Seamless Mobile Service Using Snooping Routers

Tomoyoshi Motoyama, Masato Eguchi†, and Kouichi Suto

Abstract

We describe our study of a seamless handover mobile network that uses snooping routers (SRs) and commercially available wireless local area network devices to provide micro-mobility in a mobile IP network. The SR-based mobile service includes SR automatic path learning, handover, and security functions. The prototype system described here achieved hardware handover with interruption times of only a few hundred milliseconds.

1. Seamless mobile services and the need for such services

These days, everyone expects telecommunications services to provide connections to anywhere in the world via interactive broadband networks, allowing anyone (or anything) anywhere to always communicate safely, simply, and securely with anyone or anything else. One of the technologies that will support terminal mobility in the network layer is mobile IP. In this article we describe a mobile network system using snooping routers (SRs)*1 designed to work with a mobile IP network [1] to provide a broadband mobile service with high-speed handover*2 capabilities. Wireless access services using conventional high-speed wireless local area networks (wireless LANs), such as hotspot services, are restricted to zones that can be reached from a given access point (AP) and make it difficult for a terminal to move freely across zone borders while maintaining communications. The mobile system described here can be used to maintain communications while allowing terminals to freely cross between zones (**Fig. 1**).

2. Features of the SR mobile system

In hotspot services, and in other services using wireless LAN technology in which the development of handover services will reduce packet loss rates and interruption times, it is preferable to be able to use existing wireless systems and equipment without having to add any new software or hardware. This will not only reduce the amount of capital investment required for the introduction of new services, but will also help reduce the cost of monitoring or maintaining lines. The SR mobile system is designed to use unmodified commercially available wireless LAN devices. The main features of this system are described below.

2.1 Use of commercially available wireless LAN devices

Handover systems may broadly be divided into network-driven and terminal-driven systems. In a network-driven system, the network must track the positions of terminals and control the terminal handover, so the wireless LAN devices used must be modified, which makes the development costs extremely high. In contrast, the SR mobile system is a terminal-driven system: it uses commercially available products for

† NTT Access Network Service System Laboratories
Chiba-shi, 261-0023 Japan
E-mail: eguchi@ansl.ntt.co.jp

*1 Snooping router (SR): This router automatically creates downstream path information tables by snooping on the upstream packet header information, so unlike a conventional router, it does not need to create path information tables in advance.

*2 Handover is a term used in wireless LAN, cellular telephone, PHS (personal handy phone system), and other mobile communications systems to refer to an operation performed so that communication can continue when a mobile unit moves from a communications area associated with one access point to a communications area associated with a different access point.

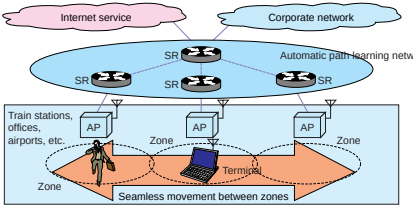

Fig. 1. Seamless mobile service by SR mobile system.

AP equipment and terminal wireless LAN cards. The application software installed in the terminals with the wireless LAN cards may be used to provide handover capabilities simply by detecting switching between APs and notifying an SR. Thus, the development cost is much lower than that of a network-driven system.

2.2 Applicability to existing networks

The SR mobile system uses tunneling protocols*3, so it can be used not only on IP networks but also on multiprotocol label switching (MPLS) and other types of networks, and it is easy to provide two-way connectivity with mobile IP services that require the availability of an IP network.

2.3 Distribution of functions to eliminate dependence on access methods

While the SR mobile system has been designed for wireless LAN terminal services, it may also be used with wired access systems. For instance, its design lets a user move from an office using a wireless LAN to another office that uses a wired access system, without changing any of the terminal's settings. SRs have security termination capabilities, and terminal and user information is managed centrally, so it is possible to freely modify the system to allow for future development or for different security procedures for different access methods.

*3 Tunneling protocol: A protocol that allows for the encapsulation of packets from a lower-layer protocol into packets designed for use in a higher-layer protocol, making it possible to communicate between two points located within different networks.

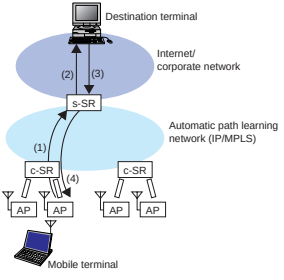

Fig. 2. Automatic path learning network.

3. Automatic path learning network

The operation of the automatic path learning network of the SR mobile system is shown in **Fig. 2**. The path learning procedure is described below.

(1) A client SR (c-SR), which accommodates multiple APs, is installed on the terminal side. When an outgoing data packet transmitted from a terminal is received, a path table entry is created. This records the input physical (or logical) port and sending IP address. The data packet is then encapsulated into an IP packet and transmitted to the server SR (s-SR).

