무선랜에서의 캐시를 이용한 효율적인 핸드오프 기법 및 성능분석에 대한 연구

이 남 훈, 이 구 연, 이 용*
강원대학교 컴퓨터정보통신공학과, 정보보호진흥원*
전화 : 033-250-6397 / 핸드폰 : 011-9797-8775

A Study for effective handoff technique using cache on IEEE 820.11 wireless LAN and performance analysis.

Nam Hoon Lee, Goo Yeon Lee, Yong Lee*
Dept. of Information and Telecommunication Engineering, Kangwon University,
Korea Information Security Agency*
E-mail : shotstop@www.kangwon.ac.kr

Abstract

IEEE 802.11 무선랜에서 보안 문제는 무선 구간의 암호화와 인증 문제를 들 수 있다. 본 연구에서는 무선랜에서 핸드오프 인증으로 인해 발생하는 지연을 줄이기 위한 방안으로 WEP 키를 저장할 수 있는 캐시를 AP에 적용하는 방안에 대하여 연구하였다. 본 연구 결과에 의해 핸드오프가 빈번하게 일어나는 무선 인터넷 환경에서 각 AP에 캐시를 사용하여 초기 인증시 생성된 WEP 키를 저장하여 재사용함으로써 핸드오프 처리 지연에 대한 개선 효과가 있음을 확인할 수 있었다. 이와 같은 결과를 최근 활성화 되고 있는 무선 인터넷에 활용하면 향 후 폭발적으로 늘어날 무선 단말기의 핸드오프시 지연에 효율적으로 대응할 수 있을 것이다.

I. 서론

고도의 정보화 사회가 도래하면서 보다 효율적인 정보 전달을 위해 새로운 통신 네트워크에 대한 필요성이 대두되었다. 기존의 랜을 무선으로 확장시킨 무선랜은 시간과 공간을 초월하여 네트워크 자원을 사용가능하게 만들었으며, 무선 스테이션 사용이 대중화됨에 따라 무선랜 서비스에 대한 요구도 점차 증가하고 있다.

무선랜은 유선랜이 제공하지 못하는 이동성을 제공하는 반면에 전파라는 전송 매체를 사용함으로써 보안에 대한 취약성을 내포하고 있다. 이를 해결하기 위해 무선랜의 인증방법으로 open system, 공유키, MAC 주소 기반 인증방법이 있으나 인증방식의 신뢰성과 MAC 주소의 필터링에 대한 과도한 부담을 요구한다. 이와 같은 기존의 인증방식의 문제점을 해결하기 위해 IEEE 802.1x가 도입되었으며, 이는 동적인 키 생성을 이용하여 무선 구간의 데이터 기밀성을 해결하고, AP와 인증 서버를 분리함으로써 무선 단말기 사용자에 대한 제약 없는 글로벌 로밍 서비스를 제공하고 서비스를 요청하는 무선 스테이션의 수에 무한한 확장성을 제공할 수 있게 되었다. 그러나 무선 스테이션이 이동중에 한번 방문한 AP와 재인증이 발생하게 되고, 이 경우 처음과 동일한 인증과정으로 인하여 지연이 중복 발생하게 된다. 이러한 중복된 핸드오프 지연은 안정적인 서비스를 받는데 불필요한 요소가 되므로 핸드오프 지연과 오버헤드를 줄이는 방법에 대한 연구는 필수적이다.

본 논문에서는 무선 스테이션의 이동 패턴의 유사성을 추출하고, AP에 캐쉬를 적용하여 WEP key를 재사용함으로써 핸드오프 지연을 줄이는 방안을 연구하였다..

2장에서는 IEEE 802.11 무선랜의 인증 방법에 대해서 살펴보고, 3장에서는 AP에 캐시를 적용하여 WEP

이 논문은 2003년도 강원대학교 두뇌한국21 사업에 의하여 지원되었슴.

key를 재사용하는 구조를 제안한다. 4장에서는 제안한 캐시를 적용한 인증 방법과 기존의 인증 방법과의 성능을 비교 평가하고 5장에서는 본 논문의 결론을 맺는다.

