Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE DIRECT®

ELSEVIER

Computer Networks 42 (2003) 493–502

COMPUTER NETWORKS

www.elsevier.com/locate/comnet

System integration of WAP and SMS for home network system

Chi-Hsiang Wu, Rong-Hong Jan *

Department of Computer and Information Science, National Chiao Tung University, 1001 Ta Hsueh Rd., Hsinchu 30050, Taiwan

Received 12 October 2001; received in revised form 16 December 2002; accepted 1 February 2003

Responsible Editor: S.K. Das

Abstract

This paper proposes a Home Network System (HNS) architecture integrated with Wireless Application Protocol and Short Message Service to support the connectivity between home and Internet/Global System for Mobile Communication (GSM) networks. The HNS architecture includes an HNS gateway and three home network subsystems, i.e., home appliance, security and messaging subsystems. The main objective of the integrated system is to remotely monitor and control the devices in the HNS via laptop computer or a GSM mobile terminal. In addition to responding to remote queries, the managed devices (e.g., home appliances or burglar alarm system) can actively send alerting messages to a mobile terminal when an abnormal state occurs. Through the HNS gateway, the monitoring and control information is diffused to the Internet/GSM network. An implementation of the HNS system is described in this paper as an illustration of the feasibility of the proposed architecture.

Keywords: Home networking; Wireless application protocol; Short message service

1. Introduction

In recent years, interest in home networking has increased significantly due to technological innovations and market forces. Improvements in microprocessor computing power and memory capacity, associated with decreasing costs, have ensured their widespread use. In addition, the development of the Internet has engendered new ideas for living and working that utilize every facet of technology. Many of these ideas offer achievable means of integrating information, processing and control for every individual user and device.

In order to utilize appliances efficiently and effectively and to increase comfort in the home, a Home Network System (HNS) is proposed. HNS is a small network that allows the connection of computers, audio and video equipment, washing equipment and home automation subsystems (e.g., heating and air-conditioning systems, lighting systems, etc.) in an integrated, cooperative environment designed to increase comfort and ensure the sharing and management of home resources as well as the provision of new, enhanced services.

Several specifications used in home automation already exist, including Consumer Electronic Bus (CEBus) [1,2], European Home System (EHS) [3,4],

* Corresponding author. Fax: +886-3-5721490.
E-mail address: rhjan@cis.nctu.edu.tw (R.-H. Jan).

1389-1286/03/$ - see front matter
doi:10.1016/S1389-1286(03)00198-1

European Installation Bus [5], BatiBUS [6], and so on; various technological characteristics and market penetration are taken into account in adoption. Network technologies such as cable TV (CATV), Integrated Services Digital Network (ISDN), Asymmetric Digital Subscriber Line (ADSL), and Digital Power Line are in different stages of standardization and implementation, but the basic characteristics offered by these standards are plug-and-play compatibility, simple installation, distributed control, multiple applications, and future-orientation.

Attractive services and applications are also required for an effective HNS. Ref. [7] proposes an architecture to support home Internet connectivity that provides HNS remote monitoring and control with computers. Wang et al. [8] present a HNS, called as *Aladdin*, which emphasized the dependability issues. In the Aladdin system, they propose (1) a soft-state method to track the health of the network entities, including devices, sensors, daemon processes, etc., (2) a system architecture to enhance the dependability of powerline control operations, and (3) a monitoring tool to automatically detect and diagnose unreliable device behaviors. In [9], Bergstrom et al. propose a home network server, called as Global Home Server, which emphasizes the communication security issues. Their system can leverage limited resources to provide confidentiality, authentication, authorization, and integrity for remote monitoring and control of home automation devices. In this paper, we present a HNS, which emphasizes the integration of personal communication techniques. Then, users can remotely control and monitor the home devices by a mobile phone at any time and in any place, even when they are moving.

In recent years, the development in personal communication has grown quickly-hundreds of millions of mobile phones are currently used all over the world. And while such widespread technological advances are exciting, it is even more exciting for individuals to operate their home appliances with a mobile phone, from the office or other exterior locations. For example, in the winter individuals may turn on their home heating systems in advance via mobile phone so that the desired room temperature is achieved before the individual arrives home.

