A Cost-effective Ubiquitous Wireless Access Network

Masayoshi Nakayama[†], *Shuichi Yoshino,*
and Masashi Shimizu

Abstract

Public wireless LAN service businesses, if they are to be a success, will have to be able to expand their service areas. This paper describes a cost-effective public wireless access system that combines low-cost private wired access links with wireless LAN networks. For this purpose, we propose an authentication scheme with certificates for public terminals and a link-sharing scheme including bandwidth control. The two-stage authentication scheme protects the access link from unauthorized users. The multiple wireless LANs making up the wireless network can provide several service classes. We evaluated the proposed system by computer simulation and the results indicate that it effectively utilizes the access links. Some equipment for this system has been developed and successfully tested.

1. Introduction

Many consumers now have inexpensive, broadband (over 1 Mbit/s) access links to the Internet. The wireless LAN market is also expanding very rapidly due to its convenience and flexibility. Of course, seamless connectivity to the Internet is required, and to meet this market need, several wireless LAN access services have been developed and put into commercial service.

On the other hand, the capital investment needed to construct wireless networks has recently become a significant burden on operators facing strong competition. For operators, constructing many base stations to expand the wireless coverage area has been regarded as an important means of increasing the number of subscribers. In particular, when providing a wireless LAN service, such as a hot-spot service, the operator must install a great many base stations because each one covers only a very small area. Consequently, at this early stage of the business, operators must invest enough capital to construct base stations, and at the same time, win customers. Some startup companies have appeared in the wireless market with innovative schemes for expanding the coverage area. Boingo Wireless Inc. [1] has started offering commercial roaming services between wireless Internet access providers to expand coverage areas cost-effectively. In this way, Internet access service providers and network operators are forcing a change in the traditional cost strategy by making significant price reductions in a competitive market.

Against this background, NTT has developed a new network concept with the aim of establishing a cost-effective ubiquitous network by combining wired access links and wireless networks. This paper describes the proposed network, in which a public network is constructed from private networks, and its key technologies, which are authentication and link sharing. We evaluated the effectiveness of the proposed network concept by computer simulation and assessed the performance of prototype equipment to determine its feasibility.

2. System concept

We decided that the following three requirements had to be met by the wireless network to achieve a cost-effective nomadic broadband network.

- Provide multi-Mbit/s access links

[†] NTT Network Innovation Laboratories
Yokosuka-shi, 239-0847 Japan
E-mail: nakayama.masayoshi@lab.ntt.co.jp

- Provide seamless access to the network, indoors and outdoors
- Use popular and easy-to-install terminal equipment

We chose the wireless LAN (IEEE802.11 [2]) as the wireless network considering its low construction cost and availability. However, the conventional public wireless access systems are constructed by operators and the construction cost for preparing enough coverage for consumers is huge. Moreover, the operator must obtain the right to install the base station at each location, which can be expensive, and construct cables to the base stations. Thus, it is difficult to start up services of this kind. To enable an operator to expand the service area economically, we propose to utilize existing private wireless systems for public use.

The service concept is shown in **Fig. 1**. Conventional wireless LAN systems are constructed separately, and wireless users can use their wireless terminals only in their private wireless network area and in the public area. That is, they cannot use their wireless terminals in another user's private wireless network area as part of the public wireless network area. Private wireless networks do not always use all of their available bandwidth and operators usually purchase the surplus bandwidth for the public network. The basic concept of the proposed service is that if users install a gateway connecting a private network with a wired access link, they can access public networks via other gateways. The system configuration is shown in **Fig. 2**. The terms *owners* and *members* are explained in the next paragraph. It consists of i) wired access links for *owners*, ii) a core network, iii) wireless access networks which allow *members* to access the core network, iv) gateways, v) edge nodes, and vi) an authentication server installed in the core network by the operators. The typical wireless LAN coverage is not large and the service areas of the wireless networks cannot be located consecutively like a typical wireless hot-spot service, considering the investment cost. Such a system need not provide a handover function to keep the connection while the user moves to another service area. That is, even if a user can move to an adjacent wireless service area, the user must re-connect to the wireless access network in the system that we consider.

