Activities of Wi-Fi Alliance to Promote Interoperability of Wireless LANs

Takeo Ichikawa, Yasuyoshi Kojima[†], and Tetsu Sakata

Abstract

The Wi-Fi alliance established by wireless LAN vendors promotes interoperability between wireless LAN products manufactured by different vendors to expand the wireless LAN market. Users can construct a wireless network using products certified by the Wi-Fi Alliance without any interoperability problems even when the products come from different vendors. This article describes the activities of the Wi-Fi Alliance and wireless LAN standardization activities related to it.

1. Introduction

A few years ago, wireless LANs (WLANs) were only for specific users who needed a wireless computing environment at their offices or factories because of the high price of WLAN products. These days, they are not only for enterprise users but also for consumers who use them to access the Internet from their homes, because many types of WLAN products ranging from enterprise to consumer use have been put on the market by many vendors and the cost of WLAN products has decreased dramatically. The Wi-Fi Alliance[*1] is one of the alliances of WLAN vendors for promoting the WLAN market.

2. Standardization of wireless LANs

The activities of the Wi-Fi Alliance [1] are related to WLAN standardization in the IEEE 802.11 working group (WG) [2]. Some standards that have been established in IEEE 802.11 WG are shown in **Table 1**. In 1997, IEEE 802.11 WG established the first international WLAN standard called the IEEE 802.11 standard. This standard defines a common MAC (medium access control) layer and three types of physical layer: direct sequence spread spectrum (DS-SS) and frequency hopping (FH) in the 2.4-GHz band and infrared rays (IR). WLAN products cannot communicate with other products using a different physical layer. Moreover, the maximum data rate defined in IEEE 802.11 standard is 2 Mbit/s, which was too low to satisfy user demand for high throughput. Thus, IEEE 802.11 WLAN products were expensive and suitable only for specific enterprise users.

In 1999, IEEE 802.11 WG published two high-speed WLAN standards called IEEE 802.11a and IEEE 802.11b. An IEEE 802.11a WLAN has a maximum data rate of 54 Mbit/s using orthogonal frequency division multiplexing (OFDM) as the physical layer in the 5-GHz band. An IEEE 802.11b WLAN has a maximum data rate of 11 Mbit/s using complementary code keying (CCK) as the physical layer in the 2.4-GHz band obtaining badkward compatibility with the IEEE 802.11 DS-SS WLAN.

In 2003, IEEE 802.11 WG released the third high-speed WLAN standard called IEEE 802.11g for WLANs in the 2.4-GHz band. It offers a maximum data rate of 54 Mbit/s using the same OFDM physical layer as IEEE 802.11a and has backward compatibility with IEEE 802.11b WLANs using the same CCK scheme. Because its physical layer is the same as IEEE 802.11a and IEEE 802.11b, which use another frequency band, dual-band WLAN products complying with both IEEE 802.11a and IEEE 802.11g have already been released by many vendors. Nowadays, IEEE 802.11b WLAN products have the top share

[†] NTT Access Network Service Systems Laboratories
Yokosuka-shi, 239-0847 Japan
E-mail: kojima@ansl.ntt.co.jp

[*1] Wi-Fi Alliance: Established in the U.S.A. in 1999, its name was initially WECA (Wireless Ethernet Compatibility Alliance) and later changed to Wi-Fi Alliance.

Table 1. Standardization in IEEE 802.11 WG and interoperability tests in Wi-Fi Alliance.

Standard	Overview	Status	Interoperability test of Wi-Fi Alliance
IEEE802.11	2.4-GHz wireless LAN (max 2 Mbit/s)	Completed in 1997	Not applicable
IEEE802.11b	2.4-GHz wireless LAN (max 11 Mbit/s)	Completed in 1999	Started
IEEE802.11g	2.4-GHz wireless LAN (max 54 Mbit/s)	Completed in 2003	Started
IEEE802.11a	5-GHz wireless LAN (max 54 Mbit/s)	Completed in 1999	Started (Dual-band test is included.)
IEEE802.11d	Operation in additional regulatory domains	Completed in 2001	Not started
IEEE802.11e	MAC enhancement (QoS)	In progress	Not started
IEEE802.11h	Extensions in the 5-GHz band in Europe	Completed in 2003	Not started
IEEE802.11i	MAC enhancement (security)	In progress	Test of WPA, which is a subset of IEEE 802.11i draft, has been started.
IEEE802.11j	4.9–5-GHz operation in Japan	In progress	Not started
IEEE802.11n	Enhancements for higher throughput	In progress	Not started

