ISSN: 2710-0588 DOI: 10.29556/FSE.202107_1(4).0015

Research on Network Encryption Technology and Related Algorithms

Wenhua Zhang[1,*], Youchan Zhu[1] and Jinlei Qin[1]

[1]School of Control and Computer North China Electric Power University, Engineering Research Center, Ministry of Education, Complex Energy System Intelligent Computing, Baoding 071003, Hebei Province, China.

*Corresponding author Email: ncepuzwh@163.com

Abstract

In order to ensure the security performance of computer network information communication, a credible environment must be provided. Once a computer has a network failure, it is easily attacked by hackers, and it is difficult to effectively ensure the security of data and information. The core method is encryption, and cryptographic algorithms are the basis for network security encryption. The in-depth study of encryption technology and algorithms is of practical significance to our country's network information security work. This article first analyzes the domestic and foreign network security threats, and after comparing the performance of data encryption technology and related algorithms in the communication process, the AES algorithm, which is fast and easy to implement, is selected for in-depth study, and in order to improve the efficiency of the algorithm, it explores The optimization method of AES algorithm.

Keywords

Network Information; End-to-end Encryption; AES Algorithm.

1. Introduction

With the advent of the Internet era and the widespread application of e-commerce, networks are interconnected and information exchanges across the globe. The Internet has penetrated into people’s daily lives. People have expanded from communication, emails, etc. to online medical care, online transportation, online learning, online shopping, etc. through the Internet, and the Internet has gradually penetrated into various industries such as medical care, transportation, education, and finance. China, and greatly promoted the development of these industries, so that all walks of life have better development prospects. Through the Internet, people's lives have generally become networked. While the Internet brings convenience to people, it also brings troubles. According to statistics in 2019, the number of Internet users worldwide reached 4.388 billion, while China has increased by 50.67 million in the past year, a growth rate of 6.7%. With the increase in the number of people using the Internet, network security issues have become increasingly obvious. The computer's network technology is very sensitive, coupled with the rampant of Trojan horses and virus programs, the user's sensitive information can be easily obtained during network data transmission. Therefore, protecting network information security has become a top priority [1].

2. Data encryption technology type

When transferring data from the source host to the destination host, it is vulnerable to attacks from attackers on different levels of data, thereby destroying the integrity and security of the data. When data information is transmitted on the network, it is often encapsulated by various layers of protocols, and the information of the destination node needs to be known through the header information, so the header information cannot be encrypted, which gives criminals an opportunity to take advantage. Intruders usually use illegal means to obtain the private information of customers transmitted on the network, which makes it difficult to ensure network security. Therefore, relevant departments must attach great importance to the hidden dangers of data and information in network transmission [2]. Although the network security technology we currently have is difficult to completely prevent computer viruses or hackers, we can still use certain data encryption methods to improve the level of network security and protect the confidentiality of user data.

2.1. Link encryption

The network is made up of countless nodes. We can think of it as connecting every two nodes together and finally conveying information to the destination. The link encryption technology encrypts the data transmitted on the link between every two nodes into incomprehensible ciphertext, thereby ensuring that the data information is not obtained. After the information is sent from the first sender, it will be encrypted until it reaches the next transmission node to decrypt it. After the decryption is successful, when entering the next link, another key is used to encrypt the information before transmission, and then decrypt to obtain the corresponding information. This goes over and over again, until the information is transmitted to the final destination node [2].

The encryption method used in this encryption technology is completely automatic in the network and does not require human manipulation, so the user is not aware of the internal process. Of course, this encryption method also has obvious shortcomings. The same encryption method needs to be selected in the entire network link, and although the data is encrypted before the information is sent from the initial node, it seems that the entire process is completely transmitted in ciphertext, but in fact, the information is in the form of plaintext after decryption. The central processing unit of the computer through the node. In other words, the information at the switching center is easy to obtain. The cost of ensuring security at the node is relatively high, so it is not appropriate.

2.2. Node encryption

From the above analysis, it can be known that the link data encryption technology has the risk of information leakage at the node. Node encryption technology has made improvements to this leakage risk. Node encryption protects illegal information leakage, similar to the previous method, which is achieved by encrypting the link that transmits data information. At the intermediate node, the incoming data is encrypted first, and at the subsequent nodes, the message is decrypted and then encrypted with a different key, which can ensure that the data information is presented in the form of ciphertext during transmission, avoiding attacks The person recognizes the data information during transmission [3]. The plaintext data will not be exposed to the central processing unit of the computer, and is always protected in the encryption module.

Node encryption technology improves the problem of easy leakage of plaintext information in the link encryption at the switching center node, but we need to know the encryption method used by the data information transmitted by the previous node and the transmission path to the next node, and the relevant information and routing of the header are needed. The information is transmitted in plain text and cannot be encrypted. Therefore, an attacker can use this vulnerability to obtain network communication services by analyzing relevant information. The node encryption method does not achieve absolute confidentiality.

