Seamless Connection of Wireless LAN

By Kenichi ARIGA,* Takeaki MINAMISAWA,* Norio UCHIDA,* Eiichi ISHIZUKA,* Yoshitaka NAKAYAMA* and Takuya MURAKAMI†

ABSTRACT A drop in prices of wireless LAN equipment has promoted its diffusion in various areas including business enterprises, households and in the public domain. However, unlike the mobile phone network that develops under the management of mobile carriers, wireless LAN is under the independent management of a large number of LAN carriers. Consequently, the terminal setup for connection varies between access points and the users are required to set up their terminals according to the type of access point. Although the emergence of roaming carriers has changed the situation with some access points in the public domain by improving the ease of connection with the use of dedicated software, this improvement is still not available widely, such as for intra-corporate and household networks. In this paper, we describe the features and functions of wireless LAN access permission control middleware that allows users to setup the terminals using the same framework regardless of the control systems of access points. This middleware can also determine the possibility of terminal setup information downloading and restrict the downloaded information according to the personal information of the users.

KEYWORDS Wireless LAN, Mobile phone

1. INTRODUCTION

Thanks to its high speed and low cost, wireless LAN is widely used by both business enterprises and households. As the diffusion of public access network services using wireless LAN has recently been increasing its applications are tending to proliferate more than ever.

The scale of the Japanese wireless LAN equipment market was 478 billion yen in 2003 but is expected to grow by 80% in 2005 to 85.5 billion yen. The third generation mobile phone incorporating the wireless LAN function, which is scheduled to be released in the fall of 2004 is also expected to create a new market for wireless LAN.

However, as current wireless LAN systems are mainly designed for use with PCs, their use with mobile telephones present some technical problems.

To implement communications via wireless LAN, it is required to correctly setup; ① setting items proper to wireless LAN (SSID, WEP, IEEE802.1x authentification method, etc.); ② general setting items for network connection (IP address, DNS server address, DHCP server address, gateway address, etc.); ③ setting items proper to each service (SIP server address, proxy setting, VPN for intra-corporate network connection, etc.); for each terminal. However, to setup the above is generally accompanied by problems, including; ① presence of multiple combination patterns; ② necessity of knowledge about the network; ③ difficulty in entering many setting values composed of complicated series of numerals and letters into a mobile terminal.

To solve the above problems, the authors have developed the Wireless LAN Access Permission Control Middleware that enables user identification and downloading and automatic setting of the setup items with one touch operations. This development will enable access to the networks easily and securely and the enjoyment of the services offered by them anywhere.

The following sections outline this middleware and give some actual examples of the system configurations.

2. TRENDS OF THE COMPETING COMPANIES

Since the wireless LAN presupposes the use of a PC as described above, some software products are released to simplify the network setup operation on a PC.

These software products can roughly be classified into two types. The first type searches in advance for

*Ubiquitous Platform Development Division
†System Platforms Research Laboratories

the nearest access point according to the setup information input by the user and enables either an automatic connection or a manual connection by the user selecting one from the list. The Wireless Client Manager of Windows XP is this type of product.

Other types of products employ software and databases provided by roaming carriers. For example, iPass, which provides a roaming business at a global level, distributes dedicated client software "iPassConnect™" to its users free of charge and allows them to access the central database and acquire setup information for the wireless LAN access points that are contracting with iPass. With "iPassConnect™," the user in each region has to select an access point manually and the entire database is downloaded to the PC.

If such software is run on a device with an inferior user interface to the PC, such as a mobile phone, the following problems will occur;

1) The user must perform a large amount of operations including typing of the initial setup information and selection of access point;
2) The user must have knowledge of the authentification of wireless LAN, etc. for the terminal setup;
3) The software consumes a large amount of memory.

The newly developed Wireless LAN Access Permission Control Middleware is equipped with features that can solve the above problems.

3. WIRELESS LAN ACCESS PERMISSION CONTROL MIDDLEWARE

The Wireless LAN Access Permission Control Middleware is equipped with features that can solve the problems listed above. The outline of the system is as described in the following sections.

