임의의 수인 LC 값을 long-term 키를 사용하여 암호화하고, AAA 서버가 이동노드를 인증할 때 사용하는 Credential(CR) 값을 생성한다.

2 단계: 이동노드는 Authentication Request(AReq) 메시지를 MAG에 전송한다. 이때 전송되는 AReq 메시지에는 이동노드를 식별하고 보안위협에서 보호하기 위한 LC 값, CR 값, 이동노드의 Network Access Identifier(NAI), Identity of the MAG(MAGID)과 Replay Protect Indicator(RPI)를 포함한다. AReq 메시지를 받은 MAG는 AReq 메시지에서 얻은 이동노드의 정보들을 AA-MAG-Request(AMR) 메시지에 담아 AAA 서버로 전송한다. AAA 서버는 AMR 메시지에 담긴 LC 값을 long-term 키를 이용하여 암호화하고 CR 값과 함께 비교하여 이동노드의 인증을 시작한다. 만약 두 값이 정상이라면 이동노드의 인증에 성공하게 되고, AAA 서버는 AA-LMA-Request(ALR) 메시지를 Local Mobility Anchor(LMA)에 전송한다. LMA는 ALR 메시지의 응답으로 AA-LMA-Answer(ALA) 메시지를 AAA 서버에 전송하고, ALA 메시지를 받은 AAA 서버는 AA-MAG-Answer(AMA) 메시지를 MAG에 보낸다. MAG는 long-term 키를 이용해서 AMA 메시지를 복호화하고, AMA 메시지를 통해서 이동노드의 인증 성공을 확인한다. 또한, LMA's identify(LMAID)를 등록하고, 이동노드의 인증 결과를 Home Network Prefix(HNP)를 담은 Authentication Reply(ARep) 메시지를 이동노드에게 보내서 알려준다.

3 단계: ARep 메시지를 이동노드에게 보낸 후, MAG는 Proxy Binding Update(PBU) 메시지를 LMA에 전송한다. PBU 메시지를 수신한 LMA는 PBU 메시지에 있는 정보를 이용하여 이동노드에게 할당할 HNP와 Proxy care-of address(Proxy-CoA)에 대한 Binding Cache Entry(BCE)를 설정하고 MAG와의 양방향 터널을 설립한다. 그리고 MAG에게 BCE 업데이트와 양방향 터널 설정이 완료되었다는 것을 알려주기 위해서 Proxy Binding Acknowledgement(PBA) 메시지를 전송한다. 이후부터 이동노드는 PFMIPv6 도메인에 있는 동안 통신이 가능해진다.

핸드오버 인증과정은 이동노드가 기존의 MAG에서 NMAG로 이동했을 경우이다. 이때는 첫 번째 등록과정의 1, 3 단계의 과정은 같고 2 단계의 과정은 조금 차이가 있으며, 2 단계에서 다음과 같은 수행과정이 추가된다.

2 단계: 이전의 MAG(previous MAG: PMAG)는 이동 노드가 NMAG에서도 통신을 계속 하기 위해서 보낸 AReq 메시지를 받은 후, NMAG에게 Handover Initiate(HI) 메시지를 보낸다. 이후 인증메시지를 AAA 서버와 LMA에 전송하는 수행과정은 이니셜 인증과정과 같다. AAA 서버로부터 AMA 메시지를 받은 NMAG는 Handover Acknowledgement(HAck) 메시지를 PMAG에게 보낸다. PMAG는 이동노드의 인증 성공을 알리기 위해서 이동노드에게 ARep 메시지를 보낸다.

III. 인증기법을 이용한 향상된 전송방안

Zhou의 방법은 핸드오버 과정 동안 높은 수준의 보안성을 제공하였지만, AAA 기법과 등록메시지 등 많은 메시지를 포함하고 있어서 시그널 메시지와 핸드오

버 지연시간이 증가하는 문제점을 갖게 된다. 이러한 문제점을 해결하기 위해서, PFMIPv6에서 인증기법을 이용한 향상된 전송방안을 제안한다. 제안된 방법은 Zhou의 방법을 참고하여, 이동노드가 AAA서버에 인증하는 과정과 LMA에 등록하는 과정을 동시에 수행한다. 또한, PFMIPv6의 수행과정을 따르기 때문에 Predictive와 Reactive 모드가 존재한다. Reactive 모드는 핸드오버 지연시간이 짧아 예측하기 힘들기 때문에, 제안된 방법에서는 Predictive 모드에 중점을 두고 수행한다.

