Wearable Key: Device for Personalizing nearby Environment

Nobuyuki Matsushita, Shigeru Tajima, Yuji Ayatsuka, Jun Rekimoto
Interaction Laboratory,
Sony Computer Science Laboratories Inc.
3-14-13 Higashi-Gotanda, Shinagawa-ku,
Tokyo, 141-0022, JAPAN
+81 3 5448 4380
{matsu, tajima, aya, rekimoto}@csl.sony.co.jp

ABSTRACT

This paper describes a system that allows users who obtain a "wearable ID key" to personalize dynamically ubiquitous computers by simply touching them. We call the concept of providing personalized service by touch *"Active Personalization"*. For active personalization, users only have to wear a digital key and do not have to carry around other computers. When users touch ubiquitous computers with their wearable key, the keyholes of the ubiquitous computers recognize their IDs and can personalize the computers. We developed a new network technology between keys and keyholes that enables digital information to be carried through a person's body based on a near-field technology we call *TouchNet*.

1 Introduction

Ubiquitous computing and wearable computing have been posed as polar opposites even though they are often applied very similarly. Both ubiquitous and wearable computing have their own advantages [8][13]. Many people think that the computing environment in the future will be an integrated one in which ubiquitous and wearable computers cooperate. Therefore, exploring different cooperation styles is an important and interesting topic [4][11].

Since one of the purposes of these systems is computing without typing commands, defining and detecting the user's context is a very important issue. Ubiquitous and wearable computers show information that is adapted for the user, invoke appropriate applications, and provide other helpful and personalized services. If computers can detect context more precisely, they can provide better services.

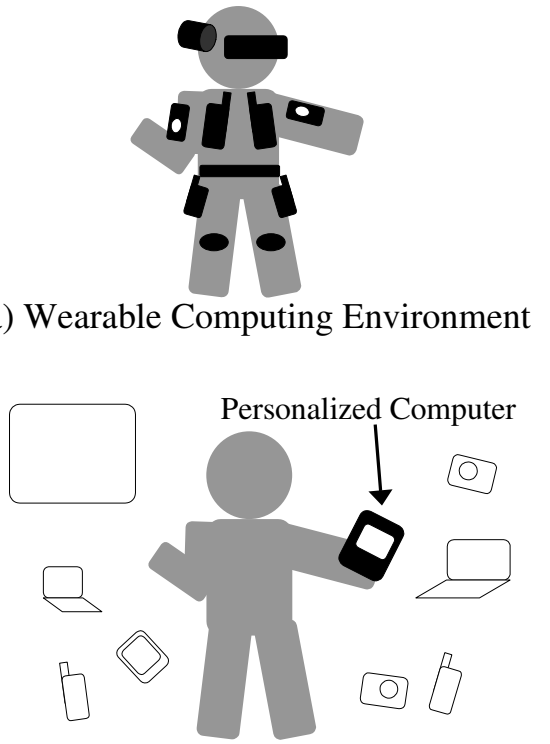
Most traditional context-aware systems use location information to determine context [9][7][14][12]. However, context continuously changes even when a user stays in the same place. For example, the contexts differ when the user writes a memo or phones another person. Location information is insufficient for supporting such situations.

People are almost always holding or touching something while performing daily tasks: a pen to write a memo, a cellular phone to talk to someone, a door knob to open a door, a keyboard to type, a drawer to take something out, and so on. Therefore, touch could be used as a trigger to change detailed context to invoke specific services. For example, when you pick up the receiver your own address book would appear on the screen.

We call the concept of providing personalized service by touch *"Active Personalization"* (Figure 1). Here, we describe a wearable key that sends an ID to objects via the body. Data is transferred via the body by a network module called *TouchNet* [1].

In the next section we describe the features of active personalization through a scenario, and technical issues are discussed in subsequent sections.

Proceedings of the Fourth International Symposium on Wearable Computers (ISWC'00)
0-7695-0795-6/00 $10.00 @ 2000 IEEE



(a) Wearable Computing Environment

(b) Active Personalization Environment

Figure 1: Comparison between Wearable Computing Environment and Active Personalization Environment: (a) Wearable Computing Environment: the user wears and carries around many personalized computers. (b) Active Personalization Environment: the user personalizes ubiquitous computers while holding and touching them.

