情報保護學會論文誌
第19卷 第1號, 2009. 2

중앙집중식 WLAN 환경에서의 안전하고 효율적인 로밍 메커니즘*

박 창 섭,† 우 병 덕,‡ 임 정 미

단국대학교

A Secure and Efficient Roaming Mechanism for Centralized WLAN Environment*

Chang-seop Park,† Byung-duk Woo,‡ Jeong-Mi Lim

Dankook University

요 약

최근 들어 IEEE 802.11 WLAN(Wireless Local Area Network) 서비스에 대한 수요의 증가와 함께 WLAN 환경에서 실시간 멀티미디어 서비스를 이용하려는 사용자의 관심이 날로 증가하고 있다. 그러나 IEEE 802.11i의 보안 정책은 MS(Mobile Station)의 이동이 빈번하게 발생하는 WLAN 환경에서 끊김 없는 실시간 멀티미디어 서비스를 제공하기에는 핸드오프 지연 시간이 너무 길어 이를 보완하기 위한 기법들이 제안되고 있다. 또한 IEEE 802.11i에서 제시하고 있는 세션 키 도출 과정 및 핸드오프 메커니즘에는 DoS(Denial-of Service) 공격 가능성이 내포되어 있다. 본 논문은 이러한 문제점을 해결하기 위해 중앙집중식 WLAN 환경을 기반으로 안전하고 효율적인 핸드오프 메커니즘을 소개한다. 상호인증 및 세션키 도출로 사용되는 802.11i의 4-way Handshake 과정이 2-way Reassociation 과정으로 대체된다.

ABSTRACT

Recently, there is a drastic increase in users interested in real-time multimedia services in the WLAN environment, as the demand of IEEE 802.11 WLAN-based services increases. However, the handoff delay based on 802.11i security policy is not acceptable for the seamless real-time multimedia services provided to MS frequently moving in the WLAN environment, and there is a possibility of DoS attacks against session key derivation process and handoff mechanism. In this paper, a secure and efficient handoff mechanism in the centralized WLAN environment is introduced to solve the security problems. The 4-way Handshake for both mutual authentication and session key derivation is replaced by the 2-way Reassociation process.

Keywords : IEEE 802.11i, WLAN, Fast Handover, Centralized WLAN, 4-Way Handshake

접수일(2008년 10월 6일), 수정일(2008년 12월 22일), 게재확정일(2009년 1월 23일)

* 본 논문은 2007년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음 (KRF-2007-313-D00771).

† 주저자, csp0@dankook.ac.kr

‡ 교신저자, sayttre@dankook.ac.kr

Ⅰ. 서 론

최근 WLAN(Wireless Local Area Network) 환경에서 VoIP(Voice over Internet Protocol)와 같은 실시간

멀티미디어 서비스를 이용 하려는 사용자의 관심이 날로 증가되고 있는 가운데 안전하고 신속한 핸드오프는 WLAN 서비스에 있어서 가장 중요하게 고려해야 할 부분으로 대두되고 있다. 이로 인해 빠른 핸드오프와 밀접한 관계를 가지고 있는 인증과 무선 구간 데이터 보안에 대한 문제는 WLAN 표준화 초기 단계에서부터 현재에 이르기 까지 끊임없이 연구 되고 있다. WLAN 표준화 초기에 인증과 보안을 위해 802.11b의 WEP(Wired Equivalent Privacy) 방식을 채택했으나 WEP 설계 자체에 오류가 있어 신뢰성을 완전히 잃어버렸고 이를 보완하기 위해 IEEE 802.11i는 국제 WLAN 보안표준을 제정하였다[1].

IEEE 802.11i는 새로운 형태의 보안 구조인 RSN(Robust Security Network) 보안 구조를 표준에 반영함으로써, WLAN에서의 데이터 프라이버시 기능을 더욱 강화하였다. 802.11i의 필수구현 항목으로 정의 되어 있는 802.1x 인증 방식은 포트 기반 접근 제어를 통해 WLAN 사용자 인증을 수행 할 수 있으며 무선 구간 데이터 보안에 필요한 마스터키를 전달 할 수 있다. 그러나 MS의 핸드오프 시 마다 다수의 메시지를 수반하는 802.11i의 인증 절차를 수행해야 하기 때문에 이로 인한 지연시간은 끊김 없는 실시간 멀티미디어 서비스를 제공하는데 큰 문제점으로 남아 있다. 이를 해결하기 위해 IEEE 802.11f의 IAPP(Inter Access Point Protocol), 802.11i는 Pre-Authentication 방식과 Key Caching 방식, 그리고 PKD(Proactive Key Distribution) 방식 등이 제안되고 있다. 또한, IEEE 802.11r에서는 새로운 표준안 제정을 위한 마무리 작업을 하고 있다. 이 중에서 PKD 방식은 사용자가 핸드오프를 수행하기 이전에 AS(Authentication Server)가 보안관련 파라메터를 주위 AP(Access Point)에 사전 분배하는 방식으로 핸드오프에 소요되는 지연을 단축시킬 수 있다는 측면에서 우수한 기법으로 인정받고는 있으나, 불필요한 메시지가 필요 이상으로 발생된다는 단점을 지니고 있다. 본 논문은 안전하고 신속한 핸드오프를 지원하고 불필요한 핸드오프 관련 메시지의 발생을 제어하기 위해서 WLAN 구성요소에 AC(Access Controller)를 추가한 중앙집중식 WLAN 환경을 구성하여 AS의 부담을 현저히 줄이고 Reassociation Request/Response 메시지를 이용한 세션 키 도출 메커니즘을 제안한다. Reassociation 메시지를 이용하여 세션키를 도출 할 경우 802.11i에서의 4-way Handshake 과정을 생략할 수 있고 이는 핸드오프 지연시간의 단축뿐만 아니라 4-way Handshake가 잠재적으로 안고 있는 DoS 공격의 가능성 또한 차단한다.

본 논문은 다음과 같은 구성으로 제안 하고자 하는 메커니즘을 설명한다. 2장에서는 인증 및 핸드오프에 관한 기존 연구 들을 살펴본다. 3장에서는 본 논문이 제안하고자 하는 핸드오프 메커니즘을 소개한다. 2장 및 3장에서 언급하는 핸드오프는 MS가 동일한 ESS (Extended Service Set)에 소속된 2개의 상이한 BSS(Basic Service Set)간을 로밍(Roaming)할 경우에 수행되는 2-계층에서의 핸드오프를 지칭한다. 3장을 통해 중앙집중식 WLAN 환경에서 Reactive 방식을 이용한 마스터 키 생성 메커니즘 및 Reassociation 과정에서의 제안 프로토콜을 상세히 설명한다. 4장에서는 본 논문이 제안하고 있는 로밍 메커니즘에 대한 안전성을 분석한다. 5장은 기존 연구들과 제안 메커니즘의 성능을 NS2(Network Simulator2)를 이용한 시뮬레이션 Test를 통해 비교 분석한 후 마지막으로 6장을 통해 본 논문의 결론을 맺는다.

