무선랜 환경에서 안전한 핸드오프를 위한 메커니즘 개선에 관한 연구

준회원 조 지 훈*, 정회원 전 준 현**

A Study on Improvement of Mechanism for Secure Handoff in Wireless Networks

Ji Hoon Cho* *Associate member*, Joon Hyeon Jeon** *Regular Member*

요 약

무선랜은 특성상 단말의 이동이 빈번하게 발생하며, 핸드오프(Handoff)시마다 반복되는 인증으로 많은 오버헤드를 야기 시킨다. 따라서 본 논문에서는 안전하고 신속한 핸드오프를 위해 IEEE 802.11f의 IAPP(Inter Access Point Protocol)를 사용하며, 제안된 Context Block과 IEEE 802.11i의 4-way handshake만을 이용하여 핸드오프시에 RADIUS 서버와의 통신을 요구 하지 않음으로써 효율성을 높였다. 또한 발생할 수 있는 Replay attack과 DoS 공격 등의 문제를 사전에 차단하기 위해 Context Block에 인증필드를 추가함으로써 보안상 취약점을 개선하였다.

Key Words : Handoff, IAPP, IEEE 802.11i, Wireless

ABSTRACT

One of major characteristics in wireless LAN is terminal's frequent mobility, so it makes many overheads in the process of authentications repeatedly at each handoffs. So I propose IAPP(Inter Access Point Protocol) of IEEE 802.11f, modified context block and 4 way handshake of IEEE 802.11i, in order to implement secure and rapid handoff. The context block, I proposed, doesn't makes any communication with RADIUS server at handoff period. Therefore, it guarantee higher efficiency than existing handoff mechanisms. Also it can improve security vulnerability by padding authentication field in the context block for providing in advance against Replay and DoS(Denial of Service) attacks.

Ⅰ. 서 론

인터넷 사용자의 증가와 무선통신 기술의 발전으로 무선랜의 수요가 급증하였다. 무선랜은 이동성이 많이 요구되는 특수한 사업장이나 레이아웃이 자주 교체되는 백화점 등을 중심으로 기업에 도입되기 시작하여 이제는 일반적인 사무 환경에서도 그 중요도가 점차 확대 되고 있다. IEEE 802.11기반 무선랜의 표준화 초기에 보안을 위해 설계 되었던 WEP(Wired Equivalent Privacy) 알고리즘의 취약성이 알려지면서[1] 무선랜 MAC 계층 보안 기능 향상을 위한 표준화를 진행하기 위해 IEEE 802.11 TGi가 결성되었고, 2004년 6월에 IEEE 802.11i 표준이 완료되어, 현재 무선랜 시장은 빠른 성장을 보이고 있다. 그러나 IEEE 802.11i에서는 무선랜 사용자의 신속한 이동성, 특히 보안성 강도를 유지하면서 무선단말이 액세스포인트(AP, Access Point)를 옮겨 다니는 이동성 보장에 대해서는 해결책을 제시하지 못하였다.[2] 무선랜은 그 특성상 사용자 이동이 빈번하게 발생하며, 핸드오프(Handoff) 시마다

* 동국대학교 영상정보통신대학원 네트워크관리학과 (hoon@dgu.edu)
** 동국대학교 정보통신공학과 조교수 (memory@dgu.edu)
논문번호 : KIC2005-08-318, 접수일자 : 2005년 8월 2일

완전인증(Full authentication)을 수행하기 때문에 많은 오버헤드를 야기시킨다.[3] 따라서 핸드오프시 유연한(seamless) 서비스를 제공하기 위해서는 핸드오프 지연시간을 최소화 할 수 있는 안전하면서도 빠른 인증 메커니즘이 필요하다.

무선랜에서의 핸드오프는 동일 네트워크 내에서 이루어지는 데이터 링크 계층의 핸드오프(Layer2 Handoff)와 서로 다른 네트워크로의 이동을 의미하는 네트워크 계층의 핸드오프(Layer3 Handoff)로 구분할 수 있다. 2계층 핸드오프는 무선단말(MS, Mobile Station)이 자신이 속한 기본 서비스 셋(BSS, Basic Service Set)에서 다른 셀로 이동할 때, 기존 액세스 포인트(AP, Access Point)와의 연결을 끊고 새로운 액세스 포인트와 재결합 하는 물리적인 이동을 의미한다. 이에 비해 3계층에서의 핸드오프는 대부분 Moblie IP를 이용하게 되며, 2계층 핸드오프 이후 외부 네트워크에서 부여 받은 가상주소(CoA, Care-of-Address)를 등록하는 등의 절차를 포함한다. 이들 핸드오프 과정은 사용자가 한 지역에서 다른 무선 지역으로 이동할 때 세션의 단절을 예방하여 계속적인 서비스를 받도록 지원한다. 여기서 3계층 핸드오프는 2계층 핸드오프가 선행된 후에 네트워크 변동이 있을 경우 진행되는 과정으로, 3계층 핸드오프의 성능을 말함에 있어서 2계층 핸드오프의 정확한 분석이 반드시 요구된다.[4]

이에 따라 본 논문에서는 2계층에서의 빠르고 안전한 핸드오프를 위한 방법으로 IEEE802.11f 표준에 정의된 IAPP(Inter Access Point Protocol)의 Context Block과 IEEE 802.11i 표준의 4-way handshake만을 이용하여 핸드오프시에 RADIUS(Remote Authentication Dial-in User Service, RFC 2865) 서버와의 통신을 요구하지 않음으로써 효율성을 높이고, 추가적인 인증필드로 보안향상 방법을 제안하였다.