The following business model (**Fig. 3**) achieves both a cost-effective network and an expanded coverage area. Subscribers to a private network can choose to become *owners* by installing a gateway and making a contract with an operator. This gives them the right to access wireless public networks via other *owners'* gateways and allows the operator to lease part of the bandwidth of the *owner's* wired access links to accommodate the wireless public network. Ordinary public users, whom we call *members*, can then use them to access the core network. These days, broadband access services for consumers are highly competitive and prices are low. Therefore, operators need to reduce costs. They could reduce the cost of this system by sharing the cost of the base stations with *owners*.

However, the success of this model depends on operators giving attractive incentives to *owners*. We propose the following revenue sharing scheme as the *owner's* incentive. The operator measures the *owner's* contribution to the networks based on traffic information, such as the number of accessing *members* and the quantity of data transmitted by *members*. The operator then distributes profits among *owners* in accordance with these contributions. This should be

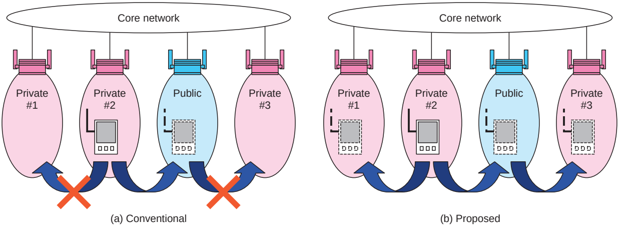

Fig. 1. Service concept.

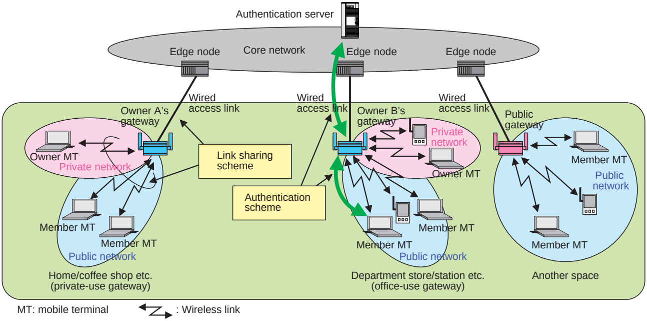

Fig. 2. System configuration.

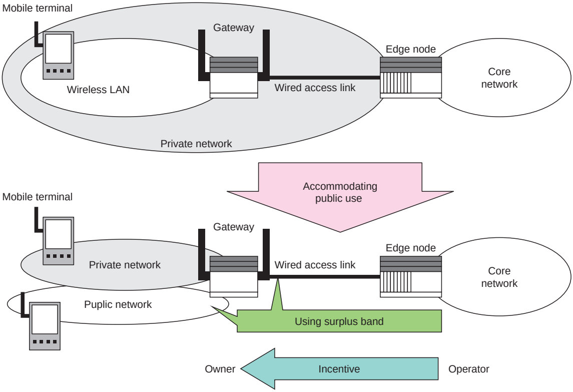

Fig. 3. Business model.

sufficient incentive for an owner to rent out his or her access link's bandwidth.

As described above, the new entity in this scheme is the *owner*, who is the go-between between the operators and the subscribers. For a user to willingly install a gateway to become an *owner*, not only an incentive but also two more key conditions are needed: security and guaranteed bandwidth. It will be necessary to establish a link-sharing method to secure the *owner's* bandwidth. Additionally, *owners* want to keep the same security level as the private wireless network and want to avoid unauthorized access via their gateway by fraudulent users. The operator devolves part of its authority to the *owners*, and this authority is maintained by giving the proposed network a method for authenticating its *members.*

3. Link sharing scheme

Access links are shared by *owners* and *members*. Thus, some bandwidth must be reserved for *owners* to maintain an acceptable degree of Internet connectivity. In our access link control scheme, both the gateways and edge nodes control the transmission speed of packets bound for the access links. This should be able to provide bandwidth control for both asymmetric traffic and one-way traffic. Because the wireless LAN network's access scheme is one of random access, the network cannot precisely control its bandwidth. Consequently our wireless network configuration scheme has a wireless network consisting of several wireless LANs, each using a different frequency.

