계층적 캐싱을 이용해 로밍 확장성을 높인 인증 프레임워크

(A Scalable Authentication Framework for Fast Remote Roaming with Hierarchical Caching)

이 희 진 † 송 유 경 † 이 명 수 †† 김 종 권 †††
(Heejin Lee) (Yu-Kyong Song) (Myung Soo Rhee) (Chong-Kwon Kim)

요 약 국제 로밍 및 이기종 망간 핸드오버가 활성화된 환경에서 사용자에게 부드러운 통신 서비스를 지원하기 위해서는 보다 빠르고 확장성이 뛰어난 인증 기법이 필요하다. 본 논문은 빠른 로밍을 지원하기 위한 확장성 높은 인증 프레임워크에 관한 것으로, 직간접적으로 구성된 도메인간의 일반적인 신뢰 관계를 바탕으로 계층적 캐싱을 구성한다. 계층적 인증 캐싱을 이용할 경우 확장성을 보장함은 물론 인증 지연 및 인증으로 인한 망의 부하를 줄일 수 있으며, 이를 수학적으로 분석하였다.

키워드 : 인증, 국제 로밍, 이기종 망간 핸드오버, 빠른 핸드오버, 확장성, SSO, 신뢰 관계

Abstract As the demand on ubiquitous communication increases, global roaming and vertical handover will be prevailing in the near future. Since this environment is accompanied by the frequent handovers at remote sites, a scalable and fast authentication becomes prerequisite for ubiquitous communication. In this paper, we suggest a framework for scalable and fast authentication, using hierarchical caching based on general trust relationship among domains. At the end, we show that the proposed scheme achieves reduced authentication delay and network overhead through an analytic method with fluid flow model.

Key words : Authentication, international roaming, vertical handover, fast handover, scalability, SSO, general trust relationship

1. 서 론

언제 어디에서나 끊기지 않는 통신 서비스를 제공하기 위해, 향후 국제 로밍은 물론 이기종 망간 핸드오버가 보편화될 것으로 전망된다. 이런 환경에서는 이동 단말의 인증 도메인간 로밍이 더욱 잦아지는데, 이 때 인증 지연이 지나치게 길어지면 부드러운 로밍 서비스를 제공할 수 없게 된다. 또한 원거리에서 홈도메인으로 발생하는 인증 요청이 잦아지므로 망 부하가 더욱 심각해질 것이다. 따라서 본 논문은 이동 단말에게 안전하게 확장 가능하고 빠른 로밍을 지원할 수 있는 인증 기법을 제안하고자 한다.

기존에 제안된 원격지 인증 기법은 기본적으로 이동 단말이 홈도메인에서 벗어난 원격지에서 인증을 시도하는 경우, 원격지의 인증서버가 홈도메인의 인증서버와 직접 연동하여 인증을 받게 된다. 예를 들면, RADIUS (Remote Authentication Dial-In User Service[1])나 DIAMETER[2]의 프락시(proxy) 및 전달(relay) 기능을 각종 EAP(Extensible Authentication Protocol)-method[3,4] 등의 기존 인증 프로토콜과 함께 사용하면 원격인증을 지원할 수 있다. 이때, 전달되는 인증 정보의 형태와 경로는 다양하나, 다른 도메인으로의 로밍이 일어나, 그에 따른 인증을 시도할 때마다, 홈도메인의 서버와 직접적인 연동을 피할 수 없다는 공통점이 있다. 이와 같은 원격지에서의 홈도메인과의 연동은 인증 지연을 증가시키고, 부드러운 핸드오버와 로밍의 확장성을 저해하는 요인이 된다.

예외적으로 원격 인증서버가 이동단말 및 사용자에

· 본 연구는 KT정보보호단의 지원을 받아 수행되었음.
† 학생회원 : 서울대학교 전기.컴퓨터공학부
heejin@popeye.snu.ac.kr
songyk@popeye.snu.ac.kr
†† 정 회 원 : KT 정보보호단 팀장
msrhee@kt.co.kr
††† 종신회원 : 서울대학교 전기.컴퓨터공학부 교수
ckkim@popeye.snu.ac.kr
논문접수 : 2004년 12월 29일
심사완료 : 2005년 7월 26일

대해 과거에 인증이 성공한 사실을 여러 방법을 통해 확인할 수 있고, 인증 정보가 만료(expire) 되지 않았을 경우, 홈도메인에서 직접 인증을 받지 않고 사용자의 인증 요청을 수락할 수 있다[5,6]. 그러나 [5,6]은 특별한 경우에 대한 최적화 방안으로, 모든 경우에 적용되지 않는다. [7]은 응용계층 로밍 기법으로 리커버리 프락시(Recovery Proxy)를 사용하여 클라이언트의 요청이나 서비스 결과를 캐싱하게 하고, 클라이언트가 재요청을 하는 경우 프락시에서 리트리브하는 방식을 제안하였고, [8]은 [7]을 확장한 것으로 프락시 서버를 여러 지역에 분산하는 기법을 제안하였다. 그러나 [5,6] 및 [7,8]은 과거의 인증 정보를 확인할 수 있는 원격지 서버가 새로운 서버의 인증 요청 (이기종망간 로밍으로 인한)을 홈도메인 서버를 대행해 처리해 주지 않는 한계가 있다.

또한 커버로스(Kerberos) v5의 포워더블 티켓 (forwardable ticket)[9]은 일종의 인증 대행 기능이 있어서, 새로운 원격지에 대한 인증을 과거에 인증 사실을 확인할 수 있는 서버에서 대행할 수도 있다. 그러나 이동단말 및 사용자에게는 현재 위치에서 인증 지연 및 망 부하가 가장 작은 인증 대행 서버에 대한 정보가 없기 때문에 인증 지연 감소를 보장할 수 없게 된다. 또한 커버로스 v5에서는 인증을 요청하는 원격 도메인과 홈도메인 혹은 인증 대행 도메인 사이의 인증 체인을 형성하기 위해, 두 도메인 사이에서 직접 신뢰 관계에 있는 모든 도메인의 서버가 참여해야 하므로, 평균 인증 지연의 증가는 물론, 중간 서버의 부담이 커져 확장성이 떨어지는 단점이 있다.

WCDMA(Wideband Code Division Multiple Access[10]) 에서는 사용자가 인증을 요청한 원격지의 도메인으로 홈도메인의 사용자 프로파일을 가져와, 원격지의 베이스 스테이션(base station: BS)을 옮겨 다니는 동안 홈도메인으로 인증 요청하는 것을 방지하고 있다. 그러나 이는 WCDMA간 로밍에 국한된 방식이므로, 이기종의 다른 도메인으로 사용자가 로밍하는 경우에 대한 확장 가능한 일반적인 인증 방식을 구체화할 필요가 있다. 다시 말해, WCDMA에서는 인증 정보를 캐싱할 에이전트의 계층 구조를 동적으로 관리하고, 계층 구조를 이용해 인증 지연을 최소화하기 위한 빠른 인증 절차를 구체적으로 제시하고 있지 않다.

따라서 본 논문에서는 원격지에서 잦은 로밍이 발생할 때, 로밍 품질을 향상 시키기 위해서 인증 지연 및 인증으로 인한 망의 부하를 최소화 시킬 수 있는 인증 프레임워크를 제안하고자 한다. 특히, 홈도메인과 원격 도메인간에 존재하는 계층 구조가 없는 일반적인 신뢰 관계(general trust relationship)를 바탕으로 계층적 인증 캐싱을 형성하므로, PKI와 같이 계층적 신뢰 관계를 이용한 기존 기법이 갖는 확장성의 한계를 극복하였다.

본 논문은 2장에서 기존에 제안되었던 인증 기법과 단점을 설명하고 3장에서 본 논문에서 제안하는 인증 프레임워크 및 프로토콜을 기술한 후 4장에서 플루이드 플로우 모델을 이용해 인증 지연 및 망 부하 성능 분석을 한다. 이어, 5장에서는 4장에서 세운 모델을 통해 얻은 분석 결과를 바탕으로 제안된 프레임워크와 기존 기법의 성능을 비교 분석한다. 끝으로 6장에서 결론을 맺고 향후 과제에 대해 논한다.

2. 도메인 간 인증(Inter-domain Authentication)을 위한 기존 기법

이기종망간 로밍을 포함해 도메인간 로밍 (Inter-domain Roaming)으로 인해, 원격지에서 인증을 받을 수 있는 기존 기법은 다음과 같다.

2.1 프락시(Proxy) 기반 인증

프락시 기반의 인증 방법은 사용자와 홈도메인 인증 서버간의 인증 프로세스를 사용자가 방문하고 있는 지역 인증서버가 중계하는 인증 방식이다. 이때, 사용자는 인증 정보 (예 ID 및 Credential)를 프락시인 지역 인증서버에게 전달하고, 지역 인증서버는 그 인증 정보를 홈도메인의 인증서버로 전달한다. RADIUS[1]는 가장 널리 쓰이고 있는 사용자 인증 프로토콜로, 사용자가 원격지에서 인증을 시도할 때, 홈도메인의 인증서버와 연동하여 인증을 받아야 하는 단점이 있다. 따라서 홈도메인에서 멀리 떨어진 원격지에서는 인증 지연 (Authentication Delay)이 길어질 수 밖에 없다. 이때 사용자가 홈도메인과 간접적인 신뢰 관계에 있는 원격지에서 인증을 받기 위해서는, 직접적인 신뢰 관계로 연결된 중간 도메인들을 거쳐서 홈도메인과의 연동을 시도하게 되어 지연은 더 길어진다. 그리고 사용자가 자신의 인증 정보를 원격지 인증서버 (사용자와 원격지 서버 사이에는 신뢰 관계가 없다)에게 노출해야 하므로 신원 보호(Identity Protection)가 어렵게 된다.