3.1 Specifications

Wireless LAN Access Permission Control Middleware has been developed to target running on wireless LAN mobile phones and has the following features.

1) The possibility of the introduction without modification of the existing network configuration

This software can be introduced without modifying the configuration of the existing network or settings of the wireless LAN access points. Introduction is easily achieved by simply installing the setup boxes and the setup distribution control server.

2) Compatibility with various authentification schemes

The security of a wireless LAN network may be protected by a variety of configuration methods. The access points are accessible by anyone, but further connection may be permitted based on authentification e.g. by using a web page or adopting a protocol such as 802.1x at the stage of connection to the access point.

This software can deal with these configurations by describing their definitions in the setting file. The setting file adopts the XML description so that it may be extended, even when the addition of new authentification methods becomes necessary.

3) The possibility of setup information acquisition through the cellular network

Setup information can be downloaded by multiple means. When a wireless-LAN/3G dual mobile terminal is used, the setup information may also be downloaded using 3G.

4) Improved usability achieved by hiding the wireless LAN setup

As the wireless LAN setup would be complicated by enhancing the security, users without knowledge of wireless LAN might experience lots of difficulties. With this software however, the wireless LAN setup is automatically performed by the middleware in the terminal so that the user does not have to be familiar with the details of the wireless LAN setup.

5) The possibility of connection rule definition according to user needs

If everything were automated, the user would be connected to an unintended access point. To prevent this happening, a mechanism is provided to allow each user to set the user rules in advance and select the connection access point automatically according to the user rules.

3.2 System Overview

As shown in **Fig. 1**, the basic model is composed of the mobile terminals in which the middleware is installed, the setup boxes that are used to distribute the setup data, authentificate the users and also function as the proxy authentification, the setup distribution control server that manages the setup boxes, and the authentification server for use in user authentification.

The mobile terminals and setup boxes exchange information by infrared communication (IrDA), while the setup boxes, authentification server and setup

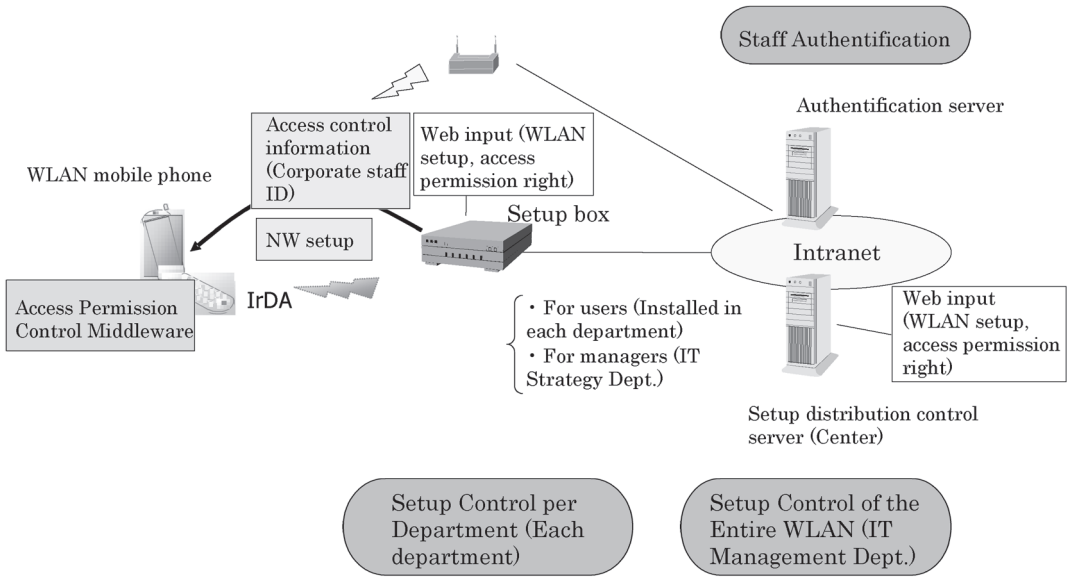

Fig. 1 System overview.

distribution control server are connected via LAN.

The model shown in Fig. 1 assumes that the application is installed in a corporate office.

