

Secure Communication Infrastructure for Mobile Computing

Tetsuya Kawano
Susumu Matsui
Toshikazu Yasue
Chisato Konno

OVERVIEW: The business operations of companies are becoming increasingly centered around data systems and networks as the information-oriented society continues to evolve. User demands are no longer confined to the conventional office-centered environment, but now are being extended to business operations in the field as well. For example, today's users are asking for the capability to (1) access enterprise databases from the field to obtain client and inventory information, and for the ability to (2) transmit e-mail and status reports from home to the office for additional efficiency. Meanwhile, all the elements needed to meet these demands are now becoming available with the development of compact, lightweight, powerful portable terminals; the availability of basic and application software for portable terminals; the deployment of mobile telecom infrastructure technologies; and the growing attention of the business community to the potential of mobile computing. But in order to build a seamless computing system environment that supports mobile computing, a mobile environment must be constructed that compares favorably with the enterprise LAN environment in terms of (1) faster transmission bit rates, (2) enhanced security, and (3) adequate assurance of Internet addresses for mobiles. To provide solutions to these and other issues and to propose a mobile computing environment based on optimum security, Hitachi offers a wide product range of portable terminal equipment and other hardware products as well as software products. Hitachi is developing and deploying a system that provides a robust communications platform supporting secure mobile computing based on leading-edge communications and security technologies.

INTRODUCTION

ALONG with the rapid spread of the Internet, the deployment of enterprise intranets has not just been confined to large-scale corporation but is seeing rapid deployment in small-to-medium sized firms as well. This development is having a profound impact on the way companies conduct business. Up to now, data communications have largely been conducted within or between the central offices and the branches of the same companies, but now we are seeing a ground swell of interest in secure mobile computing. These expectations are driven by the development of smaller, lightweight, high-performance terminals; longer-life batteries; basic software tailored for portable terminals; and rapid advances in mobile computing technologies.

This will permit more efficient business operations by enabling mobile professionals to communicate or transmit data from remote locations such as from home or from a client's site, to retrieve customer information

or product inventory data from the company's database when they are in the field, and by enabling salespeople in the field to make efficient use of available data in preparing quotations or securing orders.

This article will discuss mobile communication needs, wireless technologies expected to emerge in the near-term future, security technologies that are indispensable for achieving system reliability, and the next-generation Internet protocol version 6 (IPv6) as a communications platform for supporting secure mobile computing in the context of Hitachi products and industry trends.

OVERVIEW OF THE MOBILE COMMUNICATIONS NEEDS

Fig. 2 illustrates the needs of corporate users for mobile computing and underlying mobile communications infrastructure that can enhance business efficiency and broaden business opportunities.

