The 24th IEEE International Conference on
Distributed Computing Systems Workshops
Hachioji, Tokyo, Japan
23-24 March 2004

Sponsored by
IEEE Computer Society and
The Information Processing Society of Japan (IPSJ)
Aware-Mail: an Event-driven Mail System for Wearable Computing Environments

Naoki MIURA†, Masakazu MIYAMAE†, Tsutomu TERADA‡, Masahiko TSUKAMOTO† and Shojiro NISHIO†

† Graduate School of Information Science and Technology, Osaka University
{naoki-m, miyamae, tuka, nishio}@ist.osaka-u.ac.jp

‡ Cybermedia center, Osaka University
tsutomu@cmc.osaka-u.ac.jp

Abstract

In recent years, e-mail has become widespread explosively and it became one of very important communication tools which anyone can use easily. Here, the wearable computing has also attracted a lot of attention. In wearable computing environments, a user brings and uses his/her own computer wherever he/she goes. Therefore, we can construct a new mail system by utilizing the features of wearable computing such as "hands-free", "always on", and "supporting daily life". In this paper, we propose a mail system for wearable computing environments, called Aware-Mail (Active Wearable system Applying Rule-based Engine for Mail). Our system provides new type of communications in wearable computing environments, such as automatic mail processing according to the user’s situation and exchanging information with other users by mail-based P2P communications.

1. Introduction

In recent years, e-mail has become widespread explosively. There are forty-three millions of personal computers mostly used for e-mail and browsing WWW pages in Japan[2]. Moreover, e-mail has currently come to be available on a cellular phone, and there are also fifty-four millions of cellular phones with the e-mail functionality in Japan[1]. As a device for e-mail has been changing from a stationary host to a cellular phone, the intended purpose of e-mail has also been changing from formal use (ex. business letters) to casual use (ex. chats and greetings).

Here, as a result of miniaturization and weight saving technologies, the wearable computing[4][6] attracts a lot of attention, which is a new computing style where users wear their computers wherever they go. Wearable computing has following three characteristics compared with conventional computing forms:

1. Hands-free: users use the computer without hands most always because they wear the computer and browse information on a wearable display.
2. Always on: the wearing computer is always powered. Therefore, users can use the computer whenever they want to use it.

Considering these characteristics, the intended purpose of e-mail may change according to the change of a device from a cellular phone to a wearable computer as well as the case of change from a stationary host to a cellular phone.

In this paper, we propose an e-mail processing system for wearable computing environments, called Aware-Mail (Active Wearable system Applying Rule-based Engine for Mail). Aware-Mail has three features: 1) rule-based e-mail processing, 2) command-mail, and 3) mail-based P2P (Peer to Peer) data sharing. We employ the framework of ECA rule for realizing the adaptive e-mail processing and information sharing. Aware-Mail will create a new communication method in wearable computing environments. The remainder of this paper is organized as follows. Section 2 explains the design of Aware-Mail. Section 3 describes the implementation of our system and Section 4 shows the service example. In Section 5, we consider the security problems of our system and Section 6 presents the conclusion and future work.

2. Design of Aware-Mail

Aware-Mail has the following three features:
1. Rule-based e-mail processing

Arrived e-mails are processed automatically by rules described beforehand.

2. Command-mail

Aware-Mail can send/receive not only mails described in plain text but also command-mails which enable various processings on the receiver’s computer.

3. Mail-based P2P data sharing

Aware-Mail enables the P2P data sharing based on data transmission using e-mail.

We describe the details of these features in the remainder of this section.

2.1. Rule-based e-mail processing

In wearable computing environments, users always wear their computers. As a result, users require various services using user’s context acquired by attached sensors (ex. changing the notification method of received mail according to the user’s situation, and replying to received mail automatically as long as the user is engaged in other works.)

In order to realize such functions, it is necessary to perform various processings according to emerging events happen in the system. Thus, Aware-Mail employs the framework of ECA rule to describe the system behaviors. ECA rule is the behavior description language used in an active database system which is one of the database technologies[3][5][7]. Each ECA rule consists of three parts: the event, the condition, and the action. The event part describes an occurring event in the system. The condition part describes conditions for executing the following action. The action part describes operations to be carried out when the event occurs and the conditions are satisfied. Figure 1 shows an example of ECA rules that changes the notification method of received mail according to user’s situation. Rule 1 displays the content of received mail in a pop-up window if the user is not using the computer. Rule 2 reads out the content of received mail if the user is not using the computer. Table 1 shows the list of events and actions which can be used in Aware-Mail. Using these events and actions, we can realize various services.