2장에서는 관련연구로 IEEE 802.11i 표준과 IEEE 802.11f의 IAPP 프로토콜과 기존 핸드오프 방법에 대해 살펴보고 3장에서 IAPP를 이용한 핸드오프시 보안 향상을 위한 구조를 제안한다. 4장에서는 제안구조를 사용한 핸드오프의 성능을 분석하고 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

2.1 IEEE 802.11i[6]

IEEE 802.11i 표준은 사용자 인증과 키 교환의 큰 틀로써 IEEE 802.1x를 사용한다고 규정하고 있

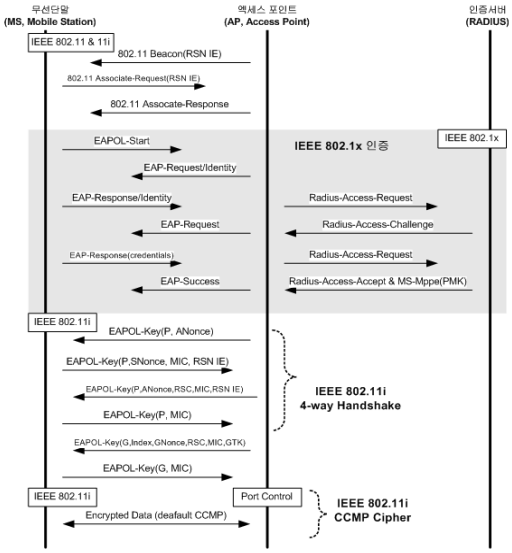

그림 1. IEEE 802.11i의 보안 접속 흐름도

으며, 나아가 구체적인 키 교환 방식인 4-단계 핸드쉐이크(4-way handshake)방식, 그리고 새로운 무선 구간 암호 알고리즘(cipher shites)의 정의를 포함하고 있다. 그림 1은 IEEE 802.1x 표준과 IEEE 802.11i 표준이 적용되는 무선랜 보안 접속 흐름도이다. 이처럼 무선단말이 인증과 키 교환을 완료해서 액세스 포인트를 통한 외부 네트워크 연결이 허가되기 위해서는 IEEE 802.11접속, IEEE 802.1x인증, IEEE 802.11i 키 교환, 무선 구간 데이터 암호화가 유기적으로 연결되어야 한다.

2.1.1 IEEE 802.11i의 인증

IEEE 802.11i에서는 IEEE 802.1x를 통해 사용자 인증을 수행하며, 무선 구간 보안에 필요한 마스터 키(PMK, Pairwise Master Key)를 전달한다. 그림 1에서 MS-MPPE(PMK)부분이 인증 서버가 액세스 포인트에게 마스터 키(PMK)를 전달하는 절차이며, 이 마스터 키를 이용하여 일대일 대칭키(PTK, Pairwise Transient Key)교환을 하게 되고 그 결과에 따라 포트제어(Port Control)를 수행한다.

그리고 IEEE 802.11i 표준의 중요한 특징으로 사전인증(Pre-Authentication)방식이 있는데, 이는 인접 액세스포인트들에게 미리 마스터 키(PMK)를 캐쉬(cache)해놓음으로써 무선 단말의 핸드오프시 빠른 인증을 제공한다. 하지만 이 사전인증 방식은 RADIUS서버에 많은 로드를 발생시키고, 사전인증이 실패 했을 경우 또 다시 모든 인증(Authentication with Full IEEE 802.1x) 절차를 거쳐야 하는

문제가 있다.

2.1.2 IEEE 802.11i의 키 교환

IEEE 802.11i 표준은 키를 사용하는 대상에 따라 크게 2가지 세션 키가 존재할 수 있으며, 이를 위한 각각의 키 교환 방식으로 세분화 할 수 있다.

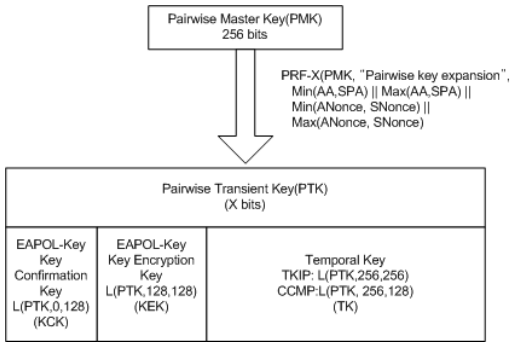

그림 2. Pairwise key hierarchy

첫 번째는 하나의 무선 단말과 액세스 포인트 사이의 일대일 통신 보호용 대칭키(PTK, Pairwise Transient Key) 교환을 위한 4-단계 핸드쉐이크(4-way handshake)방식이고, 두 번째는 액세스 포인트가 다수의 무선 단말과 일대다 통신을 할 때 사용하는 그룹키(GTK, Group Transient Key)교환을 위한 그룹키 핸드쉐이크(Group Key Handshake)방식이다.

