브로커를 통한 모바일 IPv6 네트워크의 효율적인 계층적 인증기법

An Efficient Hierarchical Authentication Scheme through Brokers in Mobile IPv6 Networks

정 하 권* 정 종 필**
Ha-Gwon Jung Jongpil Jeong

요 약

신속하고 안전한 이동성 서비스는 유비쿼터스 환경에서 중요한 이슈가 되고 있다. IETF(Internet Engineering Task Force)는 이러한 이슈들에 대응하기 위하여 네트워크 자원의 사용을 안전하게 하고 법적으로 보장하는 핵심기술 같은 많은 의미있는 작업들을 해오고 있으며 기존의 MIPv6(Mobile IPv6)에서 핸드오버 지연과 시그널링 오버헤드 같은 문제를 보완하기 위하여 HMIPv6(Hierarchical Mobile IPv6)를 제안하였다. 현재 HMIPv6에 관한 연구의 대부분은 HMIPv6와 AAA(Authentication, Authorization, Accounting) 프로토콜 사이의 상호작용 절차를 최적화하기 위한 방법에 초점을 맞추고 있다. 해당 논문에서는 AAA 절차에서 인증대기를 최소화하는데 중점을 둔 비용 효율적인 계층 인증 기법을 제안한다. 이 기법에서는 MAP(Mobility Anchor Point)에 배포되어진 AAA 서버들, Root AAA 서버가 관리하는 몇몇의 Leaf AAA 서버들 그리고 홈 도메인 안에 있는 AAA 서버를 대신하는 브로커들의 계층적 AAA 아키텍처를 제안한다. 이 시뮬레이션 결과는 제안된 기법이 이전의 전통적인 인증 조합 모델링과 비교하여 핸드오프 지연과 인증대기 시간이 상당히 줄어들었음을 보여준다.

ABSTRACT

As quick and secure mobility service is becoming a critical issue in the ubiquitous environment. Internet Engineering Task Force (IETF) has done a lot of meaningful work in order to cope with the critical issues, which is a key technology of guaranteeing the legally and safely using of network resources, they has proposed Hierarchical Mobile IPv6 (HMIPv6) to complement for such problems as handover latency and signaling overhead in existing MIPv6. Most of the current research about HMIPv6 focuses on how to optimize the interactive processes between the HMIPv6 and AAA (Authentication, Authorization, Accounting) protocol. This paper describes a cost-effective hierarchical authentication scheme, which makes its focus on minimizing the authentication latency in AAA processing. In this scheme, a hierarchical AAA architecture is proposed, in which the AAA servers are deployed on the Mobility Anchor Point (MAP), the Root AAA server manages several Leaf AAA servers and the Brokers on behalf of the AAA server in home domain. The simulation results shows that the proposed scheme reduces the handoff and authentication latency evidently compared to the previous traditional authentication combination modeling.

☞ keyword : 계층적 인증기법, 브로커, 모바일 IPv6, HMIPv6, MIPv6, Broker

1. 서 론

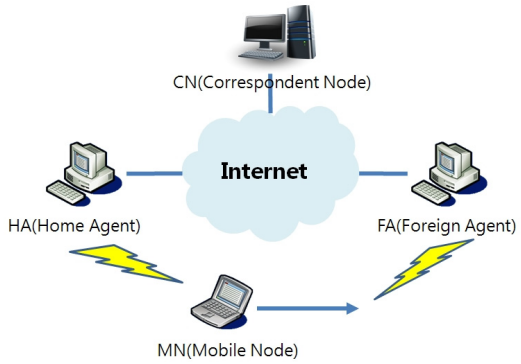
미래의 모바일 네트워크는 이기종의 무선 액세스 기술을 위해 All-IP 서비스를 제공하고, 인터넷과 연동하여 진화한 무선시스템과 함께 이동성의 수요가 급격하게 늘어날 것으로 보인다. IP 기술의 활성화에 따라 차세대 통신망은 IP 기반의 핵심망을 기반으로 하여, 다양한 종류의 액세스망을 수용하는 형태로 발전하고 있으며, 액세스망도 기존의 무선 LAN을 포함하여 IP 기술을 기반으로 하는 액세스망들이 점차 주류로 등장하고 있다. 이러한 차

* 정 회 원 : 성균관대학교 정보통신대학원 컴퓨터공학과 (공학석사) junhg7@skku.edu
** 정 회 원 : 성균관대학교 정보통신공학부 (공학박사) jpjeong@skku.edu
[2011/03/21 투고 - 2011/03/25 심사(20011/05/11 2차 - 2011/06/01 심사완료]

세대망 구조에서 효율적인 이동성 지원을 위해서는 IP 기술에 기반한 이동성 지원 기술이 필수적이다. 이러한 상황 아래서 IETF(Internet Engineering Task Force)는 차세대 네트워크를 위한 기본 프로토콜로서 Mobile IPv6(MIPv6)[1]의 이동성 지원을 제안하였으며, MIPv6을 위한 두 가지 대표적인 확장 기법인 Fast Handover MIPv6(FMIPv6)와 Hierarchical MIPv6(HMIPv6)의 이동성관리[2,3]가 나중에 제안되었다. MIPv6는 이동단말이 홈 망에서 사용하는 홈 주소 외에 이동단말의 현 위치를 알려주는 CoA(Care of Address)를 가지며 이를 위치 변경 시마다 이동단말로부터 먼 곳에 위치할 가능성이 있는 홈 에이전트나 상대노드(CN)에 등록(Binding Update)을 수행하여야 한다. 이 경우 이전 서브넷에서 새로운 서브넷으로의 등록이 완료되기 전까지 상대노드에 대한 연결성을 잃어버리게 되며 이로 인한 패킷 손실과 지연을 가져오게 된다. 이러한 패킷 손실과 지연은 VoIP와 같은 실시간성이 요구되는 응용에서는 수용할 수 없는 정도가 될 수도 있다.