'3GPP-WLAN(Third Generation Partnership Project-Wireless Local Area Network) 상호연동 시나리오'[11]는 RADIUS 및 DIAMETER[2]를 쓸 수 있는 좋은 예이다. '3GPP-WLAN 로밍 모델'에서, 직접적인 신뢰 관계가 있는 도메인 사이의 로밍과 신뢰 관계가 없는 도메인 사이의 로밍 시의 사용자 인증 과정을 살펴보면 다음과 같다. 로밍 모델은 3GPP[10]가 주체가 되며, 3G (3세대)망에만 계정을 가지고 있는 사용자 (Mobile Station)가 3G망의 데이타 서비스뿐 아니라 WLAN 서비스도 동시에 사용할 수 있도록 고려한 시나리오이다.

사용자는 WLAN망으로 로밍 한 후, 최초 EAP-response/

identity 메시지를 통해 자신의 ID를 WLAN망의 인증 서버로 전달한다. 단, 여기서 사용자의 ID, 즉 NAI-1 (Network Address Identifier)은 username@home_domain의 형태이며 home_domain은 사용자의 홈도메인인 3G망에 해당한다. 사용자의 ID를 전달 받은 WLAN 서버는 해당 3G망 (사용자의 홈도메인)과 직접 신뢰 관계가 있는지 확인한다. 그리고 WLAN망과 사용자의 3G망 사이에 로밍 협약이 맺어져 있다면 해당 3G망으로 바로 AAA(Authentication, Authorization and Accounting) Access-request 메시지를 보내게된다. 한편, WLAN망과 사용자의 홈도메인 사이에 직접적인 신뢰 관계가 없을 경우에는 WLAN망이 자신과 로밍 협약을 맺고 있는 3G망의 목록을 담아서 사용자에게 Network advertisement 메시지를 보낸다. 그러면 사용자는 Visited 3G망을 선택하여 그에 맞게 NAI-2를 구성한다. NAI-2는 username@visited_3G_PLMN.Home_3G_PLMN (Public Land Mobile Network)의 형태가 된다. 그래서 이 Visited 3G망을 경유하여 결국 사용자의 인증 요구 메시지가 홈 3G망까지 프락싱(Proxying)되는 것이다. 이렇게 사용자의 인증 요구 메시지가 3G AAA Server에 전달되면, 3G AAA Server는 HLR (Home Location Register), HSS(Home Subscriber Server)와 연동하여 사용자의 WLAN subscription profile과 인증 정보를 알아내고, EAP-AKA(Extensible Authentication Protocol - Authentication and Key Agreement[3])나 EAP-SIM(Extensible Authentication Protocol - Subscriber Identity Module[4]) 등에 기반한 인증 및 키 분배 과정이 이루어진다. 이를 통해 인증이 성공하면 3G AAA Server는 Access-accept메시지를 전송하고, 사용자는 WLAN서비스를 받을 수 있게 된다. 결국, WLAN망의 인증서버는 사용자와 홈도메인 간 인증 작업의 중간에서 둘 사이의 메시지를 전달해주는 RADIUS 클라이언트 역할을 하고, 3G 홈도메인의 인증서버가 RADIUS 서버가 되어 EAP method등을 통해 인증하는 구조가 된다.

[12]는 WLAN 도메인들 사이에서의 기본적인 로밍 기법을 제안하고 있다. 사용자가 홈도메인을 떠나 원격망으로 이동하면 원격지의 지역 인증서버가 자신의 공개키 인증서를 이동단말에 전달하여 안전한 SSL (Secure Socket Layer) 채널이 형성된다. 사용자는 이 채널을 통하여 자신의 인증 정보를 지역 인증서버로 전달한다. 이 때 사용자의 인증 정보는 username@home_domain, 암호 등이 된다. 그리고 지역 인증서버는 인증 정보를 사용자의 홈도메인 인증서버로 전달하여 인증 결과를 기다리게 된다. 이러한 방법은 홈도메인의 중재를 필요로 하므로 인증 지연을 야기시키는 문제를 가진다. 또한 암호 기반의 인증이므로 강력한 보안을 제공하지 못하고, 사용자의 인증 정보가 원격지 인증서버에 노출이 된다. 또한 PKI(Public Key Infrastructure)의 사용에 따르는 CA(Central Authority) 의 확장성 및 신뢰관계의 계층구조 상의 문제가 내재하게 된다.

이상과 같이 프락시 기반 인증은 직접 신뢰 관계가 있는 도메인 간 로밍이나 간접적인 신뢰 관계가 있는 도메인 간 로밍의 경우 모두, 홈도메인 서버와의 직접적인 연동을 피할 수 없다는 단점이 있다.

2.2 SSO(Single Sign On) 인증 기법

빠른 로밍을 위해서는 로밍에 따른 재인증 없이 통신이 지속되도록 하는 것이 유리한데, 이때 SSO(Single Sign On) 인증 기법을 사용할 수 있다. SSO 기법에서 사용자는 본인이 등록되어 있는 홈도메인으로부터 정식 인증을 받으면 그 후에 다른 도메인이나 서버로 이동해서 간단한 지역 인증 절차를 거치면 서비스를 받을 수 있다. SSO 인증의 대표적인 방법으로 커버로스[9]를 들 수 있으며, 최근 제안된 기법으로 [13-16]가 있다. 그러나 이들은 모두 글로벌 로밍을 지원하기 위해 필수적인 확장성을 보장하지 못한다.

커버로스에서는 인증서버가 사용자를 인증하기 위하여 비밀키 암호화(Symmetric Key Cryptography)방식을 사용한다. 그리고 인증서버는 전체 네트워크의 N개의 서버와 N명의 사용자 모두와 신뢰 관계를 가지며 비밀키를 공유한다. 커버로스 시스템에서 사용자가 각각의 서버에 인증 받기 위해서는 각 서버에 맞는 티켓(Ticket)이 필요하다. 이 티켓은 TGS(Ticket Granting Server)가 발급하는데, 사용자는 우선 TGS에 대한 티켓을 발급 받기 위하여 인증서버로부터 인증을 받고, 그 결과 획득한 TGS에 대한 티켓, TGT (Ticket Granting Ticket)을 사용 하여 TGS에게 사용하고자 하는 서버에 대한 티켓을 요청하게 된다. 이 과정에서, TGS로부터 각 서버에 대한 티켓을 받을 때에는 재인증을 받을 필요 없이 TGT만으로 가능하다는 점에서 SSO 인증이 된다.

커버로스에서는 크로스-렐름(Cross-Realm) 인증을 지원하는데 이는 사용자가 다른 도메인의 서버를 사용할 수 있도록 하는 방법이며, 이 메커니즘을 통해서 도메인 내에서의 SSO인증뿐 아니라 서로 다른 도메인 사이에서의 SSO 인증도 지원한다. 이를 위해 커버로스 시스템에서는 망의 각각의 도메인을 렐름(Realm)으로 정의하며, 각 렐름은 고유의 인증서버와 TGS, 사용자들로 구성된다. 크로스 렐름 인증을 위해서 두 렐름 사이에 Inter-Realm Key라는 공유키(Shared Key)가 필요하다. 그림 1은 커버로스의 크로스-렐름 인증 과정을 나타낸 것이다.

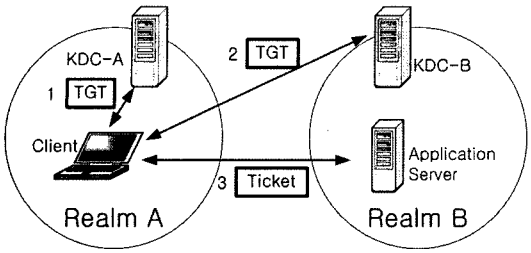


그림 1 커버로스의 'Cross-Realm 인증' 과정으로 두 렐름 간에 직접 신뢰 관계가 있는 경우

그림 1은 Realm A에 속한 사용자가 Realm B에 속한 어플리케이션 서버를 사용하기 위해서 Realm B의 TGS에게 크로스-렐름 인증을 받는 과정으로 다음과 같은 단계를 거친다. 1) 사용자는 'Realm B'에 있는 어플리케이션 서버에 대한 티켓을 자신의 TGS (그림에서 KDC)에게 요청한다. 그러면 Realm A의 TGS는 Realm B와 직접 신뢰 관계에 있는지 확인한다. 그림 1은 Realm A와 Realm B사이에 직접 신뢰 관계가 있는 경우이다. 따라서 Realm A의 TGS는 바로 Realm B의 TGS에 대한 TGT을 사용자에게 발급해 줄 수 있다. 이 때, TGT은 두 렐름 사이의 공유키로 암호화되어 사용자에게 전달된다. 2) 사용자는 Realm B의 TGS에게 자신의 홈도메인에서 발급 받은 TGT을 제시하고 어플리케이션 서버에 대한 티켓을 요청한다. 그러면 'Realm B'의 TGS는 공유키로 TGT을 확인하고 어플리케이션 서버에 대한 티켓을 발급해 준다. 3) 사용자는 Realm B의 TGS로부터 받은 티켓을 사용하여 서비스를 받을 수 있다. 커버로스는 홈도메인의 인증서버로부터의 재인증이 필요 없는 SSO을 제공하지만, 그림에서 볼 수 있듯이 다른 도메인의 서비스를 받기 위해서는 홈도메인(홈도메인의 TGS)과의 연동이 필요하게 된다.