Global System for Mobile Communication (GSM) [10] has already been widely deployed. Wireless Application Protocol (WAP) [11] has also been developed for mobile devices, such as mobile phones and personal digital assistants (PDAs), to access the Internet. Thus, the GSM user may make voice calls and also receive news, send and receive e-mails, and browse the Web pages with a WAP mobile station (MS).

Fig. 1 illustrates HNS architecture, which is centered on a personal computer connected to a GSM network/Internet and home network. This computer, called a HNS gateway, connects to home devices and runs a home automation management application that supervises home devices. In this paper we organize home devices into appliance, security, and messaging subsystems, respectively. The appliance subsystem consists of home appliances such as refrigerator, television, and so on. Security subsystem includes surveillance, burglar alarms, etc. Telecommunication devices such as answering machines and e-mail applications provide messaging services.

The home user can actively connect to the HNS gateway, as well as monitor and control the status of the HNS with a WAP mobile station or a laptop computer. The HNS gateway communicates with remote clients using the WAP or HTTP protocol [12], and translates the request messages it receives to the protocol used in the HNS. In addition, the HNS gateway can actively notify the home user when an abnormal state occurs. For example, an appliance can send an alerting message to the HNS gateway if an abnormal state occurs. The HNS

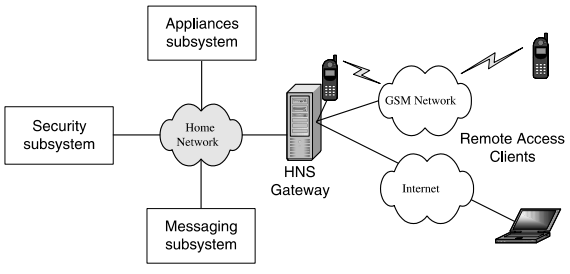

Fig. 1. Home network system architecture.

gateway receives this alerting message and relays it to the user using GSM Short Message Service (SMS) [13]. The home user may control the appliance remotely via WAP MS or go home immediately upon receipt of the message.

In this paper we propose a HNS architecture, integrated with WAP and SMS, to support the connectivity of home and Internet/GSM networks. The main objective of the integrated system is to remotely monitor and control the devices in the HNS via laptop computer or GSM mobile terminal. In addition to responding to queries, the managed devices (e.g., home appliances or burglar alarm system) can actively send alerting messages to a mobile terminal when an abnormal state occurs. An implementation of the HNS system is described in this paper as an illustration of the feasibility of the proposed architecture.

The remainder of this paper is organized as follows: Section 2 describes the proposed HNS architecture, Section 3 presents the implementation of the HNS, and the summary is given in Section 4.

2. Proposed system architecture

As shown in Fig. 1, the proposed HNS is composed of three subsystems, i.e., appliance, security, and messaging subsystems. Home devices in common use in each subsystem are summarized in Table 1. These subsystems are connected to a HNS gateway. The following are three proposed methods for communicating with home devices from remote locations:

1. *WAP:* As shown in Fig. 2(a), the home user actively connects to the HNS gateway to monitor and control, via WAP MS, the status of each home device.
2. *HTTP:* As shown in Fig. 2(b), the user can retrieve and set the control data of each home device via laptop computer connected to the HNS gateway.
3. *SMS:* As shown in Fig. 2(c), a mobile station with SMS capability can communicate with the HNS via SMS protocol. With SMS, the user can monitor and control the home devices.

Table 1
Devices in common use in each subsystem

Appliance subsystem	Security subsystem	Messaging subsystem
Air-conditioning	Surveillance	Answering machine
Lighting	Burglar alarm	Fax machine
Television		E-mail services
Video and audio player		
Refrigerator		
Microwave oven		

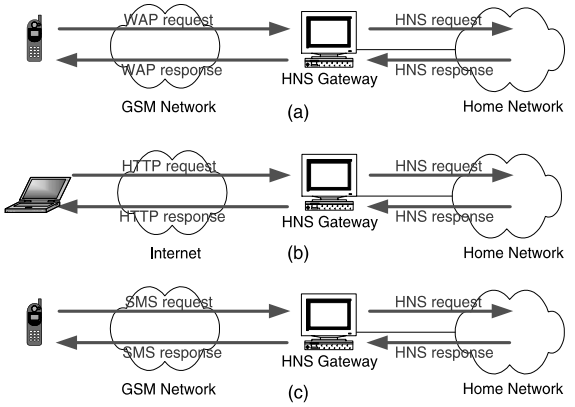

Fig. 2. Communication with the HNS in (a) WAP and (b) HTTP (c) SMS.