특히 IETF의 MIPv6의 이동성 지원 기법 중 하나인 HMIPv6의 경우 이동성 처리를 위하여 반드시 인증이 선행되어야하고 인증에 대한 성능은 곧 이동성 지원 성능에 크게 영향을 미치게 된다. 즉, 만일 이동단말이 홈 망에서 먼 거리에 위치한 경우 기존 연구들의 AAA(Authentication, Authorization, Accounting) 인증 방식에서는 긴 등록시간을 유발하여 망에 불필요한 트래픽을 유발시켜 패킷손실을 가져오게 된다. 본 논문에서는 이러한 문제를 해결하기 위하여 이동단말이 홈망에서 먼거리에 위치한 경우 인증요청 메시지를 홈 도메인에 있는 AAA 서버(AAAH)로 전달하는 대신 본 논문에서 제안하는 AAAH의 모든 역할을 수행하면서 이동단말과 더 가까운 거리에 위치하고, 보안적인 측면에서 신뢰관계를 형성하고 있는 브로커(Broker)에게 전달하여 보다 나은 성능을 달성할 수 있음을 보인다.

논문의 구성은 다음과 같다. 2장에서 관련연구에 대해서 살펴본다. 3장에서는 제안하는 계층적 AAA 아키텍처, 시스템 모델링, 비용분석에 대해서 설명한다. 4장에서는 제안한 아키텍처의 비용분석을 통한 성능평가를 보인다. 5장에서는 결론과 향후 연구내용을 기술한다.



(그림 1) MIPv6의 구조

2. 관련연구

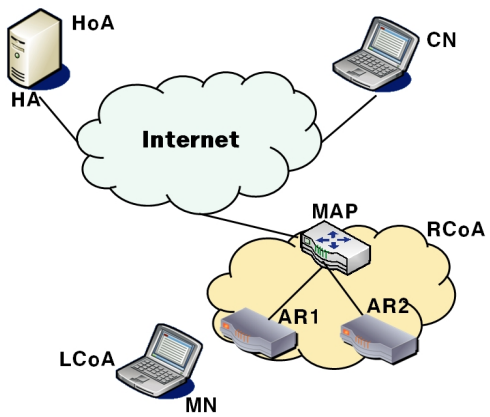
Mobile IP에서 이동단말의 네트워크 핸드오버 시 이동단말에 대한 적절한 이동성을 제공하기 위하여 Mobile IP 성능 개선 작업이 IETF의 Mobile IP WG(Working Group)을 중심으로 활발히 이루어지고 있으며, IETF는 유비쿼터스 환경에서의 안전한 모바일 서비스를 위해 AAA에 관하여 네트워크 자원의 사용을 안전하게 하고 법적으로 보장하는 핵심기술 연구 등의 의미 있는 작업들을 해오고 있다. 현재 HMIPv6에 관한 연구의 대부분은 HMIPv6와 AAA의 프로토콜 사이의 상호작용 절차를 최적화하는 방법에 초점을 맞추고 있다[4-7].

2.1 지역 이동성 관리 방법

이동단말이 서브넷을 변경하는 경우 항상 홈 망에 있는 홈 에이전트로 현재 위치에 대한 등록을 수행하여야 하며, 또한 경로 최적화 방법이나 MIPv6를 사용하는 경우 상대노드(CN)에 대해서도 등록(Binding Update)을 수행하여야 한다. 만일 이동단말이 홈 망에서 먼 거리에 위치한 경우 이러한 등록 방식은 긴 등록 시간을 유발하여 망에 불필요

한 트래픽을 유발시키게 된다. 따라서 이동단말의 이동 특성을 고려한 신속한 Handoff 처리 및 서비스 재개를 위한 인증 방법이 제공되어야 한다. 이러한 문제를 해결하기 위한 지역 이동성 관리 방법의 기본 개념은 Mobile IP 작업 그룹 내에서 지역 이동 특성을 가지는 경우, 이동단말의 이동 경계를 지역적 범위 내에서 별도 처리할 수 있도록 각 지역 도메인이 지역 이동성 에이전트를 가지며 지역 내의 이동성은 지역 이동성 에이전트 MAP (Mobility Anchor Point)을 설치하여 처리하게 함으로써 홈 에이전트나 상대노드에 이동단말의 지역적인 이동성을 숨기고 지역 도메인 내에서의 이동을 대신 처리하도록 하고 있다.

MIPv6는 서브넷을 이동할 때마다 상대노드와 홈 에이전트에 대한 바인딩 갱신을 수행하여야 한다. 상대노드에 대한 바인딩 갱신을 인증하기 위하여 사용되는 RR(Return Routability)의 경우 홈 에이전트에 대한 바인딩 갱신과 동시에 수행되는 경우에도 최소 1.5 RTD(Round Trip Delay)가 필요하다. 이러한 RTD로 인하여 핸드오버 시에 서비스의 단절이 발생하게 되며 또한 백본 망에서의 신호 트래픽 증가와 상대노드 및 홈 에이전트에서의 무선 구간에서 신호 증가를 가져온다. 따라서 지역적 이동성을 관리하는 지역 앵커를 도입한다면 바인딩 갱신에 필요한 지연을 줄일 수 있을 뿐만 아니라 이동성 신호의 양을 줄일 수 있다. HMIPv6 에서는 이를 위하여 (그림 2)에서와 같이 앵커의 역할을 수행하는 MAP을 새로이 도입한다. MAP은 개념적으로 지역적인 홈 에이전트로 동작하며 MIPv6에 대한 변경을 최소로 하면서도 성능 향상을 가져올 수 있다. HMIPv6는 MAP이라는 새로운 엔티티를 도입하였지만 이동 단말에 대해서는 최소한의 확장만이 필요하고 상대노드와 홈 에이전트에 대해서는 변경을 필요로 하지 않는다. 또한 MAP을 사용함으로써 MAP 영역 내에서의 이동은 상대 노드나 홈 에이전트에 숨겨지게 된다. (그림 2)에서 AR(Access Router)은 무선 인터페이스를 가지는 액세스 라우터를 나타내며, HMIPv6에서 이동 단말은 3가지 주