ISSN: 2710-0588 DOI: 10.29556/FSE.202107_1(4).0015

2.3. End-to-end encryption

Encryption of data transmission at the application layer is called end-to-end encryption. After the data is encrypted at the sender, it will not be decrypted until it reaches the receiver. Therefore, end-to-end encryption is an improvement on the above two encryption methods. Except for the header information, all the other messages are ciphertext and are propagated throughout the transmission process. While node encryption is used in intermediate nodes, each pair of nodes has its own key. When information is transmitted between nodes, it needs to be decrypted with the unique key of the previous pair of nodes, and then encrypted with its own key. It is ensured that the data is not in plain text when passing through the intermediate nodes, so that the data will not be illegally obtained [4].

Compared with the previous two encryption methods, this encryption method has great advantages. It can be implemented at the transport layer or application layer. The synchronization problem of other encryption technologies is also avoided in the end-to-end encryption system. Because the packets are independent of each other and the encryption is different, even if a packet is transmitted incorrectly, This encryption technology also has an independent transmission path during data transmission and will not interfere with the transmission of other data packets. In an end-to-end encrypted system, only the two parties communicating can obtain the transmitted data, and criminals and even service providers cannot monitor the communication information. Although this method is more reliable than the previous methods, the intermediate nodes have their own encryption methods and keys, and the management of a large number of keys is not convenient. In general, since the destination address is frequently used during the transmission of the message, the system will not encrypt the message related to the destination address, so it is easy for an attacker to analyze the communication service [5].

2.4. Advanced Encryption Standard

The end-to-end encryption technology can more effectively protect the data information in the communication process. The information related to the path does not need to be encrypted during the transmission process. Therefore, only the terminal device needs to be set as a device with encryption technology, and the required cost is lower. Therefore, the end-to-end encryption technology is relatively more widely used.

The realization of the algorithm is the core of the encryption technology. There are two commonly used encryption algorithms, symmetric encryption and asymmetric encryption algorithms. In end-to-end communication, data transmission efficiency is very high, and the speed advantage of symmetric encryption algorithm is very obvious. Therefore, the introduction here focuses on the Advanced Encryption Standard (AES) of the symmetric encryption algorithm.

The AES algorithm encryption process mainly includes generating round keys, key expansion, round key addition, round transformation and the last round transformation. The encryption process includes several conversion stages [6]. The encryption process starts from the round key addition stage. The conversion will be performed according to the key length and iteration (Nr times) respectively, and then nine rounds of iterative operations. Each round of iterative operations includes four rounds of transformation, and the sequence is byte substitution, Row shift, column confusion and round key addition, the last round of transformation omits the part of column confusion, and only includes three processes of byte substitution, row shift and round key addition [7].

The round transformation is the core of the entire encryption process. The four processes are as follows:

Byte conversion: (Sbox replacement) provides non-linearity and confusion, constructed by multiplicative inverse and affine transformation.

Row shift: (rotation) spread between columns, mainly for byte cyclic shift operation.

Column mixing: (linear combination) provides inter-byte diffusion, where each column vector is multiplied by a fixed matrix. Bytes will be treated as polynomials instead of numbers.

Round key plus transformation: (Each byte of the state key and rounding key is XORed with the rounding key byte) provides confusion.

```
Roundkey(CipherKey); //round key plus
  for (int i=0; i<9; i++)
 {
   Round-key[m][n]= Round-key[m][4i+n];//Key
   ByteSub(state);//byte transformation
   ShiftRow(state);//row shift
   MixColumn(state);//Column mixing
   Roundkey(CipherKey); //round key plus
  }
 //Perform the last round of transformation
```

The core is as above, this is the process of the AES encryption algorithm.

3. Application of Encryption Technology and Suggestions for Improvement

3.1. Application

Data encryption technology has a wide range of applications in e-commerce, database file security, etc. Information leakage will cause great security risks to computer network systems. The application of data encryption technology can effectively eliminate some potential risk factors in the network and reduce the security risk factor. For example, the application of data encryption technology can ensure the confidentiality of the information and the security of its property by verifying the identity of the customer. Generally speaking, in terms of information security protection, e-commerce network users usually choose a variety of data encryption methods to form a strong security protection network. At the same time, methods such as bundled registration or password protection are adopted to enhance the security of transaction data operation. As for the network database, the user's personal privacy information is stored in it. When building the network database, data encryption should be used to build a database with a higher level of security.

3.2. Suggestions for Improvement

From the above analysis, we can see that end-to-end encryption is more widely used and more secure. Therefore, in this chapter we propose an improved scheme for the AES algorithm. In the encryption and decryption process of AES, round conversion plays a central role. The improvement of the efficiency of the round conversion module has a huge impact on the efficiency of end-to-end encryption technology. In order to improve the efficiency of encryption, in the improved scheme, look-up tables are used as many times as possible to replace the tedious XOR calculation.

