Optimization of Data Encryption Technology in Computer Network Communication

Wenqing Yang

Library and Information Center, Jiangxi Industry Polytechnic College, Nanchang, China

*Corresponding author e-mail: yangwq@jxgzy.edu.cn

Abstract. In recent years, computer network communication system has been widely used in many industrial fields, which brings great convenience to people's daily life and work. Therefore, this paper describes and analyzes the current situation and characteristics of the application of data encryption technology in computer network communication security. This paper points out the common threats to the current network security, discusses the data encryption technology applied to the network communication security, including link encryption technology, node encryption technology and end-to-end encryption technology, and deeply analyzes the application of data encryption technology in the computer network communication security. The results show that the MSE value of data 1 is 42.453, that of data 2 is 87.324, and that of data 3 is 87.324674.

Keywords: Computer, Network Communication, Data Encryption

1. Introduction

With the rapid development of China's economy, the level of scientific and technological intelligence and information intelligence is deepening. This is the only way of scientific development, but the development of society has gradually put forward higher requirements and challenges for computer network information technology. In the era of big data, computer and Internet technology bring more convenience to people's life and work, but also leave a lot of security risks. We must solve the problems of information security and data theft when people use computers.

With the continuous progress of science and technology, many people have studied data encryption technology. For example, some domestic teams have studied the field of computer network communication. Compared with bio IBE scheme, this scheme reduces the cost. Based on the idea of Abe, this paper proposes a ciphertext policy hidden vector encryption (cphve) scheme which supports multi-user encryption and search operation at the same time. The scheme uses attribute based access policy to encrypt keywords. When the user's attributes conform to the policy, they can search for keywords. This paper proposes a protocol to distribute session key effectively in this environment to establish a secure channel. Suppose that the target network consists of many local trusted centers, and each center has many users connected to it. This scheme combines the concept of public key distribution and RSA encryption scheme as a basic mathematical tool, but eliminates the related
storage problems [1]. Some experts have studied the network transmission encryption algorithm of vector data, and proposed a new hybrid encryption technology, which can use the payload field of multi connection streams as the carrier. This technology is mainly divided into three stages. Firstly, the state of the network is analyzed. Then, the insertion point is selected according to the protocol, the hidden data is inserted into the packets injected into the network. In this paper, we evaluate the hybrid covert method and user datagram protocol (UDP) connection under two kinds of network load, and make a trade-off analysis between throughput and detectability. This paper discusses the important security features that make the wireless network more stable. It includes the important module of building WLAN security, secure data transmission, data encryption, wireless security type and other issues, making it a more stable platform to provide and build secure digital network. In this paper, we propose a method to ensure security as long as at least one party is trustworthy and the other party may be corrupt. Before the detailed OPNET simulation to evaluate the cost of the new method compared with the standard GSM, the pseudo collision probability is derived through analysis [2]. Some experts have studied data encryption and key management, and summarized the implementation of a secure data authentication model for wireless body area network, which uses a single private key to exchange in the configuration process. A secure WBAN system is proposed, but the security parameters need to be added in WBAN system. Existing systems must ensure the security of using limited resources. Trying to solve these security problems, considering the limitation of available power, bandwidth and other resources, helps to achieve a more secure and time-saving system in place, and provides an effective online health monitoring scheme for WBAN [3]. Although the research results of data encryption technology are quite abundant, there are still some shortcomings in the data encryption technology of computer network communication.

In order to study the optimization of data encryption technology in computer network communication, this paper finds the long-term and short-term storage network through the research of computer network communication and data encryption technology. The results show that this method is conducive to the optimization of data encryption technology in computer network communication.

2. Method

2.1. Computer Network Communication

The computer security network communication management module is an intermediate module connecting the trusted guarantee server and the trusted cloud computing server[4]. It is used to establish a reliable connection between cloud computing server and trusted Assurance server[5]. The trusted cloud computing server requests to join the cloud environment, and the communication operations such as establishing and disconnecting the connection for the trusted function request need to be realized through the security communication management module[6]. Similarly, all connected trusted cloud computing servers in the cloud environment are managed by the security communication management module, and all requests to the trusted security server are processed and responded by the module[7].

2.2. Data Encryption Technology

(1) Data encryption technology

Of course, there are many algorithms, and there is no final conclusion[8], and there is no strict standard implementation[9]. The algorithm has been developing continuously and is always optimized[10]. As long as it is convenient to use in a certain time and certain environment, it can be used. Encryption algorithm is a process of generating unreadable ciphertext through a series of operations and transformations between the original plaintext and the key. The key and algorithm are of great significance to the encryption process. The key is also an algorithm. It is formed by a specific algorithm. It is usually encapsulated in a class library in a program and can be called directly.

