The Application of Security Mechanisms Based on Wireless Infrared Data Communications with IrDA

Sheng-Cheng Yeh*, [a]
[a] Department of Computer and Communication Engineering, Ming Chuan University
*No.5, The-Ming Rd, Gwei-Shan, Taoyuan Country 333, Taiwan, R.O.C.
*Email: peteryeh@mcu.edu.tw

Horng-Jyh Lin [b], Wan-Shin Shie [b], and Wen-Chang Lee [b]
[b] Department of Electronic Engineering, Vanung University

Abstract

The transmission technology used in Infrared data communications is the same as that found in familiar consumer electronic devices used for remote control of TV sets, VCRs, and other entertainment products, as well as in wireless keyboards and wireless printer connections for laptop computers. In this paper, the IrDA (Infrared Data Association) communication interface on PDA (Personal Digital Assistant) device or mobile phone is used to develop a doorkeeper system, which provides the wireless communication security mechanism such as password transmission, verification and query/response between clients and servers. Crypto graphic algorithms are just one piece of picture when it comes to providing security in a doorkeeper system. The next thing we need is a set of mechanisms and protocols for solving various problems. However, the corresponding encryption technique and validation mechanism are presented based on IrDA interface of PDA in the paper. The sign-in, sign-out data and the photo picture are recorded, extracted and compiled, for query and tracking purpose in the doorkeeper system, as indicated in our experimental results.

Keywords: IrDA, PDA, Security mechanism, Doorkeeper system

I. Introduction

IrDA communications are achieved using transceivers that modulate noncoherent infrared light. Thus, the security and interface problems encountered in radio and microwave systems are not present [1][2]. In this research the IrDA protocol has been used to implement a wireless doorkeeper system. Also, an authentication protocol is provided when the two participants who want to authenticate each other-think of them as a client and a server -already share a secret key [3]. This situation is analogous to a PDA user (the client) having an account on a doorkeeper system (the server), where both client and server know the password for the account [4]. The system structure is shown as Figure 1. The Centralized Database Control Server (CDCS) will provide the encryption and validation service through the Internet and the PDA user will connect through IrDA interface with the Monitor Station [5]. The improvement of data transmission security, ease of maintenance, and cost reduction are the goals of this paper. Therefore, the doorkeeper system should offer an alarm function and integrates the computer network to monitor/control from a remote site.

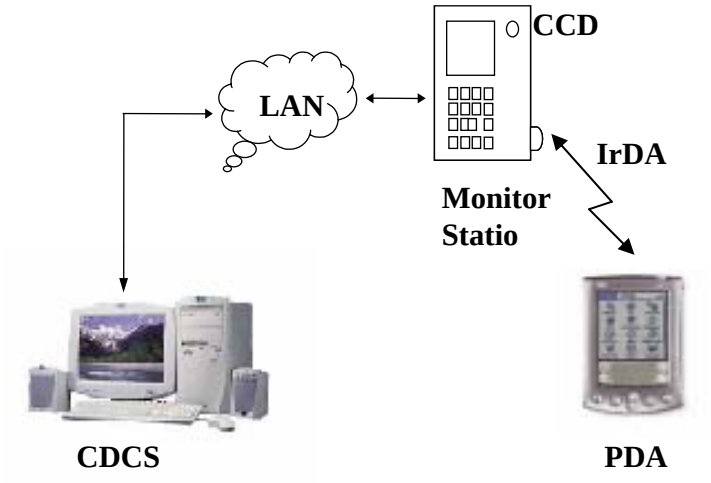

Figure 1: The architecture of doorkeeper system based on wireless IrDA interface

There are three units: (1) Monitor Station (MS), executing the validation and control process, (2) Mobile Device, PDA with IrDA interface, (3) Centralized Database Control Server (CDCS), the database server. Microsoft CE operation system supports the Monitor Station and Mobile Device. The encryption, decryption, message transmission and message reception are developed using eVB (Embedded Visual Basic) programming tool because of the high adaptability and ease. In addition the eVB can be edited in PC Windows, which means timesaving and money saving. The CDCS uses Microsoft SQL Server 2000 and Microsoft Visual Basic to create a database server service.

