UBIQUITOUS NETWORK TECHNICAL ROOM MONITORING SYSTEM MODEL USING WEB SERVICE

Ha Quoc Trung[1]

[1]Department of Data Communication and Computer Network, School of Information and Telecommunication Technology, Hanoi University of Science and Technology, Hanoi, Vietnam
trunghq@soict.hut.edu.vn

ABSTRACT

Ubiquitous computing allows more efficient exploitation of information systems, economizes user cost and effort to use the information system. The network technical room monitoring problem, arising from network management practice, is important to operate the network, to discover and resolve unpredictable situation. In addition, many of monitoring and sensor product are shipped with closed proprietary software, and the interoperability between them is very difficult. In this article, the author present several ubiquitous computing technologies, propose a model of ubiquitous monitoring system for network technical room. This model allows monitoring the network technical room remotely, via variable terminal devices and variable communication infrastructure. The model has been implemented in Hanoi University of Science and Technology (HUST) Network Information Centre with IP Cameras and RFID devices.

KEYWORDS

Ubiquitous, pervasive, monitoring, distributed system.

1. INTRODUCTION

In network management practice, there are many cases that users without technical competence try to modify network configuration both logically such as access to control terminal and physically such as switching cables. These cases lead to network fails that are difficult to discover and repair. These situations raise the need of a monitoring system for the technical room. This kind of monitoring system provides additional information about what is the fail happened, who is responsible for the fail and how to recover the fail [1]. In addition, nowadays network-monitoring systems can monitor the network devices, network communication channels, but not the space that they are situated [3]. The network technical room monitoring system, in integration with the classic monitoring system, allows monitoring the device environment and to facilitate failing discovering and recovering.

With the availability of ubiquitous computing equipment, especially monitoring cameras, card readers, sensors, the task of space monitoring can be done in integration of several systems from different kinds [5].

Unfortunately, the monitoring equipment, the sensor systems are normally offered with specific, proprietary software to manage and exploit the devices. So the integration of the systems is difficult, base on fact that very little real-time information is allowed to be accessed from external programs. Anyway, these systems normally offer a web interface allowing users (not user's application) to access collected data.

In order to integrate different products in to an unified system, an intermediated component is needed. The functionality of the component is two folds. In relation with the monitoring device, the component must act as the end user, collects and store real-time information and store. In relation with the ubiquitous monitoring system, this component provides real-time processed information, raises triggers and generates event. In our solution, the component is simulated and implemented by a computer, but in the future, this computer can be embedded.

In this article, based on ubiquitous computing technology, a model for network technical room monitoring system is proposed. The model allows: (i) using IP camera and RFID card reader to monitor network technical room; (ii) access the monitoring system via different kind of end user devices and communication infrastructures. The model is experimentally implemented and tested at Hanoi University of Science and Technology's Network Information Center.

The paper is organized as the following: section 1 gives an introduction, section 2 describes several ubiquitous monitoring technologies such as IP camera, RFID, and some frame work to develop ubiquitous application; section 3 presents the model of network monitoring system; section 4 gives information about implementation and testing and section 5 gives some conclusion and perspectives.

2. UBIQUITOUS TECHNOLOGIES

In order to monitoring in an indoor space, the following technologies can be used:

IP camera allows monitor and store audio-video information about preconfigured space. A monitoring system using IP camera consists of one or multiple IP camera, distributed on monitored locations, and a concentrated display in a dedicated for monitoring goals space. The IP cameras and the displays are connected by a cable, in some case wireless network, and are controlled by software. The producer of the system normally provides this software. Common functionalities of such system are:

- Continuously capture picture or video from monitored space.
- Control of detail and quality of the picture and video (i.e. focus, zoom…).
- Storage of video and picture (by some rotation mechanism)
- Detection abnormal situation: motion, interruption of connection, …
- Provide an easy-to-use interface for the users.

Normally, a system of such type is well packaged, ready for use. If users need some special functionality of the system, the producer provides an API allowing users to develop new functionality. Unfortunately, the API is proprietary, expensive, and support only specific hardware and software from the vendor. That makes the development of new functionality hard.When using the motion detection function of the IP camera for authentication, a disadvantage of IP camera is that we cannot authenticate the person, caused by low quality image. IP Camera is better used in combination with other authentication methods such as fingerprint, RFID or magnetic readers. Anyway, audio-video content information that can be used for validating authentication results [4]. This is the reason why in our solution includes the IP

Camera component. As mentioned before, one of the problems is the difficulty to develop the function to interact with other systems.

