Journal of Applied Analysis and Computation
Volume 6, Number 5, November 2016, 1126–1134
Website:http://jaac-online.com/
DOI:10.11948/2016074

DESIGNING NETWORK ENCRYPTION MACHINE BASED ON HENON CHAOTIC KEY ALGORITHM*

Chunlei Fan[1], Qi Zhang[1], Haoran Sun[1], Bingbing Song[1]
and Qun Ding[1,†]

Abstract Nowadays, embedded network products are widely used in various technological fields. However, when such products are used, the transmission of network data could not be guaranteed with high security. To address the issue, this paper designed a network encryption machine based on S3C6410 processor and DM9000 Ethernet controller. The hardware circuit of this encryption machine is designed and developed with conciseness and stability. In software design, an improved algorithm of chaotic encryption based on Henon mapping is proposed. The algorithm overcomes the shortcoming in combining Logistic and Tent chaotic sequences. Moreover, the paper demonstrates some comparative experiments about autocorrelation and randomness. The results indicate that the new algorithm based on Henon chaotic sequences has a good performance in safety and is able to meet the requirements of confidential communications.

Keywords Embedded system, Henon mapping, key stream generator, network encryption.

MSC(2010) 62P30, 97P30, 97R50.

1. Introduction

As we are entering the 21st century, with the development of science and technology, especially the Internet, network science and technology bring enormous convenience to the modern society and an unprecedented impact on industry. Meanwhile, embedded systems are more and more widely used. Embedded devices have been developed rapidly in research labs and used widely in many fields such as electronics industry, military, and personal consumption [13]. However, a number of embedded network products do not have high enough security. Therefore, how to ensure high security in embedded network communications has become an urgent issue to solve.

Knowing the current situation, people begin to introduce chaos systems into cryptography for network security, where network data are secured by utilizing desirable characters of chaotic systems. At present, researchers have carried out a lot of investigations and have already gained some achievements in this respect [9–11].

[†] the corresponding author. Email address: qunding@aliyun.com (Q. Ding)
[1] School of Electronic Engineering, Heilongjiang University, Harbin 150080, China

[*] 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) and Postgraduate Technology Innovation Project (YJSCX2015-022HLJU).

References [3,12] propose a high-security encryption algorithm by combining chaotic maps with cryptographic techniques. Reference [5] analyzes the security of a digital chaos-based encryption system. References [2, 6] embedded a chaotic encryption algorithm into hardware circuit. Furthermore, the feasibility and effectiveness of chaotic systems are demonstrated by encrypting network data. However, major research of chaotic encryption is based on the chaos theory and computer simulation at present, which did not apply chaotic maps to embedded systems.

To address this problem, in this paper a network encryption machine based on a chaotic stream cipher is designed to enhance the security of network data encryption, which combines Henon map based encryption and the embedded Linux system with Ethernet. In addition, this paper proposes an improved algorithm based on Henon chaotic sequences, which overcomes some disadvantages by combining Logistic chaotic sequences with Tent chaotic sequences. The new algorithm based on Henon chaotic sequences has a good performance on safety and is able to meet the requirements of confidential communications. Therefore, the design of the system can achieve secure network data communications and file transfer with fast speed and high security. It will be useful for research and applications in the field of embedded Ethernet.

2. Hardware Design of Network Encryption Machine

2.1. Overall framework of hardware design

The design concept of network encryption machine 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, the DM9000 independent module is designed for connect to the ARM11 processor by connectors. Moreover, this system has serial port and JTAG port for program download and testing. The physical map of hardware circuit is shown in figure 1.

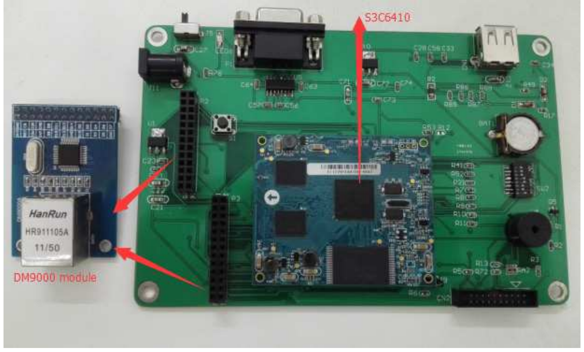


Figure 1. Physical map of hardware circuit.

2.2. Main circuit design of network encryption machine

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.

