한국ITS학회논문지
제8권, 제6호 (2009년 12월)
pp. 112~120

Wireless LAN(IEEE 802.11)에서 인증시간 단축을 위한 보안 메커니즘에 관한 연구

A Study on the Security Mechanism to Reduce Authentication Time in Wireless LAN(IEEE 802.11)

홍 경 식* 서 종 수** 고 광 용*** 정 준 하**** 이 철 기*****
(Kyung-Sik Hong) (Jong-Soo Seo) (Kwang-Yong Ko) (Jun-Ha Jung) (Choul-Ki Lee)

요 약

무선랜을 ITS에 적용하기 위해서는 무선 구간 보안성 향상과 이동성 지원을 위한 빠른 접속이 요구된다. 그러나 IEEE 802.11i 보안 표준을 적용하는 경우 보안 강화를 위한 IEEE 802.1X 사용자 인증 및 4-Way handshake 과정을 수행함으로써 접속 지연이 발생하여 ITS에 그대로 적용하기에는 무리가 있다. 본 논문에서는 이러한 문제를 해결하기 위해 Key Table을 이용한 Password 인증 및 데이터 암호화 메커니즘을 제안하고, 성능 분석을 통해 검증하였다.

Abstract

Both security enhancement in wireless and fast access for mobility are required to employ wireless LAN in ITS (Intelligent Transportation Systems). However, for the case of employing IEEE 802.11i security standard, it is known that the user authentication procedure of IEEE 802.1x and 4-way handshake procedure for stronger security enforcement may not be suitable for ITS due to its large delay. In this paper, we propose fast authentication method to resolve the above authentication delay problem, and verify its performance via simulation analysis.

Key words: IEEE 802.11, IEEE 802.1X, IEEE 802.11i, authentication, security, access time

* 주저자 : 도로교통공단 교통과학연구원 연구원
** 공저자 : 연세대학교 전기전자공학과 교수
*** 공저자 : 도로교통공단 교통과학연구원 선임연구원
**** 공저자 : 도로교통공단 교통과학연구원 수석연구원
***** 공저자 : 아주대학교 ITS대학원 교수
† 논문접수일 : 2009년 10월 13일
† 논문심사일 : 2009년 11월 10일
† 게재확정일 : 2009년 11월 11일

Ⅰ. 서 론

현재 국·내외에서는 Wireless LAN을 ITS에 적용하여 실시간 교통정보 수집제공시스템을 구현하고자 하는 연구가 활발히 이루어지고 있다. Wireless LAN을 활용하여 ITS에 적용하기 위해서는 무선 구간 보안성 향상과 이동성 지원을 위한 빠른 접속이 요구되나, IEEE 802.11i 등 강력한 보안 표준을 적용하게 되면 사용자 인증 및 데이터 보안을 위한 Key 교환절차 과정을 거치게 되는데, 이는 접속 지연 요소로 작용하여 ITS에 그대로 적용하기에는 무리가 있다고 할 수 있다.

ITS에 무선 통신기술을 적용하기 위한 접속시간 요구 조건을 교통공학의 측면에서 분석해보면 일반적으로 차로별 포화차두시간은 2 sec로써 일반적인 도로 형태를 편도 3차로의 4지 교차로 기준으로 설정하면 12대의 차량이 교차로 중심을 향해 동시 진입할 수 있다고 가정할 수 있으며, 12대의 STA를 장착한 차량이 2 sec 이내에 접속이 완료되기 위해서는 산술적으로 개별 STA은 최소 167 msec 이내에 접속이 완료되어야 한다고 할 수 있다.

본 논문에서는 167 msec 이내에 인증을 포함한 IEEE 802.11 접속을 보장하고, 무선을 사용하는 Wireless LAN의 취약점인 보안 관련 문제를 해결하기 위하여 STA과 AP 간의 보안 접속 메커니즘을 개선하였다.