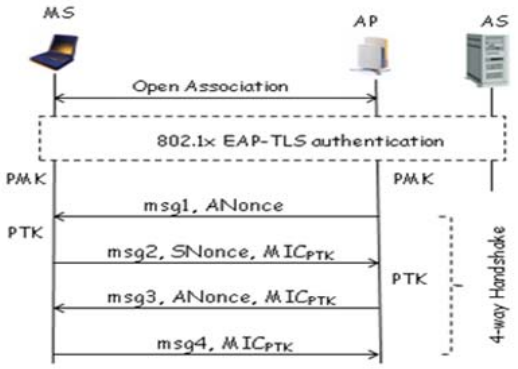
Ⅱ. 관련 연구

현재의 WLAN 망에서는 MS(Mobile Station)가 새로운 AP(Access Point)로 이동할 경우 IEEE 802.11i 보안 정책에[2] 따라 IEEE 802.1x[3] 기반의 인증 절차를 수행하고 4-way Handshake를 통해 새로운 세션 키를 도출해 낸다. [그림 1]은 MS와 AP를 경유한 AS(Authentication Server)사이의 인증 및 세션 키 생성을 보여주는 예로써 802.1x EAP-TLS Authentication 과정을 통해 MS와 AS사이의 상호인증 및 PMK(Pairwise Master Key) 도출을 진행한다. PMK 도출 후 4-way Handshake를 통해 MS와 AP사이의 데이터 전송 시 데이터 암호화에 사용할 세션 키인 PTK (Pairwise Transient Key)를 생성한다[4]. 4-way Handshake는 4개의 메시지 교환으로 구성된다. 메시지 교환은 쌍방에서 독립적으로 선정한 난수 SNonce, ANonce 그리고 MS와 AP의 MAC(Medium Access Control) 주소 MS, AP를 기반으로 세션 키 PTK = prf

(SNonce, ANonce, AP, MS)를 생성하고, 이를 기반으로 상호인증 및 키 확인(Key Confirmation)을 위한 목적이다[4]. 이때, prf ( )는 pseudo random function의 약어이다. 첫째 메시지를 제외한 나머지 메시지들에는 PTK를 이용하여 각각의 메시지에 대한 무결성을 보장하는 MIC(Message Integrity Code) 값, 즉 MIC_{PTK}가 포함된다.

MS의 핸드오프 시 마다 802.11i 보안 절차에 따라 802.1x 인증을 수행하기 때문에 이로 인한 지연시간은 끊김 없는 실시간 멀티미디어 서비스를 제공하는데 심각한 문제점으로 남는다. 이와 같은 문제를 해결하기 위해 802.11i에서는 Pre-Authentication[2] 방식을 제안하고 있으며, 802.11f[5]에서는 IAPP를 활용하여 핸드오프 시 지연시간을 줄일 수 있는 방식을 제안하고 있고, 그 외 PKD(Pro-active Key Distribution)[6] 방식과 같이 빠른 핸드오프에 관한 여러 연구들이 진행 되고 있다. 선 인증이 있을 경우 핸드오프 시 AP와 MS 사이에 교환 되는 메시지 수는 일부 감소하며 이는 핸드오프 지연 시간을 줄이게 된다. 그러나 802.11i에서 제안하고 있는 Pre-Authentication 기능이나 현재까지 연구되어 온 방식들은 선 인증 과정에서 인증 서버(Authentication Server)의 로드를 증가시키고 제약적인 범위에서만 선 인증이 가능 하다는 문제점을 남기고 있다. 또한 세션 키 생성을 위한 절차인 4-way Handshake 단계는 첫째 메시지에 대한 DoS공격이 가능하다는 문제점을 내포 하고 있다[7,8].

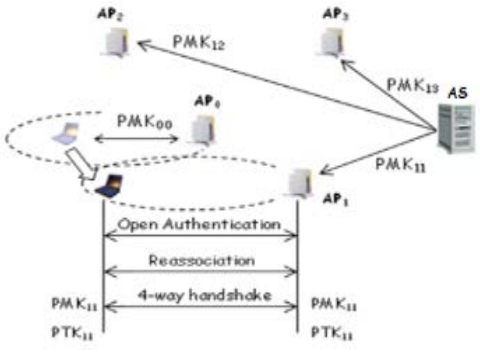
802.11i에서 제안 하고 있는 Pre-Authentication은 MS가 현재 접속된 AP를 통해 향후 핸드오프 할 AP들에 대해 사전에 인증을 시도하는 방식으로 Pre-Authentication 결과로써 생성된 PMK와 해당 MS와의 관계는 PMKID(PMK Identity)로 식별이 가능하다. 그러나 이 Pre-Authentication 방식은 인증 서버에 많은 부하를 발생시키고, 사전인증 이 실패 했을 경우 또 다시 전체 인증(Authentication with Full IEEE 802.1x) 절차를 거쳐야 하는 문제가 있다. 802.11f의 IAPP (Inter-Access Point Protocol)는 AP간 2계층 전달 정보 및 AP의 Security Context 정보를 공유함으로써 MS의 신속한 이동을 지원할 수 있는 프로토콜로 MS, 둘 이상의 AP, DS(Distribution System), 인증 서버로 구성된



[그림 1] IEEE 802.11i 인증 및 세션 키 도출 과정

환경에서 동작한다. 이처럼 서로 다른 AP간의 정보교환을 통한 방식은 단말의 Context 정보를 교환함으로써 핸드오프 시 인증에 걸리는 지연 시간을 줄일 수 있다는 장점이 있지만 AP 상호간 보안상의 독립성을 보장해 주지 못한다는 문제점을 내포 하고 있다.

