무선 랜 환경에서 안정적인 로밍을 위한 선행 인증기법 설계

A Design of Proactive Authentication Technique for Stable Roaming In Wireless LAN Environment

홍 순 자* 구 용 완**
Soon-ja Hong Yong-Wan Koo

요 약

제 4 세대 이동 통신망 SBI2K(Systems Beyond IMT 2000)의 사용화가 예상되고, 무선 랜 사용자의 이동서비스(mobile service) 요구가 증가됨에 따라 단말기의 이동성(mobility)을 지원하는 새로운 인증 방법이 요구된다. 무선 랜은 전파라는 전송매체를 사용하기 때문에 보안에 취약하다. 현재 무선 랜의 보안기능을 일관성 있게 제공하는 기술로 WPKI (Wireless Public Key Infrastructure)가 있다. WPKI는 인증서 사용이 필수적인데, 이것은 인증서 검증 및 CRL검색으로 인하여 핸드오프 성능에 많은 부담으로 작용된다. 본 논문에서는 무선 랜의 안정적인 이동 서비스를 위해 WPKI의 기술을 사용하면서 핸드오프에 영향을 주지 않는 기법을 제시한다. 제시한 기법은 통신 데이터의 암호화에 필요한 비밀 키를 단말과 로밍 서버가 선행하여 습득하는 것이다.

Abstract

Wireless LAN is intrinsically weak in security of transmissions.

WPKI (Wireless Public Key Infrastructure) is a well known method to deal with the security issues in wireless LAN. The authentication required by the method becomes a source of unreliability of the hand-off performance. This paper suggests a solution to overcome the instability while using the WPKI technique. Prior to getting into the next region, a station is provided with the keys of the surrounding regions so that the possible delay problem can be avoided during the actual hand-off time. Thereby the hand-off instability can be solved in the WPKI framework.

☞ Keyword : WPKI, 무선 랜, 로밍 서버(Roamimg Server), 선행인증기법(Pre-Authentication)

1. 서 론

무선 랜 기술은 IEEE 802.11b의 표준화가 완성되고 무선 단말기의 사용자가 급속히 증가함에 따라 빠른 성장속도를 보이고 있다. 제4세대 이동 통신망 SBI2K(Systems Beyond IMT 2000)의 상용화가 기대되는 가운데, 전송기술의 한계와 통신비용의 문제 등으로 인하여 공항, 호텔, 대학, 병원과 같이 이용자가 밀집되어 있는 Hot-Spot영역의 데이터 통신수단으로 사용되던 무선 랜이 이제는 고속 이동성 지원을 위한 IP 기반의 무선접속 표준 개발이 시급한 시점까지 도달했다. 이동 통신의 대중화로 인하여 무선단말기 사용자의 이동서비스 요구가 높아지고 제4세대 이동통신망의 연구와 표준이 확립되는 시점에서 이동을 지원하는 무선네트워크 환경의 개발이 시급하다.

무선 랜 사용자는 유선네트워크 서비스와 크게 다르지 않은 안정적인 환경을 제공받기 원한다. 그러나 데이터의 전파를 통해 브로드캐스트되는 무선통신의 특성상 일정 범위 안에 있는 다른 사용자들의 도청 및 실시간 공격 등으로 인한 보안상의 문제를 일으킬 수 있다. 또한 무선네트워크의 이동사용자가 무선데이터 전송지역을 이탈 시

* 정 회 원 : 수원대학교 일반대학원 컴퓨터학과(박사)
hsj109@suwon.ac.kr
** 종신회원 : 수원대학교 IT대학장, 컴퓨터학과 교수
ywkoo@suwon.ac.kr
[2006/06/06 투고 - 2006/07/03 심사 - 2006/08/01 심사완료]

발생하게 되는 AP(Access Point)간 지연요구에 따른 서비스 단절 현상과 핸드오프의 비효율성에 관한 문제점들이 지적되고 있다.

WEP(Wired Equivalent Privacy)알고리즘에서 키 스트림의 단순성으로 인하여 실시간 공격과 도청으로 인한 평문의 노출, DoS 공격이 가능하다는 점은 IEEE 802.11b 표준의 보안상의 문제점으로 지적되었다[1]. 무선 랜 표준인 IEEE 802.11b에서의 인증은 사용자 인증이 아닌 디바이스 인증에 머물고 있는 실정이며 이 또한 매우 취약하다. 이에 따라 강력한 사용자 인증을 제공할 수 있는 메커니즘으로 IEEE 802.1x가 개발되었다. IEEE 802.1x에서는 EAP-TLS, LEAP, PEAP 등의 다양한 사용자 인증 메커니즘의 사용이 가능한데, 이러한 사용자 인증 메커니즘은 모두 공개키 암호기술을 이용하고 있어 무선 랜 환경에서의 WPKI(Wireless Public Key Infrastructure) 구축이 절실히 요구된다[2][3][4].