커버로스는 직접 공유키를 나눠 갖고있지 않으나, 간접적인 신뢰 관계에 있는 도메인 사이의 크로스-렐름 인증도 제공한다. 이때 그림 2와 같이 직접 신뢰관계에 있는 렐름 사이에 부모-자식 관계를 맺는 트리(Tree)를 구성하여, 계층적 관리가 이루어진다. 그림 2에서 도메인 B는 도메인 A, D, E와 각각 신뢰 관계를 맺고 있으며 키를 공유하고 있다. 도메인 B와 G의 경우와 같이 직접적인 신뢰 관계가 없는 도메인 사이의 크로스-도메인 인증은 두 도메인 사이의 중개 도메인 들을 경유하여 일어나게 된다. 예를 들어, 도메인 B에 속한 사용자가 도메인 G의 애플리케이션 서버를 사용하고자 하는 경우 다음과 같은 과정을 거친다. 우선, 사용자는 홈도메인 (도메인 B)의 TGS에게 도메인 G에 대한 티켓을 요청한다. 도메인 B는 도메인 G와 직접 신뢰 관계가 없으므로 그림 2의 계층구조에서 G로 가는 최단 경로(Shortest Path)상에 있는 도메인 A에 대한 티켓을 사용자에게 준다. 그러면 사용자는 다시 도메인 A의 TGS에게 도메인 G에 대한 티켓을 요청하게 되고, 도메인 A 역시 도메인 G와는 직접 신뢰 관계가 없으므로 도메인 C에 대한 티켓을 발급해 준다. 사용자는 도메인 C의 TGS로부터 원하던 도메인 G에 대한 티켓을 받을 수 있게 된다. 이와 같이, 간접적인 신뢰 관계에 있는 두 도메인 사이의 크로스-렐름 인증은 홈도메인 서버와의 연동뿐 아니라 신뢰 계층 구조 상의 중간 도메인 서버와의 연동도 요구되므로 인증 지연이 길고, 확장성이 떨어지는 단점이 있다.

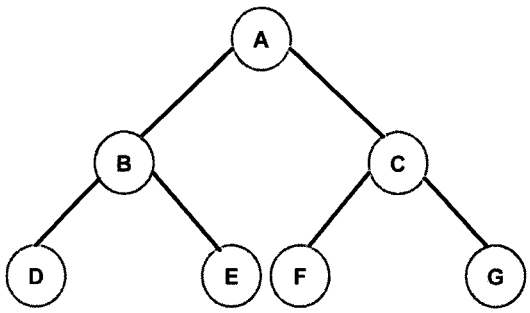


그림 2 신뢰 계층 구조

[13]는 홈도메인 인증서버의 개입 없이 이동단말과 원격지 인증서버 사이의 상호인증을 가능하게 하는 기법을 제안한다. 기본적으로는 공개키 암호화 방식(public key cryptographic technique)을 사용하지만, 기존의 X.509와 같은 공개키 인증서가 아닌 각 도메인들에서 직접 발급하는 공개키 인증서를 사용하도록 한다. 즉, 기존의 공개키 인증서를 사용하면 도메인들 마다 서로 다른 인증센터(CA: Certificate Authority)와 신뢰 관계가 있으므로 로밍을 위해서 인증체인(certificate chain)을 형성해야만 한다. 따라서 이동단말과 각 도메인 모두가 루트 인증센터(root CA)로부터 그 이하 체인 상의 모든 CA들과 신뢰 관계가 있어야 원격지에서의 인증이 가능하게 된다. 따라서 본 논문은 인증서를 CA를 통하지 않고도 각 도메인에서 생성하는 기법을 제안한다. 예를 들어 도메인 X는 자신의 비밀키/공유키 쌍 (private/public key pair: SK_X/PK_X)을 직접 생성하며 이때 자신과 신뢰 관계를 맺고 있는 도메인 Y 및 Z로부터 자신의 공유키에 서명하도록 한다. 그 결과 도메인 X의 공개키 인증서는 $SK_Y<<PK_X>>$, $SK_Z<<PK_X>>$의 형태가 된다. (여기서 'A<<B>>'는 B가 A로 암호화된 것을 의미한다.) 도메인 X는 가입자에게 자신의 비밀키

로 서명된 공개키 인증서 SK_X<<$PK_{subscriber}$>>를 발급해 준다. 이와 같은 변형된 공개키 인증서를 사용한 이동단말과 지역 인증서버 사이의 최초 상호 인증은 SSL 핸드쉐이크 프로토콜(Secure Socket Layer handshake protocol)과 같은 형태로 이루어진다. 즉, 도메인 Y에 속한 이동단말이 도메인 X로 이동하면, 원격지 인증서버는 자신의 공개키 인증서 SK_Y<<PK_X>>를 사용자에게 제시하고 사용자는 자신의 도메인으로부터 전달 받은 PK_X를 사용하여 도메인 Y를 인증하고, 사용자는 공개키 인증서를 원격지 인증서버에 제시하여 상호 인증이 가능하게 된다. 핸드쉐이크 과정을 모두 거치고 나면 사용자와 원격지 이동단말 사이에 인증값(shared secret)이 생성되고 최초 인증을 거친 원격지 도메인 내에서의 로밍 시에는 이 인증값을 사용하여 지역적 인증이 가능하다. 홈도메인 서버나 CA의 도움 없이 지역적 인증이 가능하다는 장점이 있지만 이동단말이 로밍을 시도하는 도메인 사이에 직접적인 신뢰관계가 있어야 한다는 한계가 있다.

[14]에서는 도메인간 인증을 위하여 각 도메인의 인증서버 이외에 로밍 프로바이더(RP: roaming provider)라는 서버를 사용하는 방법을 제안한다. RP는 각 도메인들과 신뢰 관계를 유지하는데, RP와 신뢰 관계를 맺고 있는 도메인들 사이에서 사용자의 로밍이 가능하다. 우선, 사용자는 RP로부터 사용자 계정 및 암호 혹은 인증서와 같은 인증 정보를 얻는다. 그리고 도메인 X 로 로밍을 원하는 경우, 이 인증 정보를 도메인 Y의 인증서버로 전달하고 인증서버는 RP로부터 사용자를 인증 받게 된다. 이 경우 도메인 Y는 RP와 신뢰 관계를 맺고 있어야 한다. 이때 사용자의 인증 정보가 서비스 공급자에게 누출이 된다는 문제가 발생한다. 이를 극복하기 위해서는 도메인의 인증서버도 사용자에게 인증을 받도록 하는 상호 인증이 필요하다. [14]에서 제안한 기법은 각 도메인의 인증서버에서 사용자의 인증 정보를 관리할 필요 없이 여러 도메인을 연결해주는 RP에서만 그 역할을 담당하고 사용자 로밍도 대행해 준다는 장점이 있다. 또한 RP를 지역적으로 여러 군데에 위치시킬 경우 홈 도메인을 경유하는 로밍에 비해 인증 지연이 감소될 수 있다. 그러나 이 방법 또한 RP와 직접적인 신뢰 관계를 갖는 도메인간 로밍에만 사용 가능하다는 한계가 있다. 또한 도메인 별로 사용자 정보를 관리하고 있는 상황에서 인증 정보를 통합 관리하기에는 현실적인 어려움이 따른다.