제안된 방법은 Zhou의 방법을 참고하여 AAA 서버와 LMA, MAG는 미리 설정된 키를 갖고 사용한다. AAA 서버와 MAG는 같은 도메인 안에 위치하며, 두 구간사이는 Diameter 프로토콜로 설정된다. 또한, Zhou의 방법과 같이, 이니셜과 핸드오버 인증과정으로 나누어 수행한다. 제안된 방법의 메시지흐름은 Zhou의 방법에서 1단계는 같으며, 2-3단계에서의 다른 점은 다음과 같다.

이니셜 인증과정은 그림 3에서처럼, 이동노드로부터 AReq 메시지를 전송받은 MAG는 PBU 메시지를 포함한 AMR 메시지를 생성하여 AAA 서버로 전송한다. AAA 서버는 AMR 메시지로부터 PBU 메시지를 분리하고, 이동노드의 정보를 추출한다. 추출한 정보를 통해서 AAA 서버는 AMR 메시지에 담긴 LC 값을 long-term 키를 이용하여 암호화하고 CR 값과 함께 비교하여 이동노드의 인증을 시작한다. 만약 두 값이 정상이라면 이동노드의 인증에 성공하게 되고, AAA 서버는 PBU 메시지를 담은 ALR 메시지를 LMA에 전송한다. LMA는 ALR 메시지를 통해서 PBU 메시지를 추출하여 이동노드를 등록한다. LMA는 ALR 메시지의 응답으로 PBA 메시지를 포함한 ALA 메시지를 AAA 서버에 전송한다. AAA 서버는 이동노드의 등록성공을 알리기 위해서 MAG에게 PBA 메시지를 담은 AMA 메시지를 보낸다. MAG는 AMA 메시지를 복호화하고, 이 메시지를 통해서 이동노드의 NAI를 얻어 이동노드의 인증을 확인한다. 또한, LMAID를 등록하고 이동노드의 인증결과를 알리기 위해서 HNP를 포함한 ARep 메시지를 이동노드에게 전송한다.

핸드오버 인증과정은 그림 4에서처럼, 이동노드에게 AReq 메시지를 받은 PMAG는 PBU 메시지를 HI 메시지에 포함하여 NMAG에 전송한다. 이후 인증메시지에 등록메시지를 포함하여 AAA 서버와 LMA에 전송하는 수행과정은 이니셜 인증과정과 같다. NMAG는 이동노드의 인증결과를 알리기 위해서 HNP를 포함한 HAck 메시지를 PMAG에 전송한다. PMAG는 HNP를 포함한 ARep 메시지를 이동노드에게 전송한다. MAG와 PMAG로부터 ARep 메시지를 받은 이동노드는 자신의 인증결과를 확인한 후, PFMIPv6 도메인 안에서 상대노드와 자유로운 통신을 할 수 있게 된다.

Zhou의 방법과 달리, 제안된 방법은 PBU와 PBA 메시지들이 인증메시지들에 담겨 전송되기 때문에, ARep 메시지가 MAG에서 이동노드로 전달되기 전에 등록과정이 완료된다. 따라서 제안된 방법을 통해 시그널링 비용과 핸드오버 지연시간을 줄일 수 있다.