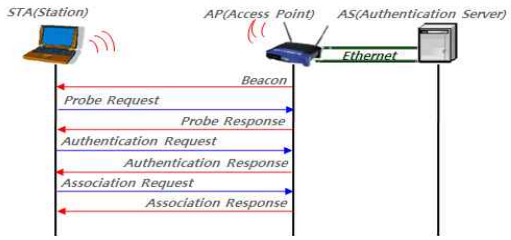
본 논문의 제2장에서는 IEEE 802.11의 접속절차와 보안 표준 및 이동성 지원을 위한 IEEE 표준 및 관련 연구를 검토하고, 제3장에서는 인증 시간 단축을 위하여 Key Table을 이용한 Password 인증 및 데이터 암호화 메커니즘에 대하여 제안하였다. 그리고 제4장에서는 IEEE 802.11i 보안 표준과 본 논문의 제안 방식에 대한 인증 소요시간 비교 시험을 진행하였다.

Ⅱ. 관련 연구 고찰

1. IEEE 802.11 접속 절차 및 보안

1) IEEE 802.11 접속 절차 [1]

IEEE 802.11 표준에서 정의된 접속 절차는 <그림 1>과 같이 ① 채널 탐색 과정(Beacon/Probe), ② 인증 과정(Authentication) ③ 연결 설정 과정(Association)으로 이루어진다.



<그림 1> IEEE 802.11 접속 절차
<Fig. 1> The access process of IEEE 802.11

2) IEEE 802.11 보안 요소

802.11 표준을 제정한 IEEE와 Wi-Fi Alliance 등과 같은 단체에서 Wireless LAN 보안 강화를 위해서 발표한 표준 및 방안들은 크게 Wireless LAN에서의 장치/사용자 인증(Authentication) 부분과 안전한 데이터 전송을 위한 데이터 암호화(Encryption) 부분으로 구분되어진다.

2. IEEE 802.1X

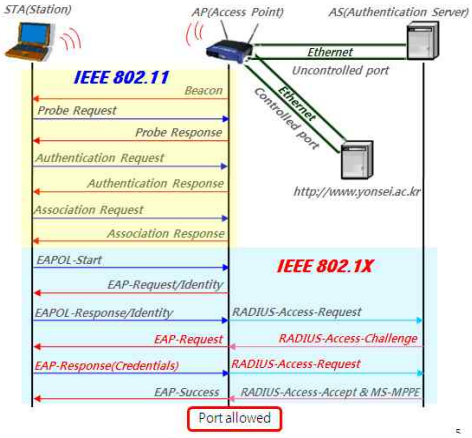
IEEE 802.1X는 논리적으로 포트를 제어하는 개념을 도입하여 링크계층에서 IEEE 802 LAN을 인증하는 메커니즘에 관한 표준으로 제정된 것이다. 즉, Wireless LAN 뿐만 아니라 이더넷, 토큰링 등 전체적인 인증관련 Framework이다 [2, 3].

1) IEEE 802.1X 인증 구성 요소

IEEE 802.1X 표준을 구현하기 위해서는 요청자(Supplicant), 인증자(Authenticator), 인증서버(Authentication Server)의 3가지 구성요소가 필요하며 일반적인 인증서버로는 RADIUS가 많이 사용되고 있다.

2) IEEE 802.1X 인증 절차

IEEE 802.1X 인증 프로토콜 진행의 전체적인 흐름은 <그림 2>와 같다.



<그림 2> IEEE 802.1X 인증 절차 흐름도
<Fig. 2> IEEE 802.1X authentication process flow

확장 가능한 EAPOL(Extensible Authentication Protocol Over LAN) 프로토콜을 사용하여 사용자를 인증하며, <그림 2>의 절차에 따라 인증이 완료되면 Port를 개방하여 접속을 허용하는 방식이다.

이러한 IEEE 802.1X 규격은 Wireless LAN 구조의 관리에서 허가를 얻은 사용자와 장치에게만 서비스를 제공하기 위해서 포트 기반의 네트워크 접속 제어 구조를 통해 인증을 하는 것으로 인증 성공 이후에 무선 구간에서 송수신되는 데이터에 대한 암호화에 대한 대비는 하지 못하게 되는 단점이 존재하게 된다 [2].