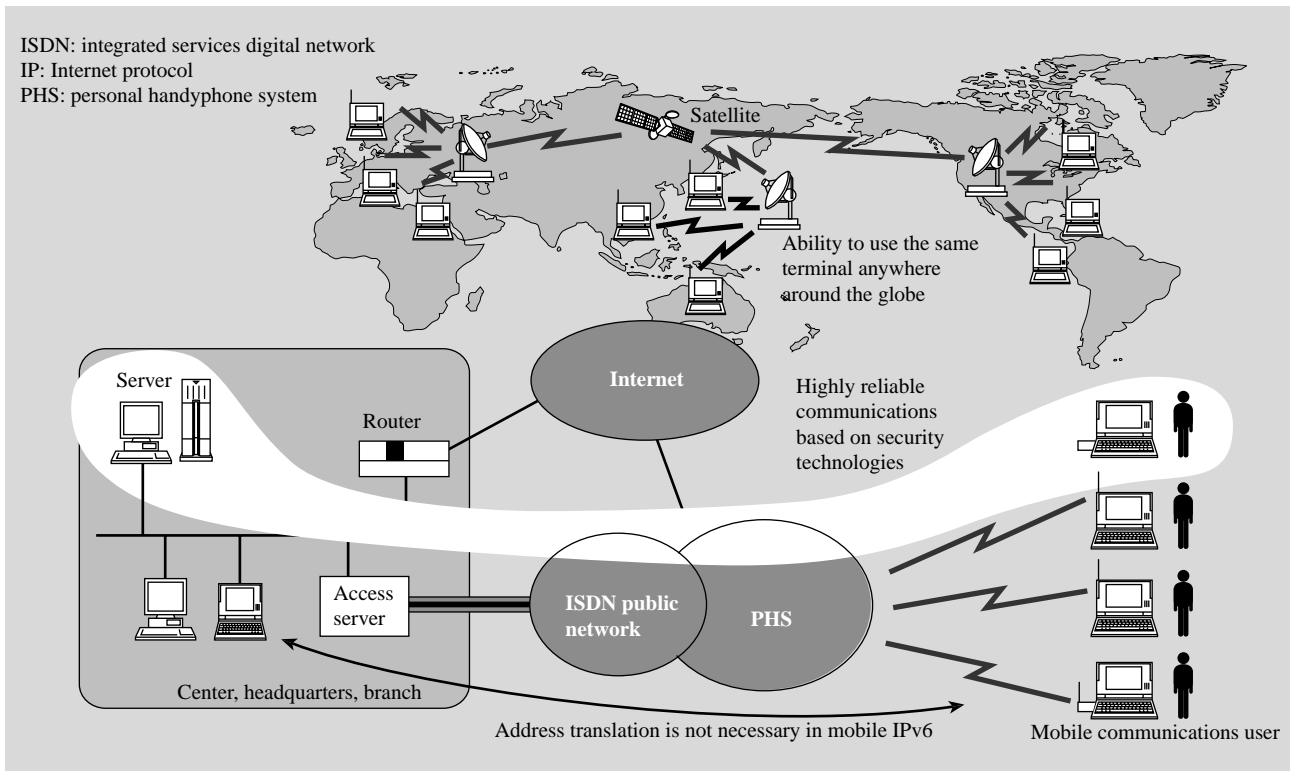


Fig. 1—Mobile Communications Overview.

Today there is a pronounced emphasis in companies on secure mobile computing to extend business at home and abroad and to promote business efficiency.

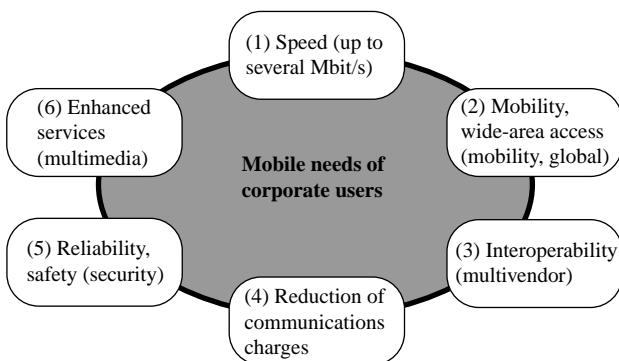


Fig. 2—Mobile Communications Needs of Corporate Users.

The needs of corporate users regarding mobile communications can be summarized in six key concepts.

Network communications media can be broadly classified as fixed landline and wireless facilities.

Fixed wire facilities consist of copper and fiber-optic cables, and support highly reliable communications services at high bit rates. The disadvantage of landline facilities is that the call origination and reception points are fixed and thus are not well suited to professional mobile endeavors using portable terminals. Wireless, on the other hand, support communications services that do not rely on physical cabling. This class of services is not constrained by

the deployment of physical wiring and offers much greater flexibility in deploying unconstrained systems. This makes it possible to provide communications environments that support simple communications anytime and anywhere, an environment that is particularly well suited to portable terminals.

Until now, wireless services has been predominantly voice-oriented applications using analog cell phones and mobile phones, and because conventional wireless could only transport data at a sluggish 2.4 kbit/s, the only office tasks it was capable of supporting were e-mail and receiving and placing orders. Now, however, we are already seeing substantial improvements in the reliability of wireless communications through the digital technology and such security technologies as encryption and authentication. And with the availability of high 2-Mbit/s transmission when International Mobile Telecommunication 2000 (IMT-2000) is implemented, this will lead to a transformation of the core ways in which we currently use data communications. This will not only expand the breadth and range of applications, it will also open the way to multimedia communications that incorporate images and a significant reduction of tariff charges.

