Monitoring System Using Smart Phones

Ms.G.C.Priya  
Assistant Professor, Department of Computer Applications  
Saveetha Engineering College  
Anna University, Tamilnadu  
E-Mail: priya.mohank@gmail.com

Ms.G.Gayathri  
Assistant Professor, Department of Computer Applications  
Saveetha Engineering College,  
Anna University, Tamilnadu

Ms.R.Parameswari  
Assistant Professor, Department of Computer Applications  
Saveetha Engineering College  
Anna University, Tamilnadu

ABSTRACT

This paper presents the implementation details of an easily affordable monitoring system for business or personal use. This system detects any intrusion and immediately intimates the owner of the setup about the same. The owner will be able to view the video of the happenings using smart phones from a remote location. The live video can also be viewed from a PC. This application allows the user to track the activities happening at a particular location.

Keywords: Intrusion detection, smart phone, PDA

1. INTRODUCTION

Security is a concept similar to safety. The nuance between the two is an added emphasis on being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security.

In the corporate world, various aspects of security were historically addressed separately notably by distinct and often non-communicating departments for IT security, physical security, and fraud prevention. Today there is a greater recognition of the interconnected nature of security requirements, an approach variously known as holistic
security, “all hazards” management, and other terms. Inciting factors in the convergence of security disciplines include the development of digital video surveillance technologies and the digitization and networking of physical control systems.

As security is a critical factor, creating an application to know the events happening at a particular location at anytime using a smart phone from a remote location is a very interesting and challenging task. It provides an efficient, operational and economical way to secure the environment just on the tip of fingers.

Multimedia transport has stringent bandwidth, delay, bit-rate, energy loss and efficient video compression requirements. It is a great challenge to support applications such as monitoring system in wireless ad-hoc networks, which are characterized by frequency link failures and congestion. All hardware and software API’s are used towards progressive success and optimization to minimize the gap between theory and technical limitations.

The trend of network convergence and smart phone accessibility in the Internet are bringing new challenges to the connectivity management of end hosts and multimedia based transport. This leads to the knowledge of functioning of the webcam and smart phones and their interfacing with the hardware.

This paper is organized as follows: In section 2, we discuss the research relevant to the system we have built. In section 3, we describe the overall architecture of Media based monitoring system and its components. We also discuss various design decisions that were taken and the rationale behind them. We analyze the performance aspect of the monitoring system along with various issues that we encountered during the overall implementation. Finally, we summarize our work and discuss future enhancements that we feel are necessary for this system to be deployed effectively.

2. RELATED WORK

A digital video surveillance system is an appliance that has embedded image capture capabilities which allows video images or extracted information to be compressed, stored or transmitted over communication networks or digital data link. This appliance can be used for any type of monitoring, either for business or personal use.
Zanny, Duro and Ortego [1] discuss the problem face with face recognition and propose a PC-based Door-opening system. The main components of this system include an Image acquisition device (webcam), a PC and an actuator (door-opening device). This system has been basically proposed to control the entry into a particular room. This is compared with the use of fingerprint sensors. The proposed system is more efficient than fingerprint sensors in the way that webcams are at least five times cheaper than fingerprint sensors and they give full control over all the parameters and settings.

WiVision [2] describes a wireless video delivery system, which uses IEEE 802.11 wireless LANs as the last mile for both real-time video distribution and on-demand video playback. WiVision can air both live events such as on-campus seminars and sports activities, and pre-stored video streams such as course lectures and financial analysis sessions, to mobile users, who can tune into selected channels of their choice from their laptops or PDAs. An innovative feature of WiVision is the support for random video access based on keyword-search, where keywords are extracted from the closed-caption text embedded in TV programs. In addition, WiVision is able to broadcast video streams on the wireless link while seamlessly working with commercially available media players. This paper presents the implementation details of the real-time acquisition and network transport components of a fully operational WiVision technology can also be used in surveillance networks where the closed circuit monitoring data can be streamed in real-time to the wireless handheld devices carried by security personnel.

The IP-based real time video surveillance system [3] provides a way to monitor the scene on the spot at any time anywhere. An embedded system acts as a sink of the system. The camera device is a front end, ad the PC-based software is for the client. This weak coupling system is very flexible, efficient and low price. Using WAP technique, cell phone can be used as a client [4].