[15]는 사용자의 계정을 하나로 통합하여 인증서를 보안 토큰 서비스(Security Token Service)에서 관리하고 인증하는 기법을 제안한다. 사용자 인증은 Security Token Service에서 하고, 토큰을 관리하는 써큘레이터(Circulator)를 두어 인증된 사용자에게 토큰을 생성하여 주고 도메인 간에 토큰을 교류시키는 방식으로 다음과 같은 단계를 거친다. 우선, 로밍 서비스를 받고자 하는 사용자는 로밍 시 사용할 동적 토큰을 받기 위해 Circulator에 접속한다. Circulator가 인증서를 통해 사용자를 인증하고 사용자에게 동적 토큰을 발급해준다. 여기서 동적 토큰은 '(D_1,D_2,,,,D_n)'과 같은 일련의 토큰 집합의 형태로 사용자에게 전달되며 사용자는 로밍 시 이 일련의 토큰들을 한번에 하나씩 사용하게 된다. 이때, 동적 토큰은 'D_{n-1}'을 통하여 'D_n'을 인증할 수 있도록 만들어진다. 어떤 사용자가 도메인 X에 처음 접속을 시도하는 경우 사용자는 첫째 토큰 'D_1'과 자신의 인증서를 제시하고, 도메인 X는 Circulator를 경유하여 사용자를 인증하게 된다. 이후 도메인 X는 토큰과 인증서를 보관하는데, 토큰 값과 인증서가 서로 연관되어 저장이 된다. 만일 사용자가 도메인 X를 다시 방문하면 사용자는 다음 토큰인 'D_2'를 제시하고 도메인 X는 저장되어 있던 'D_1'을 사용하여 'D_2'를 인증할 수 있다. 인증 과정을 다시 거칠 필요 없이 토큰만 사용하여 사용자를 인증할 수 있게 된다. 문제는, 사용자가 다른 서비스 제공자로 로밍 시 토큰의 인증을 어떻게 하는가 이다. 만일 사용자가 도메인 X에서 'D_2'를 사용하고 나서 도메인 Y로 옮겨가 'D_3'를 제시 한다면 도메인 Y는 'D_2'값을 알고 있어야 할 것이다. 이 역할을 Circulator가 담당하게 된다. 즉, Circulator는 각 도메인에서 사용자의 최신 토큰 사용 내역을 수집하여 다른 도메인에서도 동일한 토큰 내역을 유지하도록 해준다. 동적 토큰을 사용한 SSO 기법은 일회용 토큰(one-time token)을 사용하여 토큰의 재사용(Replay 공격)을 막고 있다. 하지만 Circulator가 도메인을 적절히 방문하지 못하였을 때에는 직접 인증이 불가능하다. 또한, 정상적으로 인증이 수행된다 하더라도 Circulator와 각 도메인에서 모든 사용자의 토큰 값들을 저장하고 있어야 하므로 확장성이 현격히 떨어지게 된다.

[16]에서는 WLAN 도메인 사이의 로밍을 다루고 있다. 선재 키 분배(Proactive Key Distribution) 혹은 선인증(Pre-Authentication) 개념을 사용하여 인증 지연을 줄이는 방법을 소개한다. WLAN에서는 802.1x 프로토콜을 이용하여 사용자 인증을 수행한다. 즉, 사용자가 홈 도메인 인증서버로부터 인증을 받고 나면, 인증서버가 사용자와 해당 AP사이에 PMK(Primary Master Key)라는 공유키를 나눠 갖게된다. Proactive Key Distribution은 사용자의 홈도메인 인증서버가 사용자가 다른 도메인으로 로밍을 시도하기 전에, 로밍이 예상되는 도메인들에게 새로운 인증 정보 (PM_K)를 미리 분배해 두는 방법이다. 예를 들어 어떤 사용자가 도메인 X에서 서비

스를 받고 있을 때, 홈도메인 인증서버가 사용자의 로밍을 예측하여 인근 도메인 Y에 속한 AP_{new}로 새로운 PM_K를 미리 생성하여 전달한다. 이 때 홈도메인 인증서버가 도메인 Y의 인증서버를 경유하여 AP_{new}로 요청 메시지를 전달하게 되는데, 이를 위해서는 두 도메인 (홈도메인과 도메인 Y) 사이에 신뢰 관계가 존재하여야 한다. 결과적으로 사용자가 도메인 Y로 로밍을 시도할 때 홈도메인 인증서버를 경유하지 않고도 미리 공유된 PM_K를 사용하여 도메인 Y에서 서비스를 받을 수 있게 된다. 그러나 이러한 방법은 자칫 잘 못된 예측으로 엉뚱한 AP에 불필요한 정보 (fresh PM_K)를 캐싱하게 되는 문제가 있다. 따라서 홈도메인에서 사용자 이동 예측을 정확히 하기 위해 각 지역에 맞는 방대한 자료가 필요함은 물론, 홈도메인에서 모든 사용자의 움직임을 실시간으로 추적 관리해야 한다는 점에서 확장성이 떨어지는 단점이 있다.

2.3 캐싱(Caching) 기법

사용자의 인증 정보를 원격지 서버에서 캐싱하고 있어서 사용자가 원격지에 접속을 시도할 때 홈도메인으로 인증 요청을 하는 것을 방지하도록 하는 기법들이 있다. 대표적으로 쿠키(Cookie)를 이용한 기법[17]으로, 웹 기반의 애플리케이션에서 주로 사용되는 방법이다. 이 때, 원격지 서버는 사용자가 방문 시 사용자의 세션 정보를 쿠키의 형태로 저장하게 된다. 그리고 사용자가 그 원격지 서버를 재방문 시에는 재인증 절차를 거칠 필요 없이 쿠키를 제시하여 인증을 받을 수 있다. 하지만 이러한 쿠키 기반의 캐싱 기법은, 사용자가 한번 방문했던 원격지 서버에 다시 접속했을 경우에만 유효한 방법으로, 일반적인 의미에서 확장성이 좋다고 할 수 없고, 제 3자의 인증을 대행해 주지는 못한다.

다른 방법으로는, AKA(Authentication and Key Agreement)의 경우에서는 인증을 요청한 사용자의 홈도메인에 있는 사용자 인증 정보를 원격지 도메인으로 캐싱한다. 앞서 설명한 바와 같이 인증 정보를 캐싱할 에이전트(Agent)의 계층 구조를 동적으로 관리하고, 그러한 계층 구조를 이용해 인증 지연을 최소화하기 위한 빠른 인증 절차를 구체적으로 제시하고 있지 않기 때문에 확장성 면에서 떨어지는 단점이 있다.

3. 계층적 인증 캐싱 기법

2장에서 설명했던 기존 기법은 사용자 로밍 시 원격지 서버에서 인증을 받기 위해서 홈도메인 서버와의 연동을 필요로 하거나 간접적인 신뢰 관계에 있는 도메인 사이의 로밍은 직접 신뢰 관계에 있는 도메인 사이의 로밍보다 훨씬 복잡한 과정을 거치게 된다. 무엇보다 로밍의 규모가 수적, 지역적으로 커지면 모든 도메인 사이에 직접적인 신뢰 관계를 맺는다거나, 홈도메인에서 사용자를 실시간 관리하는 것이 어려워지므로 제 3자를 거쳐 간접적으로 연결된 신뢰 관계에 있는 도메인 사이의 로밍을 효율적으로 지원할 수 있는 방법이 요구된다. 따라서 본 논문에서는 원격 로밍이 잦은 환경에서, 확장성을 보장하면서 빠른 인증 기법을 제시한다. 사용자는 홈도메인과 간접적인 신뢰 관계에 있는 원격지에서 서비스를 받기 위해 인증 요청을 시도할 때, 계층구조가 아닌 일반적인 도메인간 신뢰관계를 통해 계층화된 캐싱 구조를 구성하여 홈도메인의 도움 없이 원격지에서 인증 절차를 마칠 수 있다.

3.1 인증 구조 및 과정

그림 3에서와 같이, 로밍 인증에 참여하는 구성 요소는 사용자; 사용자의 계정 및 서비스 계약(Service Agreement), 과금, 통계정보 등을 관리하는 홈도메인의 인증서버 (그림 3의 AAAH: Home AAA Server); 그리고 사용자가 홈도메인을 떠나 서비스를 받으려고 하는 원격지의 인증서버, (그림 3의 AAAL: Local AAA Server); AAAH와 직간접적으로 신뢰 관계를 유지하고 인증 정보를 캐싱하여 로밍 인증을 대행할 하나 이상의 캐싱 에이전트 및 그들의 계층 구조 (그림 3의 CAH: Caching Agent Hierarchy)로 구성된다.

이때, AAAH와 AAAL은 직접적으로 신뢰 관계를 유지하고 있거나, 그림 4에서 임의의 두 노드 사이와 같이, 직접 신뢰 관계를 갖는 하나 이상의 노드들을 사이에 두고 간접적인 신뢰 관계에 있음을 전제로 한다. 경우에 따라서 신뢰 관계를 동적으로 체결할 수도 있다. 또한 임의의 노드 사이의 최적 경로 정보가 알려져 있으며, 경로상의 노드는 상기 라우팅 정보에 따라 메시지를 프락싱(proxying)하거나 전달(relay)하기도 할 의무가 있다. 캐싱 에이전트 후보는 AAAH 및 AAAL과 직간접적으로 신뢰 관계에 있는 노드로, 캐싱 에이전트로

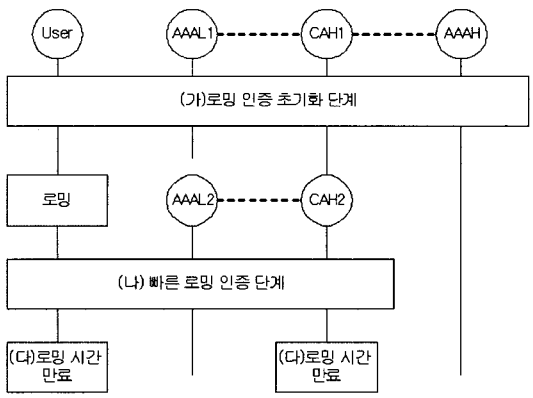


그림 3 로밍의 인증 구조 및 과정

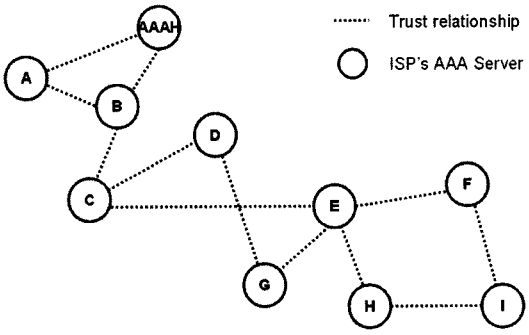


그림 4 도메인간 신뢰 관계

선택되면 AAAH를 루트로 하는 계층 구조의 한 노드가 된다. 계층 구조의 바람직한 예는 부모와 자식의 관계가 분명한 트리 구조를 형성하는 것이다. 극단적인 모습으로, 모든 캐싱 에이전트가 AAAH의 자녀로 구성 될 수도 있고, 모든 캐싱 에이전트가 한 줄로 부모 자식 관계를 유지할 수도 있다.

