Network Data Encryption Technology based on Hardware Protocol and Algorithm

Wang Linjing,Tang Guoliang

Henan University of Traditional Chinese Medicine,Zhengzhou 450008,China

Xuexi123@163.com

Keywords: Hardware encryption, Network data, Register, Single chip microcomputer, Gold code.

Abstract. In order to improve the security of network data transmission and avoid the leakage of transmission data, this paper proposes an enhanced data transmission security and reliability scheme, and design a new data encryption and decryption system using hardware encryption protocol and algorithm. The main function of the network hardware encryption machine includes the single chip microcomputer, FPGA and El interface; the main function of the single chip microcomputer is to enter the initial key, in which FPGA is responsible for generating the encrypted key stream; the E1 interface is responsible for receiving and transmitting data; the password system uses 63 bit Gold code, and using DS21348 register completes the level conversion of HDB3 and TTL, to realize the full duplex communication of encryption and decryption. Finally, the encryption system is tested, it can be found that the system can effectively complete the data encryption and decryption operations in the process of data transmission, and it can be converted into the plaintext ciphertext, and can also reduce decrypt the cipher text to ensure the security of information. The fuzzy chaos degree of system encryption and the accuracy of decryption are higher, which can weaken the intensity of attack and improve the reliability of the system.

Introduction

With the rapid development of network technology and electronic information technology, FPGA has been widely used in the field of encryption because of FPGA design is flexible and reliable, which plays an important role in the design of encryption hardware system. Hardware encryption method does not occupy computer resources, the encryption process is effectively isolated with the external system, and there are higher data transmission protection ability, higher algorithm program performance and better independence [1,2]. The encryption machine is composed of single chip microcomputer, FPGA and El communication interface, in which encryption algorithm can be programmed by VHDL language, it has higher the security of data transmission; the terminal uses the higher degree of encryption equipment, such as computer, POS machines and so on, which can improve the security and confidentiality of data transmission.

Network Data Stream Encryption and Decryption Principle

Network data encryption technology based on the hardware protocol uses the stream cipher algorithm, and the stream cipher algorithm is composed of two parts, including key and password [3-5]. The key is stored in the encryption device, and the password algorithm is not changed in a long time. The encryption principle is shown in Figure 1.

Figure 1 shows the schematic diagram of hardware protocol network data encryption, encryption and decryption end apply a same initial key. In encryption, there are stream cipher and plaintext dissimilarity, and each period of time is joined the encrypted data; in decryption, the ciphertext and password flow XOR can get the original plaintext, in which synchronous mode uses 63 Gold code [6]. The received data volume and Gold code need to do cross correlation operation, if the relevant results satisfy the three value characteristics, it shows that they join the synchronization Gold code, and then to call the decryption algorithm and to decrypt the encrypted data, restoring the transmission data, so as to complete the entire process of encryption and decryption.

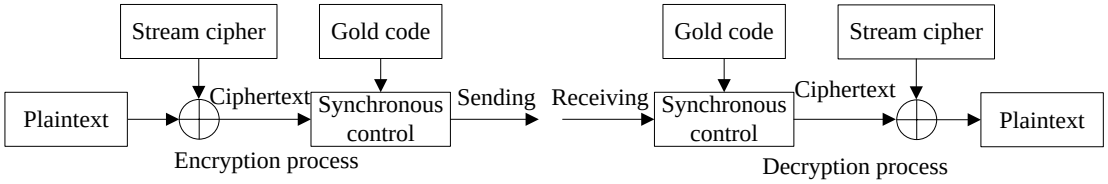

Fig. 1 The schematic diagram of encryption

Network Encryption Hardware System Design

Network hardware encryption machine system is mainly composed of three parts, including single chip microcomputer, FPGA and El 121 [7]. The main role of single chip microcomputer is to enter the initial key, FPGA is responsible for generating encrypted key stream, and E1 interface is responsible for receiving and sending data to achieve protocol data and communication.