그림 3은 IEEE 802.11i 표준에서의 4-단계 핸드쉐이크(4-way handshake)키 교환 절차로 동적키 생성을 위한 이 절차는 EAPOL-Key 서술자를 이용하여 진행되고 마스터 키(PMK)의 인증 및 생성이 성공한 후에 시작된다. 이는 마스터 키(PMK)가 여전히 네트워크상에서 유효하게 사용될 수 있는지 확인하고, 통신하는 무선단말의 MAC 주소와 마스터 키(PMK)의 연결성을 보장하며, 스테이션 간 채널을 확보하는데 사용될 하위 계층 암호 키 사용을 동기화 함으로써 IEEE 802.1x 인증절차를 완료한다.

그룹키 핸드쉐이크(Group Key Handshake)는 그림 3과 같이 4-단계 핸드쉐이크(4-way handshake)가 완료된 다음 두 번의 키 교환절차를 거친다. 액세스포인트에서 일대다 그룹키(GTK, Group Transient Key)를 생성하여 암호화 한 후 EAPOL-Key 서술자를 이용하여 무선단말에 전송하면 단말은 EAPOL-Key 암호화 키 정보를 이용하여 복원해 낸다.

2.2 IAPP(Inter Access Point Protocol)

동일 서브네트워크에서 서로 다른 액세스포인트

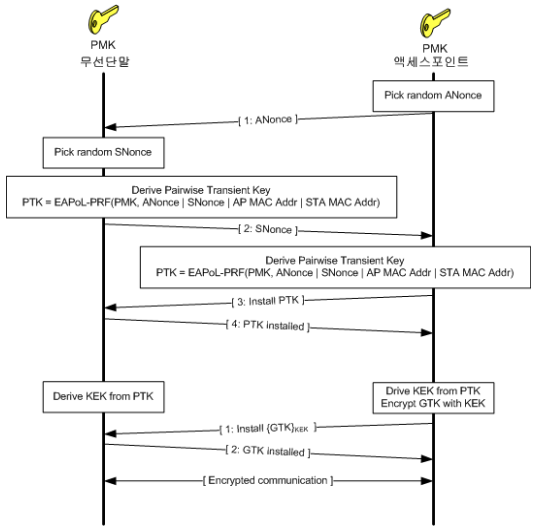

그림 3. 4-단계 핸드쉐이크(4-way handshake)[1)]

간 이동성을 보장하기 위한 프로토콜인 IAPP(Inter Access Point Protocol)는 액세스포인트간 2계층 포워딩(Layer2 forwarding) 정보 및 액세스포인트의 보안 컨텍스트(Security Context) 정보를 공유함으로써 단말의 신속한 이동을 지원할 수 있는 프로토콜로 IEEE 802.11f 표준문서에 정의 되어 있다. IAPP는 이동 무선단말, 둘 이상의 액세스포인트, 분산시스템(DS, Distribution System), RADIUS 서버로 구성된 환경에서 동작한다.

2.2.1 IAPP의 구조

IEEE 802.11f표준의 IAPP에서는 무선단말과 새로운 액세스포인트 사이에 사용할 정보를 이전 액세스포인트로부터 획득하는 과정에서, 두 액세스포인트 사이에 ESP(IP Encapsulating Security Payload)보안 시 사용할 보안정보(Security Context)를 공유하기 위하여 RADIUS 서버로 요청하는 구조로 일반적인 분산시스템(DS)에서 액세스포인트들 간의 서비스 프리미티브, 기능들과 프로토콜들을 기술하고 있다. 액세스포인트 간의 IAPP 패킷을 전달하는데 신뢰성을 위해 TCP를 사용하고 있으며 망에 있는 브릿지나 스위치 같은 2계층 장치들은 IAPP에

1) ANonce: Random number of AP
EAPoL: EAP encapsulation over LAN
EAPoL-PRF: EAPoL Pseudo-Random Function
GTK: Group Transient Key, KEK: Key Encryption Key
MAC: Medium Access Control,
PMK: Pairwise Transient Key, PTK: Pairwise Master Key
SNonce: Random number of Station

의해서 자신의 2계층 포워딩 테이블을 수정하게 된다.

IAPP 서비스 프리미티브 중 일부는 IAPP의 올바른 동작과 보안 기능을 도와주는 RADIUS 프로토콜에 의해서 이루어진다. 그 예로, IAPP 개체는 확장 서비스 셋(ESS, Extended Service Set)의 한 부분으로 등록하는 경우, 다른 액세스 포인트들의 기본서비스셋ID(BSSID, Basic Service Set IDentification)가 주어졌을 때 그 액세스포인트의 IP주소를 찾는 것이 가능하게 할 경우 그리고 IAPP 패킷을 보호하기 위한 보안 정보를 획득할 수 있도록 하기 위해서 RADIUS 프로토콜을 사용하게 된다. 때문에 각각의 액세스 포인트가 RADIUS 서버를 찾고 사용하는 것이 가능해야 한다. 또한 IAPP는 라우팅 프로토콜이 아니기 때문에 802.11 데이터 프레임을 무선단말로 어떻게 전달할 것인가에 대해서는 정의하지 않고 있다. 그리고 데이터 프레임의 전송을 위해서 분산시스템(DS)에 있는 기본 네트워크 기능들을 사용한다. 분산시스템의 데이터 전송 서비스는 무선단말들이 연결(Associate) 되거나 재연결(Reassociate) 되었을 때 그것의 네트워크 계층의 주소를 올바로 유지했을 때 동작 할 수 있다. 때문에 무선단말은 네트워크 계층 주소가 설정되지 않았다면 트래픽이 무선단말에 전달되기 전에 결합된 기본 서비스 셋(BSS)으로 트래픽을 전달하기 위한 주소를 획득해야 한다.

