Operation of an Advanced Wireless Access System

Masamitsu Nakura†*, Masafumi Yoshioka, Hiroki Yoshioka, Junichi Iwatani, and Yoshitaka Shimizu*

Abstract

To satisfy the demand for mobile communications with high-speed Internet access, we have developed an Advanced Wireless Access (AWA) system with a wireless transmission capacity of up to 36 Mbit/s. The AWA system provides distinctive services such as bandwidth guarantee in the wireless layer and non-authentication multicasting. This article describes the operations that are required to apply the AWA system.

1. Introduction

The explosive growth of Internet usage and mobile communications has increased the demand for services that can be received anytime and anywhere using the same operating environment. To satisfy this demand, we have developed an Advanced Wireless Access (AWA) system that has a maximum wireless transmission capacity of 36 Mbit/s. This high-speed wireless access system provides highly secure communications through both encryption using the Data Encryption Standard (DES) and mobile terminal (MT) authentication. It also provides stable streaming services such as video delivery by using a bandwidth guarantee function in the wireless layer and offers broadcast services called “non-authentication multicasting.” The AWA system can be applied widely from small-scale systems to large-scale ones. This article describes the operations that are required to apply the AWA system.

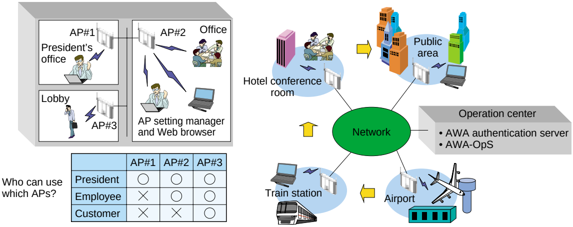
2. Two methods of using the AWA system

The AWA system can be used in two different authentication modes according to the number of access points (APs) and MTs connected to the network (NW): AP authentication mode and NW authentication mode. A switch at the AP can switch between these two modes. Figure 1 shows examples of these modes.

In AP authentication mode, MT information (MT authentication information and bandwidth-guarantee information for receiving guaranteed-bandwidth services) is registered beforehand in APs and each AP carries out MT authentication in an autonomously distributed manner. If equipment for authenticating MTs were installed within the network, then the authenticating equipment in a business establishment would have to be started up every time the power was turned on after being switched off. The AP authentication mode lets MTs connect immediately after the AP power has been turned on. The drawback of this mode, though, is that MT information must be stored in every AP. Because there is a limit to the number of MTs that can be registered in an AP (maximum of 1024), the AP authentication mode is more suitable for a medium-scale system than a large-scale one.

When two or more APs using AP authentication mode are set up within the same LAN, AP connections can be restricted to particular users by modifying the set of MTs registered in each AP. For example, an AP that anybody including customers can use might be installed in the building’s lobby, one that only company employees can use in the office area, and one that only the company president can use in the president’s office. For this purpose, a Web browser and AP Set-

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



	AP#1	AP#2	AP#3
President	○	○	○
Employee	×	○	○
Customer	×	×	○

(a) AP authentication mode

(b) NW authentication mode

Fig. 1. Examples of using the AWA system.

ting Manager are provided as operation tools.

In NW authentication mode, MT information is centrally managed on an AWA authentication server installed within the network and this server centrally performs all MT authentications. Although the AWA authentication server must be up and running at all times in the network, a new MT can be added at any time by simply adding MT information to the server. As a result, NW authentication mode can be applied to a large-scale system having a large number of APs and MTs such as wide-area hot-spot services at airports, train stations, hotel conference rooms, and public spaces. An AWA operation server provides operations such as monitoring a large number of APs.

3. AWA system operation

3.1 Operations in AP authentication mode

Figure 2 shows a conceptual image of AWA system operations provided by the Web browser and AP Setting Manager, which can be used over either wireless or wired connections.

