# IEEE 802.11 무선랜 DoS 공격에 안전한 인증 및 세션키 분배 메커니즘

우병덕*, 박창섭*
*단국대학교 전자계산학과
e-mail : sayttre@dankook.ac.kr

# An Authentication and Session Key Distribution Mechanism Secure Against DoS Attacks in the 802.11 WLAN

Byung-Duk Woo*, Chang-Seop Park*
*Dept. of Computer Science, Dan-Kook University

**요 약**

최근 들어 IEEE 802.11 WLAN 서비스에 대한 수요의 증가와 함께 WLAN 환경에서 실시간 멀티미디어 서비스를 이용하려는 사용자의 관심이 날로 증가하고 있다. 그러나 IEEE 802.11i 의 보안 정책은 MS 의 이동이 빈번하게 발생하는 WLAN 환경에서 끊김 없는 실시간 멀티미디어 서비스를 제공하기에는 핸드오프 지연 시간이 너무 길다. 본 논문은 DoS 공격에 취약한 기존 802.11i 에서의 4-*way Handshake* 를 대체하는 신속하고 효율적인 인증 및 세션키 분배 메커니즘을 제안한다.

## 1. 서론

WLAN(Wireless Local Area Network)기술은 네트워크 구축 및 유지 보수의 편리성과 함께 인증과 보안 관련 기술의 발전으로 인해 그 수요가 최근 몇 년간 폭발적으로 증가하였고 최근에는 WLAN 환경에서의 실시간 멀티미디어 서비스에 대한 사용자의 관심이 날로 증가하고 있다. 그러나 인증과 보안이라는 측면은 WLAN 에서 끊김 없는 실시간 멀티미디어 서비스를 제공하는데 큰 걸림돌이 되었고 이를 해결하기 위해 현재까지 많은 연구가 진행 되고 있다. WLAN 표준화 초기에 인증과 보안을 위해 IEEE 802.11b 의 WEP(Wired Equivalent Privacy) 방식을 채택했으나 WEP 설계 자체에 오류가 있어 신뢰성을 완전히 잃어 버렸고 이를 보완하기 위해 IEEE 802.11i 는 국제 WLAN 보안표준을 제정하였다. 802.11i 는 MS(Mobile Station, Supplicant), AP(Access Point), AS(Authentication Server) 라는 3 개의 컴포넌트로 구성되어 있으며 IEEE 802.1x 기반의 사용자 인증 방식 및 동적 키 교환 방식을 사용하여 사용자 인증 및 무선 구간에서의 보안 문제를 해결해 주고 있다. 그러나 MS 의 핸드오프 시 마다 802.11i 의 인증 절차를 수행해야 하기 때문에 이로 인한 지연시간은 끊김 없는 실시간 멀티미디어 서비스를 제공하는데 큰 문제점으로 남아 있다. 이와 같은 문제를 해결하기 위하여 본 논문은 AC(Access Controller)를 추가한 중앙집중식 WLAN 환경을 구성하여 AS 의 부담을 현저히 줄이고 Reassociation Request/Response 메시지를 이용한 PTK 도출 메커니즘을 제안한다.

