포트레벨 보안을 위한 인증 프록시 시스템의 성능분석

정회원 이 동 현*, 이 현 우**, 정 해 원**, 윤 종 호***

Performance of an Authentication Proxy for Port Based Security Systems

Dong-Hyun Lee*, Hyun-Woo Lee**, Hae-Won Jung**, Chong-Ho Yoon*** *Regular Members*

요 약

본 논문에서는 IEEE802.1x 모듈이 탑재된 액세스 포인트에 사용자 인증 캐시테이블을 추가함으로써, 액세스 포인트가 인증서버를 대신하여 사용자 인증처리를 하는 기능을 제안하고, 성능을 분석하였다. 기존의 IEEE802.1x 시스템 환경에서는 반드시 인증서버에서 사용자 인증처리를 수행해야 했기 때문에 사용자는 인증서버의 사용자 인증처리 완료 후, 액세스 포인트의 물리적 포트 사용에 대한 권한을 부여 받을 때까지 대기하여야만 하였다. 그러나 본 논문에서 제안된 방식은 인증서버의 사용자 인증정보를 액세스 포인트의 사용자인증 캐시테이블 목록에 임시 저장함으로써, 액세스 포인트가 인증서버를 대신하여 사용자 인증처리 및 액세스 포인트의 물리적 포트 사용 권한을 부여할 수 있도록 한 것이다. 따라서, 인증관련 데이터 트래픽의 양을 줄일 수 있으며, 인증서버의 사용자 인증처리에 대한 부하를 줄일 수 있다. 또한 이러한 인증용 캐시테이블을 운영자가 관리모드로 액세스 포인트에 접속하여 직접 구성할 경우에는 인증서버 구축에 대한 비용의 추가부담이 없어지는 효과도 있다. 그리고 제안된 방식에 대한 모의 실험을 통해 인증서버가 인증처리를 하는 것보다 액세스 포인트가 사용자 인증처리 기능을 대행하는 것이 인증지연 시간을 감소시킬 수 있음을 검증하였다.

ABSTRACT

In this paper, we present an efficient authentication proxy for IEEE 802.1x systems based on the port-based access control mechanism. An IEEE 802.1x system consists of PC supplicants, a bridge with authentication client functions, and an authentication server. For the network security and user authentication purposes, a supplicant who wants to access Internet should be authorized to access the bridge port using the Extended Authentication Protocol (EAP) over LAN. The frame of EAP over LAN is then relayed to the authentication server by the bridge. After several transactions between the supplicant and the server via the bridge, the supplicant may be either authorized or not. Noting that the transactions between the relaying bridge and the server will be increased as the number of supplicants grows in public networks, we propose a scheme for reducing the transactions by employing an authentication proxy function at the bridge. The proxy is allowed to cache the supplicant's user ID and password during his first transaction with the server. For the next authentication procedure of the same supplicant, the proxy function of the bridge handles the authentication transactions using its cache on behalf of the authentication server. Since the main authentication server handles only the first authentication transaction of each supplicant, the processing load of the server can be reduced. Also, the authentication transaction delay experienced by a supplicant can be decreased compared with the conventional 802.1x system.

* (주)이오넥스(lewislee@lycos.co.kr), ** 한국전자통신연구원 네트워크연구소(hwlee@etri.re.kr, hw-jung@etri.re.kr),
*** 한국항공대학교 전자·정보통신·컴퓨터공학부(yoonch@mail.hangkong.ac.kr)
논문번호 : 030030-0120, 접수일자 : 2003년 4월 8일

Ⅰ. 서 론

IEEE802.1x는 2001년 6월, "Standards for port based Network Access Control" 제목의 보안관련 표준으로써, 브리지 또는 무선 액세스 포인트(AP)의 물리적인 포트의 사용권을 외부의 인증서버로부터 획득해야만 사용자 PC의 망 접근을 허용하는 절차에 대한 규정이다[1]. 그림 1의 기존 LAN 시스템에서는 대부분의 PC들이 인증절차 없이도 브리지의 물리적인 포트를 통하여 LAN에 접속된 다른 PC나 서버들에 접근할 수 있기 때문에 망에 대한 공격이 가능한 문제점이 있다. 또한, 단말마다 계정관리, 과금처리 등의 부가기능이 불가능하다. 그러나 기존의 브리지에 802.1x의 포트레벨 보안기술 인증절차를 수행하도록 한 경우에는 개별적인 과금 정책이나, 사용제한, 대역할당 등 사용자 개인별로 제어할 수 있는 장점이 있다. 결국, IEEE802.1x의 목표는 최종단 망 시스템인 브리지 또는 AP에서 인증을 수행한 사용자 PC들이 망에 접근할 수 있도록 하는 것이다.