선 인증과 관련된 PKD 방식은 NG(Neighbor Graph)라 불리는 향후 접속을 시도할 가능성이 있는 후보 AP들을 선정하여 MS의 인증정보를 선 분배시키는 방식으로 NG 영역 내의 AP들은 한 MS의 사전인증을 위해 분배된 키를 서로 다른 형태로 보유하고 있으므로 동일한 인증정보를 가지는 위험성을 제거하였다. [그림 2]는 NG를 이용한 PKD 방식에서 MS의 핸드오프 시 발생하는 선 인증 과정을 보여 주고 있다. MS는 WLAN 서비스를 이용하기 위해 AP_0로 최초 접속을 시도 할 때 전체802.1x EAP-TLS Authentication을 통해 PMK_{00}를 만들게 되고 이것을 이용하여 PTK_{00}를 도출 하여 WLAN 서비스를 이용하게 된다. PTK_{00} 도출 후 AS는 AP_0의 NG 정보를 이용하여 MS가 다른 AP로 핸드오



[그림 2] PKD방식의 핸드오프 과정

프 하기 전에 AP_0의 NG 내에 있는 AP들([그림 2]의 AP_1, AP_2, AP_3)에게 MS와 공유할 PMK_{ij} (i: MS의 association 순서, j: AP번호), 즉 PMK_{11}, PMK_{12}, PMK_{13}를 계산 후 전달한다. 추후 MS가 AP_0의 NG 내에 있는 AP_1의 영역으로 로밍 할 경우 이미 AS로부터 전달 받은 PMK_{11}이 있기 때문에 전체 802.1x EAP-TLS authentication 과정을 거치지 않고 바로 4-way Handshake를 통해 PTK_{11}을 도출 할 수 있다. 하지만 사용자의 인증정보를 한 홉 단위 거리의 AP들에 대해서만 분배되어 NG 영역 이외의 AP로 MS가 핸드오프를 할 경우, 또 다시 전체 802.1x EAP-TLS Authentication 과정을 진행 하게 되어 고속의 인증기능을 제공할 수 없는 단점이 있으며, 한 홉 단위 거리 안에서 AP로 MN이 핸드오프를 하게 되었을 때는 빠른 고속의 인증이 가능하지만 목적지 AP를 제외한 NG 리스트에 있던 AP들은 불필요한 키를 저장해야 하며 서버 또한 불필요한 키 계산으로 인한 부하가 발생한다는 문제점이 있다.

Ⅲ. 제안 핸드오프 메커니즘

본 논문은 중앙집중식 WLAN 환경을 기반으로 MS의 핸드오프 시 802.11i에 명시되어 있는 MS와 AP간의 상호인증 및 세션 키 분배 프로토콜을 개선하여 핸드오프 시간 단축 및 4-way Handshake에 대한 DoS 공격 가능성을 제거하는 핸드오프 메커니즘을 제안 한다.

3.1 중앙집중식 WLAN 환경

무선 네트워크 구축 시 핵심 장비인 AP는 무선 네트워크의 발전과 함께 다양한 기능을 직접 관리 할 수 있도록 별도의 OS를 운영하는 등 여러 가지 방식으로 진화 되어 왔다. 그러나 빠른 무선 인터넷과 편리한 관리라는 측면이 부각되고 있는 현 시점에서 모든 기능을 AP에만 집중 시키는 방식은 더 이상 주목 받지 못하고 있다. 대다수의 IT 담당자들은 네트워크 설계 시, 설치 후 관리를 어떻게 해야 할 지에 대해 고민하고 있고 이런 문제점을 해결하기 위해 다양한 방안이 나오고 있는데 그 중 가장 주목 받고 있는 방식은 중앙집중식 WLAN 관리이다. 중앙집중식 WLAN 관리는 무선과 유선 네트워크가 만나는 접점 장치인 스위치를 사용하여 여러 대의 AP 를 중앙에서 직접 관리 하는 방식으로 WLAN 스위치가 무선 네트워크에 대한 상태 정보 및 설정 정보를 관리함으로 관리의 편리성을 제공할 수 있으며 AP를 단순히 안테나처럼 사용함으로써 예전처럼 AP를 도난당할 경우 보안관련 설정의 노출에 대한 걱정을 할 필요가 없어진다. 본 논문에서는 이러한 중앙집중식 WLAN 환경에서 AP와 AS의 부담을 줄이고 고속의 핸드오프를 지원하는 안전하고 효율적인 로밍 메커니즘을 제안하고자 한다.

3.2 설계원리

IEEE 802.11 WLAN에서는 MS가 새로운 AP로 핸드오프 할 때 대상이 되는 AP(Target AP)로 Reassociation Request 메시지를 보내게 되고 이에 대한 응답으로 Reassociation Response 메시지를 받게 된다[9]. Reassociation 메시지에 포함된 Qparam에는 MS가 새로운 AP에게 Reassociation을 요청하는 과정에서 필요한 Capability, Listen Interval, SSID 등이 포함되고 Pparam에는 MS의 Reassociation 요청에 따른 AP의 응답과정에서 요구되는 Status Code, AID 등이 포함된다. 이들에 따른 세부적인 설명은 본 논문에서 제시하는 보안 메커니즘과 직접적인 연관이 없기에 생략한다. Reassociation 후 MS와 AP는 802.11i 보안 정책에 따라 802.1x 기반의 인증 절차를 수행하고 4-way Handshake를 통해 새로운 세션 키를 도출한다. 이로 인한 지연시간은 실시간 멀티미디어 서비스에 있어서 끊김 없는 서비스를 제공하는데 문제점으로 남고 있으며 이를 해결하기 위해 연구된 PKD 방식과 같은 선 인증 방식들은 인증서버 및 네트워크에 상당한 부담을 초래하고 있다. 또한 세션 키 도출을 위한 최종 단계인 4-way Handshake 과정은 보호되지 않는 첫 번째 메시지에 대한 DoS 공격이 가능하다는 문제점을 안고 있다. 본 논문에서 제안하고자 하는 방식은 핸드오프 시 MS와 AP사이의 PMK, PTK, Nonce 생성 알고리즘을 수정하고 Reassociation Request / Response 메시지에 새로운 필드 (Field)를 추가하여 PTK 도출에 사용함으로써 4-way Handshake의 DoS 공격 가능성을 제거하고 PKD 방식과 같이 서버와 네트워크에 부하를 증가시키는 선 인증 방식의 문제점을 해결하고자 한다.