2 Active Personalization

Active personalization is the concept that the ubiquitous computing environment provides users with personalized services by touch. When a user holds or touches ubiquitous computers, computers identify the user and are personalized dynamically while the user is holding or touching them.

Let us start with a theoretical scenario that takes place after active personalization has become commonplace.

While on a trip with a friend, you see an interesting car on the street. You regret not having brought your camera, so you borrow one from your friend, and take a picture of the car. The camera identifies your ID to be personalized as your camera and sends the picture to your database.

When you reach the hotel and touch the bell on the front desk, you can check in, and a room number is displayed. The door of your room unlocks as you grasp the door knob. When you hold the TV remote control, the picture of the car you took with your friend's camera is displayed on TV. You hand the control to your friend, your friend selects the movie your friend bought yesterday from lists displayed on the TV.

The concept of active personalization can be summarized by the features outlined in the following subsections.

2.1 Fine Grains of Authentication

With active personalization, finer grains of authentication occur than the ones used to log onto conventional PCs. When users log onto desktop computers, the right to use them continues until the user logs off, and the user must be authenticated only when they log on. However, when the user borrows the camera to take a picture, the camera is personalized only while the user is holding it: e.g., the pictures taken by the user must be stored by his or her database. It is too laborious to type a password to personalize the camera whenever the user presses the shutter button.

Active personalization is triggered by touch, and makes it possible to personalize ubiquitous computers in a short time. Ubiquitous computers are personalized while the user is touching them. When the user takes user's hands off computers (of course with some grace time), computers are depersonalized.

2.2 Low Cost of Authentication

With active personalization, the cost of authentication is lower than that required to buy something with a credit card. When a user buy something at a shop with a credit card, it is reasonable for the user to sign, because the user has spent their own money. However, when a user borrows a camera, it is not so critical that they own the picture.

There is trade-off between cost and benefit of authen-

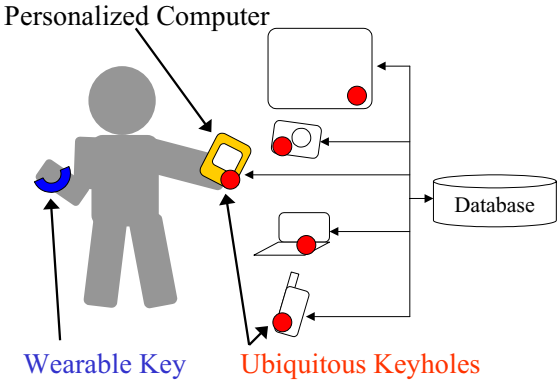


Figure 2: System Design: the user can personalize ubiquitous computers by simply wearing a key. Ubiquitous computers with keyholes are networked and share a database.

tication, low-cost authentication like active personalization, enables the environment to provide minor but helpful services.

3 System Design

To achieve the concept described in the previous section, we are currently developing a prototype system based on wearable and ubiquitous computers. Figure 2 shows the overall system design of the prototype. The system shares a database on the network through wired or wireless communication.

3.1 Wearable Keys and Ubiquitous Keyholes

For active personalization, users only have to wear a key. With this key, users do not have to carry around other computers.

In a ubiquitous computing environment, almost all computerized devices, such as PCs, PDAs, and doors and drawers are networked by wired and wireless network technology. By attaching ubiquitous keyholes to these devices, they will be able to identify the wearable keys.

When a ubiquitous keyhole detects a user, the device can be personalized according to the user's data. On the network, a shared database stores user data, such as profiles, documentation, charge information, and operational logs. For instance, computers will be able to download documentation, manage access control and accounting, and record a user log.

3.2 Communication between Keys and Keyholes

Communication between wearable keys and ubiquitous keyholes is available only while the user is holding or touching devices in the ubiquitous computing environment.

To achieve this, we developed a new network technology that enables digital information to be carried through a person's body based on a near-field technology we call TouchNet. Because keys and keyholes exchange small data such as IDs or password to identify users, the network is not required to be broadband. The most important feature is the existence of a communication path that can be controlled according to whether users touch keyholes with keys or not. In the next section, we describe the details of the TouchNet.