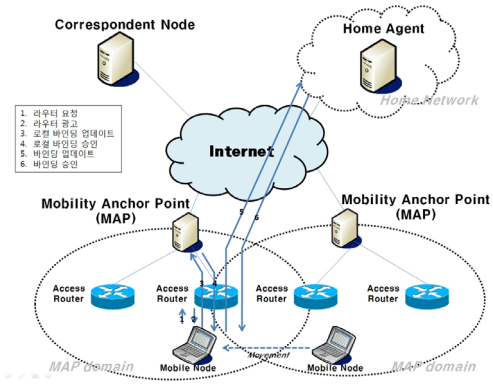


(그림 2) HMIPv6의 구조

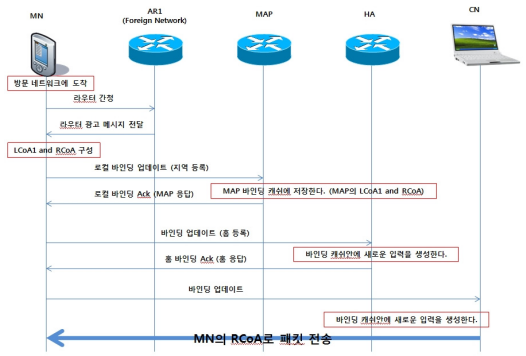
소를 가지게 된다. 즉, 홈 망에서 구성한 고유한 HoA(Home of Address), 액세스 망에서 구성한 CoA(LCoA) 그리고 MAP을 기반으로 구성한 CoA(RCoA)를 가진다. 상대노드와 홈 에이전트는 이동 단말의 위치를 RCoA로 인식하며 이 주소로 데이터를 전송하고 MAP은 RCoA(Regional Care of Address)와 LCoA(Local Care of Address)간의 바인딩 정보를 이용하여 데이터를 최종적으로 이동단말에게 포워딩시켜준다.

2.2 HMIPv6의 등록 절차

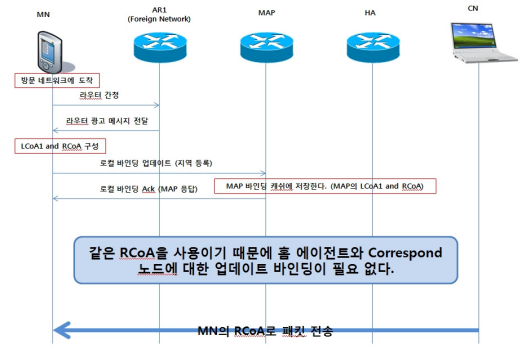
HMIPv6에서는 이동단말의 이동을 두 가지로 분류한다. 하나는 한 MAP 도메인 내에서 액세스 라우터간 이동을 가르키며 이것을 Micro Mobility 핸드오버라고 말한다. 다른 하나는 이동단말이 한 MAP 도메인에서 다른 MAP 도메인으로 이동했을 때를 가리키며 이것은 Macro Mobility 핸드오버라고 말한다. 본 논문에서는 Micro Mobility와 Macro Mobility의 두 경우를 고려하여 설명한다. (그림 3)에서와 같이 이동단말이 새로운 MAP 도메인으로 진입하였을 때, 이동단말은 새로운 액세스 라우터로부터 Router Advertisement (RA) 메시지를 수신한다. 이동단말은 액세스 라우터의 Prefix를 기반으로 LCoA를 생성하고, 이동노드가 스스로 LCoA에 대



(그림 3) HMIPv6의 기본 동작 과정



(그림 4) HMIPv6에 MAP 등록 절차



(그림 5) HMIPv6에 같은 MAP안의 지역적 등록 절차

한 DAD(Duplicate Address Detection)를 수행한다. LCoA 주소는 이동단말이 액세스 라우터를 이동할 때마다 새롭게 생성된다. 그리고 이동단말은 RA 메시지의 MAP option에 포함된 MAP의 Prefix를 기반으로 새로운 RCoA를 생성한다. RCoA 주소는 이동단말이 다른 MAP 도메인으로 이동하기 전까지 변경되지 않는다.

이동단말은 RCoA와 LCoA를 생성한 후 두 주소를 포함한 Local Binding Update (LBU) 메시지를 MAP에게 보낸다. MAP은 LBU 메시지를 수신한 후, RCoA 주소에 대한 DAD 검사를 수행한다. MAP은 이동단말의 RCoA 주소가 도메인 내에서 유일함을 확인한 후 MAP은 자신의 Binding Cache에 이동단말의 두 주소를 저장한다. 이 후 MAP은 MIPv6에서 이동단말의 HA(Home Agent)가 이동단말의 HoA와 CoA에 대하여 Proxy를 수행하는 것처럼, Proxy Neighbor Advertisement 메시지를 이용하여 이동단말의 RCoA로 도달하는 패킷들을 가로채어 이동단말의 LCoA로 터널링하여 전달한다. MAP이 이동단말의 RCoA와 LCoA를 Binding Cache에 저장한 후, 이동단말은 자신의 HA에게 위치 등록을 하기 위하여 Binding Update 메시지를 보낸다. Binding Update 메시지에는 HoA와 CoA로써 RCoA를 포함한다. HA는 이동단말의 HoA와 RCoA를 저장한 후, 이동단말에게 Binding Acknowledgement 메시지를 전송하는데 이 때 목적지 주소는 이동단말의 RCoA가 된다. MAP은 이동단말의 메시지를 가로채어 이동단말의 LCoA로 패킷들을 터널링하여 전달한다. HA와의 위치 등록이 완료된 후, 이동단말은 상대노드들에게 위치 등록을 할 수 있게 된다.

만일 이동단말이 MAP 영역 내에서 다른 AR로 이동하는 경우 HA/CN에 대해서는 동일한 RCoA를 가지므로 바인딩 갱신을 필요로 하지 않으며 LCoA를 갱신하는 지역적 바인딩 갱신만이 필요하게 된다. 즉 동일한 MAP 영역 내에서의 이동단말의 이동은 (그림 5)에서 보는 바와 같이 HA/CN에 투명하게 이루어진다. 이동 단말이 상대노드로 데이터를 전송하는 경우 MAP 간의 터널링을 통해서 전송하며, 상대노드와의 직접적인 전송을 하고 하는 경우 RCoA를 소스 주소로 하여 상대노드로 직접 데이터를 전송할 수도 있다.