These methods employ a request-response mechanism, which allows a home user to monitor home appliances and control them, for example, users may turning on/off, check voice and e-mail messages, view real-time images captured by the surveillance system, and so on. That is, the request-response mechanism allows users to *pull* information from the HNS gateway and *post* control data to HNS gateway (i.e., set the control data to HNS gateway). In addition to pulling and posting information, the methods also offer a *push* mechanism that is very useful. That is, the HNS gateway can actively use WAP push [14], HTTP push mechanisms or SMS to send messages to a mobile station or laptop computer. For example, in the home appliance subsystem, an appliance can actively send an alerting message to the HNS gateway (by *posting information*) when detecting

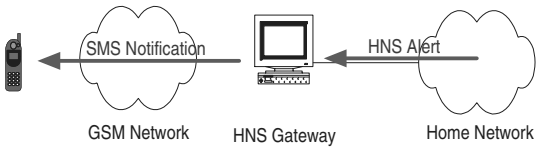

Fig. 3. Notification sent by SMS.

an abnormal situation or a warning signal. The HNS gateway receives this alerting message and then pushes it to the home user in SMS (see Fig. 3). Similarly, in the security subsystem, an alerting message can be sent when a burglar alarm rings or a surveillance system detects intruders. In the messaging subsystem, the HNS gateway notifies the home user when new e-mails arrive in the mail server, or new messages are recorded on the answering machine.

2.1. HNS management protocol

In HNS, we propose a management protocol that allows managers to configure, diagnose, and maintain home devices that are connected to HNS. The proposed management protocol employs the concept of a client-server model, which, in turn, forms the basis for a manager–agent model (Fig. 4). The network management model consists of an agent entity residing in each managed device, and the manager, residing in the HNS gateway, is used to control the devices. The manager issues commands to the agent for reading or modifying the data maintained by the agent. In normal situations, the agent entity only responds to the manager's queries. However, the agent entity is capable of reporting an event to the manager if an abnormal state occurs.

The management information transferred between the manager and the agents is handled by the management services. In [7], a set of management services that allowed the manager to control, monitor and reconfigure the agents was designed. Within the limitations of mobile handsets such as small screens, limited computing power and memory capacity, however, some services defined in [7] are not suitable for remote monitoring and control of HNS with mobile handsets. Home users are only concerned with the status of home appliances while they are in remote locations; for this reason, two management services (also known as two commands), "HS_GET_DATA" and "HS_SET_DATA", are employed in the proposed HNS management protocol. The HS_GET_DATA command is used to read a data parameter of a specific node, and the HS_SET_DATA command is to change a data parameter in a specific node. Conceptually, HNS management protocol contains only these two commands that allow the manager to retrieve data from a managed agent, or to set data into an agent. All other operations may be defined by these two commands. For example, although we do not have an explicit reboot command in HNS management protocol, an equivalent operation can be defined by declaring a data parameter that gives the time until the next reboot. Thus, the manager can assign the parameter a value (including zero).

The format of the command is shown in Fig. 5; the "service" field specifies HS_GET_DATA or HS_SET_DATA. "Object" fields are atomic entities, and are uniquely identified in a system by an object identifier, with one or more services applicable to them. "Data" is the value of the object and, like object, is optional. The values of several objects can be retrieved or set in a command. Objects for a specific HNS standard are built through cooperation of industry partners who establish the HNS standard.