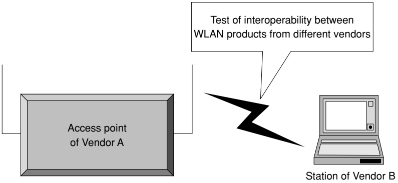
Test of interoperability between WLAN products from different vendors
Access point of Vendor A
Station of Vendor B

Fig. 1. Activities of Wi-Fi Alliance.

among the three standards, but IEEE 802.11a/g dual-band products are expected to become dominant in the near future. In the meantime, IEEE 802.11 WG has been discussing a QoS (quality of service) support mechanism (IEEE 802.11e) and enhanced security mechanism (IEEE 802.11i) as MAC layer enhancements.

3. Interoperability testing

After the standards documents have been published, WLAN vendors will manufacture WLAN products such as WLAN PCMCIA cards and access points based on standards. However, if different vendors implement a standard differently, the products will not be able to communicate with each other. For example, a station made by vendor B may not be able to communicate with an access point made by vendor A as shown in **Fig. 1**.

In the Wi-Fi Alliance, interoperability tests for three types of WLAN (IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g) have been conducted as shown in Table 1 and Fig. 1. The interoperability tests for IEEE 802.11a/g or IEEE 802.11a/b dual-band WLAN products are included. A WLAN vendor that is a member of the Wi-Fi Alliance can apply to test its WLAN products. If a product passes the test, the Wi-Fi Alliance permits the vendor to label the product with a "Wi-Fi Certification Mark", which is one of the Wi-Fi Alliance's trademarks. Users can utilize multi-vendor WLAN products without any interoperability problems, as long as they use Wi-Fi certified products. The number of Wi-Fi Alliance members has reached 200 and 900 Wi-Fi products have been certified. Both numbers are continuing to increase.

4. WPA

The main WLAN feature that attracts both enterprise and consumer users is that WLAN allows terminals to be moved and does not need cables to connect to the computer network. Since radio waves can be easily intercepted by people in the radio coverage area of the WLAN, a security mechanism is important for WLANs. The IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g WLAN products use WEP*2, which is defined in the IEEE 802.11 standard, to encrypt radio data packets. However, several security problems with WEP have been reported.

(1) WEP has some weak points related to encryption, and free software available on the Internet can break it.

(2) WEP cannot derive and update an encryption key automatically between an access point and stations. A network administrator informs users of an encryption key and has users set the encryption key.

(3) All stations that communicate with an access point shall use the same encryption key.

(4) WEP cannot authenticate each user or station individually.

To improve security, a new standard called IEEE 802.11i has been discussed in IEEE 802.11 WG. It is expected to enhance security by:

(1) offering an individual user or station authentication mechanism using IEEE 802.1X,

(2) overcoming WEP weaknesses by employing TKIP*3 or CCMP*4 as new encryption methods, and

(3) supporting the PSK*5 mechanism for consumer users who are difficult to manage with an authentication server such as RADIUS*6 server.

IEEE 802.11i will improve WLAN security, but its standardization has not been completed. The Wi-Fi Alliance regards the security weaknesses of current WLANs as a severe problem hindering the expansion of the WLAN market, so it has defined a new security standard called WPA (Wi-Fi protected access), which is a subset of the IEEE 802.11i draft standard. As **Fig. 2** shows, WPA supports IEEE 802.1X, TKIP, and PSK to achieve sufficiently strong security for an infrastructure network composed of an access point and stations, but does not have AES or an *ad-hoc* mode in which a network is composed of only stations without an access point. Most WLAN users use infrastructure networks, so WPA should satisfy most of the current security demands.

