Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **3**, May **2015**

Design of Embedded Ethernet Interface Based on Chaotic Stream Cipher

Chun-Lei Fan, Song-Yan Liu and Qun Ding

Key Laboratory of Electronic Engineering College of Heilongjiang Province
Heilongjiang University, Harbin, China
qunding@aliyun.com

Received November, 2014; revised January, 2015

Abstract. *Nowadays, embedded network products are widely used in various fields. However, when these products are used, the transmission of network data couldn't be guaranteed with a higher security. To address this issue, this paper designed an embedded network security interface. Network interface is studied based on S3C6410 processor and DM9000 Ethernet controller, the hardware circuit of network card interface is designed and developed with conciseness and stability. On the side of software design, an improved algorithm of chaotic encryption based on logistic mapping is proposed. According to binary sequences generated from improved algorithm to encrypt network packets. Besides, The DM9000 platform device driver is designed with the purpose of NIC to work properly. Finally, through to the whole system experimental debugging, this has confirmed the validity and security of system.*

Keywords: Embedded system, DM9000, Chaotic encryption, Ethernet interface

1. **Introduction.**

As we enter the 21st century, with the development of the science and technology, the Internet is developing rapidly. Network development brings enormous convenience for modern society. It also has brought an unprecedented impact. At the same time, embedded system is more and more widely used. Embedded devices has been developed rapidly in the research lab and used widely in many fields such as industry, military department and personal consumption [1]. However, a number of embedded network products haven't a higher security in our daily life. Therefore, how to ensure that the security of embedded network communications become an urgent issue to solve. There is a desire to search a highly efficient response plan.

According to the situation, people begin to introduce chaos system in cryptography field. The security of network data would be improved by utilizing characters of chaotic system. At present, the researchers have carried out a lot of investigations and have already gained some achievements in this respect [2, 3, 4]. References [5, 6] propose a high-security encryption algorithm by combining chaotic mapping with cryptography. Reference [7] analyzes the security of digital chaos encryption system. References [8, 9] are able to apply chaotic encryption algorithm to hardware circuit. Furthermore, the feasibility and effectiveness of system are demonstrated by encrypting network data. However, major research of chaotic encryption is based on the theory and simulation at present, which did not apply chaotic mapping to the embedded field.

For this problem, in this paper, embedded Ethernet interface based on chaotic stream cipher is designed to enhance the security of network data, which combines logistic chaotic encryption, embedded Linux system with Ethernet. In addition, the paper proposed an improved algorithm of Logistic chaotic sequences, and it overcomes some disadvantages by combining Logistic chaotic sequences with Arnold transformation. The new algorithm of Logistic chaotic sequences has a good performance on safety and has the ability to meet the requirements of confidential communication. Therefore, the design of system can achieve network data communication and file transfer with rapidity and security. It will play a positive role in the research and application in the field of embedded Ethernet.

The rest of this paper is organized as follows. Section 2 gives the hardware design of embedded network interface and DM9000 driver programs are studied in Section 3. Furthermore, improved algorithm of Logistic chaotic sequences are discussed in Section 4. Finally, overall test of system is showed in Section 5.

2. **Hardware Design of Embedded Network Interface.**

2.1. **Overall framework of hardware design.** The design concept of embedded system network interface uses S3C6410 processor as the core of the system. It connects with nand flash and SDRAM so that Linux embedded operating system can run normally. In addition, a DM9000 independent module is designed for connect to the ARM11 processor by connectors. Besides, this system has serial port and JTAG port for program download and testing. The physical map of hardware circuit is shown in figure 1.