The proposed scheme is shown in **Fig. 4**. It divides wireless LANs physically and part of the access link logically to accommodate a public network made up of private networks. The *owner* avoids degraded throughput by holding an access competition in the wireless LAN network. When a mobile terminal (MT) enters the area controlled by a gateway, it should select a frequency (i.e., a wireless LAN network). To select an appropriate one, it detects the extended service set ID (ESSID) of each wireless LAN within the gateway. If there is a wireless LAN that has the MT owner's ESSID, the MT selects that wireless LAN for private use. If none of the wireless LANs has the MT owner's ESSID, then it selects one at random for public use. Moreover, we define bandwidth control signals transmitted between the gateway and edge router so that the bandwidth can be centrally managed by the *owners*. This scheme ensures the consistency of the bandwidth management data kept in the equipment and greatly facilitates maintainability.

4. Authentication scheme

The authentication scheme must identify users and ensure that the *owner's* access to the core network is not used as a means of unauthorized access. We use a mutual authentication method based on certificates to prevent the gateway from asking the core network

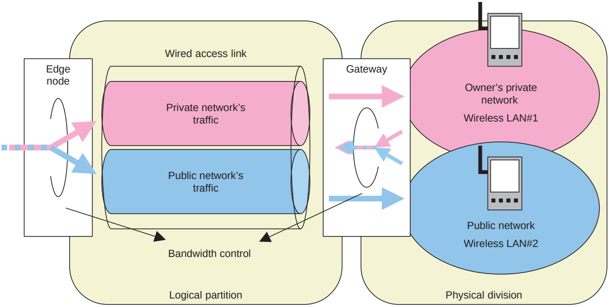

Fig. 4. Proposed link-sharing scheme.

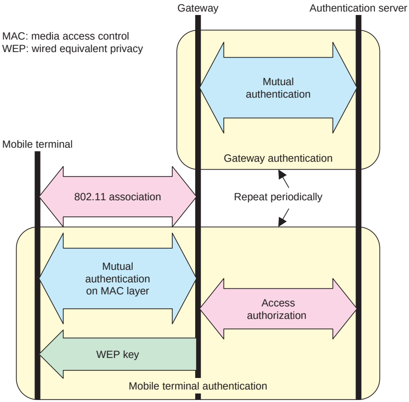

Fig. 5. Proposed authentication scheme.

about public users. We also use a two-stage authentication scheme to prevent access to the link by unauthorized users (**Fig. 5**). Gateways and mobile terminals accessing the *member* network have individual certificates including an individual public key, an individual secret key, and a public key obtained from a Certification Authority (CA).

4.1 Gateway authentication

The gateways gather traffic information to measure the *owner's* contribution in the business model. One obvious problem is that without adequate countermeasures, unscrupulous gateway *owners* could reap benefits by falsely manipulating traffic information. To eliminate this possibility, we propose that the authentication server should periodically authenticate the gateways. *Owners* install certificates and public keys on their gateways. Gateways use certificates for mutual authentication with an authentication server during startup. Afterwards, *member* terminals can access the Internet via the *owner's* gateways. Mutual authentication between gateways and the authentication server is repeated periodically to maintain the security level of the network.

4.2 Mobile terminal authentication

The mobile terminal first searches for a frequency carrying the beacon signal based on the ESSID to access the public network via another *owner's* gateway. When it detects a public network frequency, the mobile terminal becomes associated with this gateway to communicate on the media access control (MAC) layer. After that, the mobile terminal and gateway mutually authenticate each other by exchanging certificates. The gateway asks the authentication server for authorization to authenticate the mobile terminal. If this is granted and the gateway successfully authenticates the mobile terminal, it gives a wired equivalent privacy (WEP) key to the terminal. All packets for mutual authentication are defined in the MAC-layer frame and are terminated at the gateways. IEEE802.1x [3] technology has been used for similar authentication procedures in wireless networks and is employed as a standard function in Windows XP and Windows CE, popular terminals that can be used in this system without modification or the installation of any additional programs. However, with IEEE802.1x technology, before a gateway has authenticated a mobile terminal, it allows the mobile terminal to transmit authentication packets to the authentication server via access links. Our scheme, on the other hand, does not allow unauthorized terminals to transmit any packets over links. Furthermore, the mobile terminals can detect unauthorized gateways because the authentication is performed in both directions. Mobile terminals should run this authentication periodically to maintain the owner's security level.