II. 배경지식

IEEE 802.11 무선랜은 무선매체의 통신 범위를 나타내는 기본 서비스 영역(BSA: Basic Service Area), 서비스 영역을 확대하기 위하여 한 개 이상의 BSA를 연결한 확장 서비스 영역(ESA: Extended Service Area) 그리고 무선 매체와 유선 네트워크를 연결시키며 핸드오프, 서비스 제어, 동기화 등의 기능을 제공하는 액세스 포인트(AP: Access Point)로 구성된다.

현재 무선랜에서의 인증 방식은 크게 다음과 같이 4가지로 나눌 수 있다.

2.1 SSID(Service Set ID) 인증 방법

무선랜에서 사용하는 인증 방법 중 가장 간단한 방법으로 SSID를 이용하여 무선 스테이션을 인증한다.

무선 스테이션이 무선 네트워크에 접속 하고자 할 경우에는 무선 스테이션이 SSID가 포함된 probe request를 전송하면 SSID가 일치하는 무선 네트워크에서 무선 스테이션에게 response를 보내고 접속을 허용하게 된다. 그러나 이 방법은 사용자에 대한 인증이라기 보다는 무선 스테이션이 무선 네트워크를 선택하는 방법으로 여겨지고 있다. 이 방법은 무선 스테이션이 암호화하지 않은 SSID를 브로드캐스트로 전송하기 때문에 SSID가 다른 사용자들에게 노출되기 쉽다.

2.2 오픈시스템(Open System) 인증 방법

무선 스테이션에 설치된 무선랜 카드의 48비트 MAC 주소를 이용하여 특정 MAC 주소를 가진 무선 스테이션의 접속만을 허용하는 방법이다. 무선 스테이션이 MAC 주소가 포함되어 있는 authentication request를 AP로 전송하게 되면 AP는 자신이 저장하고 있는 MAC 리스트를 검색하여 리스트에 있는 무선 스테이션에게만 네트워크 접속을 허용한다. 그러나 무선 스테이션이 암호화되지 않은 MAC 주소 전송하므로 다른 사용자가 MAC 주소를 재 사용할 수 있으며, AP에는 한정된 숫자의 MAC 리스트만을 저장할 수 있으므로 사용자가 증가하게되면 허가된 사용자도 무선 네트워크를 사용할 수 없는 문제가 발생하게 된다.

2.3 공유키(Shared Key) 인증 방법

AP와 무선 스테이션의 무선랜 카드가 공통적으로 가지고 있는 WEP(Wired Equivalent Privacy)키를 이용하여 데이터를 암호화하고 사용자를 인증하는 방법이다.

무선 스테이션으로부터 authentication request가 오면 AP는 텍스트와 사용할 WEP 키를 지정한 authentication challenge를 전송한다. 무선 스테이션은 지정된 WEP 키를 이용하여 전송 받은 텍스트를 암호화하여 AP에 재전송 한다. AP는 암호화되어 재전송된 텍스트를 WEP 키로 복호한 후 원문과 비교하여 인증을 허가하게 된다. 그러나 공유키 인증 방법도 암호화에 사용되는 WEP 키의 수가 고정되어 있으며, 무선랜 카드와 AP가 공유된 키 테이블을 가지고 있어야 하는 단점이 있다. 또한 WEP 키 자체도 초기화 벡터 값이 작기 때문에 공격자가 스니핑을 통해 평문의 텍스트와 암호화된 텍스트, 초기화 벡터값을 획득한 후 WEP 알고리즘을 사용하면 pseudo-random stream에 대한 유추가 가능하여 WEP 키를 추정할 수 있게 된다.

2.4 EAP(Extensible Authentication Protocol) 인증 방법

IEEE 802.1X에서 표준으로 정의된 EAP를 이용하는 방법으로 무선 스테이션과 AP 사이에 세션을 형성하여 세션기반 인증을 실시하게 된다.

EAP를 이용한 인증 모델은 무선 네트워크 서비스를 제공받으려는 supplicant와 서비스 요청자에 대한 인증 절차를 수행하는 authenticator, 그리고 인증을 수행하는authentication server로 구성된다.