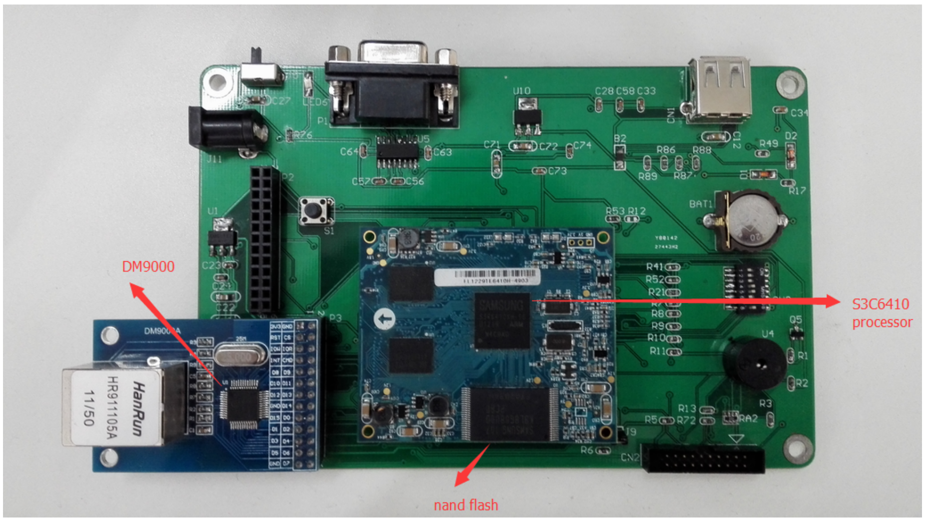


FIGURE 1. Physical map of hardware circuit

2.2. **Main circuit design of ethernet interface.** The interconnection design of S3C6410 and DM9000 are the most important in the hardware design of the embedded Ethernet interface. Ethernet micro-controller is connected to the bus of processor. Therefore, network data can be exchanged on the external bus. The wiring connection diagram is shown in figure 2.

The DM9000 of system adopts 16-bit working pattern. DM9000 data bus D[0..15] are connected to the processor's DATA[0..15] for network data transmission. Break request signal and EINT9 are linked together. The IOR and IOW serve as read/write command pin with low-level effectively. CS signal pin of chip select is connected to the processor's CSN0 and 0x10000000 as NIC port address. Therefore, DM9000 address port 0x10000000 and data port 0x10000004 are defined according to chip select CSN0. The access control of DM9000 is controlled by CMD pin. CMD pin is read as high-level for access to the data port and low-level access address port. Moreover, the input of address port is the

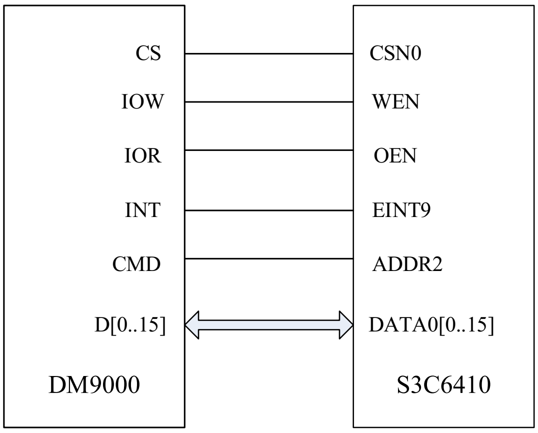


Figure 2. The wiring diagram of S3C6410 and DM9000

data port register address before accessing any card registers. The address of the register should be saved in the address port [10, 11].

3. **Design of DM9000 Driver Programs.** The DM9000 network device driver of this system is designed based on the platform driver architecture. Platform device as a virtual device can effectively simplify the design difficulty of the driver [12]. It has two parts of platform_device and platform_driver. The actual design flow chart is shown in figure 3.

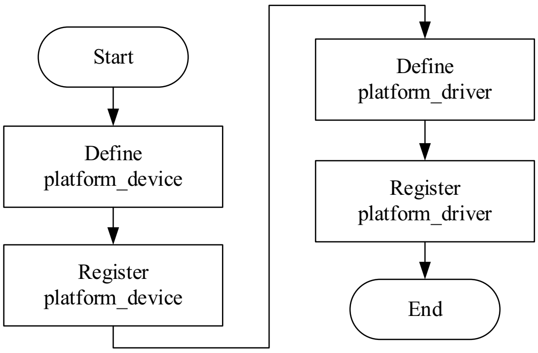


Figure 3. Design flow chart of platform device drivers

Firstly, s3c_device_dm9000 structure is defined as platform device according to design flow chart of platform device drivers. Secondly, static structure resource allocates some resources for requirement of DM9000 network device, such as interrupt signal, chip selects, etc. Finally, programs need to finish platform_device structure's registration. With the completion of the tasks, platform driver dm9000.c is written. The key functions of programs are analyzed and designed in detail in the paper.