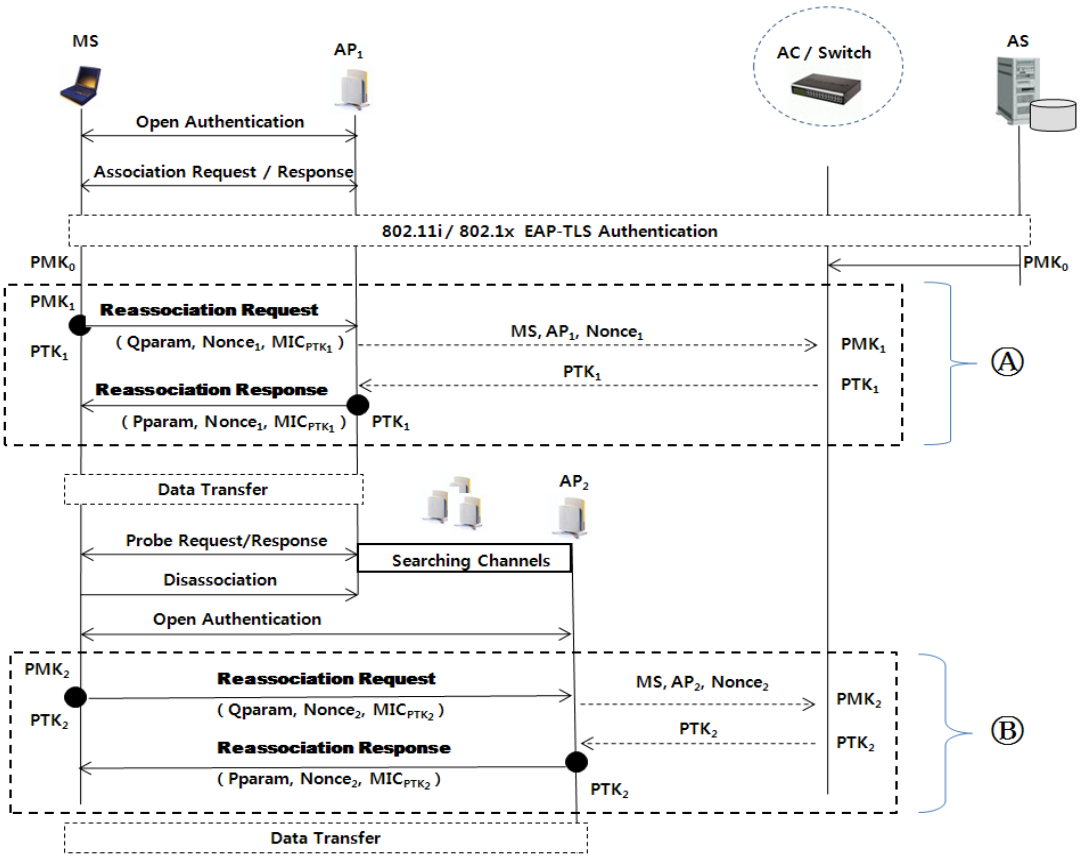
[표 1] 기호 설명

h( )	일 방향 해쉬함수 128bit MD5 암호와 알고리즘
prf( )	pseudo random function의 약어
j	시뮬레이션 환경에서의 AP 번호
PMK_j	AP번호 j번과 Reassociation 과정 중 사용하는 PMK
$Nonce_j$	AP번호 j번과 Reassociation 과정 중 사용하는 Nonce
PTK_j	AP번호 j번과 Reassociation 과정 중 사용하는 PTK
MIC_{PTK1}	AP번호 j번과 Reassociation 과정 중 사용하는 PTK1로 계산된 MIC값

3.3 제안 프로토콜

본 논문은 802.11i에서 무선 네트워크를 구성하고 있는 3개의 컴포넌트 (MS, AP, AS) 이외에 WLAN 스위치를 추가한 중앙집중식 WLAN 환경을 가정하고 Reassociation 과정을 통해서 새로운 PMK를 도출하는 알고리즘을 개선함과 동시에 Reassociation Request 및 Response 메시지에 PTK 도출을 위한 파라미터를 추가하여 PTK를 도출하는 안전하면서도 빠른 핸드오프를 지원하는 개선된 프로토콜을 제안 한다. [그림 3]은 본 논문에서 제안하는 중앙집중식 WLAN 환경의 핸드오프 과정에서 상호 인증 및 세션 키 도출 과정을 보여주고 있다. 본 논문에서 제안하고 있는 프로토콜은 MS와 AS, AP와 AC, AC와 AS사이에는 안전한 채널 (Secure Channel)이 사전에 존재한다고 가정한다.

MS는 AP_1과 최초의 Association 작업을 통해서 AS와의 802.1x Full EAP-TLS Authentication을 성공적으로 수행하고 초기 PMK 값인 PMK_0을 생성한다. AS는 AC에게 PMK_0을 안전하게 전달한다. 802.11i의 4-way Handshake 대신에 본 논문에서는 [그림 3]의 A에서와 같이 Reassociation Request / Response 메시지에 인증



[그림 3] 제안 프로토콜

및 세션 키 생성에 소요되는 파라미터를 위한 새로운 필드를 추가하는 방식을 채택한다. 여기서의 Reassociation은 새로운 AP와의 Association이 아닌 단지 인증 관련 파라미터를 전달하기 위한 목적이다. 먼저 MS는 초기 PMK_0를 기반으로 AP_1과 공유할 세션 키 PTK_1 생성을 위해 다음의 계산을 수행한다. (j=1 인 경우). 이때, h ( )는 일 방향 해쉬함수, prf ( )는 pseudo random function의 약어이다.

$PMK_j = prf\ (PMK_0,\ MS,\ AP_j)$ (식1)
$Nonce_j = h\ (PMK_j)$ (식2)
$PTK_j = prf\ (PMK_j,\ Nonce_j,\ MS,\ AP_j)$ (식3)

PMK_1은 MS가 AP_1과 공유할 PTK_1의 생성을 위해서 사용되는 값이지만, 이 값은 AP_1에게는 노출되지 않는 MS와 AC간에만 공유되는 값이다. $Nonce_1$은 MS와 AP_1사이에서 그 어느 한쪽에 의해서 일방적으로 결정될 수 없는 난수(Random Number) 이기 때문에 4-way Handshake 에서와 달리 하나의 Nonce를 사용하여 상호 인증이 가능하다. $Nonce_1$이 생성 되면 PTK_1을 최종적으로 도출 할 수 있게 된다.

• 단계 1 : Reassociation Request 전송

MS는 Reassociation Request 메시지를 작성하여 AP_1에게 전송한다. 이 메시지에는 Reassociation과 관련된 기본 파라미터(예: Current AP Address)인 Qparam, $Nonce_1$, MIC_{PTK1}가 포함된다. 이때 Reassociation Request 메시지의 기본 파라미터 중 $Nonce_1$과 MIC_{PTK1} 값을 위한 PTK_1은 (식 1), (식 2), (식 3)을 이용하여 하기와 같이 도출 된다.

$PMK_1 = prf\ (PMK_0,\ MS,\ AP_1)$ [식 1을 따름]
$Nonce_1 = h\ (PMK_1)$ [식 2를 따름]
$PTK_1 = prf\ (PMK_1,\ Nonce_1,\ MS,\ AP_1)$ [식 3을 따름]

이미 언급한 바와 같이 최초 MS와 이미 Association 작업이 완료된 AP_1간의 Reassociation은 단지 인증을 위한 목적이다. 따라서 “Current AP Address”는 AP_1의 MAC Address가 된다. 이때, MIC_{PTK1}는 Reassociation Request 메시지 내의 모든 필드를 PTK_1로 계산한 MIC 값으로 Reassociation Request 메시지에 대한 무결성을 보장한다.