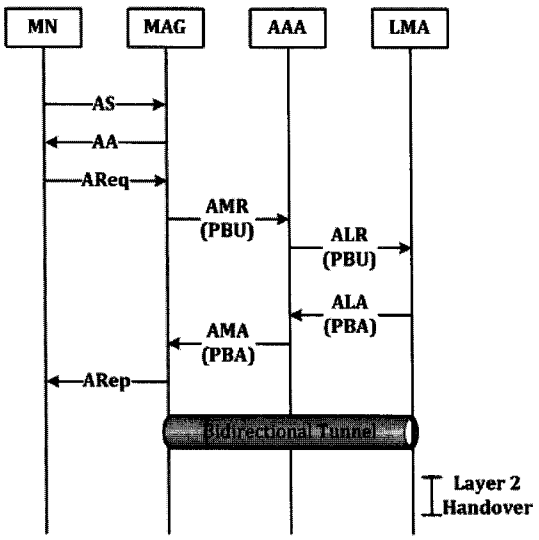


그림 3. 제안된 방법의 이니셜 인증과정 메시지흐름
Fig. 3. Message flow of the initial authentication procedure for the proposed scheme.

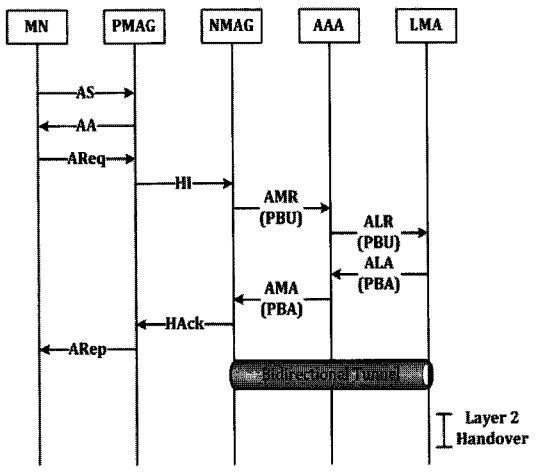


그림 4. 제안된 방법의 핸드오버 인증과정 메시지흐름
Fig. 4. Message flow of the handover authentication procedure for the proposed scheme.

Ⅳ. 성능 평가

4.1 시그널링 비용 분석

이번 장에서는 제안된 방법과 Zhou의 방법의 시그널링 비용과 핸드오버 지연시간을 각각 비교분석한다.

제안된 방법과 Zhou의 방법의 시그널링 비용은 Zhou의 방법에 참고하여 분석한다. 따라서 시그널링 비용은 이동노드가 AS 메시지를 MAG에게 보낸 시점부터 MAG가 PBA 메시지를 받는 시점까지를 합산하여 나타낸다. 이 방법을 이용하여 이니셜 인증과정에서 기존 연구의 시그널링 비용을 $C_{Initial}^{Conven}$로 표기하며 식 (1)로 나타내고, 이니셜 인증과정에서 제안된 방법의 시그널링 비용을 $C_{Inital}^{Proposed}$로 표기하며 식 (2)로 나타낼 수 있다.

$$C_{Initial}^{Conven} = 2(N_h + N_{al} + N_a)c_s + c_v + 3c_{us} + c_g + 2N_{ua}c_s \quad (1)$$

$$C_{Initial}^{Proposed} = 2(N_h + N_{al} + N_a)c_s + c_v + 3c_{us} + c_g \quad (2)$$

위 식 (1)과 (2)에서 사용된 파라미터는 다음과 같다.

- c_s: 한 홉에 대한 전송 비용
- c_v: AAA 서버에서 사용되는 검증비용
- c_{us}: 한 쌍의 암호화와 복호화 비용
- c_g: 키 생성 비용
- N_{ua}: MAG와 LMA 사이 간격에 대한 거리
- N_a: MAG와 이동노드 사이 간격에 대한 거리
- N_{al}: LMA와 AAA 서버 사이 간격에 대한 거리
- N_h: AAA서버와 이동노드 사이간격에 대한 거리
- N_m: PMAG와 NMAG 사이 간격에 대한 거리

AAA 서버와 이동노드 사이 간격은 메시지가 왕복 전송되기 때문에 2 홉으로 나타낸다. 따라서 등록메시지를 제외한 인증메시지들을 합한 홉 수는 $2(N_h + N_{al} + N_a)$로 나타낼 수 있다. AAA 서버에서 한번 검증되기 때문에, c_v의 계수는 1로 나타낸다. 암호화와 복호화 비용은 3번의 과정이 있는데, 첫 번째는 AAA 서버와 이동노드 사이에서의 값에 대한 암호화와 복호화 비용이고, 두 번째는 LMA와 AAA 서버 사이의 세션 키에 대한 암호화와 복호화 비용이며, 세 번째는 AAA 서버와 MAG 사이의 세션 키에 대한 암호화와 복호화 비용이다. 따라서 암호화와 복호화 비용은 $3c_{us}$로 나타낸다. AAA 서버가 MAG와 LMA에서 사용하기 위해서 키가 한 번 생성되기 때문에, c_g의 계수는 1로 나타낸다.