5. Simulation of link sharing scheme

We evaluated the proposed scheme by computer simulation. We defined two simulation models (**Fig. 6**). Model #1 consists of a wired access link and a wireless LAN network. Model #2 is configured with a wired access link and two wireless LAN networks operated by one gateway. In Model #1, all mobile terminals are in the same wireless LAN network. The

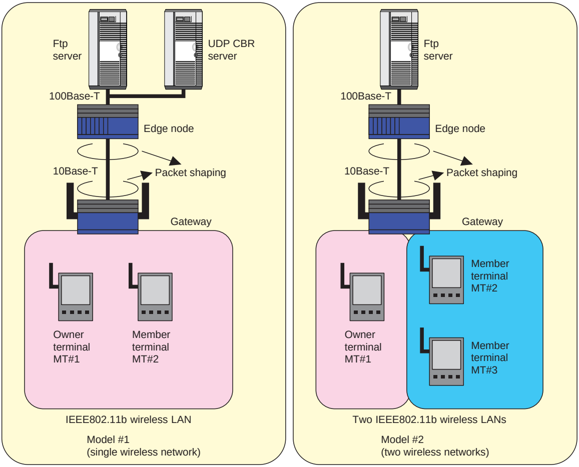

Fig. 6. Simulation models.

wired access links are 10Base-T Ethernet links, and the wireless networks are IEEE802.11b networks. The bandwidth of the access link is controlled by defining the committed access rate (CAR) for each network. Applications transmitted over the networks are ftp (file transfer protocol) and UDP (user datagram protocol) constant bit rate (CBR) traffic. For such traffic, the application server transmits UDP packets to the mobile terminals. Mobile terminals ‘get’ and ‘put’ files by using ftp. We evaluated the average data transmitting/receiving rate of the mobile terminals on the MAC layer and the utilization of the access link.

5.1 Bandwidth control point

First, we estimated the bandwidth control for downlink traffic. The gateway and edge node were selected as the bandwidth controlled points in Model #1. In case 1, the gateway controlled the downlink bandwidth. Case 2 used our access link control scheme and the edge node controlled the access link. There were two mobile terminals in the wireless network. In this simulation, the downlink bandwidth for the *member* network in the access link was 1 Mbit/s. The *owner's* bandwidth was not limited. *Member* mobile terminal (MT#2) received UDP CBR packets and *owner* terminal (MT#1) got files by ftp. The simulation results are shown in **Fig. 7**.

Although the CBR traffic transmission rate increased, the data reception rate of MT#2 was kept constant by limiting the downlink bandwidth. There were no differences between the two cases in this regard. However, in case 1, the data receiving rate of MT#1 decreased with increasing UDP CBR traffic because the UDP CBR traffic occupied the bandwidth of the access link and MT#1 did not use enough bandwidth for the ftp protocol. Thus, we could confirm that the proposed scheme can control the bandwidth of one-way traffic such as streaming traffic.

5.2 Wireless network configuration

In the next simulation, we estimated the advantage

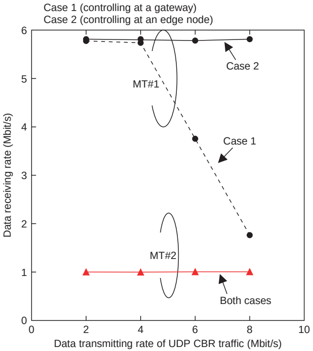

Fig. 7. Effect of bandwidth control.