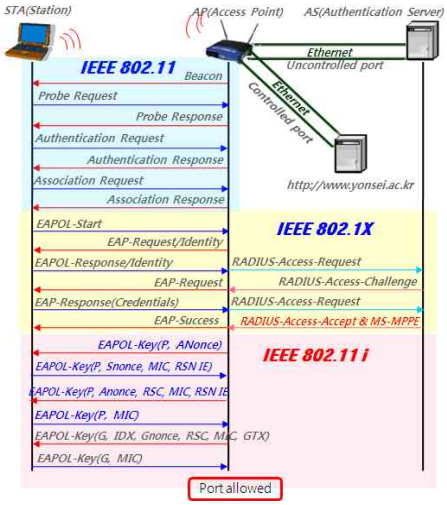
3. IEEE 802.11i [4]

IEEE 802.11i 표준은 Wireless LAN의 동일한 BSS(Basic Service Set) 내에서 AP와 STA 사이에 ① 사용자 인증 방식과 ② 키 교환 절차 및 ③ 강력한 무선구간 데이터 암호화 절차를 정의하여 RSN (Robust Security Network)를 구축하여 Wireless LAN 사용자를 보호를 목표로 표준화 되었다 [5].

IEEE 802.11i 표준에서 정의한 전체적인 보안 접속 절차는 <그림 3>과 같다.

1) IEEE 802.11i 인증 방식 및 키 교환 절차

IEEE 802.11i 표준에서는 필수 인증 방식으로



<그림 3> IEEE 802.11i 보안 절차
<Fig. 3> IEEE 802.11i security process

IEEE 802.1X를 정의하고 있으며, 또한 사전 공유키 (Pre-Shared Key) 인증 방식을 옵션으로 정의하여 별도의 인증 서버가 필요 없이 AP와 STA이 미리 특정한 키를 공유하여 바로 4-Way Handshake 과정을 거쳐 일대일 대칭 키를 교환하고 그 결과를 참조하여 포트를 제어하는 방식이 제시되었다.

IEEE 802.11i 표준에서의 키 교환 절차는 4-Way Handshake 방식으로 설명된다. IEEE 802.1X 인증이 성공한 후 인증서버로부터 Radius-Access-Accept & MS-MPPE(PMK)를 통하여 받은 PMK(Primary Master Key)를 이용하여 해당 통신 세션 과정에서 사용할 일대일 대칭키(PTK, Pairwise Transient Key) 및 그룹키(GTK, Group Transient Key)를 교환하게 된다 [4].

2) IEEE 802.11i 암호화 알고리즘

IEEE 802.11i에서는 데이터 보호를 위해 WEP (Wired Equivalent Privacy) 이외에 접속 과정에서 AP와 STA 사이에서 설립된 암호화 키를 사용하는 TKIP(Temporal Key Integrity Protocol)와 CCMP(Counter mode with CBC-MAC Protocol)를 정의하고 있다. TKIP은 기존의 WEP을 확장하는 방법을 적용하고, 프레임마다 MIC(Message Integrity Code)을 포함하도록 하여 H/W의 변경 없이 구현이 가능하도록 하였

으며, CCMP는 CCM 모드를 사용하는 AES(Advanced Encryption Standard) 암호 알고리즘을 사용하도록 규정하고 있다 [5].

3) IEEE 802.11i 사전 인증

IEEE 802.11i 보안 표준에서는 STA의 고속 로밍 지원을 위한 옵션으로서 ① 키 캐싱(Key Caching) 과 ② 사전인증(Pre-Authentication) 방법을 정의하고 있다. 이를 통해 1대의 AP에 접속하여 인증을 하면서 주변에 이웃한 AP에 대하여도 사용자 인증을 하고, 또한 한번 인증이 성공하면 PMK를 캐시하고 있어서 기존의 IEEE 802.11i 보안 표준에 의한 인증 방식에 비하여 인증에 소요되는 시간을 단축시킬 수 있는 장점이 있다.

그러나 키 캐싱에 의한 경우라도 항상 4-Way Handshake 과정을 거쳐 이로 인한 접속 지연이 발생하게 되며, 현재 접속한 AP를 통하여 이웃한 AP에 사전인증을 받는 경우에는 IEEE 802.1X에서 정의한 전체 인증 절차를 모두 수행하게 됨으로 인증서버에 대량의 부하를 발생시키는 단점이 발생한다 [6].