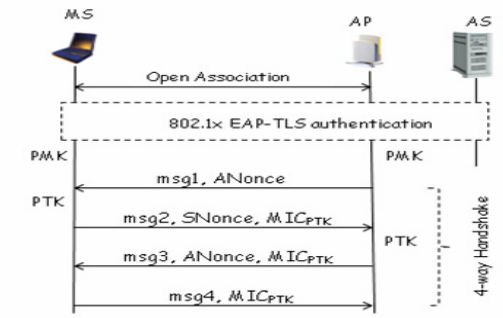
## 2. 관련연구

현재의 WLAN 망에서는 MS 가 새로운 AP 로 이동할 경우 IEEE 802.11i 보안 정책 [2]에 따라 IEEE 802.1x [5] 기반의 인증 절차를 수행하고 *4-way Handshake* 를 통해 새로운 세션키를 도출해 낸다. (그림 1)은 MS 와 AP 를 경유한 AS 사이의 인증 및 세션키 생성을 보여주는 예로써 802.1x EAP-TLS authentication 부분을 통해 MS 와 AS 사이의 상호인증 및 PMK (Pairwise Master Key) 도출을 진행한다. PMK 도출 후 *4-way Handshake* 를 통해 MS 와 AP 사이의 데이터 전송 시 데이터 암호화에 사용할 세션키인 PTK (Pairwise Transient Key)를 생성한다. *4-way Handshake* 는 4 개의 메시지 교환으로 구성된다. 메시지 교환은 쌍방에서 독립적으로 선정한 난수 SNonce, ANonce 그리고 MS 와 AP 의 MAC (Medium Access Control) 주소 *MS*, *AP* 를 기반으로 세션키 PTK = prf (SNonce, ANonce, *AP*, *MS*)를 생성하고 이를 기반으로 상호인증 및 키 확인 (key confirmation)을 위한 목적이다. 이때, prf ( )는 pseudo random function. 첫째 메시지를 제외한 나머지 메시지들에는 PTK 를 이용하여 각각의 메시지에 대한 무결성을 보장하는 MIC (Message integrity Code) 값, 즉 $MIC_{PTK}$ 가 포함된다. MS 의 핸드오프 시 마다 802.11i 보안 절차에 따라 802.1x 인증절차를 수행하기 때문에 이로 인한 지연시간은 끊김 없는 실시간 멀티미디어 서비스를 제공하는데 심각한 문제점으로 남는다.
이와 같은 문제를 해결하기 위해 802.11i 에서는

Pre-Authentication [2] 방식을 제안하고 있으며, 802.11f [3]에서는 IAPP (Inter Access Point Protocol)을 활용하여 핸드오프 시 지연시간을 줄일 수 있는 방식을 제안하고 있고, 그 외 PKD (Pro-active Key Distribution) [7] 방식과 같이 빠른 핸드오프에 관한 여러 연구들이 진행 되고 있다.

802.11i 에서 제안 하고 있는 Pre-Authentication 은 MS 가 현재 접속된 AP 를 통해 향후 핸드오프 할 AP 들에 대해 사전에 인증을 시도하는 방식으로 Pre-Authentication 결과로써 생성된 PMK 와 해당 MS 와의 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. 802.11f 의 IAPP (Inter-Access Point Protocol)는 AP 간 2 계층 전달 정보 및 AP 의 Security Context 정보를 공유함으로써 MS 의 신속한 이동을 지원할 수 있는 프로토콜로 MS, 둘 이상의 AP, DS(Distribution System), 인증 서버로 구성된 환경에서 동작한다. 이처럼 서로 다른 AP 간의 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 AP 들을 선정하여 MS 의 인증정보를 선 분배시키는 방식으로 NG 영역 내의 AP 들은 한 MS 의 사전인증을 위해 분배된 키를 서로 다른 형태로 보유하고 있으므로 동일한 인증정보를 가지는 위험성을 제거하였다. 하지만 사용자의 인증정보를 한 홉 단위 거리의 AP 들에 대해서만 분배되어 NG 영역 이외의 AP 로 MS 가 핸드오프를 할 경우, 또 다시 전체 802.1x EAP-TLS authentication 과정을 진행 하게 되어 고속의 인증 기능을 제공할 수 없는 단점이 있으며, 한 홉 단위 거리 안에서 AP 로 MN 이 핸드오프를 하게 되었을 때는 빠른 고속의 인증이 가능하지만 목적지 AP 를 제외한 NG 리스트에 있던 AP 들은 불필요한 키를 저장해야 하며 서버 또한 불필요한 키 계산으로 인한 부하가 발생한다는 문제점이 있다.