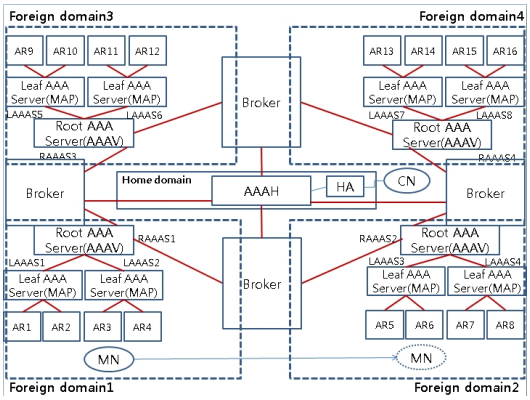
2.3 HMIPv6의 인증과 등록을 줄이기 위한 연구

[5]는 Root AAA서버(RAAAS)를 이용하여 도메인 내 이동 시 인증과 등록에 대한 지연이 줄어들 것임을 보여주고 있으며, [6]는 모바일 IPv6 및 AAA의 결합된 프로그램을 제시했다. 이는 AAA 프로토콜에서 핸드오프 메시지 이동으로서 상호작용 및 비용이 줄어들 것임을 보여준다. [7]은 링크 계층 핸드오프 시간의 전체를 사용하여 AAA의 프로세스를 수행할 수 있게 최적화된 빠른 핸드오프 절차를 보여주고 있다. [8]는 HMIPv6 아키텍처로 통합하여 Local 이동을 위한 지연 및 신호 메시지의 양을 줄일 수 있는 인증 체계를 제안했다. 그러나 이 기법은 단지 내부 지역 이동에 응용할 수 있고, 이동단말들이 도메인 간 이동이 잦을 때 효과가 적다. 게다가 [9]는 MIPv6의 보안 이슈에 책임이 있고, 모든 AAA 참여자들의 토폴로지에 관심이 많은 TAON(Topological-aware AAA Overlay Network) 모델을 제공했다. 그러나 그것들의 배포와 비용을 만드는 추가기능을 위한 안내가 없다. [10]의 전체 비용과 시간 지연에 대한 비교분석은 더 큰 범위로 줄어들게 된다. 하지만 여전히 이동단말의 이동성을 고려하는 동안 추가 조사를 해야 한다. 지금까지 언급한 참고 문헌에서, 기존의 연구들이 근본적으로 핸드오프 및 인증대기를 정말로 줄여줄 수 없다고 결론지을 수 있으며, 이 논문에서는 보다 나은 성능을 달성하기 위한 효율적인 인증 기법을 제안한다.

3. 계층적 인증 제안기법

3.1 계층적 AAA 제안 아키텍처

홈 도메인 내에서 이동단말이 이동할 때 홈 도메인에 있는 AAA 서버(AAAH)에서 네트워크에 대한 액세스를 얻기 위해 AAA 서비스를 해야 한다. 또한 이동단말의 방향이 홈 도메인 밖으로 이동하여 이동단말이 변경될 때 마다 방문한 도메인 (AAAV)

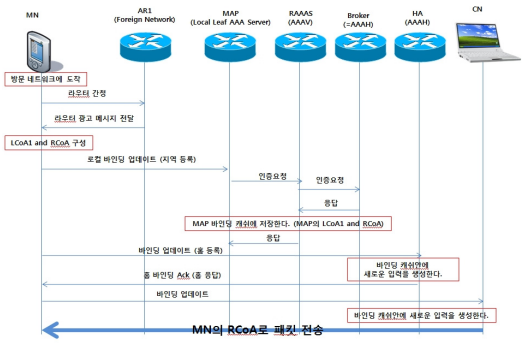


(그림 6) 계층적 인증 제안기법

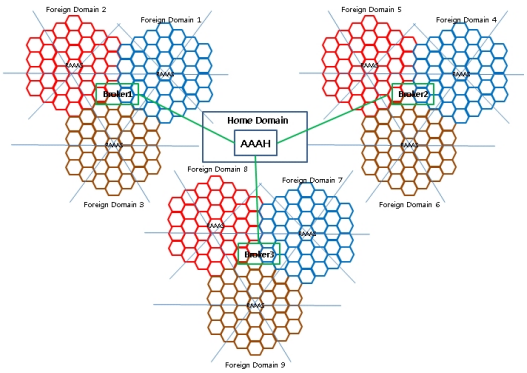
에서 AAA의 서버에 의해 인증되어야 하며, 아래와 같은 명확한 인증 절차를 거쳐야 한다.

첫 번째로 이동단말은 Local Leaf AAA 서버(LAAAS)로 인증 요청을 보내고, LAAAS는 요청 메시지를 AAAV 역할로서 행동하는 Root AAA 서버(RAAAS)로 전달한다. 두 번째로 Foreign 도메인에서 이동단말이 처음으로 도착하는 경우 아무 관련 없는 식별 정보가 Local RAAAS 내에 저장되고 AAAH에서 인증과 권한 허가를 필요로 하게 된다. 그러므로 인증요청 메시지는 AAAH로 전달되어지고 마침내 관련된 응답메시지가 RAAAS를 통하여 이동단말에게 전달되어지게 된다. 그러나 이때 이동단말이 홈 망에서 먼 거리에 위치한 경우 이와 같은 인증 방식은 긴 등록 시간을 유발하여 망에 불필요한 트래픽을 유발시키게 됨으로 인증요청 메시지를 AAAH로 전달하는 대신 AAAH의 대리인으로서 모든 역할을 수행하고 이동단말과 더 가까운 거리에 위치하면서 보안적인 측면에서 신뢰관계를 형성하고 있는 (그림 6)의 Broker에게 전달하고 마침내 관련된 응답 메시지를 RAAAS를 통하여 이동단말에게 전달한다.

그 후 이동단말이 Foreign 도메인 밖으로 이동하지 않는 경우, 단지 다른 LAAAS 관리 도메인 안에서 이동은 RAAAS의 인증만을 요구하게 된다. Foreign 도메인 안에서 RAAAS는 이동단말을 위한 AAA 서비스를 제공하는 AAAH의 대리인으로서



(그림 7) 제안 기법의 홈 도메인 내 등록 절차



(그림 8) 도메인 사이의 배포되어진 Broker의 환경

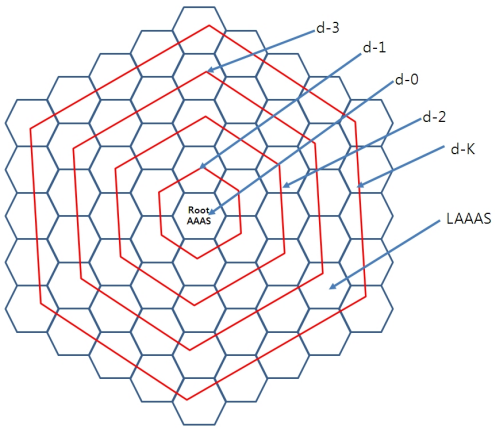
활동한다. 예전 RAAAS 관리 도메인에서 이동단말이 밖으로 이동하여 새로운 Foreign 도메인에 도착할 때 인증 매개 변수를 포함한 관련 정보가 외부 도메인에 처음 도착한 이동단말의 인증절차와 동일하게 Broker를 통하여 새로운 RAAAS에 전송된다. (그림 7)은 제안 기법의 홈 도메인 내 등록절차를 보여준다.