4 TouchNet

We have been developing a network technology that enables digital information to be carried through the body named TouchNet [1] since 1993 using near-field technology like BodyNet [2]. The following sections describe the principle, features, and implementation of a TouchNet module.

4.1 Principle

The TouchNet transmitter is made up of a signal generator, a modulator, and a transmitter electrode (Figure 3). The receiver is made up of a receiver electrode, a demodulator, and a signal detector. The transmission signal is FSK (Frequency Shift Keying) modulated and fed to the transmitter electrode. By touching both electrodes, the modulated high-frequency signal is conducted by the person's body and then demodulated by the receiver to reproduce the original signal. The explicit signal path is from the transmitter electrode to the receiver electrode via the body; the return path is a near electromagnetic field.

The body can be thought of as a container with conductive liquid inside, and the high-frequency signal is conducted by the surface and then returned via

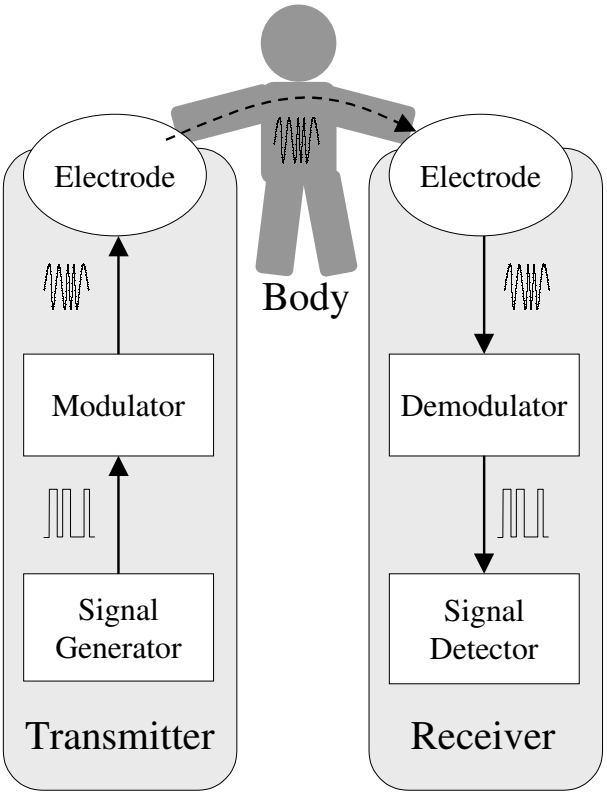


Figure 3: Principle of TouchNet: The transmission signal is FSK modulated and fed to the electrode. By touching both electrodes, the modulated high-frequency signal is conducted by the person's body and then demodulated by the receiver.

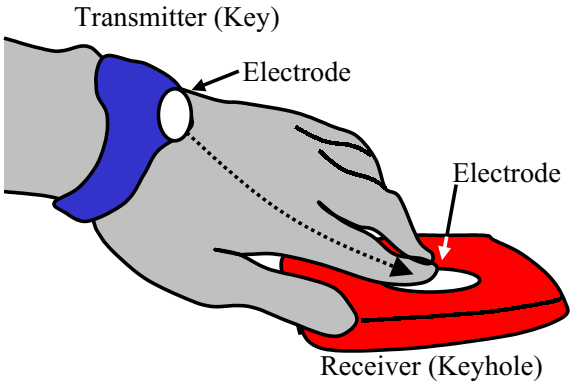


Figure 4: Key and Keyhole: When the user wears a wristwatch-like transmitter generating a user-unique ID signal with the electrode in contact with the body, the receiver identifies the user.

Figure 5: ToucnNet Module: The module size is 20×48 mm and can be put into a wearable key and ubiquitous keyholes. The transmission speed is 9600 bps, and the module has half-duplex communication.

the electromagnetic field. The strength of the near electromagnetic field is inversely proportional to the cube of the distance, so the communication distance is limited. However, as will be shown in this paper, this limitation is exploited. In addition, the strength of the modulated signal is small, and the data transmission channel only exists when touching both electrodes.

4.2 Features

As described above, the TouchNet system can only transmit data while both the transmitter electrode and the receiver electrode are connected via the human body.