2.2. Command-mail

Generally, since users use a handy input device not suited for input of long sentences in wearable computing environments, sending a reply is a very difficult work for users. Therefore, if a user can reply to received mail by selecting prepared alternatives like questionnaire, it solves the problem of input devices in wearable computing environments. We make it possible by sending a e-mail with ECA rules. We call this type of e-mail command-mail. Figure 2 shows a screen shot of executing the command-mail and Figure 3 shows the example of attached ECA rules. Command-rule 1 displays a "yes/no" button when the mail is unsealed. Command-rule 2 returns a mail for notice of attendance and Command-rule 3 returns a mail for notice of absence and deletes these rules when the "yes" button is selected. Command-rule 3 returns a mail for notice of absence and deletes these rules when the "no" button is selected.

Since command-mail is an e-mail with ECA rules, it is possible to send ECA rules that provide various functions.
2.3. Mail-based P2P data sharing

Since users always wear their computers and store various data (ex. photos, sounds) in wearable computing environments, they will demand to exchange these data with other users. However, the opponent is not always connected to a network when a user wants to exchange information. Therefore, it is effective to use the mail for communication between hosts because the mail communication is asynchronous. From this point of view, we realize the mail-based P2P data sharing. Figure 4 shows the overview of behaviors in mail-based P2P data sharing. When a user requests information, the system automatically searches the persons who are admitted to send the P2P mail from user’s address book and sends an information requesting mail (IRM) to them. All commands which the receiver executes, such as retrieving information, returning information, and dissemination of mail, are described in the IRM. When the system receives an IRM, it searches the requested information automatically. If the requested information is found, the system returns the mail with the information, and if the requested information is not found, the system disseminates IRMs to other users by referring his/her address book. The user can acquire information from wide range users by using mail-based P2P data sharing.

We realize this function by command-mail. Figure 5 shows the example of rules attached to an IRM. Since the process of mail-based P2P data sharing is not visible to users, we have to consider the security management carefully. We describe the security management of our system in Section 5.

3. Implementation

We implemented the prototype of Aware-Mail on the A-WEAR[8]. A-WEAR is the rule processing engine for wearable computing environments that our research group has developed. Since we can extend functions of A-WEAR freely by adding plug-ins, we realized the functions of Aware-Mail as several plug-ins for A-WEAR. Figure 6 shows a snapshot of using our system.

We implemented the system using Microsoft Visual C++ 6.0 Enterprise Edition on SONY PCG-SRX7S/PB. We also used Microsoft Access as the database engine. Figure 7
[Information requesting rule 1]
E : Receive this mail
C : Receiver has the requested information
A : Return a mail with requested information and delete these rules

[Information requesting rule 2]
E : Receive this mail
C : Receiver do not have the requested information
A : Disseminate IRM to other users by referring the address book

Figure 5. The rules attached to IRM

Figure 6. A snapshot of using the prototype

shows the example of A-WEAR format rules that have same meaning as rules in Figure 3.

4. Service example

We consider the following scenario as a service example of Aware-Mail.

- A user wants the photo of the solar tower in Expo Memorial Park in Suita city. However, he/she is sick and cannot go there. Consequently, the user requests people who are in good health and stay around the solar tower to photo it and return it to the user.

Figure 8 shows the rules for this scenario. Information requesting rule 1 disseminates IRM to other users by referring address book if his/her location is not near by the Expo Memorial Park or his/her body temperature is more than 37 centigrades. Information requesting rule 2 requests to take photos, and sets up a timer if his/her location is near by the Expo Memorial Park and his/her body temperature is no more than 37 centigrades. Information requesting rule 3 returns the mail with the photos, and deletes the timer and these rules. In this way, we need only to use ECA rules to handle specific situations for providing services. If the system cannot understand the ECA rules such as the rule including unknown events and actions, these rules are ignored and affect nothing to the system.

5. Discussion on security issues

Since command-mail can perform various processings on receiver’s computer, we have to investigate the security management carefully. Moreover, we need to control the dissemination of IRM in mail-based P2P data sharing. We describe them in this section.

5.1. Security for command-mail

There are two situations that Aware-Mail receives malicious command-mails. One is transmission of malicious
command-mails and the other is interpolation of attached rules on communication pathway. Following solutions can be considered to improve the security of Aware-Mail and they are already implemented by using ECA rules.

**Authentication of sender**
When Aware-Mail receives a command-mail, it retrieves the information of the sender from the local database. The system determines whether the sender is registered to be trusted by referring this information. If and only if the receiver trusts the sender, the system executes the received command-rules. As a result, Aware-Mail executes command-mail only from trusted users, and the system prevents execution of malicious command-mail sent by unknown persons. However, senders can disguise their mail addresses because SMTP do not have the way to authentication. Moreover, users who are registered to be trusted may send malicious rules. Although resolve of these problems is a future work, we plan to propose the method to evaluate the rightness of the mail address by referring the transmission logs of the sender.