3. SYSTEM ARCHITECTURE

For media based monitoring system, the device detecting the intrusion such as IR Tx and Rx will be connected to the PC which has webcam and internet connection. In both the cases-intrusion/no intrusion, corresponding digital output is sent to the serial port of the PC.
The webcam will be triggered in case of a positive intrusion, and will start recording the video. Correspondingly, an SMS is sent to the happening at a site we need to connect the PC with which the webcam is connected and the server part of this application should be running there in. In the server side, JMF API will be running which can handle multimedia. The main components of this handling media are:

a) the capture device
b) media processing units and players
c) the storage device

The video is captured using webcam. For programmatic control over the media, a processor is created for the following purposes.

a) Demultiplexing
b) Transcoding
c) Multiplexing
d) Rendering

In the demultiplexing stage, different streams of media are demultiplexed or extracted from a composite stream. Transcoding involves a change in the encoding format of the media. During multiplexing into a single stream. Rendering involves the presentation of the media.

For storing video in a particular format, data sink is created, which stores the captured video in a specific format on the server. Simultaneously, an alarm is activated at the PC’s end to alert the people around regarding intrusion.

Next, we can start the client part loaded in the smartphone, with which we can view the recorded video. The client part can also be a PC, where the live video captured by the webcam is streamed.

For streaming directly on a PC, RTP protocol is used. The Real-Time Transport Protocol (RTP) is an Internet protocol standard the specifies a way for programs to manage the real-time transmission of multimedia data over either unicast or multicast network services. RTP combines its data transport with a control protocol (RTCP), which makes it possible to monitor data delivery for large multicast networks. Monitoring allows the receiver to detect if there is any packet loss and to compensate for any delay jitter. RTP runs on top of the User Datagram Protocol (UDP), although it can use other
transport protocols. Both the Session Initiation Protocol (SIP) and H.323 use RTP. The owner can open the JMStudio and by giving the IP address of the video streaming server, live streams of the video can be viewed.

The overall design of the system can be explained by the following Figure 1.

![Figure 1 Overall design of Proposed System](image_url)

### 3.1 Intrusion Detection

In this hardware implementation module, intrusion is detected using IR transmitter and receiver which are connected to the Em Pro GPS-GSM kit, which in turn is connected to the serial port of the server. It gives a digital output, using which the webcam is triggered in case of a positive output. If intrusion occurs (Figure 2) an SMS is also sent to the owner, as shown in Figure 3 below.
3.2 Video Capture

Based on the output of the intrusion detection module, the server triggers the webcam. The captured video is stored in a particular format using the processor settings for the source detection, processing the video and creating the sink for media storage. This video file can be sent to the owner’s Smart Phone [5,6]. The live video is streamed using RTP (Real Time Protocol) to the connected PC. Simultaneously, an alarm is generated to notify the surroundings, as shown in the Figure 4 below.

![Block Diagram](image)

**Figure 4 Triggering a video**

3.3 Video transmission using Smart Phone

In this module, the client reads the file from the server (Figure 5.) using a smartphone, on receiving an SMS alert. The owner can then view the happenings at the desired location and can store the video accordingly, as shown in Figure 6. Also, the streamed video can be viewed from a PC using RTP and RTCP protocol.

RTP components include: a sequence number, which is used to detect lost packets; payload identification, which describes the specific media encoding so that it can be changed if it has to adapt to a variation in bandwidth; frame indication, which marks the beginning and end of each frame; source identification, which identifies the originator...
of the frame; and intramedia synchronization, which uses timestamps to detect different delay jitter within a single stream and compensate for it.

RTPC components include: quality of service (QoS) feedback, which includes the numbers of lost packets, round-trip time, and jitter, so that the sources can adjust their data rates accordingly; session control, which uses the RTCP BYE packet to allow participants to indicate that they are leaving a session; identification, which includes a participant’s name, e-mail address, and telephone numbers for the information of other participants; and intermedia synchronization, which enables the synchronization of separately transmitted audio and video streams. The block diagram is shown in Fig 5 below.

4. CONCLUSION

Transmitting video over wireless channels to/from smart devices has gained increased popularity in a wide range of applications. This framework can take various form and be applied to achieve the optimal trade off between energy consumption and video delivery quality during wireless video transmission. The framework presented here is general in the sense that it can be used in a variety of different application and network settings which makes it technically, operationally and economically feasible for security purposes.

The performance of the monitoring system can be improved in the following ways:

- Extracting a frame from the captured video and sending it as an MMS to the client’s Smart Phone.
- Streaming the live video to the client’s Smart Phone, thereby avoiding time delay.
Controlling the webcam from the Smart Phone.

Additionally, the system can be made more efficient by using the latest video compression techniques and protocols.

5. REFERENCES