When a user wears a transmitter with the electrode in contact with the body, the receiver can detect the touch or existence of the user by detecting the modulated high-frequency signal (Figure 4). If the transmitter generates a user-unique ID signal, the receiver not only detects the existence, but also identifies the user. This is one unique feature of the TouchNet system and can be used to identify who touched what in a networked TouchNet environment. Therefore, active personalization is achieved by using this system.

4.3 Implementation of TouchNet Module

We designed a custom transceiver module based on the technology described above (Figure 5). The module is made up of a modulator, a demodulator, a filter, a tuning amplifier, an electrode, an RS-232C interface,

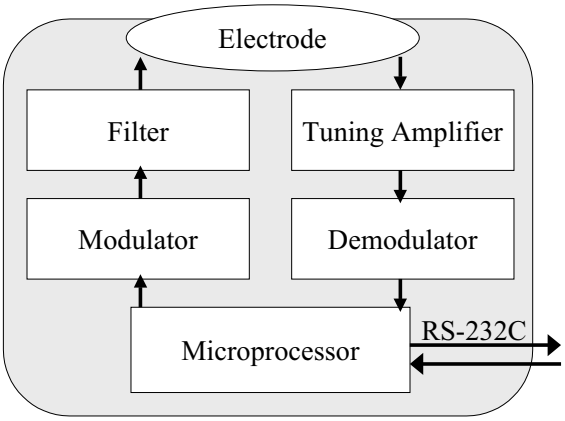


Figure 6: Block Diagram of TouchNet Module: The module is made up of a transmitter, a receiver, an electrode, an RS-232C interface, and a controller microprocessor.

and a controller microprocessor (Figure 6).

The microprocessor (Microchip Technology, Inc. 16F84A) generates the transmission signal and recognizes the received signal. The data transmission and reception between one set of modules are as follows. For transmission, the signal generated by the microprocessor is FSK modulated by carriers of 10 and 14 MHz and fed to the transmission electrode after filtering out the harmonics. The RF signal is conducted by the body to the receiver electrode. The input signal is tuning amplified by the receiver module and then demodulated. The demodulated signal is fed into the microprocessor, which eventually processes the data. The transmission speed of the current system is 9600 bps, and the module has half-duplex communication. This specification is enough to exchange small data such as IDs or password between keys and keyholes.

The module is equipped with an RS-232C interface, and can communicate with PCs and PDAs. This makes it easy to connect the TouchNet module to the network via an existing PC network.

The firmware of the microprocessor is programmed in C (HI-TECH C). The firmware is in-system programmable and is easily adapted to use with the TouchNet module for such tasks as converting RS-232C from

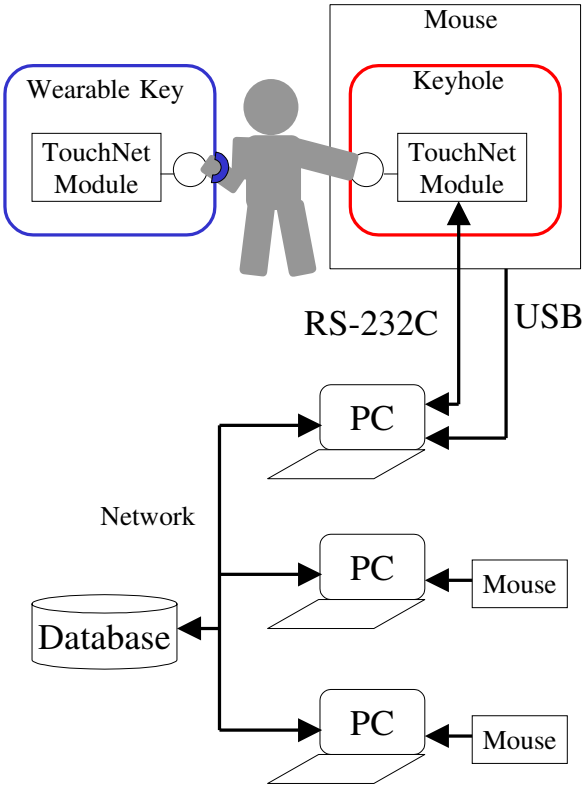


Figure 7: Setting of Hardware: TouchNet modules are installed in a wearable key and ubiquitous keyholes. When the PC identifies the user, the PC downloads the user data from database to personalize the PC.

a PC to a TouchNet connection, constructing an ID transmitter for a wearable unit, and implementing a specific protocol for identification.