**Encryption of rules**
Malicious operations may be performed if rules attached to command-mail are altered on communication pathway. Thus, we have solved this problem by encrypting the rules attached to command-mail before the system sends it. However, even if command-rules are encrypted, the troubles may occur such as deletion of data and disclosure of personal information by attached rules. Although resolve of these problems is a future work, we plan to propose the method to analyze the content of received rules and forbidding execution of these malicious actions. In the case of using this method, it is also important to control the policy of permission/prohibition of actions in response to the sender.

### 5.2. Control of IRM dissemination

We have to control the dissemination of IRM in mail-based P2P data sharing. If not, the dissemination of IRM may not stop and the number of IRM increases in the geometric progression. Therefore, we implemented the mechanisms of dissemination control of IRM and prevention of re-execution of the same IRM. These mechanisms have been also realized by ECA rules.

- **Dissemination control of IRM**
We use following two methods alternatively to restrict the dissemination frequency and the number of dissemination at a time.

1. **Control by the information requesting person**
   In this method, the information requesting person has decided the total number of dissemination beforehand. When a relay person disseminates IRMs, he/she retrieves opponents permitted to send IRM by referring his/her address book and sends a check mail that includes the total number and mail addresses of dissemination candidates to the information requesting person. The information requesting person has also the policy that regulates the number of dissemination and the dissemination candidates concretely. When receiving a check mail, the information requesting person decides the receivers of IRM by investigating the information described in the mail, his/her policy, and the remaining number of dissemination. When a relay person receives the mail returned by the information requesting person, he/she decides the number of dissemination by comparing the permitted number of dissemination with his/her policy and dissemnates IRMs.

2. **Control by IRM in itself**
   In this method, the information requesting person describes the dissemination frequency and the maximum number of dissemination at a time in
an IRM. The dissemination frequency described in the IRM is reduced whenever the IRM is disseminated. A relay person does not disseminate IRM any more if the dissemination frequency described in the received IRM is 0. Otherwise, he/she decides the number of dissemination by comparing the maximum number of dissemination at a time described in IRM with his/her policy and retrieves opponents permitted to send IRM. Then, a relay person disseminates IRMs.

The former method can control dissemination completely. However, there are problems that a lot of mails are exchanged and all mail addresses of relay persons are revealed to the information requesting person because they send a check mail to the information requesting person before disseminating IRMs. The latter method can minimize the exchange of mails, and mail addresses of relay persons are not revealed to unknown persons because mails are exchanged between only acquaintances. However, there is a problem that the information requesting person can’t control IRM if once he/she sent it.

- Prevention of executing the same IRM
  A user may receive exactly the same IRMs from multiple users. To prevent the execution of same IRMs, the system attaches an unique ID to IRM on its generation. When a user received an IRM, the system judges whether the IRM was received for the first time by referring IRM IDs stored in the local database. The system stores the IRM ID and executes received rules in the case that the IRM ID is not stored. As a result, we can prevent re-execution of the same IRM.

5.3. Security for mail-based P2P data sharing

In mail-based P2P data sharing, it is very important to manage sharing data. Especially, private data and copyright data should be treated carefully. Moreover, there are possibilities of troubles such as reception of malicious rules. For resolving these problems, we employ the mechanisms to restrict sharing information and record logs described as follows. These mechanisms are also implemented by using ECA rules.

- Restriction of sharing information
  In our system, users store information about only sharing data in the database specialized for mail-based P2P data sharing. As a result, user’s private data are not shared.

- Recording logs
  Our system records logs to the local database when receiving and disseminating an IRM. We can bring out the cause of troubles by tracing the stored logs.

6. Conclusion

In this paper, we proposed Aware-Mail, which is an event-driven mail system for wearable computing environments. Aware-Mail realizes the new mail communication in wearable computing environments by utilizing three functions (rule-based e-mail processing, command-mail, and mail-based P2P data sharing).

In the future, we plan to propose methods for preventing misrepresentation of mail address and execution of malicious rules. Moreover, we plan to evaluate the usefulness of our system by field tests.

Acknowledgments

This research was supported in part by “The 21st Century Center of Excellence Program” of the Ministry of Education, Culture, Sports, Science and Technology, Japan, and Special Coordination Funds for Promoting Science and Technology of the Ministry of Education, Culture, Sports, Science and Technology of Japan.

References