Broker와 AAAH는 최초 신뢰관계를 가지기 위해 인증 및 등록을 수행한다. 이는 최초 Broker가 설치되는 배포 시점에 이루어지게 되고, 해당 Broker가 설치될 때 Broker내에 관련된 AAAH에 대한 위치정보와 근접한 도메인에 대한 정보를 입력하고, 해당 Broker가 속한 AAAH에는 Broker에 대한 위치정보와 최초 인증 값이 저장된다. 이 후 Broker와 AAAH간의 인증 및 등록에 대해서는 신뢰관계가 형성되어 있으므로 본 논문에서는 고려되지 않는다. 즉, 이동단말이 도메인 사이를 이동 시 이동단말은 AAAH에게 인증과 권한허가를 요청하는 것이 아닌 Broker에게 인증과 권한허가를 요청하게 되며 이 때 Broker는 이미 AAAH와 신뢰관계가 형성되어 있게 됨으로 이동단말에 대한 인증과 권한요청을 처리하기 위해 AAAH로부터 인증 및 등록을 수행하지 않고 Broker와 가장 근접한 도메인에 위치한 움직임의 경우 AAAH를 대신하여 인증과 권한요청에 대한 응답을 이동단말에게 돌려주게 된다.

Broker는 각 Foreign 도메인에 근접한 위치에 배포되어 지며, 이동단말은 가장 가까운 도메인에 위치한 Broker에게 인증 요청메시지를 전달하여 응답메시지를 돌려받는다. 예를 들어 (그림 8)과 같이 여러 개의 육각형의 셀로 이루어진 도메인에서의 이동단말에 움직임의 경우 내부 도메인의 움직임은 이동단말이 속한 도메인에 가장 중앙에 위치한 RAAAS에게 인증과 권한 허가를 요청하게 되지만, 도메인 사이의 움직임의 경우에는 각 도메인에 가장 근접하게 위치한 Broker에게 요청하게 되며(최초 Broker와 AAAH의 인증 및 등록을 통하여 신뢰관계를 형성하며 Broker로부터 가장 근접한 도메인들에 대해서 이동단말의 도메인 사이에 움직임을 파악하여 이동단말이 속한 도메인에 가장 근접한 Broker에게 인증과 권한에 대한 요청을 하게 됨), 요청된 인증정보는 해당 Broker에게만 존재하게 된다. 즉, 도메인 사이에 존재하는 서로 다른 Broker는 각각의 Broker내에 저장된 인증정보를 서로 동기화 하지 않으며, 서로 다른 Broker에 존재하는 각각의 인증정보 또한 가지고 있지 않게 된다.

3.2 시스템 모델링

계층적 모바일 IP네트워크 [11]의 모델을 참고로 하여, 이 기법은 MAP위에 LAAAS를 배치한다. 그리고 홈 도메인과 각각의 Foreign 도메인 사이의 가장 근접한 거리에 신뢰관계가 형성된 Broker를 위치시킨다. (그림 9)에서 보여지는 바와 같이 RAAAS는 중앙(Layer0)에 있고, 그것으로부터 분산



(그림 9) RAAAS Domain States

되고 형성된 계층 1, 2와 기타 등이 있다. 6각형은 각 레이어 원형의 평탄하지 않은 선들과 계층 K에서 중앙으로의 거리가 m으로 설정되어 있다. 만약 관리 도메인이 K+1 계층들을 가지고 있고, 가장 바깥쪽의 한 계층이 계층 K라면 여기서 K는 관리 도메인의 크기와 관리도메인의 반경을 정의하는 것을 보여준다. RAAAS에서 LAAAS까지의 주어진 간격 사이에서 이동단말이 관리 도메인 밖으로 이동 시 발생하는 확률의 계산을 위하여 특정 간격 안에서 발생하는 어떤 사건 발생률의 분포를 표현하는데 사용되어지는 매개변수 λ를 가지는 푸아송 분포(Poisson distribution)를 사용하였다. 우리는 이동단말이 하나의 LAAAS 로부터 다른 LAAAS로의 이동[12]인 움직임을 정의했다. 그리고 [13]과 비슷한 방법을 통해 RAAAS 도메인에서 떠나는 이동단말의 평균 이동 시간을 계산했다.

이동단말이 RAAAS 도메인에서 떠날 때 까지 이동하는데 m시간을 필요로 한다고 가정할 때 내부 도메인 인증에 m-1, 도메인 사이 인증은 m 으로 정의하며, K는 RAAAS가 관리하는 LAAAS 계층의 수를 의미하며, 관리 반경을 나타낸다. m시간 움직임 이후에 이동단말이 관리 도메인 밖으로 이동할 확률을 0에서 K사이에 있는 누적 푸아송 확률 분포 함수로 나타내면 아래와 같다.

$$P^m = \left(\sum_{N=0}^{k}\frac{\lambda^N e^{-\lambda}}{N!}\right)^{m-1}\left(1-\sum_{N=0}^{k}\frac{\lambda^N e^{-\lambda}}{N!}\right);1\le m\le\infty \quad (1)$$

RAAAS 관리 도메인 밖으로 이동단말이 이동하기 전 평균 시간은 아래와 같다.

$$E(m)=\sum_{N=0}^{\infty} m\times p^m=\frac{1}{\left(1-\sum_{N=0}^{k}\frac{\lambda^N e^{-\lambda}}{N!}\right)} \quad (2)$$

주어진 몇 가지 값의 의미는 위의 (표 1)과 같다.