(2) Symmetric encryption algorithm

Controller layer encryption technology, also known as physical layer encryption technology, refers to
the encryption and decryption algorithm and key added to the controller, through hardware to achieve
data encryption and decryption, encryption speed and key management costs are very small, file
system layer encryption is the same, is a transparent encryption and decryption technology. But the
controller layer encryption uses the same key to encrypt all the data stored in the FLA device. This is a
comprehensive encryption method, encryption particles are too large[11].

(3) The importance of data encryption
The best of data security is to prevent data leakage through file encryption. Before transmission, the
data is encrypted, converted into ciphertext, and then transmitted. Even if it is intercepted or copied in
the process of transmission, the data can not get the correct information. Encryption method:
encryption data. However, the encrypted data is easy to lose its availability and business attributes,
which is difficult to develop and use. This method is only suitable for business scenarios with strong
demand for data protection, such as irreversible algorithms for group information statistical analysis,
such as data table mapping, algorithm mapping, etc., such as irreversible algorithms for random
interference and scene disorder, reversible algorithms for location conversion, etc., which can ensure
the reversibility of business attributes. As encryption technology is the most basic and core technical
means of network information, the effectiveness of encryption depends on the encryption algorithm.
Through the physical protection and encapsulation of encryption card, the whole encryption process is
transparent, which makes the security foundation of the whole system stable and firm. The hardware
platform chooses the trusted platform recognized by the industry, namely industrial control computer,
which effectively ensures the security of the hardware foundation of the system. The whole process of
encryption and key management is encapsulated on the security card whole system[12].

2.3. Long Term and Short Term Memory Network
The network structure of long-term and short-term memory fuses long-term and short-term memory
by adding gate control, which solves the problem that only short-term memory is generated due to
RNN gradient disappearance to a certain extent, as shown in equation (1):

\[ f_t = \sigma(W_f h_{t-1}, x_t + b_f) \]

Accuracy B is the ratio of the total number of correct text detection boxes to the total number of all
text detection boxes; recall rate is the ratio of the total number of correct text detection boxes to the
total number of real labeled text detection boxes; C measure can comprehensively evaluate accuracy B
and recall rate. Where h is the real annotation text detection box, W is the text detection box to be
predicted, which represents the best match real annotation text detection box, and represents the best
match actual text detection box, as shown in formula (2):

\[ \hat{C}_r = \tan(W_r [h_{t-1}, x_t + b_r]) \]

As the key element of encryption, the larger the key space is, the more times the algorithm is
exhausted, and the more difficult it is to crack. Therefore, the size and complexity of key space are
closely related to the security of vector geographic data encryption algorithm. If the length of the key
is set to R, the size of the key space * (3) is calculated as follows:

\[ P_{rec} = \frac{N_{rec}}{N_{total}} \]

(3)

The m after operation is related to the size of N. the larger the total number of data n is, the larger
the range of key value is. The key space of integer key is (4):

\[ K_m = N \]

(4)
3.1. Extraction of Experimental Objects
In order to improve the security of scrambling, group the sequence if the whole sequence is cracked. 
Different groups have different scrambling keys. The length of packets is closely related to the 
efficiency of scrambling. Different packet length on the efficiency of scrambling algorithm, 
experiments are carried out on the sequences with N length, and the sequences are divided into 1-N 
groups. After grouping, each group is simply scrambled in the group, and the time required for the 
operation of the whole sequence under different packet lengths is analyzed. No matter how long the 
package is, the length of the sequence generated by the 3D sequence is the total length of the data. 
Therefore, the generation and processing time of scrambling key are not included in the calculation of 
sequence encryption efficiency.

3.2. Experimental Analysis
After the network equipment receives the message, the processing flow is: first, restore the message 
content to the format according to the code, then analyze the message, analyze the syntax correctness, 
and verify the version and authentication information. If the syntax is correct and the validation is 
passed, the valid data will be further separated and displayed to the administrator. If necessary, 
according to the data corresponding operation, and return the reply information. After the failure of 
parsing or verifying the validity of the packet, the parsing module returns the captured packet, reports 
the exception to the management side, and discards the received message. A unique integer set by a 
network device for each packet, by which different instructions can be distinguished. Because in fact, 
the request is handled by the underlying program. When the response packet arrives, the program 
should compare the request number in the packet with that in the previous packet. The request number 
is also used to identify duplicate messages. In order to make up for the defects of the protocol and 
ensure the security of the network management system, a new security mechanism is introduced. 
Asymmetric encryption algorithm, because of its good security characteristics, can solve the problems 
of packet information being easily stolen, tampered and simple authentication mechanism, and become 
a better choice to make up for security defects.

4. Discussion

4.1. Encryption Effect
In order to quantify the security of encryption, the point set before and after encryption can be used to 
evaluate the security of encryption. MSE is a measure of the difference between the two. The MSE, 
encryption effect, as shown in Table 1.

| data   | MSE     |
|--------|---------|
| Data 1 | 42.453  |
| Data 2 | 87.324  |
| Data 3 | 124.674 |

It can be seen from the above that the MSE value of data 1 is 42.453, the MSE value of data 2 is 
87.324, and the MSE value of data 3 is 124.674. The results are shown in Figure 1.
Through the MSE value of the data before and after encryption, we can see that the data before and after encryption has a great degree of difference, the interference to the data is great, the encryption effect is very good, and the availability of the data is damaged.