The Monitor Station includes an alarm module, which provides warning audio, flashing light, door lock and photo capture. The alarm module consists of an 89C51 microprocessor and is complied with assembly language. The module uses RS232 interface and can be replaced with RS422 for long distance transmission or replaced with a wireless transceiver. The CMOS CCD component captures the photo picture for checking the identification of users.

The rest of the paper is organized as follows. Section II explores the handshaking procedures between PDA terminals and Monitor Stations. Section III proposes the control management of CDCS with multiple Monitor stations. Section IV illustrates how to implement the doorkeeper system. Finally we give a short conclusion in section V.

II. Wireless Information Security Handshaking

The client and server authenticate each other using a tree-way handshake protocol similar to the one described in the algorithm used by TCP to establish and terminate a connection [6]. This situation is analogous to a PDA user (the client) having an account on a doorkeeper system (the server), where both client and server know the password for the account [4].

The operation interface of PDA user terminal is shown in Figure 2. When Monitor Station is powered on, it will stay in the idle state. When the users log in data is accepted, the Monitor Station transmits the data to CDCS for identity validation and CDCS recodes the log file, which includes photo. The validation result will open the entrance gate or set alarm.

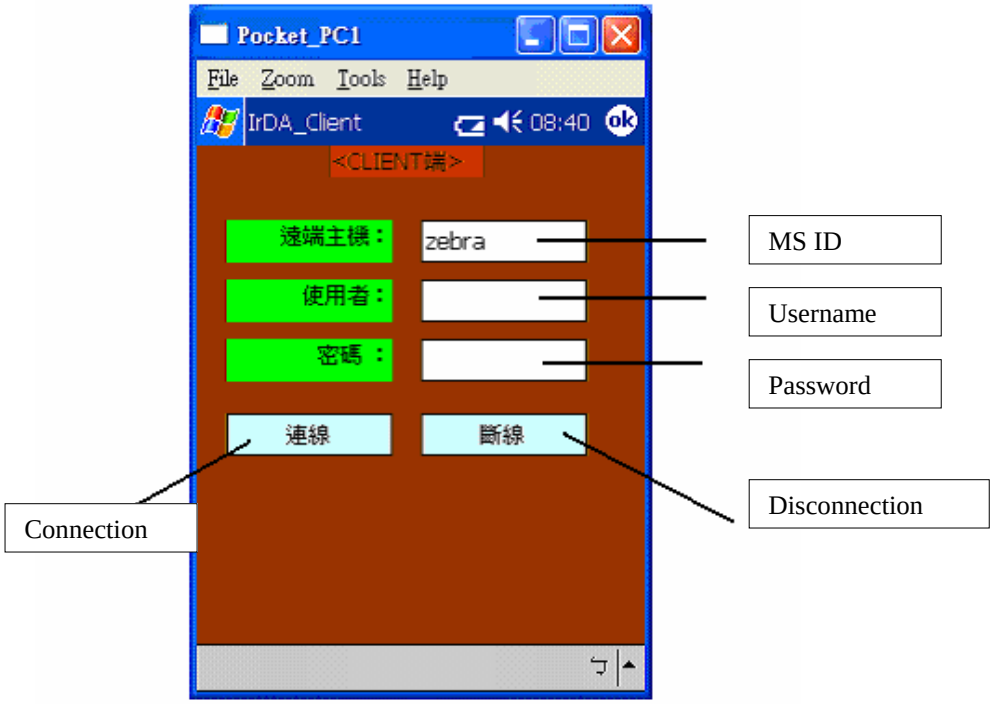

Figure 2: The operation interface of PDA user

The demonstration takes about 3 seconds, which is acceptable in most cases. Since the IrDA is for short range (1 meter) and high directivity [7], this further improves the security for the query/answer process. These main handshaking processes are described below:

1. Monitor Station always waits for Mobile Device login.
2. Client terminal uses Monitor Station ID for Request.
3. Monitor Station accepts the correct ID, then responses to the client terminal, and asks for encrypted Username and Password.
4. Monitor Station decrypts the Username and Password, and checks with Local Database server, if accepted then records the log file and opens the entrance gate; otherwise it records the log file and sets the alarm.
5. At the same time, Monitor Station calls the CCD component to captures the photo picture of the client.