In addition, the current state of wireless communications has evolved in such a way that different carriers, countries, and regions support their own interfaces: PCS (personal communications system) in the U.S., GSM (global system for mobile communications) in Europe, and PHS (personal handyphone system) in Asia. However, international standards are currently under study by the International Telecommunications Union (ITU) that should within the near-term future permit communication anywhere in the world by the same terminal.

SYSTEM BUILDING TECHNOLOGIES

In this section we will describe the current state and future direction of wireless data communications, the basic platform supporting mobile computing.

Current State of Wireless Data Communications

In Japan today there are two wireless data communications platforms that can be employed nationwide, the personal digital cellular (PDC) system and the personal handyphone system (PHS).

The key specifications of the two systems are compared in Table 1. A fundamental difference between the PDC and PHS systems is in the size of their cells; that is, the area covered by a single radio base station. Cells in the PDC system are on the order of several kilometers, while those in the PHS are on the order of several hundred meters. This difference affects the time that mobiles can be used as well as the distance mobiles can travel in the two systems. Since PDC cells are so much larger than PHS cells, considerable power is needed to communicate with a base station, and usage time at the same battery capacity is relatively short. Furthermore, considerable processing overhead is involved to effect switching (or handoff) when a terminal moves from one cell to another, and this can result in calls being dropped. The fact the cells are smaller in the PHS compared to the PDC system means that handoffs occur more frequently when moving at the same speed, which leads to increased overhead and the possibility of calls being terminated. In other words, the terminal mobility speed is slower in the PHS than in the PDC system. The current mobility speeds of the PDC system and the PHS are said to be approximately 80 km/h and 20 km/h, respectively. But comparing the data transmission capability, PDC currently supports full-duplex modem transmission at 9.6 kbit/s, while PHS supports 29.2-kbit/s data transmission. As one can

TABLE 1. Specifications of the PDC System and PHS
PHS is superior in terms of speed, but PDC offers a number of advantages.

Item	PDC system	PHS
Frequency band	800 MHz/1.5 GHz	1.9 GHz
Multiplexing	TDMA	
Channel bit rate	14 kbit/s	32 kbit/s
Cell radius	Several kilometers	Several hundred meters
Quality output	800 mW	10 mW
Mobile speed limit	Approx. 80 km/h	Approx. 20 km/h
Data transmission rate	9.6 kbit/s	29.2 kbit/s

TDMA: time-division multiple access

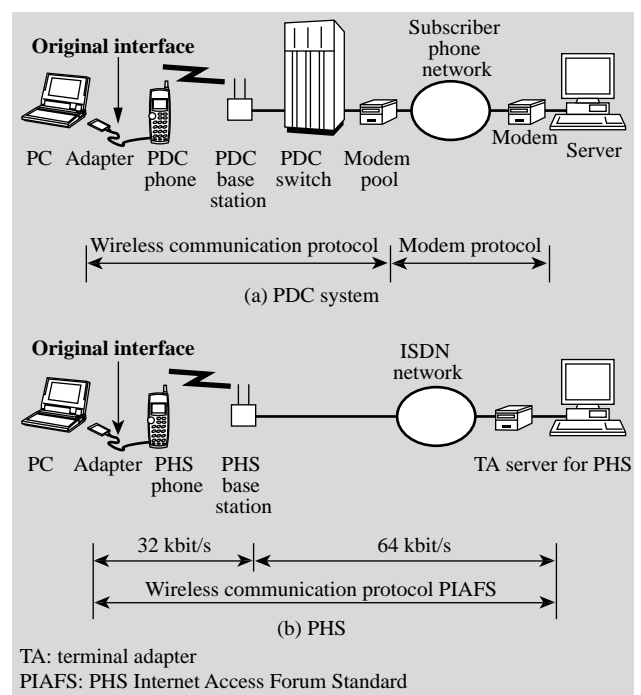


Fig. 3—Data Transmission: PDC System versus PHS.
The PDC system implements modem pull in the network thus enabling communication with a conventional modem on the server side. By contrast, PHS requires a dedicated TA on the server side.

observe from Table 1, this difference depends on the channel bandwidth—that is, the bandwidth occupied by a call.

