Internet of Things Applications for Intelligent Surveillance System

Wei Liu, Pengyu Liu and Kebin Jia
Beijing University of Technology, Beijing
E-mail: liuwei1987@emails.bjut.edu.cn
Tel: +86-10-67391957

***Abstract*—Since surveillance system plays an important role in security management, IP (Internet protocol)-based surveillance systems are widely used by now. The emerging Internet of Things effectively promotes the development of multimedia network techniques, in which applied to intelligent surveillance is one of the most successful applications. This paper deals with an intelligent surveillance system, which includes entrance guard, SMS (Short Message Service) alert, network and video analysis modules. The key technologies of this system include RFID (Radio Frequency Identification), IPv6 - IPv4 exchanges, and the SMS auto-warning technology. The surveillance system has been successfully applied to the telecommunications field, and is also an IPv6-based application, completely integrated to RFID technology and SMS (Short Message Service) alert module. The simulation results show that the system achieves the target of real-time tracking and detection.**

I. INTRODUCTION

"Internet of Things" was originally proposed by Bill Gates in his book "The Road Ahead" and IBM's "wisdom of the Earth" program went further to promote its development. Applications for "Internet of Things" in intelligent surveillance system are the topic of this document. It can significantly reduce the staff charge, increase efficiency, and have many application prospects. It also lays the basis for intelligent surveillance technology at this stage, a smooth transition to the field of Internet of Things.

"Internet of Things" is defined as: every item connected to the Internet using IP, including matters like the imminent depletion of IP address space. The shortage of IPv4 address space limits directly the development of Internet of Things technology. By now, in order to alleviate the lack of IPv4 address, NAT and CIDR technology are deployed into it, but it is still hard to stop the IPv4 address depletion. As a result, IPv6, the pillar for the next generation of the Internet, is on agenda.

This whole system is based on IPv6 network structures. The server can be accessed remotely using two ways. Firstly, we access to the different network segments by using the IPv6 public network. Secondly, we use the ISATAP protocol (Intra-Site Automatic Tunnel Addressing Protocol) to provide an IPv6 connection between IPv6 servers and IPv4 clients. The integration of RFID technology to the surveillance system, the automatic warning, IPv6 exchanging visits to IPv4 and moving target detection are presented below.

Nowadays, some advanced countries like the United States, Japan, Korea, or Europe have made a lot of researches on the Internet of things, with a number of applications and solutions, such as smart grid and smart transportation. In China, research for Internet of things has also known some success, such as, the IPv6 video surveillance systems services during the Beijing 2008 Olympic Games. The good results were deployed in Beijing, Shanghai and Guangzhou by China Unicom.

This article is organized as followed: Section II provides the integrated framework of the whole system and its components. The key technologies of the system, according to their functions, will be discussed in Section III. In Section IV, we have the implementation of the system. Finally, we would summarize our work and discuss future enhancements.

II. SYSTEM STRUCTURE AND FUNCTION MODULE

The system is implemented on Java platform, which fully integrates video surveillance system, IPv6 network addressing, RFID technology and SMS alert module.

The system consists of a data acquisition layer, a network transmission layer and application layer. The data acquisition layer includes IP camera, entrance guard and RFID based detector, which can acquire the information inside the computer room and transmit to the application layer through the network. Now the collection point is developed in the 15 control room to surveillance. The network transmission layer access the different network segments by using IPv6 public network or using ISATAP to provide connectivity between IPv6 servers to IPv4 clients.

The architecture of the system is shown in Fig.1.

System function consists of a video analysis module, an entrance guard module combined to an SMS alert module.