(2) The s-SR decapsulates the packet received from the c-SR, creates a path table entry that records the sending IP address and the physical (or logical) port from which the data packet was input, and then transmits the packet to the destination

terminal.

(3), (4) When data packets are received from the destination terminal, the s-SR and c-SR perform the reverse procedure to steps (1)–(2), and they search the automatically generated path table to determine how to transmit the packet through the physical output port.

4. Authentication procedure performed at the start of communications

The authentication procedure performed at the start of communications is shown in **Fig. 3**.

(1) Authentication data (i.e., user ID and password) is sent from the mobile terminal to an authentication proxy server (AS).
(2) The AS sends the authentication data to a RADIUS (remote authentication dial-in user service) server located within the Internet or a corporate network.
(3) After authentication has been performed by the RADIUS server, the results are sent back to the AS.
(4) The AS sends authorization to the mobile terminal. At the same time an encryption key is distributed to the c-SR and mobile terminal.
(5) The mobile terminal then issues a request for the transmission of the IP address to the Internet or corporate network DHCP (dynamic host configuration protocol) server, and at the same time path information is automatically added to the c-SR and s-SR path tables.
(6) The Internet or corporate network DHCP server then transmits the IP address to the mobile terminal.

When all of the above steps have been performed, user authentication and IP address acquisition have been completed.

5. Handover

The handover procedure used for mobile terminals in the SR mobile system is shown in **Fig. 4**.

5.1 Wireless data link handover

As a wireless terminal moves, it continues to receive a beacon signal*4 put out at regular intervals from the local AP. When the terminal moves to a point where the received signal grows weak, the wireless link is temporarily severed and the mobile terminal begins to search for a different channel with a stronger signal. When the search has been completed, a new wireless data link is established with another available AP (Fig. 4(ii)).

5.2 Path switching in an automatic path learning network

Path switching in the automatic path learning network described here is triggered by the completion of the handover of a wireless data link and performed by updating the path table and sending the encryption key to the SR located within the handover destination area. In the SR mobile system, the handover of a wireless data link is detected by monitoring performed in the applications layer of mobile terminals. The procedure performed during terminal movement is shown in Fig. 4 as (iii) and (iv). Note that section (iv) of Fig. 4 (path switching request and settings) corresponds to the special processing performed in

*4 Beacon signal: a signal transmitted by an AP to notify a wireless LAN card of its existence. The wireless LAN card receives beacon signals transmitted from nearby APs and establishes a communications link with the AP sending the clearest beacon signals.

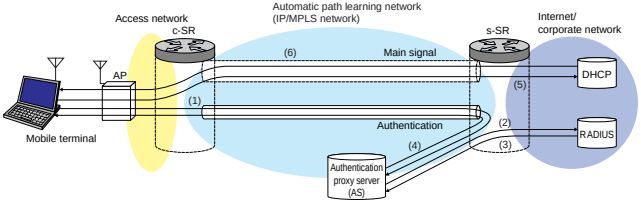

Fig. 3. Authentication procedure performed at start of communications.

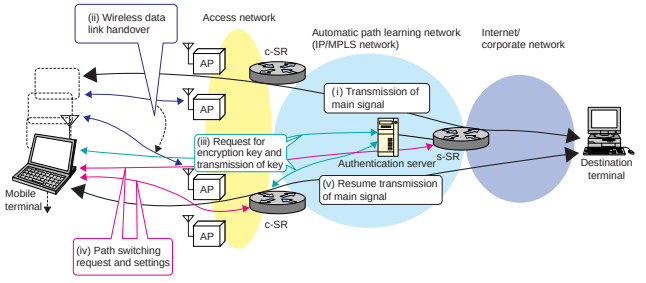

Fig. 4. Handover procedure.

this system for the rewriting of SR path tables.

6. Security features

Wireless links are used for access in a mobile environment, so user authentication, encryption, and other security features are essential.

6.1 Endpoints for the provision of security features

In line with our basic objective of being able to use commercially available wireless LAN devices in unmodified form, mobile terminals and c-SRs are specified as the endpoints at which authentication and encryption are performed, and wireless LAN devices are designed to be used without modification of any kind as simple bridge units. This eliminates the need for any of the security processing load to be performed at APs and enables the development of faster handover for wireless data links.

6.2 Distribution of functions between the SR mobile system and authentication servers

Here we have assumed that terminal authentication will be performed by RADIUS servers located within the Internet or a corporate network and that the SR mobile system will include proxy servers that will act for the RADIUS servers. Note, however, that the re-authentication that must be performed as a result of terminal movement following initial authentication is intended to reduce handover time by using cache information in the proxy servers.