무선랜 환경에서는 무선 스테이션이 supplicant가 되고 AP가 인증을 실제 수행하는 authenticator 역할을 맡게 되며, RADIUS(Remote Authentication Dial-In User Service)서버가 authentication server의 임무를 맡게 된다.

EAP에서는 포트 기반의 접근제어를 사용하는데 이를 위하여 uncontrolled port와 controlled port가 사용된다. uncontrolled port는 무선 스테이션이 RADIUS와 같이 인증에 필요한 인증 관련 자원만을 사용할 수 있는 포트로써, 인증이 성공적으로 이루어지면 controlled port를 이용하여 네트워크 자원을 자유롭게 사용할 수 있게 된다.

III. 제안구조

본 논문에서는 AP에 캐시를 적용하여 초기 인증시 생성된 WEP key를 저장하여 재사용함으로써 한번 인증과정을 거친 AP로의 핸드오프시 기본적인 인증절차를 거치는 것이 아니라 간단한 접속요청 메시지를 전송하여 인증에 소요되는 시간을 줄임으로써 끊김없는 데이터의 전송을 위한 절차를 제안하였다.

3.1 초기 로그인시 인증 방법

무선 스테이션이 AP에 로그인을 할 경우 기본적인 인증 절차에 의해서 인증을 하게 되고, 인증 후에 생성한 WEP key를 AP의 캐시에 저장을 하는 방법이다.

그림 1과 같이 무선 스테이션이 AP1에 로그인 할 경우, AP1에서 인증과정이 일어나고, 이때 생성된

WEP key를 캐시에 저장하여둔다. 이 후 무선 스테이션이 AP1을 다시 접속할 경우, 이때 저장한 WEP key를 사용하여 인증절차를 줄이게 된다. 물론 WEP key를 이용하여 안정된 데이터 전송을 하게 된다.

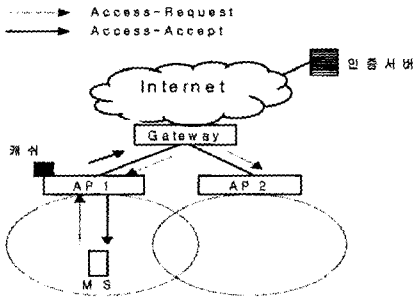

그림 1. 초기 인증 과정

제안된 초기 인증 방법은 다음과 같은 과정을 거친다.

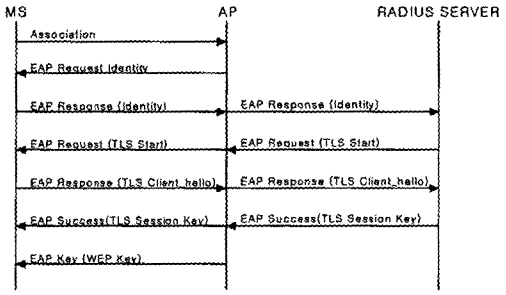

그림 2. 기본적인 초기인증 절차

그림2는 무선 스테이션과 AP 그리고 RADIUS 인증서버와의 인증절차이다. 우선 association이 이루어지고 난 다음 AP에서는 EAP request/identity 메시지를 보내게 되고 무선 스테이션은 EAP response/identity로 답하며, 이는 RADIUS 서버로 전달된다. RADIUS 서버는 적절한 인증유형의 EAP request로 무선 스테이션에 전달되고 무선 스테이션은 EAP response를 RADIRS 서버에 보내어 인증을 하게 된다. 인증과정이 성공적으로 끝나면 WEP key를 무선스테이션에 보내게 되고 WEP key는 세션키로 사용되어 암호화 기능으로 사용되게 된다. 이후 생성된 WEP key를 이용하여 데이터 전송을 하게 된다.