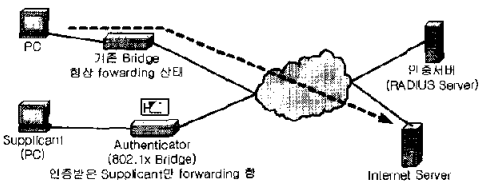


그림 1. 기존 LAN시스템과 IEEE802.1x 시스템의 구성비교

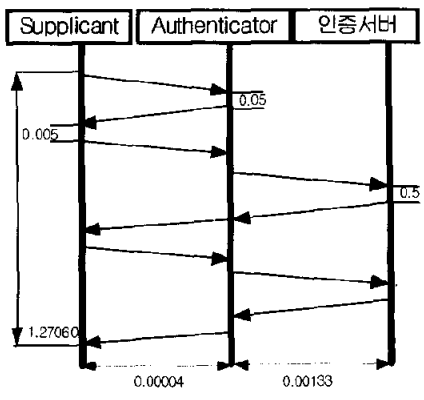
본 논문에서 제안된 방식은 IEEE802.1x 모듈이 탑재된 AP에 사용자 인증용 캐시테이블을 추가함으로써, AP가 인증서버를 대신하여 사용자 인증처리를 할 수 있게 되었다. 이 방식은 인증서버의 사용자 인증정보를 AP의 사용자인증 캐시테이블 목록에 임시 저장하여서, AP가 인증서버를 대신하여 사용자 인증처리 및 AP의 물리적 포트 사용권한을 부여할 수 있도록 함으로써, 사용자 대기시간이 단축되는 장점이 있다.

본 논문의 구성은 다음과 같다. 서론에 이어 제II장에서는 기존의 방식과 제안된 방식의 사용자 인증처리를 비교하였다. 제III장에서 상태천이도와 프로토콜 동작을 설명하였고, 제IV장에서는 필요한 캐시테이블 및 RADIUS 속성값을 정의하였다. 제V장은 인증 프로토콜 동작을 설명하였다. 그리고 제VI장에서 모의실험에 의한 성능분석을 수행하였다. 마지막 제VII장에서 결론을 내린다

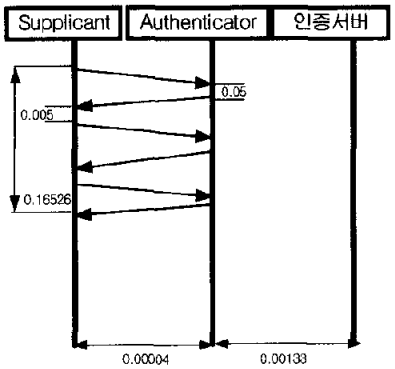
Ⅱ. 기존의 IEEE802.1x 시스템과 제안 방식의 사용자 인증처리 과정의 비교

IEEE802.1x 규정에 따르는 시스템 구성요소는 그림 2처럼 supplicant 기능을 수행하는 PC, authenticator 기능을 수행하는 브리지 또는 AP, 그리고 authenticator와 연결된 인증서버(authentication server)로 구성된다. 이때, authenticator인 브리지 또는 AP는 인증서버에 대하여, 클라이언트로 동작한다. 여기서, supplicant는 브리지 또는 AP의 물리적인 포트의 사용권을 외부의 인증서버로부터 받아야만 한다.