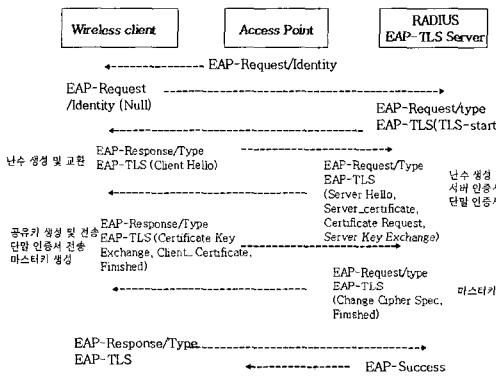
그런데 WPKI는 강력한 보안성을 제공하는 반면 인증서 검증이나 CRL(Certificate Revocation Lists)검색 등의 오버헤드를 일으키는 원인이 된다. 또한 이러한 점은 이동 무선단말 사용자가 기존의 AP지역에서 새로운 AP지역으로의 이동 시에도 사용자 인증과정 등에 많은 지연을 발생시키는 원인이 되며, AP구간마다 이러한 비효율적인 검증을 매번 반복하게 된다.

이동을 지원하는 무선네트워크의 환경구축을 위해서는 무선단말기 사용자가 이동 시에도 무선 랜 전송기술의 한계로 인해 발생하는 서비스 단절현상 및 비효율적인 핸드오프를 극복할 수 있는 방안이 제시되어야 한다. 본고에서는 이러한 해결책을 위해서 앞서 연구되었던 선행 인증기법을 응용하여 핸드오프 시 인증 딜레이 현상에 대한 해결책을 찾고 안정적인 서버인증에 대해서 설계한 후, 이동지원 서버(Roaming Server)를 통해 상호인증을 선행하는 환경을 설계한다.

2. 무선랜 인증

2.1 EAP-TLS(Transport Layer Security)

802.1x 단말에 사용되는 보안 메커니즘인 EAP-TLS는 클라이언트 서버간의 어플리케이션에서 도청이나 간섭, 메시지 위조와 같은 비권한 제어를 방지할 수 있다. EAP-TLS는 TLS 핸드쉐이크를 EAP 프로토콜로 확장한 방법으로써 상호인증과 키 분배에 대한 메커니즘을 포함한다. (그림 1)은 EAP-TLS의 핸드쉐이크 과정을 보여주고 있다.



(그림 1) EAP-TLS 상호 인증 및 키 분배

2.2 IEEE 802.11i

IEEE 802.11i는 무선 랜 보안을 강화하기 위하여 추가된 무선 랜 규격이다. 단말기의 사용자 인증 및 단말기와 AP 사이의 키 생성 과정, 데이터 암호화 복호화 과정에 대한 규격에 대한 정의를 다루고 있다.

사용자 인증 방식 중, IEEE 802.1x를 따르는 사용자 인증 방식에서는 단말기가 AP의 중개를 통하여 원격지에 있는 인증 서버로부터 인증을 받게 된다. 그리고 단말기가 인증에 성공하면 AP는 단말기와 데이터 보안에 사용될 암호화키를 교환한 후, 망 접속을 허용하며 TKIP 또는 CCMP

알고리즘을 이용하여 데이터 프레임을 암호화하여 통신하게 된다. 단말기가 선인증을 받지 않고 로밍을 하게 되면, 단말기는 새로운 AP와 인증 및 키 교환 과정을 모두 다시 수행하여야 한다. 망 구성의 상황에 따라 인증 서버와 단말기의 재접속 요구가 발생하게 되며 그러한 과정에서 데이터 통신이 단절되어 지연현상을 일으키게 된다.