of using two wireless networks. The bandwidth control points were a gateway and an edge router, and the simulation models were Models #1 and #2. The uplink bandwidth for the *member* network was 1 Mbit/s and the downlink bandwidth varied from 1 to 4 Mbit/s. The *member's* mobile terminal (MT#1) and *owner's* mobile terminal (MT#2) got files by ftp. The *member's* mobile terminal (MT#3) 'put' files by ftp. The simulation results are shown in **Fig. 8**. The utilization of the access link using the two wireless networks was 10% more than that of the access link with a single wireless network. Furthermore, MT#1's data receiving rate for Model #2 was about 1.2 times higher than that of Model #1. In Model #1, the MT could not reach the 10-Mbit/s wired access link efficiency because the maximum throughput of the wireless LAN (about 6 Mbit/s) was less than that of the access link, and there was access competition between member terminals and the owner's terminal in the wireless network. On the other hand, in Model #2, the total throughput of the wireless networks was larger than that of the access link, so the MT could effectively utilize the bandwidth. The proposed wireless network configuration scheme protected the *owner's* bandwidth from the *members'* accesses on an access network including wireless networks, so it can efficiently accommodate public networks on private networks.

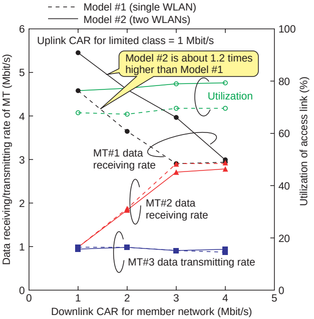

Fig. 8. Effect of wireless LAN configuration.

6. Developed equipment

The gateways have two 10/100-Mbit/s Ethernets (for the access link interface and the owner network interface) and two IEEE802.11b wireless LANs. The edge nodes have one core net interface and two access link interfaces. The gateways and edge nodes both have an IP packet routing function. The gateways also have IP/MAC filtering and a DHCP (dynamic host configuration protocol) server function. **Figure 9** shows the developed equipment and **Table 1** shows its specifications.

The gateways and edge nodes use a CBQ (class-based queuing) algorithm [4] as the packet scheduler to provide accurate bandwidth control and effective utilization of the access link. The CBQ algorithm has the characteristic that if some classes have surplus bandwidth, other classes can use it. The link-sharing system uses the CBQ algorithm to provide effective utilization of the access links. Furthermore, it is possible for the *owner* to consolidate the management of the access link bandwidth because the gateways and edge nodes can exchange bandwidth-control signaling packets.

Fig. 9. Gateway and edge node equipment.

Table 1. Specifications of developed equipment.

Equipment	Description	Specifications
Gateway	Features	IEEE802.11b compliant
		10/100-Mbit/s Ethernet
		Packet routing
		Packet filtering
		DHCP
	Interfaces	10/100Base-T × 2
		Wireless LAN × 2
	Dimensions	430 mm (W) × 280 mm (D) × 50 mm (H)
Edge node	Features	10/100-Mbit/s Ethernet
		Packet routing
	Dimensions	430 mm (W) × 280 mm (D) × 50 mm (H)

The authentication server, gateways, and authentication module have a mutual authentication function based on X.509 [5] certificates. Therefore, they can certify each other autonomously. These modules complete mutual authentication within one second.

We conducted experiments to test the bandwidth control performance of the equipment we developed. **Figures 10, 11**, and **12** show the experimental setups and results.

In the first experiment, to measure the packet forwarding performance of the devices, we evaluated the throughput of an application running on mobile terminals. We assigned the downlink bandwidth of the access link for the *member* network. The applications were ftp for the *owner* terminal and UDP CBR for the *member* terminal. The transmission rate of UDP CBR was larger than the assigned bandwidth of the downlink for the *member* network. To prevent any decrease in throughput because of the wireless link characteristics, we replaced the wireless LAN by a 10base-T Ethernet for the access network.

Figure 11 compares the assigned bandwidth with the throughput of the MT's application. The throughput of the *member* terminal did not exceed the specified bandwidth, and the total throughput of the access link was about 8 Mbit/s.

In the second experiment, we evaluated the utilization of the access link to estimate the bandwidth control performance. Traffic was only UDP CBR for the *member* network. Figure 12 compares the transmitted packet length with the utilized bandwidth of the access link. Despite the change in transmitted packet length, the equipment could control the utilized bandwidth, keeping it within its assigned limits.