그러나 제안된 방식은 IEEE802.1x 모듈이 탑재된 AP에 사용자 인증 캐시테이블을 추가함으로써, AP가 인증서버를 대신하여 사용자 인증처리를 할 수 있다. 그림 2는 인증서버에서 사용자 인증처리 동작과정과 브리지 또는 AP에서 사용자인증처리 동작과정이다. 그리고 각 시스템의 처리 및 지연에 대한 시간을 다음과 같이 가정하였다. 단말과 AP 사이의 전송대역은 11Mbps로 정의 하였고, AP와 인증서버의 전송대역은 1.544Mbps(T-1)로 정의한다. 그리고 시뮬레이션 환경에서 각 시스템에서의 처리 지연시간을 사용자PC는 0.005초로 가정하였고, AP에서는 0.05초로 가정하였다. 그리고 인증서버에서는 0.5초로 가정하였다. 이 시스템의 처리 및 지연시간을 고려해보면, 인증서버 대신에 AP에서 사용자 인증처리를 수행하도록 함으로써 제안된 방식의 경우 사용자 대기시간이 단축됨을 알 수 있다.



(a) 기존방식



(b) 프록시를 사용한 방식

그림 2. 기존방법과 프록시를 사용한 방식의 인증처리 지연시간 비교

그리고 제안된 방식을 가진 AP는 사용자 인증처리대행을 위하여 사용자 ID와 암호를 사용자인증 캐시테이블에 저장하는 기능, supplicant의 사용자ID가 사용자 캐시테이블에 있는지검사하는 기능을 추가 하고, 인증처리 기능의 일부인 MD5 Challenge 기능이 추가되었다. 그리고 AP와 인증서버간 사용자 비밀번호 송수신시 사용될 인코딩기능과 디코딩 기능을 추가되었다. 표 1은 기존의 방법과 제안된 방법에서 추가된 기능을 요약한 것이다.

표 1. 802.1x표준과 프록시를 위해 추가된 기능

IEEE802.1x표준

SUPPLICANT	AUTHENTICATOR	인증서버
EAPOL_START EAP(RESPONSE) EAPOL_END	브리징 기능(Controlled Port) EAP 프로토콜 FORWARDING (Uncontrolled Port) Radius Client EAP(REQUEST_ID)	EAP(REQUEST) RADIUS 서버 사용자 인증 EAP SUCCESS/FAIL

추가된 기능

SUPPLICANT	AUTHENTICATOR	인증서버
	사용자 인증용 캐쉬테이블 암호화된 사용자 비밀번호 전송요구 EAP(REQUEST_AUTH) 사용자 인증 EAP SUCCESS/FAIL 암호 디코딩	암호화된 사용자 비밀번호 전송 암호 인코딩

Ⅲ. 제안된 Backend authentication 기능부의 상태천이

AP에 내장되는 backend authentication 기능부는 인증서버에 대한 인증프로토콜의 클라이언트 기능을 수행한다. 그림 3은 IEEE802.1x 브리지 또는 AP의 상태천이도 중 캐시기능이 추가된 backend authentication 기능부의 상태천이도이다.

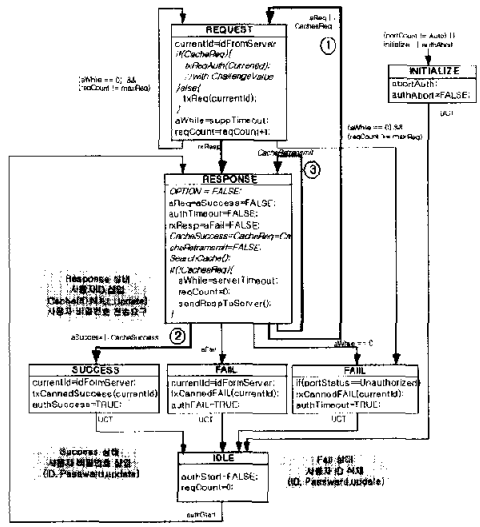


그림 3. 사용자 인증처리가 가능한 backend authentication의 상태도

◆ 제안된 방식의 동작 절차는 다음과 같다. 먼저, INITIALIZE 상태에 의해 backend authentication 환경이 초기화 되고 IDLE 상태로 천이된다. 그리고 IDLE 상태에서는 authStart 이벤트 발생으로 RESPONSE 상태로 천이한다.