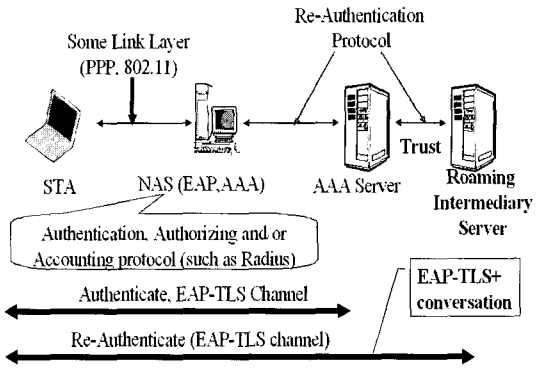
2.3 선행 인증(Pre-Authentication)을 통한 빠른 핸드오프

S. PACK 등은 무선 단말기가 기본 서비스 영역에 들어오면, 현재 AP뿐만 아니라 인접한 다수의 AP들과 인증 절차를 선행하여 핸드오프 시 재인증에 대한 지연을 최소화하여 빠른 핸드오프를 가능하게 할 수 있음을 보이고 있다. 현재의 AP와 인접한 AP들의 집합을 핸드오프 영역(frequent hand-off region)으로 정의하게 되는데, 이는 무선 단말기의 움직임 패턴과 AP의 위치에 의해 결정된다. 또한 이러한 요소를 결정하기 위해서는 사용자의 로깅 정보와 핸드오프 이벤트에 대한 로깅 데이터베이스 시스템이 사용되게 된다[5].

3. WPKI 기반의 선행 인증 기법 설계

무선 랜의 인증 보안을 위해서는 WPKI 기반의 802.1X의 인증 기술이 최적임을 알 수 있다. 그러나 WPKI에서는 인증서 사용이 필수적인데, 이것은 인증서 검증 및 CRL 검색의 오버헤드가 핸드오프 성능에 많은 부담으로 작용된다. 본 논문에서는 WPKI기반의 AP간 상호 인증 기법을 사용하면서 동시에 빠른 핸드오프 수행이 가능한 기법을 제안한다. 또한 선행 인증을 통해서 상호인증의 절차를 간소화하여 이동 무선 랜 사용 시 접속 단절 현상을 최소화하고자 하였다.

이와 같이 로밍(Roaming)을 지원하는 무선 랜 환경에서 이동통신보안을 지원하는 로밍 서버(로밍 지원 AAA서버)는 필수적이다[6][7][8]. 본 논문

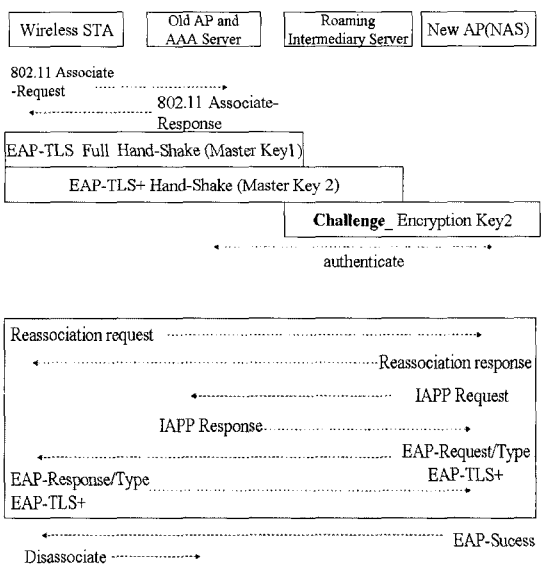


(그림 2) 선행 인증을 위한 로밍 서버의 역할

에서는 (그림 2)와 같이 로밍 서버를 이용하여 이웃한 AP와의 인증 절차를 선행하는 새로운 EAP 인증 유형을 설계한다.

3.1 초기 접속 및 핸드오프 핸드쉐이크

이동성을 지원하는 무선 랜 환경에서 이동 단말기와 각 AP, 로밍 서버간의 초기 인증 및 핸드오프 시 재인증은 (그림 3)과 같은 과정을 거친다. 본 과정에서는 EAP 인증방법 중 EAP-TLS Handshake를 기반으로 한다.

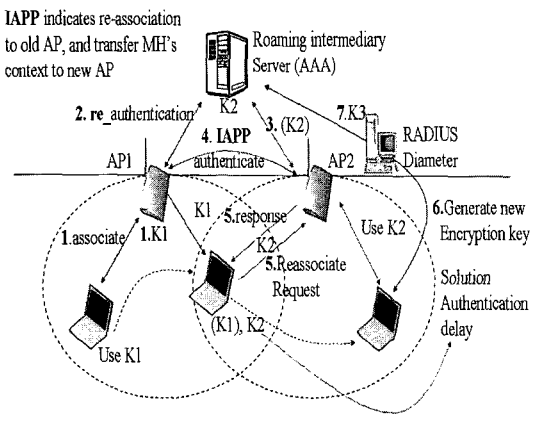


(그림 3) 마스터키2 생성을 통한 단말의 핸드오프 과정

3.2 New 마스터 키 생성을 통한 선행인증 과정

(그림 4)는 로밍을 위한 선행인증 키 생성 및 핸드오프 과정을 보여주고 있다.