2.2.2 IAPP의 동작

IAPP는 그 액세스포인트에서 다양한 로컬 이벤트가 발생 할 때, 한 액세스포인트의 관리항목(management entity)이 다른 액세스포인트들과 통신함으로써 사용되는 통신 프로토콜로 액세스포인트간 2계층 포워딩 정보와 콘텍스트정보를 공유함으로써 무선단말의 빠른 이동성을 제공하게 된다. 그림 4는 재연결(Reassociation) 시의 IAPP 메시지 교환을 나타낸다.

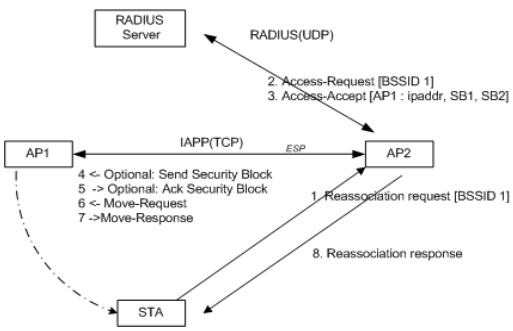

그림 4. 재연결(Reassociation) 시의 IAPP 메시지 교환

이러한 IAPP의 동작은 'IAPP-ADD.request'와 'IAPP-MOVE.request', 그리고 'IAPP-CACHE-NOTIFY. request'에 의해 시작된다.

2.2.2.1 IAPP-ADD.request에 의해 시작되는 동작

IAPP가 'IAPP-ADD.request'를 받았을 때 그것은 'ADD-notify'패킷과 Layer2 Update frame을 보내야만 한다. 'ADD-notify' 패킷은 IAPP IP 멀티캐스트 주소인 224.0.1.178로 전송 된다.(RFC 1112: 1989) 이때 액세스포인트의 MAC과 IP를 가진다. 이 메시지는 무선단말에 의해서 보내진 Association request에 있던 Sequence Number보다 테이블에 있는 값이 오래된 것이라고 판단되면 그 정보를 삭제한다. 'ADD-notify' 패킷의 목적은 오래된 연결(association)을 제거하는 것이며 association 테이블의 갱신은 2계층 업데이트 프레임(Layer2 Update frame)에 의해서 수행된다. 이 프레임은 결합된 무선단말의 MAC주소를 사용하여 보내지고 브리지, 스위치 그리고 액세스포인트들과 같은 2계층 장치들의 포워딩 테이블을 갱신한다.

2.2.2.2 IAPP-MOVE.request에 의해 시작되는 동작

IAPP 개체가 'IAPP-MOVE.request'개체를 받았을 때 그것은 'MOVE-Notify'패킷을 이전 액세스포인트로 보내고 그 액세스포인트로부터 'MOVE-response' 패킷을 받는다.

'MOVE-Response'는 무선단말의 연결(association)을 위한 컨텍스트 블럭(Context block)을 이전 액세스포인트로부터 새로 접속할 액세스포인트로 전달한다.

'MOVE-Notify'와 'MOVE-Response'는 액세스포인트들 사이의 TCP세션으로 전달되는 IP 패킷이다. 이전 액세스포인트의 IP주소는 재연결(reassociate) 메시지의 BSSID를 매핑 함으로써 알 수 있는데 이 매핑은 RADIUS서버와의 메시지 교환을 통해 이루어진다. 이를 위해선 RADIUS 서버가 Call Check service-type을 지원해야만 한다. 만약 'MOVE-response' 패킷의 암호화가 요구된다면 RADIUS Reply는 새로운 액세스포인트에게 이전 액세스포인트의 IP주소 외에 추가적으로 이전 액세스포인트와 새로운 액세스포인트 각각에 대한 보안 블럭(Security Block)을 보내줘야 한다. 이 보안블럭들은 액세스포인트간 보안 연결을 위한 정보를 각각 포함 하고 있고, RADIUS 레지스트리에 등록된 액세스포인트의 BSSID secret으로 암호화 되어 있다.

새로운 액세스포인트는 RADIUS 서버로부터 받은 보안블럭을 보안블럭(Security-Block) 패킷에 포함시켜 이전 액세스포인트로 전송한다. 이것은 액세스포인트들 사이의 IAPP TCP연결에서 처음으로 교환되는 메시지이다. 이전 액세스포인트는 'ACK-Security-Block' 패킷을 리턴 한다. 이 시점에 두 액세스포인트는 상호간 앞으로의 정보교환에 사용될 공유키를 갖게 된다.

2.2.2.3 프로액티브 캐싱(Proactive caching)

프로액티브 캐싱(Proactive caching)은 무선단말이 이동할 액세스포인트에 미리 무선단말의 컨텍스트 정보를 캐싱(caching)해 놓음으로써 빠른 로밍을 지원하기 위한 방법이다.