3.2 핸드오프시 인증 방법

무선 스테이션이 이동중에 기존의 BSA를 벗어날 경우에는 다른 BSA의 서비스를 받아야 한다. 이때 무선 스테이션은 새로운 AP와 인증 과정을 거쳐야 한다. 그림 3과 같이 핸드오프 과정 중 인증을 할 경우에는 무선 스테이션이 재접속 요청과 자신의 ID값을 전송하면 AP에서는 먼저 캐시에 요청된 스테이션의 ID로 생성된 WEP key가 있는지 확인을 한다. key가 있다면 성공 메시지를 보내어 최소한의 지연으로 데이터 전송이 가능하지만, 없다면 full authentication 과정을 거쳐야 한다.

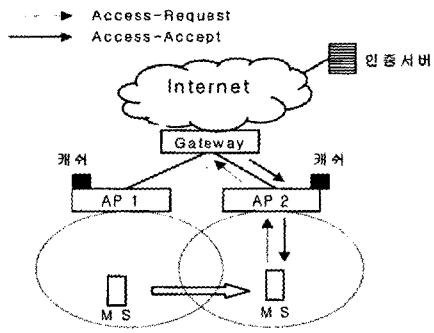

그림 3. 핸드오프시 인증 과정

무선 스테이션은 서비스를 제공하는 AP의 SNR(Signal to Noise Ratio)을 주기적으로 모니터링하다가 SNR 값이 기준치 이하로 떨어지면 새로운 AP를 찾기 위하여 scanning을 시작하여 가장 큰 SNR을 갖는 AP를 선택한다. 이때 무선 스테이션은 새로운 AP에 대한 인증이 끝나기 전까지 이전 AP와 세션을 계속 유지해야한다.

제안된 핸드오프 과정 중 캐시에 WEP key가 존재할 경우 인증 방법은 다음과 같은 과정을 거친다. 그림4와 같이 우선 reassociation이 이루어지고 난 다음 무선 스테이션은 AP로 EAP request/identity를 보내고, AP는 무선 스테이션의 ID값으로 cache에 WEP key가 있는지 확인한 후, key가 존재하면 EAP success 메시지를 보내게 된다. 이후 저장된 WEP key를 이용하여 데이터를 전송하게 된다.

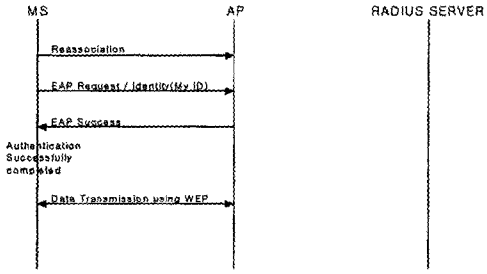

그림 4. 핸드오프 과정 중 인증절차

AP의 캐시가 전부 찼을 경우에는 캐시교체알고리즘인 FIFO(First In First Out), LIFO(Last In First Out) 그리고 현재 주로 사용되는 LRU(Least Recently Used) 방식을 사용하여 WEP Key를 교체하는 방식을 연구하였다.

Ⅳ. 성능분석

본 논문에서는 시뮬레이션 프로그램(SMPL)을 이용하여 핸드오프시 기존의 인증 방법과 제안한 캐시를 이용한 인증 방법의 성능을 평가하였다.

4.1 시뮬레이션 모델

시뮬레이션 환경은 AP의 위치를 그림5와 같이 배치하였으며, AP의 개수는 N * N 개를 적용하였다.

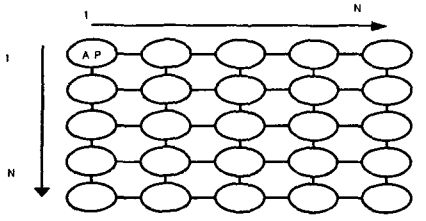

그림 5. 시뮬레이션 환경 (AP의 위치)

항목	값
AP의 갯수	N * N
WEP Key가 없을때의 인증시간	24ms
WEP Key가 존재할때의 인증시간	6ms
캐시 크기	0 ~ 100
총 핸드오프 횟수	1000000번
무선스테이션의 수	100대