3.3 비용분석

지역이동의 총비용 C_{total} 은 세 가지 파트로 구성된다. 등록 신호의 전송비용(C_{reg}), 인증 신호의 전송비용(C_{auth}), 패킷 전송비용(C_{trans}). 본 논문에서등록과 인증신호의 전송비용은 C_{RA} 로 정의한 것과 함께 고려되어지며C_{trans} 는 패킷 처리와 전송비용을 의미한다.

$$C_{total}=C_{reg}+C_{auth}+C_{trans}=C_{RA}+C_{trans} \quad (3)$$

우리는 제안된 효율적인 결합 메커니즘과 이전 메커니즘의 등록과 인증신호 전송비용의 분석을 수행한다. 이동단말이 Foreign 관리 도메인으로 들어올 때 이동단말의 첫 번째 인증과 등록은 그것의 홈 도메인 안에서 완료되어진다. 제안된 기법의 도메인 사이의 인증비용은 C_{first} 로 정의한다. 그리고 다른 인증들은 내부 도메인의 다른 것 들이며, C_{other} 로 표시한다.

$$C_{first}=RA_B+RA_R+2C_{ML}+4C_{LR}+2C_{RB} \quad (4)$$
$$C_{other}=RA_R+2C_{ML}+2C_{LR}$$

(표 1) 매개변수의 의미

정 의	의 미
C_{ML}	RAAAS 도메인에서 이동단말이 이동할 때 LAAAS와 이동단말 사이의 인증 신호와 등록의 전송비용을 대표한다.
C_{LR}	Root AAA 서버와 서버가 제공하는 등록기능 사이의 인증 신호와 등록의 전송비용을 대표한다.
C_{RB}	RAAAS와 Broker 사이의 인증 신호와 등록의 전송비용을 대표한다.
C_{RH}	RAAAS와 AAAH 사이의 인증 신호와 등록의 전송비용을 대표한다.
RA_B	Broker의 등록과 인증 신호 처리 비용을 대표한다.
RA_H	AAAH 의 등록과 인증 신호 처리 비용을 대표한다.
RA_R	RAAAS 의 등록과 인증 신호 처리 비용을 대표한다.
μ	이동단말이 관리 도메인 내외에 서로 다른 네트워크로 이동하여 목적지에 도착하였을 때의 평균 도착 비율을 대표한다.
T	Foreign 도메인 내에 머무르는 이동단말의 상주시간을 대표한다.
P_H	AAAH의 패킷 처리 비용을 대표한다.
P_B	Broker의 패킷 처리 비용을 대표한다.
P_R	RAAAS의 패킷 처리 비용을 대표한다.
L_{HR}	AAAH와 RAAAS 사이의 거리를 대표한다.
L_{BR}	Broker와 RAAAS 사이의 거리를 대표한다.
L_{RL}	RAAAS와 LAAAS 사이의 거리를 대표한다.
η	단위 거리의 전송비용을 대표한다. 단위는 단지 한 홉이다.
K	RAAAS가 관리하는 LAAAS들의 계층들의 수를 대표한다.

이전 기법에서 매 번 발생되는 인증비용 C_{each} 는 아래와 같이 표시한다.

$$C_{each} = RA_H + RA_R + 2C_{ML} + 4C_{LR} + 2C_{RH} \quad (5)$$

본 논문에서 홉은 거리의 단위이며 유선링크의 전송비용은 거리의 직접적인 비율이다. 또한 거리 단위 전송 비용은 η으로 정의되고, 무선 링크 전송 비용은 유선링크 만큼의 θ 시간으로 나타낸다. 수식은 아래와 같이 표현 할 수 있다.

$$C_{first} = RA_B + RA_R + 2\eta(\theta + 2L_{RL} + L_{BR}) \quad (6)$$

$$C_{other} = RA_R + 2C_{ML} + 2C_{LR}$$

$$C_{each} = RA_H + RA_R + 2\eta(\theta + 2L_{RL} + L_{HR})$$

제안된 기법의 등록과 인증신호 전송비용을 나타내는 $C_{proposed-RA}$ 와 이전 기법의 등록과 인증신호 전송비용을 나타내는 C_{Pre-RA} 의 Foreign 관리 도메인 내의 등록과 인증신호 전송 평균비용은 아래와 같이 각각 계산되어 질 수 있다.

$$C_{\mathrm{Pr}oposed-RA} = \frac{C_{first} + (E(m)-1)\times C_{other}}{(E(m)-1)\times T} \quad (7)$$

$$C_{\mathrm{Pr}e-RA} = \frac{E(m)\times C_{each}}{(E(m)-1)\times T} \quad (8)$$

이전 기법과 제안된 기법의 패킷 전송비용은 아래와 같이 각각 계산되어 질 수 있다.

$$C_{pre-trans} = \mu \times (P_H + P_R + \eta \times (L_{HR} + L_{RL}))$$
$$C_{trans} = \mu \times (P_B + P_R + \eta \times (L_{BR} + L_{RL})) \quad (9)$$

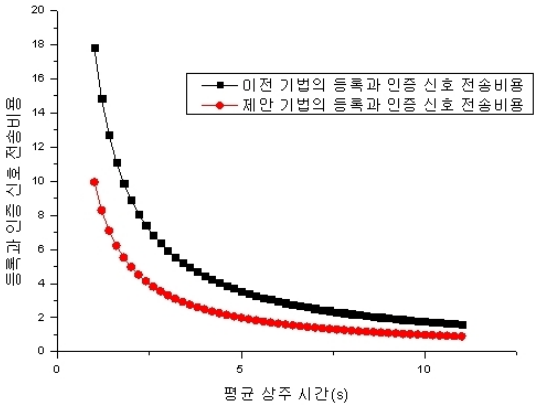
이전기법과 제안기법의 가장 큰 차이점은 이전 기법의 경우 내부 도메인과 도메인 사이의 인증 및 등록 시 매 번 AAAH를 통하여 비용이 발생하게 되고, 이동단말이 홈 망에서 더 먼 거리에 위치한 경우에도 AAAH와 RAAAS 사이의 인증 및 등록비용이 발생하게 된다. 또한 RAAAS와 AAAAH 거리만큼의 패킷 전송비용이 발생한다. 이에 반해 제안기법의 경우 인증 및 등록 시 첫 번째 인증은 AAAH가 아닌 각 도메인에 근접한 위치에 존재하는 Broker를 통하여 비용이 발생하게 되며, 이 후 다른 내부 도메인 인증은 RAAAS를 통하여 비용이 발생한다. 그리고 이동단말과 더 가까운 거리에 위치한 Broker 와 RAAAS 사이의 인증 및 등록비용, Broker와 RAAAS 거리만큼의 패킷전송비용이 발생하게 된다.

4. 성능평가

우리는 이동단말이 홈 망에서 보다 먼 거리에 위치했을 경우의 가정을 바탕으로 수학적 모델링을 적용하였으며, 이후에 적용한 매개변수 값은 [5]를 참조하였다. 수학적 모델링은 이동단말의 평균 상주시간, 평균 도착비율, Broker 또는 AAAH의 거리 등의 의존하는 연속성 모델을 표현하였으며, 매개변수 값의 매 변화마다 각 변화에 따른 예측 값을 제공한다. 본 논문에서는 수학적 모델링에 따른 데이터를 얻기 위해 주어진 매개변수 값을 가지고 수식에 따른 데이터를 추출하였다. 다음에 나오는 결과는 (표 2)에 정의된 값들에 부합되게 얻어진다. (그림 10)은 이전 기법과 제안된 기법의 기간 내 평균 상주시간 T에 대해 등록과 인증신호전송비용에 대한 영향을 나타낸다.