• 단계 2 : AC의 PTK 생성

Reassociation Request 메시지를 전송 받은 AP_1은 PMK_1을 모르고, 따라서 PTK_1을 계산할 수 없기에 AC에게 PTK_1을 요청하게 된다. 이를 위해서 AP_1은 AC에게 MS, AP_1, $Nonce_1$을 전송한다. AC는 이를 기반으로 위의(식 1), (식 2), (식 3)을 이용해 하기와 같이 PTK_1을 계산하고 이를 AP_1에게 안전하게 전달한다.

$PMK_1 = prf\ (PMK_0,\ MS,\ AP_1)$ [식 1을 따름]
$Nonce_1 = h\ (PMK_1)$ [식 2를 따름]
$PTK_1 = prf\ (PMK_1,\ Nonce_1,\ MS,\ AP_1)$ [식 3을 따름]

MS와 공유할 PTK_1을 전달 받은 AP_1은 (단계 1)에서 전달받은Reassociation Request 메시지에 대한 무결성 검사를 수행한다. 만약, 무결성 검사가 실패하면 프로토콜은 여기서 멈추게 된다. 만약 성공할 경우에는 AP_1은 MS에 대한 인증이 성공한 것을 의미하며 또한 MS와의 키 확인 (Key Confirmation) 역시 성공적으로 수행됨을 의미한다.

• 단계 3 : Reassociation Response 전송

후속적으로 AP_1은 Reassociation Response 메시지를 작성하여 MS에게 회답하게 된다. 이 메시지에는 기본적인 파라미터(예: Association ID)인 Pparam, $Nonce_1$, MIC_{PTK1}가 포함되며, 이는 궁극적으로 이 메시지에 대한 무결성 보장을 위한 목적이다. 이를 전달받은 MS는 PTK_1을 기반으로 메시지에 대한 무결성을 점검한다. 성공적인 무결성 점검은 결국 MS 입장에서는 AP_1에 대한 인증이 성공적으로 이루어 졌으며 또한 키 확인 역시 성공적으로 수행되었음을 의미한다.

MS가 현재의 AP인 AP_1의 영역으로부터 벗어나기 시작하면 Probe Request/Response 메시지를 통해서 주변의 여러 AP들 중에서 핸드오프 할 AP를 선정하게 된

다. [그림 3]에서는 최적의 AP로 AP_2를 선정하였고, Disassocaition 메시지를 통해서 AP_1과의 Association을 종료한다. [그림 3]의 B는 MS가 AP_1과 최초 Association 후 WLAN 서비스를 이용하다 AP_2로 핸드오프 하는 과정을 보여 주고 있다. 이 과정은 [그림 3]의 A와 동일하며 PMK_2, $Nonce_2$, PTK_2의 생성을 위해서 j=2인 경우의 (식 1), (식 2), (식 3)을 사용하여 하기와 같이 PMK_2, $Nonce_2$, PTK_2를 도출해 낸다.

$PMK_2 = prf\ (PMK_0, MS, AP_2)$ [식 1을 따름]

$Nonce_2 = h\ (PMK_2)$ [식 2를 따름]

$PTK_2 = prf\ (PMK_2, Nonce_2, MS, AP_2)$ [식 3을 따름]

Ⅳ. 안전성 분석

우리는 3장을 통해 본 논문에서 제안된 프로토콜의 진행 단계 및 설계원리를 살펴보았다. 4장에서는 제안된 프로토콜의 안전성에 대해 분석하고자 한다. 분석은 크게 Nonce와 재생공격, DoS 공격에 대한 대응, PMK 캐싱(PMK Caching)에 대해 살펴보고자 한다.

4.1 Nonce와 재생공격

802.11i에 명시된 세션 키 도출 과정을 보면 PTK 도출을 위해 4-way Handshake를 진행 한다. 이때 MS와 AP는 각자의Nonce를 생성하고 이를 PTK 도출을 위한 파라미터로 사용한다. 이처럼 MS와 AP가 각기 상이한 Nonce를 생성하고 이를 4-way Handshake에 사용하는 이유는 MS와 AP간의 상호 인증 및 4-way Handshake 과정 중 메시지 재생공격을 방지하기 위함이다. 본 논문에서 제시하고 있는 PTK 생성 알고리즘은 한 개의 Nonce만 사용하고 있으나 Nonce 생성 방식을 (식 2)와 같이 구성함으로써 MS와 AP간의 상호 인증을 확립할 수 있다. 또한, PTK 도출 과정에 사용하는 Reassociation Request/Response 메시지에 MIC 값을 추가하여 Reassociation Request/Response 메시지에 대한 무결성을 보장하여 메시지 재생공격을 차단하고 있다.

4.2 DoS 공격에의 대응

802.11 WLAN 서비스에서 MS는 한 번에 하나의 AP와 연결 후 서비스를 이용할 수 있다. 그렇기 때문에 핸드오프 시 MS는 현재 서비스를 받고 있는 AP와 Disassociation 과정 후, 핸드오프의 대상이 되는 AP와 새로운 세션 키를 생성하여 WLAN 서비스를 지속적으로 이용해야 한다. 그런데 이 과정에서 발생되는 Disassociation 메시지와 세션 키 도출을 위한 4-way Handshake 단계는 모두 각기 다른 유형의 DoS 공격에 노출 되어 있다.

Deauthentication & Disassociation 메시지는 MS가 AP로 일방적으로 보내는 암호화 되지 않은 메시지로써 AP는 해당 메시지에 대한 응답을 보내지 않는다. 이처럼 Deauthentication & Disassociation 메시지는 해당 메시지 자체에 대한 인증이 결여되기 때문에 공격자가 Deauthentication & Disassociation 메시지를 위조하여 DoS 공격을 가하면 MS는 WLAN 서비스의 연결이 끊기게 되어 Authentication & Association 과정을 다시 수행해야 한다. 4-way Handshake 단계는 총 4회의 메시지 교환으로 이루어지는데 이때 첫 번째 메시지는 보호되지 않은 상태로 전송된다는 취약점을 가지고 있다([그림 1] 참조). 이러한 취약점 때문에 공격자는 임의로 다수의 첫째 메시지를 만들어 낼 수 있고 이를 이용하여 공격자는 MS와 AP간의 PTK 불일치를 유발하여 프로토콜의 정상적인 진행을 방해하는 DoS 공격을 시도할 수 있게 된다. 4-way Handshake의 첫째 메시지에 대한 DoS 공격을 방어하기 위한 몇 가지 방식이 연구되었지만 현재까지 연구된 방식들은 DoS 공격에 대한 잠재적인 문제점을 여전히 내포하고 있다.