(그림 1) 802.11i 의 인증 및 세션키 도출 과정

## 3. 제안 핸드오프 메커니즘

본 논문은 중앙집중식 WLAN 환경을 기반으로 MS 의 핸드오프 시 802.11i 에 명시되어 있는 MS 와 AP 간의 상호인증 및 세션 키 분배 프로토콜을 개선 하여 핸드오프 시간 단축 및 *4-way Handshake* 에 대한 DoS 공격 가능성을 제거하는 핸드오프 메커니즘을 제안한다.

### 3-1 중앙집중식 WLAN 환경

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 AP 를 단순히 안테나처럼 사용함으로써 예전처럼 AP 를 도난 당할 경우 보안관련 설정의 노출에 대한 걱정을 할 필요가 없어 진다.

### 3-2 설계원리

IEEE 802.11 WLAN 에서는 MS 가 새로운 AP 로 핸드오프 할 때 대상이 되는 AP 로 Reassociation Request 메시지를 보내게 되고 이에 대한 응답으로 Reassociation Response 메시지를 받게 된다. Reassociation 후 MS 와 AP 는 802.11i 보안 정책에 따라 802.1x 기반의 인증 절차를 수행하고 *4-way Handshake* 를 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 세션키 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 MS 와 AP 사이의 PMK, PTK, Nonce 생성 알고리즘을 수정하고 Reassociation Request / Response 메시지에 새로운 필드 (Field)를 추가하여 PTK 도출에 사용함으로써 *4-way Handshake* 의 DoS 공격 가능성을 제거하고 PKD 방식과 같이 서버와 네트워크에 부하를 증가시키는 선 인증 방식의 문제점을 해결하고자 한다.

### 3-3 제안 프로토콜

본 논문에서 제안하고 있는 프로토콜은 MS 와 AS, AP 와 AC, AC 와 AS 사이에는 안전한 채널 (secure channel)이 사전에 존재한다고 가정한다. MS 는 $AP_1$ 과 최초의 Association 작업을 통해서 AS 와의 802.11i / 802.1x Full EAP-TLS Authentication 을 성공적으로 수행하고 초기 PMK 값인 $PMK_0$ 와 $PMK_0$ 를 기반으로 $AP_1$ 과 공유할 세션키 $PTK_1$ 을 생성한 후 모든 인증 작업을 마친다. 인증 작업을 완료한 후 WLAN 서비스를 이용하던 MS 가 현재의 AP 인 $AP_1$ 의 영역으로부터 벗어나기 시작하면 Probe Request / Response 메시지를 통해서 주변의 여러 AP 들 중에서 핸드오프 할 AP 를 선정하게 된다. (그림 2)에서는 최적의 AP 로 $AP_2$ 를 선정하였고, Disassocaition 메시지를 통해서 $AP_1$ 과의 association 을 종료한다. (그림 2)의 A

는 MS 가 $AP_1$ 과 최초 Association 후 WLAN 서비스를 이용하다 $AP_2$ 로 핸드오프 하는 과정을 보여 주고 있다. 핸드오프 과정에서 802.11i 의 *4-way Handshake* 대신에 본 논문에서는 (그림 2)의 A 에서와 같이 Reassociation Request / Response 메시지에 인증 및 세션키 생성에 소요되는 파라메터를 위한 새로운 필드를 추가하는 방식을 채택한다. 먼저 MS 는 초기 $PMK_0$ 를 기반으로 $AP_1$ 과 공유할 세션키 $PTK_1$ 생성을 위해 다음의 계산을 수행한다 (j=1 인 경우). 이때, h ( )는 일방향 해쉬함수, prf ( )는 pseudo random function.