Ⅲ. Key Table을 이용한 보안 메커니즘

1. 개요

IEEE 802.1X 사용자 인증 및 4-Way Handshake 절차로 인한 지연 시간을 단축하기 위하여 본 논문에서 제안하는 인증 기법은 IEEE 802.11i 표준에서 옵션 인증 방식으로 지원하는 PSK 방식과 유사하다고 할 수 있으나, 핵심적인 차이점은 사전에 공유된 하나의 Key를 256개의 Key Table 개념으로 확장하여 동일 Key를 사용할 경우의 Key 유출의 가능성을 줄이고, 인증에 사용되는 Key를 데이터 암호화에도 그대로 사용을 하여 4-Way Handshake 과정도 생략할 수 있도록 하였다.

이러한 본 논문에서 제안하는 인증 방식은 ① IEEE 802.11i에 의한 사용자 인증과 데이터 암호화를 통한 Key Table 생성 과정, ② 256개의 Key로 구성된 Key Table에서 Random하게 선택한 Key로 Password를 암호화하여 인증을 받는 과정, 그리고 ③ 인증이 성공한 후에 통신 데이터에 대한 암호화 과정으로 요약 된다.

2. IEEE 802.11i 보안을 통한 Key Table 생성

Key Table이 없는 STA에서는 Key Table을 생성하기 위한 세션(Muli-SSID : AUTH)으로 접속을 시도하여 IEEE 802.11i 인증 과정을 거친 후 CCMP 암호화 알고리즘을 이용하여 AP에서는 STA Vendor에 해당하는 Key Table을 전송하게 된다. Key Table 수신을 완료한 STA은 재부팅한 후 인증 절차를 거치게 된다.

AP에서는 STA과 통신을 하기 전에 초기 기동 과정에서 센터와의 통신을 통하여 STA Vendor에 해당하는 Key Table들을 가지고 있다고 가정한다. Key Table 생성과정은 Key Table Version이 상향 조정된 경우에도 Key Table Update를 위하여 동일한 과정을 거친다.

STA 및 AP에서 가지고 있는 Key Table 구조는 <그림 4>와 같다.

<STA Key Table>

Vendor Index	1		
Password	16Bytes Password (Encrypted with AES)		
Key version	1		
Key Index	0	...	255
Expired	0 /1		0/1
Primary Key	128bit		128bit

<AP Key Table>

Vendor In.	1		~	255
Password	SHA2-256 Hash 값			SHA2-256 Hash 값
Key version	1			1
Key Index	0	...	255	0 ... 255
Expired	0 /1		0/1	0/1 0/1
Primary Key	128bit		128bit	128bit 128bit
암호화 정책 플래그 : 비트정의(1B)			Group Key : 128비트코드(16B)	

<그림 4> STA 및 AP의 Key Table 구조
<Fig. 4> Structure of key table for the STA and AP

STA의 Key Table은 ① Vendor Index, ② 인증에 필요한 Password, ③ Key Table 갱신에 필요한 Key Table Version, ④ Password 및 데이터 암호화에 사용하는 Key를 지정하기 위한 Key Index, ⑤ Key (256개)로 이루어지며, AP의 Key Table은 STA의 Password를 SHA2 HASH 형태로 보관하고 있는 것을 제외하고는 STA의 Key Table 구조와 동일하며, 제조사 수 만큼 추가된 구조이다.

