Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

Design and Implementation of Data Encryption for Networked Control Systems

Ke-Ya Yuan, Jie Chen, Guo-Ping Liu, *Senior Member, IEEE*, Jian Sun

Abstract—**Control systems are widely used in daily life and support various important infrastructure, such as power, hydraulics, petrochemicals, transport, telecom, etc. Once the control system is attacked, the consequence would be unthinkable. The DES (Data Encryption Standard) encryption algorithm is open, and it has the merit of large encryption strength and fast computational speed. This paper describes the DES algorithm, the hardware and software design of the DES hardware encryption system based on the DES encryption algorithm and FPGA (Field Programmable Gate Array). The hardware design includes the design program of the DES hardware encryption system, the design of S-box and the design of circuit architecture. The software design is mainly to write a s-function of the DES hardware interface. An experiment of a networked DC motor speed control based on DES is described, and this networked control system has the function of hardware encryption.**

I. Introduction

The importance of network security has been significantly increasing in the past few years. But the network security in networked control systems has not been thought much of. The past design of control systems almost did not have any application of security technology by internal integration, and at most applied some simple techniques to prevent an unauthorized access, such as codes and keys. The common control system is always composed of various equipments produced by different manufacturers and the integrators always do not consider security design for the whole system. In addition, the users of the control system are not security experts and they don't know how to make the system more secure. Being introduced into control systems, the Internet brings much convenience to people on one hand, but on the other hand it makes the system be more vulnerable to be attacked [1-4].

In March 2000, the SCADA (Supervisory Control And Data Acquisition) system of a sewage treatment plant which lay in Maroochy Shire, Queensland, Australia was attacked by some attackers via wireless networks, and some parameters were modified which resulted in the effluent recharge [5]. So as an emerging control system which is vulnerable to be attacked, the networked control system has an urgent need to have a security research before it is used, and to set up system security frameworks, security strategies and measures to ensure its practicability. At present the research on networked control systems is mainly concentrated on system modeling, algorithm design and how to reduce the network delay. There has been very few specialized research on security of networked control systems at present. Only the Auburn University of USA has done the research on the security of networked control systems.

The Data Encryption Standard (DES) algorithm is the most widely used encryption algorithm and has been a federal standard since 1977. Although soon to be replaced by the Advanced Encryption Standard (AES) algorithm, DES will still remain in the public domain for a number of years, such as IPSec protocols, ATM cell encryption, the Secure Socket Layer (SSL) protocol, etc [6-9]. Practice has proved that the DES algorithm could satisfy the most requirements of safety. The DES algorithm realized by software always occupies system resources to a large extent, which can cause a serious decline of the system performance. But the DES algorithm itself does not have a large number of complex mathematical calculations and only has logical operations and table look-up operations in the encryption/decryption process and the generation process of the key. So it is an ideal solution to implement the DES algorithm via hardware for better system performance and faster encryption/decryption speed [10].

II. The Design of a DES Hardware Encryption System

1. *Introduction to the DES Encryption Algorithm Principle*

Both the plain text (the data before encryption) and the encryption key of the DES operation are 64 bits. The original data need to be permutated initially and then have a serious of iterative computations with a sub-key (generated by the encryption key). At last the cipher text (the data after encryption) can be achieved after the inverse permutation. The decryption process is just like the encryption process. As shown in Fig.1, the DES algorithm begins from the initial permutation of the 64-bit plain text. The cipher text can be obtained after the 16 rounds of encryption operations and inverse initial permutations. In each round, the 32-bit data at the right part of the 64-bit data and the key are transferred to the encryption function together. Then the operational results from the encryption function and the 32-bit data at the left

This work is supported by National Science Foundation of China under Grant 60528002, 60621001 and the National High Technology Research and Development Program of China (863 Program) under Grant 2007AA04Z202.
Ke-Ya Yuan is with Institute of Automation, Chinese Academy of Sciences, Beijing, China e-mail: yuankeya@hotmail.com.
Jie Chen and Jian Sun are with Institute of Automation, Beijing University of Technology. Beijing 100081, China. Email: chenjie@bit.edu.cn.
G.P. Liu is with the Faculty of Advanced Technology, University of Glamorgan, UK, and is also with the CTGT Center in Harbin Institute of Technology, China.

