情報保護學會論文誌
第13券 第6號, 2003. 12

무선랜 정보보호를 위한 accounting 및 보안 세션의 설계

양 대 헌*†‡, 오 경 희**, 강 유 성**, 함 영 환**, 정 병 호**

Design of Accounting and Security Sessions for IEEE 802.11 Network

DaeHun Nyang*†‡, KyungHee Oh**, YouSung Kang**,
YoungHwan Ham**, ByungHo Chung**

요 약

무선랜은 매체의 특성상 유선보다 메시지의 도청 및 변조가 쉬우므로, 안전한 무선랜의 사용을 위해 IEEE 802.11i, IEEE 802.1x/1aa 등의 표준이 마련되었다. 이들 프로토콜은 RADIUS, EAP-TLS 등과 함께 무선채널의 메시지 인증 및 기밀성을 보장하며 사용자 인증 및 접근제어를 담당한다. 이 논문에서는 무선랜의 상용서비스를 위한 accounting 세션을 IEEE 802.1x의 인증 세션을 이용해 구현하는 방법을 제안하고, 이를 이용해 accounting을 수행하는 state machine을 설계한다. 또한, 무선랜에서 AP와 스테이션간의 무선 보안 채널을 생성하기 위한 키교환 메커니즘을 제시한다. 이 키교환 메커니즘은 IEEE 802.1aa와 연동이 되도록 설계하였다.

ABSTRACT

Wireless LAN in itself is vulnerable to eavesdropping and modification attack, and thus, IEEE 802.11i and IEEE 802.1x/1aa have been defined to secure the wireless channel. These protocols accompanied by RADIUS and EAP-TLS provide users of wireless LAN with integrity and confidentiality services, and also they perform authentication and access control of wireless ports. In this paper, we suggest a method to implement accounting session using authentication session of IEEE 802.1x and accounting state machine is designed with the accounting session. Also, we propose a key exchange mechanism to establish secure channel between stations and an access point. The mechanism is designed to be inter-operable with IEEE 802.1aa.

keyword : *Wireless LAN, IEEE 802.1x, IEEE 802.11i, accounting*

Ⅰ. 서 론

인터넷의 사용자의 급격한 증가와 함께 옥외에서도 인터넷을 사용하고자 하는 요구가 늘어났다. 이에 따라 2.4GHz 대역에서 핫스팟(hot spot)이라고 불리는 지역을 중심으로 무선랜 서비스가 시작되었다. 사업자가 공항이나 카페 등 사람들이 많이 모이는 지역에 Access Point(AP)를 설치해 놓으면, 가입자는 PCMCIA 또는 미니PCI 형태의 무선랜 카드를 이용해 노트북이나 PDA로 근처의 AP에 접속하여 인터넷을 서비스 받는 형태이다. 현재 IEEE 802.11b 표준을 따르는 무선랜 서비스는 최대 11Mbps의 전송속

* 인하대학교 정보통신대학원 정보보호연구실(nyang@inha.ac.kr)
** 한국전자통신연구원 무선인터넷보안연구팀({khoh, youskang, yhham, cbh}@etri.re.kr)
† 주저자, ‡ 교신저자, 논문접수일 : 2003년 7월 8일, 심사완료일 : 2003년 10월 22일

도를 지원하며, 최근 2.4GHz 대역에서 54Mbps를 지원하는 IEEE 802.11g 그리고 5GHz 대역에서 54Mbps를 지원하는 IEEE 802.11a의 표준화 작업이 완료되었다. 더 넓은 대역폭을 가지는 이들 표준을 따르는 제품의 출시는 무선랜 사용자의 증가를 촉진시킬 것으로 예상된다.

무선랜은 매체의 특성상 유선보다 메시지의 도청 및 변조가 쉬우며, 이를 위해 IEEE 802.11 에서는 WEP(Wired Equivalent Privacy)이라는 프로토콜을 정의하고 있다.[10] 하지만, 다수의 WEP 보안 취약점이 발견되었고, 이를 보완하기 위해 Working Group IEEE 802.11의 Task Group I에서 무선랜을 위한 새로운 보안 프로토콜을 설계하고 있다.[1] 또한 무선랜의 상용서비스를 위해서는 사용자 인증, 접근제어, 과금 등의 기능이 제공되어야하며, 이들 기능 중 일부는 IEEE 802.1x라는 표준을 통해 지원되고 있다.[2]

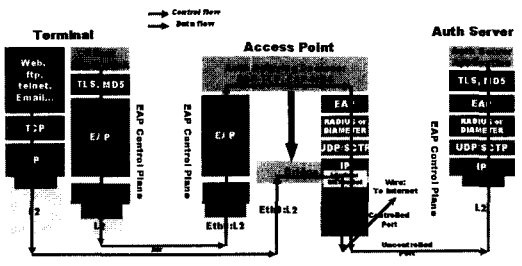
이 논문에서는 무선랜에 필요한 두 가지 보안 세션을 설계하는 방법을 제시한다. 하나는 무선랜의 상용서비스를 위해서 반드시 필요한 accounting을 위한 세션을 구현하는 것으로, IEEE 802.1x의 인증 세션을 이용해 accounting 세션 관리 모듈을 설계하는 방법을 제시한다. 이는 표준 state machine에 몇 가지 상태 변수를 추가함으로써 쉽게 구현할 수 있으며, 표준에 부합(conform)한다. 이와 함께 accounting 세션을 이용해 실제로 accounting을 수행하는 state machine을 제안한다. 다른 하나는 무선랜에서 AP와 스테이션간의 무선 보안 채널을 생성하기 위한 것으로, 이들 간의 키교환 메커니즘을 제시한다. 기본적으로 IEEE 802.11i를 따르며, IEEE 802.1aa와 연동이 되게 하였다.[3] 또한 병합될 수 있는 상태들을 합쳐서 state machine의 상태 개수를 줄임으로써 구현의 복잡도를 낮추었다. 그 외에도 에러처리를 위한 몇 가지 천이(transition)를 추가하여 키교환 state machine의 완성도를 높였다.