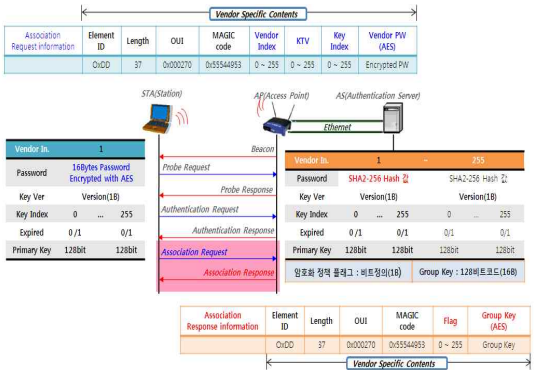
3. Key Table을 이용한 Password 인증 및 데이터 암호화

1) 개요

802.11i 보안 표준을 이용하여 STA에서 Key Table을 생성한 후 IEEE 802.11 표준에서 지원하는 Association Frame의 Vendor Specific Contents를 활용하여 Password 인증 및 데이터 암호화를 위한 Key 지정 과정을 갖게 된다. 이렇게 함으로써 IEEE 802.11 표준에서 정의한 ① 채널 탐색 과정(Beacon/Probe), ② 인증 과정(Authentication), ③ 결합 과정(Association)의 3단계의 접속 절차만을 거치면서 인증을 완료할 수 있게 되어, IEEE 802.11i에서 정의한 IEEE 802.1X 사용자 인증 과정 및 4-Way Handshake 과정에 소요되는 시간을 단축할 수 있게 된다.

2) Key Table을 이용한 Password 인증

전체적인 인증 절차는 <그림 5>와 같으며, IEEE 802.11에서 정의된 Association Request 및 Association Response의 Vendor Specific Contents Field를 새롭게 정의하여 인증에 활용하였다.



<그림 5> Association Req/Res를 이용한 인증 과정
<Fig. 5> Authentication process using association Req/Res

STA와 AP 간 인증 절차는 다음과 같다.

STA에서 Association Request 패킷 중 Vendor Specific Contents 항목에 다음과 같이 정의된 정보를 설정하여 AP로 인증을 요청한다.

① STA의 ⅰ) Vendor Index, ⅱ) Key Table의 Version을 설정

② 256개의 Key 중 1개를 Random하게 지정하여 Password를 AES 암호화 알고리즘을 이용하여 Encryption. 이 때 사용되는 IV(Initial Vector)는 NULL 값으로 설정

③ Password를 암호화하는데 사용한 Key의 해당 ⅲ) Key Index를 설정하고, ⅳ) AES로 암호화된 16bytes의 Password를 설정

④ STA에서는 상기 ⅰ), ⅱ), ⅲ), ⅳ) 4가지 항목을 Association Request의 Vendor Specific Contents에 실어서 AP로 인증을 요청

STA의 인증 요청에 대하여 AP에서는 다음의 과정을 거쳐 STA에 인증 성공/실패 여부와 인증 후에 응용서비스용 데이터 통신에서 사용될 암호화 정책 및 Group Key를 전송한다.

① STA에서 전송한 Association Request Packet 중 Vendor Index, Key Table Version, Key Index를 체크하여 해당 Key 확인

② Key Index의 Expiration 여부 체크, 만료가 되지 않은 Key인 경우 AES로 암호화된 Password를 해당 Key로 복호화

③ 평문화된 Password를 다시 SHA2-256 HASH 값으로 변환하여 Key Table의 Password와 비교

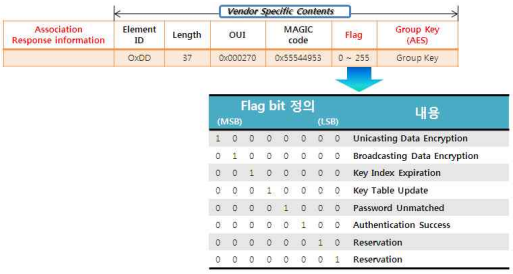
④ 비교 후 인증이 성공된 경우, 암호화 정책에 대한 Flag 및 Group Key를 STA에서 Association Request에서 설정한 Index의 Key로 암호화하여 전송

인증 과정을 거친 후 STA과 AP는 해당 통신 세션이 진행되는 과정에서는 인증 시 지정한 Key Index에 해당하는 Key로 Unicasting Data를 암호화하여 송수신하고, 수신 데이터를 수신하여 해당 Key로 복호화하여 사용한다. 또한 AP로부터 일방적으로 Broadcasting하는 데이터는 Association Response에 포함된 Group Key를 통하여 복호화하여 사용한다.

3) 데이터 암호화 및 정책 결정

인증에 성공한 이후에는 인증 과정에서 지정된 Index의 Key 또는 Group Key를 이용하여 AES-CBC 모드(Cipher Block Chaining Mode)를 적용하여 암호화하여 전송한다.