4.2. Encryption Efficiency
On the premise of ensuring security, the pursuit of algorithm efficiency is a problem that cannot be ignored. In order to verify the effectiveness of the algorithm, the above four kinds of data are encrypted and decrypted respectively. At the same time, in order to compare the efficiency of the algorithm with the classical symmetric classical simulated in MATLAB, and the above data is encrypted and decrypted with AES algorithm, as shown in Table 2.

| data  | point  | size  | Encryption time (s) |
|-------|--------|-------|---------------------|
| Data A| 532.34 | 36KB  | 1.42                |
| Data B| 656.43 | 38KB  | 5.92                |
| Data C| 678.42 | 74KB  | 2.84                |
| Data D| 721.43 | 94KB  | 3.73                |

As can be seen from the above, the number of data A is 532.34, the size is 36KB, and the encryption time is 1.42s; the number of data B is 656.43, the size is 38KB, and the encryption time is 5.92s; the number of data C is 678.42, the size is 74KB, and the encryption time is 2.84s; the number of data D is 721.43, the size is 94kb, and the encryption time is 3.73s. The results are shown in Figure 2.

Figure 1. Encryption security experiment

Figure 2. Data encryption algorithm based on step-by-step encryption
It can be seen from the above that with the increase of the number of points, the time required for data encryption and decryption is correspondingly longer, but the overall efficiency requirements are met.

5. Conclusion
In recent years, information communication technology and Internet technology have developed rapidly. The computer network communication system has been widely used in various fields, which brings great convenience to people's daily life and study. A series of security issues are more and more concerned by people. This paper describes the application of data encryption technology in the security of computer network communication. Combined with the current application situation, the paper discusses its existing application technology and analyzes a new application technology with higher performance. This paper introduces the data encryption technology of computer network communication and the application of data encryption technology in network communication, aiming to provide some ways healthy and orderly network communication.

References
[1] Lina, Gong, Li, et al. The Application of Data Encryption Technology in Computer Network Communication Security.[J]. AIP Conference Proceedings, 2017, 1834(1):1-5.
[2] Fan A , Wang Q , Debnath J . A high precision data encryption algorithm in wireless network mobile communication[J]. Discrete & Continuous Dynamical Systems, 2019, 12(4&5):1327-1340.
[3] Kiarie L K , Langat P K , Muriithi C M . Application of Spritz Encryption in Smart Meters to Protect Consumer Data[J]. Journal of Computer Networks and Communications, 2019, 2019(3):1-10.
[4] Vidal, José R, Pla, Vicent, Guijarro, Luis., Flexible Dynamic Spectrum Allocation in Cognitive Radio Networks Based on Game-Theoretical Mechanism Design[J]. Lecture Notes in Computer Science, 2017, 6641(11):164-177.
[5] Li, Xirong. Multimedia Systems (accepted) (will be inserted by the editor) Tag Relevance Fusion for Social Image Retrieval[J]. Multimedia Systems, 2017, 23(1):29-40.
[6] Groza B , Murvay S , Herrewege A V , et al. LiBrA-CAN: Lightweight Broadcast Authentication for Controller Area Networks[J]. ACM Transactions on Embedded Computing Systems, 2017, 16(3):1-28.
[7] Vyas B , Vajpayee A . Local Data Security Through Encryption[J]. International Journal of Emerging Trends & Technology in Computer Science, 2017, 47(2):137-141.
[8] Tang X , Tan L , Hussain A , et al. Three-dimensional Voronoi Diagram-based Self-deployment Algorithm in IoT Sensor Networks[J]. Annales des Telecommunications, 2019, 74(7-8):517-529.
[9] Kumar S , Yadav S , Kumar D . Secured Communication using Data Dictionary through Triple DES[J]. International Journal of Computer Applications, 2017, 166(3):40-44.
[10] Khalil M I . Medical Image Steganography: Study of Medical Image Quality Degradation when Embedding Data in the Frequency Domain[J]. International Journal of Computer Network and Information Security, 2017, 9(2):22-28.
[11] Bernardini C , Marchal S , Asghar M R , et al. PrivICN: Privacy-preserving content retrieval in information-centric networking[J]. Computer Networks, 2019, 149(FEB.11):13-28.
[12] Tiwari B , Tiwari V , Das K C , et al. [Lecture Notes in Networks and Systems] Proceedings of International Conference on Recent Advancement on Computer and Communication Volume 34 || Reversible Data Hiding by Utilizing AES Encryption and LZW Compression[J]. 2018, 10.1007/978-981-10-8198-9(Chapter 8):73-81.