II. 무선랜 정보보호 시스템 개요

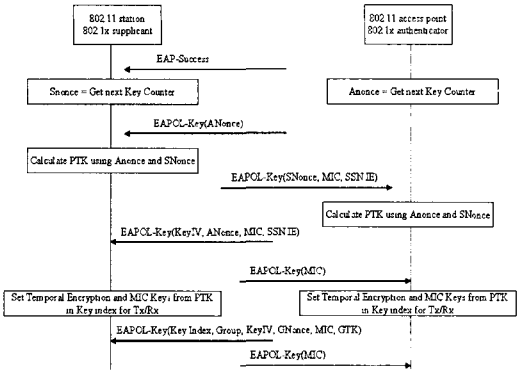
무선랜 정보보호 시스템은 포트기반 접근제어에 기초한 IEEE 802.1x, 무선구간 정보보호를 위한 IEEE 802.11i를 근간으로 한다. 여기서 IEEE 802.1x는 사용자 인증을 수행할 뿐만 아니라, 인증된 사용자의 트래픽만을 선택적으로 bridging하기 위한 방안을 제공한다. IEEE 802.1x에서는 사용자 인증을 위한 프레임 웍만을 제공하며, 인증 프로토콜에서 교환될 메시지를 전송하는 방법을 규정하고 있다. IEEE 802.1x에서 인증 프로토콜은 EAP(Extensible Authentication Protocol)를 사용하도록 하고 있으며, EAP는 특정 인증 프로토콜이 아닌 다양한 인증 프로토콜을 수용하는 구조를 가지고 있다.[5] 따라서 사용목적에 맞는 인증 프로토콜을 EAP의 상위에 올려서 인증 프로토콜을 구현할 수 있다. EAP를 이용한 인증 프로토콜로는 EAP-MD5, EAP-TLS(Transport Layer Security), EAP-TTLS(Tunneled TLS), EAP-PEAP(Protected EAP)등이 있으며, EAP-MD5는 인증만을 목적으로 하는 경우 그리고 강한 인증이 요구되지 않는 경우에 사용된다.[5,6,9,11]

IEEE 802.1x framework에서 스테이션은 supplicant, AP는 authenticator의 역할을 하며, 사용자 인증을 수행하는 개체(entity)는 인증 서버(backend authentication server)가 된다. 즉 인증 프로토콜에 참여하는 개체는 supplicant와 인증 서버가 되고, authenticator는 인증 프로토콜에 사용되는 메시지를 단순히 relay하는 역할만을 수행한다. 또한 authenticator는, 인증 절차가 완료되고 난 후 인증 서버로부터 인증 결과에 대한 메시지를 전달 받아 해당 사용자의 패킷을 bridging 할 것인지 말지를 port별로 제어하게 된다. 이때, authenticator와 인증 서버는 RADIUS(Remote Authentication Dial-In User Service) 프로토콜을 통해 제어메시지와 인증 메시지를 주고받게 된다.[7] 따라서 IEEE 802.1x를 통해 접근제어를 하려는 AP는 IEEE 802.1x에서 요구하는 EAP, EAPOL(EAP Over LAN), RADIUS 등의 프로토콜 스택을 가지고 있어야한다. [그림 1]은 스테이션, AP, 인증 서버의 프로토콜 계층간의 관계를 보여주고 있다.

EAP-MD5를 사용하는 경우, 스테이션과 인증 서버간의 키교환은 수행되지 않지만, EAP-TLS등의 프로토콜처럼 인증과 키교환을 동시에 수행하는 프로토콜을 사용하면 인증 절차가 완료되고 난 후 스테이션과 인증 서버는 비밀키를 공유하게 된다. 이렇게



〔그림 1〕 IEEE 802.1x 프로토콜 구조



〔그림 2〕 IEEE 802.11i Key handshake

공유한 비밀키를 이용해서 스테이션과 AP사이의 무선구간에 암호 채널을 설정하게 된다. 즉, backend authentication는 자신이 가지고 있는 비밀키를 안전한 방법으로 AP에게 전송하고, AP는 스테이션과 같은 비밀키를 공유하게 된다. 이렇게 공유한 비밀키 정보를 이용해서 IEEE 802.11i에서 정의하는 키교환 과정을 수행하면, 메시지 보호(confidentiality) 및 메시지 인증(integrity)를 위한 키가 생성된다. [그림 2]는 IEEE 802.11i에서 정의하는 4-way 핸드쉐이크 프로토콜을 설명하고 있다. 각자가 생성한 Nonce, 인증 서버와 공유하고 있는 비밀키 등을 이용해서 unicast 트래픽을 보호하기 위한 pairwise 세션 키, multicast 트래픽을 보호하기 위한 그룹 세션 키를 생성한다. 이들 세션 키는 각각 encryption 키와 MIC 키로 구성되며, 사용자가 login해서 logout할 때까지의 세션 동안만 사용된다. 또한, 관리명령(management action)에 의한 rekeying event가 발생할 때에 세션 키를 다시 교환하기도 한다.

조금 더 자세히 핸드쉐이크 과정을 살펴보면, IEEE 802.1x의 EAP-Success 메시지가 전송되면 이는 인증이 완료되었음을 의미한다. 따라서 AP는 자신의 nonce(=ANonce)를 스테이션에게 전송하고 스테이션은 자신의 nonce(=SNonce)와 ANonce를 이용해서 PTK를 계산한다. 이렇게 계산된 PTK를 이용해서 SNonce를 전송하는 메시지의 MIC(Message Integrity Check)을 계산해 AP에 전송한다. AP는 전송받은 SNonce와 자신의 ANonce를 이용해 PTK를 계산하고 전송되어 온 MIC를 확인한다. 맞다면, 초기벡터(Initialization Vector)를 스테이션에게 전송하고, 이에 대한 확인 메시지를 스테이션이 AP에 전송한다. 이렇게 해서 스테이션과 AP는 PTK의 핸드쉐이크 과정을 완료하게 된다.

Ⅲ. Accounting

IEEE 802.1x에는 인증 세션을 규정하고 있지만, accounting 세션에 대해서는 언급하고 있지 않다. 무선랜을 상업적으로 사용하기 위해서는 accounting이 필수적이다. 따라서 사용자의 무선랜 사용량에 따라 패킷 과금을 하거나 시간에 따라 과금을 해야 하고 이에 대한 정보의 수집은 AP에서 이루어져야한다. 따라서 AP내에 accounting을 위한 모듈을 구현해야한다. 이 절에서는 accounting 세션을 IEEE 802.1x의 인증 세션을 이용해 구현하는 방법을 제안하고, 이렇게 정의된 accounting 세션에 대한 accounting을 수행하기 위한 accounting state machine을 설계한다.

3.1 인증 세션을 이용한 accounting 세션의 구현

먼저 IEEE 802.1x의 인증 메커니즘을 간단히 살펴보자. IEEE 802.1x에서 인증은 여러 개의 state machine으로 정의되며, 이 state machine에는 Port Timer state machine, Authenticator PAE(Port Access Entity) state machine, Backend authentication state machine, Controlled Direction state machine 등이 있다.