핸드오버 인증과정의 PMAG와 NMAG 사이에서 전송되는 HI와 HAck 메시지의 전송 비용은 왕복 전송이기 때문에, $2N_m c_s$로 나타낸다. 등록과정에서 사용되는 MAG와 LMA 사이의 PBU와 PBA 메시지의 전송비용은 왕복 전송이기 때문에, $2N_{ua}c_s$로 나타낸다. 이니셜 인증과정의 시그널링 비용과 같은 방법으로 핸드오버 인증과정의 시그널링 비용을 나타낸다. 이니셜과 핸드오버 인증과정의 제안된 방법은 인증메시지에 등록메시지를 포함하여 전송하기 때문에 등록메시지의 전송비용이 사용되지 않는다. 따라서 핸드오버 인증과정에서 기존 연구의 시그널링 비용을 $C_{Handover}^{Conven}$로 표기하며 식 (3)로 나타내고, 핸드오버 인증과정에서 제안된 방법의 시그널링 비용을 $C_{Handover}^{Proposed}$로 표기하며 식 (4)로 나타낼 수 있다.

$$C_{Handover}^{Conven} = 2(N_h + N_{al} + N_a)c_s + c_v + 3c_{us} + c_g + 2N_m c_s + 2N_{ua}c_s \quad (3)$$

$$C_{Handover}^{Proposed} = 2(N_h + N_{al} + N_a)c_s + c_v + 3c_{us} + c_g + 2N_m c_s \quad (4)$$

이니셜과 핸드오버 인증과정의 시그널링 비용을 합하여 시그널링 비용의 평균값을 구할 수 있다. 따라서 기존 연구와 제안된 방법의 시그널링 비용의 평균값을 각각 $C_{Average}^{Conven}$와 $C_{Average}^{Proposed}$로 표기하며, 식 (5)와 (6)으로 나타낼 수 있다.

$$C_{Average}^{Conven} = \lambda_\mu C_{Initial}^{Conven} + \lambda_\mu \max(N_s - 1, 0) C_{Handover}^{Conven} \quad (5)$$

$$C_{Average}^{Proposed} = \lambda_\mu C_{Initial}^{Proposed} + \lambda_\mu \max(N_s - 1, 0) C_{Handover}^{Proposed} \quad (6)$$

위 식 (5)와 (6)에서 λ_μ는 호 도착률이며, 이동노드가 여러 MAG들의 경계를 가로지를 때 발생하는 핸드오버 인증과정의 평균값을 $\max(N_s - 1, 0)$으로 나타낸다. N_s는 이동노드가 MAG를 지나가는 수의 평균값

이고, μ_r/η로 나타낸다[5].

4.2 핸드오버 지연시간 분석

핸드오버 지연시간은 이동노드가 MAG에게 AS 메시지를 전송하고 다시 MAG로부터 ARep 메시지를 받을 때까지의 등록과정과 인증과정을 나타내었다. 핸드오버 지연시간을 분석하기 위해서, 이니셜 인증과정에서의 핸드오버 지연시간과 핸드오버 인증과정에서의 핸드오버 지연시간을 구한다. 그리고 핸드오버 지연시간을 합하여 핸드오버 지연시간의 평균값을 구한다. 먼저 이니셜 인증과정에서 기존 연구의 핸드오버 지연시간을 $T_{Initial}^{Conven}$로 표기하며 식 (7)로 나타내고, 제안된 방법의 핸드오버 지연시간을 $T_{Initial}^{Proposed}$로 표기하며 식 (8)로 나타낼 수 있다.

$$\begin{aligned} T_{Initial}^{Conven} &= 2(N_h + N_{al} + N_a)(t_{pr} + t_{tr}) \\ &\quad + 3t_m + 2t_v + 3t_{us} + t_g \\ &\quad + 2N_{ua}(t_{pr} + t_{tr}) \end{aligned} \tag{7}$$

$$\begin{aligned} T_{Initial}^{Proposed} &= 2(N_h + N_{al} + N_a)(t_{pr} + t_{tr}) \\ &\quad + 3t_m + 2t_v + 3t_{us} + t_g \end{aligned} \tag{8}$$

위 식 (7)과 (8)에서 사용된 파라미터는 다음과 같다.