또한 본 논문에서 제안하는 보안 메커니즘에서는 세션 중 교환되는 정보의 중요도에 따라서 암호화 여부를 결정할 수 있도록 유연한 보안 정책을 활용할 수 있도록 한다. <그림 6>에서와 같이 Association Response의 Vendor Specific Contents 내에 Flag Field를 두고, 센터 서버에서 지정한 보안 정책(Unicasting Data 및 Broadcasting Data에 대한 암호화 적용 여부 결정 가능)에 따라 유연하게 대응할 수 있도록 하고 있다.



<그림 7> Association Response의 Flag Field 세부 설명
<Fig. 7> Association response의 flag field description

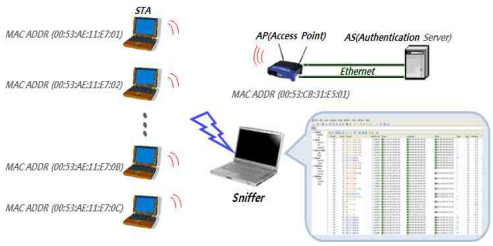
Ⅳ. 인증 시간 비교 시험 및 결과 분석

1. 시험 개요 및 측정 방법

IEEE 802.11i에서 정의한 보안 표준을 준수하는 인증 및 데이터 암호화 방식과 본 논문에서 제안하는 Key Table을 이용하여 인증 받는 방식을 비교 시험하여 결과를 분석하였다.

인증 시간 비교 시험 구성은 <그림 7>과 같으며, STA은 Active Scan을 하도록 설정하고, AP의 채널은 스캔 채널 중 하나로 설정하고 Sniffer를 동일 채널로 설정한 후 AP의 RF 스위치를 개방하여 STA과 AP 간에 무선 상에서 교환하는 패킷을 캡쳐하는 형태로 시험을 진행하였다.

인증에 소요되는 시간만을 비교하기 위하여 CSMA/CA의 MAC Protocol이 적용되는 IEEE 802.11에서의 STA 간의 경쟁에 의한 접속 지연 요인의 배



<그림 6> 인증시간 측정 시험 구성도
<Fig. 6> Experiment diagram of authentication time measurement

제를 위해 1대의 STA에 대한 인증 소요시간을 측정하는 시험과 다수 STA(6대)를 동시에 접속시켜 경쟁 환경에서의 마지막으로 접속되는 STA이 인증을 포함한 접속 완료 소요시간을 측정하였다. 이 시험에서는 모든 STA에 동일하게 4개의 채널을 스캔하도록 하여 보다 실질적인 시험 결과를 반영하도록 하였다. 스캔 채널은 IEEE 802.11a에서 사용하는 전파 대역 중 DFS(Dynamic Frequency Selection) 대역을 제외하고 Active Scan이 가능한 5.725 ~ 5.825 GHz 대역에서 동시 사용 가능한 Ch149, Ch153, Ch157, Ch161로 설정하였다.

2. 시험 결과 및 분석

1) 1대의 STA에 대한 인증시간 시험 결과

<표 1>은 각 방식별로 1대의 STA에 대하여 각 인증 단계별로 총 5회를 측정하여 평균치를 정리한 결과이다.

<표 1> 1대의 STA에 대한 인증 시간
<Table 1> Authentication time for the STA

(단위 : msec)

	IEEE 802.11i	제안 방식	개선율(%)
Authentication	10.26	17.36	94
Association	1.02	2.87	
IEEE 802.1X	322.08	-	
4-Way Handshake	19.84	-	
Total	353.20	20.23	

IEEE 802.11i 보안 표준을 적용한 인증 방식과 본 논문의 제안 방식에서의 핵심적인 차이점은 ① Association 과정에서의 인증과 ② IEEE 802.1X 인증과 4-Way Handshake 과정의 생략 여부이다.