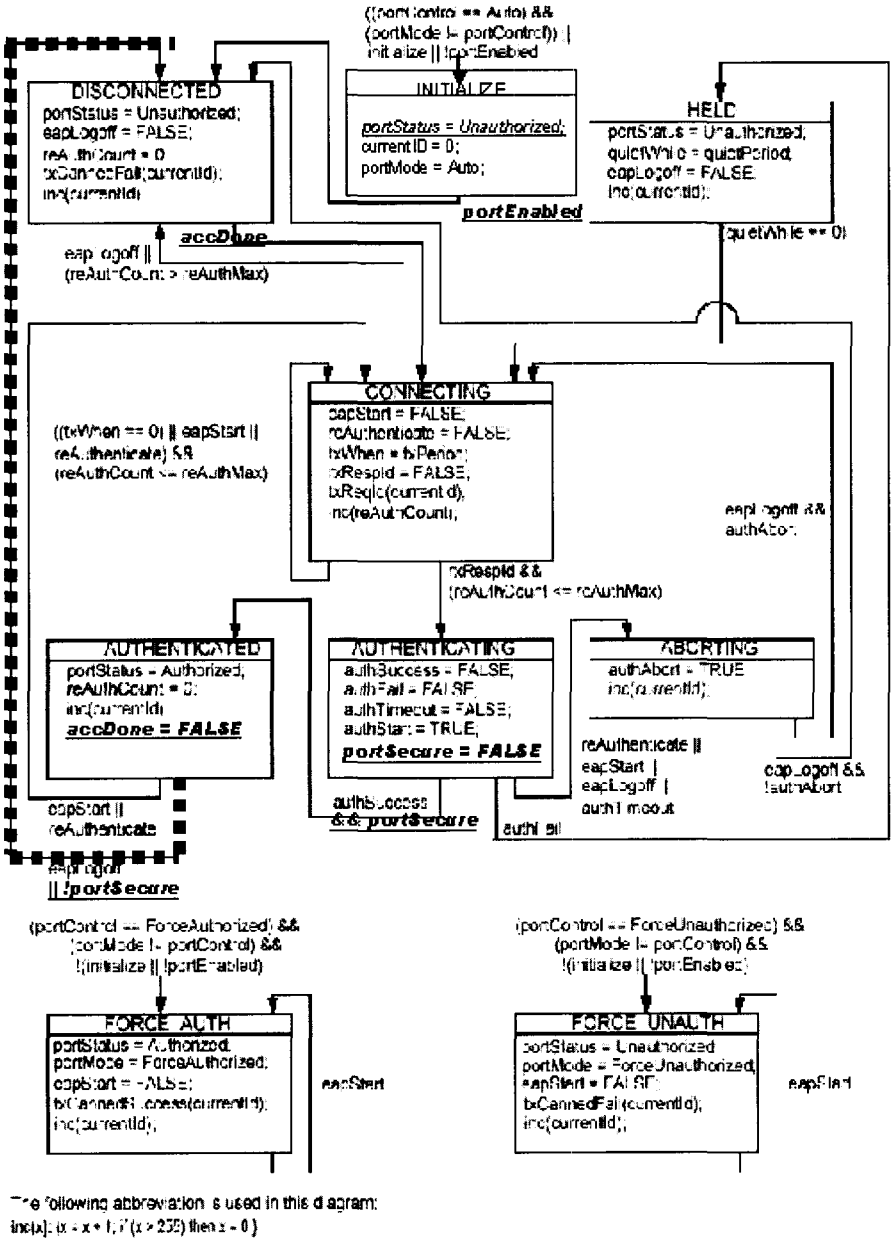
Port Timer state machine은 인증 과정 중 발생하는 오류 처리 대기 시간, 재전송 대기 시간 등의 관리를 위한 타이머를 유지한다. Authenticator PAE는 스테이션의 supplicant PAE와 함께 인증에 필요한 무선구간의 데이터를 주고받는 역할을 하며, Backend authentication state machine을 구동한다. Backend authentication state machine은 authentication PAE state machine에 의해 실행되어, 인증 서버와 RADIUS 패킷을 주고받으며 스테이션 인증을 수행하고 결과를 AP의 bridging module에 알려 해당 사용자로부터의 패킷을 bridging 할 것인지 drop 할 것인지를 결정하게 한다.

IEEE 802.1x의 인증 세션은 authentication PAE state machine의 상태 변화에 의해 정의 된다. 즉, AUTHENTICATED 상태에서 시작한 authentication 세션은 DISCONNECTED 상태가 되면 종료된다. 그 외의 모든 상태에서 인증 세션은 존재하지 않는다. accounting 세션은 기본적으로 인증 세션과 같은 lifetime을 가지므로, 인증 세션이 정의되는 상태 구간을 이용해서 accounting 세션을 정의한다.

accounting 세션의 시작과 함께 accounting이 처리되어야 하는데, 이 논문에서는 accounting state machine을 정의해서 처리하도록 했다. accounting을 위

한 state machine은 다음 절에서 설명한다.

accounting 세션의 시작과 끝을 정의하고 이를 accounting state machine에 알리기 위해 authentication PAE state machine에 accDone 이라는 상태변수를 추가한다. accDone은 TRUE 또는 FALSE 값을 가지는 boolean 변수로 accounting 세션이 활성화 되어있는 동안만 FALSE 값을 가진다. 즉, accounting 세션은 accDone이라는 변수에 의해 정의된다. 앞서 살펴본바와 같이 accounting 세션은 인증 세션과 같은 lifetime을 가지므로, authentication PAE state machine에서 인증이 완료된 상태에서 accounting 세션을 시작하고, 사용자가 logoff하거나 그외 다른 이유로 세션이 종료되는 경우 accounting 세션을 종료한다. 여기서 accounting 세션의 종료는 authentication PAE state machine에서보다는 accounting state machine에서 수행하는 것이 논리의 구성 면에서 더 편리하므로, accoun-