6.3 Central management and distribution of encryption keys

To guard against eavesdropping and DoS (denial of service) attacks in the wireless LAN, the system has been designed to transmit main signals between mobile terminals and c-SRs in encrypted form. While it is necessary to distribute encryption keys to the c-SR and mobile terminal, which serve as the encryption endpoints, by handling the management and distribution of keys centrally in proxy servers we have made it easy to increase handover speeds. In addition, key distribution is performed by predicting the c-SR containing the destination AP of the mobile terminal from the physical location of APs, and the proxy servers are designed to distribute keys before handover actually takes place. This eliminates the need for mobile terminals to request the redistribution of encryption keys and makes it possible to reduce handover time.

6.4 Flexibility in application to standard technologies

As noted above, the performance of security functions in the SR mobile system is distributed between SRs, mobile terminals, and proxy servers. This eliminates the need for any modifications to existing wireless LAN facilities and equipment and makes it possible to respond flexibly to any future developments in standard technologies.

7. Evaluation results for prototype system

7.1 System composition

(1) Snooping router

In order to evaluate the resulting handover performance, a prototype snooping router was created consisting of the basic hardware and firmware for performing automatic path setting and encryption key generation and storage. The external appearance of the prototype SR is shown in **Fig. 5**.

(2) Proxy server (authentication server)

A proxy server was created by installing RADIUS server software on a commercially available personal computer (PC). The server was used to transmit encryption keys to mobile terminals and the SR in response to requests from mobile terminal application software.

Fig. 5. View of prototype SR.

(3) Mobile terminals

Commercially available Windows laptop PCs were used as mobile terminals, and applications software was installed on them for the transmission and reception of packets needed in performing handover trigger detection, key distribution, and other functions.

7.2 Results

Handover tests performed using the prototype SR, commercially available APs, and commercially available mobile terminals with wireless LAN cards showed that the maximum interruption time during handover was a few hundred milliseconds, which will have almost no adverse effects on ordinary Internet usage. This indicates the suitability of the SR mobile system as a micro-mobility system for providing mobile broadband service.

8. Possible uses

Most hotspots these days have only one AP. Even if multiple APs exist, usage is restricted to those within the same subnet. However, if the SR mobile system is used as a bridge between hotspot APs, then a terminal could move between zones while continuing to receive Internet access even when moving between areas belonging to different subnets (see **Fig. 6(a)**).

In addition, when this system is used in a corporate network, it can be used to access the network from a terminal that moves between multiple AP zones

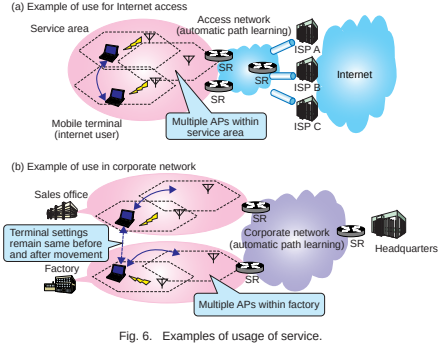

Fig. 6. Examples of usage of service.

located within an office or factory. It is also possible to continue to use a corporate network without changing any terminal settings when a terminal moves from a factory using a wireless LAN to another office within the same company (**Fig. 6(b)**).

In the future, we plan to further reduce interruption times to develop a system capable of handling high-speed movement such as a moving car or train. Remaining issues to be addressed include identifying in detail the operations of handovers in the wireless layer and making improvements in the upper layers to reduce processing times.

Reference

[1] C. Parkins, "IP Mobility Support for IPv4," RFC2002, IETF, Aug. 2002.

Tomoyoshi Motoyama
Broadband Service Promotion Headquarters, NTT West Corporation. He received the B.E. degree in engineering systems from Tsukuba University, Tsukuba, Ibaragi in 1998. In 1998, he joined NTT Access Network Service Systems Laboratories, Chiba, Japan. He was engaged in R&D of ATM access transport systems, ATM routers, bandwidth control equipment, and mobile access systems. In 2003, he was transfered to NTT West Corporation.

Masato Eguchi
Research Engineer, Access Service and Network Architecture Project, NTT Access Network Service Systems Laboratories.
He received the B.E. and M.E. degrees in civil engineering from Tohoku University, Sendai, Miyagi in 1992 and 1994, respectively. In 1994, he joined NTT Access Network Service Systems Laboratories, Tsukuba, Japan. He was engaged in R&D of inspection systems for conduits. In 1999, he joined NTT Communications and engaged in business incubation and access network service creation. In 2003, he returned to NTT Access Network Service Systems Laboratories.

Kouichi Suto
Senior Research Engineer, NTT Access Network Service Systems Laboratories.
He received the B.E. degree in electrical engineering from Iwate University, Morioka, Iwate in 1977. Since joining NTT Laboratories in 1977, he has been active in developmental research on optical fiber trunk transmission systems and optical fiber subscriber transmission systems. From 1999 to 2002, he was engaged in development of an access control server system for IP-VPN service. Since 2002, he has been engaged in developmental research on access network services using ADSL and/or FTTH systems. He received the Electronics Letters Premium from IEE in 1978. He is a member of IEEE.