(1) Web browser

Because a Web browser provides operations using a Web server function built into the AP, it is available soon after the purchase of an AWA system without any bothersome installation. These AP operations from a Web browser include functions for writing and reading AP and MT information to and from APs. Here, AP information includes IP addresses of APs, AP identification information that is announced to MTs, and an authentication flag indicating whether authentication is enabled or disabled.

(2) AP Setting Manager

Because AP Setting Manager can manage many APs, this tool is convenient for advanced system management such as setting up a different MT for each AP and managing MT information centrally. It provides functions such as offline editing, online writing, and online reading of AP and MT information. It also provides the three online functions below.

1) AP remote reset: allows resetting from a remote location. This function is convenient when an AP is installed in a high place and AP reset processing is required.

2) AP announcement control: can suspend or begin AP services without turning the AP power on or off. When the AP power supply is on all day, this function is convenient for suspending AP announcements at the close of business and starting them again at the start of business.

3) AP search: searches for APs that are currently connected to the network and operating.

The AP's default setting does not support MT authentication. Therefore, after a customer purchases an AWA system, AP and MT information must first be written to the AP by wireless connection. After initial AP setting has been completed, then for security purposes, AP needs to enter a state where MT authentication is performed when actual usage begins. This is done by changing the authentication flag in the AP information from “non-authentication” to “authentication”.

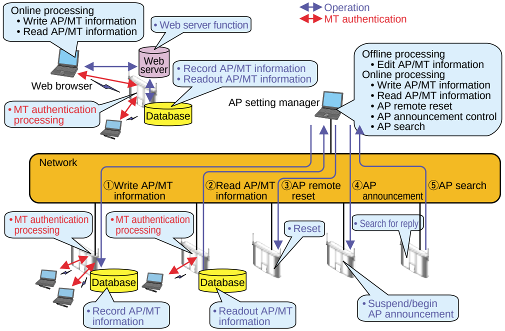


Fig. 2. Operations in AP authentication mode.

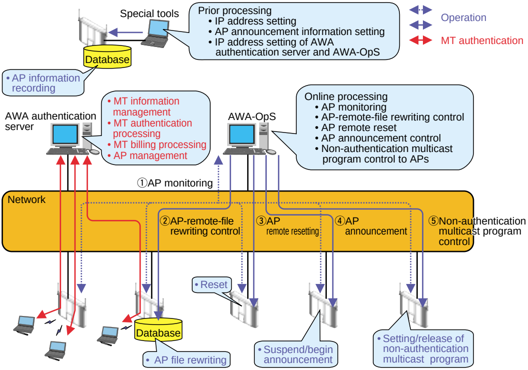

Special tools
Prior processing
• IP address setting
• AP announcement information setting
• IP address setting of AWA authentication server and AWA-OpS
Operation
MT authentication
Database
• AP information recording
AWA authentication server
• MT information management
• MT authentication processing
• MT billing processing
• AP management
AWA-OpS
Online processing
• AP monitoring
• AP-remote-file rewriting control
• AP remote reset
• AP announcement control
• Non-authentication multicast program control to APs
①AP monitoring
Network
②AP-remote-file rewriting control
③AP remote resetting
④AP announcement
⑤Non-authentication multicast program control
• Reset
Database
• AP file rewriting
• Suspend/begin announcement
• Setting/release of non-authentication multicast program

Fig. 3. Operations in NW authentication mode.

3.2 Operations in NW authentication mode

Figure 3 shows a conceptual image of AWA operations provided by the AWA authentication server and AWA-OpS. The AP's IP address, AP announcement information, and IP addresses of the AWA authentication server and AWA-OpS are written in the AP with a special tool, when the AWA system is used in NW authentication mode. After this writing processing has been completed, the AP can receive requests from MTs.

The MT information needed to judge an MT connection is centrally managed on the AWA authentication server, and it is possible to connect an MT to AP after the MT information has been registered with this server. In addition, this server incorporates a double-login-prevention function to prevent access from an unauthorized user and a function to register APs permitted to access this server and prevent the connection of unauthorized APs.