[그림 3] 인증 세션을 이용한 accounting 세션의 정의

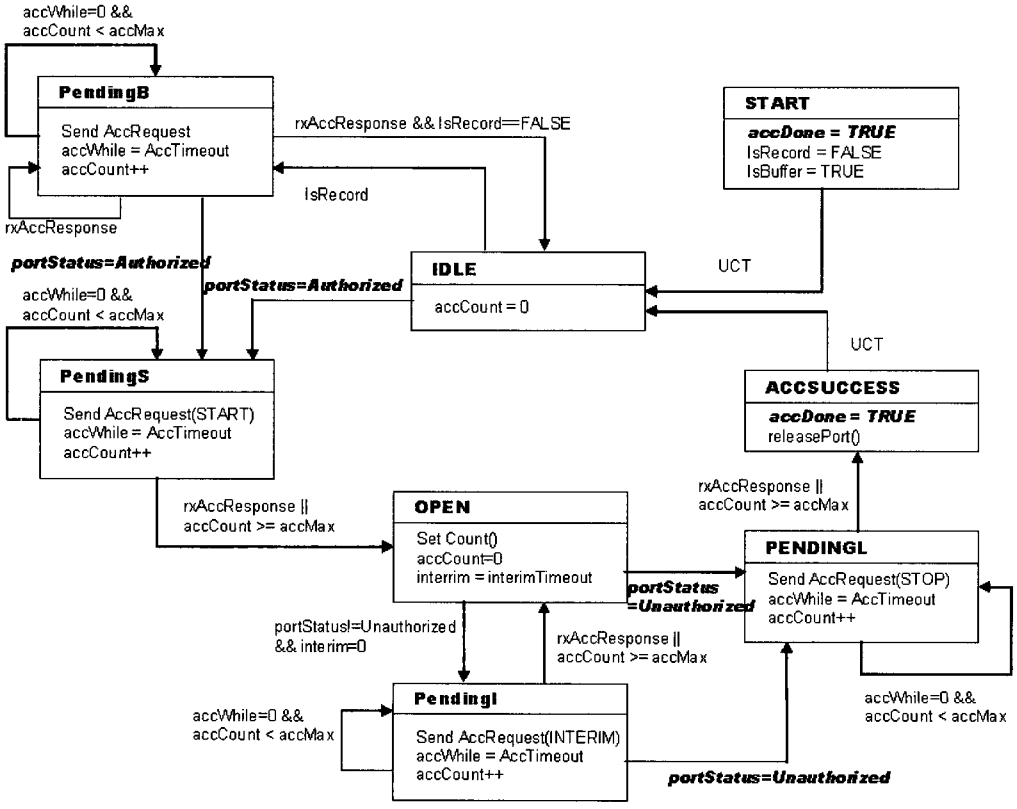
ting 세션의 종료를 위한 명령은 accounting state machine에 둔다.

인증 세션은 authentication PAE state machine이 AUTHENTICATED 상태가 될 때 시작된다. 따라서 여기에 accDone을 FALSE로 하는 명령을 추가한다. IEEE 802.1x의 authentication PAE state machine에서는 DISCONNECTED에서 CONNECTING 상태로의 천이가 UCT(UnConditional Transition)이지만, accounting을 위해서는 accounting state machine에 의해 accounting에 관련된 처리가 완료될 때까지 기다려야 하므로, accDone을 천이조건(transition condition)으로 대체한다. [그림 3]은 accounting 세션이 추가된 새로운 authentication PAE state machine을 보여주고 있다. 그림에서 굵은 점선으로 표시된 부분이 accounting 세션을 정의하고 있다. 즉, 사용자 인증이 완료되어서(AUTHENTICATED 상태) 접속이 해제된 상태(DISCONNECTED)까지가 하나의 accounting 세션이 된다.

또한, portSecure 라는 상태 변수를 추가해, IEEE 802.11i에서 교환된 키를 이용한 보안 채널이 설정되어있는지를 확인한다. 따라서 인증 또는 accounting 세션은 인증이 성공했음을 알리는 authSuccess 뿐만 아니라 보안 채널의 설정이 완료되었음을 알리는 portSecure 변수까지도 TRUE 값을 가질 때 시작된다. 비슷하게, 인증 또는 accounting 세션의 종료는 eapLogoff가 TRUE 값을 가지거나 portSecure가 FALSE 값을 가지면 종료된다.

3.2 Accounting state machine의 설계

이 절에서는 authentication PAE state machine에 의해 구동된 accounting 세션을 처리하는 state machine을 제안한다. authentication PAE state machine에서 사용자 인증이 완료되면, accounting을 시작해야한다. accDone이 FALSE가 됨으로써 accounting state machine을 시작한다. accounting state machine은 backend authentication state machine이 RADIUS 서버와 인증을 위한 패킷을 주고받는 것처럼 accounting을 위한 RADIUS 패킷을 RADIUS 서버와 주고받는다. [그림 4]는 제안하는 accounting state machine이다.



〔그림 4〕 Accounting state machine

accounting state machine이 IDLE상태에 있을 때 사용자 인증이 완료되면 포트상태변수(PortStatus)가 "인증완료(Authorized)"값을 가지며, accounting state machine은 PendingS 상태가 된다. PendingS 상태에서 accounting 서버의 응답(rxAccResponse)을 받으면 OPEN 상태가 되어 accounting이 시작된다. 이 상태에서 미리 정의된 시간(Interim)이 경과하면 클라이언트는 PendingI 상태가 되어, accounting을 위한 interim 패킷을 주기적으로 전송한다. OPEN 이나 PendingI 상태에서 포트가 "비인가(Unauthorized)" 값을 가지면 인증 세션이 종료되었음을 의미하므로 클라이언트는 PendingL 상태가 되어 마지막 accounting 패킷을 전송하고, 여기서 응답패킷을 받으면 ACC_SUCCESS 상태에서 accDone을 TRUE로 함으로 accounting 세션을 종료하게 된다. 즉 accounting 세션은 accounting state machine의 IDLE 또는 PendingB 상태에서 출발하여 PendingS, OPEN, PendingI, PendingL를 거쳐 ACC_SUCCESS 상태에서 종료된다.

accounting 처리가 완료되기를 기다리며 DISCONNECTED 상태에 머물러 있던 authentication PAE state machine은 accounting state machine에 있는 ACC_SUCCESS 상태의 accDone=TRUE 이벤트에 의해 CONNECTING 상태로 이동하고, 다시 새로운 인증을 수행한다.

PendingS, PendingI, PendingL 상태에서 클라이언트가 정해진 횟수만큼 accounting 패킷을 전송했음에도 accounting 서버로부터 응답 패킷을 받지 못하면 accounting 패킷을 버퍼에 저장 후 다음 상태로 진행한다. 버퍼에 저장된 accounting 패킷은 PendingB 상태가 되면 가장 오래된 패킷 순서대로 다시 전송되고 서버의 응답이 오면 버퍼에서 지워진다.