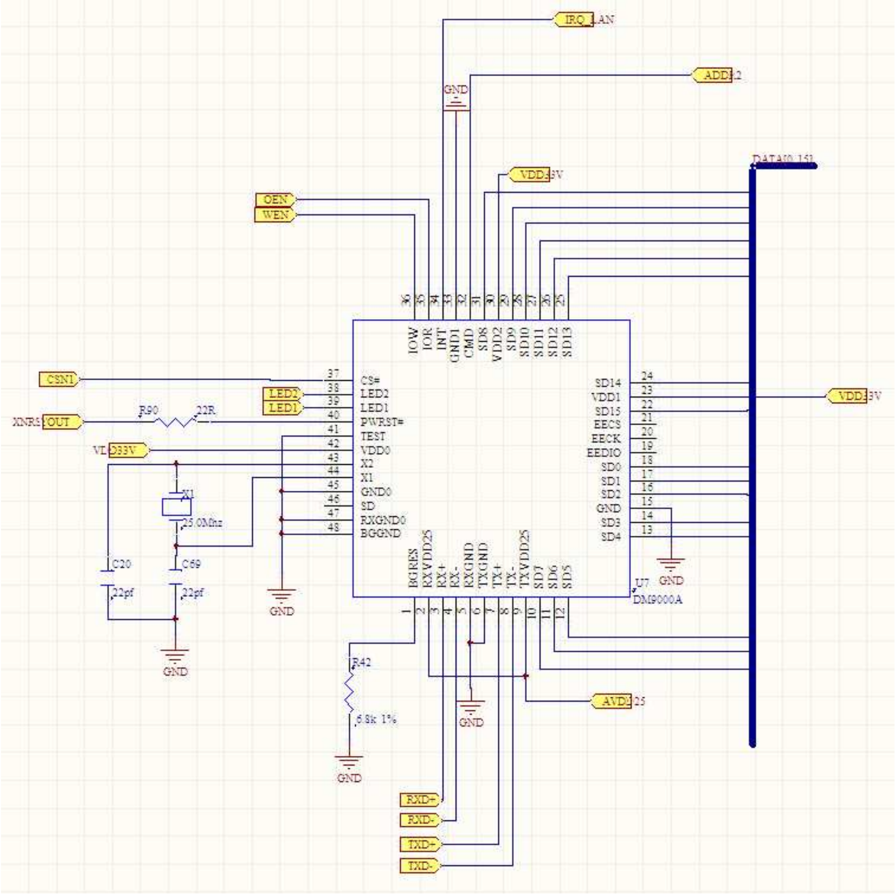


Figure 2. Schematic diagram of DM9000 module.

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 EINT 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 CSN1 and 0x10000000 as NIC port address. Therefore, DM9000 address port 0x10000000 and data port 0x10000004 are defined according to chip select CSN1. 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 data port register address before accessing any card registers. The address of the register should be saved in the address port [4].

The transmission part of the DM9000 module's data packet is written in the buffer zone, which will be sent automatically after the execution of the command. As an integrated Ethernet controller chip, data transmission, verification, bus data packet collision detection is done by the chip itself, only need to configure the relevant parameters. The DM9000 receives the Ethernet data packets and then automatically sends the data to the buffer zone and sends out the interrupt signal, CPU can receive data through DMA (Direct Memory Access) in the interrupt routine. And then through the remote DMA to read back the data from the DM9000 memory space to the ARM processor.

3. Improved Algorithm of Henon Chaotic Sequences

3.1. Improved algorithm implementation scheme

Aiming at machine with finite precision would make digital chaotic binary sequences into similar short period sequences so that it lowers the security of chaotic encryption system for the problem. In this paper, a new improved algorithm is proposed, this algorithm is designed by using hybrid multiple chaotic systems, and a new pseudo random sequence generator is designed. Here, it is called a mixed chaotic sequence generator. The schematic diagram of the mixed chaotic sequence generator is shown in Figure 3.

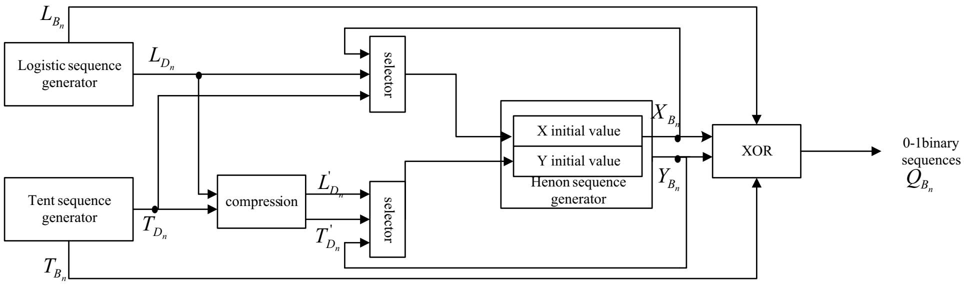


Figure 3. Schematic diagram of the mixed chaotic sequence generator.