III. CDCS and MS Management

A more likely scenario is that the two participants know nothing about each other, but both trust a third party. This third party is sometimes called an authentication server, and it uses a protocol to help the two participants (PDA user and Monitor station) authenticate each other [4]. In the paper the Centralized Database Control Server (CDCS) provides the encryption and validation service through the computer networks and the PDA user connects through IrDA interface with the Monitor Station. The CDCS just likes an authentication server, and to be a centralized controller for the proposed doorkeeper system.

The CDCS utilizes Microsoft SQL Server and Microsoft Visual Basic to develop communication and data base application programs. The CDCS and multiple MS flow control are depicted in figure 3. Briefly, the CDCS requests MS to change account and authorization;

this can be conducted periodically or manually, after modification it will be synchronized immediately. MS initializes the request to combine the user data or release MS memory; this can be conducted periodically or manually. In this research the MS is implemented using PDA with CCD, and alarm control and door lock control module, etc. There are two kinds of signal between CDCS and multiple MS interface. One for the control signal from CDCS to MS is to identify and synchronize the accounts. The other for the traffic signal from MS to CDCS is to transmit the Log file data and release the memory space of MS.

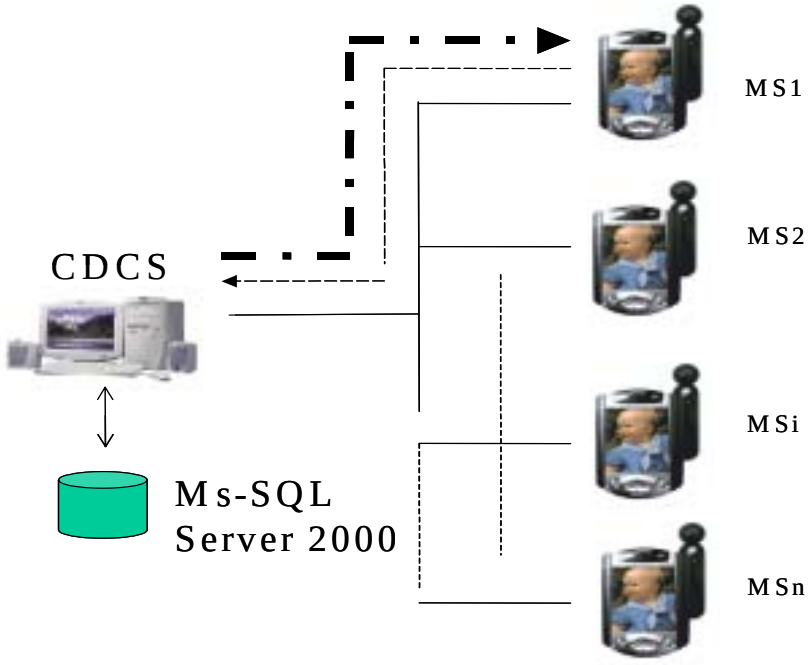

Figure 3: Control process between CDCS and multiple MS

IV. Doorkeeper System Design

The doorkeeper system consists of nine functional blocks, and executes the command from MS as shown in Figure 4. It stays so long in an idle state, before it receives the command from RS232 and conducts the corresponding action. The blocks are depicted as follows.

1. RS232 interface circuit: providing standard RS232 communication interface.
2. Input circuit: including two push buttons to control the loop time, and three DIP switches to set CCD exposure time.
3. Status display circuit: displaying the system status.
4. Power supply circuit: providing 5V/1A and 3.3V/500mA DC.
5. Alarm control loop: alarm audio ON/OFF switch.
6. Flashing light control loop: flashing light ON/OFF switch.
7. Door lock control loop: magnetic valve ON/OFF switch.
8. Photo captures circuit: CMOS CCD module.
9. Microcontroller: 89C51 control the system.