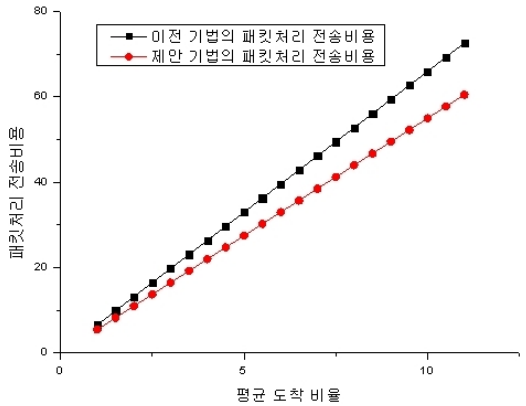
(표 2) 매개 변수들의 값

RA_H	RA_B	RA_R	P_H	P_B	P_R	η	θ	λ	L_{HR}	L_{BR}	L_{RL}
6	4	3	4	3	2	0.05	10	4	8	6	4



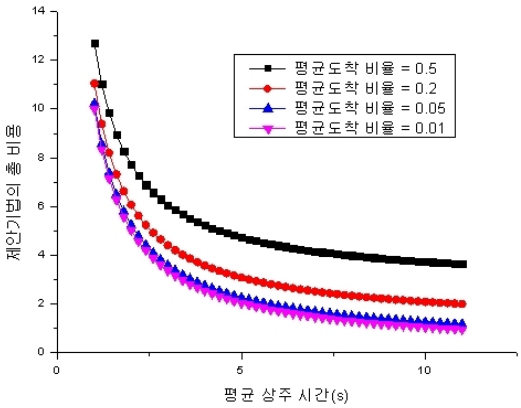
(그림 10) 이전 기법과 제안된 기법 사이의 인증신호와 등록 전송비용의 비교

(그림 10)의 데이터 변화 흐름으로부터 평균 상주시간 T의 증가 값에 따라 등록과 인증 신호 전송비용이 항상 줄어드는 것을 볼 수 있으며, 이것은 이동단말의 상주 시간의 증가에 따라 총 시스템 비용이 줄어드는 것을 의미하며 이전 기법과 비교해서 제안된 기법을 사용하였을 때 총 비용이 적어도 45% 감소 할 수 있음을 보여준다.



(그림 11) 이전 기법과 제안된 기법 사이의 패킷 처리 전송 비용의 비교

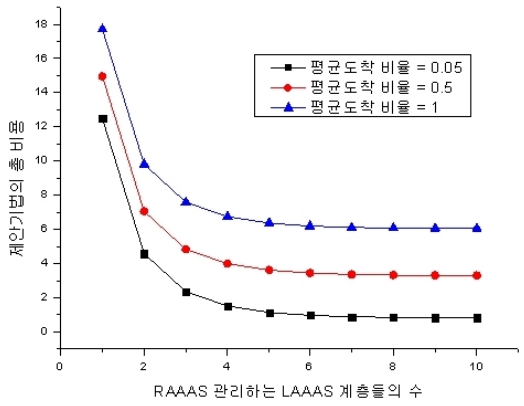
(그림 11)은 이전 기법과 제안된 기법의 이동단말의 평균 도착 비율 μ에 대해 패킷처리 전송 비용에 대한 영향을 나타낸다. 그림 11의 데이터 변화 흐름으로부터 이동단말이 하부 네트워크로부터 다른 네트워크로 이동하는 평균 도착 비율의 증가와 함께 패킷처리 전송비용이 증가하는 것을 볼 수 있으며, 평균 도착 비율이 증가할수록 이전 기법과 비교하여 제안된 기법을 사용하였을 때 평균 도착 비율의 증가와 함께 패킷 처리 전송 비용이 큰 폭으로 감소하는 것을 보여준다. (그림 12)에서 평균 상주 시간 T의 증가 값에 따라 제안기법의 총 비용이 감소하는 비용변화를 볼 수 있으며, 평균 도착 비율 μ의 값이 클수록 총 비용이 커지는 것을 알 수 있다. 또한 이론적인 분석으로부터 총 비용은 이동단말의 평균 도착 비율과 상주하는 시간에 의해서 영향을 받는 것으로 결론지을 수 있다.



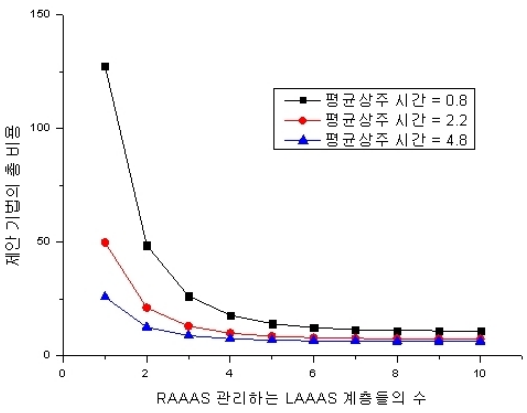
(그림 12) 평균 상주시간 증가에 따른 평균 도착 비율 값 사이의 총 비용의 비교

(그림 13)과 (그림 14)는 평균 도착 비율을 의미하는 μ값들과 평균 상주 시간을 의미하는 T의 값들에 의해서 RAAAS가 관리하는 LAAAS 계층들의 수를 의미하는 K값의 변화에 따른 총 비용의 구체적인 변화를 나타낸다.

(그림 13)은 RAAAS 관리 도메인 내에 이동단말의 평균 도착 비율 μ의 값이 클수록 더 큰 총 비용이 드는 것과 같이 총 비용에 영향을 주는 것을 보여준다. (그림 14)는 RAAAS 관리 도메인 내에 이동단말의 평균 상주 시간이 총 비용에 영향을 주는 것을 나타내며 이것은 평균 상주 시간 T가 작을수록 비용은 커진다는 것을 보여준다.