Fig. 3 is a schematic showing how data transmissions are handled by the PDC and PHS systems. The connection between the adapter and client terminal can be implemented by either an RS-232C PC or by a PCMCIA (Personal Computer Memory Card International Association). Adapters are connected to cell phones using a 16-pin proprietary digital interface,

which differ for the PDC and PHS systems. On the network side, PDC implements a modem pool approach in which the PDC wireless protocol with the adapter is converted to the modem protocol. By contrast, PHS provides a 32-kbit/s bearer channel connection linking a server to the ISDN on the network side.

Future Trends in Wireless Data Communications

Current cellular mobile radio systems such as PDC and PHS are considered digital second-generation standard services (coming after the analog first-generation standards). Although second-generation system support terminal mobility or roaming within systems, they are incapable of supporting terminal mobility between different systems, say between Japan and Europe. The data rates of second-generation systems, moreover, do not exceed 32 kbit/s. Meanwhile, efforts are being stepped up on the third-generation cellular mobile radio standard called IMT-2000, and services are expected to become operational from the year 2000. IMT-2000 will provide global roaming (i.e., worldwide terminal mobility coverage) and support multimedia communications at high data rates from 384 kbit/s to 2 Mbit/s. To provide high-speed multimedia communications, Code Division Multiple Access (CDMA) that can accommodate variable-speed traffic is being applied as the radio transmission multiple access scheme, and Asynchronous Transfer Mode (ATM) is being applied as the network between wireless base stations and mobile switches.

With the advent of IMT-2000 third-generation radio systems, seamless interconnectivity with the Internet is indispensable. This means that a mobile Internet capability must be implemented featuring packet routing for efficient handling of Internet Protocol (IP) packets over wireless networks, and a mobile IP functionality to realize terminal mobility at the IP level. These capabilities will enable a genuine mobile computing platform that can support communications regardless of whether it is carried over fixed landline or wireless facilities.

SECURE MOBILE COMPUTING TECHNOLOGIES

In this section we will examine two types of technologies that are necessary to ensure a secure mobile computing environment: Internet-related technologies and data security technologies.

Internet-Related Technologies ^{1,2)}

The Internet consists of a vast collection of subnetworks that are connected to other subnetworks by routers. Every device connected to the Internet is identified by its own unique address which is called an IP address. An IP address consists of a subnetwork address in combination with a unique device address.

Mobile terminals also employ IP addresses to communicate in the Internet environment. However, if a portable terminal moves from one subnetwork coverage area to another area, then the IP address must change because the subnetwork address has changed. A fundamental issue for supporting mobile computing over the Internet is therefore how to achieve IP address resolution automatically. Three address resolution methods are listed in Table 2.

Each of these three methods is appropriate under different circumstances depending on the mode of use. A homepage, for example, uses client/server type communication, and employs the automatic allocation and automatic generation methods. However, when directly calling an address such as in the case of

TABLE 2. IP Address Resolution Methods

Proper use depends on the mode of operation. The IPv4 automatic allocation function applies to Windows 95 and Windows NT, but Hitachi's IPv6-compliant Router supports all of the blank areas.*

Method \ Version	Current Internet IPv4	Next-generation Internet IPv6	Facilities
Automatic allocation	○	△	Medium
Static	○	△	Large
Automatic generation	—	○	Small

○ : Internet Engineering Task Force (IETF) standard

△ : Being studied by the IETF

— : Capability not available

* Windows and Windows NT are registered trademarks of U.S.-based Microsoft Corporation in the U.S. and other countries.



Fig. 4—Hitachi's IPv6-compliant Router.

This robust router provides mobile support functionality for Internet terminals.

