무선랜 FILS 를 위한 EAP/EAP-RP 기반의 빠른 인증 기고에 대한 고찰

이석준, 김신효
한국전자통신연구원 사이버융합보안연구단 사이버객체보안연구팀
e-mail : {junny, shykim}@etri.re.kr

Consideration on the Contribution of Fast Authentication for FILS using EAP/EAP-RP in IEEE 802.11

Sokjoon Lee, Shin Hyo Kim
Smart Things Security Research Team, ETRI

요 약

IEEE 802.11 규격[1]은 2.4GHz 및 5GHz 대역에서 무선 근거리 접속 통신을 위한 국제 표준이다. 1997 년 2.4GHz 대역에서 1, 2 Mbps 의 속도를 지원하는 최초의 규격이 정의된 이래, 속도 개선을 위한 변복조 방식, 보안, QoS 등 다양한 요구 사항을 만족하기 위하여 표준이 지속적으로 개정되어 왔으며 2012 년 새로 개정된 표준이 발표된 바 있다. 특히, 최근 들어서 스마트폰의 무선랜 사용량이 폭발적으로 증가하고 무선랜 접속을 위한 핫스팟 역시 수가 크게 늘면서, 보안성을 유지하면서도 무선랜의 초기 연결접속 시간을 최소화(FILS; Fast Initial Link Setup)함으로써 무선랜 접속 요청 이용자 수에 확장성을 갖는 무선랜 규격을 제정할 필요성이 생기면서 IEEE 내에 802.11ai Task Group[3]이 승인되어 현재 표준화 작업을 진행중에 있다.

IEEE 802.11 무선랜 규격에서 초기 연결접속 시간의 상당 부분을 네트워크 발견, 보안 접속, 인증 등에 소요하게 되어, IEEE 802.11ai 에서는 보안성을 떨어뜨리지 않으면서도 빠르게 인증을 하기 위한 매커니즘에 대해 논의 중이다. 본 논문에서는 IEEE 802.11ai 에서 논의 중인 “FILS 를 위한 EAP/EAP-RP 기반의 빠른 인증” 기술에 대해 살펴보고, 이의 장단점을 분석하여 보다 개선된 형태의 빠른 인증 기법을 제안하고자 한다.

1. 서론

최근 스마트폰의 등장으로, 언제 어디서나 개인화된 서비스와 함께 콘텐츠의 이용이 보편화되고 있다. 사용자들은 스마트폰을 들고 다니면서 이동시에는 저속/고비용의 3G/4G 네트워크를 이용하고, 집, 공항, 커피숍 등 고정된 장소에서는 IEEE 802.11 규격[1]의 무선 근거리 접속 통신을 통하여 웹 서핑, 고화질의 비디오 등 다양한 형태의 멀티미디어 콘텐츠를 소비하고 있다. IEEE 802.11 무선랜 기술은 근거리에서 AP 를 통해 인터넷 접속을 저비용으로 손쉽게 가능하게 한다.

특히 현재 수십~수백 Mbps 급의 802.11n 네트워크가 점점 보편화되고 조만간 수 Gbps 급의 초고속 무선랜 서비스도 가능해질 것으로 예상됨에 따라, 무선랜의 이용 단말 수와 데이터 통신량, 인터넷 접속을 가능케 하는 핫스팟(Hot Spot)의 수 역시 크게 늘어날 것으로 보인다.

그러나, 누구나 무분별하게 무선랜을 통한 인터넷 접속을 허용할 경우, 네트워크 품질 저하 및 보안에 대한 문제가 발생할 수 있으므로, 무선랜 서비스 제공자들은 무선랜 이용자에 대한 관리 및 보안성을 위하여 IEEE 802.1X[2] 기반의 사용자 인증 및 WPA 기반의 데이터 보호 기법을 제공하는 것이 일반적이다. 또한, 무선 단말들은 물리적으로 고정된 위치에 있지 않으므로 고정된 IP 주소를 사용하기 보다, DHCP 와 같은 프로토콜을 이용하여 동적으로 IP 를 할당받는다. 이들 기술은 향상된 보안성과 편리한 이동성을 보장하지만, 초기 연결접속을 위한 시간이 길어지는 단점이 있다.

