Analysis on the Security Enhancement Model of Communication System Based on Chaotic Encryption and Analytic Hierarchy Process

Qianfei Huang

Abstract

In this paper, we conduct research on the security enhancement model of communication system based on the chaotic encryption and analytic hierarchy process. The communication of the information network is completed by the communication protocol. The communication protocol can be divided into application layer, transport layer, network layer, link layer and physical layer. By using the communication protocol, the security control of the network communication can meet the needs of the information network security communication. This paper integrates the chaos system to further implement the robust system architecture. The algorithm of this paper tries to make the maximum value of the above three parameters in each iteration step by step and the output feedback to dynamically change these parameters. Compared with other algorithms, our method can adopt more related theories to perform the better result.

Keywords: Security Enhancement; Communication System; Chaotic Encryption; Analytic Hierarchy Process

Introduction

Along with the widespread application of computer network, the security of the communication data became a noticeable issue. Some data security transport protocols such as TLS, IPSec, etc., had been widely deployed and gone through the examination of practice, provides the secrecy, integrity and the authentication for communication data. The communication of the information network is completed by the communication protocol. The communication protocol can be divided into application layer, transport layer, network layer, link layer and physical layer. By using the communication protocol, the security control of the network communication can meet the needs of the information network security communication, and guarantee the confidentiality, integrity and systematic availability of the information transmission. Based on the theoretical review, we can summarize the transaction security agreement as the following aspects.

- The agreement design idea of MSEC work team separates the group key management and data security that only solves the problem in group key management.
- Based on the client/server architecture, TLS and DTLS provide security functions such as the authentication, key negotiation, key update, encryption, integrity protection, and anti-replay. The TLS and DTLS protocols do not have to change the system core beneath
the transport layer, and applications can easily establish secure connections by calling their standard APIs while making them the most widely deployed.

- MSEC protocol group uses group key management protocol and some data security protocol separately. Each group key management protocol needs to be operated in the form of guard process or the application program.

- Looking from data security, the ESP and AH that these two agreements because the MSEC agreement race currently mainly supports realize on the IP level that needs to operate in the essence of operating system. This realization mode besides cannot provide the standard data security API transfer connection to make the portability of program bad will also affect the application may the deployment, system function realization to ESP and AH is not possibly same because of the different operating systems.

The use of chaos to secure communication can be roughly divided into 3 categories: 1) the direct use of chaos to secure communication; 2) using synchronization of chaos for secure communications; 3) chaotic digital coding of asynchronous communication. In the following sections, we will focus on the second application form. Before the systematic analysis, in the figure one, we firstly show the basic architecture of the communication system.

![Figure 1. The General Architecture of the Communication System.](image)

**The Proposed Methodology**

**The Chaotic Encryption and Analysis.** In order to overcome the change of the chaotic sequence characteristics is caused by the computer precision issue, and this article uses the space and time two-dimensional chaotic system model to have the two-dimensional chaos pseudo-random sequence, compared with the one-dimensional sequence as improved the security of algorithm. Simultaneously uses parameter stochastic variable thought the two-dimensional chaotic sequence to encrypt through the logical regression equation in the definite orders. In the formula 1~2, we define the projections, respectively with the systematic modelling implementation.

\[
x_{n+1} = 4x_n (1 - x_n)
\]

\[
x_{n+1} = \cos(3 \arccos x_n)
\]

When the chaotic sequence is stable in the accordance with certain time interval and the lattice distance corresponding to the formation of the two-dimensional chaotic real chaos sequence after the final, on real sequences of binarization using symbolic function method, as the binarization method, the most commonly used method is the sign function method which is defined below.

\[
x_n^i \text{(binary)} = \text{sgn}\left\{x_n^i - E\left(x_n^i\right)\right\}
\]
Extracts some grid point the real value sequence to draw its density distribution map in the Matlab environment willfully, as can be seen, the density distribution of this sequence value is asymmetrical about E. With real value sequence binaryzation that this method will have, in the two value sequences of obtaining 0,1 integers are not balanced, then affects the random property of sequence. For this core drawback, we revise the original formula into the equation 4.