- t_{pr}: 한 홉에 대한 메시지 전파 시간
- t_{tr}: 한 홉에 대한 메시지 전송 시간
- t_m: MAG에서의 메시지 전송과 대기 시간
- t_v: AAA 서버에서의 메시지 전송과 대기 시간
- t_{us}: 한 쌍의 암호화와 복호화 시간
- t_g: AAA 서버에서의 키 생성 시간

이동노드가 MAG를 3번 통과할 때, 인증과정도 3번 필요하므로 $3t_m$로 나타낸다. AAA 서버에 인증메시지가 2번 전송되므로 $2t_v$로 나타낸다. AAA 서버는 LMA와 MAG에 대한 키가 필요하기 때문에, t_g의 계수는 1로 계산된다. 암호화와 복호화에 대한 시간은 시그널링 비용에서의 암호화와 복호화 비용처럼 계산하여 $3t_{us}$로 나타낸다. 핸드오버 인증과정에서 기존 연구의 핸드오버 지연시간을 $T_{Handover}^{Conven}$로 표기하며 식 (9)로 나타내고, 제안된 방법의 핸드오버 지연시간을 $T_{Handover}^{Proposed}$로 표기하며 식 (10)으로 나타낼 수 있다.

$$\begin{aligned} T_{Handover}^{Conven} &= 2(N_h + N_{al} + N_a)(t_{pr} + t_{tr}) \\ &\quad + 3t_m + 2t_v + 3t_{us} + t_g \\ &\quad + 2N_m(t_{pr} + t_{tr}) \\ &\quad + 2N_{ua}(t_{pr} + t_{tr}) \end{aligned} \tag{9}$$

$$\begin{aligned} T_{Handover}^{Proposed} &= 2(N_h + N_{al} + N_a)(t_{pr} + t_{tr}) \\ &\quad + 3t_m + 2t_v + 3t_{us} + t_g \\ &\quad + 2N_m(t_{pr} + t_{tr}) \end{aligned} \tag{10}$$

이니셜과 핸드오버 인증과정의 핸드오버 지연시간을 합하여 핸드오버 지연시간의 평균값을 구할 수 있다. 따라서 기존 연구와 제안된 방법의 핸드오버 지연시간의 평균값을 각각 $T_{Average}^{Conven}$와 $T_{Average}^{Proposed}$로 표기하며, 식 (11)과 (12)로 나타낼 수 있다.

$$\begin{aligned} T_{Average}^{Conven} &= \lambda_\mu T_{Initial}^{Conven} \\ &\quad + \lambda_\mu \max(N_s - 1, 0)\, T_{Handover}^{Conven} \end{aligned} \tag{11}$$

$$\begin{aligned} T_{Average}^{Proposed} &= \lambda_\mu T_{Initial}^{Proposed} \\ &\quad + \lambda_\mu \max(N_s - 1, 0)\, T_{Handover}^{Proposed} \end{aligned} \tag{12}$$

4.3 성능 평가 결과

참고문헌[9~12]에서 사용된 파라미터 값을 참고하여 기존 연구와 제안된 방법의 시그널링 비용과 핸드오버 지연시간을 호 도착률과 홉 수로 비교한다. 참조된 파라미터의 값은 아래의 표 1과 같다.

그림 5는 시그널링 비용의 평균값을 호 도착률에 따른 값으로 계산하여 기존 연구와 제안된 방법을 각각 나타내었다. 이 그림에서 시그널링 비용의 평균값이 증가함에 따라서 호 도착률도 점진적으로 증가하였으며, 기존 연구는 제안된 방법에 비해 시그널링 비용의 증가가 큼을 보여준다. 따라서 이 그림에서 제안된 방법은

표 1. 시스템 파라미터
Table 1. System Parameters.