인증의 단계는 그림 3에서 보인 바와 같이 '원격 로밍 인증 초기화' 단계; '빠른 원격 로밍 인증' 단계; 소프트 스테이트 (Soft State)로 유지되는 인증 정보의 사용 시한이 만료되는 '로밍 시한 만료'의 3단계로 구성된다. 이제 각각의 단계를 자세히 살펴보기로 한다. 그림 3에서 CAH1에 AAAL1이나, AAAL1과 CAH1사이의 캐싱 에이전트 후보가 선택될 경우, CAH1은 CAH2로 갱신되는데 자세한 내용은 다음에 설명한다.

3.1.1 로밍 인증을 위한 초기화 단계

이 단계는 사용자가 AAAH로부터 기존 방식 (예: TLS, AKA 같은 개별 인증 프로토콜 및 각종 EAP-method, 커버로스와 같은 SSO 기법 등 이용)을 이용해 인증을 받는 과정에서, AAAH와 AAAL간의 신뢰경로 상에 있는 캐싱 에이전트에게 인증 정보를 할당하고 계층 구조를 초기화 하는 과정이다. 그림 5와 같이 캐싱 에이전트 후보자들은 사용자가 AAAH로부터 기존 방식을 이용해 인증을 받는 과정에서, 사용자로부터 AAAH 방향으로 자신의 능력 정보를 전달한다. 능력 정보를 받은 상위 노드는 (최초의 캐싱 에이전트 계층 구조는 AAAH에서 시작하여 AAAH를 루트로 계층 구조를 키워간다.) 해당 후보를 계층 구조에 포함시킬지를 합(hop) 수, 본인의 능력, 후보자의 능력 등을 고려해 판단한다.

그리고 그림 6과 같이 후보자를 계층에 포함시키기 위해서는 부모 노드는 사용자에 대한 원격 인증 정보를 후보자에게 할당, 안전한 경로를 통해 전달하고 계층 구조 목록에 후보자를 등록하는 CAH 목록 갱신을 한다. 후보자가 계층 구조에 참여하게 되면 부모 혹은 상위 노드로부터 할당 받은 원격 인증 정보를 캐싱하고, 캐싱

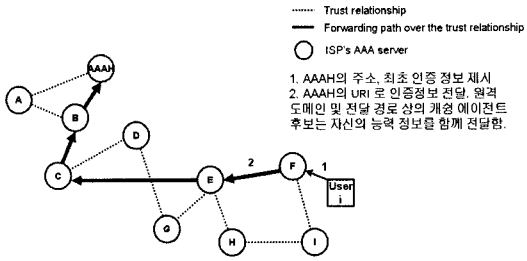


그림 5 캐싱 에이전트 후보자들의 능력 정보 전달

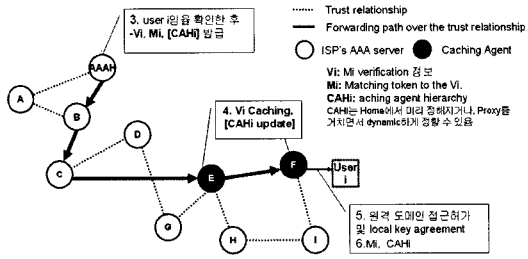


그림 6 캐싱 계층 구조 구성

한 정보를 이용해 이후 사용자에 대한 인증 요청을 처리할 의무를 갖게 된다. 또한 원격 로밍 인증의 초기화 단계에서, CAH는 사용자에게 캐싱된 원격 인증 정보에 대한 대응(Matching) 정보와 CAH의 목록을 안전하게 전달한다. 대응 정보는 사용자가 CAH에서 로밍 인증을 받을 때 제시하도록 할 목적으로 쓰인다. CAH가 캐싱할 원격 인증 정보에 대응되는 대응 정보를 사용자에게 발급하면, 사용자는 원격 인증 요청 시 대응 정보를 CAH에 제시하고, CAH는 원격 인증 정보와 제시된 대응 정보를 이용해 인증 처리를 수행한다. CAH의 목록은 계층 구조를 반영하며, 가능한 축약 방식을 동원해 짧게 만들 수 있다.

3.1.2 빠른 로밍 인증 단계

이 단계는 사용자의 로밍으로 인해 새로운 원격지에서 인증 요청이 발생할 때마다 AAAH를 대행해 CAH가 빠른 로밍 인증 요청을 처리해주는 과정이다. 그림 7과 같이 사용자가 새로운 도메인으로 로밍하면, 사용자는 새로운 AAAL에게 사용자의 CAH를 제시한다. 그러면 AAAL은 자신과 가장 가까운 (인증 지연이 가장 적은) 캐싱 에이전트를 CAH 중에서 선택하여 사용자가 제시하는 대응 정보를 이용해 캐싱 에이전트로부터 빠른 로밍 인증을 받는다. 가장 가까운 사용자를 선택하는 방법으로 Diameter에서와 같은 기존 기법을 사용할 수 있다. 예를 들어, 각 도메인의 인증서버는 도메인간 라우팅을 위해 Diameter Routing Table과 같은 기능을 하는 테이블을 유지하고 있는데, 이 테이블에서 CAH상

의 에이전트 중 hop count가 가장 작은 에이전트를 선택하면 된다. 이때, 사용되는 캐싱 정보와 그에 대한 대응 정보를 이용한 로밍 인증은 대칭키 및 대칭키를 이용한 티켓 (예: 커버로스의 티켓 및 포워딩 티켓), 그와 유사한 방식 (쿠키 및 토큰 등을 이용한 SSO 기법)을 사용할 수 있고, 서버가 제시한 Challenge에 대해 바른 Response를 하는 방식 (예: AKA)을 취할 수 있다. 여기에서 대응 정보는 Challenge에 대해 바른 Response를 만드는 정보나 Response 자체 일 수 있으며, 캐싱 정보도 이와 같은 방식을 취할 수 있다.

만약, CAH에서 사용하는 인증 정보가 개별 캐싱 에이전트 마다 다를 경우, AAAL이 선택한 캐싱 에이전트에 해당하는 대응 정보를 사용자로부터 받아 전달한다. 이때, AAAL이 선택한 노드 (캐싱 에이젼트)에서 루트 방향으로 인증 요청이 전달되는 경우를 대비해, 선택된 노드의 하나 이상의 상위 노드 (최상위 노드는 루트 노드이며, 모든 세대가 다 포함 되어야 하는 것은 아님)가 요구하는 대응 정보를 함께 보낼 수 있다.

또한, 부득이한 사유로 로밍 인증을 위해 선택된 캐싱 에이전트가 인증 요청을 처리할 수 없는 경우에 (유효한 인증 정보가 없거나, 에이전트가 동작을 멈추는 등의 이유) 인증 처리를 할 수 없게 된 캐싱 에이전트는 사용자의 CAH상의 부모 및 상위 노드에게 인증 요청 (대응 정보와 CAH를 포함)을 전달한다. 따라서 사용자가 처음부터 인증 절차를 거치지 않고도 투명한 인증을 받을 수 있게 된다. 최악의 경우에는 CAH 경로상의 모든 노드에서 인증처리가 불가능하여 AAAH까지 인증 요청이 전달 될 수도 있다. 이로써, 중간 캐싱 에이전트의 오동작에 영향을 받지 않는 투명한 서비스를 보장할 수 있다.

이때, 캐싱 에이전트에서 로밍 인증이 실패한 경우에는 해당 캐싱 에이전트가 AAAL에게 그 결과를 통보하는 것이 아니라 CAH 상에서 하나 이상의 상위 노드 (AAAH에게 곧장 인증 실패 확인은 요청 할 수 있음)가 인증 실패를 확인하도록 한다. 이는 악의적으로 캐싱 에이전트가 로밍을 방해하는 행위나, 오동작으로 인한 인증 실패를 방지하기 위함이다.