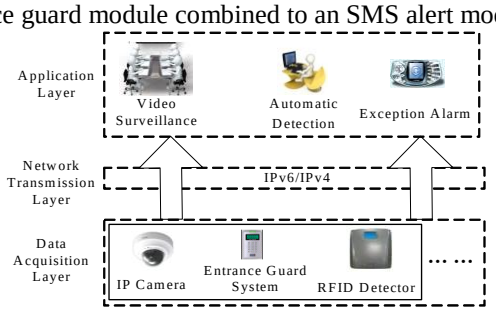


Fig. 1 Architecture of the surveillance system

A. *Video Analysis Module*

This module improves the existing remote video surveillance system, supports network transmission under IPv6 environment and is fully integrated to the two others modules.

The main purpose of this module is to detect moving objects. The detection algorithm based on frame differences combined to the edge feature of images, is adopted by the system to detect the moving objects. The specific implementation process will be elaborated in the next section.

B. *Entrance guard module*

RFID Technology is used for the entrance guard module which is performed by the entrance guard controller, RF detectors, magnetic switches, etc. The framework of the entrance guard module is shown in Fig.2.

The core component of RFID technology is an electronic tag which diameter is less than two millimeters. Information stored within the electronic tag can be obtained by detecting radio wave emitted by sensors (sensing distance includes several centimeters to several meters). Personnel and appliances represented by electronic tags can be identified. RFID technology [1] with its powerful ability to identify objects [2], has become an important part of Internet of Things, and it is integrated with the remote surveillance system which will greatly promote the application of Internet of Things.

C. *SMS Alert Module*

SMS alert module is connected to the server by the GSM Modem using a standard RS232 serial port. It achieves the function of notifying the proper person in charge when emergence exceptions occurred. When the server receives the video or gets some exception information, SMS alert modules will read the phone number, text messages and other related information from the server's database, and then sends AT commands to GSM Modem automatically. Thus it will send alarm message to the relevant staff.

SMS alert module is made with the following parts:

GSM Modem is a non-intelligent device, which communicates through the computer's serial port, controlled by AT commands [3]. SMS module is an embedded wireless communication module of GSM [4], which is the main electronic component to achieve SMS send and receive functions. It establishes a wireless connection to operator's message center thanks to the SIM card. This internal SMS module uses a Siemens TC35i [5].

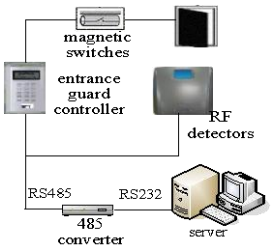


Fig. 2 Framework of the entrance guard module

GSM Modem integrates the system to assist the intelligent surveillance. We can see many advantages transmitting warnings by sending short messages automatically instead of having a person on duty. On one hand, it is able to notify the alarm information to officers immediately; on the other hand, it can provide an effective method to increase efficiency for businesses. That will improve the possibility of using the company's application for intelligent surveillance.

III. KEY TECHNOLOGIES OF THE SYSTEM

The workflow of the whole system can be shown in Fig.3 and the key technologies will be detailed in the following part.

A. *Network Deployment*

The topological graph of the network is shown in Fig.4. In order to access the server in different network segment, we configure the routers to provide the function of IPv6 address auto assignment.

To establish a connection between IPv4 and IPv6, we use ISATAP. This protocol is an IPv6 transition mechanism that allows creating IPv6-to-IPv4 tunnels automatically within a same site. Each host queries an ISATAP router within the site to obtain address and routing information. Packets sent to the IPv6 Internet are routed via ISATAP routers, and packets destined to other hosts from the same site are tunneled directly to the destination. The ISATAP tunnel in the system is "isatap.sjtu.edu.cn".