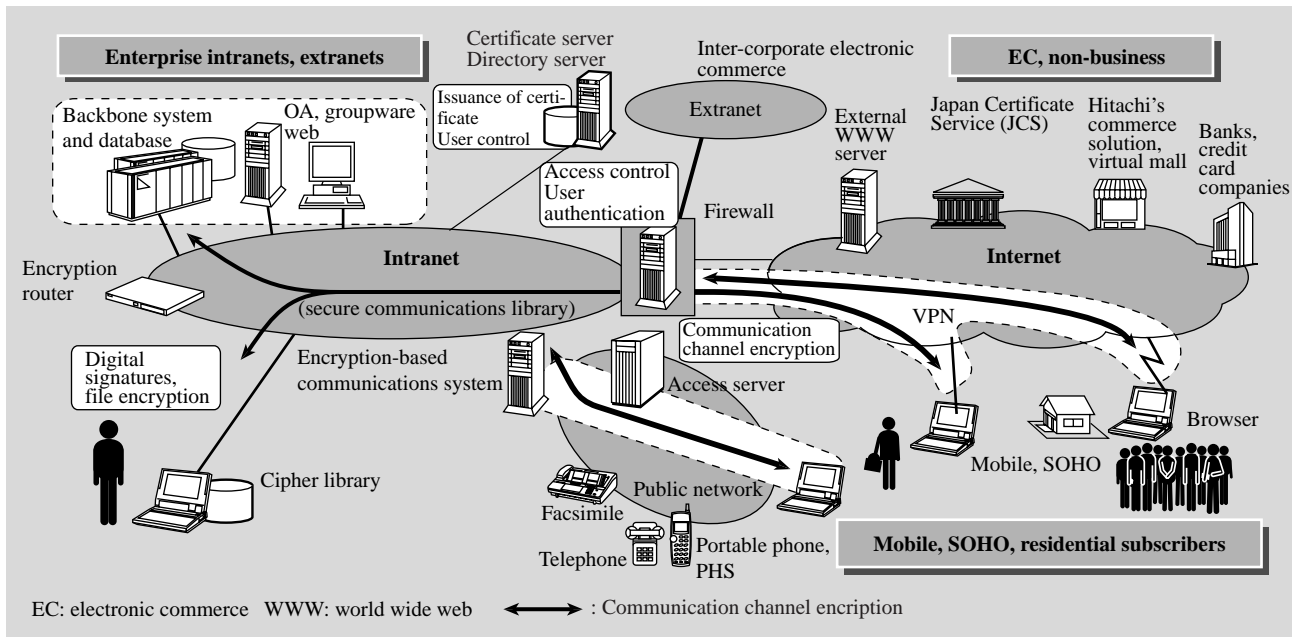


Fig. 5—Overview of Data Security.
Overview of security concerns and solutions in the mobile environment.

Internet telephony, the static fixed method is used.

The next-generation of IP (IPv6) will resolve the major problem facing the current IP (IPv4) that the unassigned pool of public addresses is quickly being exhausted and will also make it possible for mobile terminals to automatically generate their own IP addresses.

In a bold industry initiative, Hitachi has developed the IPv6-compliant router shown in Fig. 4 that supports both fixed and dynamic automatic allocation of IP addresses. Now let us take a closer look at these allocation methods.

(1) Automatic allocation method

A DHCP (Dynamic Host Configuration Protocol) server is implemented, and the network manager sets aside a block of IP addresses in advance for allocation. Then when a mobile terminal establishes a connection, an IP address is automatically allocated.

(2) Fixed method

Routers and gateways equipped with mobile IP agents are deployed in subnetworks at the origin and destination of mobiles. When a terminal equipped with mobile IP functionality travels, the agents at the starting and destination points cooperate to automatically send data for the terminal to the destination point.

(3) Automatic generation method

An IPv6-compliant router periodically allocates subnetwork addresses within those subnetworks. When

a terminal connects to the network, it receives this subnetwork address and automatically generates an IP address by combining the address with its own device address.

Information System Security Technologies³⁾

Information system security is extremely important for enterprise systems that allow access from small offices and home offices (SOHO) and from mobile systems over open networks such as a public switched telephone network. There is a range of system security capabilities that would be desirable to implement including ways to detect and prevent masquerading attempts, data alternation, wiretapping with data that was received over an open network, and a way to prevent someone from denying that he sent information when he actually did send the information. Fig. 5 is an overview of the security measures that are available to protect information systems. Let us take a closer look at the main considerations and countermeasures that are involved.