파라미터	값
$c_s/c_v/c_{us}/c_g$	$10\,hops/20\,hops/1\,hops/1\,hops$
$N_{ua}/N_h/N_m$	$4\,hops/4\,hops/1\,hops$
N_a/N_{al}	$2\,hops/2\,hops$
$t_{pr}/t_{tr}/t_m$	$40\mu s/20ms/15s^{-1}$
$t_v/t_{us}/t_g$	$15s^{-1}/2ms/2ms$
$\lambda_\mu/\eta/\mu_r$	$0.1\text{min}^{-1}/0.3\text{min}^{-1}/\frac{1}{3}min^{-1}$

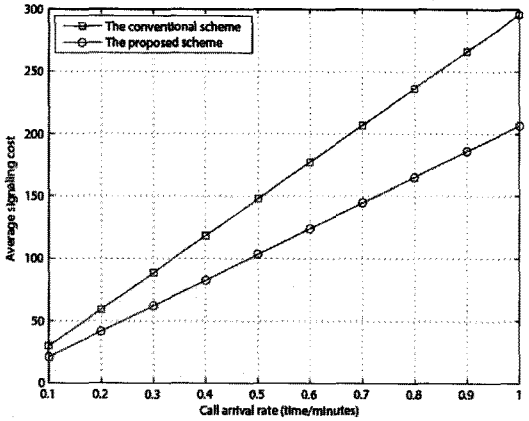


그림 5. 호 도착률에 따른 시그널링 비용
Fig. 5. Signaling cost depending on the call arrival rate.

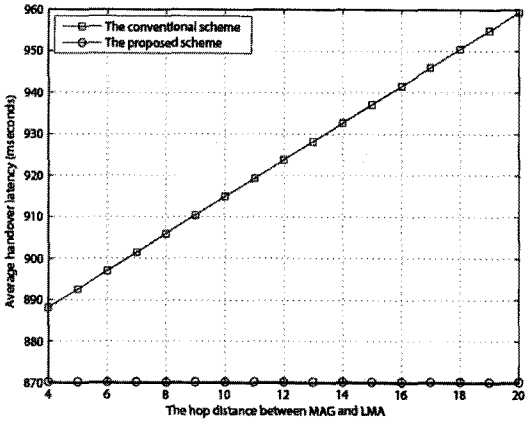


그림 6. 홉 수에 따른 핸드오버 지연시간
Fig. 6. Handover latency depending on the hop.

기존 연구에 비해 시그널링 비용이 낮음을 나타낸다.

그림 6은 핸드오버 지연시간의 평균값을 MAG와 LMA 사이 간격에 대한 거리에 따른 값으로 계산하여 기존 연구와 제안된 방법을 나타내었다. MAG의 거리를 4 홉에서 20 홉까지라고 가정하였다. 이 그림에서 기존 연구는 거리가 증가하면서 핸드오버 지연시간도 증가하였고, 제안된 방법은 등록메시지의 비용이 추가되지 않기 때문에 변함이 없었다. 따라서 기존 연구는 제안된 방법에 비하여 핸드오버 지연시간의 증가폭이 점차 커지는 결과를 얻었다. 또한, 제안된 방법은 기존 연구에 비해 핸드오버 지연시간이 단축됨을 알 수 있다.

V. 결 론

기존 연구는 PFMIPv6 도메인에서 AAA 기법을 사용하여 높은 보안성을 얻고자 하였다. 그러나 기존 연구는 인증과정에서 시그널링 메시지가 많이 필요하고 그에 따른 시그널링 비용의 증가와 핸드오버 지연시간이 길어지는 문제점이 있었다. 이러한 문제점을 해결하기 위해서 PFMIPv6 기반에서 AAA 기법을 사용하여 높은 보안성을 제공하고, 시그널링 비용과 핸드오버 지연시간을 줄이는 방법을 제안했다.