표 1. 시뮬레이션 환경 파라미터

full autnentication의 인증지연시간은 유선구간의 ping을 이용한 round trip 값과 무선구간의 round trip 값을 이용하여 계산하였다. 캐시에 key가 존재할 경우 인증지연시간은 AP까지의 무선구간의 round trip값을 이용하여 계산하였다. 캐시 크기는 0부터 무선스테이션의 개수인 100까지로 설정하였다. 100으로 설정한 이유는 각 AP에서 모든 무선 스테이션의 WEP key를 가질 수 있는 수이기 때문이다. 또한 핸드오프 횟수, 즉 시뮬레이션 횟수는 1,000,000번으로 설정을 하였으며, 처음 cold start 값을 제거하기 위하여 처음 10,000번의 값은 무시하였다. 무선 스테이션은 100대를 임의적으로 AP에 위치시켰다. 이후 초기인증과정 후 핸드오프시에 일어나는 변화에 대해 성능을 평가하였다.

4.2 성능평가

제안한 방법의 성능 평가를 위해서 AP에서의 캐시 사이즈에 따른 무선 스테이션의 평균 handoff latency를 살펴보았다.

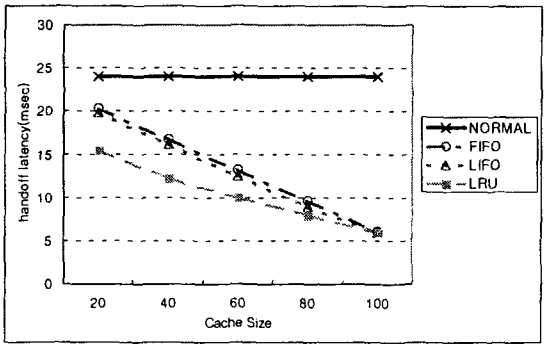

그림 6. cache size의 변화에 따른 handoff latency의 변화

그림6는 cache size를 변화시키면서 그에 따른 handoff latency의 변화를 측정하였다. cache를 적용하지 않은 경우(cache size가 0인 경우)에는 무선 스테이션의 평균 handoff latency가 기존 normal한 방법과 성능이 동일하지만, cache size가 점점 커짐에 따라 cache를 이용하여 제안한 방법이 보다 효율적으로 핸드오프 지연을 줄이고 있다는 것을 확인 할 수 있다. 또한 캐시 교체 알고리즘을 가장 간단한 FIFO 방식과 현재 주로 사용되고 있는 LRU방식을 비교한 결과, FIFO 방식보다는 LRU 으로 WEP key를 교체하여, 보다 핸드오프 지연시간을 줄이게 되어 성능이 월등히 좋아진 것으로 나타났다.

V. 결론

본 논문에서는 IEEE 802.11 무선랜에서 AP에 캐시를 적용시키는 방법을 제안하고 그 성능을 시뮬레이션을 통해서 기존의 방법과 비교 평가하였다. 성능 평가 결과 cache를 사용함으로 인해서 handoff latency가 일반적인 방법보다 현격히 줄어들었으며, 그 중에서도 현재 주로 사용되는 LRU 캐시 교체 알고리즘이 가장 좋은 성능을 나타낸 것을 알 수 있었다. 이와 같이 제안된 기법을 이용하게 되면 hot spot 지역에서 핸드오프시에 일어나는 오버헤드를 줄일 수 있으며, 무선랜 사용자에게 보안적인 측면과 QoS 측면 모두를 만족시킬 수 있을 것이다.

참고 문헌

[1] IEEE, "Wireless LAN Media Access Control(MAC) and Physical Layer Specification," IEEE, 1999

[2] IEEE, "Standard for Port Based Network Access Control," IEEE, 2001

[3] VeriSign, "Secure Global Roaming for 802.11 WLANs," VeriSign, 2002

[4] Jesse Walker, "Authenticated Key Exchange," IEEE, 2001

[5]Tim More, Bernard Aboba, "Authenticated Fast Handoff," IEEE, 2001

[6]Sangheon Pack and Yanghee Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model," IFIP TC6 Personal Wireless Communications 2002, Singapore, pp.175-182, October 2002.

[7]Bernard Aboba, Ashwin Palekar, "IEEE802.1X and RADIUS Security," IEEE, 2001