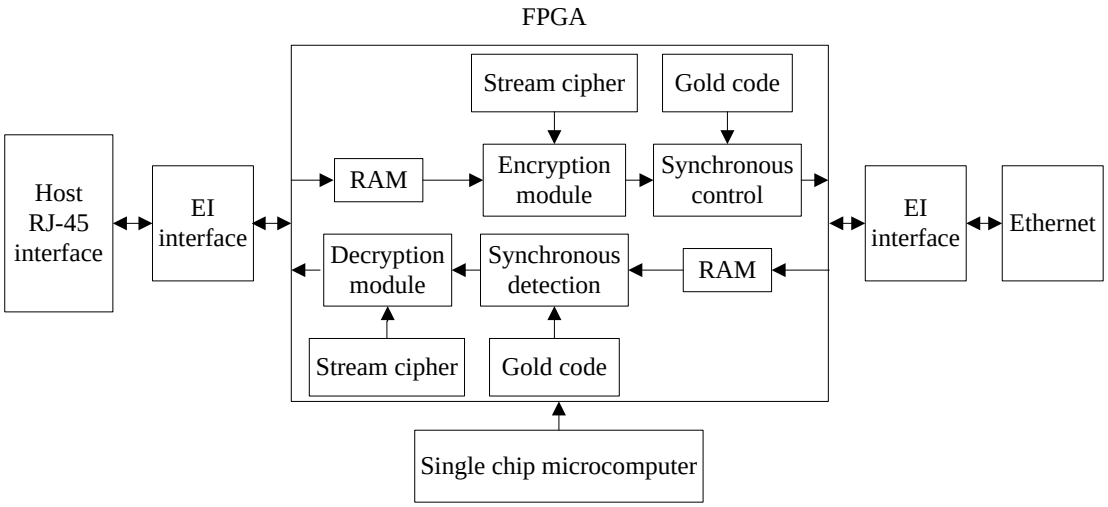

Fig. 2 network data encryption hardware system design framework

Figure 2 shows the hardware system frame diagram of network data encryption, the communication link uses the E1 standard, the external link connects 121 interfaces, the interface device is DS21348. DS21348 uses register that selects the E1 line interface unit, and it can configure hardware mode to complete HDB3 and TTL level conversion [8]. The system can achieve the way of encryption and decryption full duplex communication, in which the encryption time sequence diagram is shown in Figure 3.

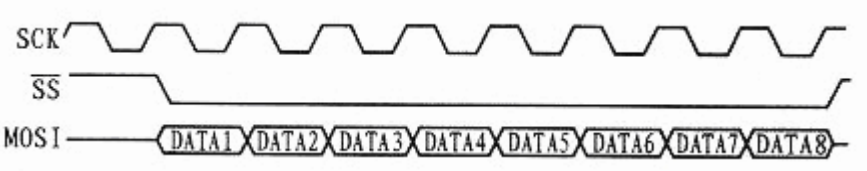

Fig. 3 Encryption timing diagram

Figure 3 shows the encryption timing diagram using 4 signal lines, in which the serial clock is SCK, machine input and host output use MOSI, and machine output and host input use SS. FPGA uses EP20F256C6 in CyeloneII series, the device is the low cost architecture FPGA, which can provide up to 18751 logic units, the hardware can efficiently complete the core operations of encryption and decryption. The encryption and decryption process are shown in Figure 4 and Figure 5.