따라서, IEEE 802.11ai Task Group[3]에서는 보안성을 유지하면서도 무선랜의 초기 연결접속 시간을 최소화하여 빠른 초기 연결접속(이하 FILS; Fast Initial Link Setup)을 달성함으로써 무선랜 접속 요청 이용자 수에 확장성을 가지는 무선랜 규격을 제정하기 위한 표준화 활동을 진행중에 있다. 본 논문에서는 이 Task Group 에서 논의 중인 “FILS 를 위한 EAP/EAP-RP 기반의 빠른 인증” 기술[4]에 대해 살펴보고, 이의 장단점을 분석하여 보다 개선된 형태의 빠른 인증 기법을 제안하고자 한다.

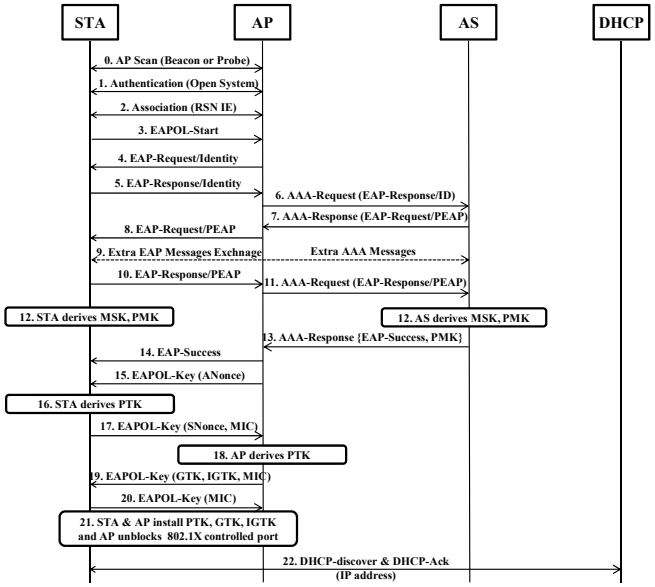
2. EAP/EAP-RP 기반의 빠른 인증 분석

앞서 1 장에서 언급한 바와 같이, IEEE 802.11ai Task

Group 은 무선랜의 초기 연결접속 시간을 최소화하여 FILS 을 달성하기 위한 표준화 활동을 진행 중으로, 2010 년 12 월 승인되어 2014 년 표준 완료를 목표로 하고 있다. FILS 을 위해 AP/Network 발견, 연결 설립/보안 관련 메시지 교환, 상위 계층과의 절차 병합 등의 영역에 대한 효율적인 프로토콜 설계 및 보안성 검토 등에 초점을 맞추어 표준화를 진행 중에 있다.

2.1 보안 관련 메시지 교환 이슈

일반적인 무선랜에서 초기 연결접속을 위한 절차는 (그림 1)과 같다.



(그림 1) 무선랜 초기 연결접속 절차

(그림 1)에서 보는 바와 같이, 인증 및 접속을 하는데 상당히 많은 패킷을 주고받음을 알 수가 있다. Authentication 과 Association Request/Response 패킷 교환의 경우 보안 정보를 주고받는 의미 외에는 인증 효과가 있지 않으며, EAP 인증, EAPOL 4-way Handshake(키 교환), DHCP 등이 서로 완벽히 분리되어 있다든지, EAP 패킷이 802.1X uncontrolled port 의 데이터 프레임으로만 전송됨으로써 생기는 오버헤드가 존재한다.

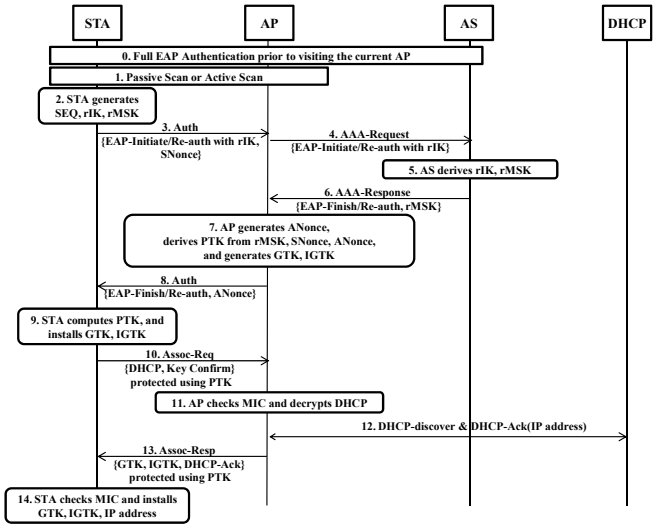
따라서, 여기에서 발생하는 인증 메시지 교환 횟수를 줄이거나, 각 메시지들을 통합하여 전달할 수 있다면 인증에 걸리는 시간을 최소화할 수 있을 것이다. 다만, IEEE 802.11ai TG 에서는 이러한 기법 등을 도입하더라도 보안 강도가 줄어들지 않는 기술 표준을 개발하고자 한다.