7. Conclusion

We proposed a wireless system that combines wired and wireless links allowing public ubiquitous networks to be constructed from private networks. We described the system's authentication and link-sharing schemes. The authentication scheme lets the public network be accommodated by private net-

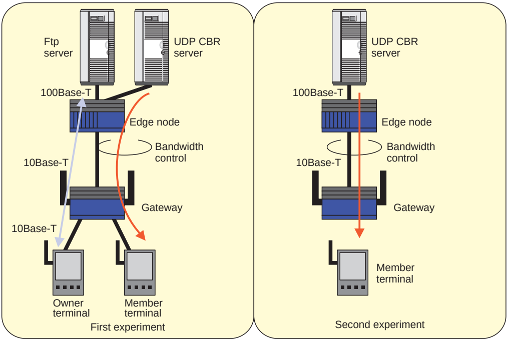

Fig. 10. Experimental setups.

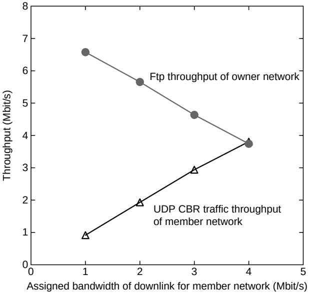

Fig. 11. Packet forwarding performance comparison.

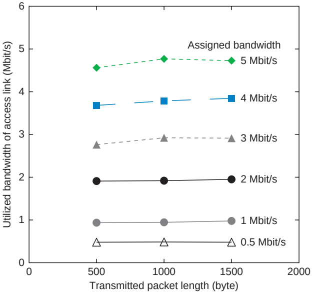

Fig. 12. Bandwidth control performance comparison.

works and distributes profits among users by using gateway authentication and a two-stage terminal authentication process with certificates. The use of a class-based queuing algorithm as the bandwidth control and multiple wireless networks means that the proposed link-sharing scheme provides various classes of service on access networks including the wireless system. We have developed equipment for this network to explore the feasibility of the proposed technologies and have shown that the equipment developed to date has sufficient processing capacity to provide two classes of service on a 10-Mbit/s access link.

If operators adopt these technologies and our proposed business model, they will be able to use their subscriber's private networks to establish a public network. Such a network would be cost-effective and ubiquitous.

References

[1] Boingo Wireless, Inc., http://www.boingo.com/

[2] IEEE, "LAN MAN standards of the IEEE computer society. Wireless LAN medium access control (MAC) and physical layer (PHY) specification," IEEE Standard 802.11, 1997.

[3] IEEE, "Standards for local and metropolitan area networks: Standard for port based network access control," IEEE Draft P802.1X/D11, Mar. 2001.

[4] S. Floyd and V. Jacobson, "Link-sharing and resource management models for packet networks," IEEE/ACM Transactions on Networking, 3(4), Aug. 1995.

[5] ITU-T "Recommendation X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks."

Masayoshi Nakayama

Senior Research Engineer, Wireless Systems Innovation Laboratory, NTT Network Innovation Laboratories.

He received the B.E. degree in electrical engineering from Kobe University, Kobe in 1984. He joined NTT Laboratories in 1984 and engaged in R&D on satellite communication and Internet systems and *ad-hoc* network systems. His current interest is wireless networking technology for ubiquitous services and mobile satellite Internet systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Shuichi Yoshino

Senior Research Engineer, Wireless Systems Innovation Laboratory, NTT Network Innovation Laboratories.

He received the B.E. and M.E. degrees in mechanical engineering from Kanazawa University, Ishikawa in 1990 and 1992, respectively. He joined NTT Laboratories in 1992 and engaged in R&D on satellite Internet systems. His current interest is wireless networking technology for ubiquitous services. He is a member of IEICE.

Masashi Shimizu

Senior Research Engineer, Supervisor, Wireless Systems Innovation Laboratory, NTT Network Innovation Laboratories.

He received the B.E. and M.E. degrees in mechanical engineering from Keio University, Yokohama in 1986 and 1988, respectively. He joined NTT Laboratories in 1988 and engaged in research on pointing control for deployable space antennas and surface error compensation through feed distribution control. His recent interest focuses on active RFID and its applications. He is a member of IEICE.