'IAPP-CHCHE-NOTIFY.request'에 의해 시작되는 이 동작은 단말의 MAC주소를 이용하여 IAPP의 캐쉬(cache)에 있는 단말들의 컨텍스트 정보를 찾게 되고, 이때 캐쉬의 내용에 단말의 정보와 부합되는 컨텍스트를 찾게 되면 캐쉬의 내용을 곧바로 적용함으로써 빠른 핸드오프를 가능하게 한다. 여기서 이동할 액세스포인트는 선행된 구성없이 동적으로 이웃하는 엑세스포인트들을 학습함으로써 식별되며 액세스포인트는 네이버 그래프(Neighbor graph)를 통해 이웃하는 액세스포인트들을 효율적으로 관리하고 네이버 그래프는 재결합 과정을 진행해 나가면서 동적으로 학습된다. 또한 프로액티브 캐싱(Proactive caching)이 실패 했을 경우엔 기존 방법대로 그림 5처럼 IAPP의 키 교환 과정을 거치게 된다.

2.3 IEEE 802.11i에서의 핸드오프(Handoff)

IEEE 802.11i 환경에서 가능한 핸드오프 방법으로는 기존 IEEE 802.11 기반 무선랜에서 일반적으로 사용되던 일반적인 핸드오프 방법 외에 사전인증(Pre-Authentication)을 이용한 방법이 대표적이고 RADIUS 서버를 이용한 방법과 앞서 설명한 IEEE 802.11f의 IAPP를 이용한 방법 등이 있다.

2.3.1 사전인증(Pre-Authentication)

IEEE 802.11i 표준의 중요한 특징 중의 하나인 사전인증은 무선 단말이 현재 접속된 액세스포인트 뿐만 아니라 인접해 있는 이웃 액세스포인트에게도 인증을 요청해서 미리 다수의 액세스포인트들로부터 인증을 받아 놓는다는 것이다. 결과적으로 사전인증의 최종 단계에서 목표 액세스포인트(Target AP)는 자신이 직접 속해 있지 않은 무선 단말과 관련된 마스터 키(PMK)를 캐쉬하고, 무선 단말은 향후 핸드오프 가능성이 있는 액세스포인트에게 미리 인증을 받음과 동시에 동일한마스터 키(PMK)를 캐쉬하게 되는 것이다. 이는 무선 단말기의 움직임 패턴과 액세스포인트의 위치에 의해 결정되며 이를 결정하기 위한 사용자의 로깅정보와 핸드오프 이벤트에 대한 로깅 데이터베이스 시스템이 사용되게 된다. 이러한 사전인증은 그림 5처럼 새로운 액세스포인트를 통해 IEEE 802.1x의 모든 인증과정(Full IEEE 802.1x Authentication)을 거침으로서 RADIUS서버의 로드(load)가 증가하여 오버헤드가 발생하고 EAP-Logoff 메시지를 이용한 서비스 거부공격(DoS attack)에 취약하다.

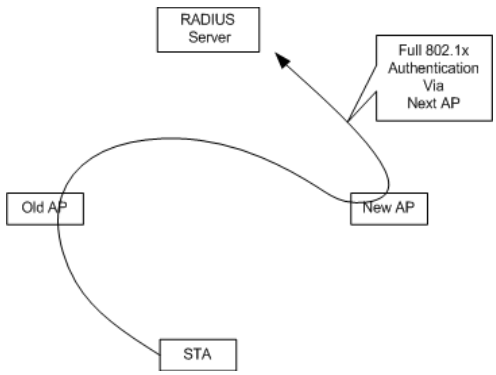

그림 5. 사전인증 (Pre-authentication)

또한 사전인증이 실패했을 경우 또 다시 IEEE 802.1x의 모든 인증과정을 거쳐야 하는 단점이 있다.[2][7][9]

2.3.2 일반적인 핸드오프

IEEE 802.11i 표준에서 사전인증이 실패하거나 사전인증을 지원하지 않을 경우 일반적인 핸드오프 방법을 사용하게 된다. 일반적인 핸드오프는 무선단말이 이동할 액세스포인트와의 재연결을 위해 기존의 액세스포인트와 연결을 끊고 그림 1과 같이 IEEE 802.1x의 초기 인증 절차부터 재인증이 요구되므로 핸드오프시 지연이 크다.

2.3.3 RADIUS 서버를 이용한 핸드오프

RADIUS 서버를 이용한 핸드오프는 핸드오프시 필요한 세션키인 마스터 키(PMK)를 RADIUS 서버가 직접 이동할 액세스포인트에 전달하는 방식이다. 이는 일반적인 핸드오프와 달리 IEEE 802.1x 인증과정을 거치지 않고 바로 4-단계 핸드쉐이크(4-way

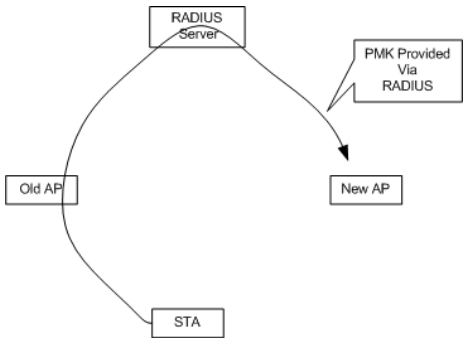

그림 6. RADIUS 서버를 이용한 핸드오프

handshake) 프로시져를 시작할 수 있어 일반적인 핸드오프에 비해 지연이 적다.