① 무선 단말기가 스캐닝을 통해서 AP1을 선택한 후 접속을 요청하고 EAPOL을 통한 해당 NAS와 상호 인증을 시행하여 통신에 필요한 마스터키(Master Key1)를 생성한다.
② 단말기는 선행인증을 위하여 로밍 서버와 2차 인증을 시도한다. 로밍서버는 다음 인증 시 필요한 새로운 마스터키를 선행하여 생성하며 자신과 이동단말기는 새로운 비밀키(Key2)를 습득하여 저장한다.
③ 단말기는 Key1을 통하여 이동 서비스를 받고 로밍 서버는 단말기의 이동을 탐지하여 이동할 새로운 AP2(NAS)에게 자신이 단말기와 인증하였던 마스터키2의 Encryption 정보를 보낸다.
④ 새로운 AP2에게 단말기의 이동이 포착되면 AP2는 단말기에 이전의 AP1 정보를 얻고 그 정보를 통하여 AP1에게 IAPP 요청을 하여 사용자 및 서비스 정보를 확인한다.
⑤ 로밍 서버는 재접속 요청을 한 이동 단말이 AP1에 수행하던 단말임을 확인한 후 새로운 AP2(NAS)에 자신과 서버와 비밀성 보장을 위해 저장하였던 Encryption Key(Key2)를 이용하여 단말기와 키 인증을 수행하고 서비스를 허가한다. 마지막으로 인증 서버는 다음 핸드오프 인증 선행을 위해 단말기에 메시지를 보낸다.



(그림 4) 선행된 Master Key를 이용한 상호 인증과정

4. 성능평가

본 장에서는 제안된 선행 인증 기법에 대해 모의 네트워크와 큐잉모델을 통하여 성능을 분석한다. 1차적으로 모의 네트워크를 통한 인증시간 및 인증 절차를 분석하고 그 결과를 토대로 큐잉모델에 대입하여 설계한 알고리즘의 성능을 평가한다.

모의 네트워크를 위해 사용된 장비로는 IEEE 802.1x EAP-TLS 기반의 라디우스 서버 'HP PRO-Lion ML110'을 사용하였고, AP는 3Com에서 제작한 제품을 사용하였다. 또한 이동 스테이션은 Symbol의 PPT8846 CE.Net을 사용하였다. 평가를 위한 네트워크 구성은 IEEE 802.1x EAP-TLS 기반으로 인증시간 분석을 위해 (그림5)와 같은 환경으로 실험하였다.

4.1 모의 네트워크 사용 장비

- 라디우스 서버 : CPU : Intel® Pentium® 4 프로세서 630 3.0GHz
  RAM : 512MB(1 x 512MB)
  HDD : 72GB SCSI
- Access Point : 3COM 3CRWE454G72
- 이동 Station (RF Terminal) : Symbol PPT8846 CE.Net
- HUB : 3COM 3C16470
- 네트워크 패킷 분석용 단말 : LG Xnote 듀얼코어 1024 RAM

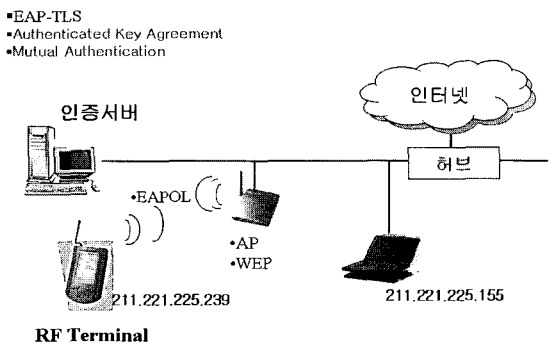
이동 스테이션이 인증을 수행할 때까지 걸리는 시간을 측정하는 방법을 정의하고 그 기준을 기

반으로 하여 큐잉모델에 적용할 데이터를 추출한다. 측정 기준은 인증절차를 Start하여 Success할 때까지의 시간을 기록한다.

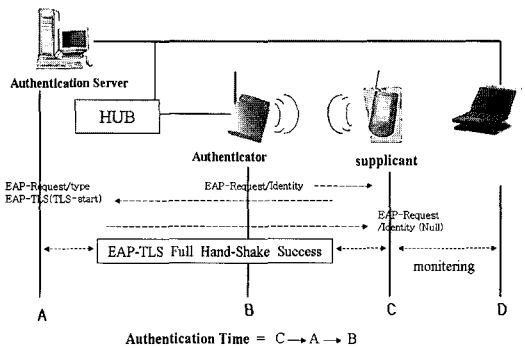
이동스테이션과 인증 서버사이의 인증 절차에 대한 기록은 (그림 6)에서 허브와 연결된 '네트워크 패킷 분석용 단말'에서 'Ethereal 네트워크 모니터링 툴'을 실행하고 OS 타이머를 사용하여 핸드쉐이크 과정(start부터 success할 때까지 과정)의 시간을 기록한다.