본 논문에서 제안하고자 하는 핸드오프 메커니즘은 Reassociation Request/Response 메시지를 사용하여 PTK를 도출해 내므로 4-way Handshake 과정을 생략할 수 있다. 이는 4-way Handshake에 대한 DoS 공격을 원천적으로 차단시키는 결과를 얻을 수 있는 것이다. 또한 Reassociation Request/Response 메시지 교환 전에 이미 MS와 AP사이에 사용할 PTK가 만들어 진 상태이고 이를 이용하여 Reassociation Request/Response 메시지에 MIC 값을 첨부하여 무결성을 입증하듯이 Deauthentication & Disassociation 메시지 또한 동일한 방식으로 보호 한다면 Deauthentication & Disassociation 메시지에 대한 DoS 공격에 대해서도 방어 할 수 있다.

4.3 PMK Caching

MS의 이동으로 인한 핸드오프가 발생 할 때 MS가 이전에 방문했던 AP를 다시 방문하는 상황이 발생 할 수 있다. 이때 좀 더 빠른 핸드오프를 지원하기 위해 802.11i에서는 PMK Caching기능을 지원하고 있다 PMK Caching이란 MS와 AS 사이에 상호인증으로 생성된 PMK를 MS와 AP가 지속적으로 Cache하여 재사용함으로써 향후 MS가 이전 접속했던 경험이 있는 AP로 다시 재접속을 시도할 경우 Cache된 PMK 정보를 이용하여 인증 절차를 마무리하는 방식이다. 본 논문에서 제시하는 핸드오프 메커니즘 또한 PMK Caching 기능을 지원하며 만약 PMK의 Lifetime이 초과되어 해당 PMK가 삭제될 경우 본 논문에서 제시한 PMK 생성 알고리즘을 동일하게 적용한다. 단 MS가 이전에 방문했던 AP를 다시 방문하는 경우 PTK 도출을 위한 Nonce 생성 알고리즘은 (식 4)를 사용하여 생성한다.

$$Nonce_j = h(PMK_j, Timestamp) \quad (식4)$$

MS가 이전에 방문했던 AP를 다시 방문하는 경우에 Cache된 PMK를 사용하든지 PMK의 Lifetime이 초과되어 새로운 PMK를 생성해서 사용하든지 동일한 PMK를 사용하게 되고 이때 해당 PMK를 가지고 PTK 생성 시 사용할 Nonce를 계산한다면 일 방향 해쉬함수 특성상 동일한 Nonce가 계산된다. 이는 Key Freshness를 보장하기 위한 난수 값을 재사용하기 때문에 보안상 잠재적인 문제점을 가지게 된다. 이를 방지하기 위해 MS가 이전에 방문 했던 AP로 재방문 할 경우 비콘 프레임(Beacon Frame)의 Timestamp 필드의 값을 Nonce생성에 (식 4)와 같이 사용하여 재방문 시 Nonce 값의 재사용을 막을 수 있다.

Ⅴ. 비교(성능)분석

이번 장에서는 본 논문에서 제시한 핸드오프 메커니즘의 성능을 기존 선 인증 방식들과 비교 분석한다. 성능의 비교 분석을 위해 NS2(Network Simulator2)를 이용하며 WLAN 환경변화 (AP의 개수, MS의 개수)에 따른 핸드오프 관련 메시지의 개수 및 핸드오프 지연시간을 비교 분석 한다.

5.1 기존 연구의 문제점 및 비효율 성

핸드오프 시 인증에 따른 지연시간을 최소화하기 위해 802.11i에서는 Pre-Authentication 방식을 제안하고 있으며 802.11f 에서는 IAPP 프로토콜을 제안하고 있다.

802.11i에서 제안하고 있는 Pre-Authentication 방식은 핸드오프가 발생하기 전 향후 핸드오프 할 가능성이 있는 AP들에 대해 사전에 인증을 시도하는 방식이다. 그러나 어떻게 향후 핸드오프 할 가능성이 있는 AP들을 선정하는지에 대해서는 표준에서 언급하고 있지 않다. 이와 관련 하여 제안된 연구 중 PKD 방식은 NG를 이용하여 향후 핸드오프 할 가능성이 있는 AP들을 선정하고 핸드오프 발생 전 인증작업을 진행함으로써 MS의 로밍 시 핸드오프 지연 시간을 최소화 하고 있다. 그러나 PKD 방식과 같은 Proactive 방식은 AS와 AP사이의 많은 메시지 교환을 요구하고 있으며, 향후 핸드오프 할 AP들에게 선 분배해야 하는 PMK 계산과 관련하여 AS에 과중한 부담을 발생시키고 있다. 또한 MS의 밀도가 높은 지역에서 MS의 로밍이 빈번하게 발생할 경우 AP가 유지해야 하는 사전 인증 정보가 계속해서 갱신되기 때문에 특정 MS가 향후 핸드오프 할 AP와 사전 인증 후 실제 핸드오프가 발생 하였을 때 인증 정보가 다른 MS들의 인증 정보로 갱신되어 전체 인증 과정을 다시 거쳐야 하는 문제가 발생 할 수 있다.

802.11f에서 제안하고 있는 IAPP 프로토콜은 MS가 현재 서비스를 받고 있는 AP(Old AP)의 서비스 영역을 벗어나 새로운 AP(New AP)의 서비스 영역으로 로밍 할 경우 Old AP와 New AP사이에 Security Block 메시지 교환 및 Move 메시지 교환 등 총 4회의 메시지 교환을 추가 하여 핸드오프 시 지연 시간을 단축시키고 있다. 그러나 AP 상호간 보안 관련 메시지 교환 작업은 AP들 간의 보안상의 독립성을 보장해 주지 못한다는 심각한 문제점을 내포하고 있다.

5-2 모의실험에서는 PKD 방식과 본 논문에서 제안하고 있는 메커니즘을 다양한 WLAN 환경변화 속에서 핸드오프 시 AS 와 AC가 전송하는 인증 관련 메시지 개수 및 핸드오프 지연시간을 비교 분석한다.