978-1-4244-2794-9/09/$25.00 ©2009 IEEE

part of the 64-bit data have a XOR operation [11]. The S-box (S choice function) is the heart of the DES algorithm, by which the nonlinear transformation can be realized.

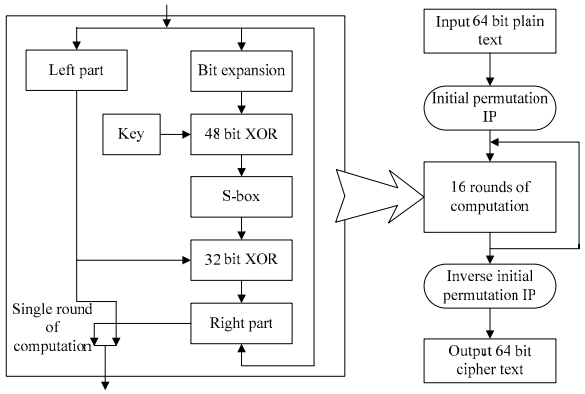

Fig. 1 DES Algorithm flow chart

2. *The Design Program of the DES Hardware Encryption System*

To achieve the highest encryption performance, the entire pipeline implementation program is taken. Because the 16 rounds of operation are as same as each other, the round operation units can be implemented by hardware and be composed to be an entire pipeline architecture by sequential cascade if the on-chip resources are adequate. With this pipeline architecture, each dada block can move into the next level of the pipeline unit for the next round operation after completing the current once. The round operation unit of this level can deal with the output data of the superior pipeline unit without extra waiting time. At an ideal state, there are 16 data blocks being serial disposed at the same time. Compared with the architecture without pipeline, the pipeline architecture can improve data processing speed 16 times, but on the other hand it occupies a large number of hardware resources.

In contrast with the entire pipeline implementation program, the resource priority program implements an encryption key transform function and an operation function of encryption key and data by hardware, and it implements one DES encryption operation by repeating to call this hardware structure 16 times. This program can reduce the hardware consumption significantly, but affect the encryption performance at a certain extent.

In this design, the EP2C8 with Cyclone II structure produced by Altera Company is used to be the vector of the algorithm, and it has 8,256 logic gates and 182 I/O ports. The encapsulation of the EP2C8 is PQ208. Considering both the performance and the resource occupation, the implementation form based on resource priority is taken finally. By setting a round counter in the round function, the number of the round operations will be calculate, and the encryption data and the original data will be distinguished before entering the round function operation for the purpose of the multiplexing function of the round function. The overall program is described in Figure 2.

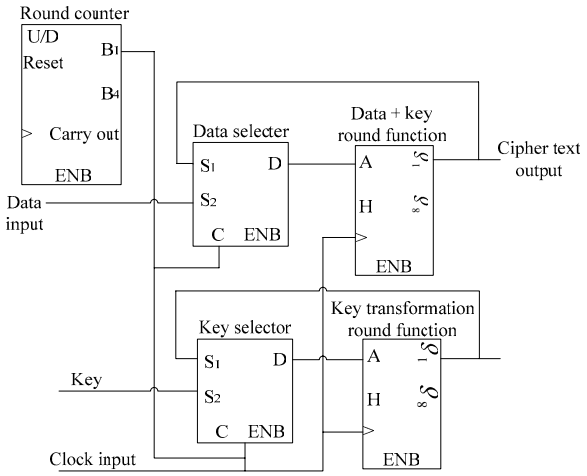

Fig. 2 the implementation program of DES Algorithm

3. *The Design of S-box*

S-box is the key steps of the DES algorithm because S-box is a complicated non-linear function, while the other operation is linear. It is precisely because of the non-linear transformation of S-box that the plain text can be confused well and be with strong security. The hardware implementation of S-box has a certain degree of difficulty and the hardware design of S-box is the main factor which can influence the encryption/decryption speed of the DES algorithm.

There are two ways that can be chosen to set up a circuit model of S-box with Verilog language. One is to describe the circuit directly using the multiple selection statement—CASE in the Verilog language. Another is to use the library function supplied by the development tool and the EAB in the device. When setting the circuit model of S-box, it is necessary to take full account of the internal structure of the device and take an appropriate form of expression for saving device resources and improving the algorithm efficiency. This paper takes the first way.