$PMK_j = prf\ (PMK_0, MS, AP_j)$, (식 1)

$Nonce_j = h\ (PMK_j)$, (식 2)

$PTK_j = prf\ (PMK_j, Nonce_j, MS, AP_j)$ (식 3)

$PMK_1$ 은 MS 가 $AP_1$ 과 공유할 $PTK_1$ 의 생성을 위해서 사용되는 값이지만, 이 값은 $AP_1$ 에게는 노출되지 않는 MS 와 AC 간에만 공유되는 값이다. $Nonce_1$ 은 MS 와 $AP_1$ 사이에서 그 어느 한쪽에 의해서 일방적으로 결정될 수 없는 난수 (random number) 이기 때문에 *4-way Handshake* 에서와 달리 하나의 Nonce 를 사용하여 상호 인증이 가능하다. $Nonce_1$ 이 생성 되면 $PTK_1$ 을 최종적으로 도출 할 수 있게 된다.

**(단계 1 : Reassociation Request 전송)**

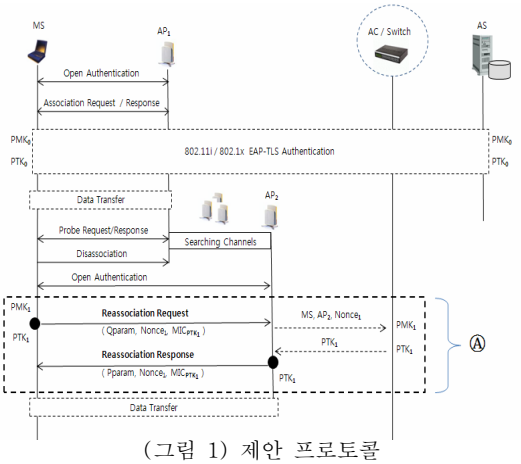
MS 는 Reassociation Request 메시지를 작성하여 $AP_2$ 에게 전송한다. 이 메시지에는 Reassociation 과 관련된 기본 파라메터 (예: current AP address)인 Qparam, $Nonce_1$, $MIC_{PTK_1}$ 가 포함된다. 이때, $MIC_{PTK_1}$ 는 Reassociation Request 메시지 내의 모든 필드를 $PTK_1$ 로 계산한 MIC 값으로 Reassociation Request 메시지에 대한 무결성을 보장한다.

**(단계 2 : AC 의 PTK 생성)**

Reassociation Request 메시지를 전송 받은 $AP_2$ 는 $PMK_1$ 을 모르고, 따라서 $PTK_1$ 을 계산할 수 없기에 AC 에게 $PTK_1$ 을 요청하게 된다. 이를 위해서 $AP_2$ 는 AC 에게 *MS*, $AP_2$, $Nonce_1$ 을 전송한다. AC 는 이를 기반으로 위의 (식 1), (식 2), (식 3)을 이용해 $PTK_1$ 을 계산하고 이를 $AP_1$ 에게 안전하게 전달한다. MS 와 공유할 $PTK_1$ 을 전달 받은 $AP_2$ 은 (단계 1)에서 전달받은 Reassociation Request 메시지에 대한 무결성 검사를 수행한다. 만약, 무결성 검사가 실패하면 프로토콜은 여기서 멈추게 된다. 만약 성공할 경우에는 $AP_2$ 는 MS 에 대한 인증이 성공한 것을 의미하며 또한 MS 와의 키 확인 (key confirmation) 역시 성공적으로 수행됨을 의미한다.

**(단계 3 : Reassociation Response 전송)**

후속적으로 $AP_2$ 는 Reassociation Response 메시지를 작성하여 MS 에게 회답하게 된다. 이 메시지에는 기본적인 파라메터 (예: Association ID)인 Pparam, $Nonce_1$, $MIC_{PTK_1}$ 가 포함되며, 이는 궁극적으로 이 메시지에 대한 무결성 보장을 위한 목적이다. 이를 전달받은 MS 는 $PTK_1$ 을 기반으로 메시지에 대한 무결성을 점검한다. 성공적인 무결성 점검은 결국 MS 입장에서는 $AP_2$ 에 대한 인증이 성공적으로 이루어 졌으며 또한 키 확인 역시 성공적으로 수행되었음을 의미한다.