A setup box is installed in each department, while the setup distribution control server and authentification server are installed in the IT management department. Each setup box stores the setup information of the wireless LAN controlled by each department, that of a network service such as VoIP, etc., according to the network management policy. The setup box also generates the access control information that is stored in each mobile terminal for use in checking the authentification for the setup information downloading based on the rights information from the authentification server (corporate staff ID, etc.). It communicates with the terminals by means of infrared communication (IrDA).

The setup distribution control server maintains and administers the setup boxes in the various departments. Its operations include the log management and initial setup of the setup boxes.

The setup information distributed from the setup box to the mobile phones is described in XML as shown in **Fig. 2** and has a data structure that can be classified into categories in order to facilitate extension of the setup information. The setup information is composed of a group of ESSIDs, the settings required for authentification (WEP key, 802.1x/WPA), DHCP server address required for network connection, subnet mask, default gateway address and DNS server address setup.

The following section describes details of the newly

```
<?xml version="1.0" encoding='utf-8'?>
<!DOCTYPE autoconfig SYSTEM "autoconfig.dtd">
<autoconfig>
    <!-- NETWORK SETTING -->
    <netconf>
        <description>Wlan Spot</description>
        <!-- SITE IDENTIFIER -->
        <siteid>wlanspot.example.com</siteid>
        <!-- GROUP OF ESS-IDs BELONGING TO THE SITE -->
        <essids>
            <ess id="yokohama ">
                <ipref refid="ipcnf:auto"/>
                <secref refid="sec:wlanspot_example_com"/>
                <propref refid="prof:example_com"/>
            </ess>
            <ess id="tokyo">
                <ipref refid="ipcnf:auto"/>
                <secref refid="sec:wlanspot_example_com"/>
                <propref refid="prof:example_com"/>
            </ess>
        </essids>
        <!-- IP SETTING -->
        <ipconfigs>
            <ipconfig id="ipcnf:auto">
                <dhcp>yes</dhcp>
            </ipconfig>
        </ipconfigs>
        <!—L2 NETWORK SECURITY SETTING -->
        <securities>
            <security id="sec:wlanspot_example_com">
                <wepconfig authmode="open" index="0">
                    <wepkey index="0">abcdefg</wepkey>
                </wepconfig>
            </security>
        </securities>
        <!-- NETWORK PROPERTY SETTING -->
        <properties>
            <propertyset id="prof:example_com">
                <property name="connectivity">Internet</property>
                <property name="provider">Provider</property>
                <property name="bearer">WLAN</property>
                <property name="bandwidth">10</property>
            </propertyset>
        </properties>
    </netconf>
</autoconfig>
```

Fig. 2 XML description.

developed middleware and setup box.

3.3 Client Software Overview

As shown in **Fig. 3**, each terminal consists of two layers; the connection control functions for checking the conditions for access point connection and the automatic login functions for logging into the access point indicated by the connection control functions. The terminal is implemented by the PDA running the Linux OS.

3.3.1 Automatic Login Functions

The automatic login functions include the network auto login function and the network service automatic login function.

The network automatic login function includes the function for acquiring the setup information from outside and storing it in the database, and the interface for confirming the higher level of the possibility of connection. It searches a wireless LAN access point in the proximity of the terminal, collates the found access point with the access point information in the setup information database and, when the access point is found in the database, inquires of the connection control functions whether or not the connection to the access point is permissible. If the connection is permitted, the network automatic login function establishes connection to that wireless LAN access point.

The method of access point connection is variable depending on the authentification method and encryption method. The related information is also stored in the setup information database.

The automatic login functions recognize the format and attempt connection using the authentification and encryption method that match each access point.

The network service automatic login function performs the settings required for receiving network services (VoIP, mail, etc.) on the wireless LAN and logs in the services automatically. Currently, VoIP service login function is implemented. Namely, it performs registry of the SIP server based on the SIP server address and SIP-URI information in the setup information.

3.3.2 Connection Control Functions

The connection control functions include four functions of "shared object management function," "VoIP agent function," "network agent function" and "policy control function." Each of these functions is described separately in the following.