(1) Access control

To ensure that only authorized users are given access to corporate information systems, firewalls are implemented at ports between enterprise LANs and open networks. Firewalls regulate access to LANs by a variety of special access granting protocols, by regulating IP addresses, port numbers, through user authentication, and various other means. Two firewall

products that are currently available are Gauntlet*¹ and FireWall-1*².

(2) Data protection, communication channel encryption

To protect information while it is being transmitted through accessible communication networks such as telephone lines, and Internet, transmitted data is encrypted. By encrypting data that is sent over the network, this essentially turns an ordinary circuit into a Virtual Private Network (VPN). This capability can be implemented as an add-on function to a firewall by a dedicated subsystem.

(3) Authentication

To provide references for an on-line individual or organization, digital certificates based on the X.509 international standard are issued by a certificate server. Because authentication is performed on a per certificate unit basis by the certificate server, this enables one to verify whether the person operating the client machine is indeed the one who he purports to be.

(4) Digital signatures

One can detect whether data has been tampered with or verify the completeness of data by attaching a digital signature to the transmitted data. In addition to the library specifically for digital signatures, we also developed a secure communication library that encrypts transmitted data without the user being aware it is being done and detects tampering by means of digital signatures.

The above are basic data security technologies. Some of these security products are based on well-known de facto encryption standards such as RSA and DES, but other products have been developed around Hitachi's own symmetric key encryption system MULTI2 which is highly secure and registered to ISO. Plans are also in place to apply the Hitachi's elliptic curve encryption product, a robust next-generation public-key encryption scheme.

CONCLUSIONS

In this article we have surveyed the current state and future trends of wireless data communications technologies as a communications platform for supporting mobile computing systems. We highlighted the critical necessity for Internet addressing and data security technologies to support mobile computing, and presented an overview router and security products

that incorporate these technologies.

In the future, we will continue contributing to standardization efforts promoting these leading-edge technologies, while at the same time continuing to offer a diverse array of products and solutions that anticipate the needs of users.

REFERENCES

- (1) S. Thompson, et al., "IPv6 Stateless Address Auto-configuration," RFC-1971 (August 1996).
- (2) C. Perkins, "IP Mobility Support," RFC-2002 (October 1996).
- (3) R. Sasaki, et al., "Internet Security," Ohm-sha (1996).

ABOUT THE AUTHORS



Tetsuya Kawano

Joined Hitachi, Ltd. in 1978 and now works at the System Product Planning Dept. of the Strategic Business Development Div. at the Information Systems Business Planning Div. He is currently engaged in the development of network products and support for network service product standardization, and can be reached by e-mail at t-kawano@comp.hitachi.co.jp.



Susumu Matsui

Joined Hitachi, Ltd. in 1980 and now works at the Network Platform Center of the 4th Division of the Systems Development Laboratory. He is currently engaged in the research and development of mobile computing communications. Mr. Matsui is a member of the IEEE, Information Processing Society of Japan, and The Institute of Electronics, Information, and Communication Engineers, and can be reached by e-mail at matsui@sdl.hitachi.co.jp.



Toshikazu Yasue

Joined Hitachi, Ltd. in 1970 and now works at the Network Dept. of the General Purpose Computer Div. He is currently engaged in the development of next-generation Internet products. Mr. Yasue is a member of The Institute of Electronics, Information, and Communication Engineers, and can be reached by e-mail at yasue@ebina.hitachi.co.jp.



Chisato Konno, D.Sci.

Joined Hitachi, Ltd. in 1977 and now works at the System Product Planning Dept. of the Strategic Business Development Div. at the Information Systems Business Planning Div. He is currently engaged in the planning of security-related products. Mr. Konno is a member of the Information Processing Society of Japan, and the Japan Society for Industrial and Applied Mathematics, and can be reached by e-mail at c-konno@comp.hitachi.co.jp.

*1 Gauntlet is trademark of Network Associate, Inc. of the U.S.

*2 FireWall-1 is a trademark of Check Point Software Technology, Ltd.