보안 관련 메시지 혹은 인증 메시지 교환의 최소화와 관련한 이슈는 주로 Qualcomm 및 Huawei 등을 중심으로 제안되고 있는데, Qualcomm 의 경우에는 재접속시 EAP 재인증 프로토콜(EAP-RP; EAP Reauthentication Protocol)을 사용함으로써 EAP 인증 및 EAPOL 4-way Handshake 의 메시지 수를 최소화하는 것이 주된 아이디어이며, Huawei 의 경우에는 Authentication/Association 메시지, EAP 인증, EAPOL 4-way Handshake, DHCP 프로토콜 메시지를 최대한 통합함으로써 메시지 교환 횟수를 최소화하는 것이 목표이다.

2.2 Qualcomm 의 EAP-RP 적용 프로토콜

Qualcomm 에서는 FILS 를 위해서 EAP-RP[5]를 적용하는 아이디어를 제안하였다. EAP-RP 는 EAP 인증 및 키 교환을 하고 난 뒤에 재인증을 하고자 할 때 EAP 인증을 새로 하는 것이 아니라, 기존에 맺은 공유 마스터 키를 이용하여 서로 같은 키를 유도할 수 있는지를 확인함으로써 인증 및 키 교환을 1 번의 메시지 교환으로 완료하는 프로토콜이다. 따라서, 이 아이디어는 최초의 인증시에는 적용할 수 없으며, 이 때에는 기존 (그림 1) 절차 혹은 2.3 절에서 소개되는 최적화된 EAP 기반의 FILS 기술을 따라야 한다.

몇 번의 기고과 검토, 수정 등을 통하여 2012 년 7 월 샌디에고 회의에서 제안된 프로토콜이 2 개가 있는데, 이 중에서 상대적으로 프로토콜이 깔끔하여 주로 거론되고 있는 프로토콜은 (그림 2)와 같다.



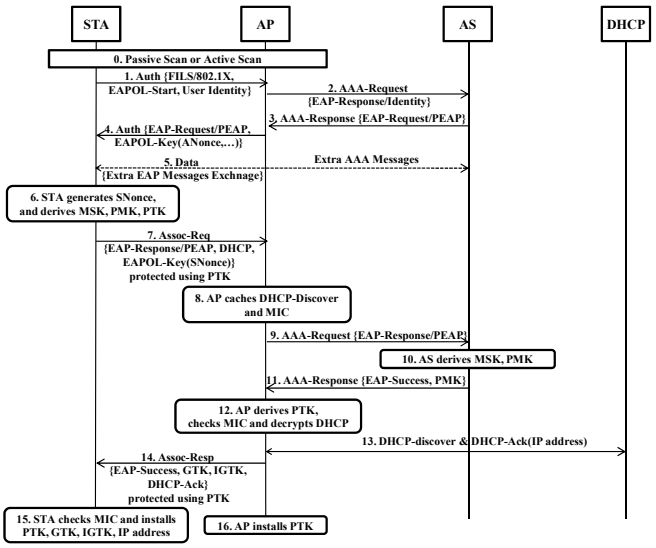
(그림 2) EAP-RP 를 이용한 빠른 재인증

2.3 Huawei 의 최적화된 EAP 기반 FILS

Huawei 는 FILS 를 위하여 Authenticatioin/Association 메시지, EAP 인증, EAPOL 4-way Handshake, DHCP 프로토콜 메시지를 최적화하여 통합함으로써 메시지 교환 횟수를 최소화하고자 한다. 예를 들어, AP Scan 이후 최초로 교환하는 메시지인 Authentication 프레임에 대해서 기존의 무선랜 접속 절차에서는 아무런 데이터 없이 이 프레임을 전송하지만, 여기에서는 EAPOL-Start, User Identity 정보 등을 같이 전송하도록 하고 있다. 그 이후에는 Association 프레임에 EAP 인증 메시지와 DHCP 메시지를 같이 전송하는 등, 기존에 절차적으로 구분된 메시지를 최대한 통합하는 것을 목표로 하고 있다.