(1) Shared Object Management Function

This includes the function for the secure downloading of rights information and setup information from external devices and that for managing the acquired tickets. With the new development, the information from external devices is acquired by means of infrared communication (IrDA) but the means of communication is expandable to those using a "iαppli*" of PDC, RFID and setup-dedicated wireless LAN.

*iαppli is a trademark of NTT DoCoMo, Inc.

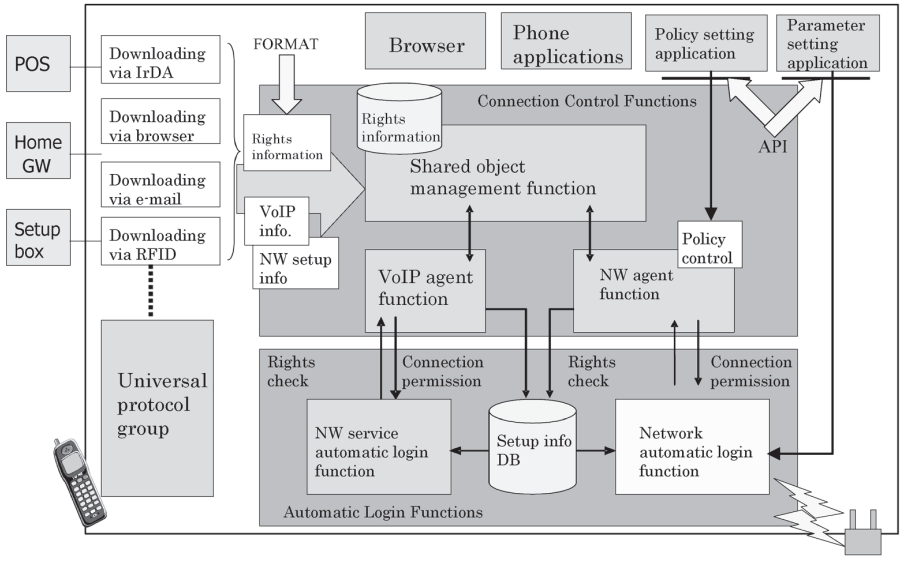

Fig. 3 Client software overview.

(2) Network Agent Function
This includes the following two functions;

- The function for analyzing the wireless LAN setup information that is acquired using the shared object management function, converting its data description format and transferring it to the network automatic login function;
- The function for judging whether or not the user is authentificated to access each wireless LAN network based on the rights information.

(3) VoIP Agent Function
This includes the following two functions;

- The function for analyzing the acquired VoIP setup information that is using the shared object management function, converting its data description format and transferring it to the network service automatic login function;
- The function for judging whether or not the user is authentificated to use VoIP based on the authentificated information.

(4) Policy Control Function
While the network automatic login function may sometimes discover more than one access point, the policy control function makes it possible to select an access point according to the networking policy that is set using a dedicated application in advance. **Figure 4** shows a format for setting the policy. This is an example for selecting an access point for connecting to a wireless LAN network with Internet connectivity and using a bandwidth of 5Mbps or higher. Here, the bandwidth and electric field strength are specified as the criteria for the priority of connection.

3.4 Setup Box Overview

The setup box contains the network setup information, corporate staff ID information issue application, network setup information issue application, and the function for secure distribution of the above information to the terminals.

The corporate staff ID information issue application generates the authentification information to be used in personal authentification. The setup box inputs the user ID and password from the terminal, accesses the authentification server using them and generates the authentification information when authentification is confirmed. The network setup information issue application decides the network setup information to be delivered to the terminal based on the authentification information stored in the terminal.

4. APPLICATIONS (SYSTEM CONFIGURATION EXAMPLE)

The newly developed system is applicable in services for private businesses, carriers and ISPs (Internet Service Providers).

Figure 5 shows an ISP service model as an example. With this model, the service provider providing the system issues common member IDs to the terminals and distributes the setup information on the access points in convenience stores and stations to them and authentificates the in situ network connections to act as ISP agents[9]. The ISP collects the charge for its services from the wireless LAN installer (service provider[10]).

The terminal setup information is assumed to be downloaded from the public wireless network such as the WCDMA or from a dedicated segment for wireless LAN setup.

