An Instant Security Early Warning System Based on Mobile Push Technology

Yuesheng Zhu, Chao Wang , Huabing Zhang

Communication & Information Security Lab   Shenzhen Graduate School, Peking University, Shenzhen, China
zhuys@pkusz.edu.cn, wangchao@sz.pku.edu.cn,   zhanghuabing@sz.pku.edu.cn

Abstract - Most of the notification mechanisms of current intelligent video surveillance systems are based on traditional methods, which either require operators on duty to receive and deal with early-warning notification from surveillance systems, or notice related personnel by broadcasting. The former costs a great deal of labor and effort, and the latter is inconvenient. Moreover, some other intelligent video surveillance systems could even only provide clues for ex post analysis, whose instantaneity performance is poor. To solve these problems of notification mechanisms in current intelligent video surveillance systems, a security early warning system based on mobile push technology which uses XMPP (Extensible Messaging and Presence Protocol) is proposed in this paper. The performance test results indicate that the proposed system not only improves the instantaneity performance, but also saves labor and effort.

Index Terms – Intelligent video surveillance, Mobile push, XMPP

1. Introduction

With the increasing demand of the protection of personal security and property security, especially in banking, transportation and etc., a variety of security warning systems based on video surveillance have begun to spread.

Since invented in the last century, the video surveillance system has been developed to the third generation. This generation is known as intelligent video surveillance based on digital video, Internet and intelligent video analysis. Ref. [1] introduces the latest development of video surveillance. Ref. [2] introduces several main technologies of intelligent video surveillance. The current intelligent video surveillance systems based on these technologies can detect the probable potential security hazards reflected in videos, and will generate an early-warning notification immediately.

These technologies mentioned above focus on the processing of video data source, instead of informing related personnel of early-warning information. So, when an early-warning notification is generated, the operator on duty is still necessary for dealing with it, which costs a great deal of labor and effort. Besides, some solutions use broadcasting to announce early-warning messages, it is inefficiency. Several business intelligent surveillance softwares begin to use email to establish the notification system, but it is only a temporary measure due to the poor instantaneity and inconvenience of email in the mobile communication.

As the mobile communication technology has been more and more popular, mobile notification is the most convenient and instant way to make alarms. This paper attempts to improve the notification mechanism of intelligent surveillance system, and proposes an instant security early warning system based on mobile push technology. Ideally, our method can free the operator on duty and also has good instantaneity.

Ref. [3] lists the current mainstream mobile push technologies, i.e. WAP Push, Blackberry Push Mail of Blackberry, APNs of Apple's iOS and C2DM of Google's Android. Now the C2DM has been replaced by Google Cloud Messaging (GCM). C2DM and GCM allow third-party applications to use the official Google Cloud push server. In this paper, the proposed system is based on Android platform. Since this paper focuses on technological exploration, we set up our own push server, rather than GCM.

An instant security early warning system based on mobile push technology on the Android platform is proposed in this paper, which designs the surveillance part based on intelligent video surveillance technology and the push part based on XMPP. The implementation platform is Google Android 2.3.

2. The Proposed System Architecture

The architecture of the proposed system includes two important parts, surveillance part and push part as shown in Fig. 1. For the surveillance part, a method of motion detection [4], named inter-frame difference method, is adopted, by reason of its maturity and effectiveness. For the push part, XMPP is used to realize the mobile push function. The inter-frame difference method and XMPP will be introduced later on. Besides, we establish the Content Server and the database. Content Server is in charge of managing the screenshots taken from Surveillance Server and providing access to these images for terminals. The database is in charge of storing accounts' information, accounts' subscription data and images form Content Server.

The workflow of the proposed system is as follows:

1) The motion detection system of Surveillance Server monitors and analyses the video streaming from each camera continuously. Once something abnormal is detected, Surveillance Server will get a screenshot of the video from the camera and submits it to Content Server.

2) Content server receives the screenshot and stores it. Content Server returns a URL of the image to Surveillance Server.

3) Surveillance Server submits to Push Server the URL, the time of the screenshot and the ID of the camera which the screenshot is from.