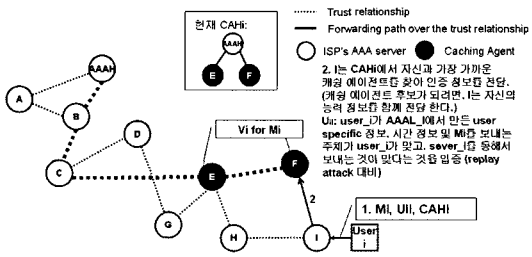


그림 7 빠른 로밍 인증

그리고 그림 7에서 인증 정보를 가장 가까운 캐싱 서버로 전달하는 과정에서 AAAL과 선택된 캐싱 서버 간의 경로에 있는 AAAL (그림 7의 노드 I)을 포함한 노드들은 캐싱 에이전트 후보가 될 수 있으며, 원하는 경우 자신의 능력 정보와 결정에 필요한 기타 정보를 함께 전달 할 수 있다. 그림 8과 같이 원격지 로밍 인증이 성공하고, 예에서와 같이 AAAL이 캐싱 에이전트로 선택이 되면, 그림 8의 예시와 같이 CAH가 갱신된다. 갱신의 주체는 선택한 에이전트 혹은 선택 받은 에이전트가 될 수 있다.

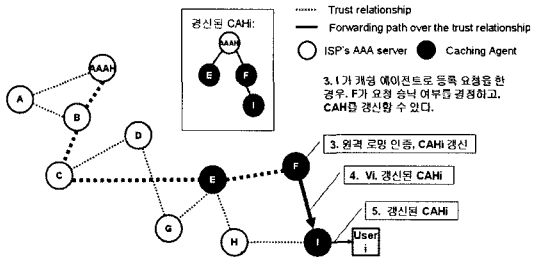


그림 8 CAH의 갱신 과정

다음 그림 9에서와 같이 사용자가 노드 H가 AAAL인 새로운 도메인으로 로밍 하고자 할 경우 앞서 설명한 방법으로 빠른 원격지 로밍 인증이 가능하다. 그림 9의 예시에서는 노드 I와 가장 가까운 CAH상의 캐싱 에이전트로 노드 E가 선택이 되었고, 앞의 과정을 통해 노드 H가 CAH에 추가된 경우 갱신된 CAH를 보여준다.

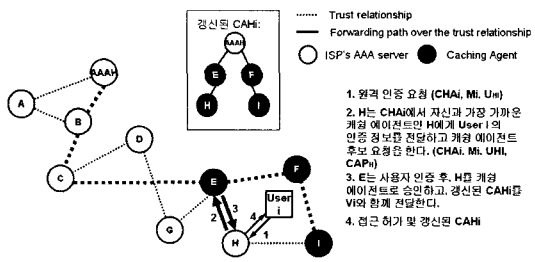


그림 9 빠른 로밍 인증의 예시

그림 3의 (나) 에서 AAAL이 CAH의 최적 노드와 인증 정보를 주고받는 과정에서 AAAL로부터 CAH방향으로 캐싱 에이전트 후보는 자신의 능력을 전달할 수 있고, 지금까지 설명한 방식에 따라 CAH 에 추가될 수 있다. 그리고 인증 요청을 수행한지 오래 되었거나, 자주 인증 요청이 들어오지 않는 노드는 해당 알고리즘에 따라 CAH에서 삭제할 수 있다. 따라서 그림 3의 (가)

이후에 사용자가 로밍하는 경로에 따라 최적의 캐싱 에이전트가 계층 구조에 추가되고 필요 없는 노드는 삭제되기도 하며 CAH는 동적으로 재구성된다. 이때, 재구성된 계층 구조는 필요에 따라 CAH에 의해 사용자에게 전달될 수 있다.

3.1.3 로밍 시간 만료

그림 3의 (다)는 로밍 인증을 허용하는 시한이 소프트 스테이트로 유지되므로 시간이 만료될 경우 특별한 메시지를 주고받지 않아도 각자 만료되어 더 이상 로밍 인증을 위해 사용되지 않는다. 시한이 만료되기 전에 (가) '로밍 인증을 위한 초기화'를 하면 로밍 인증 서비스를 계속 받을 수 있다. 이때, 정책에 따라 캐싱된 정보와 대응 정보를 모두 새로 받아 오게 하거나, 지난 정보를 계속 사용하게 할 수 있다. 단, 일정 시한 안에 새 정보로 갱신하여 사용하도록 하는 것이 바람직하다.

이와 같이 그림 3의 (가), (나), (다)의 동작을 통해 원격지에서의 로밍으로 인해 잦은 인증 요청이 발생할 때, AAAH가 직접 인증에 관여하지 않고도 인증 지연을 최적화하는 CAH를 구성하여 빠른 로밍 인증을 실현할 수 있다.

3.2 계층적 캐싱 구조를 이용한 빠른 패이징 기법

계층적 캐싱 관리 기법을 사용하면, 국제 로밍 및 이기종망간 핸드오버가 활성화된 환경에서 사용자의 위치 관리가 가능하며 이를 통해 확장 가능한 패이징 시스템으로 활용이 가능하다. 이때, AAAH는 캐싱 계층 구조로 패이징 요청을 보내고, 계층을 따라 패이징 요청이 마지막까지 전달되면 리프(Leaf) 노드에서 루트(Root) 노드로 응답이 전달된다. 응답이 전달 될 때, 경로 상에 있는 계층 구조의 노드 중에서 가장 최근의 유효한 정보가 토너먼트 형식으로 전달이 된다. 따라서 계층적 캐싱 구조를 이용해 패이징을 구현할 경우, 사용자의 위치 관리를 위한 비용을 절감하고 패이징 지연을 단축시킬 수 있다.

4. 성능 분석

계층적 인증 캐싱 기법의 인증 지연과 망 부하를 분석하기 위해, 캐싱 에이전트의 계층 구조와 도메인의 구성 및 사용자의 이동 모델을 단순화 시켰다. 분석의 단순 명료성을 위해 도메인 모델을 원이나 육각형 대신, 노드의 이동성을 표현하고, 전체 성능의 경향성을 나타내기에 충분한 정사각형 모델을 선택하였다. 그림 10은 전체 분석 모델을 도식한 것으로 깊이가 K인 캐싱 에이전트 (CA)의 계층 구조이다. 이때, 단계-k의 캐싱 에이전트는 N_{cak} 개의 하부 구조를 갖게 된다. 그림 10은 깊이가 2인 계층 구조로 CA2는 N_{CA2} = 3개의 도메인에 속한 AAAL에서 발생하는 인증 요청을 처리해 주는 구조이다.

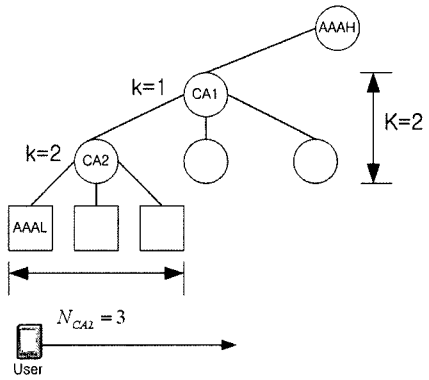


그림 10 분석 모델

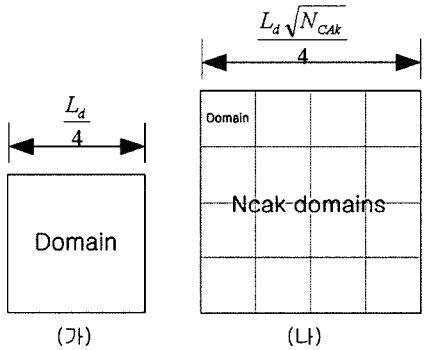


그림 11 도메인 구성

그림 11의 (가)와 같이 본 분석에서 사용한 도메인은 정사각형으로 둘레의 길이가 L_d 일 때, N_{CAK} 개의 도메인을 하부 구조로 갖는 CAK의 인증 커버리지 영역의 둘레의 길이는 식 (1)과 같고,

$$L_{CAK} = L_d\sqrt{N_{CAK}} \quad (1)$$

이를 일반화시켜 CA_k의 인증 커버리지 영역의 둘레의 길이는 식 (2)와 같이 구할 수 있다.

$$L_{CAk} = L_{CA(k+1)}\sqrt{N_{CAk}} \quad (2)$$

본 분석에서는 노드의 이동 패턴이 플루이드 플로우 모델 (Fluid Flow Model)을 사용하였다. 각 도메인에 분포한 이동 단말, 즉 노드의 밀도가 ρ node/m^2, 평균 속도가 υ이고, 이동 방향은 [0, 2π]에서 균일분포 (uniform distribution)을 따를 때, 단위 시간당 한 도메인의 경계를 지나가는 노드의 수, R_d는 [18]에 따라 다음과 같다.

$$R_d = \frac{\rho\upsilon L_d}{\pi} \quad (3)$$

식 (3)을 이용하면 한 노드가 발생시키는 인증요청률

인 단위 시간당 한 노드가 넘는 도메인의 수, r_d는 식 (4)와 같이 구할 수 있다.

$$r_d = \frac{R_d}{N_d} = \frac{16\upsilon}{\pi L_d} \quad (4)$$

여기에서 도메인 내의 노드 수, $N_d = L_d^2\rho/16$ 이다.