The process of round transformation is shown in Fig.1, where A is the initial matrix, E is the matrix after round transformation, and ai, j are the elements of the corresponding S box in the byte transformation A matrix. This is a table lookup operation, and we get B matrix; B matrix obtains C matrix after row shifting; step three is column mixing transformation, and finally round key plus transformation to obtain E.

$$b_{i,j} = S[a_{i,j}] \longrightarrow \begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix} = \begin{bmatrix} b_{0,j} \\ b_{1,j-1} \\ b_{2,j-2} \\ b_{3,j-3} \end{bmatrix} \longrightarrow \begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \oplus \begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix} \longrightarrow \begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}$$

Fig. 1 Wheel Transformation Process Diagram

Now combine these four steps to get:

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \bullet \begin{bmatrix} S[a_{0,j}] \\ S[a_{1,j-1}] \\ S[a_{2,j-2}] \\ S[a_{3,j-3}] \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}$$

Fig. 2 Merge graph

The change for each column can be transformed into:

$$e_j = \begin{pmatrix} 02 \\ 01 \\ 01 \\ 03 \end{pmatrix} S[a_{0,j}] \oplus \begin{pmatrix} 03 \\ 02 \\ 01 \\ 01 \end{pmatrix} S[a_{1,j}] \oplus \begin{pmatrix} 01 \\ 03 \\ 02 \\ 01 \end{pmatrix} \mathrm{S}[a_{2,j}] \oplus k_{0,j} \oplus k_{1,j} \oplus k_{2,j} \oplus k_{3,j} \tag{1}$$

The test results of the improved algorithm are as follows:

Table 1. Test Results

128bit	Before Improvement (MB/s)	After Improvement (MB/s)
First Speed	1.56	2.52
Second Speed	1.45	2.47
Average Speed	1.505	2.495

It can be seen that the encryption speed has been significantly improved.

In the improved method, the original four-step operation is changed to each column can directly look up the table for XOR, that is to say, the four operations that must be performed for each column are combined into a single look-up method. Each column in a round reduces the number of XORs, which can improve the operation efficiency of the round conversion [8]. This improved method can theoretically increase the speed of encryption and decryption, thereby increasing the efficiency of end-to-end communication.

4. Summary

Security is one of the most important problems in today's information age, and the gradual maturity and improvement of encryption technology has increasingly become an excellent solution for Internet security. This paper studies the security of computer networks from both theoretical and technical aspects, and compares and analyzes the performance of encryption technology, link encryption technology, node encryption technology, and end-to-end encryption technology that can be adopted. At the same time, it has an in-depth understanding of the relevant performance. Algorithm (AES), summarizes and analyzes the optimization method of the algorithm in order to improve the speed and efficiency. However, improvements need to be made in the following two directions: 1. The algorithm optimization for end-to-end encryption is not in place. The next step is to implement efficient simulation of the algorithm and optimize other parts of the algorithm; 2. End-to-end encryption the application research of the end encryption system needs to be further deepened to understand the efficient practical application products.

References

[1] Tatjana Welzer, Hannu Jaakkola, Bernhard Thalheim et al. Information and Information Security [J]. Frontiers in Artificial Intelligence and Applications, 2016,280.

[2] Shang W. Development and Trend Analysis of Computer Network Security in China [J]. Electronic Technology and Software Engineering, 2016,(1):196-197.

[3] Yongjun Tang. Talking about data encryption technology in computer network information security [J]. Technological Innovation and Productivity, 2019, 000(008):77-79.

[4] Nan Zheng, Ping Zhou . Application analysis of data encryption technology in computer network security [J]. Electronic Technology and Software Engineering, 2014(01):233-233.

[5] Lu Guo. Application of Data Encryption Technology in Computer Network Communication Security [J]. China High-Tech Enterprise, 2015, 000(012):52-53.

[6] Lang Rongling, Xia Yu, Dai Guanzhong. Research on Advanced Encryption Standard (AES) Algorithm [J]. Small Microcomputer System, 2003(05):905-908.

[7] Weilong Zhang. Application analysis of data encryption technology in computer network communication security [J]. Technological Innovation and Application, 2015(27):85-85.

[8] A. Amir Alkodri, B. Isnanto, Supardi, Anisah, S. Hadi Saputro and A. Dendi Rachmatsyah, "Use of the Advanced Encryption Standard Algorithm for Encryption Short Message Service on Real Count Applications," 2020 8th International Conference on Cyber and IT Service Management (CITSM), 2020, pp. 1-6, doi: 10.1109/CITSM50537.2020.9268868.

[9] Jian Zhang. Implementation and application design of AES algorithm in end-to-end communication encryption module [D]. Beijing University of Posts and Telecommunications, 2011.