4) Push Server accesses Database to query the accounts which has subscribed for this camera ID. Then Push Server

pushes an early-warning message to these accounts, which contains that URL and some other information.
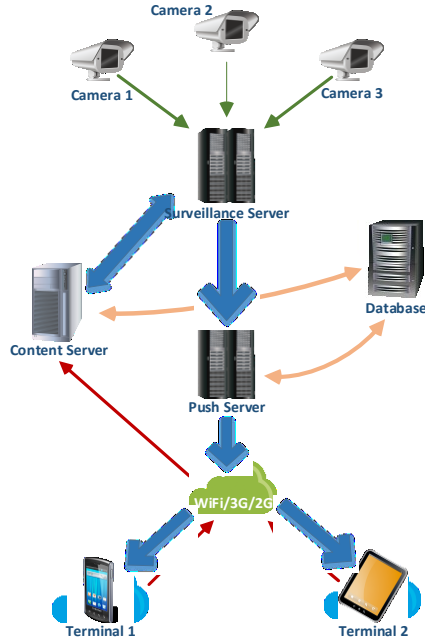

Fig. 1 The architecture of system

5) Upon receiving this message, users can use their mobile terminal to access the URL to view the screenshot.

A. Inter-frame Difference Method

Inter-frame difference method [5] is based on the time information of the image. Its rationale is to subtract each frame from the nth one before it, and then get the difference. The calculating formula is as follows:

$$D_k(x,y)=\begin{cases}1; & |I_k(x,y)-I_{k-n}(x,y)|\geq T\\ 0; & |I_k(x,y)-I_{k-n}(x,y)|<T\end{cases}. \quad (1)$$

T is a threshold value that we set. k is the ordinal number of frames. I_k is the gray value of the corresponding pixel in the kth frame.

We define N_k is the quantity of pixels, the D_k of which is equal to 1. If N_k is greater than a threshold value, we judge that there is something abnormal in the kth frame and it may imply some potential hazards.

B. XMPP

XMPP (Extensible Messaging and Presence Protocol) [6] is a communications protocol based on XML. The protocol was originally named Jabber. XMPP is one of the four major instant-messaging protocol. And the other three are IMPP, PRIM and SIP. Among the four protocols, the advantages of XMPP contain decentralization, open standards, history, security and flexibility. As a result of these points, XMPP has been adopted by a lot of IM softwares such as Google Talk.

The technology standard of XMPP can be found in [7] and [8]. Although based on C/S structure, XMPP do not have its official server. Every user can set up his/her own XMPP sever. The basic network structure of XMPP contains three roles:

client, server and gateway. The basic network form of XMPP is that single client connects to single server through the TCP/IP protocol. The transport stream of XMPP is based on XML, instead of binary form. This design facilitates the development and troubleshooting.

Because of the flexibility and user-friendliness, the propose system in this paper adopts XMPP protocol to structure the push system.

3. System Realization

The technical realization of this system mainly includes two parts. One is surveillance system, and the other is push system.

A. Surveillance System

Each frame of the video form surveillance camera will be grayed at first. Then, the potential security hazard would be detected by system through inter-frame difference method introduced above.

Then the system get a screenshot of the frame, in which potential hazard has been detected. Next Surveillance Server submits the screenshot to Content Server, and receives the URL of this screenshot from it.

At last, Surveillance Server sends a message to push server, which contains the URL, the camera's ID and the time of the screenshot. Now, the surveillance system completes its work in a single process.

B. Push System

The push system of the proposed system is realized by using an open-source software Androidpn (Android Push Notification) [8]. Androidpn is based on XMPP technology that is mentioned above.

Androidpn contains a complete server-side and client-side programs. The client-side program uses classes of asmack, which is an open-source XMPP framework based on Java Platform, to establish persistent connection with server and receive notifications.

The server-side of Androidpn is also based on Java Platform. The web part is based on Spring framework, and the management of socket connections is based on MINA framework. The architecture is shown in Fig. 2. The top layer contains four parts: Session Manager manages the session between client and server. Auth Manager manages account authentication of client. Presence Manager manages the login status of client account. Notification Manager realizes the function of push message.

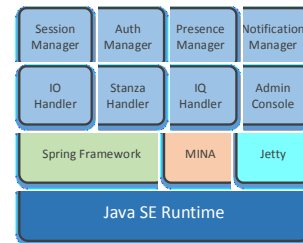The basic workflow of Androidpn is shown in Fig. 3

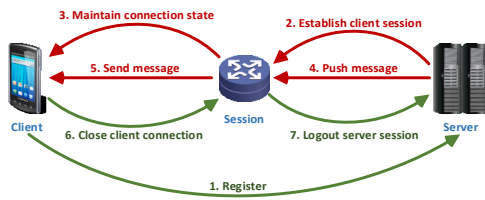Fig. 2 The architecture of Androidpn server-side

Fig. 3   The workflow of Androidpn

When the client finishes the register on server, a session would be created. The server maintains the connection and accomplishes the message push with each client through the corresponding session.