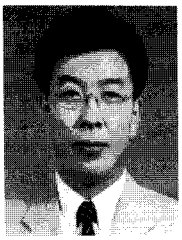
제안된 방법은 Zhou의 방법을 기반으로 하여 AAA 기법을 사용하여 인증메시지에 등록메시지를 포함해서 전송함으로써 시그널링 비용과 핸드오버 지연시간을 줄이면서 보안성도 확보할 수 있다. 성능 평가를 통해서 제안된 방법과 기존 연구를 비교 분석하였으며, 제안된 방법이 기존 연구보다 시그널링 비용을 30% 감소시키고, 핸드오버 지연시간을 2% 단축시켰음을 보여줬다. 제안된 방법은 향후 모바일 환경을 포함한 미래네트워크를 구성할 때, PFMIPv6 기술에 포함되어 효율적인 미래네트워크 환경을 구축하는데 중요한 역할을 할 수 있다.

참 고 문 헌

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6", RFC 3775, June 2004.
[2] S. Gundavelli, K. Leung, V. Devarapalli and K. Chowdhury, "Proxy mobile IPv6", RFC 5213, Aug. 2008.
[3] R. Koodli, "Fast handovers for mobile IPv6", RFC 4068, July 2005.
[4] H. Yokota, K. Chowdhury and R. Koodli, "Fast handovers for Proxy mobile IPv6", Internet draft-IETF, draft-ietf-mipshop-pfmipv6-08.txt, July 2009.
[5] H. Zhou, H. Zhang and Y. Qin, "An authentication method for proxy mobile IPv6 and performance analysis", Security and Communication Networks, Nov. 2008.
[6] S. Baek, S. Pack, T. Kwon and Y. Choi, "A localized authentication, authorization, and accounting (AAA) protocol for mobile hotspots", Proc. IEEE/IFIP WONS 2006, Jan. 2006.
[7] A. Patel, "Authentication protocol for mobile IPv6", RFC 4285, Jan. 2006.
[8] C. Perkins and P. Calhoun, "Authentication, authorization, and accounting (AAA) registration keys for mobile IPv4", RFC 3957, Mar. 2005.
[9] W. Liang and W. Wang, "On performance analysis of challenge/response based authentication in wireless local area networks", Computer Networks and ISDN Systems, Vol. 48,

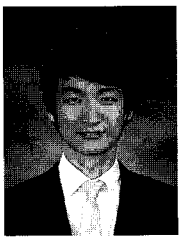
pp. 267-288, June 2005.
[10] A. Hess and G. Schafer, "Performance evaluation of AAA/mobile IP authentication", Proc. 2nd PGTS, Sep. 2002.
[11] B.J. Han, J.M. Lee, J.H. Lee and T.M. Chung, "PMIPv6 route optimization mechanism using the routing table of MAG", IEEE Systems and Networks Communications ICSNC'08 3rd International Conference on, pp. 274-279, Oct. 2008.
[12] S. Park, N. Kang, and Y. Kim, "Localized proxy-MIPv6 with route optimization in IP-based Networks", IEICE Trans. Commun., Vol. E90B, no. 12, Dec. 2007.

저 자 소 개



고 광 섭(정회원)
2007년 숭실대학교 컴퓨터학과 석사.
2008년 숭실대학교 컴퓨터학과 박사 과정.
2000년~현재 한국과학기술정보 연구원 선임연구원.
<주관심분야 : 무선통신, 센서네트워크, 병렬컴퓨팅, 통신보안>

문 영 성(평생회원)-교신저자
1983년 연세대학교 전자공학과 학사 졸업.
1986년 University of Alberta 전자공학과 석사 졸업.
1993년 University of Texas (Arlington) 컴퓨터학과 박사 졸업.
1994년~현재 숭실대학교 컴퓨터학부 교수
<주관심분야 : 클라우드 컴퓨팅, Security and authentication with Mobile IP, Mobile IPv4, Mobile IPv6>



정 의 석(학생회원)
2008년 평생교육진흥원 컴퓨터공학 학사 졸업.
2009년~현재 숭실대학교 컴퓨터학과 석사과정.
<주관심분야 : Mobility Management, Network Mobility(NEMO), Proxy MIPv6, Fast handovers for Proxy MIPv6>