The basic design idea of the hybrid chaotic sequence generator is described as below. The each real valued output sequence of Logistic sequence generator and Tent sequence generator as the initial value for the x and y of the Henon sequence generator. Which generator's output value is chosen, the 0-1 values that are generated by the x and y parts are used as the selector part of the data selector. With the output 0-1 binary sequence of the x and y parts of the Henon sequence generator, it xor the output 0-1 binary sequence of the logistic sequence generator with the tent sequence generator, the resulting sequence is the 0-1 binary sequence of the final output of the mixed chaotic sequence generator.

Using mathematical formula description, iterative algorithm of Henon sequence generator is represented by H. The output real value of Logistic sequence generator and the 0-1 binary sequences are represented by $\{L_{D_n}\}$ and $\{L_{B_n}\}$, the output real value of Tent sequence generator and the 0-1 binary sequences are represented by $\{T_{D_n}\}$ and $\{T_{B_n}\}$, the output sequence of the Logistic sequence generator and Tent sequence generator which send to the Henon sequence generator as the initial value of the y part is represented by $\{L'_{D_n}\}$ and $\{T'_{D_n}\}$, the x and y parts output 0-1 binary sequence of the Henon sequence generator are represented by $\{X_{B_n}\}$ and $\{Y_{B_n}\}$, finally the 0-1 binary sequence of the entire mixed chaotic sequence generator is represented by the $\{Q_{B_n}\}$.

First, according to the x and y output iterative value $X_{B_{n-1}}$ and $Y_{B_{n-1}}$ of the Henon sequence generator last time, to determine the input of the x and y parts are provided by the Logistic sequence generator or the Tent sequence generator. As shown below:

$$X_{B_n} = \begin{cases} H(L_{D_n}), & X_{B_{n-1}} = 0, \\ H(T_{D_n}), & X_{B_{n-1}} = 1, \end{cases} \tag{3.1}$$

$$Y_{B_n} = \begin{cases} H(L'_{D_n}), & Y_{B_{n-1}} = 0, \\ H(T'_{D_n}), & Y_{B_{n-1}} = 1. \end{cases} \tag{3.2}$$

The value of the final mixed chaotic sequence generator is expressed as follows:

$$Q_{B_n} = L_{B_n} \oplus T_{B_n} \oplus X_{B_n} \oplus Y_{B_n}. \tag{3.3}$$

3.2. The performance analysis of sequences

3.2.1. Autocorrelation Test

Autocorrelation is an important property of pseudo random binary sequences, it can carry out periodic detection of the sequences, and the perfect pseudo random sequences are δ function [14]. Suppose $x\,(n)$ is a chaotic binary sequences, $\mathrm{ac}\,(m)$ is the autocorrelation function of the sequences, the definition of autocorrelation function can be obtained by the following:

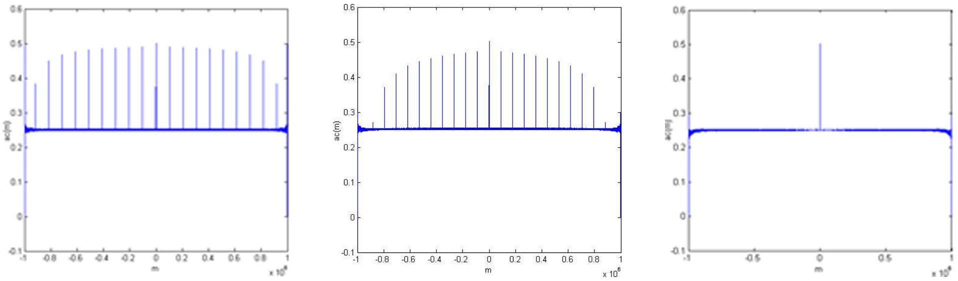
$$\mathrm{ac}\,(m) = \sum_{n=-\infty}^{\infty} x\,(n) x\,(n+m)\,. \tag{3.4}$$

In this paper, the sequences length are 10^6, then calculate the correlation function values according to the formula (3.4). The matlab simulation diagram is shown in figure 4. It can be clearly seen from the diagram that the sequences generated by the logistic and tent mapping appears the short period of the sequences in the case of the 32 limit of the calculation accuracy. However, the improved autocorrelation function of the mixed chaotic binary sequences is more close to the δ function, which shows better pseudo random property.