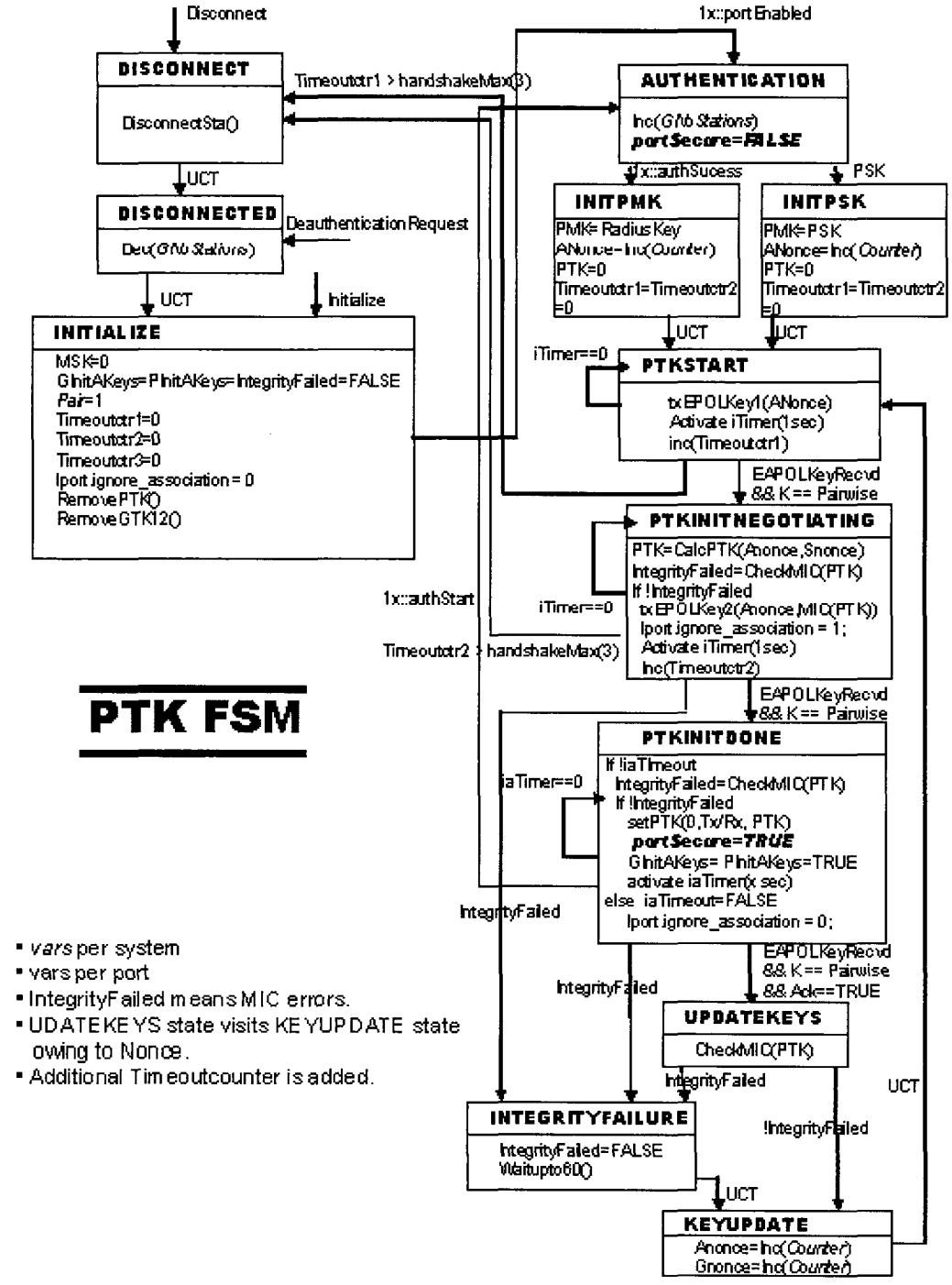
Ⅳ. IEEE 802.11i를 위한 키교환 state machine

EAP-TLS 등을 통한 인증이 끝난 후, 스테이션과 인증 서버는 비밀키를 공유하게 된다. 이렇게 공유한 비밀키는 무선구간의 정보보호를 위해서 사용되어야 하므로, 인증 서버로부터 RADIUS 패킷 형태로 AP에 전송된다. 이때 전송 채널은 미리 분배된 비밀키로 보호되어있다. 여기서 사용되는 RADIUS 패킷은 속성으로 MPPE(Microsoft Point-to-Point Encryption)를 가지며, 이 MPPE 속성을 이용해 AP로 스테이션과 인증 서버간에 공유된 키가 전송된다.[12] 스테이션과 AP 사이에 공유된 이 비밀키를 이용해 무선구간 보호를 위한 세션키를 생성하기 위해서 4-way 핸드쉐이크 프로토콜을 수행한다.

이 절에서는 이 4-way 핸드쉐이크 프로토콜을 수행하는데 필요한 키교환 state machine을 설계한다. 기본적으로 IEEE 802.11i를 따르며, portSecure 변수를 도입해서 IEEE 802.1x 와 연동이 되게 하였다. portSecure 변수가 TRUE인 조건을 추가하여 IEEE 802.11i의 키교환 과정이 완료된 후에 IEEE 802.1x의 인증 세션이 시작되도록 하였다. portSecure 변수의 초기화는 AUTHENTICATION상태에서 이루어지며, 키교환이 완료되었을 때 PTKINITDONE 상태에서 TRUE로 설정한다. 또한 병합될 수 있는 상태를 줄여서 state machine의 상태 개수를 줄임으로써 구현의 복잡도를 낮추었다. 그 외에도 에러처리를 위한 몇 가지 천이를 추가하여 키교환 state machine의 완성도를 높였다.

핸드쉐이크 프로토콜을 수행하기 전, 스테이션과 AP가 공유하는 키를 PMK(Pairwise Master Key)라고 하며, 이 PMK와 Nonce, 각자의 MAC(Media Access Control) 주소 등을 이용해 pairwise 세션 키, 그룹 세션 키를 생성한다.