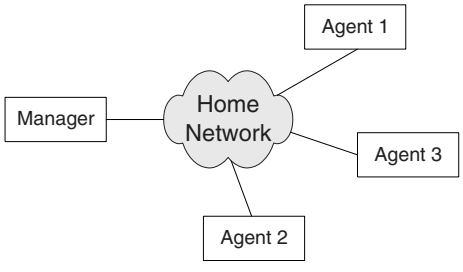

Fig. 4. Manager–agent model.

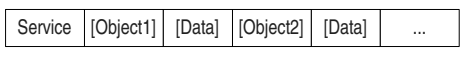

Fig. 5. Command format of management services.

2.2. HNS gateway

The HNS gateway provides the interlinking of the controlled home network and the Internet/GSM network. Specifically, such a gateway performs the protocol translations between the controlled home network protocol and the HTTP/WAP/SMS protocol, allowing for remote interaction and notification. As shown in Fig. 6, the HNS gateway consists of four parts: (1) an HNS manager responsible for service provisioning, (2) a short message driver responsible for communication between the GSM network and the HNS manager, (3) a WAP gateway, and (4) a Web server responsible for communications between the GSM network/Internet and the HNS manager. The communication protocol between the mobile station modem and the short message driver (reference point A in Fig. 6) is implemented using the SMS AT command set [15]. The HNS manager also performs protocol conversions between the HNS management protocol and HTTP/WAP/SMS protocol. For example, HNS manager employs the functions provided by the short message driver to send alerting messages received from the home network to the mobile station. In addition, the HNS gateway can connect to Internet Service Provider (ISP) mail server through cable, ADSL or dial up. Then HNS manager uses Post Office Protocol—Version 3 (POP3) [16] or Interactive Mail Access Protocol—Version 4 (IMAP4) [17] protocol to send/check mails.

As shown in Fig. 7, the protocol stack of the HNS gateway consists of two planes. The left-hand plane is the HNS "termination" protocol stack and consists of three layers. They are physical layer (PHY), HNS protocol stack and management protocol. The PHY, or transmission media, may be wired like the power line, cable and twisted pair, or wireless, such as infrared and radio, with different communication protocol. The HNS and management protocols are specified for interaction between the HNS gateway and home appliances. The HNS protocol is used to provide network functionality for the management protocol. The management protocol provides management services for the HNS. As noted earlier, each HNS standard defines its owned management protocol and is not compatible with others.

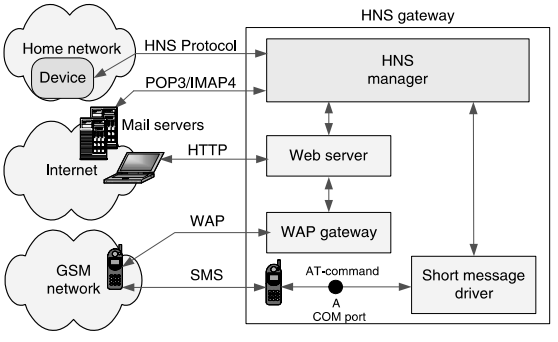

Fig. 6. Architecture of the HNS gateway.

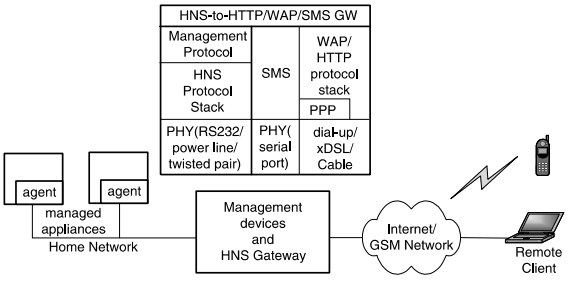

Fig. 7. Protocol stack of the HNS gateway.