5. 성능분석을 위한 큐잉모델

본 장에서는 네트워크 패킷 분석기인 Ethereal에서 추출된 데이터를 통하여 성능을 분석한다. 무선 랜 서비스를 받기위해 초기인증을 요청하는



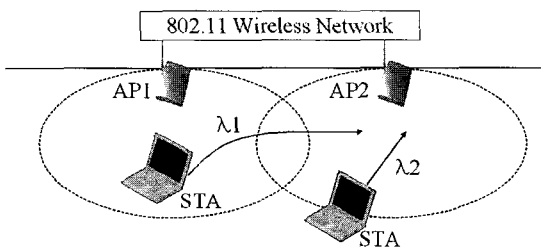
(그림 5) 모의 네트워크 구성도



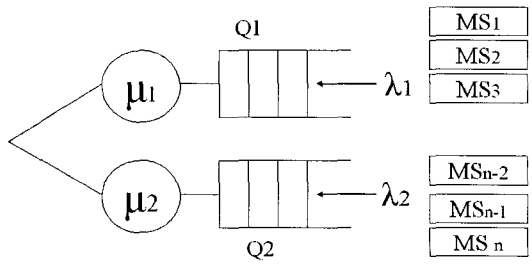
(그림 6) 스테이션과 서버의 인증시간을 측정하기 위한 구성도

무선 단말기의 발생은 포아송 분포를 갖는 확률변수로 모델화할 수 있다. 단말기가 접속을 요청할 경우 상호인증 절차가 완료될 때까지의 대기시간은 CRL 검색과 인증서 검증, 그리고 패킷 전송시간의 합으로 나타낸다. 본 논문의 성능 분석에서는 CRL검색 시간은 CRL 크기와 저장 위치에 관계없이 항상 동일하다고 가정한다. (그림 7) 또한 인증서의 종류와 상관없이 인증서 검증시간과 패킷 전송시간은 네트워크 패킷 분석기인 Ethereal를 통해 얻어진 데이터를 사용하며, 핸드오프를 요청하는 무선 단말기의 발생도 역시 포아송 분포를 가진다고 가정한다. 핸드오프 시 인증 과정은 공개키를 이용함으로써 인증 처리에 일정한 시간이 소비된다고 가정한다[9].

제안한 인증절차의 성능 분석을 위하여 (그림 7)과 같은 환경을 설정한다. 초기 접속으로 인증을 요청하는 단말기가 λ2의 도착률로 상호 인증이 시작되고 핸드오프를 요청하는 단말기는 λ1의 도착률로 상호인증이 시작된다. 하나의 AP에 초기 인증을 요청하는 무선 단말기와 핸드오프 요청을하는 무선 단말기가 모두 존재할 경우 AP는



(그림 7) 분석을 위한 환경 설정



(그림 8) 큐잉 모델

우선순위 큐잉에 의해서 핸드오프 인증 요구 단말기에 서비스를 우선적으로 수행한다. 또한 AP1과 AP2 큐잉모델은 (그림 8)과 같이 Q1, Q2의 큐로 구성된다[10]. Q1은 Q2보다 우선순위를 갖는 큐로서 핸드오프 시 인증 서비스를 처리한다. 이때의 인증 서비스 처리시간은 메시지의 암호화와 복호화 시간 그리고 패킷 전송시간의 합으로 계산한다. 또한 Q1에서의 도착률은 λ1로 나타낸다.

Q2는 초기 로그인 과정의 인증 서비스를 처리하는 큐로서 처리시간은 CRL 검색시간, 패킷 전송시간, 인증서 검증시간의 합으로 계산한다. Q2에서의 도착률은 λ2로 나타내며 Q2의 처리 순위는 Q1보다 낮은 순위를 갖는다. Q1, Q2는 FIFO(first-in, first-out)방식을 적용하며, Q2에서 초기 인증 서비스가 종료된 후에 핸드오프를 위한 인증 서비스를 수행하는 비선점 방식이 적용된다.