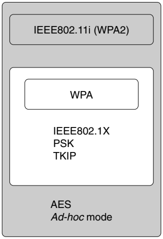

Fig. 2. Relationship between WPA and IEEE802.11i.

The Wi-Fi Alliance started WPA interoperability testing in 2003. WPA implementation is now necessary for Wi-Fi certification, so many products support WPA. When the standardization of IEEE 802.11i, which is called WPA2 (WPA version 2) in the Wi-Fi Alliance, is completed, the Wi-Fi Alliance will start interoperability testing for WPA2 products.

5. Wi-Fi ZONE

As WLAN spreads, public WLAN providers are starting hot-spot services that offer WLAN users wireless Internet access through access points they have placed in fast food shops, coffee shops, cafés,

*2 WEP (wired equivalent privacy) uses RC4 (Rivest Cipher 4) as the encryption algorithm.

*3 TKIP (temporal key integrity protocol) also uses RC4, but its key management scheme is different from that used in the WEP mechanism to improve security.

*4 CCMP (counter mode with CBC-MAC protocol (CBC: cipher block chaining)) uses the AES (advanced encryption standard) algorithm, the next-generation encryption standard in the U.S.A.

*5 PSK (pre-shared key): In PSK, WLAN users can set the master key to an access point and a station, so a RADIUS server is not needed.

*6 RADIUS (remote authentication dial-in user service) is the user authentication protocol used by most Internet service providers. In WPA, an access point and a station derive a master key for an encryption key using RADIUS and IEEE 802.1X.

restaurants, and public spaces such as stations and airports. The number of hot spots continues to increase. The Wi-Fi alliance promotes hot-spot services to expand the WLAN market. A public WLAN provider that places Wi-Fi certified access points can make its hot spots into a "Wi-Fi ZONE" [3] by applying to the Wi-Fi Alliance, which permits the provider to display the Wi-Fi ZONE mark (a Wi-Fi Alliance trademark), and register its hot spots on the Wi-Fi ZONE web page. WLAN users can search for Wi-Fi ZONE locations on this page.

6. Future plans

IEEE 802.11 WG will complete the standardizations in the near future as shown in Table 1. The Wi-Fi Alliance plans to start interoperability testing after the completion of the standardization to certificate the interoperability between WLAN products manufactured by different vendors and will continue to try and expand the WLAN market.

References

[1] http://www.wi-fi.org/

[2] http://www.ieee802.org/11/

[3] http://www.wi-fizone.org/

Takeo Ichikawa

Section Manager, Planning Department, NTT Resonant Inc.

He received the B.E. and M.E. degree in electrical engineering from Waseda University, Tokyo in 1991 and 1993, respectively. In 1993, he joined NTT Radio Communication Systems Laboratories, Tokyo, Japan and engaged in R&D of packet radio systems. From 1999 he was with NTT Access Network Service Systems Laboratories, working on R&D of high-speed wireless LANs. In 2004, he moves to NTT Resonant. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Yasuyoshi Kojima

Senior Research Engineer, Wireless Access Systems Project, NTT Access Network Service Systems Laboratories.

He received the B.E. and M.E. degrees in information & computer sciences from Toyohashi University of Technology, Aichi in 1988 and 1990, respectively. In 1990, he joined NTT Radio Communication Systems Laboratories, Tokyo, Japan. Since then he has been engaged in R&D of wireless LAN systems, cellular phone systems, and personal handy phone systems. He is a member of the Information Processing Society of Japan.

Tetsu Sakata

Senior Research Engineer, Wireless Access Systems Project, NTT Access Network Service Systems Laboratories.

He received the B.E. and M.E. degrees in electrical & electronic engineering from Kyoto Institute of Technology, Kyoto in 1986 and 1988, respectively. In 1988, he joined NTT Radio Communication Systems Laboratories, Tokyo, Japan. Since then he has been engaged in R&D of wireless LAN systems, digital modems, transmission power control system, and digital LSIs for satellite communications and personal communications. He is a member of IEEE and IEICE.