Ⅲ. 제안하는 핸드오프 메커니즘

3.1 제안방식

기존 액세스포인트에서 IEEE 802.11i의 마스터 키(PMK)가 안전한 방법으로 새로운 액세스포인트에게 보내진다면 무선단말은 IEEE 802.1x의 모든 인증(Full IEEE 802.1x)을 거치지 않고 4-단계 핸드쉐이크 프로시져를 바로 수행할 수 있다.

본 논문에서는 마스터 키(PMK)를 안전하게 새로운 액세스포인트로 보내는 방안으로 IEEE 802.11f의 IAPP의 컨텍스트 블럭(Context Block)을 이용한다.

제안하는 컨텍스트 블록 포맷(Context Block Format)은 그림 7과 같다.

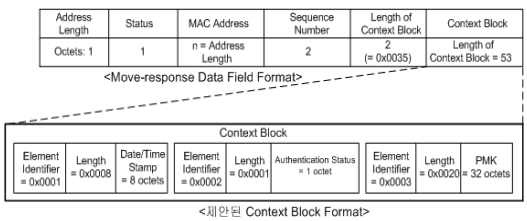

그림 7. 제안된 Context Block Format

IAPP의 컨텍스트 블럭은 Information element의 집합으로 구성 되는데, 이 Information element는 Element Identifier, Length 그리고 Information 필드로 이루어져 있다.[4]

제안하는 컨텍스트 블럭은 핸드오프시 반드시 필요한 세션키인 256비트(32octets) 크기의 마스터 키(PMK, Pairwise Master Key)와 보안향상을 위한 두 개의 인증필드로 구성된다. 자세한 구성은 표 1과 같다.

표 1. 제안된 Context Block의 Information elements

	Information element format		
	Element Identifier (2octets)	Length (2octets)	Information (n = Length)
Date/Time Stamp	0x0001	0x0008	Date/Time Stamp = 8 octets
Authentication Status	0x0002	0x0001	Authentication Status = 1 octet
PMK	0x0003	0x0020	PMK = 32 octets

여기서 Date/Time Stamp는 8옥텟의 길이를 갖고 Time Sync로 재전송 공격(Replay Attack)을 예방하는 역할을 한다.[10] 그리고 Authentication Status는 1옥텟의 길이로 4-단계 핸드쉐이크(4-way handshake)를 수행하기 전에 무선단말의 인증여부를 파악할 수 있어 액세스포인트에 대한 DoS(Denial of Service)공격과 위장 단말(Rogue Stations)을 사전에 차단할 수 있다.

3.2 제안방식의 키교환 프로시져(Key exchange procedure)

IAPP 프로토콜을 사용한 핸드오프에서 제안된 컨텍스트 블럭을 사용할 때의 키 교환 프로시져는 그림 8와 같이 진행된다.

키 교환의 순서는 먼저 새로운 액세스포인트가 단말의 'Reassociate request'로부터 핸드오프를 인지하고 기본서비스셋ID(BSSID)를 RADIUS로 전송한다. RADIUS 서버는 새로운 액세스포인트가 알려준 기본서비스셋ID(BSSID)를 이용하여 매핑된 이전 액세스포인트의 주소를 ESP를 위한 보안블럭(Security Block)과 함께 새로운 액세스포인트에게 전송한다. 새로운 액세스포인트는 이전 액세스포인

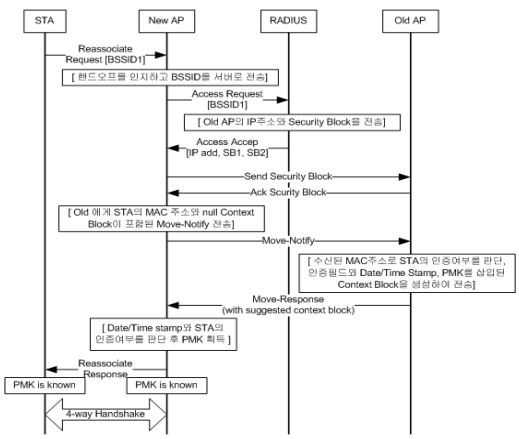

그림 8. 키 교환 프로시져

트와 ESP보안채널을 수립한 후 이전 액세스포인트에게 무선단말의 MAC 주소와 null 컨텍스트 블록 등이 포함된 'MOVE-notify'를 보낸다. 이전 액세스포인트는 무선단말의 MAC 주소가 맞는지 체크하고 새로운 액세스포인트에게 제안된 컨텍스트 블럭을 포함한 'MOVE-response' 패킷을 보낸다. 이 때 'MOVE-response' 패킷을 보낸 후, 테이블에서 마스터 키(PMK)를 지운다.

새로운 액세스포인트는 컨텍스트 블록 내의 'Date/Time stamp'를 새로운 액세스포인트의 System Time과 비교하여 새로운 액세스포인트에 지정된 값 내에 있는지 체크한다. 이것은 발생할 수 있는 재전송 공격(Replay attack)을 방지한다. 다음으로 'Authentication Status'를 이용하여 재연결을 요구하는 무선단말이 인증되었는지의 여부를 체크하고 새로운 액세스포인트는 마스터 키(PMK)를 획득하여 4-단계 핸드쉐이크 프로시져를 수행한다. 여기서 무선단말에 대한 사전인증은 액세스포인트에 대한 DoS 공격을 막고 위장 스테이션들이(Rogue Stations) 자주 나타나는 곳에 유용하다.