◆ RESPONSE 상태에서 supplicant로부터 EAP_Response(ID) 메시지를 수신하면 사용자 ID가 사용자 캐시테이블에 있는지 검사한다. 사용자 ID가 인증용 캐시테이블에 있다면 CachesReq① 이벤트가 발생하여 REQUEST 상태로 천이된다. 사용자 ID가 사용자인증 캐시테이블에 없다면 IEEE802.1x 표준 backend authentication 상태도의 동작과 동일한 절차에 따라 인증서버에게 EAP_Response(ID) 메시지를 중계한다.

◆ 또한, 이 RESPONSE 상태에서 supplicant로부터 EAP_Response(AUTH) 메시지를 수신하면 사용자인증 캐시테이블을이용하여 사용자 인증처리를 수행한다. 사용자 인증처리가 성공하면 CacheSuccess ② 이벤트가 발생하여 SUCCESS 상태로 천이되고, supplicant로 인증성공 메시지를 전송한다. 사용자 ID가 사용자인증 캐시테이블에 없다면 인증서버로 EAP_Response(AUTH) 메시지를 중계한다.

◆ 만약, 사용자ID는 일치하나 AUTH 메시지가 일치 하지 않을 경우 Cacheretransmit③ 이벤트가 발생하면, AUTH 메시지를 사용자인증 캐시테이블

에 임시 저장한 후 인증서버로 EAP_Response(ID) 메시지를 전송한다. 이후, 인증서버로부터 EAP_Request(AUTH)가 수신되고 사용자인증 캐시 테이블에 저장된 AUTH 메시지와 인증서버로부터 수신한 AUTH 메시지를 비교하여 일치하면, CacheSuccess 이벤트가 발생하여 SUCCESS 상태로 천이한다. 만약, 일치 하지 않을 경우 aFail 이벤트가 발생하여 FAIL상태로 천이한다. 이외의 나머지 상태들은 IEEE802.1x 표준 backend authentication의 상태천이도와 같이 동작한다[2][3].

Ⅳ. 캐시테이블 및 새로 정의된 RADIUS 속성값

ID	비밀번호
사용자 ID (1)	비밀번호 (1)
사용자 ID (2)	비밀번호 (2)
⋮	⋮
사용자 ID (n)	비밀번호 (n)

그림 4. 사용자 인증캐시테이블 구조

제안된 프록시 기능을 가진 브리지 또는 AP용 사용자인증 캐시테이블은 브리지 또는 AP의 물리적 포트를 사용할 때 사용자인증을 위해 사용된다. 이 사용자인증 캐시테이블은 그림 4와 같이 사용자 ID와 사용자 비밀번호 목록으로 구성되도록 하였다.

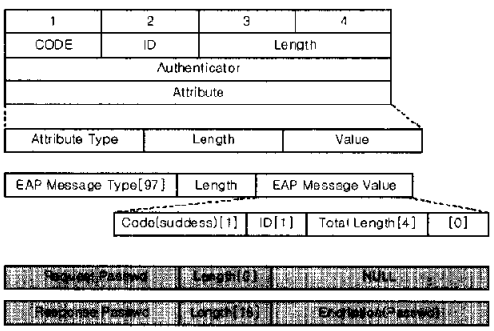


그림 5. RADIUS 속성값 및 새로 정의된 인증관련 속성값

그림 5는 새로 정의된 RADIUS 속성값에 대한 정의이다. RADIUS 속성값은 사용자ID에 대한 비밀번호 전송요구 및 응답에 사용된다[4][5]. 여기서, 비밀번호는 암호화되어 전송된다. 이 암호화된 비밀번호를 수신한 브리지는 복호화 해야 한다. 그리고 인증서버와 브리지간의 암호화와 복호화는 동일한 비밀 키와 동일한 암호 알고리즘을 사용하도록 한다. 여기서 비밀키는 반드시 브리지와 인증서버만 알고 있어야 한다[6].

Ⅴ. 제안된 인증 프로토콜의 동작

제안된 인증프로토콜 동작은 다음과 같은 3가지 경우를 예로들 수 있다.