The module is designed to be operated at 2.5 to 5V using a conventional battery. The power of the modulator and demodulator blocks is independently controlled by the microprocessor to save power. The current system consumes 50mW when the block is active, but this consumption can easily be reduced to 10mW by controlling the processor. The module sizes is 20×48 mm and can be put into a wristwatch-like unit to create a personal identification key and ubiquitous keyholes to recognize the IDs.

Figure 8: Wearable Key: The TouchNet module is put into a wristwatch-like unit. The user wears the key with the electrode of the TouchNet module in contact with the body.

Figure 9: Ubiquitous Keyhole: The TouchNet module is installed in the PC's mouse as a keyhole and connected to the PC through an RS-232C interface. The electrode of the TouchNet module is placed on top of the mouse.

The current system can not detect signal collisions, only half-duplex transmission is possible, but there are few problems in using the system as an identifier for an active personalization device. However, we are planning to develop modules that allow communication between multiple units.

5 Implementation of a Prototype System

We describe the implementation of a prototype system (Figure 7).

5.1 Setting of Hardware and Software

The wearable key contains the TouchNet module. The module is put into a wristwatch-like unit that uses a personal identification key (Figure 8). The wearable key is battery operated, and users wear the key with the electrode of the TouchNet module in contact with the body.

Sub-note PCs (Sony VAIO-C1XF) are installed in an environment as ubiquitous computers. They communicate to the network through a wireless LAN (Buffalo Airconnect). The PC applications are programmed in Java (jdk1.2.1). A TouchNet module is installed as a keyhole in the PC's mouse and connected to the PC through an RS-232C interface (Figure 9). The electrode of the TouchNet module is placed on top of the mouse. When a user controls the PC by moving the mouse, the electrodes of the key and keyhole are connected via the body (Figure 10). The key and keyhole then communicate by TouchNet technology. The wearable key sends the ID of the user to the ubiquitous keyhole.

To enable communication between keys and keyholes, a simple string-based packet that can be specified source and destination is implemented. A thruput via the packet is 800 bps, and is enough fast to be used for active personalization.

5.2 Example Sequence

Once the ID is recognized by the keyhole, the PC downloads the user data to personalize the PC. Thus, the user can personalize PCs simply by touching them with a wearable key. Because the PCs are connected to a shared database, the user can continue their work at other PCs. Ubiquitous computers can therefore be shared by many users.

For example, a drawing application appears on the display, then loads pictures that the user previously created. The menus and icons for the application are then relocated according to the user's preference. When another user holds the mouse to help a drawing

Figure 10: Personalized Computer: When the user controls the PC, the key and keyhole communicate. Once the key is recognized by the keyhole, the PC downloads the user data to personalize the PC.

Figure 11: Wearable Key with Fingerprint Reader (ENVISIONMENT): The owner of the key is identified by the fingerprint reader, and the encrypted biometrics features are sent to the keyhole.

of the previous user, the application is re-personalized automatically without a logoff and login sequence. Moreover, the user can continue the drawing at other PCs. Thus, with active personalization the ubiquitous computing environment is shared and personalized by touch.

Although we used sub-note PCs as ubiquitous computers in our implementation, we can also use any computerized devices as ubiquitous computers and share them with many people. This means that people do not have to carry around computers, but only have to wear a wearable key to personalize ubiquitous computers.

6 Related Work

In the context of wearable and ubiquitous computers, the idea of deploying machine-readable IDs in the environment is gaining popularity. Many applications exist that present context-based information such as tour-guides [9][7] and general notes related to a user's context [14][12]. In these systems location is sensed on the wearable computers either by GPS or location beacons. Similar systems have used paper labels that are recognized through machine vision to identify a location or object [3]. However, the context continuously changes even when a user stays in the same place. Location information is insufficient for supporting such situations.