The right-hand plane is SMS, HTTP and WAP protocol stacks. The SMS protocol stack is simple. It consists of SMS layer and PHY. A GSM handset connects to the gateway through the RS232 serial port for sending and receiving short messages. For HTTP and WAP protocol stacks, it consists PHY (dial-up, xDSL, and CATV), point-to-point protocol (PPP), and WAP/HTTP protocol stacks. The dial-in service is provided by the HNS gateway. The home user can dial up the HNS gateway to connect to the HNS via GSM mobile station with WAP feature through the GSM network, or with a laptop computer through the public switched telephone network (PSTN). Residential access networks such as xDSL and CATV thus become more popular; users can always utilize the HNS gateway to connect to the Internet, or dial up other ISPs to connect the HNS through the Internet. For a dial up connection, PPP is needed. At the top of a residential access network are the HTTP/WAP protocol stack. The HTTP protocol

stack includes TCP/IP, Secure Sockets Layer (SSL) and HTTP and the WAP protocol stack includes IP, UDP, Wireless Transport Layer Security (WTLS) [18], Wireless Transaction Protocol (WTP) [19] and Wireless Session Protocol (WSP) [20]. Note that WTLS (SSL) provides connection security between a WAP client (HTTP client) and HNS gateway. WTLS has been optimized for use over narrow-band communication channels and provides data integrity, privacy, authentication, and denial-of-service protection features.

On the top of two plains is the HNS-to-HTTP/WAP/SMS gateway layer (HNS-to-HTTP/WAP/SMS GW). The HNS-to-HTTP/WAP/SMS gateway layer achieves the bridging of the two planes. Therefore, such a protocol structure can support the remote monitoring and control of the HNS.

3. HNS implementation

In this section, we will present a prototype of HNS and implementation experiences in developing HNS software components.

3.1. An HNS prototype

We have implemented an HNS prototype that consists of an HNS gateway and three HNS subsystems (home appliance, security, and messaging subsystems) as shown in Fig. 1.

The home appliances do not currently have management services, as described in Section 2.1, so simulation programs have been implemented instead. We use PCs and their peripherals to emulate the appliance subsystem. TCP/IP network is used, and each appliance simulator is assigned an IP address and port number. We use charge-coupled device (CCD) cameras connecting to a PC to develop a simple surveillance system in the security subsystem. In the messaging subsystem, only e-mail services on are currently being provided. The subsystems are all connected to HNS gateway by 10 Mb/s Ethernet.

The HNS gateway is implemented on a desktop PC and a GSM mobile station with the ability to send and receive short messages and connect to the gateway through the RS232 serial port. A modem is also required by the HNS gateway to provide the dial-in service for a WAP GSM mobile station or a laptop computer. The software components required in the HNS gateway include Web server, WAP gateway, remote access service (RAS) server, short message driver, and HNS configuration tool. The short message driver provides the sending function for the HNS gateway to send short messages. The HNS configuration tool is a management tool for locally monitoring, controlling, and coordinating a diverse set of independent appliances connected to the HNS.

3.2. Developing environment

Linux was chosen as the developing platform because it has stable, open, and free features. There are many cost-free resources for Linux. In addition, Linux can run smoothly even on a PC with a Pentium CPU and small memory capacity. The HNS gateway and home appliance simulator programs are implemented on Pentium-level desktop PCs with Linux operating systems. Computer languages chosen to implement these software components are C and Tcl/Tk where Tcl/Tk is mainly used to implement graphical user interfaces (GUI).

3.3. HNS gateway implementation

HNS gateway, which we have implemented, consists of web server, WAP gateway, RAS server, short message driver and HNS configuration tool components. Each component is introduced below:

1. *Web server:* Apache server was selected as web server in the HNS gateway. It is a well-known, open source web server that performs well. Refer to http://www.apache.org/ for more information.
2. *WAP gateway:* Kannel WAP gateway was installed as a WAP gateway component in the HNS gateway. Kannel has an open source organization that developed a WAP and SMS gateway. With the exception of the WAP push feature, the WAP protocol stack is fully implemented, including WTLS [18] in the Kannel

WAP gateway. Refer to the Kannel website: http://www.kannel.org/ for more information.