1. 브리지 초기상태 또는 사용자 정보가 캐시테이블에 없는 경우

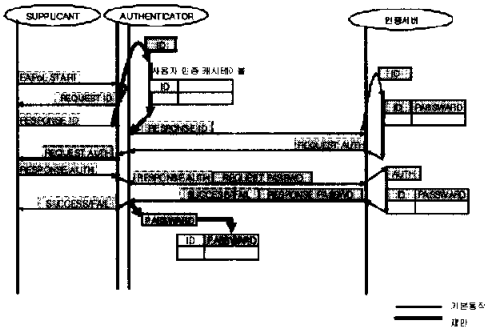


그림 6. 사용자 정보가 캐시테이블에 없는 경우의 동작과정(기존방식)

그림 6은 사용자ID와 비밀번호를 사용자캐시테이블에 등록하는 과정이다. 먼저, 단말과 브리지간 동작에서 단말은 EAP_START 메시지로 802.1x 기능이 탑재된 브리지사용요청을 한다. 이에 대한 응답으로, 브리지는 REQUEST_ID 메시지를 단말에게 전송하며 사용자 ID를 요구한다. 단말은 자신의 ID를 RESPONSE_ID 메시지로서 브리지에 응답한다. 여기까지는 IEEE802.1x 표준과 제안방식의 기본동작은 같다.

다음으로, 단말로부터 RESPONSE_ID를 수신한 브리지는 ID정보를 사용자 인증용 캐시테이블에 있는지 검사한다. 만약 사용자 ID가 인증용 캐시테이블에 없을 경우, 사용자 ID를 캐시테이블에 임시 저장한 다음, 이 브리지는 RESPONSE_ID 메시지를 인증 서버에 중계한다. 이후, 인증서버로부터 REQUEST_AUTH 메시지를 받은 브리지는 이 메시지를 단말에게 중계하고, 브리지는 단말로부터의 RESPONSE_AUTH 메시지가 오기를 기다린다.

이후, 단말로부터 RESPONSE_AUTH 메시지를

받은 브리지는 이 메시지에 인증서버와 미리 약속된 방식의 비밀번호 전송요구 속성값을 첨가하여 인증서버에 전송하고 인증서버는 단말에 전송할 EAP_SUCCESS나, EAP_FAIL 메시지에 브리지와 사전에 약속된 키값으로 암호화된 비밀번호 응답 속성값을 첨가하여 브리지로 전송한다. 만약, 사용자에게 브리지 포트의 사용허락 메시지인 EAP_SUCCESS 메시지가 도착할 경우 단말에게 브리지 포트의 사용허락 메시지인 EAP_SUCESS를 중계하고, 동일한 사용자로부터 재설정된 경우를 대비하여 캐시테이블에 해당 ID를 찾아 비밀번호를 저장한다.

반면에, EAP_FAIL 메시지가 도착 했다면 단말에게 FAIL 메시지를 전송하고 캐시테이블에 새로운 사용자 비밀번호를 등록한다. 사용자가 비밀번호의 오류에 의해서 인증처리가 실패했다면, 다음 인증처리 요청에는 브리지가 인증서버를 대신하여 사용자 인증처리를 할 수 있도록 하기 위함이다. 만약, 사용자ID 오류에 따른 EAP_FAIL 일 경우 캐시테이블에 등록된 사용자 ID를 삭제한다.

2. 사용자 정보가 브리지 캐시테이블에 있는 경우

이후, 사용자 ID와 비밀번호가 캐시테이블에 저장된 사용자가 브리지 사용에 대한 인증처리를 다시 요구하면, 브리지는 인증서버를 대신하여 브리지의 사용자 캐시테이블만 가지고 사용자 인증을 할 수 있다. 뿐만 아니라 이 방법은 그림 7의 동작 과정처럼 소규모 네트워크 망에서 인증서버를 두지 않고 브리지만으로도 사용자 인증을 할 수 있는 장점도 있다. 이것은 브리지가 인증서버의 일부 기능을 수행 하기 때문에 가능 하다.