인증을 받을 후에 같은 도메인에 라이프 타임(lifetime) 이상 머물게 될 경우 다시 인증 업데이트가 필요하다. [19]에 따라 인증 업데이트률, u_d을 구하면 다음과 같다.

$$u_d = \frac{U_d}{N_d} = \frac{\rho\upsilon L_d}{\pi N_d}\left\lfloor \frac{1}{r_d T_M} \right\rfloor \quad (5)$$

$$U_d = R_d\left\lfloor \frac{1}{r_d T_M} \right\rfloor = \frac{\rho\upsilon L_d}{\pi}\left\lfloor \frac{1}{r_d T_M} \right\rfloor \quad (6)$$

식 (6)에서 U_d는 단위 시간당 한 도메인에서 발생하는 인증 업데이트의 수이고, TM은 도메인 내에서의 인증 라이프 타임이다.

4.1 인증 지연 분석

기존 기법에서는 원격지에서 단말이 로밍을 할 때마다, AAAH로 인증 요청을 하게 되므로, 인증 요청은 도메인을 옮길 때마다 발생하므로, 기존 기법에서의 단말의 인증 요청률, r_{flat}와 인증 업데이트률, u_{flat}은 다음과 같다. 본 분석에서는 모바일 노드의 인증 라이프 타임 만료보다 빠르게 이동하는 경우를 주요 대상으로 하기 때문에 표 1에 주어진 파라미터 값의 범위 내에서는 인증 업데이트률이 0이 되므로 앞으로의 분석 과정에서 생략하였다.

$$r_{Flat} = \frac{16\upsilon}{\pi L_d} \quad (7)$$

$$u_{Flat} = \frac{\rho\upsilon L_d}{\pi N_d}\left\lfloor \frac{1}{r_d T_M} \right\rfloor \quad (8)$$

한편, 계층적 인증 캐싱 기법에서 한 노드가 발생하는 레벨 k의 캐싱 에이전트에 대한 인증 요청률, a_{CAk}는 다음과 같이 구할 수 있다.

$$a_{CA1} = r_d = \frac{16\upsilon}{\pi L_d}, \ (\mathrm{K}=1) \quad (9)$$

$$a_{CAk} = r_{CA(k+1)} - r_{CAk} = \frac{16\upsilon}{\pi}\left(\frac{1}{L_{CA(k+1)}} - \frac{1}{L_{CAk}}\right), \ (1<\mathrm{k}<\mathrm{K}) \quad (10)$$

$$a_{CAK} = r_d - r_{CAK} = \frac{16\upsilon}{\pi}\left(\frac{1}{L_d} - \frac{1}{L_{CAK}}\right), \ (\mathrm{k}==\mathrm{K}) \quad (11)$$

$D_{U,AAAH}$가 노드(User)와 AAAH 간의 라운드 트립 인증 지연일 때, 식 (7)을 이용해 기존 기법에서의 인증 지연, $D_{Flat}=r_{Flat}D_{U,AAAH}$을 구할 수 있다.

또한 $D_{U,CAi}$가 노드(User)와 CAi의 라운드 트립 인증 지연일 때, 깊이가 K인 계층적 인증 캐싱에서 한 노드가 겪는 평균 인증 지연은 다음과 같다.

$$D_K = \sum_{i=1}^{i=K} D_{U,CAi}\frac{a_{CAi}}{r_d} \quad (12)$$

4.2 망 부하 분석

본 절에서는 인증으로 인해 발생하는 망의 부하를 비교하고자 한다. 다음은 망에서 CAk로 인증 요청이 일어나는 횟수의 총합으로, k에 따라 다음과 같이 구할 수 있다.

$$A_{CA1} = R_{CA2}N_{CA1}, \ (\mathrm{K}=1) \quad (13)$$

$$A_{CAk} = R_{CA(k+1)}\prod_{i=1}^{k} N_{CAi} - R_{CAk}\prod_{i=1}^{k-1} N_{CAi} = \prod_{i=1}^{k-1} N_{CAi}(R_{CA(k+1)}N_{CAk} - R_{CAk}), \ (1 < \mathrm{k} < \mathrm{K}) \quad (14)$$

$$A_{CAK} = R_d\prod_{i=1}^{K} N_{CAi} - R_{CAK}\prod_{i=1}^{K-1} N_{CAi} = \prod_{i=1}^{K-1} N_{CAi}(R_d N_{CAK} - R_{CAK}), \ (\mathrm{k}=\mathrm{K}) \quad (15)$$

단위 인증 요청당 발생하는 망의 부하는 인증 요청을 위해 쓰이는 메시지의 수가 Ms이고, 인증 대상 (U와 XXX)간의 홉(hop) 수가 HU,XXX 일때, $O_{U,XXX}=M_sH_{U,XXX}$으로 구할 수 있다. 그리고 식 (13)~식 (15)를 인증 캐싱 기법에서의 망 부하, S_K를 계산하면 다음과 같다.

$$S_{U,AAAH} = R_d O_{U,AAAH} \quad (16)$$

$$S_K = \sum_{i=1}^{i=K} A_{CAi}O_{U,CAi} \quad (17)$$

5. 분석 결과

본 장의 분석 결과는 4장의 수식과 표 1의 파라미터 값을 따랐다.

그림 12는 4.1에서 보인 식을 이용하여 구한 평균 인

표 1 파라미터 값

Parameter	Value
K : depth of caching agent hierarchy	2~3
N_d : number of domains per CAK	가변
$NCA0$: number of CA2s per CA1	가변
ρ : node density	200/km^2
υ : node velocity	10km/hr
Ld : domain perimeter	10km
TM : authentication lifetime	24hrs
$Du,AAAH$: AAAH authentication delay (round trip)	300ms
$Du,CA1$: CA0 authentication delay	70ms
$Du,CA2$: CA2 authentication delay	40ms
$Du,CA3$: CA3 authentication delay	10ms
$Hu,AAAH$: distance between user and AAAH	30
$Hu,CA1$: distance between user and CA1	14
$Hu,CA2$: distance between user and CA2	10
$Hu,CA3$: distance between user and CA3	5
Ms: signaling cost per an authentication procedure per hop (message/authentication/hop)	1

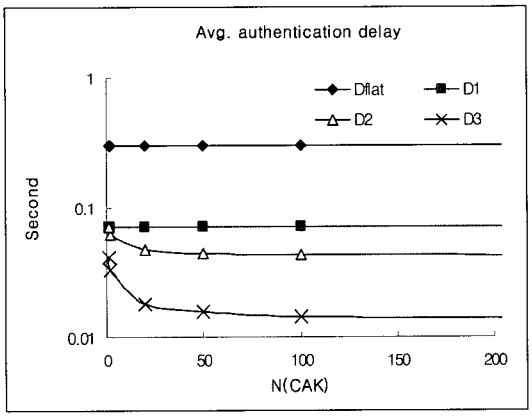
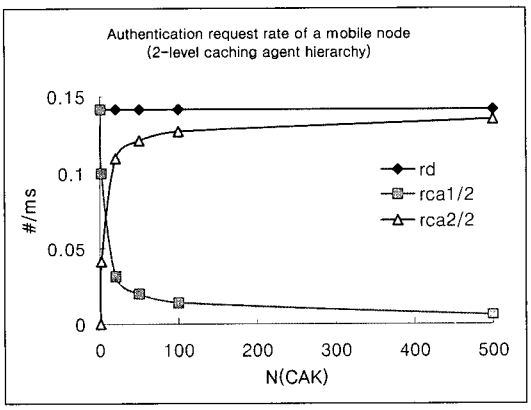
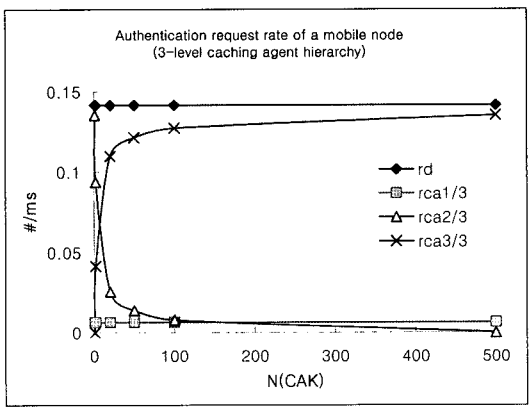


그림 12 평균 인증 지연



(가) 깊이가 2인 계층 구조



(나) 깊이가 3인 계층 구조

그림 13 노드당 인증 요청률

증 지연이다. 기존 기법들의 경우, 처음 방문하는 원격지 도메인에서 인증을 시도하는 경우, 홈도메인과 직접 연동하여 인증을 수행하는 공통점이 있는데, 특히 본 논