Qualcomm 의 제안과 마찬가지로, 몇 번의 기고와 검토, 수정 등을 통하여 2012 년 7 월 샌디에고 회의

에서 제안된 프로토콜은 (그림 3)과 같다.



(그림 3) 최적화된 EAP 기반 FILS

2.4 Qualcomm 및 Huawei 의 제안 분석

Qualcomm 의 제안은 EAP-RP 을 사용함으로써, 기존에 설립된 EAP 인증 및 키교환 과정을 재활용하는 방식으로 최적화를 이룬다. 따라서 프로토콜이 매우 간결하고, 4-way Handshake, DHCP 등을 모두 Authentication, Association 프레임 안에 포함함으로써 무선상의 4 개의 패킷만으로 인증, 키교환, IP 할당이 가능해지는 장점이 있다.

그러나, 여전히 최초의 인증시 혹은 인증 서버에서 재인증 정보가 없어진 경우에는 기존의 EAP 를 사용해야 하므로 모든 경우에 이를 사용할 수 없다. 보안 관점에서는 기존의 4-way Handshake 와 다르게 ANonce 와 SNonce 의 순서가 바뀜으로 인한 문제가 있는지를 분석해야 하며, (그림 2)의 3 번 Authentication 프레임만으로 AP 와 인증서버의 연산과 통신(4, 5, 6, 7, 8 번)을 유발함으로 인하여 무선 DoS 공격이 손쉽게 이루어질 수 있는 우려가 존재한다.

Huawei 의 제안은 기존 무선랜 규격보다 패킷 수를 현저하게 줄인다는 장점이 있다. 즉, authentication, association 프레임에 EAP, 4-way Handshake, DHCP 를 최대한 포함함으로써, 최대 12 개의 패킷 수를 절약할 수 있다.

그럼에도 불구하고, 이 제안 기법은 기존 무선랜 규격의 메시지 흐름과 자연스럽게 연결되지 않는 단점이 있다. 즉, 기존의 무선랜 규격은 Authentication 프레임 교환 후 Association 프레임, 그리고 그 이후에 Data 프레임을 교환하는 절차를 따르는데, 이 제안에서는 Authentication 프레임 교환 직후 EAP 패킷은 키 교환이 완료되기 전까지 Data 프레임으로 주고 받도록 하고 있다. 이후 단말에서 키가 생성될 때 Association 프레임을 통해 EAP 패킷을 전송하는데, 이는 기존 절차와 다르므로 기존 무선랜 규격의 State Machine 을 변경해야 가능하다. 또한 Association Request 를 보낸 후에도 만약 인증 서버에서 인증이 완료되지 않으면(즉, EAP-Success 혹은 EAP-Failure 를 전송할 수 없는 상태이면) AP 에서 단말에게 Association Response 를 보낼 수 없고 추가적으로 Data 프레임을 교환해야 하는데, 이는 프로토콜 관점에서 부적절한 것으로 보인다.

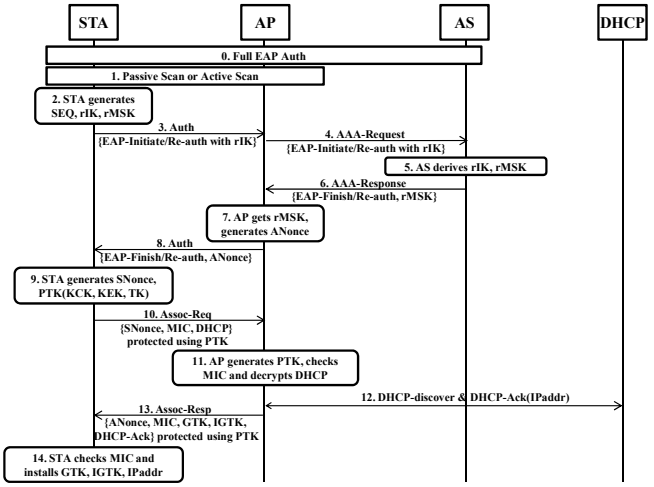
이 외에도, Qualcomm 의 프로토콜에서 EAP-RP 인증 실패가 발생한 경우, 자연스럽게 Huawei 의 프로토콜로 fallback 하여 동작하여야 하는데 두 제안이 자연스럽게 연동되지 않는 문제가 있다.