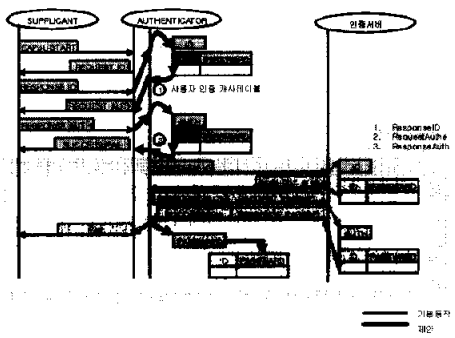


그림 7. 사용자 정보가 브리지 캐시테이블에 있는 경우의 동작과정(제안방식)

그리고 그림 7의 옵션부분인 사각형 부분은 브리지가 사용자 인증용 캐시테이블을 이용하여 브리지 사용허락 메시지를 단말에게 전송한 뒤 사용자 인증을 올바로 했는지 인증서버에게 다시 물어 보거나 주기적으로 캐시테이블을 갱신 하는 절차이다.

3. 사용자 ID정보는 있으나 비밀번호가 일치 하지 않을 경우

그림 8처럼 한 사용자가 브리지 A로부터 인증을 받은 후, 다른 지역으로 이동할 수 있다. 이때 이 사용자는 브리지 B로부터 인증을 받은 뒤 자신의 비밀 번호를 변경 후, 브리지 A로부터 다시 인증을 받을 경우도 발생하게 되어 사용자 인증 처리 과정에서 ID는 같으나 비밀 번호가 다를 경우가 발생하게 되어 사용자 FAIL이 발생할 것이다. 이러한 경우에는 인증 서버에게 다시 인증 정보를 확인 해야만 한다.

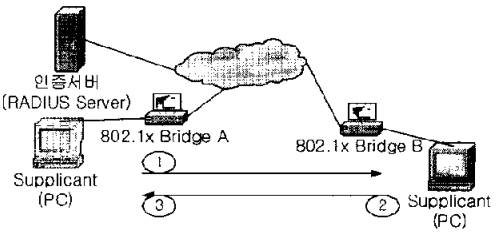


그림 8. 사용자 ID정보는 있으나 비밀번호가 일치 하지 않을 경우 발생 예

AP가 사용자 인증처리 과정에서 암호가 일치 하지 않을 경우가 발생 한다면, 브리지는 인증 절차를 다시 해야 한다. 소규모 네트워크 망에서 인증서버가 없는 경우, 이런 발생을 하지 않는다. 왜냐하면, 관리자가 사용자 등록을 직접 할 수 있기 때문이다. 여기서의 동작은 사용자 인증을 허락한 ID를 RESPONSE_ID에 실어 인증서버에게 전송한 뒤, 브리지는 인증서버로부터 REQUEST_AUTH 메시지가 수신되기를 기다린다. 인증서버로부터 REQUEST_AUTH 메시지를 받으면 브리지는 사용자 ID를 캐시테이블에서 암호를 찾아 RESPONSE_AUTH 메시지를 인증서버로 전송하고, SUCCESS 메시지를 받으면 캐시테이블을 그대로 새로 수정 한다. 만약, FAIL일 경우 접속을 끊고 캐시테이블에서 사용자 정보를 지우도록 한다.

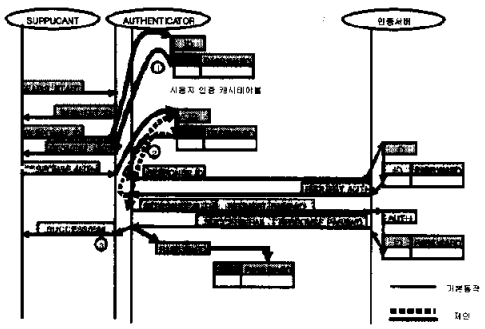


그림 9. 사용자 ID정보는 있으나 비밀번호가 일치 하지 않을 경우의 동작과정(제안방식)

VI. 모의실험 및 분석

제안한 AP의 성능을 분석하기 위하여 사용자인증 캐시테이블을 사용하였을 때, 캐시테이블의 크기에 따른 적중률과 적중률에 따른 평균 사용자 대기시간을 SIMULA를 이용한 시뮬레이션으로 분석하였다[7].