The sending and receiving of data packets are extremely important to network devices. Sending process of data packets can be described as follow. Driver activate DM9000 card and call the open function of net_device structure open the network device when a network data needs to be sent. Then hard_start_xmit function is invoked by dev_queue_xmit structure so that the data of sk_buff structure can is sent to the network physical devices. DM9000 has 16KB SRAM to act as sending and receiving data buffer. The address of data buffer ranges from 0x0000 to 0x0BFF. The area can save two complete Ethernet frame. The data frame length is written to the register TXPLH and TXPLL [13]. The sk_buff will is released and returns zero value when packets are sent successfully. The

Table 1. Field contents of receiving data

Field type	Field description
Receiving data flag byte	01H for a data 00H for no data
Status flag byte	Display RST register values Indicates that the data type
The length of the low byte	Receive data of low length identifier
The length of the high byte	Receive data of high length identifier
The data fields	Store the received data

driver will generate interrupt and inform system to send the next frame while first data completes transmission. Flow chart of sending data is shown in figure 4.

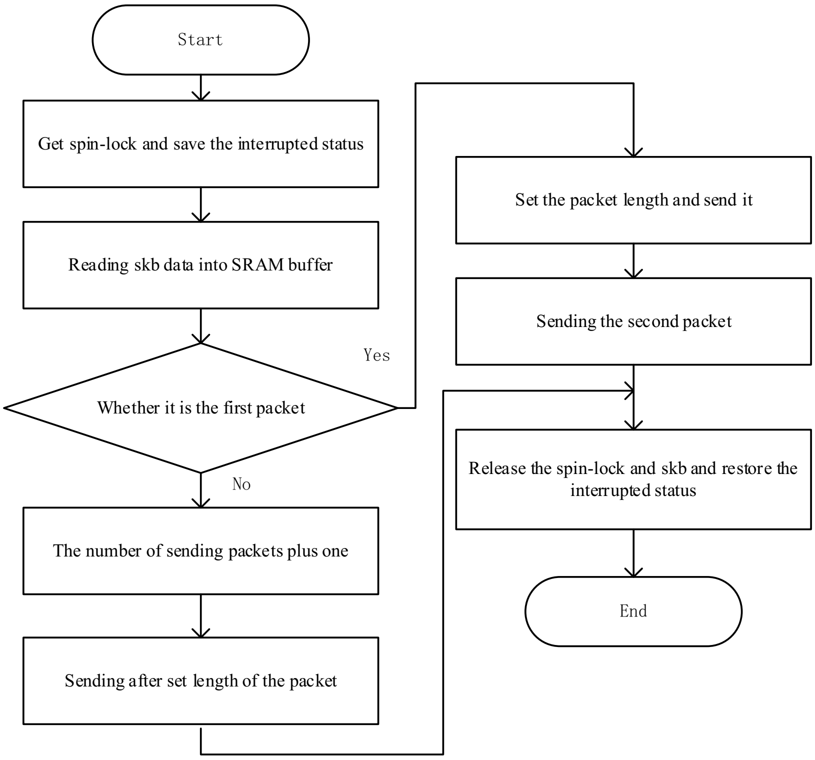

Start
Get spin-lock and save the interrupted status
Reading skb data into SRAM buffer
Whether it is the first packet
Yes
No
The number of sending packets plus one
Sending after set length of the packet
Set the packet length and send it
Sending the second packet
Release the spin-lock and skb and restore the interrupted status
End

Figure 4. The flow chart of sending data

DM9000 network equipment is through the interrupt mechanism to receive packets [14]. Driver will generate an interrupt after network device receives a packet. Sk_buff structure is allocated in interrupt function for the sake of saving data. The address of receiving data buffer ranges from 0x0C00 to 0x3FFF, then the relevant information of data is filled to sk_buff after system read the data from a hardware in the receive buffer. Finally, netif_rx function is invoked to send the packet to upper network protocol layer. It means that system will generate an interrupt after network card receives a packet. In addition, processor read the data through MRCMDX or MRCMD register and the receiving packet format and function of each field as shown in table 1.