In order to achieve the design goal of the proposed system, we make the secondary development on Androidpn. Its main part contains the enhancement of account manager, accounts' database, subscription system and so on.

The enhancement of account manager request every user to create or login an account such as a SNS. It makes the management of users efficient and convenient.

The accounts' database is based on MySQL platform. Its main function is storing accounts' registration information and subscription information. Through a retrieval of the database by using the camera's ID as the index, Push server could screen out accounts who subscribed for this camera.

The function of the subscription system is obvious. Each account can subscribe the cameras in his/her interested locations. Fig.4 shows the interface of subscription on client terminal.

Fig.5 and Fig.6 show that the mobile client terminal receives some messages and then accesses a URL in one of these messages to view the image.
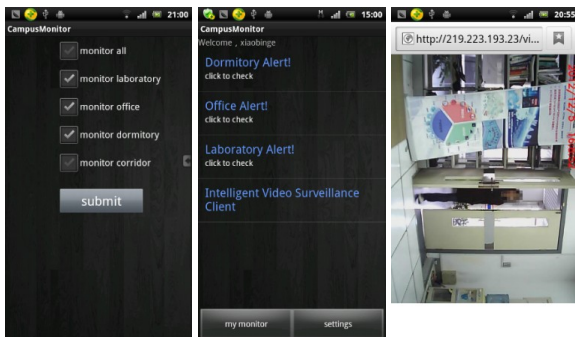

Fig.4   Subscription   Fig.5   Notifications   Fig.6   Visit the URL

4. System Test and Performance Analysis

The system is implemented in the campus. We set up 4 cameras in different places which located in laboratory, office, dormitory and the corridor of our laboratory respectively. Our system use the Mobile push technology to improve the notification system of intelligent surveillance system in order to implement non-operator on duty.

In our experiment, we test the delay between the time when the camera found something abnormal and the notification that mobile terminal receives in WiFi, WCDMA and GPRS

network environment. In each network environment we test for 20 data and average them as the result. The experiment results are shown in TABLE I.

The results in WiFi environment are better than the other two. The next is WCDMA, and the last is GPRS. This case is as expected. Even in GPRS network environment, the average delay is less than 1 second. It can be concluded from the test results that the proposed systems show excellent instantaneity, even in the case of slow transmission speeds in GPRS network environment.

From the performance tests, it is known that the design achieves the anticipated goals.

TABLE I   Test Results (Unit: ms)

	Best	Worst	Average
GPRS	316	1964	986
WCDMA	159	1394	466
WiFi	81	800	209

5. Conclusion

The notification mechanism of traditional surveillance systems cannot provide the instantaneity support for early-warning notification in surveillance systems. The proposed instant security early-warning approach based on XMPP mobile push technique cannot only improve the performance of instantaneity and efficiency of early-warning notification systems but also is a low cost solution for security surveillance.

6. Acknowledgment

7. References

[1] L. Ding, J. Chen, "Discussion on the Intelligent Video Surveillance Technology," *Intelligent Building*, vol. 8, no. 2, pp. 61-63, May 2010.
[2] M. Liu, H. Sui, J. Wang, C. Wu, "Study of Intelligent Video Monitoring Technology," *2010 Chinese Control and Decision Conference*, pp. 2789-2792 , 2010.
[3] C. Zhang, W. Zhang, "Faces of Mobile Push Technology," *Mobile Communications*, no.5, pp. 21-27, 2010.
[4] P. Schrater, D. Knill, E. Simoncelli, "Mechanisms of visual motion detection," *Nature Neuroscience*, vol.3, no.1, pp. 64, 2000
[5] S. McKenna, S. Jabri, Z. Duric, H. Wechsler, A. Rosenfeld, "Tracking Groups of People," *Computer Vision and Image Understanding*, vol. 80, no. 1, pp. 42-56, 2000.
[6] E. Bill, "XMPP.," *Computers in Libraries*, vol. 27, no. 4, pp. 22, 2007.
[7] P.Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Core," *RFC3920*, October 2004.
[8] P.Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence," *RFC3921*, October 2004.
[9] SourcrForge.net, "Android Push Notification," *Android Push Notification*, http://androidpn.sourceforge.net/ [Accessed: March-10-2013].