RFID (radio frequency identification device) [5] allows identifying people and things by tag attached to them. RFID can be used for monitoring as it provides the capability of authentication. The RFID tag is used to identify the tag bearer. The RFID system consists of RFID reader, the distributed control device and a central database system. The RFID reader reads the ID of the tag; send it to central control system. The control system then verifies the correspond credential and send it back to the control device if passed. The device then activates the mechanism to allow bearer access the protected object. The problem is that RFID tag can be attached with different object. A multiple authentication mechanism can resolve the problem. In our solution, RFID tag is included with IP Camera such that identification by tag can by batch verified by IP Camera.

RFID middleware [6,7] processes the data acquired from the reader and then updates it to the backend database or other systems. An open-source RFID middleware is appropriate for our solution to allow we add own business logic and easy to extend the system. There are numbers of different open-source option for RFID middleware like Mobitec, Fosstrak and Rifidi. The reason we use Rifidi is it have complete development tool for design, simulation, testing and a lot of API to develop we application. In addition, the middleware work not only with RFID reader, but also with bar-code scanner, sensor, and other hardware such as cameras [3].

Rifidi Edge is a complete RFID middleware platform with an edge server and development tools to enable the development and deployment of highly customized RFID applications. It contain three conceptual architectural layers:

- Sensor Abstraction Layer: allow user connect to device to collect the kind of data required for the application.
- Application Engine Layer: The Layer is intended to let application weight loss pills developers build much of the functionality of their RFID applications using esper-queries.
- Communication Layer: The edge server has several built in connectors to use, namely JMS and Web Services (via Spring's remote framework). However, as this is application-independent, it is possible to write your own connector (such as a TCP/IP socket connection) if the application needs it.

Fortunately, these characteristics make the development of new functionality of the RFID much easier.

Context-aware computing. [8] Another requirement of the system is the access by different kind of terminal devices and communication media. The computing part of the system needs to detect the terminal and communication characteristics, and then format the information suitable for this context of interaction. That is called context awareness computing [7]. In our solution, a ubiquitous engine is used to convert and reformat information suitable for different kind of terminal is needed.

Ubiquitous computing framework.[9] To implement the context awareness computation, there are variable choices of the implementation framework. In our case, we need a framework allowing connecting different sensor and monitoring system from different producers. That the reasons why we choose a general, universal and open framework. Of course, we'll have more work to develop the needed functionalities. Web Service is the tool that we choose.

Web service provides connectivity, discoverability between software component using HTTP as transmission protocol and XML as data definition language. In ubiquitous computing, web services allow ubiquitous device can send and receive information easily to processing server. We can easily customize the server, the protocol to meet the specification of the sensor part of the system.

Combine monitoring

As analyzed above, RFID authentication has several advantages: simple and flexible authentication; authenticates by RFID tag id; can be used with physical access control devices. But it also has some disadvantages: no information about access period; It is not strong enough. Every one who has a RFID tag can be authenticated.

IP camera monitoring gives us the capability to capture video and picture in a customizable way, but it can not gives us the details functional information about the monitored object.

The idea is to combine the monitoring by RFID and by IP camera in a way that authentication can be double checked by the 2 systems online or offline. The log and traces from RFID will be extended with video and pictures from the IP Camera monitoring system. These video and pictures are taken from preconfigured action for indoor – network technical room- spaces. To accomplish this task, interaction between 2 systems has to be designed and implemented, with condition that RFID sub-system is open source, while IP camera system is closed and proprietary.

3. THE SYSTEM MODEL AND FUNCTIONALITY

The system requirement: Technical room monitoring requires the following functionalities: (i) supports traceable entries, operations and exit in the working space; (ii) supports traceable activities on pre-configured equipment; (iii) provides automatically identification and authentication of the object; (iv) provides access to the system via different devices and communication media.

The system is organized in 3 subsystems: the local subsystem, the central subsystem and the monitoring subsystem. The local subsystem is for administrator-monitor. The central system consists of overall monitoring logics of the system. The monitoring points server for real-time monitoring, access control and authentication.
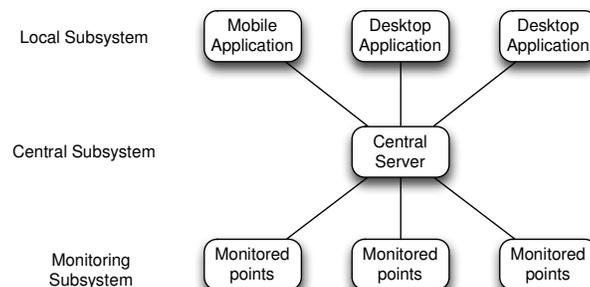

Figure 1: The system overall architecture

The monitoring subsystem has several monitoring points. Each monitoring point consists of: an IP camera, RFID reader(s), a LCD for each RIFD, a computer and a mechanical access control device (lock, barrier…).