3. 개선된 빠른 (재)인증 프로토콜 제안

3 장에서는 2 장에서 제안된 2 개의 프로토콜들에 대해 분석한 내용을 기반으로, 각 프로토콜들에 대해 단점을 개선하여 수정한 프로토콜들을 제안한다. 2 개의 프로토콜은 개별적인 단점을 보완한 것 외에도, EAP-RP 가 실패했을 때 자연스럽게 최적화된 EAP 로 fallback 할 수 있는 구조로 설계하였다.

3.1 새로 제안하는 EAP-RP 기반 재인증 기법

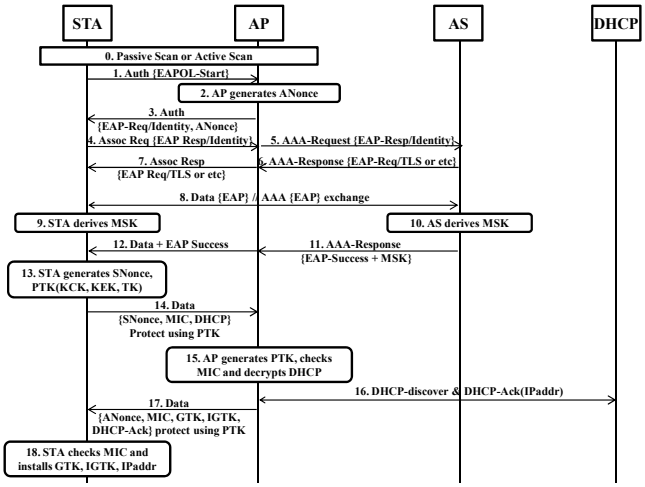
여기에서는 Qualcomm 의 제안, 즉 EAP-RP 적용 프로토콜을 수정한 프로토콜을 (그림 4)에 제안한다. (그림 4)에서는 (그림 2)와 달리, 3 번에서 SNonce 를 먼저 보내지 않고도, 키 교환이 가능해지도록 수정을 하였다. 따라서 AP 에서의 PTK 생성은 (그림 2)의 7 번에서 (그림 4)의 11 번으로 늦춰지게 된다. 그러면서도 DHCP 및 키 교환에 있어서 PTK 로 무결성을 보호할 수 있도록 하였다.



(그림 4) 새로 제안하는 EAP-RP 기반 재인증

3.2 새로 제안하는 최적화된 EAP 기반 FILS

여기에서는 Huawei 의 제안, 즉 최적화된 EAP 기반 FILS 를 수정한 프로토콜을 (그림 5)에 제안한다. 여기에서는 (그림 3)과 달리, Authentication 프레임에는 EAPOL-Start 만을 포함하고 있다. 또한, (그림 3)에서는 Authentication 프레임 이후 Data 프레임을 통하여 EAP 패킷들을 교환하고 있으나, 여기에서는 Association 프레임까지 교환한 이후 Data 프레임을 통해 EAP 패킷들을 교환하도록 수정하였다.

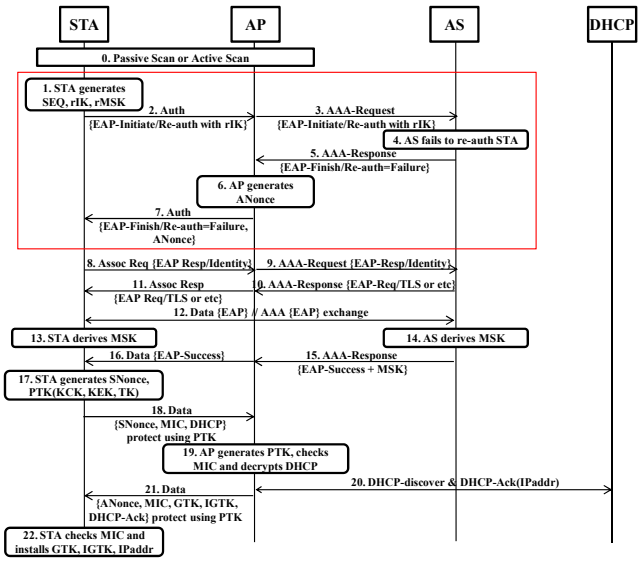


(그림 5) 새로 제안하는 최적화된 EAP 기반 FILS

3.3 제안된 프로토콜 분석

3.1 에서 제안한 프로토콜은, Qualcomm 의 제안과 다르게 ANonce 와 SNonce 의 순서가 기존의 4-way Handshake 와 동일하므로, 보안성을 동일하게 유지하는 장점을 가지고 있다. 여전히 무선랜 DoS 공격은 동일하게 가능하다는 단점을 가지고 있으며, 이 문제를 해결하려면 메시지 수를 늘리지 않고는 불가능할 것으로 보인다.