Ⅳ. 성능분석

4.1 성능분석

제안된 컨텍스트 블럭을 사용한 핸드오프와 RADIUS 서버를 이용한 기존의 핸드오프의 지연시간을 서로 비교하여 핸드오프 수행속도를 평가하였다.

$$\text{핸드오프 수행속도} : V = c/\Delta T_d \qquad (1)$$

그림 9와 표 2 그리고 수식(1)은 각각 핸드오프 수행과정, IEEE의 Latency Scale 그리고 핸드오프 수행속도(Maximum Velocity)이다.[5]

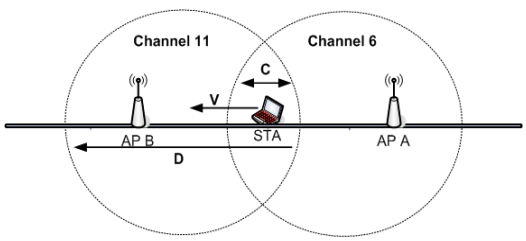

그림 9. 핸드오프 수행 시나리오[2)]

2) c: 셀의 중첩영역, v: 핸드오프 수행속도
D: 액세스포인트의 Coverage area

표 2. Latency Scale

Layer	Item	Time(ms)
L2	802.11 scan(passive)	0ms(cached), 1sec(wait for Becon)
L2	802.11 scan(active)	40~300ms
L2	802.11 assoc/reassoc (no IAPP)	2ms
L2	802.11 assoc/reassoc (with IAPP)	40ms
L2	802.1x authentication(full)	1000ms
L2	802.1x authentication (fast resume)	250ms
L2	Fast Handoff (4-way handshake only)	60ms
L3	DHCPv4	1000ms
L3	Initial RS/RA	5ms
L3	Wait for subsequent RA	1500ms
L3	DAD(full)	1000ms
L3	Optimistic DAD	0
L3	MN-HA BU	1RTT(IKE w/HA SA), 4RTT(IKE w/CoA SA)
L3	MN-CN BU	1~1.5RTT(CAM) ~2.5RTT(RR)

4.1.1 일반적인 핸드오프

IEEE802.11i 환경에서 EAP-TLS를 이용한 완전인증(Full 802.1x Authentication)을 거친 핸드오프 수행속도와 지연시간은 수식(2)와 같다.

$$\Delta T_d = \Delta T_{scan} + \Delta T_{802.1x} + \Delta T_{4way} + \Delta T_{reassoc(no\ \ IAPP)}\ ^{3)} \qquad (2)$$

예) c=2ft, △Td=1102ms, V=1.8ft/sec.

무선단말의 핸드오프 속도는 중첩된 셀 영역의 거리(c)를 전체 핸드오프 수행 지연시간으로 나눈 값이다.

수식 (2) 처럼 일반적인 핸드오프 수행속도는 무선단말이 새로운 액세스 포인트로 이동할 때마다 IEEE 802.1x의 모든 인증(Full IEEE 802.1x Authentication)을 거치기 때문에 유연한(seamless) 핸드오프를 제공하기엔 Latency가 너무 크다.

4.1.2 RADIUS 서버를 이용한 핸드오프

RADIUS 서버를 이용한 핸드오프는 마스터 키

3) V : 핸드오프 수행속도
ΔT_d : 핸드오프 지연시간
ΔT_{scan} : STA가 AP의 신호세기를 주기적으로 스캐닝 하는 시간
$\Delta T_{802.1x}$: 802.1X 인증과정을 거치는 시간
ΔT_{4way} : 4-Way 핸드쉐이크 수행시간
$\Delta T_{reassoc}$: Reassociation 시간

(PMK)를 RADIUS 서버를 통해 전송받기 때문에 IEEE 802.1x 인증과정을 거칠 필요가 없고, 대신 RADIUS 서버가 마스터 키(PMK)를 주고받는 데 걸리는 시간으로 2RTT(Round Trip Time)가 필요하다.

$$\triangle T_d = \triangle T_{scan} + 2RTT_{AAA} + \triangle T_{4way} + \triangle T_{reassoc(no\ \ IAPP)} \quad (3)$$

예) c=2ft, △Td=202ms, RTT=50ms, V=9.9ft/sec.

4.1.3 제안된 핸드오프

제안된 컨텍스트 블럭을 이용한 방법 또한 마스터 키(PMK)를 이전 액세스포인트로부터 전송받기 때문에 IEEE 802.1x 인증과정을 거칠 필요가 없고

$$\triangle T_d = \triangle T_{scan} + \triangle T_{4way} + \triangle T_{reassoc(with\ \ IAPP)} \quad (4)$$

예) c=2ft, △Td=140ms, V=14.3ft/sec.

액세스포인트간 전송되는 패킷은 ESP로 보호되기 때문에 마스터 키(PMK)의 기밀성과 무결성이 보장되는 장점이 있다.

4.2 분석결과

본 논문에서 제안된 IAPP의 컨텍스트 블럭을 이용한 핸드오프 방법은 성능분석의 결과와 같이 핸드오프시 지연시간($\triangle T_d$)이 현저히 짧기 때문에 그 수행속도가 가장 빠르다는 것을 알 수 있다.