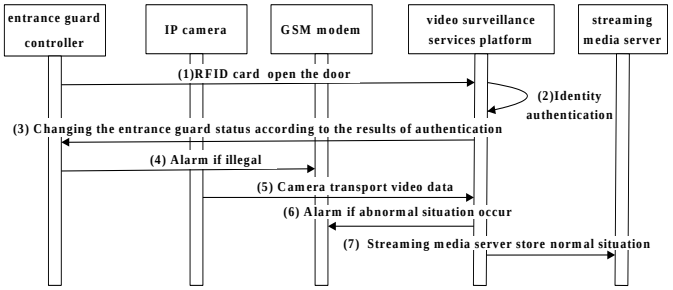


Fig. 3 Workflow of the whole system

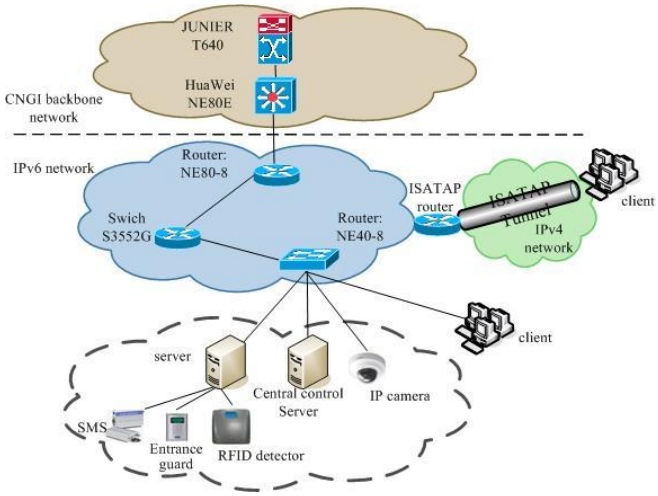


Fig. 4 Topological Graph of the network

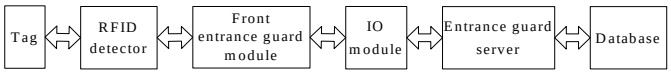


Fig. 5 Diagram of the Entrance Guard Module

B. RFID Entrance Guard Module Interface Design

The Design diagram of the entrance guard module is shown in Fig.5. Front entrance guard module identifies anyone that is using card to open the door, through the RFID detector [6]. It will receive the data and transmit the date through the custom communication protocol to the IO module by the IPv6 network, then deliver to the entrance guard server service platform. Entrance guard server is surveillance the appropriate port, and access data. If it is an illegal user or some data error, refusing requests will return to the detector, and detector alarm beeps. If it is a legal user, opening instructions will return to the detector, and then the detector opens the door, and user come in. At the same time database deposits relevant personnel information including time and send some others to the business platform. Thus, business platform can display personnel access to the system.

The specific format of custom communication protocol is as follows:

- Start symbol is composed of two bytes, and is a standard for the beginning of each frame.
- Command length is composed of four bytes.
- The number of bytes for a command word is a numeral value that the command length read.
- Check bit uses CRC32 check method.

In the design process of entrance guard module, we solve the problem by Java and C++ multi-language integration, socket for IPv6 network transmission and seamless accessing to hardware devices.

C. SMS alert Module Design

Now, common techniques for automatic warning messages generally supports only English messaging, and sending text messages in Chinese is garbled. We use complex PDU encoding format, to achieve the automatic conversion of encoding character setting, and find an effective solution to the problem of garbled messages. The SMS alert flowchart is shown in Fig.6 (Content of quotes is instruction statement).

Encoding of PDU mode consists of two steps:

- GB2321 encoding conversion to Unicode encoding.
- Unicode encoding conversion to 16-bit encoding.

The initial serial parameters of this system is described as follow: the communication format is using COM1, data bits are made of 8 bits, 1 stop bit, the baud rate is 9600bps, and there is no parity bit. To support Chinese character input, we encode the message into the PDU format. Finally we should confirm the success of sending message.