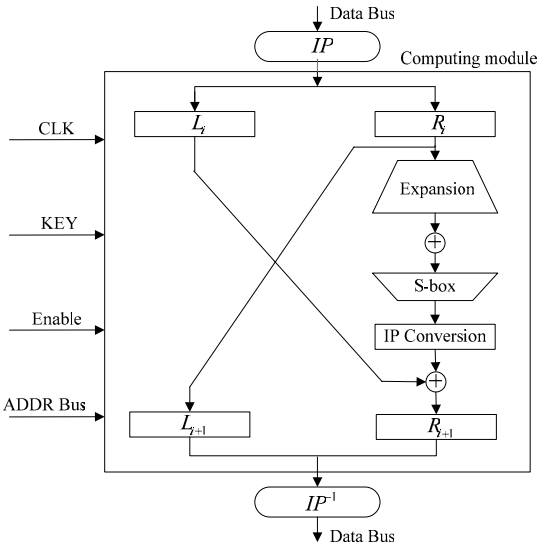

Fig. 3 the circuit architecture of the operation module of DES algorithm

4. *Design of circuit architecture*

Figure 3 shows the circuit architecture of the operation module of DES algorithm [12-13]. As shown in Figure 3, the circuit is composed of initial permutation circuit IP, 4 32-bit register— L_i, R_i, L_{i+1}, R_{i+1}, expansion permutation circuit, S-box circuit, P-box permutation circuit and the last permutation circuit IP^{-1}.

The initial permutation circuit IP is a data permutation circuit of 64-bit input and 64-bit output, and the circuit is used to make a switch of the signal between the input and output without occupation of any trigger and gate array resources except cabling resources. The extended permutation circuit, S-box circuit, P-box permutation circuit and the last permutation circuit are also without occupation of any trigger and gate array resources. The clock is an external CLK signal. After the initial permutation of the external plain/cipher text, the 64-bit data are divided into the left and the right parts with 32 bits for each part. The two parts of 32-bit data are sent into the left and the right registers— L_i and R_i, and at the beginning of the first iteration, the 48-bit data, which is generated after the data in R_i entering the expansion circuit, and the sub-key K_{i+1} generated by the circuit for it have a XOR operation with the result of the XOR operation sent to S-box. Then there are 32-bit data that are generated after the complicated operations of the S-box circuit, and the data will have a XOR operation with the left 32-bit data after being permuted by P-box. The result of this XOR operation will be sent to the right register R_{i+1} when the external enable signal is effective and the effective edge of the system clock CLK comes. The output of the R_{i+1} will be the right input of the next iterative operation, and at the same time the data in R_i will be sent to L_{i+1} to be the left input of the next iterative operation. This completes the operation of the first cycle and the second begins too. It goes on like this and when the next rising edge of the CLK comes, the ready signal and the cipher will be sent out after the 16 rounds of iterative operations.

The communication interface of the circuit consists of a 4-bit address bus, an 8-bit data bus, an encryption enable pin, and a clock input pin, etc. The clock frequency is 50MHz. Figure 4 shows the circuit board of the DES encryption system.

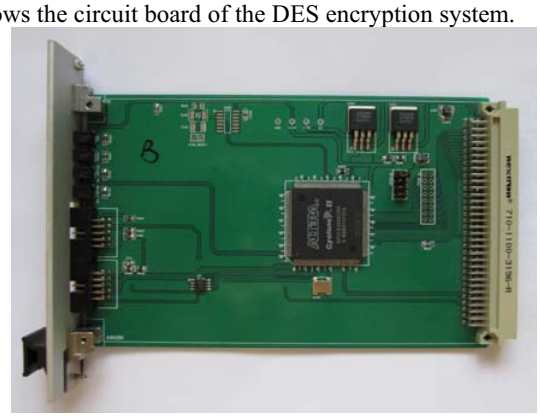

Fig. 4 the circuit board of DES encryption

4. *Performance Analysis of the DES Hardware Encryption System*

The Verilog code can be simulated by Modelsim, and the simulation waveform is shown in Figure 5.