The RFID reader is used to control the physical access to the space via mechanical device. The IP Camera is installed and configured to control the entrance and part of the space. The LCD is installed next to the entrance, serving for announcing welcome message for the user. These 3 components are controlled with a computer. This computer is autonomous, self-activate, and will be embedded. The computer provides a web-service for other part to access collected information from monitoring devices. The principal functions of each monitoring point are:

- RFID Authentication and Checking.
- Device monitoring by predefined detection zone.
- Configure monitoring devices.

Central system consists of processing server. The server collects information from monitoring points, process this information with management information in the database. The server publishes this information using a web server. On this server, context awareness module allows providing information for different access contexts. The functions of central module are:

- Users (technical administrator) management
- Devices and technical rooms management
- Grouping users and devices
- Search and summary
- Abnormal situation detection and alert.

The local system in fact is the client – end user interface. As well as we use Web Interface, the problem to resolve is to provide web information conforming to the device's and communication link's capability.

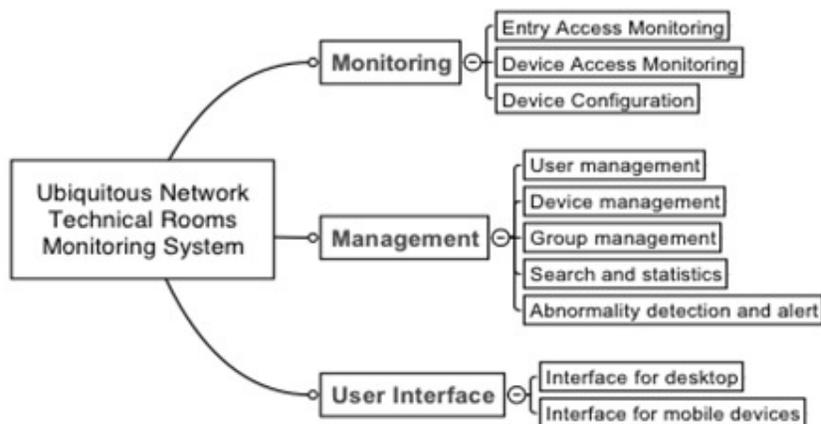The functional model of the system is described in Figure 2 : Functional Model

Figure 2: Functional model

In this article, we don't concentrate on the detail analyze of each function. We concentrate on the functions of each monitoring point. The components of each monitoring point are described on Figure 3: Monitoring point.
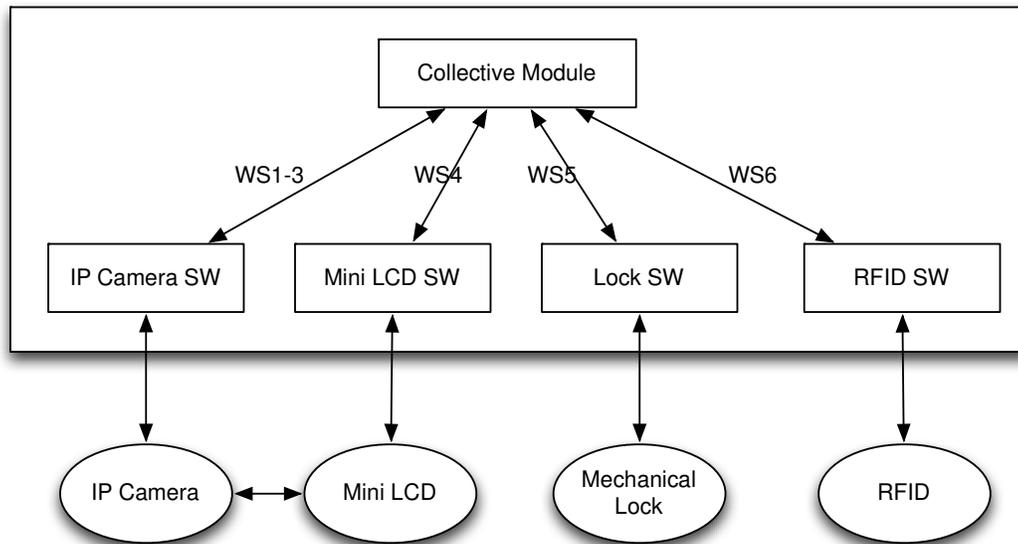
Figure 3: Monitoring point

As mentioned above, in each monitoring point we have to allow interaction between components. We use web services to transfer from normal software user interface to programmable interfaces. The list of the web services is presented in Table 1: Monitoring point web services.