3.2 에서 제안한 프로토콜은 802.11 State Machine 을 해치지 않으며 메시지 순서가 기존의 802.11 규격과 동일하다는 장점을 가지고 있다. 또한 Huawei 기법은 AP 에서 단말의 EAPOL-Start 에 User Identity 정보가 있느냐에 따라 802.1X State Machine 이 변경되어야 하나, 여기에서는 기존처럼 AP 가 EAP 메시지를 해석하지 않아도 되므로 802.1X State Machine 의 변경이 필요하지 않다는 장점도 가지고 있다.



(그림 6) EAP-RP 인증 실패시 최적화된 EAP fallback 시나리오

또한 Qualcomm 과 Huawei 의 기법이 자연스럽게 연동되지 않는 단점과 달리, 여기에서는 3.1 의 (그림 4)에서 EAP-RP 인증이 실패로 돌아갔을 때 3.2 의 (그림 5)로 자연스럽게 fallback 할 수 있는 장점이 있다.

이러한 fallback 시나리오는 (그림 6)에서 표현하였다. (그림 6)에서는 (그림 4)와 다르게 4 번에서 인증 서버가 단말을 재인증하는데 실패하고 있다. 이에 따라, 7 번에서 AP 가 단말에게 실패했음을 알리는 내용을 Authentication 프레임을 통해 전달하는데, 단말이 이를 받으면 자연스럽게 최적화된 EAP 기반 FILS 모드로 전환하여 (그림 5)의 3 번 프레임을 받은 것과 동일한 상태로 인식한 후, 이후의 절차는 (그림 5)와 동일하게 진행하도록 한다.

다만, 이렇게 함으로써 Huawei 기법에 비해 Performance 측면에서 다소 손해를 보게 된다. 패킷 수로 볼 때, 4 개의 패킷 교환이 더 필요하게 되는 것이다. 그러나 여전히 기존의 무선랜 인증과 비교할 경우 8 개의 패킷 수를 절약할 수 있으며, Huawei 기법에서 association 프레임을 보내기 전에 Data 프레임을 전송하는 등의 기존 규격 State Machine 을 파괴하는 일이 존재하지 않는 장점이 있다.

4. 결론

본 논문에서는 802.11ai TG 에서 논의중인 “FILS 를 위한 EAP/EAP-RP 기반의 빠른 인증” 기고에 대해 분석을 하였다. 이 기고는 Qualcomm 과 Huawei 에서 각각 EAP-RP 기반의 재인증이 가능한 환경과 기존 EAP 를 이용한 인증을 하는 환경으로 나누어 제안한 내용을 담고 있으며, 메시지의 수를 현격하게 줄이는 데는 성공하고 있으나, 보안성과 메시지 순서 등에 있어 기존 무선랜 규격을 해친다는 단점이 있다.

이를 위해 본 논문의 3 장에서는 이 단점을 개선하는 프로토콜을 제안하였다. 제안된 2 개의 프로토콜은 Qualcomm 과 Huawei 의 장점을 받아들이면서도 단점을 해소하여 기존 무선랜 규격의 큰 골격을 해치지 않고 있다. EAP-RP 인증 실패시 fallback 이 가능하도록 개선한 점 역시 제안 프로토콜의 장점으로, 이를 통하여 802.11 기반의 무선랜에서 보다 빠른 인증이 가능하게 될 것으로 보인다.

참고문헌

[1] 802.11-2012 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[2] 802.1X-2004 - IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control

[3] IEEE 802.11ai Task Group, http://www.ieee802.org/11/Reports/tgai_update.htm

[4] George Cherian et al, “Fast Authentication in TGai”, IEEE 802.11-11/1160r10, Jully 2012 IEEE 802 Plenary Session

[5] Z. Cao et al, “EAP Extensions for EAP Re-authentication Protocol”, IETF RFC 6696