3.2.2. Frequency Test

The focus of the frequency test is the proportion of zeroes and ones for the entire sequence. The purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to 1/2, that is, the number of ones and zeroes in a sequence should be about the same. Frequency formula is defined as follows:

$$\chi^2 = \frac{(n_0 - n_1)^2}{N}. \tag{3.5}$$



(a) logistic sequences (b) tent sequences (c) Improved sequences

Figure 4. Test simulation of autocorrelation function.

Where n_1 and n_0 represent the number of 1 and the number of 0 respectively, and N is the length of the sequence. This statistic can obey χ^2 the distribution of free degree 1. According to formula (3.5), frequency test results of the mixed chaotic sequence generator is shown in Table 1.

Table 1. Frequency test results

test item	sequence length N						
	10000	30000	50000	80000	400000	700000	1000000
n_0	5031	14997	24980	40008	199511	349283	499123
n_1	4969	15003	25020	39992	200489	350717	500877
χ^2	0.3844	0.0012	0.0320	0.0032	2.3849	2.9377	3.0765

Table 1 shows that the number of 0 and the number of 1 of the mixed chaotic sequences are both approximately equal. In addition, this χ^2 value is less than 3.841. That is to say, the mixed chaotic sequences can better satisfy the frequency test requirement.

3.2.3. Run Test

The focus of this runs test is the total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits. A run of length k consists of exactly k identical bits and is bounded before and after with a bit of the opposite value. The purpose of the runs test is to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such zeros and ones is too fast or too slow. Run test is usually used to determine if the number of run 1 or run 0 satisfies the requirements of the pseudo-randomness of digital sequences. The number of k-length run is about $1/2^k$ of the whole run in the same sequences. The run test results of digital sequences of mixed chaotic map is shown in Table 2.

From Table 2 we can find that 1-length run nearly satisfies the theoretical value $1/2$. And by this analogy, 5-length run nearly satisfies the theoretical value $1/2^5$. So the digital mixed chaotic sequence can better satisfy the run test requirement.

In addition, NIST test suite is designed to test the performance of the random number generator from the SP800-22rev1 file. We can know it contains 15 tests [1,

Table 2. Run test results

sequence length	length of runs				
	1	2	3	4	5
10000	0.4960	0.2532	0.1191	0.0639	0.03246
90000	0.4974	0.2499	0.1266	0.0631	0.03136
500000	0.5003	0.2488	0.1254	0.0625	0.03163
1000000	0.4999	0.2501	0.1253	0.0624	0.03101

8]. According to P-value based on test program, the improved sequences appears good in the test and meets the requirement. It shows the favorable pseudo-random characteristic.

4. Overall Test of System

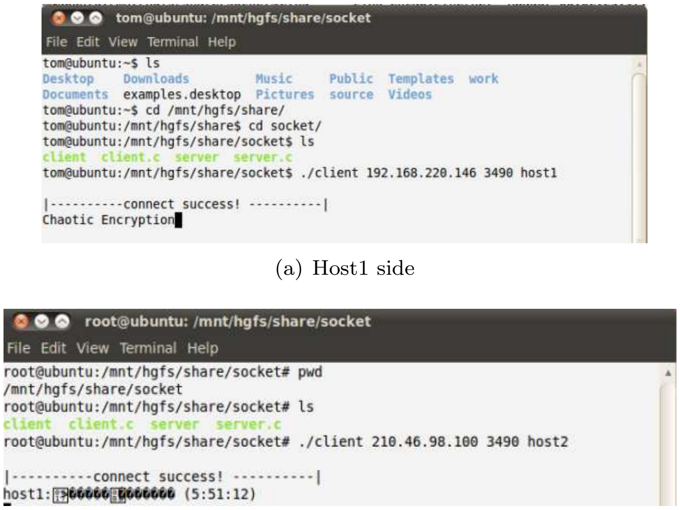
4.1. Set up development environment and compile Linux kernel

The cross development environment needs to be established for embedded application. The design of the system installs Linux operating system of ubuntu12.10 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 and generate zImage. The zImage, uboot, root file system burn to target board after completing the above steps.