본 논문의 제안 방식에서는 기본적인 Association 과정 이외에 추가적으로 Association 패킷의 Vendor Specific Contents를 활용하여 인증에 필요한 Key를 찾는 과정과 해당 Key를 통하여 Password를 복호화한 후 이를 SHA2 256bit으로 Hash 형태로 변환 후 비교 과정을 거쳐 인증 성공 여부를 결정하는 과정이 추가적으로 필요하게 된다. 상기 시험 결과를 보면 IEEE 802.11i에서의 association 과정보다 약 1.75 msec 정도가 더 소요되는 것으로 나타났는데, 이 시간이 Password 인증에 걸리는 소요시간이라고 할 수 있다. 그러나 본 논문의 제안 방식에서는 IEE 802.1X 인증 및 4-Way Handshake 과정으로 인해 전체적인 인증 소요시간에서는 약 350 msec 이상 단축되어 약 94 % 정도의 인증 시간 단축 효과가 있음을 실험 결과를 통해 확인할 수 있다.

본 논문의 시험에서는 인증에 소요되는 시간에 채널 스캔하는 시간은 제외하였는데, 일반적으로 IEEE 802.11a에서 사용하는 전파 대역 중 DFS (Dynamic Frequency Selection) 대역을 제외하고 Active Scan이 가능한 5.725 ~ 5.825 GHz 대역에서 동시 사용 가능한 채널은 총 4개로서 4개의 채널을 스캔하는데 소요되는 시간은 일반적으로 20 ~ 80 msec 정도 소요된다. 이렇게 4개 채널 스캔시간을 고려한다고 하더라도 본 논문의 제안 방식을 적용하면 최대 100 msec 이내에 인증을 포함한 접속이 완료될 수 있어 본 논문의 서론에서 최소 접속 요구시간으로 제시한 167 msec 이내에 접속이 가능하여 ITS에 적용하기에 적합한 인증 방식이라고 할 수 있다.

2) 다수 STA(6대)에 대한 인증시간 시험 결과

<표 2>는 채널스캔 시간 포함하여 방식별로 6대의 STA에 대한 인증 소요시간을 총 5회 측정하여 평균치를 정리한 결과이다.

6번째 STA이 인증을 마무리하고 접속이 완료되는 시간은 IEEE 802.11i 보안 표준 방식에 의한 것이 2,184 msec이고, 본 논문의 제안 방식은 109 msec가 소요되는 것으로 나왔다.

<표 2> 다수 STA에 대한 인증 시간(6대)
<Table 2> Authentication time for multi STAs(6EA)

(단위 : msec)

STA 대수	IEEE 802.11i	제안 방식	개선율(%)
1st	1,494	49	95
2nd	1,741	67	
3rd	1,921	88	
4th	2,004	96	
5th	2,112	102	
6th	2,172	107	

이 결과는 4개의 채널을 스캔하는 시간이 포함된 것이고, 다수 STA이 CSMA/CA의 경쟁 기반에서 동작하는 실제 Wireless LAN 환경에서 충돌 회피를 위한 지연시간으로 인하여 1대의 STA에 대한 인증 시간보다 많이 소요되는 것이라고 할 수 있다.

이 결과를 토대로 본 논문의 제1장 서론에서 ITS에 무선 통신기술을 적용하기 위한 접속시간 요구조건으로 제시한 최소 167 msec에 대한 산정 기준인 12대의 STA를 장착한 차량이 2 Sec 이내에 접속이 완료되어야 한다는 전제에 대한 만족 여부를 검토해 보면, <표 2>의 결과에서 IEEE 802.11i 방식의 경우의 경우 4개의 채널을 Active 방식으로 스캔하는 시간을 포함하여 평균적으로 4번째의 STA이 인증을 완료하고 접속을 종료하는 시간이 이미 2 sec를 지난 것으로 나왔으며, 반면 본 논문의 제안 방식은 6대의 STA이 인증을 완료하는데 평균 109 msec 정도가 소요되는 것으로 결과가 나타났는데, 최초로 접속된 STA부터 6번째로 접속된 STA까지의 접속 시간 패턴을 보면 서론에서 제시한 기준이 12대에 대하여도 2 sec 이내에는 충분히 인증을 종료하고 접속이 가능할 것이라는 추측이 가능하다.