이와 같은 큐잉 모델의 각 큐에 대한 평균 대기시간은 (식-1)과 같다[10].

$$E(W_k)=\frac{\sum_{i=1}^{2}\lambda_i E(P_i^2)}{2(1-\sum_{i=1}^{k-1}\rho_i)(1-\sum_{i=1}^{k}\rho_i)}\ (k=1,2)\ \cdots\ \text{(식-1)}$$

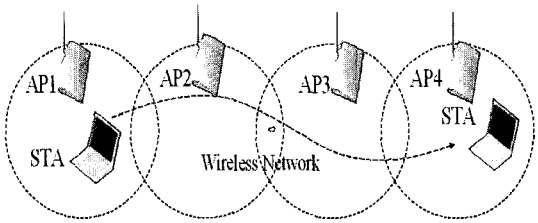
위의 식에서 W_1, W_2는 각각 Q1, Q2에서의 평균 대기시간이고, P_1, P_2는 Q1, Q2에서 하나의 인증에 대하여 소요되는 처리시간을 나타내는 랜덤변수이다. ρ_1, ρ_2는 각각 초기 인증 및 핸드오프 인증으로 인한 서버의 활용도를 나타내는 변수로서 $\rho_1=\lambda_1 E(P_1), \rho_2=\lambda_2 E(P_2)$의 값을 갖는다. 또한 E(·)는 기대치를 나타낸다.

(표 1)은 큐잉 모델에 적용되는 파라미터이다.

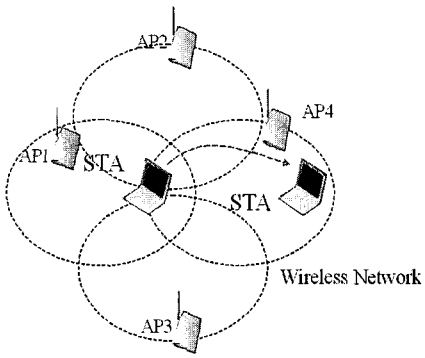
본고의 성능분석은 단말의 움직임이 예측 가능

(표 1) 파라미터의 동작 과정

파라미터	값	정 의	가 정
Wban	2Mbps	무선 네트워크 대역폭	모든 무선네트워크는 동일하다고 가정
Lban	10Mbps	유선 네트워크의 대역폭	모든 유선네트워크는 동일하다고 가정
Cser	600ms	서버를 방문하여 CRL을 검색하는데 소요되는 처리시간	모의실험을 통한 지수분포를 따른다고 가정
Vcer	32ms	인증서 필드를 검증하는데 소요되는 시간	모의실험을 통하여 예상한 데이터를 각 호스트와 서버의 성능에 관계없이 동일하다고 가정
Kenc	1.6MByte/sec	메시지 보호를 위한 암호화 작업의 처리율	각 호스트와 서버의 성능에 관계없이 동일하다고 가정
Kdec	1.6MByte/sec	암호화된 메시지에 대한 복호화 작업의 처리율	각 호스트나 서버의 성능에 관계없이 동일하다고 가정
Psiz	1KB	인증을 위해서 전송되는 메시지 크기를 나타냄	항상 동일한 값을 갖는다고 가정
Csiz	1KB	인증서의 크기	인증서 종류에 상관없이 동일한 값을 갖는다고 가정



(그림 9) 이동 경로가 예정된 패턴의 환경



(그림 10) 이동경로가 불확실한 패턴

한 '이동 경로가 예정된 패턴의 환경' (그림 9)과 단말 사용자의 움직임을 예상할 수 없는 '이동 경로가 예정되지 않은 패턴의 환경' (그림 10)의 두 가지 환경에서 성능의 차이를 분석한다.

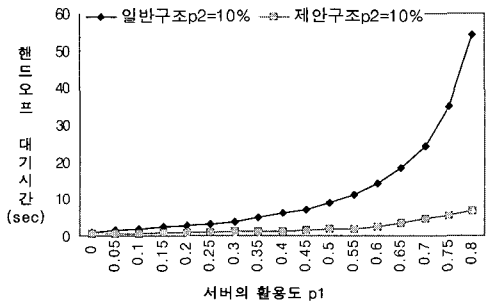
(그림 11)은 '이동경로가 예정된 환경'의 핸드오프 과정에서 '서버의 이용률'이 10%인 경우 ρ_1(핸드오프시 인증 처리율)이 모든 상황(ρ_1= 0%~80%인 경우)에서 일반적인 인증시간보다 빠른 인증시간을 기록하였으며, ρ_1이 높아질수록 성능이 현저하게 떨어지는 '일반적인 인증방법'에 비해 안정적인 인증시간을 기록하였다.