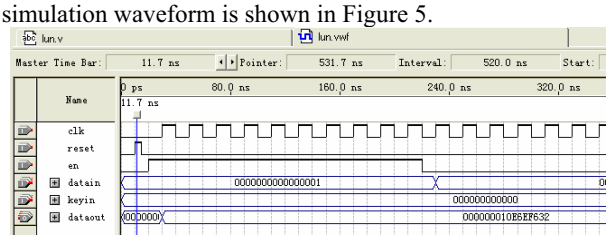

Fig. 5 ModelSim simulation waveform

The simulation waveform, shown in Figure 5, shows that the system can realize a continuous encryption/decryption of the 64-bit data in 220ns. It can also be estimated that the hardware encryption speed of the system can be 200Mbit/S, and this speed can satisfy the demands of the communication via 100M network.

III. The Software Design of The DES Encryption System

In this paper, the control strategy is implemented by the block diagram in Simulink. Using the Real-Time Workshop (RTW) of Matlab, the block diagram can be converted into executable codes and be downloaded into the controller to execute. It needs to write a s-function of the DES hardware interface to read/write the information of the hardware device in the control program. And the s-function must be written by C language, because any other language will not be supported except C when the block diagram of the simulink is converted into executable code by RTW.

The main functions of the s-function include:

a. mdlInitializedSizes: Initializing SimStruct (s-function simulation data structure defined by Matlab). It includes checking the number of the parameters, setting the input/output information of the module, setting the number of the discrete/continuous state variables, opening the DES hardware device file and getting corresponding file descriptor.

b. mdlInitializeSampleTimes: Initializing I/O device and setting sampling time and some related parameters of the module.

c. mdlOutputs: Achieving the encryption/decryption function. First, the input/output signal pointers are obtained from the s-function API and the data before encryption/decryption is read from the input signal. Then the 64-bit data will be decomposed into 8 bytes that will be written into I/O cache. After encryption/decryption, the data can be read from the buffer and the data will be evaluated to the output signal. The 64-bit data was read once every 8 bits data. That's a full process of encryption/decryption.

d. mdlTerminate: The stay proceeding. The hardware is set to be the initial state and the device is turned off.

IV. Networked Control Experiment of DC Motor Based on DES

1. *The Networked Control System—Netcon*

As the vector of this experiment, Netcon [14-15] is a generic platform of NCS simulation and realization based on Windows. It consists of the networked controller (NetController), networked visual control configuration software (NetConLink) and networked visual supervision configuration software (NetConTop). It can simulate the control method and strategy in NetConLink for several kinds of objects and automatically generate executable code, which can be executed after being downloaded to NetController. It can also constitute a local or networked control loop and control the charged objects. The NetConTop can be used to have a remote real-time monitoring and maintenance via Ethernet.

2. *The Networked Control Experiment of DC Motor Based on the DES Hardware encryption system*

In order to demonstrate the performance of the DES hardware encryption system applied in networked control systems, a networked DC Motor speed control test rig has been built, which consists of two networked controllers (NetController) and one DC motor with its driver [16-17]. The controller and the DC motor are shown in Figure 6.

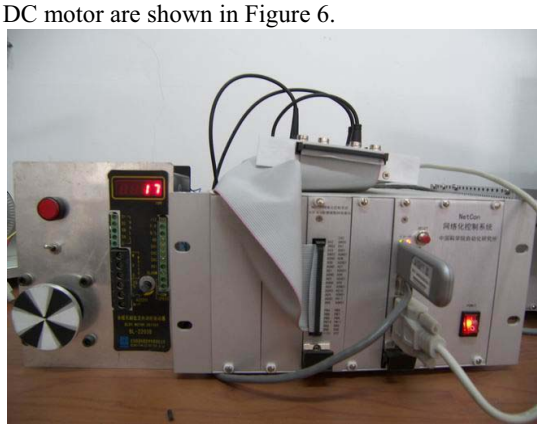

Fig. 6 the Netcontroller and the DC motor

Text In the experiment, one NetController is connected to the DC motor driver by a cable, in which there are the pulse acquisition module and the DA module that are for the sensor and actuator, respectively. The function of the pulse acquisition module is acquiring the speed of the motor at every sampling time. The function of the DES hardware encryption system is encrypting the data of the speed, sending the data out via Ethernet, receiving the control information from Ethernet, and sending the information to the motor after it being decrypted. There is a networked predictive control program running in the other Netcontroller unit. This unit receives information from the sensor via Ethernet, and the information will be sent to NPC module after being decrypted by the DES module. The NPC module can calculate the predictive control sequence, which contains the output values of the actuator at the current moment and the several future control values. The predictive control sequence will be sent out via Ethernet after being encrypted by the DES module. The IP addresses of the two NetController units are 192.168.67.139 and 192.168.67.44, respectively, and the two NetController units used port udp4001 and udp4112 to communicate each other. The schematic of the whole networked control experiment is shown in Figure 7.