3. *Remote access service server:* We chose Mgetty, a RAS server for Unix-like operating systems, as a RAS server component in the HNS gateway. Mgetty not only provides the necessary dial-in service, but also provides fax and voice-mail services if the modem supports fax and voice function. For more information, refer to http://alpha.greenie.net/mgetty/.
4. *Short message driver:* The short message driver used in the HNS gateway is based on gnokii's driver. Gnokii is an open source organization that provides tools and a user space driver for Nokia GSM mobile phones under Linux, various UNIXs and Windows. The main functions for SMS provided by gnokii include sending and receiving short messages, retrieving and editing phone-book, opening and closing net-monitor mode, remote keypad operation, and so on.
   Since gnokii can only send 7-bit, ASCII characters, the gnokii source code is modified to be able to send Chinese characters in the HNS gateway. In addition, we added the function of translating big 5 encoded characters to UCS2 encoded characters to the gnokii (big 5 is a popular Chinese character encoding scheme used in Taiwan). Gnokii can be downloaded at http://www.gnokii.org/.
5. *HNS configuration tool:* The home user needs a management tool to locally coordinate a diverse set of independent devices connected to the HNS. The HNS configuration tool should present a user-friendly interface that allows a home user to easily operate devices. In our prototype, a user-friendly configuration tool with GUI was developed to control devices in the HNS, as shown in Fig. 8. With this configuration tool, home users can easily configure home devices even though they do not know much about home networks.

Two management services, HS_GET_DATA and HS_SET_DATA have been implemented in the configuration tool. Applying these two management services, we developed the following functions for the HNS configuration tool:

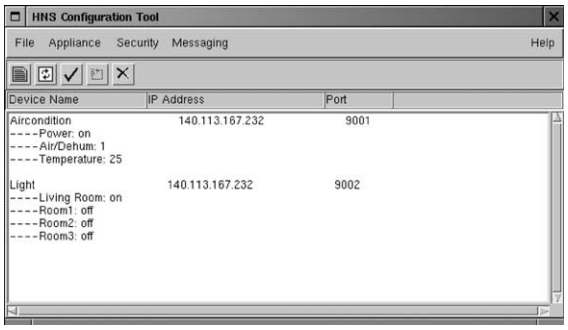

Fig. 8. HNS configuration tool.

- *List:* List all appliances managed by HNS (see Fig. 8). This function provides device look-up feature.
- *Add:* Add a new appliance to the managed list of the configuration tool. This function performs device registration for a new appliance. Three fields need to be filled: appliance name, IP address, and port number, where the appliance name must be unique. When a new appliance is added, its status is shown immediately.
- *Delete:* Remove an appliance from the managed list.
- *Refresh:* Refresh the status of appliances on the managed list.
- *Change:* Provide the capability to change object values of each appliance on the managed list.
- *Preference:* Configure a preferred method of sending alerting messages, e.g., by e-mail or by GSM SMS. When detecting an irregular situation, appliances can immediately send alerting messages to HNS gateway. The HNS configuration tool will relay these alerting messages via e-mail or SMS according to e-mail addresses or a GSM phone number chosen in the preference function.

Data inconsistency may occur when appliance statuses are changed with configuration tools or WAP handsets. In order to maintain data consistency, when adding a new appliance by the configuration tool, the new appliance is also added to the HNS's Wireless Makeup Language (WML) and HTML pages; Common Gateway Interface (CGI) [21] files, which provide communications between managed devices and HNS gateway, are

Fig. 9. HNS status.

also created for remote monitoring and controlling. On the contrary, when deleting a managed appliance, the appliance is removed automatically from the WML page and CGI files belonging to the appliance are also deleted. The "Refresh" function described above is used to obtain the real-time status of each managed appliance. The status of the HNS retrieved by a Nokia 7110 handset is shown as Fig. 9.

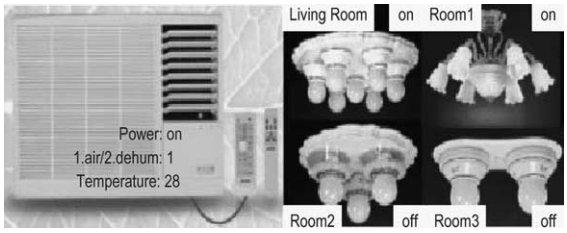

Fig. 10. The GUI for appliance objects.