(그림 1) 제안 프로토콜

## 4. 안전성 분석

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

### 4-1 Nonce 와 재생공격

802.11i 에 명시된 세션키 도출 과정을 보면 PTK 도출을 위해 *4-way Handshake* 를 진행 한다. 이때 MS 와 AP 는 각자의 Nonce 를 생성하고 이를 PTK 도출을 위한 파라메터로 사용한다. 이처럼 MS 와 AP 가 각기 상이한 Nonce 를 생성하고 이를 *4-way Handshake* 에 사용하는 이유는 MS 와 AP 간의 상호 인증 및 *4-way Handshake* 과정 중 메시지 재생공격을 방지하기 위함이다. 본 논문에서 제시하고 있는 PTK 생성 알고리즘은 한 개의 Nonce 만 사용하고 있으나 Nonce 생성 방식을 (식 2)와 같이 구성 함으로써 MS 와 AP 간의 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 MS 는 한번에 하나의 AP 와 연결 후 서비스를 이용할 수 있다. 그렇기 때문에 핸드오프 시 MS 는 현재 서비스를 받고 있는 AP 와 Disassociation 과정 후, 핸드오프의 대상이 되는 AP 와 새로운 세션키를 생성하여 WLAN 서비스를 지속적으로 이용해야 한다. 그런데 이 과정에서 발생되는 Disassociation 메시지와 세션키 도출을 위한 *4-way Handshake* 단계는 모두 각기 다른 유형의 DoS 공격에 노출 되어 있다. Deauthentication & Disassociation 메시지는 MS 가 AP 로 일방적으로 보내는 암호화 되지 않은 메시지로써 AP 는 해당 메시지에 대한 응답을 보내지 않는다.

이처럼 Deauthentication & Disassociation 메시지

는 해당 메시지 자체에 대한 인증이 결여 되기 때문에 공격자가 Deauthentication & Disassociation 메시지를 위조하여 DoS 공격을 가하면 MS 는 WLAN 서비스의 연결이 끊기게 되어 Authentication & Association 과정을 다시 수행해야 한다. *4-way Handshake* 단계는 총 4 회의 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 MS 와 AP 간의 PTK 불일치를 유발하여 프로토콜의 정상적인 진행을 방해하는 DoS 공격을 시도할 수 있게 된다. 본 논문에서 제안하고자 하는 핸드오프 메커니즘은 Reassociation Request / Response 메시지를 사용하여 PTK 를 도출해 내므로 *4-way Handshake* 과정을 생략할 수 있다. 이는 *4-way Handshake* 에 대한 DoS 공격을 원천적으로 차단 시키는 결과를 얻을 수 있는 것이다. 또한 Reassociation Request / Response 메시지 교환 전에 이미 MS 와 AP 사이에 사용할 PTK 가 만들어 진 상태이고 이를 이용하여 Reassociation Request / Response 메시지에 MIC 값을 첨부하여 무결성을 입증하듯이 Deauthentication & Disassociation 메시지 또한 동일한 방식으로 보호한다면 Deauthentication & Disassociation 메시지에 대한 DoS 공격에 대해서도 방어 할 수 있다.