V. 결 론

본 논문에서는 IEEE 802.11i 보안 적용으로 인한

접속 지연 시간을 줄이기 위하여 Key Table을 이용하여 Password 인증 및 데이터 보안 메커니즘을 적용하여 기존 IEEE 802.11i에서 정의된 IEEE 802.1X 인증 및 4-Way Handshake 과정을 생략하고, 인증을 진행할 수 있는 보안 메커니즘을 제안하여 인증 시간 단축을 이루었다. 이를 위하여 Key Table 개념을 도입하여 제조사별로 256개의 Key를 접속 시마다 랜덤하게 지정하여 고정된 공유키 사용하여 발생하는 키 유출 가능성을 최소화 하고자 하였으며, 해당 키 테이블 등의 유출되는 경우를 대비하여 Key Table의 버전을 두어 새로운 버전의 Key Table로 갱신이 가능하도록 하였다. 또한 무선구간의 Key Sniffing 등을 막기 위해 무선 구간에서 Key를 교환하는 형태가 아닌 해당 Key의 인덱스만을 전송하여 Key 유출을 방지하고자 하였다. 이를 통해 Wireless LAN을 활용하여 고속으로 이동하는 STA과 AP 간의 통신이 필수 요건인 보안을 확보한 빠른 접속 절차를 구현하여 ITS에 적용할 수 있는 가능성을 증대하였다.

본 논문에서는 Wireless LAN을 ITS에 활용하기 위하여 IEEE 802.11 규격에서 정의된 MAC Layer 계층에서의 사용자 인증 및 데이터 암호 처리에 대한 보안 메커니즘을 제안하여 접속 시간을 단축하는 것에 한정하여 고려하였다. 향후 Wireless LAN을 통한 다양한 ITS 부가서비스 구현을 위해서는 IP 기반의 Layer 3 계층의 핸드오프와 연계하여 인증 및 데이터 보안이 적용 가능하도록 하는 보안 메커니즘 연구가 추가적으로 필요할 것이다.

참 고 문 헌

[1] IEEE, IEEE Std. 802.11-2007, Part 11 : *Wireless LAN Media Access Control(MAC) and Physical Layer(PHY) Specification*, IEEE Std. 801.11, 2007.

[2] 송창렬, 정병호, 조기환, “무선랜 보안 구조,” *정보과학회지*, 제20권, 제4호, pp. 5~13, 2002. 4.

[3] IEEE, *Standard for Port Based Network Access Control*, IEEE Draft p.802.1X/D11, March. 2001.

[4] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specification Amendment 6 : Medium Access Control (MAC) Security Enhancement*, IEEE Std 802.11i, July. 2004.

[5] 강유성, 오경희, 정병호, 정교일, “무선랜 보안 표준 IEEE 802.11i,” *TTA 저널*, no. 99, pp. 123~ 130, 2005. 5.

[6] 권정호, 박종태, “IEEE 802.11 무선랜에서 고속 이동성 지원을 위한 사용자 사전 인증 기법,” *전자공학회 논문지*, 제44권 TC편, 제10호, pp. 191~200, 2007. 10.

저자소개

홍 경 식 (Hong, Kyung-Sik)

2003년 2월 : 서강대학교 전자공학과 졸업
2006년 ~ 현재 : 도로교통공단 교통과학연구원 연구원
2007년 ~ 현재 : 연세대학교 공학대학원 전파통신공학 석사 과정

서 종 수 (Seo, Jong-Soo)

1975년 2월 : 연세대학교 전자공학과 졸업
1983년 12월 : Univ. of Ottawa, Canada, 전기공학과 석사
1988년 6월 : Univ. of Ottawa, Canada, 전기공학과 박사
1995년 3월 ~ 현재 : 연세대학교 전기전자공학과 교수

고 광 용 (Ko, Kwang-Yong)

2007년 8월 : 아주대학교 교통공학박사
1996년 ~ 현재 : 도로교통공단 교통과학연구원 선임연구원

정 준 하 (Jung, Jun-Ha)

2007년 2월 : 아주대학교 교통공학박사
1998년 ~ 현재 : 도로교통공단 교통과학연구원 수석연구원

이 철 기 (Lee, Choul-Ki)

1998년 2월 : 아주대학교 교통공학박사
2000년 ~ 2004년 : 서울지방경찰청 교통개선기획 실장
2004년 ~ 2006년 : 아주대학교 교통연구센터 부센터장
2006년 3월 ~ 현재 : 아주대학교 ITS 대학원 특임 교수