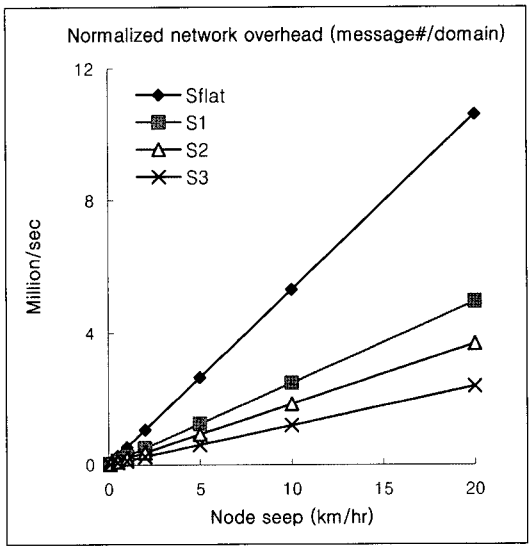


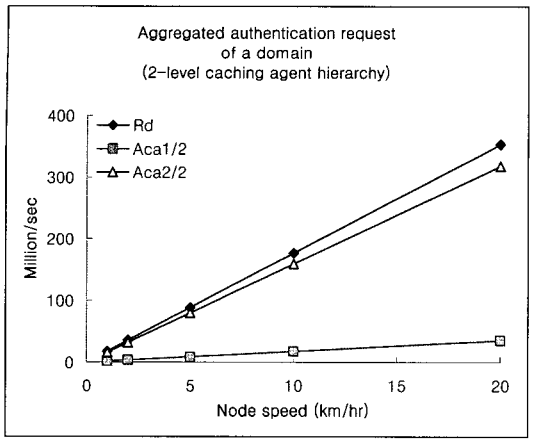
그림 14 망 인증 부하

문에서 제안한 바와 같이 계층구조를 활용하는 예 또한 없으므로, DFlat의 성능이 기존 기술의 인증 지연이 된다. 그림 12의 D1, D2, D3은 각각 계층의 깊이가 1~3일 때, N_{CAK}의 변화에 따른 평균 지연을 보인 것이다. 이때 총 도메인의 수는 1000개로 동일하며, 깊이가 3일 때, N_{CA1}은 2로 고정시킨 값이다.

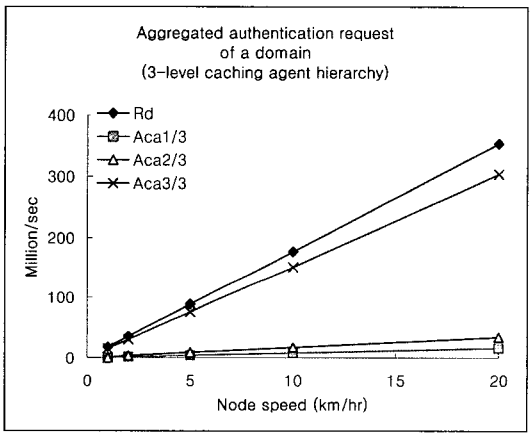
평균 인증 지연이 위와 같은 결과가 나오는데 결정적인 영향을 미친 인자인 노드당 인증 요청률의 변화를 보면 그림 13과 다음과 같다. 그림 13의 (가)에서 rd는 기존 기법에서 AAAH로의 인증 요청률이고 rca1/2와 rca2/2는 각각 2계층 구조에서 CA1과와 CA2로의 인증 요청률이다. 그림 13의 (나)에서 rca1/3와 rca2/3, rca3/3은 각각 3계층 구조에서 CA1과와 CA2, CA3으로의 인증 요청률이다.

그림 14는 4.2절의 망 부하에 관한 식과 표 1의 파라미터 값을 이용해 그린 것 이다. 이때, 2계층 구조에서 Nca1/2=10, Nca2/2=100이고, 3계층 구조에서 Nca1/3=2, Nca2/3=10, Nca3/3=50을 사용하였다. Sflat은 기존 기법에서 AAAH로 인증 요청이 몰릴 경우, 망에 가해지는 인증 부하를 구한 값이며, S1, S2, S3는 각각 계층 구조가 1~3일 때의 망 부하로, 노드의 속도를 변화에 따라 망에 끼치는 총 인증 부하를 도메인 수로 정규화한 값이다. 노드의 속도 증가는 인증 요청 횟수를 높이는 요인으로, 노드의 밀도를 증가시켰을 때와 같은 결과를 얻을 수 있다.

그림 15는 그림 14에서 보인 망 인증 부하를 결정 짓는 중요 요인으로, 망에서 CAk로 인증 요청이 일어나는 횟수의 총합인 A를 도메인 수로 정규한 값이다. 이



(가) 깊이가 2인 계층 구조



(나) 깊이가 3인 계층 구조

그림 15 망에서 CAk로 인증 요청이 일어나는 횟수의 총합

때, 노드의 속도를 변화에 따라, 인증 캐쉬의 계층 구조의 깊이가 2인 경우와 3인 경우를 분리하여 도식하였다.

6. 결 론

본 논문은 국제 로밍과 이기종망간 핸드오버의 확산으로 로밍이 잦은 환경에서 확장성은 뛰어나면서 빠른 인증 프레임워크를 제안하였다. 제안된 프레임워크는 원격지 로밍 시 경험하는 인증 지연과 인증으로 인한 망 부하를 줄일 수 있으며, 일반적인 신뢰 관계를 갖는 도메인 간의 부드러운 로밍을 지원할 수 있는 확장 가능한 인증 체계를 제공한다. 제안된 프레임워크를 기반으로 구체적인 프로토콜 및 인증 시스템을 구성하는 것이 향후 과제로 남아 있다.

참 고 문 헌

[1] Rigney, C. et al., "Remote Authentication Dial In User Services(RADIUS)," IETF RFC 2138, 1997.
[2] Calhoun, P. et al., "Diameter Base Protocol," IETF RFC3588, 2003.
[3] Arkko, J. and Haverinen, H., "EAP AKA Authentication," Internet draft, draft-arkko-pppext-eap-aka-12, Apr. 2004.
[4] Haverinen, H., "EAP SIM Authentication," Internet draft, draft-haverinen-pppext-eap-sim-13, Apr. 2004.
[5] Microsoft, .Net Passport. http://www.microsoft.com/net/services/passport/
[6] Fumiko Satoh, Takayuki Itoh, "Single Sign On Architecture with Dynamic Tokens," SAINT, 2004.
[7] B. Yao and W. K. Fuchs, "Proxy-based Recovery for Applications on Wireless Hand-held Devices". In Proc. 19th IEEE Symposium on Reliable Distributed Systems SRDS'00), October 16-18, 2000, pp. 2.10.
[8] B. Yao and W.K. Fuchs. "Recovery Proxy for Wireless Application". In Proc. 12th International Symposium on Software Reliability Engineering (ISSRE 2001), IEEE, pp. 112-119, 2001.
[9] Kohl, J. and Neuman, C., "The Kerberos Network Authentication Service (V5)," RFC 1510, 1993.
[10] 3GPP, http://www.3gpp.org
[11] Salkintzis and Apostolis K., "Interworking Techniques and Architecture for WLAN/3G Integration Toward 4G Mobile Data Networks," IEEE Wireless Communications, 2004.
[12] B. Anton and B. Bullock and J. Short, "Best Current Practices for Wireless Internet Service Provider(WISP) Roaming," Wi-Fi Alliance - Wireless ISP Roaming(WISPr), Ver. 1.0, February 2003.
[13] M. Long and C.-H. Wu, and J.D. Irwin, "Localized authentication for inter-network roaming across wireless LANs," IEE Proceedings-Commun., Vol.151, No.5, October 2004.
[14] Michael Hecker and Peter Leijdekkers and Valerie Gay, "A Testbed For Ubiquitous Computing Using Next Generation Mobile Networks," CollECTeR 2004.
[15] Fumiko Satoh and Takayuki Itoh, "Single Sign On Architecture with Dynamic Tokens," SAINT, 2004.
[16] M.S. Bargh, R.J. Hulsebosch, E.H. Eertink, A. Prasad, H. Wang, and P. Schoo, "Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs," WMASH, 2004.
[17] Samar Vipin, "Single Sign-On Using Cookies for Web Applications," WETICE, 1999.
[18] Mohan, S. and Jain, R., "Two user location strategies for personal communications services," IEEE Pers. Comm. Vol. 1, No.1, pp. 42-50, 1/4, 1994.
[19] Woo, M., "Performance analysis of Mobile IP Regional Registration," IEICE Trans. Comm., Vol. E86-B, No.2, Feb. 2003.

이 희 진

1997년 광운대학교 전자계산학과 졸업(학사). 2002년 서울대학교 전기·컴퓨터공학부 졸업(석사). 1997년~2000년 삼성전자 중앙연구소 연구원. 2002년~현재 서울대학교 전기·컴퓨터공학부 박사과정. 관심분야는 차세대 인터넷, 이동통신, 유무선통합망 등

송 유 경

2003년 이화여자대학교 컴퓨터학과 졸업(학사). 2005년 서울대학교 컴퓨터공학부 졸업(공학석사). 관심분야는 네트워크 보안, 홈 네트워크 등

이 명 수

1989년 연세대학교 전자공학과 박사. 1990년~2004년 KT 네트워크 보안연구팀장. 2004년 정보보호학회 무임 소이사. 2005년~현재 KT 정보보호기술팀장. 관심분야는 개인 정보보안 및 네트워크 보안

김 종 권

정보과학회논문지 : 정보통신
제 32 권 제 4 호 참조