4. Improved Algorithm of Logistic Chaotic Sequences.

4.1. **Logistic chaotic mapping and quantification.** Logistic mapping is a classical model of chaotic system, and its simple equations as well as good performance are widely as chaotic secure communication system [15]. The mapping is defined as

$$x_{n+1} = \mu x_n \left(1 - x_n\right), \mu \in \left(0, 4\right], x_n \in \left[0, 1\right] \tag{1}$$

Among μ is called as branch parameter, when the value area of μ is [3.5699456, 4], logistic mapping work on chaotic state and show a complex dynamic characteristics. Substituting initial value x_1 into the chaotic equation, the chaotic binary sequences were generated based on repeated iterative operation. These sequences are periodic sequences, which possess sensitive dependence on initial value and strange attractor. These features correspond with character of cryptographic key. Therefore, chaotic mapping is widely used in the secure communication system.

The original chaotic sequences $\{x_n\}$ are quantified into binary sequences $\{s_n\}$ as key sequences [16]. It has a variety of ways to quantize chaotic sequences, this paper chooses relatively simple quantitative method to avoid complex computations. It's defined as follows

$$s_n = \begin{cases} 0, x_n < c \\ 1, x_n \geq c \end{cases} \tag{2}$$

Where $c = 0.5$. When logistic mapping show chaotic state, Iterative computation value x_n will traverse on (0, 1) interval. Therefore, it can get good chaotic binary sequences by the quantitative method.

4.2. **Arnold mapping and improved algorithm of chaotic sequences.** Classical Arnold transform is a two-dimensional reversible mapping [17]. The definition can be expressed as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod} 1), A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \tag{3}$$

Among $0 \leq x, y \leq 1, 0 \leq x', y' \leq 1$.

An improved algorithm of chaotic sequence based on logistic mapping and Arnold transform is proposed in this paper, the algorithm block diagram as shown in figure 5. Firstly, as can be seen clearly from the block diagram that 0/1 sequences flow are built into N order matrix. Secondly, this matrix is iterated based on Arnold transform. Due to the matrix of order N, namely the domain of definition $x \in [0, N-1], y \in [0, N-1]$ is integer value. In this paper, the formula (3) can be converted into formula (4) with the purpose of convenient operation. Finally, according to the row order, iterative matrix element convert into a binary sequences flow. It has a simple xor operation with original chaotic binary sequences to generate the final improved sequences.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod} N), A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \tag{4}$$

In contrast with the traditional algorithm, the improved algorithm easy to implement, and it will reduce the resource consumption of hardware circuit. Besides, there are problems that the short period of chaotic sequences in the restricted computer precision will be effectively solved [18].

5. **Overall Test of System.**

5.1. **Set up development environment and compile Linux kernel.** The cross development environment needs to be established for embedded application. The design of the system installs Linux operating system of ubuntu9.10 version and cross-compilation tool chain of cross-4.2.2-eabi. DM9000 network drivers are modified in the source code after set up environment. Next, the kernel will be compiled by using the "make" command after configuration. Finally, compiling DM9000 driver into the kernel image file