(그림 12)는 '서버의 이용률'이 50%인 경우에도 ρ_1(핸드오프 시 인증 처리율)이 모든 상황(ρ_1= 0%~60%인 경우)에서 일반적인 인증시간보다 빠른 인증시간을 기록하였으며, ρ_1이 높아질수록 성능이 현저하게 떨어지는 '일반적인 인증방법'에 비해 안정적인 인증시간을 기록하였다.

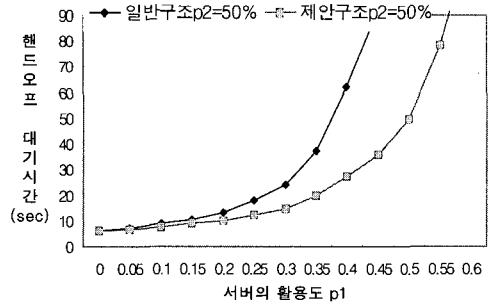
'이동경로가 불확실한 환경'의 성능을 분석 한 결과 제안구조를 통한 핸드오프 과정에서 ρ_2(초기 접속 인증을 처리하는 Q2의 이용률)이 높을수록 일정한 구간에서 대기시간이 급격히 저하되는 것을 확인하였다.

(그림 13)은 '서버의 이용률'이 10%인 경우 ρ_1(핸드오프 시 인증 처리율)이 65%미만일 때 일반적인 인증기법보다 빠른 인증시간을 기록하였으며, 65%이상일 때 인증대기시간이 기존의 방법보다 지연되는 것을 확인하였다.

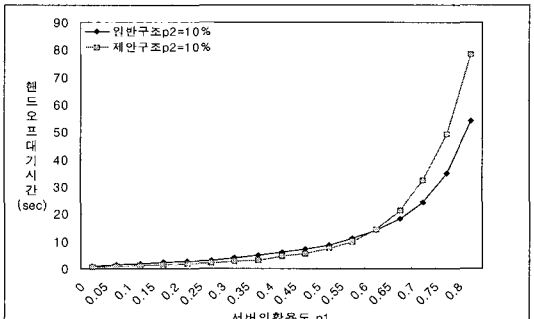
(그림 14)는 '서버의 이용률'이 50%인 경우 ρ_1



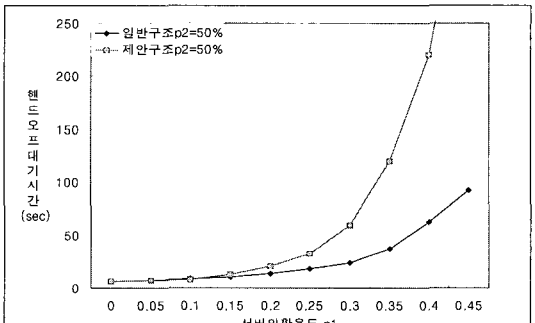
(그림 11) ρ_2=10%일 때 '이동 경로가 예정된 환경'의 성능비교



(그림 12) ρ_2=50%일 때 '이동 경로가 예정된 환경'의 성능비교



(그림 13) ρ_2=10%일 때 '이동 경로가 불확실한 환경'의 성능비교



(그림 14) ρ_2=50%일 때 '이동 경로가 불확실한 환경'의 성능비교

(핸드오프 시 인증 처리율)이 20% 미만일 때 일반적인 인증기법보다 빠른 인증시간을 기록하였으며, 20% 이상일 때 모든 과정에서 인증대기시간이 기존의 방법보다 지연되는 것을 확인하였다. 이러한 현상은 '핸드오프 영역이 교차된 지역'에서 해당 단말이 다수의 AP로부터 상호 인증을 무리하게 수행하기 때문에 발생하였다. 즉 다수의 AP와의 무리한 상호 인증으로 인해 응답 지연 및 딜레이 현상이 초래되는 것으로 보여 진다. 또한 AP에 초기 접속을 요구하는 이동 스테이션이 증가할수록 인증 서버의 이용률과 초기 접속 처리율이 높아지면서 인증절차의 심각한 오버헤드와 응답지연 딜레이 현상을 확인하였다. 다만 제안한 기법을 통해 '이동 경로가 예정된 환경'과 '인증처리 이용률이 낮은 환경'에서 기존의 방법보다 효과적인 인증 수행시간을 기록하였다.