5.2 모의실험

본 논문에서 제안하고 있는 메커니즘과 PKD 방식을 비교하기 위해 NS2를 사용하여 가상의 시뮬레이션 환경을 구축 하였다. 기본적인 실험 환경은 [표 2]와 같이 설정하였다. 전체 네트워크의 크기는 500m* 500m 이고 AP한 개의 전송 범위는 150m로 설정 하였다. AP의 배치는 [그림 4]와 같이 2차원으로 AP의 개수에 따라 균일한 간격을 두고 배치하였다. 단 MS가 AP의 전송 범위 끝으로 이동할 경우 전송 범위 내에 있어도 신호의 세기가 약해져서 데이터의 전송이 끊기므로 실험에서는 AP의 간격을 150m보다 가깝게 위치 시켰다. 시뮬레이션 환경에서 MS는 Random Waypoint Model을 사용하여 이동한다. 본 실험에서는 3.3 제안 프로토콜 설명 시 소개했던 (식 2)를 위해 암호화 알고리즘으로 일 방향 해쉬함수 128bit MD5를 사용하였고 (식 1)과 (식 3)에 의해 도출된 키 값은 512bit를 사용하였다. 기본 실험 환경에서 MS의 개수 변화, AP의 개수 변화 등 총 2가지 변화된 환경에서 핸드오프가 발생할 때 AS와 AC에서 전송되는 인증 관련 메시지의 개수 및 핸드오프 시간을 측정하였다. NG를 이용한 PKD 방식의 경우 AS가 AP들에게 인증 정보를 전달해야 하고 본 논문에서 제안하고 있는 메커니즘은 AC가 향후 핸드오프 할 AP(Target AP)로 인증정보를 전달해야 하기 때문에 AS와 AC에서 전송되는 메시지를 비교의 대상으로 선정하였다. 각 각의 실험에서 본 논문에서 제안하고 있는 방식은 Proposed로 표시하고 NG를 이용한 PKD 방식은 PKD로 표시한다.

[실험 1] MS의 개수 변화에 따른 전송 메시지 개수 비교는 [표 3]의 실험 환경을 따른다. 실험 1의 결과는 [그림 5]과 같다. 본 논문에서 제안하고 있는 메커니즘은 핸드오프가 일어날 때 AC에서 Target AP로만 PMK를 전달하므로 개수 변화와는 무관하게 핸드오프 1회당 AC가 전송하는 메시지의 개수는 고정적이다. 그러나 NG를 이용한 PKD방식의 경우 MS의 개수 증가에 따라 AS의 과부하로 인한 메시지 Drop으로 인해 전송하는 메시지의 개수가 조금씩 증가 한다.

[실험 2] AP의 개수 변화에 따른 전송 메시지 개수 비교는 [표 4]의 실험 환경을 따른다. 실험 2의 결과는 [그림 6]과 같다. 본 논문에서 제안하고 있는 메커니즘

[표 2] 기본 시뮬레이션 환경

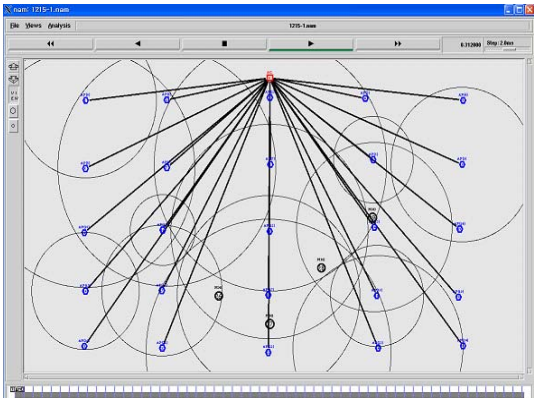
영역	500m * 500m
실험 시간	1000 sec
AP 개수	25개, 36개, 49개, 64개
MS의 이동속도	최대 1.5 m/sec
MS의 개수	5개, 20개, 35개, 50개
AP의 전송범위	150m
Mobility Model	Random Waypoint model

[표 3] [실험 1] MS 개수 변화 시뮬레이션 환경

영역	500m * 500m
실험 시간	1000 sec
AP 개수	25개, 36개, 49개, 64개
MS의 이동속도	최대 1.5 m/sec
MS의 개수	1개 고정
AP의 전송범위	150m
Mobility Model	Random Waypoint model

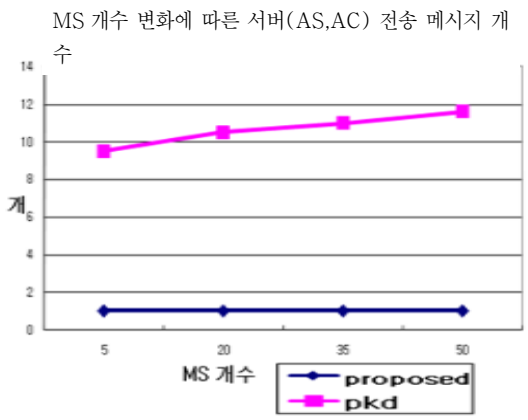
[표 4] [실험 2]AP 개수 변화 시뮬레이션 환경

영역	500m * 500m
실험 시간	1000 sec
AP 개수	49개 고정
MS의 이동속도	최대 1.5 m/sec
MS의 개수	5개, 20개, 35개, 50개
AP의 전송범위	150m
Mobility Model	Random Waypoint model

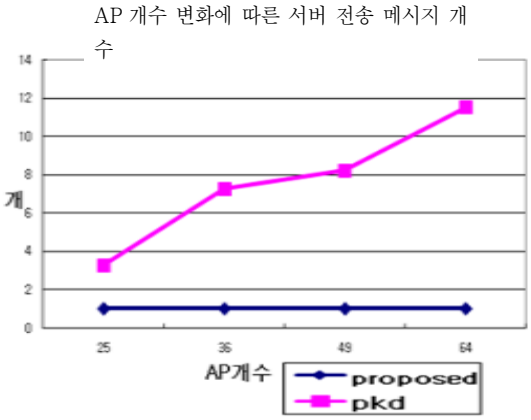


[그림 4] NS2 시뮬레이션 환경에서의 AP 배치도

은 [실험 1]과 동일하게 핸드오프가 일어날 때 AC에서 Target AP로만 PMK를 전달하므로 AP의 개수 변화와는 무관하게 핸드오프 1회당 AC가 전송하는 메시지의 개수는 고정적이다. 그러나 NG를 이용한 PKD 방식의

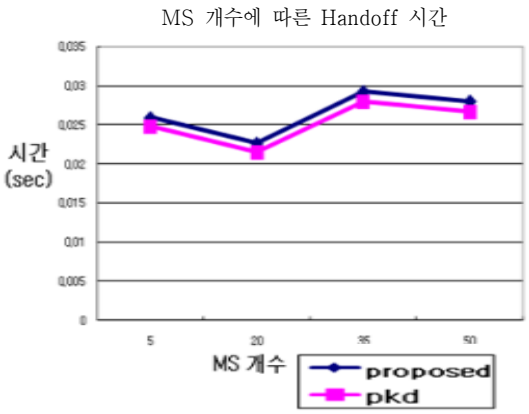


[그림 5] 실험 1의 결과



[그림 6] 실험 2의 결과

경우 WLAN 서비스 영역 내의 AP의 개수가 증가함에 따라 각각의 AP의 NG에 소속되는 AP가 증가하므로 AS가 전송하는 메시지의 개수가 증가됨을 알 수 있다.