3.4. Implementation of home network subsystems

Three subsystems (i.e., appliance, security and messaging subsystems) have been developed in our prototype. The following is a description of the implementation of an appliance simulation program, a simple surveillance system for the security subsystem, and e-mail services for the messaging subsystem:

1. *Appliance subsystem:* As mentioned above, we used appliance simulation programs as substitutes for real home appliances. Two kinds of appliances, air-condition and lights are simulated. They are represented by GUI (see Fig. 10). The air condition has three parameters: power (on/off), function (cooling/dehumidifying), and temperature. There is only on/off for the lights. We can add new appliances and change their parameters by the HNS configuration tool.
2. *Security subsystem:* A simple surveillance system using CCD camera connecting to a PC has been developed such that the home user can use a WAP handset or a PC to retrieve real-time images. Images captured by CCD camera in a small time period (e.g., 10 s) are transformed into WBMP and JPG format images. The home users can then view these WBMP format images with their WAP GSM mobile station (Fig. 11). Because of the single color and small screen size, images are not clear. Color images may be supported by new WAP specifications and the screen size of mobile phones may be larger in the future. For the home users with a laptop or desktop computer, they just connect (e.g., dial-up) to HNS gateway and view the JPG format images by the web browser.
A daemon program was developed for capturing real-time images and transforming WBMP format images. Up to now, we only provided

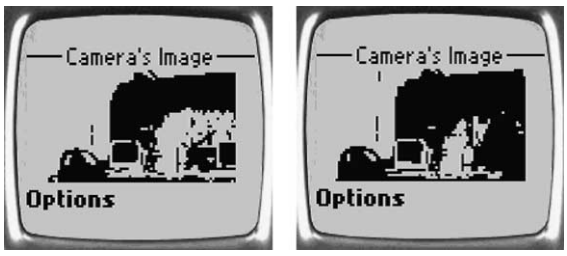

Fig. 11. Real-time images captured by CCD camera.

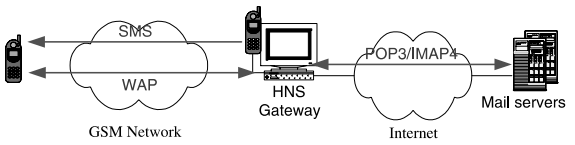

Fig. 12. Architecture of e-mail services.

real-time images viewing functions, however, the function of sending alerting short messages due to motion detection can be added easily.

3. *Messaging subsystem:* In the messaging subsystem, only e-mail services are currently implemented. Fig. 12 illustrates the architecture of e-mail services in the messaging subsystem. The mobile user may passively receive e-mail digests sent periodically in GSM SMS via the HNS gateway, or actively connect the HNS gateway to read e-mail digests with a WAP GSM mobile station. The protocol used between mail servers and the HNS gateway is POP3 or IMAP4.

Addresses of mail servers associated with user IDs, passwords, and GSM phone numbers must be given to HNS gateway in advance. The home user could configure the sending period of the SMS. Digests are composed of the "From" and "Subject" of each e-mail received from mail servers. According to the From and Subject entities, the user learns the sender and subject of an e-mail.

Because the GSM SMS is not cost-free, the SMS should be used efficiently to reduce costs. In addition to sending digests instead of complete e-mails, SMS costs can be reduced in two ways. First, the period set for receiving new e-mails should not be too brief; this decreases the frequency of sending short messages. A reasonable period is 30 min to 1 h. Second, a short message should contain as many characters as possible. In our prototype, we stuff e-mail digests with as many short message as possible. If all characters included in the e-mail use ASCII coding scheme, such as English, the 7-bit coding scheme is suggested. In this way, a short message can contain up to 160 characters. If we use 8-bit and 16-bit coding schemes, only 140 and 70 characters, respectively, can be contained in a short message. Short message services are thus far more effectively implemented.

4. Summary

In this paper, we propose an HNS architecture consisting of a home gateway and three main subsystems. This architecture provides remote monitoring and control of home appliances that are managed by the home gateway. The home gateway has the ability to actively notify home users in remote locations. That is, the home gateway can push alerting messages to home users. A configuration tool has also been designed to more easily manage home appliances. The proposed system architecture is shown to be feasible in terms of implementation. The following directions might be interesting for possible future work: (1) extend the HNS with real-time processing capability; (2) develop authentication and security mechanisms for HNS; (3) study Distributed Component Object Model (DCOM), Common Object Request Broker Architecture (CORBA) or Java Remote Method Invocation (Java RMI) for the remote invocation approach of HNS; and (4) implement more home network services and applications.