D. Video Analysis Module Design

The main purpose of video surveillance is to detect moving object. Detection algorithm using frame differences combined to edge feature of images is adopted in the system to detect the moving object. And this algorithm is more effective in the video with obvious edge of frame. The algorithm flowchart is divided like this: (As shown in Fig. 7)

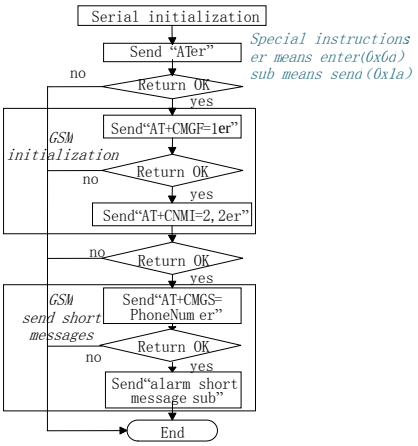


Fig. 6 SMS alert flowchart

- Firstly, setting a certain number of background frames. Then canny is used in each frame for edge extraction, and the number of edge pixels in background frames is counted.
- Construct the edge of background. If the number of pixels, which came from the former step, is greater than the threshold, the pixel is the edge of background. The threshold can be estimated this way: βNum is the number of background frames which is set in the first step, and α is the decision factor. α the bigger, the noisier, and more breaking points is the opposite. We usually set α between 0.1and 0.4:

$$T = \alpha * \beta Num \quad (1)$$

- Detect the edge in current frame and subtract the edge of tectonic background is the first edge extraction of moving object.
- After making the difference between the previous and the current frame, a median and a corrosion filter are used to eliminate the noise. Then logic and extraction operation by the first edge is carried out. Thus a second edge can be obtained. Every operation in this step achieves the combination of frame difference for the first time.
- The first time it extracts the moving edge, it may overlap the target and the edge of background. So it goes to non-athletic edge. Therefore, we make the second combination of frame differences to determine whether it is due the edge or not. The final result we get is a complete edge of moving object [7].

Once the edge extraction is finished, the moving object can be detected using mathematical morphology and connected components amalgamation method [8]. The experiment results are shown in Fig.8.

Fig.8 (a) is the original frame of a video sequence image. Fig.8 (b) is the color display after moving target detection. Fig.8 (c) is the black and white display after moving target detection. Fig.8 (d) is the final display after moving target detection.

The video frames that consist of moving object are compressed and transferred to the server to be stored. Therefore, the client can retrieve and replay them conveniently.

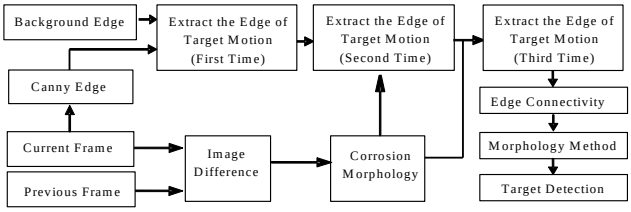
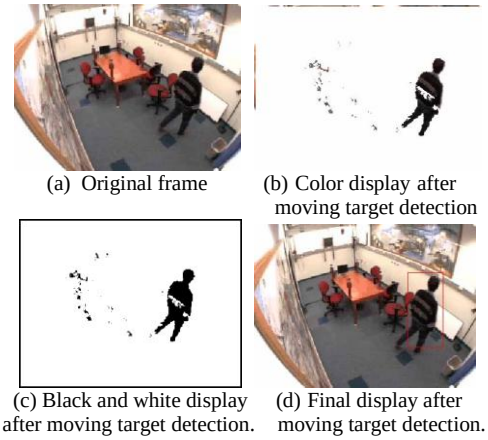


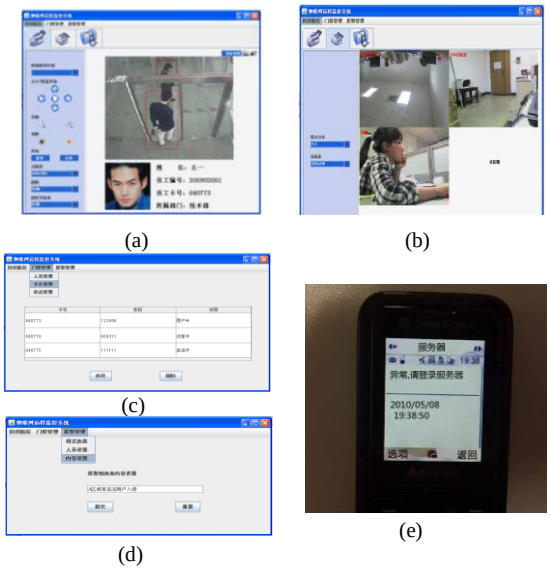
Fig. 7 Algorithm flowchart



(a) Original frame (b) Color display after moving target detection

(c) Black and white display after moving target detection. (d) Final display after moving target detection.