### 4-3 PMK Caching

로밍 시 MS 가 이전에 방문했던 AP 를 다시 방문하는 상황이 발생 할 수 있다. 이때 좀 더 빠른 핸드오프를 지원하기 위해 802.11i 에서는 PMK Caching 기능을 지원하고 있다 PMK Caching 이란 MS 와 AS 사이에 상호인증으로 생성된 PMK 를 MS 와 AP 가 지속적으로 Cache 하여 재 사용함으로써 향후 MS 가 이전 접속했던 경험이 있는 AP 로 다시 재 접속을 시도할 경우 Cache 된 PMK 정보를 이용하여 인증 절차를 마무리하는 방식이다. 본 논문에서 제시하는 핸드오프 메커니즘 또한 PMK Caching 기능을 지원하며 만약 PMK 의 Lifetime 이 초과되어 해당 PMK 가 삭제될 경우 본 논문에서 제시한 PMK 생성 알고리즘을 동일하게 적용한다. 단 MS 가 이전에 방문했던 AP 를 다시 방문하는 경우 PTK 도출을 위한 Nonce 생성 알고리즘은 (식 4) 를 사용하여 생성한다.

$$Nonce_j = h(PMK_j, Timestamp) \quad \text{(식 4)}$$

MS 가 이전에 방문했던 AP 를 다시 방문하는 경우에 Cache 된 PMK 를 사용하든지 PMK 의 Lifetime 이 초과되어 새로운 PMK 를 생성해서 사용하든지 동일한 PMK 를 사용하게 되고 이때 해당 PMK 를 가지고 PTK 생성 시 사용할 Nonce 를 계산한다면 일 방향 해쉬함수 특성상 동일한 Nonce 가 계산된다. 이는 Key freshness 를 보장하기 위한 난수 값을 재사용하기 때문에 보안상 잠재적인 문제점을 가지게 된다. 이를 방지하기 위해 MS 가 이전에 방문 했던 AP 로 재 방문 할 경우 비콘 프레임 (Beacon Frame)의 Timestamp 필드의 값을 Nonce 생성에 (식 4)와 같이 사용하여 재 방문 시 Nonce 값의 재사용을 막을 수 있다.

## 5. 결론

본 논문은 중앙집중식 WLAN 환경에서 802.11i 인증 프로토콜 및 세션 키 계산 방식을 개선하여 실시간 멀티미디어 서비스를 제공할 수 있는 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 AP 와 MS 간에 새롭게 계산해야 하는 PMK 를 AC 와 MS 사이에서 Reactive 방식을 사용하여 계산 하므로 기존 선 인증 관련 연구들이 내포하고 있던 불필요한 계산 및 인증 정보 저장의 문제를 해결하였으며 자연스럽게 AS 의 부담을 대폭 줄여주었다. 또 한 Reassociation 과정 중 Reassociation Request / Response 메시지에 PTK 도출을 위한 파라메터를 추가하여 PTK 를 도출하므로 기존 802.11i 인증 과정 중 발생 할 수 있는 DoS 공격 가능성 또한 원천적으로 봉쇄하고 있다. 이처럼 본 논문이 안전하고 빠른 핸드오프를 지원하기 위한 메커니즘을 제안하고 있지만 본 논문에서 제안하는 방식이 100% 완벽한 방식이라고 결론지을 수는 없다.

향후 연구해야 할 과제는 독립식 WLAN 환경과 중앙집중식 WLAN 환경에서 모두 적용 가능한 핸드오프 메커니즘 개발 및 해당 핸드오프 메커니즘이 두 환경을 모두 지원하면서 최적의 핸드오프를 지원한다는 것을 증명하는 것이다.

## 참고문헌

[1] IEEE 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE Standard, June 2007.

[2] IEEE 802.11i, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements, IEEE Standard, July 2004.

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

[4] IEEE 802.11r Draft Standard, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Fast BSS Transition, IEEE Standard, September 2007.

[5] IEEE 802.1x, IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Standard, June 2001.

[6] C. He, C. Mitchell, Analysis of the 802.11i 4-way handshake, in Proceedings of the ACM Workshop on Wireless Security, Philadelphia, Pa, USA, October 2004, pp.43–50.

[7] Mishra, A. Min Ho Shin Petroni, N.L., Jr. Clancy, T.C. Arbaugh, W.A, Proactive key distribution using neighbor graphs, Wireless Communications, IEEE Publication Date: Feb 2004