Acknowledgements

This work was supported in part by the Ministry of Education, Taiwan, ROC, under grant 89-E-FA04-1-4, and the Lee and MTI Center for Networking Research, NCTU, Taiwan.

References

[1] J. Desbonnet, P.M. Corcoran, System architecture and implementation of a CEBus/Internet gateway, IEEE Transactions on Consumer Electronics 43 (1997) 1057–1062.
[2] URL page: <http://www.cebus.org>, CEBus Industry Council, CEBus protocol.
[3] EHS European Home System Specification, release 1.2, EHSA, 1997.
[4] URL page: <http://www.ehsa.com>, European Home System Association, EHS Protocol.

[5] URL page: <http://www.eiba.com/specifications>, The EIB Handbook Series.
[6] URL page: <http://www.batibus.com>, BatiBus Club, BatiBus Protocol.
[7] E. Topalis, G. Orphanos, S. Koubias, G. Papadopoulos, A generic network management architecture targeted to support home automation networks and home internet connectivity, IEEE Transactions on Consumer Electronics 46 (2000) 44–51.
[8] Y.-M. Wang, W. Russell, A. Arora, J. Xu, R.K. Jagannathan, Towards dependable home networking: an experience report, in: Proc. International Conference on Dependable Systems and Networks, New York, June 2000, pp. 43–48.
[9] P. Bergstrom, K. Driscoll, J. Kimball, Making home automation communications secure, IEEE Computer 34 (2001) 50–56.
[10] M. Rahnema, Overview of the GSM system and protocol architecture, IEEE Communication Magazine 3 (1993) 92–100.
[11] WAP Forum: Wireless Application Protocol Architecture Specification, July 12, 2001, URL: <//www.wapforum.org/>.
[12] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, J. Leach, T. Berners-Lee, Hypertext Transfer Protocol—HTTP/1.1, RFC 2616, 1999.
[13] G. Peersman, P. Griffiths, H. Spear, S. Cvetkovic, C. Smythe, A tutorial overview of the short message service within GSM, IEEE, Computing and Control Engineering Journal 11 (2000) 79–89.
[14] WAP Forum, WAP Push Architectural Overview, November 08, 1999, URL: <//www.wapforum.org/>.
[15] ETSI GSM 07.07: Digital Cellular Telecommunication System (Phase 2+) AT Command Set for GSM Mobile Equipment (ME), Version 5.3.0 August 1997.
[16] J. Myers, M. Rose, Post Office Protocol—Version 3, RFC 1939, May 1996.
[17] M. Crispin, Internet Message Access Protocol—Version 4, RFC 1730, December 1994.
[18] WAP Forum, Wireless Transport Layer Security Protocol, November 05, 1999, URL: <//www.wapforum.org/>.
[19] WAP Forum, Wireless Transaction Protocol Specification, June 11, 1999, URL: <//www.wapforum.org/>.
[20] WAP Forum, Wireless Session Protocol Specification, November 05, 1999, URL: <//www.wapforum.org/>.
[21] W3C Forum, CGI: Common Gateway Interface, URL: <//www.w3.org/CGI/>.

Chi-Hsiang Wu received the B.S. degree in Business Administration from National Taiwan University in 1997 and M.S. degree in Computer and Information Science from National Chiao Tung University, Taiwan, in 2001. His research interests include wireless networks, mobile computing and wireless internet.

Rong-Hong Jan received the B.S. and M.S. degrees in Industrial Engineering, and the Ph.D. degree in Computer Science from National Tsing Hua University, Taiwan, in 1979, 1983, and 1987, respectively. He joined the Department of Computer and Information Science, National Chiao Tung University, in 1987, where he is currently a Professor. During 1991–1992, he was a Visiting Associate Professor in the Department of Computer Science, University of Maryland, College Park, MD. His research interests include wireless networks, mobile computing, distributed systems, network reliability, and operations research.