In NW authentication mode, because it is assumed that many APs will be connected to the network, a function to centrally manage APs is needed. This function is provided by the AWA-OpS. The AWA-OpS performs checkpointing on APs connected to the network and AP monitoring. It can rewrite a file in an AP from a remote location and can update the AP's control software when network services are upgraded. It can also stop the service of a specific AP by controlling its AP announcements to prevent a connected MT from being released due to erroneous maintenance work and can reset APs from a remote location.

The AWA system uses a method for centrally managing multiple MTs in order to provide bandwidth guarantee in the wireless layer. There is therefore a limit on the number of MTs that can be connected to one AP. However, with broadcast services like multicasting, there are demands to offer service to many users simultaneously. To meet these demands, the AWA system can also provide non-authentication multicasting in which an unlimited number of users can receive a multicast service from one AP. In non-authentication multicasting, the MT acts only as a receiver and no encryption in the wireless layer or MT authentication is performed between the AP and MT. The AWA-OpS can register non-authentication multicast programs with the AP and also delete them.

4. Conclusion

Our Advanced Wireless Access (AWA) system offers excellent security and provides real-time streaming services such as video delivery by using a bandwidth guarantee function in the wireless layer. Nevertheless, it would be desirable to have an end-to-end bandwidth guarantee linked with the network. In future research, we plan to improve the services and investigate user-friendly operations for the AWA system.

Masamitsu Nakura

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

He received the B.E. degree in electronic engineering from Tokyo Denki University in 1985. Since joining the Electrical Communication Laboratories, NTT, Tokyo, Japan in 1985, he has been engaged in the research and development of network control schemes of satellite communication system. Since 1995, he has been engaged in the research and development of Advanced Wireless Access System. Mr. Nakura is a member of the Institute of Electronics, Information and Communication Engineers.

Masafumi Yoshioka

Researcher, Wireless Access Project, NTT Access Network Service Systems Laboratories.

He received the B.E. and M.E. degrees in electronic engineering from Waseda University, Tokyo, Japan, in 1993 and 1995, respectively. He joined NTT Wireless Systems Laboratories in 1995. Since joining NTT, he has been engaged in research and development of error compensating and operating scheme of the Advanced Wireless Access system. He is a member of the Institute of Electronics, and Communication Engineers.

Hiroki Yoshioka

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

He received the B.E. and M.E. degrees in communication engineering from Tohoku University, Miyagi, Japan, in 1997 and 1999 respectively. In 1999, he joined the NTT Network Service Systems Laboratories. In 2000, he joined the NTT Access Network Service Systems Laboratories, where he has been engaged in research on the development of 5-GHz high-speed wireless LAN systems, especially the operations system for the Advanced Wireless Access System. Mr.Yoshioka is a member of the Institute of Electronics, Information, and Communication Engineers.

Junichi Iwatani

Engineer, Wireless LAN Development Project, First Promotion Project, NTT Access Network Service Systems Laboratories.

He received B.E. and M.E. degrees in electronics engineering from the University of Tokyo, Tokyo, Japan, in 1994 and 1996 respectively. In 1996, he joined NTT Corporation. He has been engaged in research and development of 5-2 GHz high-speed wireless LAN systems, especially in software development of access points and network interfaces of the Advanced Wireless Access System. Mr. Iwatani is a member of the Institute of Electronics, Information and Communication Engineers.

Yoshitaka Shimizu

Wireless Systems Innovation Laboratories, NTT Network Innovation Laboratories.

He received his B.E. and M.E. degrees in electrical engineering from Tokyo Institute of Technology, Japan, in 1995 and in 1997, respectively. He joined NTT Wireless Systems Laboratories in 1997. He is current engaged in the area of wireless access systems within the NTT Network Innovation Laboratories.