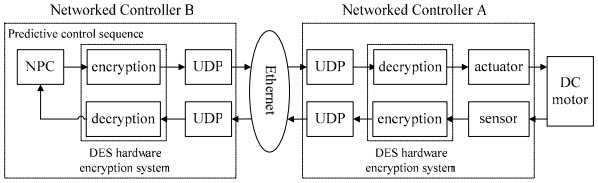

Fig. 7 schematic of the networked control experiment of DC motor

In order to validate the performance of the DES hardware encryption system in the networked control, there are two experiments that were given in this paper. The first one is the networked control experiment of the networked DC motor speed control without the DES hardware encryption system. The networked visual supervisory software—NetConTop is used to monitor the state of the two networked NetController units.

In the top part of Figure 8, the black curve is the reference value of the motor's speed and the gray curve the real-time response data of the motor's speed acquired by networked NetController Unit A. The gray curve in the middle part of Figure 8 is the response data of the motor's speed received by networked NetController Unit B via Ethernet. In the bottom part of Figure 8, the gray curve is the measured data of the system delay. The sampling period of the control system is 40ms and the curve shows that the delay of the networked control system is 0.14s.

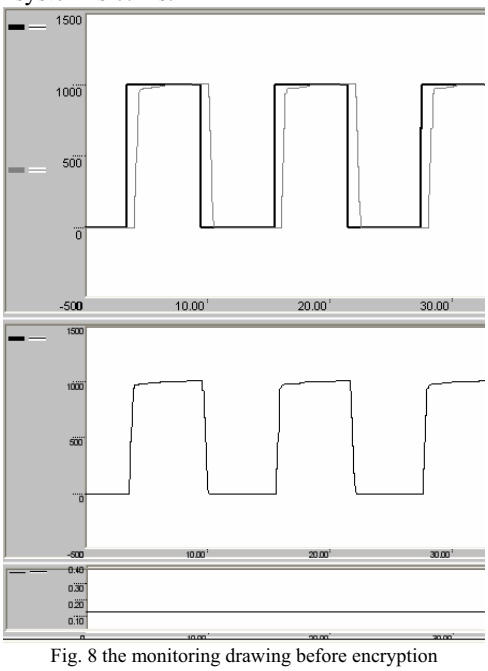

Fig. 8 the monitoring drawing before encryption

The second experiment is the networked control experiment of DC motor speed control with the DES hardware encryption system. The experimental results are shown in Figure 9.

In the top part of Figure 9, the black curve is the reference

input of the motor's speed and this set value is the same as the one in the first experiment. The gray curve in the top part of Figure 9 is the real-time response of the motor's speed acquired by networked NetController unit A. The gray curve in the middle part of Figure 9 is the response data of the motor's speed received by networked controller B via Ethernet after encryption and the curve shows that the data of the motor's speed after encryption is disorderly and unsystematic. In the bottom part of Figure 9, the gray curve is the measured data of the system delay and the curve shows that the delay of the networked control system is 0.14s. It is obviously that the DES hardware system almost has no influence on the real-time characteristic of the networked control system.

By comparison of the two figures, it can be seen that the system can achieve the function of hardware encryption. In addition, using this hardware the networked control system has a superior performance in saving system resource and keeping the real-time characteristic of the system, which makes it possible to use more complex algorithms in this system.