그림 10은 각각의 핸드오프 수행속도를 비교한 것이다. 그 밖에 제안된 컨텍스트 블럭을 사용한 IAPP의 프로액티브 캐싱(Proactive cashing)을 이용할 경우 사전인증의 핸드오프와 동등한 성능을 보이면서 사전인증과 달리 새로운 액세스포인트를 통한 EAP-TLS 인증이 없기 때문에 RADIUS 서버의

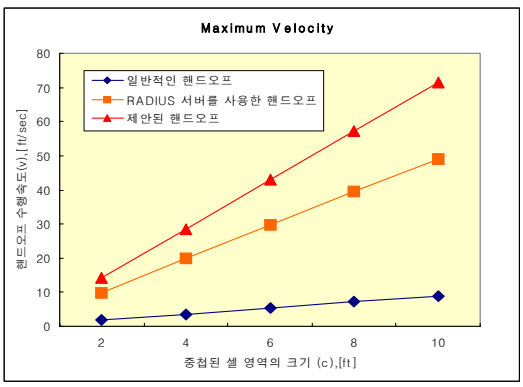

그림 10. 핸드오프 수행속도 비교

로드(load)를 경감할 수 있다는 장점이 있다. 또한 사전인증(Pre-authentication)을 지원하지 않는 디바이스 또는 사전인증이 실패했을 경우에 사전인증을 대신할 수 있다.

그리고 마스터 키(PMK)는 'MOVE-response' 패킷의 컨텍스트 블럭에 포함되어 있고 그 패킷은 항상 IAPP를 통해 새로운 액세스포인트로 ESP를 통해 보내지기 때문에 안전하다. 또 컨텍스트 블럭의 Date/Time stamp는 발생할 수 있는 재전송 공격(Reply Attack)을 방지하고, Authentication Status로 IAPP의 문제점으로 지적된 위장 단말(Rouge Station)의 출현을 사전에 차단함으로써 보안을 강화했다.

V. 결 론

무선랜의 보안 문제를 해결하기 위해 등장한 IEEE 802.11i 표준은 무선랜 시스템의 보안을 위해 다양한 기술을 통합할 있도록 하고, 새로운 키 교환 방식과 암호 알고리즘을 정의하여 무선단말의 고정 통신에 대해서는 효과적인 보안기능을 제공하지만 향후에 보다 완전한 무선랜의 보안을 위해서는 이동단말의 신속하고도 안전한 이동성을 보장하는 보다 발전된 기술이 필요하다. 이에 따라 본 논문에서는 안전하고 신속한 핸드오프 방법으로 IEEE 802.11f의 IAPP를 사용하며, 제안된 컨텍스트 블럭(Context Block)과 IEEE802.11i의 4-단계 핸드쉐이크(4-way handshake)만을 이용하여 핸드오프시 RADIUS 서버와의 통신을 요구 하지 않음으로써 효율성을 높이고 추가적인 인증필드의 사용은 보안상 취약점을 개선할 것으로 예상된다.

참 고 문 헌

[1] J.R.Walker, "Unsafe at any key size; An analysis of the WEP encapsulation", *tech. REP. 03628, IEEE 802.11 committee,* March 2000.]

[2] 강유성, "국제표준화 회의결과 요약서-주요 쟁점기술 표준화 보고서", pp. 1, November 2004.

[3] T.Moore, B.Aboba, "Authenticated Fast Handoff", IEEE 802.1-01/553, November 2001.

[4] IEEE802.11F, "IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Su-

pporting IEEE 802.11 Operation", *IEEE 802.11 committee,* IEEE Standard 802.11F, July 2003.

[5] Bernard Aboba, "Fast Handoff Issues", IEEE 802.11-03/155r0, December 2004.

[6] 강유성, 오경희, 정병호, 정교일, 정찬영, "무선랜 보안 표준 IEEE 802.11i", *TTA Journal* No 99, pp.124-129, June 2005.

[7] IEEE802.11i, "Part11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications-Amendent 6: Medium Access Control(MAC) Security Enhancements", *IEEE 802.11 committee,* IEEE Standard 802.11i, July 2004.

[8] William Arbaugh, Arunesh Mishra, Min-ho Shin, "Using Neighbor Graphs in support of fast and secure WLAN mobility", *University of Maryland College Park*, February 2004.

[9] Bernard Aboba, "IEEE 802.1X Pre-Authenticaion", IEEE 802.11-02/389r0.

[10] David L. Mills, "Network Time Protocol (Version 3) Specification, Implementation and Analysis", RFC1305, March 1992.

조 지 훈 (Ji Hoon Cho) 준회원

2003년 2월 세명대학교 컴퓨터응용수학과 졸업

2005년 8월 동국대학교 영상정보통신대학원 네트워크관리학과 석사

<관심분야> 이동 컴퓨팅, 영상통신, 유무선네트워크, 네트워크보안 등

전 준 현 (Joon Hyeon Jeon) 정회원

1984년 2월 동국대학교 전자공학과 학사

1986년 2월 한국과학기술원 전기 및 전자공학과 석사

1991년 8월 한국과학기술원 전기 및 전자공학과 박사

1991년 9월~1999년 12월 한국통신 연구소

1999년 12월~2000년 2월 한누리 살로만 투자증권

1000년 6월~2001년 2월 (주) 드림라인

2001년 9월~현재 동국대학교 정보통신공학과 교수

<관심분야> 이동컴퓨팅, 영상통신, 유무선네트워크, 네트워크보안 등