[그림 7] 실험 3의 결과

[실험 3] MS 개수 변화에 따른 핸드오프 시간 비교는 [표 3]의 실험 환경을 따른다. 실험 3의 결과는 [그림 7]과 같다. 본 실험에서는 Random Waypoint Model을 사용하여 MS의 속도 및 이동 방향을 랜덤하게 설정한다. 핸드오프 지연시간은 MS의 이동 속도와 방향에 많은 영향을 받는다. 본 논문의 실험환경에서 채택하고 있는 Random Waypoint Model의 특성 상 MS의 움직임 및 속도가 랜덤 하므로 [그림 7]과 같이 MS의 개수가 증가함에도 불구하고 핸드오프 지연시간은 증가하거나 감소한다. 또한 결과 그래프를 보면 본 논문에서 제안하고 있는 핸드오프 메커니즘이 PKD 방식 보다 핸드오프 지연 시간이 조금 더 긴 것을 확인 할 수 있다. 이는 제안 메커니즘의 경우 핸드오프가 발생 할 때 AC에서 Target AP와 MS사이에 사용 할 세션 키 도출을 위해 PMK를 계산하고 세션 키를 도출 하므로 핸드오프 전 PMK를 계산하는 PKD 방식 보다 핸드오프 지연 시간이 조금 더 긴 것이다. 그러나 두 메커니즘 간 핸드오프 지연 시간의 차이는 미세함을 볼 수 있다.

모의실험을 통해 도출된 결과와 같이 본 논문에서 제안하고 있는 메커니즘은 WLAN의 환경변화와는 무관하게 항상 Target AP로만 핸드오프 관련 메시지를 전송한다. 이는 선 인증 과정에서 AS의 부담이 가중되고 불필요한 PMK 계산 및 저장을 진행하는 기존 연구들의 단점을 해결한 것이다. 비록 PKD 방식에 비해 핸드오프 지연시간이 조금 길지만 실시간 멀티미디어 서비스 제공에 무리를 주지 않는 선을 유지하며 항상 안정적인 상태에서 AS와 AC의 부담을 가하지 않고 빠른 핸드오프를 지원하므로 Proactive 방식 보다 효율적이다.

Ⅵ. 결 론

WLAN 서비스의 수요가 급속도로 증가하고 있는 가운데 인증 및 보안이라는 측면과 끊김 없는 서비스 제공을 위한 빠른 핸드오프 지원은 둘로 나뉘어 생각해서는 안 될 하나의 과제로 남겨져 있다. 선행 된 많은 연구들과 802.11 표준은 이러한 두 가지 측면을 고루 만족시키지 못한 채 크고 작은 문제점들을 내포하고 있다. 본 논문은 이와 같은 문제를 해결하기 위해 중앙집중식

WLAN 환경에서 802.11i 인증 프로토콜 및 세션 키 도출 방식을 개선하여 실시간 멀티미디어 서비스를 제공할 수 있는 안전하고 빠른 핸드오프 메커니즘을 제안하였다. 선행 된 연구들의 배경은 독립식 WLAN 환경이지만 이는 현재 벤더들의 제품 개발 동향과는 거리가 먼 접근 방식이다. 본 논문은 최근 벤더들의 제품 개발 동향에 맞추어 중앙집중식 WLAN 환경에서의 안전하고 빠른 핸드오프 메커니즘을 제안하였다. 본 논문에서 제안하고 있는 핸드오프 메커니즘은 Reassociation 메시지를 이용하여 핸드오프 시 새로운 세션 키를 도출하고 있다. 핸드오프 과정 중 Target AP와 MS간에 새롭게 계산해야 하는 PMK를 AC와 MS사이에서 Reactive 방식을 사용하여 계산 하므로 기존 선 인증 관련 연구들이 내포하고 있던 불필요한 계산 및 인증 정보 저장의 문제를 해결하였으며 자연스럽게 AS의 부담을 대폭 줄여주었다. 또한 Reassociation 과정 중 Reassociation Request/Response 메시지에 PTK 도출을 위한 파라미터를 추가하여 PTK를 도출하므로 기존 802.11i 인증 과정 중 발생 할 수 있는 DoS공격 가능성 또한 원천적으로 봉쇄하고 있다.

참고문헌

[1] IEEE Standard 802.11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,” IEEE, IEEE Std 802.11(Revision of IEEE std 802.11-1999), June 2007.

[2] IEEE Standard 802.11i, “Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,” IEEE, July 2004.

[3] IEEE Standard 802.1x, “IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control,” IEEE, IEEE Std 802.1X-2004(Revision of IEEE Std 802.1X-2001), June 2001.

[4] C. He and C. Mitchell, “Analysis of the 802.11i 4-way handshake,” Proceedings of the 3rd ACM workshop on Wireless security(WiSe'04), pp. 43-50, Oct. 2004.

[5] IEEE Standard 802.11f, “IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter- Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation,” IEEE, July 2003.

[6] A. Mishra, M.H. Shin, N. Petroni, T.C. Clancy, and W.A. Arbaugh, “Proactive key distribution using neighbor graphs,” IEEE Wireless Communications, vol. 11, no. 1, pp. 26-36, Feb. 2004.

[7] F.D. Rango, D.C. Lentini, and S. Marano, “Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i,” EURASIP Journal on Wireless Communications and Networking, vol. 2006, no.2, pp. 1–19, Apr. 2006.

[8] C. He and J.C. Mitchell, “Security analysis and improvements for IEEE802.11i,” Proceedings of the 12th Annual Network and Distributed System Security Symposium(NDSS '05), Denial of Service Attacks, Feb. 2005.

[9] IEEE 802.11r Draft Standard, “Draft Standard for Information technology - Telecommunications and information exchange between system - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 2: Fast BSS Transition,” IEEE, Sep. 2007.

<著者紹介>

박 창 섭 (Chang-Seop Park) 종신회원
1983년: 연세대학교 경제학과 졸업
1983년: 한국 IBM 근무
1990년: 미국 Lehigh Univ. 전자계산학 박사
1990년~현재: 단국대학교 전자컴퓨터학부 교수
<관심분야> 네트워크 보안, 암호 프로토콜

우 병 덕 (Byung-Duk Woo) 학생회원
2006년: 단국대학교 컴퓨터과학과 졸업 학사
2006년: (주)EOTECHNICS 근무
2008년 3월~현재: 단국대학교 전자계산학 석사과정
<관심분야> 정보보호, 무선 네트워크 보안

임 정 미 (Jeong-Mi Lim) 종신회원
2000년 2월: 단국대학교 전자계산학과 졸업 학사
2002년 2월: 단국대학교 전자계산학과 석사
2006년 8월: 단국대학교 전자계산학과 박사
2004년 3월~현재: 단국대학교 교양학부 강의전임
<관심분야> 정보보호, 네트워크 보안