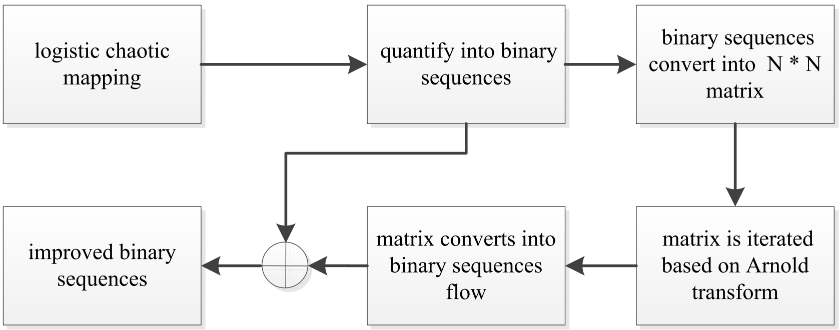
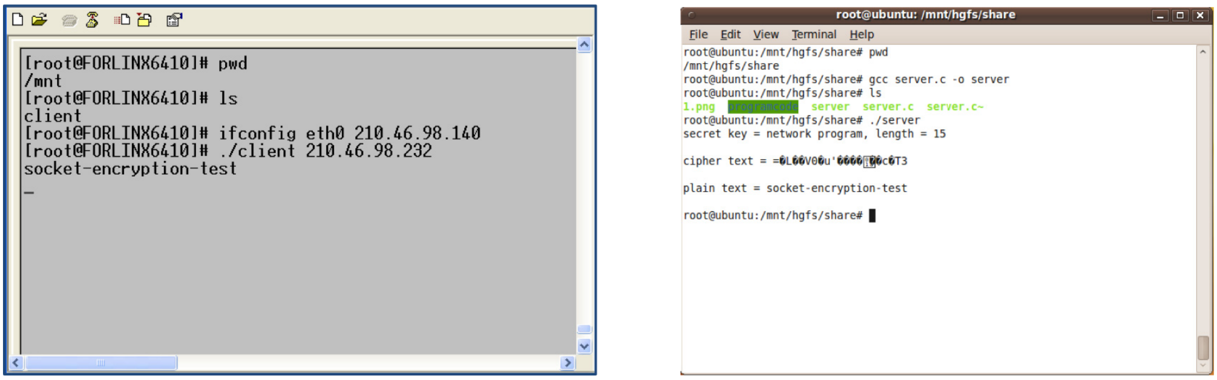

logistic chaotic mapping
quantify into binary sequences
binary sequences convert into N * N matrix
matrix is iterated based on Arnold transform
matrix converts into binary sequences flow
improved binary sequences

FIGURE 5. The block diagram of improved algorithm



```
[root@FORLINX6410]# pwd
/mnt
[root@FORLINX6410]# ls
client
[root@FORLINX6410]# ifconfig eth0 210.46.98.140
[root@FORLINX6410]# ./client 210.46.98.232
socket-encryption-test
_
```

(A) client-side

```
root@ubuntu:/mnt/hgfs/share# pwd
/mnt/hgfs/share
root@ubuntu:/mnt/hgfs/share# gcc server.c -o server
root@ubuntu:/mnt/hgfs/share# ls
1.png  programcode  server  server.c  server.c~
root@ubuntu:/mnt/hgfs/share# ./server
secret key = network program, length = 15

cipher text = =�L��V0�u'�����c�T3

plain text = socket-encryption-test

root@ubuntu:/mnt/hgfs/share# █
```

(B) server-side

FIGURE 6. The execution results of C programs

and generate zImage. The zImage, uboot, root file system burn to target board after completing the above steps.

5.2. **Chaotic encryption based on stream cipher.** This paper written the socket programs based on C/S model in order to guarantee the security of the network data transmission. The programs adopt corresponding regulation of socket in transferring message and data [19]. Besides, the paper combines improved logistic sequences with RC4 stream cipher to encrypt network data. This encryption algorithm is simple and convenient for hardware implementation. Next, we download the C programs to target board by serial port. The client. c and server. c programs are executed after start Linux embedded system. Client side sends "socket-encryption-test" to server side. The data is encrypted based on RC4 algorithm before server side receives the data [20]. The data is decrypted by the some secret key after server side receives the cipher text. The cipher text and plain text are printed on the server side. The experiment result is shown in figure 6. Therefore, this system can guarantee the security of network communication.

6. **Conclusion.**

This paper introduces a hardware design of embedded Ethernet interface based on S3C6410 ARM11 processor and DM9000 Ethernet controller. Besides, it combines improved logistic sequences with RC4 stream cipher to encrypt network data. The system is designed with high reliability and maintainability, which especially fits the Internet access and security of embedded products. Therefore, there are also important research and reference values in embedded network security device.

Acknowledgments. This work is partially supported by Natural Science Foundation of China (No. 61471158) and Institutions of Higher Learning by the Specialized Research Fund for the Doctoral Degree (No.20132301110004).

REFERENCES

[1] Z. H. Liu, *CAN-Ethernet Gateway Design and Implementation Based on ARM9*, M. S. Thesis, Chengdu University of Technology, Chengdu, China, 2009.