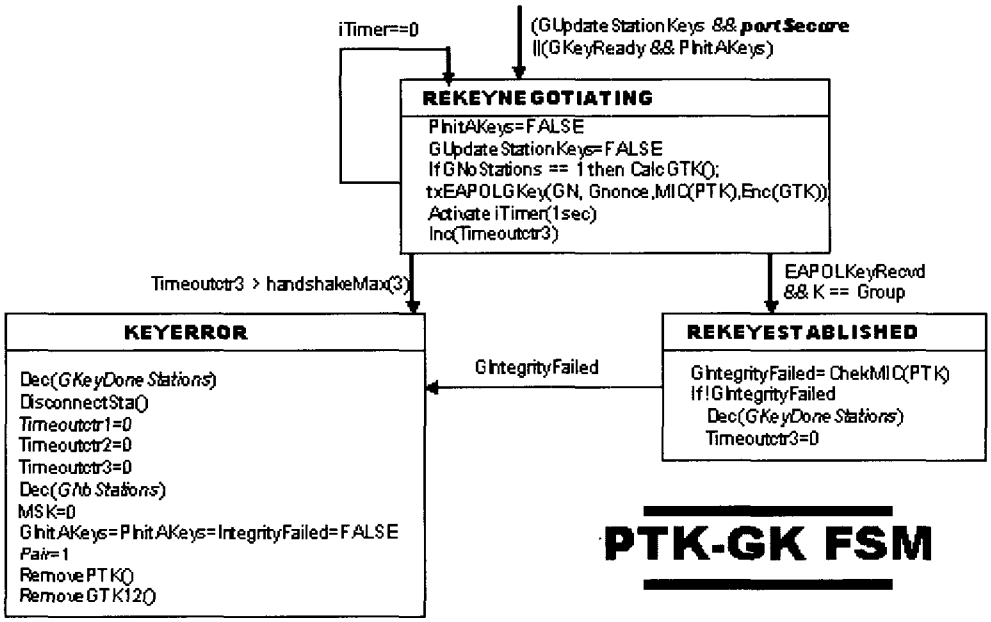
[그림 5]는 이 논문에서 제안하는 키교환 state machine이다. 우선 스테이션의 MAC이 활성화되면 AUTHENTICATION 상태로 천이하고, AP가 관리하는 스테이션의 수를 가지고 있는 global 변수인 GNoStations를 증가시킨다. IEEE 802.1x의 인증을 성공적으로 마치면 PMK를 초기화하는 INITPMK 상태로 이동한다. 이후에는 PTKSTART에서부터 PTKINITDONE 상태까지 이동하며 4 way 핸드쉐이크를 수행한다. 이 상태를 거치는 동안 핸드쉐이크를 위해 필요한 메시지를 주고받고 무선구간 보안을 위한 세션키들을 생성한다. 핸드쉐이크를 위한 메시지 흐름은 2절을 참고한다. [그림 5]에서 txEAPOLKey1()과 txEAPOLKey2()는 각각 키교환 핸드쉐이크에서 AP가 전송하는 첫 번째 메시지 두 번째 메시지를 전송해주는 함수이다. 또한 lport.ignore_association은 스테이션의 NIC(Network Interface Card)가 reboot되는 경우에 이미 associate되어 있는 상태에서 다시 association이 일어나지 못하도록 하는 변수이다. UPDATEKEYS와 KEYUPDATE 상태는 세션이 종료되기 전에 키를 갱신하기 위해 존재한다. 그림에서 이탤릭으로 표시된 변수들은 시스템에 하나만 존재하는 변수이고, 다른 것들은 포트별로 하나씩 존재하는 변수들이다.

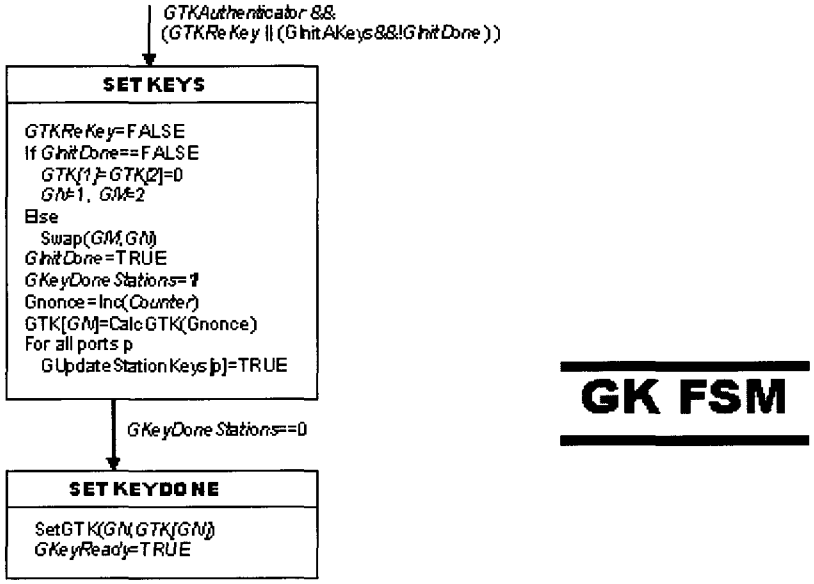


〔그림 5〕 Pairwise 키 교환을 위한 state machine

이 절에서는 pairwise 키를 위한 state machine과 그룹 키를 위한 state machine을 분리해서 설계함으로써 구현에 있어서 혼란을 피하도록 했다. PTK state machine에 있는 PTKINITDONE 상태의 GInitAKeys =TRUE 이벤트에 의해 GTK state machine이 실행된다. GTK state machine은 현재 AP에 associate 되어있

는 모든 스테이션에 그룹 세션키를 분배하고, AP의 그룹 세션키를 설정한다. 하나하나의 스테이션에 그룹 세션키를 분배하는 일은 PTK-GK state machine이 담당하며, GTK state machine의 SETKEYS 상태에 있는 GUpdateStationKeys[all ports]=TRUE 이벤트에 의해 구동된다. AP는 자신의 PTK-GK state machine에서, 이미 설정된 pairwise 키를 이용해서 새로이 생성된 그룹키를 암호화해서 전송한다. 각 스테이션은 해당 pairwise 키를 이용해 그룹키를 복호화하고 이를 확인한다. [그림 6]은 새롭게 정의한 GTK state ma-





〔그림 6〕 그룹키 교환을 위한 state machine

chine과 PTK-GK state machine이다. GK state machine의 SETKEYS 상태에서 GKeyDoneStations=1 명령은 원래 GKeyDoneStations=GNoStations 이던 것을 DoS 공격을 막기 위해 수정했다. 이에 대한 설명은 다음 절에서 기술한다.

그룹 키교환을 위한 state machine의 동작을 쉽게 이해하기위해 몇 가지 동작 시나리오를 살펴보자.