1. 캐시테이블의 크기에 따른 적중률

사용자인증 캐시테이블의 크기에 따른 적중률은 표 1의 사용자 이동률에 대한 파라미터를 적용하여 시뮬레이션 하였다. 그리고 사용자인증 캐시테이블 목록의 최대크기를 20으로 정의하였다. 여기서 캐시 알고리즘은 LFU(Least Frequently Used) 방식을 사용하였다. 그리고 이동률에 대한 적중률과, 캐시테이블의 크기변화에 따른 적중률에 대해 모의실험을 하였다. 이를 위하여, 이동(mobile) 사용자와 고정(desktop) 사용자를 가정하였는데, 그 이유는 이동성이 많은 사용자는 이동성이 없는 사용자에 비하여 AP의 캐시테이블의 갱신이 많이 발생하기 때문이다. 표 1의 이동 사용자의 이동률에 따른 모의실험 결과 그림 10과 같은 적중률을 얻었다. 고정 사용자가 이동 사용자 보다 많은 6부터 적중률이 0.5이상이 됨을 알 수 있었고, 고정 사용자와 이동 사용자 분포가 비슷한 경우의 결과는 캐시테이블크기 15부터 적중률이 0.5이상이 됨을 알 수 있었다. 마지막으로, 이동 사용자가 고정 사용자 보다 많을 경우는 캐시테이블크기가 18부터의 최대 적중률이 0.5이상이 됨을 알 수 있었다. 결과적으로 사용자의 이동률이 적을수록 적중률이 높아짐을 알 수 있었다.

표 2. 시뮬레이션 환경

	(a)	(b)	(c)
Desktop 사용자	80%	50%	20%
Mobile 사용자	20%	50%	80%

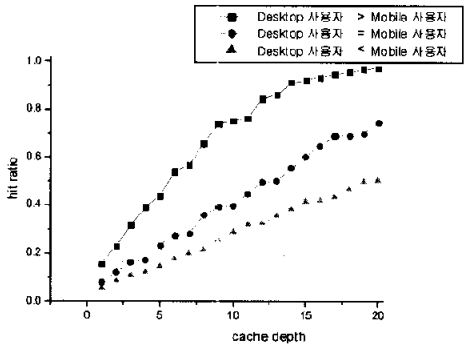


그림 10. 캐시테이블 크기에 따른 사용자의 적중률(사용자수 20)

2. 적중률에 따른 사용자 인증 대기시간

그림 11은 적중률에 따른 사용자 인증 대기시간을 시뮬레이션 하기 위한 환경이다. AP 수는 300, 100 그리고 50대의 AP, AP당 사용자 20명, 그리고 한대의 인증서버를 가지고 모의실험을 하였다. 여기서 각 시스템의 처리 및 지연 시간은 그림 2의 값들을 적용하였다.

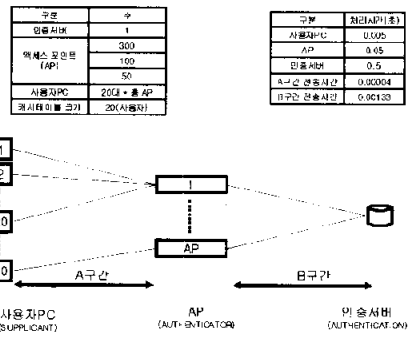


그림 11. 시뮬레이션 환경

그림 12는 사용자가 AP 사용요청을 시작한 후, 사용자가 사용자인증을 부여 받을 때까지의 사용자 대기시간을 기존방식과 비교한 것이다. 적중률 0은 기존방식에 대한 대기시간이다. 초기 사용자들의 사용자ID와 비밀번호를 캐시테이블에 등록할 때의

사용자 대기시간은 사용자 인증 캐시테이블을 사용하지 않을 때와 같다. 하지만 사용자 ID와 비밀번호가 캐시테이블에 저장된 사용자가 AP 사용에 대한 인증처리를 요구하면, 그림 12와 같이 적중률에 따른 사용자 인증 대기시간이 감소함을 알 수 있었다. 결과적으로 적중률이 높아질수록 AP사용에 대한 사용자 인증 대기시간은 감소됨을 알 수 있다. 또한 사용자 인증처리를 AP가 대행 하므로, 사용자 대기시간은 인증처리를 담당하는 AP에만 영향을 받음을 알 수 있었다.