Fig. 8 Experiment result of the algorithm



(a) (b) (c) (d) (e)

Fig. 9 Application implementation (a) The main interface of system operation (b) Three videos surveillance (c) Management of Entrance guard module (d)Management of SMS alert module (e) Schematic diagram of mobile terminal receiving warning messages

IV. Application Implementation

System frame rate reaches 20 frames per second, realizes targeting of real-time tracking moving, and support the multiple video surveillance. This can also support up to four videos surveillance at the same time. Accessing to the video surveillance module, administrators can control the position and angle of the IP camera, choose the detecting area, change the mode to multi-detection, and some other parameters of the pictures. The module also provides functions of target tracking and videos storage for further requirement. The interface for video surveillance module is shown in Fig.9 (a). It can also show us the information about the person in the surveillance area. Fig.9 (b) shows three videos surveillance. The management of entrance guard and localization module is shown in Fig.9 (c). The SMS message which is used to send alarm can be managed and queried in the SMS alarm module. You can check all messages. The receiver that sends out from the system is shown in Fig.9 (d). Fig.9 (e) shows the mobile terminal receiving warning messages.

V. Conclusions

In this paper, a remote surveillance system integrated to radio frequency identification RFID technology and Intelligent SMS alert is designed and developed. It embodies many new features such as identification and automatic warning messages in English or Chinese. What's more, it supports IPv6 network. In addition to this, the system contains RFID technology which is one of the key technologies for the Internet of Things, providing interfaces of entrance guard, localization module and SMS alert module to remote surveillance system, achieving the integration of multiple languages, accessing to the hardware seamless and solving the garbling problems of warning text messages in Chinese. The system has strong scalability and portability.

Acknowledgment

The research work is supported by the National Key Specialized Project Subject of China under Grant No. 2009ZX07212-003-02 and the National Natural Science Foundation of China under Grant No. 30970780.

References

[1] J. Landt, "The History of RFID," *IEEE Potentials*, Vol. 24, pp.7-13, Nov. 2005.

[2] A. Boukerche, H.A.B. Oliveira, E.F. Nakamura and A.A.F. Loureiro, "Localization systems for Wireless Sensor Networks," vol. 14, Dec. 2007.

[3] Rushi Sun, "GSM digital mobile communications engineering," *Beijing: People's Posts and Telecommunications*, in press, 2000.

[4] R. Rose, C. Meier, S. Zorn, A. Goetz and R. Weigel, "A GSM-network for mobile phone localization in disaster scenarios," *German Microwave Conference*, Mar. 2011.

[5] Siemens, "Cellular Engine TC35," *The Extra Compact Module for Voice and Data transmission*, 2001.

[6] R. Pathak, S. Joshi, "Recent trends in RFID and a java based software framework for its integration in mobile phones," *First Asian Himalayas International Conference on Internet*, pp. 1-5, Nov. 2009.

[7] C.R. Wren, A. Azarbayejani, T. Darrell and A.P. Pentland, "Pfinder:real-time tracking of the human body," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 19, pp. 780-785, Jul. 1997.

[8] R.A. Brown, Z. Hongmei, and J.R. Mitchell, "Distributed vector Processing of a new local MultiScale Fourier transform for medical imaging applications," *IEEE Transactions On Pattern Analysis and Machine Intelligence*,Vol. 24, pp. 689-691, 2005.