4.1 첫 번째 스테이션의 그룹키 분배 시나리오

1. 첫번째 STA가 인증을 완료하고, PTK에 의해 키 교환까지 완료되면 GInitAKeys = TRUE, PInitAKeys =TRUE에 의해 GK/PTK-GK가 구동된다.
2. PTK-GK는 구동되지만 아직 GKeyReady가 FALSE 이므로 아무 행동 없이 return한다.
3. GK는 GTKAuthenticator는 항상 TRUE, GInitAKeys가 방금 TRUE가 되었고, GInitDone은 초기값이 FALSE 이므로 SETKEYS 상태로 천이한다.
4. GK는 SETKEYS의 명령을 수행하며 마지막 명령인 GUpdateStationKeys = TRUE for all port 에 의해 모든 포트의 PTK-GK를 구동한다.
5. PTK-GK는 GUpdateStationKeys가 TRUE가 되었으므로, REKEYNEGOTIATING 상태로 천이한다.
6. PTK-GK는 Group키를 포함하는 EAPOL-key packet을 전송하고, 응답을 기다린다. 응답이 정상적으로 수신되면 REKEYESTABLISHED 상태로 천이한다.
7. PTK-GK는 GKeyDoneStations-- 를 수행하므로써, GKeyDoneStations == 0으로 만들고 다시 GK를 구동한다.
8. GK는 SETKEYSDONE 상태로 천이하고, 그룹 키를 설정한다. 또한 GKeyReady를 TRUE로 변경한다.

4.2 두 번째 스테이션의 그룹키 분배 시나리오

1. 두번째 STA가 인증을 완료하고, PTK에의해 키교환까지 완료되면 GInitAKeys = TRUE, PInitAKeys = TRUE에 의해 GK/PTK-GK가 구동된다.
2. GK는 구동되지만, 이미 초기화가 한번 되었었기 때문에 (GInitDone=TRUE), 아무 행동 없이 return 한다.
3. PTK-GK는 PInitAKeys=TRUE에의해 구동되었고, GKeyReady=TRUE 이므로(첫번째 STA의 그룹 키 분배에 의해) REKEYNEGOTIATING으로 천이한다.
4. PTK-GK는 그룹 키 분배 교환 프로토콜을 수행한다.
5. PTK-GK는 GKeyDoneStations-- 를 수행하므로써, GKeyDoneStations==0으로 만들고 다시 GK를 구동한다.
6. GK는 SETKEYSDONE 상태로 전이하고, 그룹 키를 설정한다. 또한 GKeyReady를 TRUE로 변경한다.

4.3 IV space exhaustion 또는 관리명령에 의한 rekeying scenario

7. GTKReKey=TRUE가 설정되므로 GK가 구동되고, GK는 SETKEYS 상태로 천이한다.
8. 새로운 Group 키를 생성하고, GUpdateStationKeys = TRUE for all port에 의해 모든 STA의 PTK-GK를 구동한다.
9. 각 포트의 PTK-GK는 그룹 분배 프로토콜을 수행하고, GKeyDoneStations-- 를 수행한다.
10. 모든 포트에 대해 PTK-GK가 수행완료되었을때 GKeyDoneStations=0이 되므로 GK가 구동된다.
11. GK는 SETKEYSDONE 상태로 천이하고, 그룹 키를 설정한다.

V. 구현의 복잡도 평가

이 논문에서 제안한 accounting 세션은 무선랜의 상용 서비스를 위해 반드시 필요한 요소로써, accounting 세션의 구현 방안을 제시했다는데 의의가 있다. 또한 이를 구현하는데 있어서 이미 존재하는 인증 세션에 하나의 상태변수(accDone)만을 추가해서 구현할 수 있음을 보였다. 이렇게 하므로써 accounting 세션 구현의 복잡도를 최소화했다. 또한 무선랜에서 사용가능한 accounting state machine을 설계하고, 하나의 상태변수(accDone)만을 이용해서 authentication PAE state machine의 인증 세션을 accounting state machine과 연결하므로써 구현의 복잡도를 줄였다.

IEEE 802.1x는 무선랜을 위해서 설계된 프로토콜이 아니므로, 최근에 IEEE 802.1aa라는 이름으로 무선랜을 고려한 IEEE 802.1x의 amendment가 제정되고 있다. 현재 제정되고 있는 IEEE 802.11i는 IEEE 802.1x를 이용하고 있고, 이에 따라 IEEE 802.1aa와 정확히 연동되지 못하고 있다. 이 논문에서 제시한 키교환 state machine은 IEEE 802.1aa와 연동할 수 있으며, 이를 위해 하나의 상태변수(portSecure)만을 이용해서 구현의 복잡도를 최소화했다. 또한, 여기서

제안한 키교환 state machine은 IEEE 802.11i의 상태를 병합하므로써 더 작은 수의 상태 개수를 가지도록 했다. 그 이외에도 정상적인 이벤트가 발생하지 않는 경우의 천이도 포함하므로써 키교환 state machine이 오류상황에서도 정상적으로 동작하도록 설계했다.

마지막으로, 그룹키 교환 state machine에 대한 DoS (Denial of Service) 공격 취약점을 찾아내고, 이를 보완했다. IEEE 802.11i에서 정의하는 그룹키 교환 state machine은 그룹키 교환에 협조적이지 않은 스테이션이 존재할 때 그룹키 교환 전체가 수행되지 않는 버그가 존재한다. 즉, 그룹키 state machine의 SETKEYS 상태에서 SETKEYDONE 상태로 천이하기 위해서는 GKeyDoneStations가 0이 되어야하는데, 이 상태변수는 SETKEYS 상태에서 현재 AP에 associatiate되어있는 스테이션의 수로 초기화 된다. 따라서, 이들 중 하나의 스테이션이라도 그룹키 교환에 협조하지 않는다면 AP는 그룹키를 설정할 수 없게 되고 이는 Basic Service Set 내의 통신을 불가능하게 한다. 이를 보완할 수 있는 방안을 매우 간단한 방법으로 제시하므로써(SETKEYS 상태의 GKeyDoneStations=1 명령), 그룹키 교환을 이용한 DoS 공격에 견딜 수 있도록 설계했다.

이런 여러 가지 기능의 추가를 위해 소비한 시스템 자원은 최소화 되어 있으며(2개의 상태 변수 추가), accounting 기능의 경우 또 하나의 state machine을 추가하는 형태로 정의하므로써 기존의 소프트웨어 구조에 accounting 기능의 추가를 용이하게 했다.