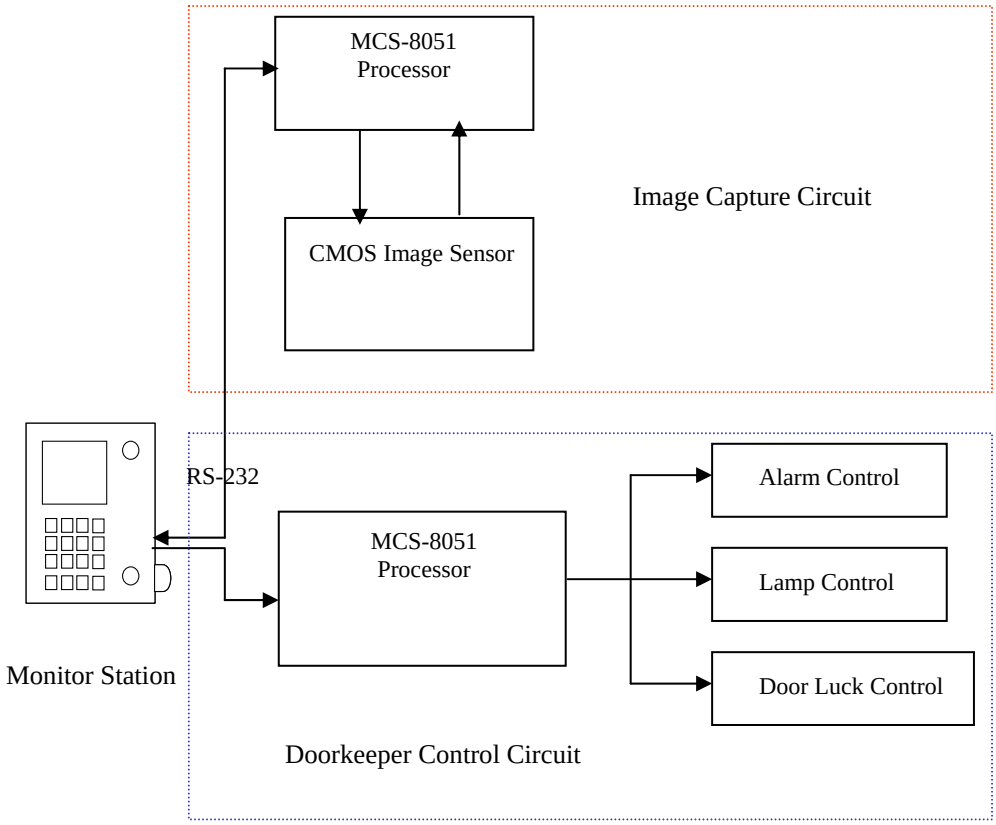

Figure 4: Block diagram of the doorkeeper system

IV. Conclusion

The paper examines mechanisms that are used to authenticate participants with IrDA protocol in a wireless doorkeeper system. Also, the research includes four major achievements: IrDA interface of PDA with MS, CDCS interface with MS, MS module design and database establishment. The demonstration verifies the hardware/software integration and successful system implementation. However, the wireless IrDA propriety of short work range (about 1 meter) and high directivity further improve the security for the query/answer process between PDA user and MS of the doorkeeper system.

Reference

[1] Patrick J. Megowan, David W. Suvak, and Charles D. Knutson, ”IrDA Infrared Communication：An Overview”, Counterpoint Systems Foundry, Inc.

[2] Charles D. Knutson, Ph.D, ”Infrared Data Communications with IrDA”, Counterpoint Systems Foundry, Inc.

[3] Ashar Aziz and Whitefield Diffie, “Privacy and Authentication for Wireless Local Area Networks”, IEEE Personal Communications Magazine, pp. 25-31, First Quarter, 1994.

[4] M.J. Beller, L.F. Chen and Y. Yacobi, “Privacy and Authentication on a Portable Communications System”, IEEE JSAC, vol. 11, no. 6, Aug. 1993.

[5] Sheng-Cheng Yeh, “The Implementation of Data Security based on Wireless Networks”, NCS 2001, vol. E, pp. 184-188, Taiwan, December 2001.

[6] Tourrilhes J., Magalhaes L., and Carter C., **“**On-demand TCP: transparent peer to peer TCP/IP over IRDA**”**, IEEE International Conference on Communications, vol. 5, pp. 3250 -3258, 2002.

[7] Sheng-Cheng Yeh, Horng-Jyh Lin, Huei-Wen Ferng, and Wen-Chang Lee, “Research of Infrared Access Technology based on Internet”, Journal of Internet Technology, vol. 4, no. 1, pp. 39-44, January 2003.