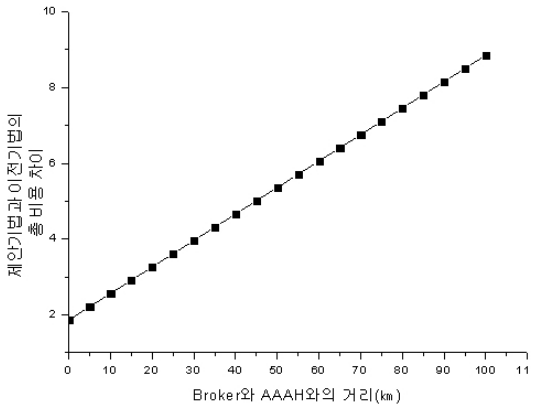


(그림 13) RAAAS가 관리하는 LAAAS 계층 수에 따른 제안 기법의 총 비용



(그림 14) RAAAS내의 평균 상주시간의 영향에 따른 제안된 기법의 총 비용

(그림 15)는 Broker와 AAAH와의 거리차이에 따른 제안기법과 이전기법의 총 비용차이 변화를 보여준다. 위 그림에서 Broker의 위치는 고정이고, 배포된 Broker의 위치가 AAAH에서 멀어질 경우 이동단말이 AAAH보다 더 가까운 위치에 존재하는 Broker를 통해 인증 및 등록, 패킷 전송 등을 수행할 때 이전 기법과 제안기법의 총 비용차이를 설명



(그림 15) Broker와 AAAH와의 거리에 따른 제안기법과 이전기법의 총 비용 차이

한다. (그림 15)의 데이터 변화 흐름으로부터 Broker와 AAAH와의 거리가 증가할 수 록 제안 기법과 이전 기법의 총 비용의 차이가 증가하는 것을 볼 수 있으며 Broker와 AAAH의 거리가 제안기법의 총 비용에 영향을 받는 것으로 결론지을 수 있다. 이는 Broker와 AAAH의 거리가 RAAAS로부터 가까이에 위치할수록 총 비용이 감소하는 것을 보여준다.

5. 결 론

계층적 인증구조를 분석하고 수립함에 있어 본 논문은 핸드오프와 인증대기를 줄이기 위한 효율적인 인증 기법을 제공한다. 이론적인 분석으로부터 총 비용은 평균 상주시간, 평균 도착 비율, RAAAS의 관리 반경, Broker와 RAAAS 사이의 거리 및 기타 등등 여러 가지 매개변수에 의해서 영향을 받는다는 것을 보여준다. 그리고 시뮬레이션 결과는 제안된 방식이 이전 기법에 비해 더 우수한 결과를 보여준다. 게다가 본 논문에서 제안한 Broker는 AAAH의 모든 기능을 수행하며 지리적으로 RAAAS에 가까이 위치하여 보다 적은 비용을 통해 신속한 Macro Mobility를 지원할 수 있음을 보여준다. 또한 Broker의 배포위치와 네트워크 토폴로지의 추가적인 의무 요구사항이 없고, 더 강한 발전성이 있는 정책을 만들 수 있다. 향후 연구과제로 Broker을 통한 QoS에 대한 연구와 보안 인증 서비스를 연구해 볼 계획에 있다.

ACKNOWLEDGMENT

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2010-0024695). 교신저자 : 정종필.

참 고 문 헌

[1] Johnson D, Perkins C, Arkko J. Mobility Support in IPv6. IETF RFC3775, 2004

[2] Youngsong Mun, Kyunghye Lee. Fast Macro Mobility Handovers in HMIPv6, draft-mun-mipshop-fhmacro-05.txt, IETF, 2010

[3] Soliman H S, et al. Hierarchical Mobile IPv6 Mobility Management. IETF RFC 4140, 2005

[4] Wei D, Liu Y H, Yu X G, et al. Research of Mobile Ipv6 Application Based on Diameter Protocol. 2006 International conference on Multi-Symposiums, Computer and Computational Sciences (IMSCCS'06), IEEE Computing Society Press, 2006

[5] WANG Li, SONG Mei, SONG Jun-de, An efficient hierarchical authentication scheme in mobile IPv6 networks September 2008, 15(Suppl.): 9 - 13

[6] Laurent M, Dupont F. Inter-domain security for mobile Ipv6.The 2nd European Conference on Universal Multiservice Networks (ECUMN 2002), IEEE press, 2002, 238 - 245

[7] Lee S Y, Huh E N, Kim S B, et al. An Efficient Performance Enhancement Scheme for Fast Mobility Service in MIPv6. 2005 International Conference on Computational

Science and its Applications (ICCSA 2005), 2005, Singapore, 2005: 628 – 637

[8] Kim M Y, Kim M S, Mun Y S. A Hierarchical Authentication Scheme for MIPv6 Node with Local Movement Property. 2005 International Conference on Computational Science and its Applications (ICCSA 2005), 2005, Singapore, 2005: 550 – 558

[9] Li J, Ye X M, Tian Y. Topologically-Aware AAA Overlay Network in Mobile IPv6 Environment. The 5th International Conference on IFIP-TC6 Networking, May 2006, Portugal, Coimbra: 2006: 293 – 306

[10] Xiao W S, Zhang Y J. Hierarchical AAA in mobile IPv6 networks. The Journal of China Universities of Posts and Telecommunications. 2006, 27(2): 50 – 55

[11] Pack S, Choi Y. Performance Analysis of Hierarchical Mobile IPv6 in IP-based Cellular Networks. IEEE 2003 International Conference of PIMRC, 2003, Beijing, China: IEEE, 2003

[12] Chiang K, Shenoy N. A Random Walk Mobility Model for Location Management in Wireless Networks. IEEE 2003 International Conference of PIMRC, 2003, Beijing, China: IEEE, 2003

[13] Jiang X, Akyildiz L F. A novel distributed dynamic location management scheme for minimizing signaling costs in mobile IP. IEEE 2002 International Conference on Mobile Computing, 2002: IEEE Trans, 2002(3): 163 – 175

◐ 저 자 소 개 ◑

정 하 권

2007년 한국교육개발원 (공학사)
2011년 성균관대학교 정보통신대학원 컴퓨터공학과 (공학석사)
관심분야 : 차세대 네트워크, 시스템 보안, 네트워크 보안
E-mail : junhg7@skku.edu

정 종 필

1997년 성균관대학교 (공학사)
2003년 성균관대학교 정보통신공학부 (공학석사)
2008년 성균관대학교 정보통신공학부 (공학박사)
관심분야 : 무선/이동 네트워크, 차량 네트워크, 네트워크 보안등
E-mail : jpjeong@skku.edu