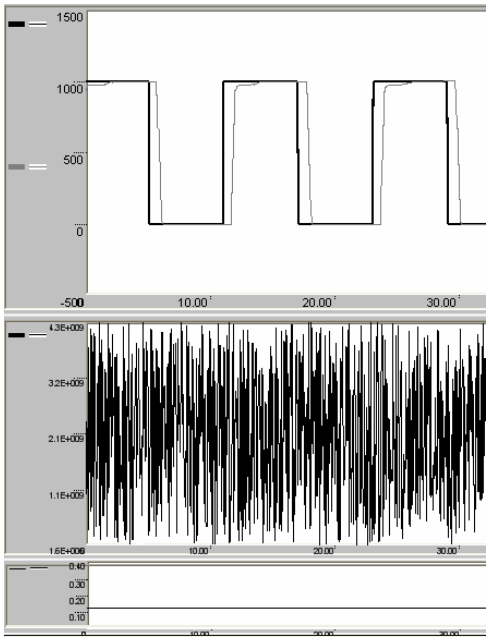

Fig. 9 the monitoring drawing after encryption

V. CONCLUSION

This paper has introduced a hardware design method of data encryption systems based FPGA and DES. It has studied the hardware realization method of the DES encryption algorithm and the operation reliability of the networked control system. It has been shown by the experiments that the method of hardware encryption is feasible and it has a greater advantage than software encryption in saving system resources and achieving better real-time characteristic. The research work in this paper will play a catalytic role to some extent in the development of the research on data security of networked control systems through more efforts.

REFERENCES

[1] Bell D.E. and LaPadula L.J., "Secure Computer System:Unified Exposition and Multics Interpretation", Miter MTR-2997,March 1976.

[2] Marin, G.A., "Network security basics", Security & Privacy, IEEE, Volume 3, Issue 6, Page(s):68 - 72 ,Nov.-Dec. 2005.

[3] Al-Shaer E., "Network Security Policies: Verification, Optimization and Testing",Network Operations and Management Symposium,NOMS 2006. 10th IEEE/IFIP, Page(s):584 - 584, 3-7 April,2006.

[4] Lincke, S.J., Holland, A., "Network security: Focus on security, skills, and stability", Frontiers in education conference - global engineering: knowledge without borders, opportunities without passports, 2007. FIE '07. 37th annual,Page(s):F1D-10 - F1D-15,10-13 Oct. 2007.

[5] Geer, D., "Security of critical control systems sparks concern Computer", Computer,Volume: 39, Issue: 1, pp.20- 23, 2006.

[6] National Bureau of Standards, Data Encryption Standard, U.S. Dept. of Commerce, FIPS pub. 46, January 1977.

[7] ANSI X9.17 (Revised),"American National Standard for Financial Institution Key Management (Wholesale)", American Bankers Association, 1985.

[8] ISO DIS 8732: "Banlung - Key Management (Wholesale): Association for Payment Clearing Services", London, December 1987.

[9] McLoone M., McCanny J.V., "A high performance FPGA implementation of DES" Signal Processing Systems, 2000. SiPS 2000. Page(s):374 – 383,11-13 Oct. 2000.

[10] McLoone, M., McCanny, J.V., "High-performance FPGA implementation of DES using a novel method for implementing the key schedule", Circuits, Devices and Systems, IEE Proceedings,Volume 150, Issue 5, Page(s):373-378, 6 Oct. 2003.

[11] Vikram Pasham, and Steve Trimberger, URL:"http://www.xilinx.com/support/documentation/application_notes/xapp270.pdf", Aug. 2001.

[12] C.Patterson, "High Performance DES Encryption in Virtex FPGAs Using Jbits" , Proc. IEEE Symp. Field-Programmable Custom Computing Machines (FCCM '01), 2000.

[13] S.Trimberger, R. Pang, and A. Singh, "A 12 Gbps DES Encryptor/Decryptor Core in an FPGA" , Proc. Cryptographic Hardware and Embedded Systems (CHES '00), pp. 156-163, 2000.

[14] Haibo Bian, G.P. Liu and Zhe Dong. "Structure Design and Application of Embedded Ethernet Based Control Systems", 2007 IEEE International Conference on Networking, Sensing and Control,page(s): 47-51, 15-17.April 2007.

[15] Haibo Bian, Xueyuan Nie, Guoping Liu, "Based MATLAB Application research of NCS", Application research of Computers Vol.23, pp14-16, 2006.

[16] Li Kunjie, Guoping Liu. "Design and Realization of Motor Control System Based on State flow and Ethernet." proceedings of the 25 Chinese Control Conference. pp.525-528, 11 August, 2006.

[17] Dong Zhe, Liu Guoping, Tao Yuegang," Design and Implementation of Networked Predictive Control over Wireless IP Networks", Proceedings of the 26th Chinese Control Conference.pp565-570, July 26-31, 2007.