Table 1: Monitoring point web services

WS	Name	Description
1	Forced monitoring	Activated when a predefined entrance is accessed, or administrators need to view the IP Camera directly. Accept monitoring commands and transfers to Camera
2	Conditional monitoring	Activated when a predefined condition is true (a device is accessed, some one operates on some devices). Based on motion detection.
3	Configuration	Receive configuration from collective modules and transfer it to camera. Configuration information is depended on monitored devices.
4	Display announce	Receive text (audio) message from collective module and send to LCD and speaker.
5	Authentication sending	Raised when RFID reader is accessed and sending information
6	Allow access	Raised when authentication is successful

4. IMPLEMENTATION AND EXPERIMENTATION

The model is implemented in the server room at the HUST's network information center. One monitoring system uses 1 camera, 1 RFID card reader, one PC to collect information from camera and RFID reader. 4 monitoring points are deployed in server room and 3 network technical rooms in the same building.

For experimental purpose, 4 devices are controlled in the server room. In each network technical room we monitor only one device. Information about 20 administrators and 3 roles are stored in the central DB. The system has been tested in 3 months.

The system helps the managers to:

- Control the entry and exit of the technical room;
- Enforce the RFID authentication by camera support;
- Control the important devices (servers and network equipment).
- Determine initiator of the selected configuration activities.
- Access system anytime and anywhere.

5. CONCLUSIONS

The paper presents the model of the ubiquitous network technical room monitoring and its experimental implementation. The main contributions are:

- Study the monitoring technical room problem
- Study several ubiquitous computing technologies
- Propose the model of the ubiquitous network technical room monitoring
- Implement the model with web services with. The model allows connecting several proprietary products.

In the future, the system will be extended to serve multiple network technical rooms, and to integrate more ubiquitous computing technologies such as batch, bioinformatics….

ACKNOWLEDGMENTS

REFERENCES

[1]   Ko, Ren-Song. (2011), Anywhere/Anytime Software and Information Access via Collaborative Assistance. Eduard Babkin, Ubiquitous Computing, 31-49.

[2]   Marie-Luce. (2011), Uncertainty and Error Handling in Pervasive Computing: A User's Perspective. Eduard Babkin. (2011), Ubiquitous Computing, 49-67.

[3]   Nicolas Ferry. (2011), Vincent Hourdin, Stéphane Lavirotte, Gaëtan Rey, Michel Riveill and Jean-Yves Tigli. (2011). WComp, a Middleware for Ubiquitous Computing, Ubiquitous Computing, 151-177.

[4]   Wanderley Lopes de Souza, Antonio Francisco do Prado, Marcos Forte and Carlos Eduardo Cirilo. (2011). Content Adaptation in Ubiquitous Computing. Ubiquitous Computing, 67-95.

[5]   Bakhouya, Mohamed. (2008). Ubiquitous and pervasive application design, Proceedings of the 2nd international workshop on Agent-oriented software engineering challenges for ubiquitous and pervasive computing.

[6]   Roussaki, Ioanna, Strimpakou, Maria and Pils, Carsten. (2007). Distributed Context Retrieval and Consistency Control in Pervasive Computing. Plenum Press, Netw. Syst. Manage., Vol. 15, 57-74.

[7]   Reyes, Fernando Martinez and Greenhalgh, Chris. (2009). The User's Touch: A Design Requirement for Smart Spaces. IJAPUC, Vol. 1, 14-28.

[8]   Grzywaczewski, Adam, et al. (2009). An Investigation of User Behavior Consistency for Context-Aware Information Retrieval Systems. IJAPUC, Vol. 1, 69-90.

[9]   Chang, Po-Chien. 1,.(2009). Understanding Consumers' Behavior when Using a Mobile Phone as a Converged Device. IJAPUC, Vol. 1, 60-74.

Authors

Ha Quoc Trung (Ph. D.) Graduated from Technical University of Sofia in 1996, speciality "Electronic, Microelectronic and Automation". In 2004 he completed his Ph. D. degree in School of Advance Research Practice (Ecole Pratique de Hautes Etudes-Paris, France). From 1999 to recent he is lecturer at department of data communication and computer network. His research interests are: distributed algorithm, system and application, ubiquitous computing.