6. 결 론

제시한 선행 인증 기법에 대한 큐잉모델의 성능분석 결과 WPKI기반의 상호 인증을 시행하더라도 유연하게 대처할 수 있었다. 성능분석을 통하여 '서버의 이용률'이 낮은 경우($\rho_2 \leqq 40\%$) 핸드오프 시 일반적인 인증기법보다 안정적인 인증시간을 기록하였다. 그러나 제안구조를 통한 핸드오프 과정은 ρ_2(초기 접속 인증을 처리하는 Q2의 이용률)이 높을수록($\rho_2 \geqq 40\%$) 일정한 구간에서 대기시간이 급격히 저하되는 현상을 보였다.

제안한 기법을 통해 인증수행을 할 경우 이동 사용자는 인증수행시간에 대한 체감 속도가 단축되게 느끼지만 인증서버 측에서는 초기접속 시 '선행 인증 핸드쉐이크'가 수행되기 때문에 인증서버의 p2활용도가 높아지게 된다. 이러한 현상은 p2의 활용비율을 높이게 되어 다른 스테이션의 인증속도에 영향을 미치게 하였다. 즉 '핸드오프 영역'에서 접속을 요구하는 이동단말이 증가될수록 AP가 모든 이동단말로부터 선인증 핸드쉐이크를 수행해야 되기 때문에 '선인증'으로 인한 서버의 이용률을 높이고 그로 인하여 인접한 스테이션의 응답 딜레이 및 오버헤드 현상을 예상할 수 있었다.

향후 연구과제로 본 논문에서 구체적으로 언급하지 않았던, 인증서 폐지방안과 AP변경 시 클라이언트 재인증 방안(IAPP정보교환)에 대한 충분한 고려가 이루어져야 할 것이다. 더 나아가서 무선 단말기의 네트워크 연결 이전에 인증서 및 인증서 폐지목록을 획득할 수 있는 방안에 대한 연구가 필요하다. 또한 AP변경 시 이전에 사용하던 '암호키 재분배' 방안에 대한 연구가 필요하다. 아울러 ρ_2(초기 접속 인증을 처리하는 Q2의 이용률)가 높을 때 인증 서버의 효율적인 버퍼 관리 문제를 해결해야 할 것이다.

참 고 문 헌

[1] 'Port-based Network Access Control', IEEE Standard 802.x, 2001.6

[2] B. Aboba, D, Simon, 'PPP EAP TLS Authentication Protocol'. IETF RFC2716. 1999. 10

[3] Secure Authentication, Access Control, and Data Privacy on Wireless LAN, http://www.funk.com/RADIUS/wlan/wlan_solns.asp, FUNK software

[4] W.A. Arbaugh, "Your 802.11 Wireless Network has No Clothes," University of Maryland, http://www.cs.umd.edu/, Mar.2001.

[5] S.Pack, Y. Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE802.x Model", IFIP TC6 Personal wireless Communication 2002, October 2002

[6] Technical Whitepaper, "Secure Global Roaming for 802.11 WLANs," Veri Sign, 2002.

[7] Jacques Caron, "Public Wireless LAN

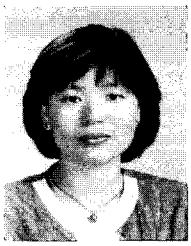
roaming issue," IETF Internet-Draft, draft-caron-public-wlan-roaming-issues-00.txt, November, 2001.

[8] Christopher Mets, "AAA PROTOCOL: Authentication, Authorization and Accounting for the Internet," Cisco Systems, http:// www. com-puter.org/internet/v3n6/w6onwire. htm

[9] Leonard Kleinrock, "Queueing analysis : a foundation of performance evaluation," North-Holland, pp. 160-165, 191

[10] Takagi, Hideaki, "Queuing analysis : a foundation of performance evaluation," North-Holland, pp. 160-165, 1991.

◐ 저 자 소 개 ◑



홍 순 자

1983년 계명대학교 의생활과학과 졸업(학사)
2003년 수원대학교 교육대학원 컴퓨터학과 졸업(석사)
2003년~현재 수원대학교 일반대학원 컴퓨터학과(박사)
관심분야 : 분산 및 운영체제, 시스템네트워크 관리, 무선 통신 등
E-mail : hsj109@suwon.ac.kr

구 용 완

1976년 중앙대학교 전자계산학과 졸업(학사)
1980년 중앙대학교 대학원 전자계산학과 졸업(석사)
1988년 중앙대학교 대학원 전자계산학과 졸업(박사)
1983년~현재 수원대학교 IT대학장, 컴퓨터학과 교수
관심분야 : 분산 및 운영체제, 실시간 시스템, 시스템네트워크 관리, 멀티미디어, 인터넷 등
E-mail : ywkoo@.suwon.ac.kr