The types of terminals packaging this middleware may include mobile phones, notebook PCs, PDAs and car-mounted terminals.

5. DEVELOPMENT OF ACHIEVEMENTS/ EFFORTS FOR STANDARDIZATION

The objective of the present research is to promote, by the use of this middleware, the use of wireless LAN to simplify the terminal setup operations of wireless LAN sites for private businesses, households and in the public domain. This policy necessitates packaging the middleware in as many wireless LAN devices as possible. For this purpose, it is required to standardize the items indicated with arrows in Fig. 3, namely the setup information, policy control information format and the middleware API.

```
<?xml version="1.0" encoding='utf-8'?>
<!DOCTYPE network-select SYSTEM "network-select.dtd">
<network-select>
    <and>
        <select type="connectivity">Internet</select>
        <select type="bearer">WLAN</select>
          <select type="bandwidth" compare="ge">5</select>
    </and>
    <order by="bandwidth"/>
    <order by="signal-level"/>
</network-select>
```

Fig. 4 Format for setting the policy.

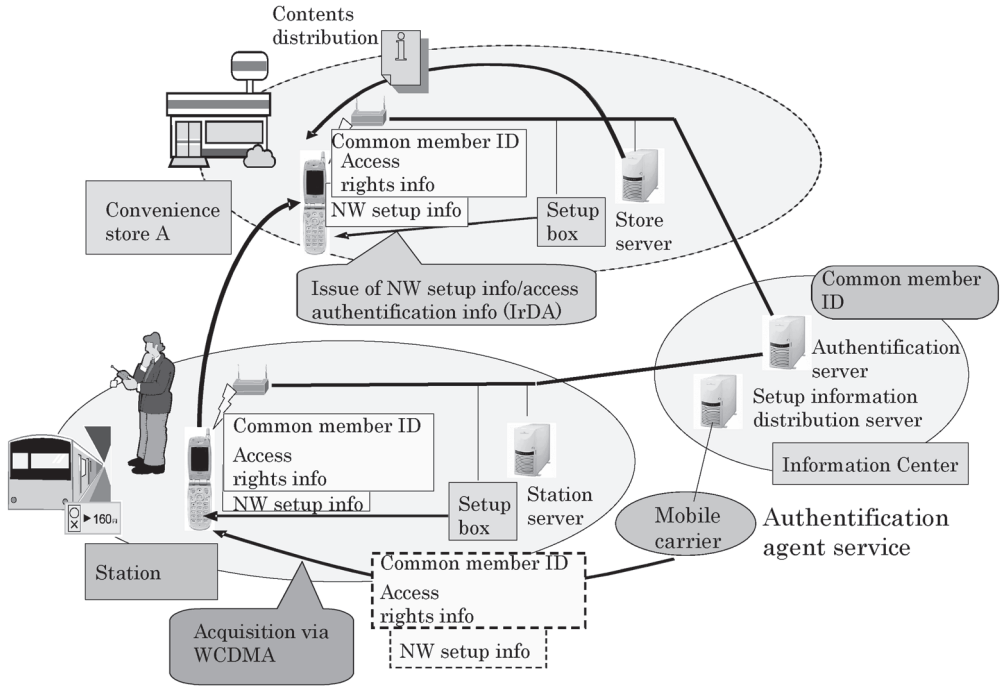

Fig. 5 Example of solution for ISP.

In consideration of the above, this R&D project is supported by the subsidization of the New Energy and Industrial Technology Development Organization (NEDO). The diffusion and promotion activities are being developed by establishing the Wireless LAN Spot Working Group of the Mobile and Home Network Systems Forum as part of the Japan Electronics and Information Technologies industries Association (JEITA). These activities specifically include a review of specifications (API and format), demonstration experiments, the examination of their results (examination of demonstration experiments scheduled for 2005) and standardization measures (the establishment of a standardization policy and selection of the destinations of proposals). In future, the destination of proposals may include OMA, W3C, WiFi-Alliance, etc. With regard to inter carrier standardization trends such as the WLAN Global Alliance of NTT DoCoMo Inc., the authors wish to propose an expansion of shared setup and authentification information databases for business enterprises and households as shown in **Fig. 6** and to make these the de facto standards.