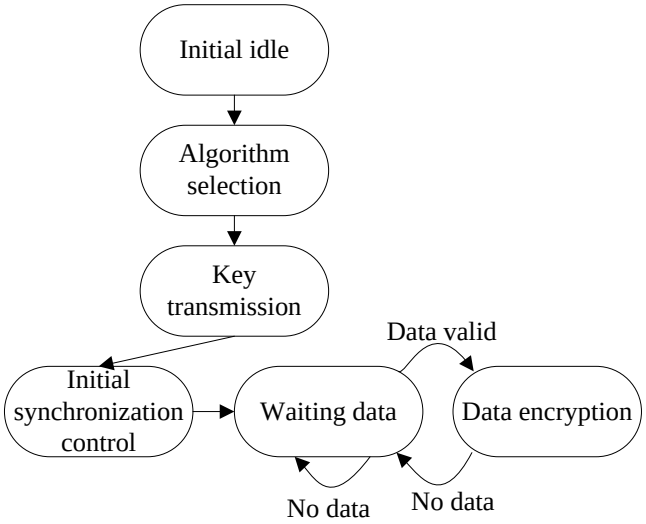

Fig.4 network data encryption process

Figure 4 shows the process of data encryption, the user can enter the initial password and algorithm through the microcontroller. The use of SPI interface transfers to FPGA, key data passes to algorithm module after FPGA gets the key; when data encryption produces effect, the system starts the encryption algorithm; if the data is invalid, the system continues to enter the waiting state.

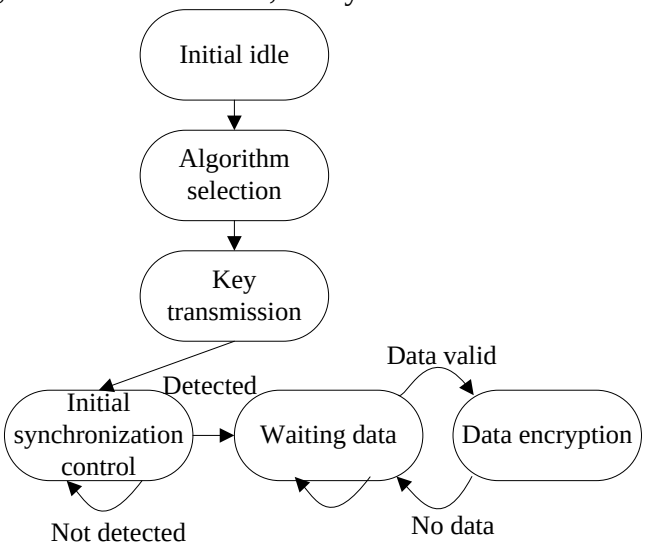

Fig. 5 Network data decryption process

As shown in Figure 5, the system firstly detects the initial synchronization Gold code in the network data decryption process, the password is valid after tested, the system will start the decryption algorithm; if the password is invalid, waiting for the data, so repeatedly, to complete the decryption process, and then it carries out two expansion after initial key sends to FPGA, so as to achieve the required number.

Network Data Encryption Machine Test based on Hardware Protocol

In order to verify the validity and reliability of hardware protocol network data encryption system, this paper tests the performance of the system [9-11]. Firstly, the system configures the network parameters, and then to set the network IP address and register SUB value. The system sets the source MAC and SIPR registers SHAR value, in which the configuration parameters are shown in Table 1.

Table 1. Network configuration parameters

W5500 hardware address	08.DC.00.01.02.08
Gateway IP address	192.168.1.0
Subnet mask address	255.255.255.0
Local IP address	192.168.0

After the system configures network parameters, it starts to data encryption. Encrypted data includes initial changes and another nine rounds of encryption transformation, in which the first nine rounds of transformation mainly includes byte replacement, line transformation, faithfully transform and round keys plus, final round transformation mainly includes byte replacement, variable change and round keys plus, and then the system can complete the data encryption process through multiple rounds of transformation, including the use of C language code are as follows [12]:

```
void aesEncrypt
( unsigned char * cache,
unsigned char * chainBlock )
{
XORBytes(cache, chainBlock, BLOCKSIZE );
Cipher(cache, expandedKey );
CopyBytes( chainBlock, cache, BLOCKSIZE );
}
```