Since people are almost always holding or touching something while performing daily tasks, touch could be a trigger to change detailed context in order to invoke specific service. There are technologies that sense the near touch, such as RF Tag [5] and Java Ring [6]. With RF Tag, users have to move their RF Tag very close to an RF reader. With Java Ring, users have to insert the ring into the keyhole. These limitations prevent natural actions from occurring. With TouchNet, even if users wear a wristwatch-like unit on their left hand, the environment reacts to the operation of the right hand. This feature enables the environment to support the user's daily work naturally. Moreover, even if detection of RF Tag and Java Ring might be used as a trigger to personalize the environment, it is difficult for the environment to determine the timing of depersonalization. With TouchNet, the environment can detect user's touch and release to determine the timing of personalization and depersonalization.

Biometric technology enables users to be identified without wearing anything [10]. With fingerprint identification, the environment can detect a user's touch and release. However, when the biometric features are stolen by ill-intentioned devices, people

can not get services because the biometric features are not encrypted, and people can not change their biometric features. The TouchNet module can encrypt the information between the key and keyhole in CPU. There is a possibility of installing the fingerprint reader in the wearable key to encrypt the biometrics feature and to identify the owner of the key (Figure 11). Active personalization is a broad concept that includes authentication.

7 Conclusion and Future Work

In this paper, we have described "Active Personalization" where people can dynamically personalize ubiquitous computers by simply wearing a key. We have developed a network technology named "TouchNet" between the key and keyhole that enables digital information to be carried through the body using near-field technology. We have also developed working a prototype to explore this concept.

There are many points that must be discussed. Does the module have to only store ID, or store data as well? How will privacy be protected? What happens if touching occurs by mistake? We plan to continue exploring these points in the wearable and ubiquitous computing environment.

Acknowledgments

The authors would like to thank Mario Tokoro for his support of this work. We would also like to thank all of the members of Interaction Lab.

REFERENCES

[1] S. Tajima. Signal transmission technology using human body and near field(static field). *Japan patent application 7-170215*, 1993.

[2] E. R. Post, M. Reynolds, M. Gray, J. Paradiso, N. Gershenfeld. Intrabody Buses for Data and Power. *Proceedings of ISWC'97*, pp.52–55, Oct. 1997.

[3] J. Rekimoto, K. Nagao. The world through the computer: Computer augmented interaction with real world environments. *Proceedings of UIST'95*, pp.29-36, Nov. 1995.

[4] N. Khotake, J. Rekimoto, Y. Anzai. InfoStick: an interaction device for Inter-Appliance Computing. *Proceedings of HUC'99*, 1999.

[5] Y. Ayatsuka, J .Rekimoto, S. Matsuoka. Ubiquitous Links: Hypermedia links embeded in the real world. *IPSJ SIGHI Notes*, number 67-4, pp.23-30. Japan Information Processing Society, Jul. 1996. in Japanese.

[6] iButton. http://www.ibutton.com/

[7] S. Feiner, B. MachIntyre, T. Höllerer, A. Webster. A touring machine: Prototyping 3D mobile augmented reality systems for exploring the urban environment. *Proceedings of ISWC'97*, pp. 74-81, Oct 1997.

[8] M. Weiser. The computer for the 21st century. *Scientific American*, pp94–104, Sep. 1991.

[9] G. Abowd, C. Atkeson, J. Hong, S. Long, R. Kooper, M. Pinkerton. Cyberguide: A mobile context-aware tour guide. *ACM Wireless Networks*, pp. 421–433, 1997.

[10] A. K. Jain, L. Hong, S. Pankanti. Biometric Identification. *Communication of the ACM*, pp. 91–98, Feb. 2000.

[11] B. J. Rhodes, N. Minar, J. Weaver. Wearable Computing Meets Ubiquitous Computing: Reaping the best of both worlds. *Proceedings of ISWC'99*, pp.141–149, Oct. 1999.

[12] J. Pascoe. Adding generic contextual capabilities to wearable computeres, *Proceedings of ISWC'98*, pp. 92–99, Oct 1998.

[13] T. Starner, S. Mann, B. Rhodes, J. Levine, J. Healey, D. Kirsch, R. W. Picard, A. Pentland. Augmented Reality Through Wearable Computing, *Special Issue on Augmented Reality*, Vol.6(4), Fall 1997.

[14] B. Rhodes. The wearable remembrance agent: A system for augmented memory. *Pseronal Technologies Journal Special Issue on Warable Computing*, Vol. 1, No. 4, pp. 218–224, 1997.