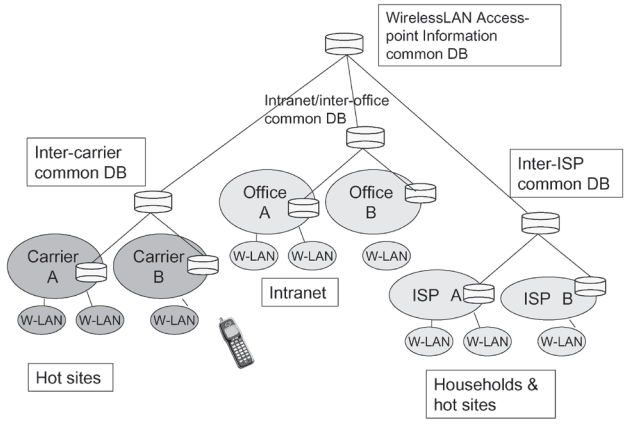

Fig. 6 WirelessLAN Spot services future.

6. CONCLUSION

The authors have recently developed Wireless LAN Access Permission Control Middleware for use in wireless LAN mobile terminals to improve the convenience of both users and terminal administrators. In the future, the authors plan to enhance the following functions of this middleware.

1) Implementation in mobile terminals
The middleware is implemented in the PDA at the present stage of development, but it will be implemented in wireless LAN mobile terminals in the future.

2) Expansion of the means of setup information acquisition

The presently developed prototype acquires the information from the setup box by means of infrared communication, but the means of acquisition will be expanded to RFID, wireless LAN and PDC.

3) Development of the interface between the setup boxes and the authentification server

The development of a universal interface between the setup box and terminals for making inquiries to the authentification server as a means of authentification for the distribution of corporate staff IDs and setup information.

4) Development of a setup distribution control server

A server for the maintenance and administration of setup boxes.

In order to verify the results of this development so far, a demonstrative experiment and evaluation will be conducted in 2005.

ACKNOWLEDGMENTS

The authors would like to express gratitude to the New Energy And Industrial Technology Development Organization (NEDO) for its support for the present research as a part of its subsidization program.

REFERENCE

[1] Y. Okuyama, T. Murakami, et al., "A Configuration Data Management Method for Wireless LAN Communication," *IPSJ SIG Technical Report*, March 2004

Received August 9, 2004

* * * * * * * * * * * * * * * * *

Kenichi ARIGA received his B.S. degree from University of Electro-Communications in 1985. He joined NEC Corporation in 1991, and is now Manager of the Ubiquitous Platform Development Division. He is engaged in the development of application platform software for mobile terminal.

Takeaki MINAMISAWA received his M.S. degree from Toho University in 1995. He joined NEC Corporation in 1995, and is now Assistant Manager of the Ubiquitous Platform Development Division. He is engaged in the development of application platform software for mobile terminal.

Norio UCHIDA received his M.Sc. degree in particle physics from University of Tsukuba in 2003. He joined NEC Corporation in 2003, and is now a staff member of Ubiquitous Platform Development Division. He is engaged in the development of application platform software for mobile terminal.
Mr. Uchida is a member of the Physical Society of Japan.

Eiichi ISHIZUKA received his B.S. degree in electronic engineering from Chiba Institute of Technology in 1991. He joined NEC Corporation in 1991, and is now a staff member of the Ubiquitous Platform Development Division. He is engaged in the development of application platform software for mobile terminal.

Yoshitaka NAKAYAMA received his B.S. degree in mechanical engineering from Hiroshima Institute of Technology in 1992. He joined NEC Corporation in 1992, and is now a staff member of the Ubiquitous Platform Development Division. He is engaged in the development of debugger, embedded OS, and security access control.

Takuya MURAKAMI received his B.Eng. and M.Eng. degrees from Nagoya University in 1993 and 1995. He joined NEC Corporation in 1995, and is now Assistant Manager of the System Platforms Research Laboratories. He is engaged in the development of networking platform software for mobile terminal.

* * * * * * * * * * * * * * * * *