Data decryption process is the initial transformation and the ten round of the inverter. The first is round key transformation, and then the first nine rounds of the iteration goes through the right shift, reverse byte replacement, round key plus and reverse column mixed transform, the final round of the transformation goes through the right shift, reverse byte replacement and round key plus transformation, to complete the entire data decryption process, in which *C* language code is as follows [13]:

```
void aesDecrypt(
unsigned char * cache,
unsigned char * chainBlock )
{
unsigned char temp[ BLOCKSIZE ];
CopyBytes( temp, cache, BLOCKSIZE );
InvCipher(cache, expandedKey );
XORBytes(cache, chainBlock, BLOCKSIZE );
CopyBytes( chainBlock, temp, BLOCKSIZE );
}
```

In order to verify the validity and reliability of the system, the system has been tested the encryption system，including data transmission, encryption effect, decryption accuracy, system stability and operation speed and other aspects, in which test results are obtained as shown in Table 3.

Table 2. The test results of the encryption system

Design requirements	Test values (%)
Sending and receiving data integrity	99.28
Data encryption chaotic ambiguity	99.87
System running stability	98.25
System decryption accuracy	99.52
Effective computation ratio	95.23

Table 2 shows the test results of the encryption system, the results can be seen that sending and receiving data integrity, encryption chaos fuzzy degree and system decryption accuracy all achieve more than 99% when the encryption system carries out in the data transmission, and the system stability the effective calculation proportion are higher than 95%, and the accuracy and stability of the system are also higher.

Summary

Using hardware encryption protocol and algorithm, single chip microcomputer, FPGA and El interface, and 63 bit Gold code, this paper designs a new encryption and decryption’s full duplex communication network data encryption system. In order to verify the validity and reliability of the

system, the system were tested, through the test we find that the system can effectively use the network transmission data plaintext to carry on encryption and decryption, in which the sending and receiving data integrity, encryption chaos fuzzy degree and decryption system accuracy are more than 99%, the stability of the system and the proportion of available operations are more than 95%, the accuracy and stability of the system are higher, the system protection is also better.

References

[1] S.G. Yan, H. Wu, S.X. Xue. Design and implementation of ethernet data transmission system based on W5300. Electronic design engineering, 2014, 13(9): 92-94.

[2] M.X. Yao. Research and implementation of encryption algorithm in network information security. Computer knowledge and technology, 2011,12 (28): 25-29.

[3] L.S. Liu. Discussion on the encryption algorithm based on RSA. Computer knowledge and technology, 2014, 3 (21): 20-23.

[4] Y. Liu. Research on enterprise private cloud platform construction technology. Computer time, 2014(6): 38-41.

[5] Q.Y. Ou, K. Zhao. Cloud software platform in the application of multimedia classroom. Chinese technology information, 2014(16): 242-243.

[6] Z. Lu. Design of embedded media player based on STM32F103VCT. Journal of Hunan Industrial Vocational and technical college, 2014, 18 (5): 34-39.

[7] Q. Pan, C.X. Pei. High IPv6 network traffic sampling measurement method based on information entropy theory. Journal of Jilin University, 2013, 39 (5): 1339-1342.

[8] K. Deng, Y.W. Zhang. An improved S/KEY authentication algorithm. Network security technology and applications, 2013 (11): 91-92.

[9] H.F. Li, J. Zhou, J. Fan. Large multicast key management system based on agent. Hefei Industrial University Journal, 2013, 29 (8): 988-991.

[10] R. Gao, C.Y. Wang. Research on smart home gateway based on embedded system. Technology venture, 2013, 22 (4): 147-149.

[11] N. Luan. Several single-chip system encryption methods. Applied science, 2014, 11(2): 110-113.

[12] C.Y. Wu. AES security and its impact research. Academic research, 2013, 24(2): 140-142.

[13] Wang B.Y., Liu S., W. Zhang, L. Zhu. Image acquisition and transmission system based on hardware protocol stack W5100. Electronic technology applications, 2013, 27 (2): 92-96.