Ⅵ. 결론 및 향후 연구방향

이 논문에서는 무선랜의 상용서비스를 위한 정보보호 기술들을 제시했다. 먼저 accounting 세션을 효율적으로 구현하고 관리하기 위한 방법을 IEEE 802.1x의 인증 세션을 이용해 제안하고, 이를 이용해 accounting을 수행하기 위해 accounting state machine을 설계했다. 또한, 무선 구간의 정보보호를 위해서 정의된 IEEE 802.11i의 키교환 state machine을 보완하여 DoS 공격에 강하도록 했고, IEEE 802.1aa와의 연동이 가능하도록 정의했다. 새로운 기능의 추가와 안전성 강화를 위해 드는 비용을 최소화하기 위해 상태변수 및 새로운 state machine의 추가만을 요구하도록 설계했다. 이 논문에서 제안한 state machine들을 이용하면 IEEE 802.1x 및 IEEE 802.11i를 지원하고 accounting 기능이 있는 AP를 개발할 수 있다.

향후에는 IEEE 802.11f를 이용한 security context 정의에 대한 연구가 필요하다.[4] 현재는 reassociate request 메시지를 이용하는 IEEE 802.11f의 smooth한 handover를 지원하지 않으므로, 핸드오버가 일어나는 경우 IEEE 802.1x 인증과정 및 IEEE 802.11i의 키교환 과정을 다시 수행해야한다. 이는 핸드오버 절차를 매우 더디게 하여 seamless 핸드오버를 막는 장애요인이 된다. IEEE 802.11f에서는 reassociate request 메시지를 이용하며, AP 사이에 QoS 및 보안과 관련된 정보를 주고받을 수 있도록 프로토콜을 정의함으로써 seamless 핸드오버가 가능하도록 했다. 하지만, 재인증을 피하기 위해 어떤 정보를 주고 받아야하는지에 대해서 IEEE 802.11의 task group f에서는 정의하고 있지 않으므로 이에 대한 연구가 필요하다. 이를 위해서는 가능한 적은 계산량과 작은 크기의 메시지를 이용하여야 하며, 안전성의 측면도 고려해 정의해야한다.

또한, 인증 서버와 authenticator 사이의 AAA(Authentication, Authorization and Accounting)에 RADIUS 대신 DIAMETER를 이용하는 것에 대한 연구도 필요하다.[8] 현재는 AAA 서비스를 위해 RADIUS를 사용하고 있지만, 네트워크 환경의 변화에 따라서 기능상의 제약 및 성능의 문제로 RADIUS가 더 이상 좋은 해결책이 아닐 수 있고, 이는 DIAMETER라는 peer-to-peer 프로토콜을 이용해 효과적으로 대체할 수 있을 것이다.

마지막으로, 제안하는 메커니즘에 대한 정확성(correctness), 안정성(reliability, stability) 등에 대한 formal한 평가가 필요하다.

참 고 문 헌

[1] Draft Amemdment to STANDART FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control(MAC) and physical layer(PHY) specifications: Specification for Enhanced Security, IEEE Std 802.11i/D5.0, August 2003

[2] Standards for Local and Metropolitan Area Networks: Standard for Port based Network Access Control, P802.1X/D11, March 27, 2001

[3] Draft IEEE Standard for Local and Metropolitan Area Networks - Port Based Network Access Control-

Amendment 1: Technical and Editorial Corrections, IEEE Draft P802.1aa/D5, February 27, 2003

[4] Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, IEEE P802.11F/D5, January, 2003.

[5] RFC 2284, PPP Extensible Authentication Protocol (EAP). L. Blunk, J. Vollbrecht. March 1998.

[6] RFC 2716, PPP EAP TLS Authentication Protocol. B. Aboba, D. Simon. October 1999.

[7] RFC 2138, Remote Authentication Dial In User Service (RADIUS). C. Rigney, A. Rubens, W. Simpson, S. Willens. April 1997.

[8] Internet Draft, DIAMETER Base Protocol, Pat R. Calhoun, John Loughney, Eric Guttman, Glen Zorn, Jari Arkko, December 2002.

[9] Internet Draft, EAP Tunneled TLS Authentication Protocol(EAP-TTLS), Paul Funk, Simon Blake-Wilson, November 2002.

[10] Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control(MAC) and physical layer(PHY) specifications, 1997

[11] Internet Draft, Microsoft's PEAP version 0, Vivek Kamath, October 2002.

[12] RFC 3078, Microsoft Point-to-Point Encryption, G. Pall, G. Zorn, March 2001.

〈著者紹介〉

양 대 헌 (DaeHun Nyang)
1994년 2월 : 한국과학기술원 과학기술대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 8월 : 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 재직
2003년 3월~현재 : 인하대학교 정보통신대학원 전임강사
<관심분야> 암호이론, 암호프로토콜, 네트워 보안 프로토콜

오 경 희 (KyungHee Oh)
1999년 2월 : 연세대학교 컴퓨터 과학과 졸업
2001년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 12월~현재 : 한국전자통신연구원 무선인터넷보안연구팀 연구원
<관심분야> 암호프로토콜, 무선랜 보안

강 유 성 (You Sung Kang)
1997년 2월 : 전남대학교 전자공학과 졸업
1999년 8월 : 전남대학교 전자공학과 석사
1999년 11월~현재 : 한국전자통신연구원 무선인터넷보안연구팀 연구원
<관심분야> 암호 프로토콜, 무선랜 보안, 스마트카드

함 영 환 (YoungHwan Ham)
1994년 2월 : 성균관대학교 컴퓨터공학과 졸업
1996년 2월 : 성균관대학교 컴퓨터공학과 석사
1995년 12월~1999년 10월 : 한국전자통신연구원 슈퍼컴퓨터 센터 연구원
2000년 6월~2001년 10월 : (주) 이니텍 연구원
2001년 12월~현재 : 한국전자통신연구원 정보보호연구본부 연구원
<관심분야> 네트워 보안 프로토콜, 무선인터넷 보안

정 병 호 (Byungho Chung)
1988년 2월 : 전남대학교 전산통계학과졸업
2000년 2월 : 충남대학교 컴퓨터 과학과 석사
2000년 3월~현재 : 충남대학교 컴퓨터 과학과 박사수료
1998년 2월~2000년 6월 : 국방과학연구소 선임연구원
2000년 6월~현재 : 한국전자통신연구원 무선인터넷보안연구팀 팀장
<관심분야> 무선/이동 QoS, MONET Security, 네트워 보안 프로토콜