[2] T. Y. Wu, T. T. Tsai, and Y. M. Tseng, Efficient Searchable ID-based Encryption with a Designated Server, *Annals of Telecommunications*, vol. 69, issue 7-8, pp. 391-402, 2014.

[3] T. Y. Wu, Y. M. Tseng, Publicly Verifiable Multi-secret Sharing Scheme from Bilinear Pairings, *IET Information Security*, vol. 7, issue 3, pp. 239-246, 2013.

[4] T. Y. Wu, Y. M. Tseng, and T. T. Tsai, A Revocable ID-based Authenticated Group Key Exchange Protocol with Resistant to Malicious Participants, *Computer Networks*, vol. 56, no. 12, pp. 2994-3006, 2012.

[5] S. J. Deng, D. Xiao, F. H. Tu, Design and Implementation of Chaos Encryption Algorithm Based on Logistic Formula, *Journal of Chongqing University*, vol. 27, no. 4, pp. 61-63, 2004.

[6] Y. W. Wang, X. Y. Wang, Design of Digital Chaotic Encryption Algorithm Based on Dual Chaotic Maps, *Journal of Southeast University*, vol. 35, no. Sup(II), pp. 128-131, 2005.

[7] G. J. Hu, Z. J. Feng, Security Property of a Class of Digital Chaotic Encryption System, *Journal of Electronics and Information Technology* , vol. 25, no. 11, pp. 1514-1518, 2003.

[8] Q. Liu, J. Q. Fang, and G. Zhao, Research of Chaotic Encryption System Based on FPGA Technology, *Acta Physica Sinica*, vol. 61, no. 13, pp. 1-6, 2012.

[9] B. Chen, G. H. Liu, and Y. Zhang, Hardware-realized Method of Chaotic Encryption, *Journal of UEST of China*, vol. 35, no. 1, pp. 32-35, 2006.

[10] C. Han, K. R. Wang, Design and Realization of Embedded System Network Interface Based on DM9000, *Industrial Control Computer*, vol. 20, no. 4, pp. 17-18, 2007.

[11] X. K. Chen, S. J. Jiang, Design of Embedded Network Interface Controller Based on ARM9 and ARM Linux, *First International Conference on Future Computer and Communication*, Wuhan, China, pp. 142-149, 2009.

[12] H. Q. Huang, J. D. Wu, DM9000AE and Application on Embedded Ethernet, *Industrial Control Computer*, vol. 19, no. 11, pp. 90-93, 2006.

[13] Q. Wang, *Design of Network Card Drivers Based on Linux and DM9000*, M. S. Thesis, Liaoning University, Liaoning, China, 2013.

[14] J. Q. Zhou, F. X. Zhou, Development of network driver program based on embedded Linux, *Computer Engineering and Des*, vol. 30, no. 22, pp. 5124-5127, 2009.

[15] J. X. Chen, Z. L. Chu, An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism, *Optics Express*, vol. 21, no. 23, pp. 27873-27890, 2013.

[16] Y. B. Zheng, J. Pan, and Y. Song, Research on the Quantifications of Chaotic Random Number Generator, *International Journal of Sensor Networks*, vol. 15, no. 1, pp. 139-143, 2014.

[17] Z. J. Tang, X. Q. Zhang, Secure image encryption without size limitation using Arnold transform and random strategies, *Journal of Multimedia*, vol. 6, no. 2, pp. 202-206, 2011.

[18] B. X. Du, X. L. Geng, and F. Y. Chen, Generation and realization of digital chaotic key sequence based on double K-L transform, *Chinese Journal of Electronics*, vol. 22, no. 1, pp. 131-134, 2013.

[19] X. P. Wang, Communicational Mechanism of Socket and Winsock in TCP/IP Environment, *Aeronautical Computing Technique*, vol. 34, no. 2, pp. 126-128, 2004.

[20] M. Matsui, Key collisions of the RC4 stream cipher, in *16th International Workshop*, O. Dunkelman (eds.), Berlin/Heidelberg/New York, Springer-Verlag, LNCS 5665, pp. 38-50, 2009.