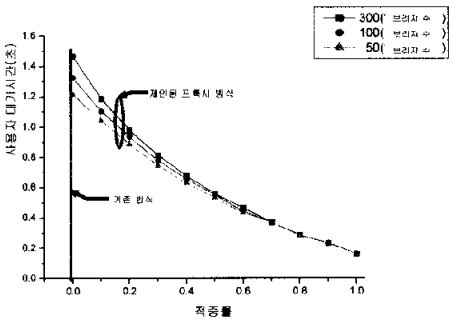


그림 12. 적중률에 따른 사용자 인증 대기시간

Ⅶ. 결론

본 논문에서 제안한 인증서버를 대신한 AP 또는 브리지에서 사용자 인증처리 기능은 캐시테이블을 사용하여 AP에서의 사용자 인증처리에 의한 물리적 포트 사용권한을 부여할 수 있는 방식이다. 이 경우, 브리지와 인증서버간의 인증관련 메시지의 트래픽을 줄일 수 있으며, 인증서버의 사용자 인증처리에 대한 부하를 줄일 수 있다. 그리고 모의 실험을 통해 사용자 인증처리에 따른 대기시간이 줄어들었음을 검증하였다. IEEE802.1x에서 사용하는 EAP는 일반적으로 다양한 인증 프로토콜(TLS, TTLS, OTP, MD5)을 사용할 수 있다. 본 논문에서는 MD5와 같은 일방향 인증에 기초한 것이며, 만약 일회용 패스워드(OTP)나 양방향 인증을 제공하는 TLS 등의 인증프로토콜을 사용할 경우는 AP에 대한 별도의 성능분석이 요구된다.

또한 제안된 방식을 사용하면 AP의 인증용 캐시테이블을 운영자가 직접 구성할 경우에는 인증서버 구축에 대한 비용의 추가부담이 없어지는 효과도 있다.

참 고 문 헌

[1] IEEE Std 802.1x, Standards for Local and Metropolitan Area Network, Standard for Port based Network Access Control, 2001.

[2] Blink and Vollbrecht, RFC 2284, PPP Extensible Authentication Protocol, Mar. 1998.

[3] B. Aboba, D. Simon, RFC 2716, PPP EAP Authentication Protocol, Oct. 1999.

[4] C. Rigney, et al., RFC 2058, Remote Authentication Dial In User Service (RADIUS), Jan. 1997.

[5] C. Rigney, and W. Willats, RFC 2869, RADIUS extension, Jun. 2000.

[6] W. Stallings, Cryptography and Network Security, Prentice-Hall, 1999.

[7] SIMULA web site: www2.cee.hw.ac.uk/~rjp/

이 동 현(Dong-Hyun Lee) 정회원

2001년 2월 : 한국항공대학교 통신정보공학과 학사
2003년 2월 : 한국항공대학교 대학원 통신정보공학과 석사
2003년 2월~현재 : (주)이오넥스 연구원

<주관심분야> 무선랜, 인증 및 보안, 프로토콜

이 현 우(Hyun-Woo Lee) 종신회원

1993년 2월 : 한국항공대학교 전자공학과 학사
1995년 2월 : 한국항공대학교 대학원 통신정보공학과 석사
2003년 2월 : 한국항공대학교 대학원 통신정보공학과 박사 과정수료
1995년 2월~현재 : 한국전자통신연구원 네트워크서비스연구부 선임연구원

<주관심분야> 트래픽 혼잡제어, 통신망 연동, 무선랜

정 해 원(Hae-Won Jung) 정회원

1980년 2월 : 한국항공대학교 항공통신정보공학과 학사
1982년 2월 : 한국항공대학교 대학원 항공전자공학과 석사
1999년 2월 : 한국항공대학교 대학원 항공통신정보공학과 박사

1982년 3월~현재 : 한국전자통신연구원 라우터연구부 10GB H/W팀 팀장

<주관심분야> 기가비트이더넷, 무선랜, 홈네트워킹

윤 종 호(Chong-Ho Yoon) 정회원

1984년 2월 : 한양대학교 전자공학과 학사
1986년 2월 : 한국과학기술원 전기 및 전자공학과 석사
1990년 8월 : 한국과학기술원 전기 및 전자공학과 박사
1995년 8월~1996년 8월 : University of Arizona 방문교수
1991년 8월~현재 : 한국항공대학교 전자·정보통신·컴퓨터공학부 교수

<주관심분야> 컴퓨터 통신망, 성능분석