And then set up the experimental environment, running server core board ARM program, so that it is in the monitor block state, then run two PC client program and make it also connects to the server, through the network, we can carry out the information by the network communication, host1 transfer plaintext to host2, because the network is not safe enough, so the ARM board is used to encrypt the information by the chaotic sequences before transmission [7], the experimental results are shown in figure 5. From the graph, we can see that the host1 sends a plaintext “Encryption Chaos” to host2, and then encrypted by the ARM chaotic encryption system, it ensures the security of network communication data.

5. Conclusion

This paper introduces a hardware design of network encryption machine based on S3C6410 ARM11 processor and DM9000 Ethernet controller. Besides, it combines improved Henon sequences with 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.



tom@ubuntu: /mnt/hgfs/share/socket
File Edit View Terminal Help

```
tom@ubuntu:~$ ls
Desktop    Downloads         Music     Public  Templates  work
Documents  examples.desktop  Pictures  source  Videos
tom@ubuntu:~$ cd /mnt/hgfs/share/
tom@ubuntu:/mnt/hgfs/share$ cd socket/
tom@ubuntu:/mnt/hgfs/share/socket$ ls
client  client.c  server  server.c
tom@ubuntu:/mnt/hgfs/share/socket$ ./client 192.168.220.146 3490 host1

|----------connect success! ----------|
Chaotic Encryption█
```

(a) Host1 side

root@ubuntu: /mnt/hgfs/share/socket
File Edit View Terminal Help

```
root@ubuntu:/mnt/hgfs/share/socket# pwd
/mnt/hgfs/share/socket
root@ubuntu:/mnt/hgfs/share/socket# ls
client  client.c  server  server.c
root@ubuntu:/mnt/hgfs/share/socket# ./client 210.46.98.100 3490 host2

|----------connect success! ----------|
host1:▯������▯������� (5:51:12)
```

(b) Host2 side

Figure 5. Experimental results.

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) and Postgraduate Technology Innovation Project (YJSCX2015-022HLJU).

References

[1] A. Akhshani, A. Akhavan and A. Mobaraki, *Pseudo random number generator based on quantum chaotic map,* Communications in Nonlinear Science & Numerical Simulation, 19(2014)(1), 101–111.

[2] B. Chen, G. H. Liu and Y. Zhang, *Hardware-realized method of chaotic encryption,* Journal of UEST of China, 35(2006)(1), 32–35.

[3] 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, 22(2013)(1), 131–134.

[4] C. Han and K. R. Wang, *Design and realization of embedded system network interface based on DM9000,* Industrial Control Computer, 20(2007)(4), 17–18.

[5] G. J. Hu and Z. J. Feng, *Security property of a class of digital chaotic encryption system,* Journal of Electronics and Information Technology, 25(2003)(11), 1514–1518.

[6] Q. Liu, J. Q. Fang and G. Zhao, *Research of chaotic encryption system based on FPGA technology,* Acta Physica Sinica, 61(2012)(13), 1–6.

[7] A. Shrobek, *Cryptanalysis of chaotic stream cipher,* Physics letters A, 363(2007)(1), 84–90.

[8] X. M. Wang, W. F. Zhang and W. Guo, *Secure chaotic system with application to chaotic ciphers,* Information Sciences, 221(2013)(1), 555–570.

[9] T. Y. Wu and Y. M. Tseng, *Publicly veriable multi-secret sharing scheme from bilinear pairings,* IET Information Security, 7(2013)(3), 239–246.

[10] T. Y. Wu, T. T. Tsai and Y. M. Tseng, *Ecient searchable ID-based encryption with a designated server,* Annals of Telecommunications, 69(2014)(7), 391–402.

[11] 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, 56(2012)(12), 2994–3006.

[12] Y. B. Zheng, J. Pan and Y. Song, *Research on the quantifications of chaotic random number generator,* International Journal of Sensor Networks, 15(2014)(1), 139–143.

[13] Y. F. Zhou, L. W. Li and L. L. Zou, *Practical Tutorial of Embedded Linux, Publishing House of electronics Industry,* beijing, 2014.

[14] Y. Zhou, C. Y. Zhu and Y. M. Wang, *Study on the performances of logistic digital chaotic sequences,* Modern Electronics Technique, 19(2006)(9), 69–71.