$$x_n^i \text{ (binary)' } = \text{sgn}\{x_n^i - E\{x_n^i\}\} + \text{sgn}\{x_n^i - +E\{x_n^i\}\}$$ (4)

Here, we need to integrate the DE for the systematic implementation. The data encryption standard is a block password of use key encryption, in the 1976 by the National Bureau of Standards of federal government of the United States was determined for the Federal Information Processing Standard, internationally widely spreads afterward. It based on using the symmetrical algorithms of 56 keys, this algorithm, because contains some secret design elements, relatively short key length as well as was suspected contains the back door of US national security Bureau, but has the dispute in the beginning, therefore DES by intensely the academism-type examination, and promoted the block password and development of cryptanalysis modern by this. Considering the characteristics of the key, we can then summarize the features as the follows.

- **Data packet.** Reads the image data with Matlab, the data that will then obtain carries on 64 bits definite orders grouping, after initial permutation is then divided various is 32 bits two parts.
- **Generating key.** Select the Lorenz initial value of the chaotic system, chaotic sequence is generated by the value of four order Runge-Kutte integral method, 56 bits of data as the initial key replacement operations on initial key, then the 56 bit replacement into each of two 28 bits.
- **Decryption.** AES encryption and decryption algorithm using the same algorithm, but the use of sub-key in the reverse order, so the decryption process only sub-key in the reverse order and then, we can get the original signal.

Carries on for the first time the initial permutation, repeat and grouping according to the DES algorithm to the data, then inserts in 16 rounds iterations by the chaotic sequence of Lorenz equation production as the sub-key, finally carries on the counter initial permutation, encrypted scrambled text. In the figure 2, we show the chaotic encryption pattern as reference.
The Signal Analytic Hierarchy Pattern. The analytic hierarchy process is Saaty determines the nature in one that the 1970s proposed with, analysis method of system, hierarchization that the quota unified. It people's thinking process mathematization to complicated system that subjective judgment qualitative analysis quantifying focusing on human, difference numerical between evaluation factors, and thus determines various evaluation factors the weight. This method can deal with the traditional minimization method unsolvable issue, is applicable to the fuzzy comprehensive assessment system specially. The main idea of AHP is through the relevant factors analysis of complex systems and their relationship, simplify the ordered hierarchical structure. These elements merge into different levels, establish judgment matrix in each layer, the relative weight of the layer elements, and finally calculate the multi factors combination weights for the overall goal provide the basis for decision-making and the selection. The steps of AHP can be then summarized as the follows.

- Classifies the factors involved in the problem, and then constructs a hierarchical model of the interconnections among the factors. Generally, the factors can be divided into three categories. (1) Criterion class. This is a measure of whether the goal can be achieved. (2) Measure class. Refers to realizing the plan, method, method goal. (3) Target class. This is the object to be evaluated. From the goal to the criterion and to the measure immediate influence relations arrangements among various factors in the different levels, then constitutes a level structure drawing from top to bottom.

- Step by step a paired comparison, some are inverse squares. Pairwise comparison is a method of determining the order of merit of these factors in a number of ways by taking into account a number of factors by making a pairwise comparison of all possible combinations.

This article used the AHP method to analyze to the uniformity of judgment matrix, obtained the judgment matrix the uniformity to have the following rule: Namely with one does to compare by the absolute value of determinants value its matrix corresponds, if smaller than one explained that the uniformity of this matrix is good, when specially the determinants value is the basic explained that this judgment matrix has the complete uniformity; If the absolute value is bigger than 1 to analyze the element of matrix again, if satisfies the order uniformity to explain
that the matrix uniformity can accept, otherwise needs to adjust. In the figure three, we show the architecture.

![Diagram](image.png)

Figure 3. The Analytic Hierarchy Pattern Demonstration.

**The Communication System Stability Analysis.** If duplicates an autonomous chaotic system the suitable subsystem, so long as the Lyapunov exponent of subsystem to lose, then the chaos signal of response system is quick and in drive system corresponding chaos signal synchronization. The multi-vibrator is a self-excited oscillator electric circuit and this electric circuit does not need the external connection trigger pip to have the square pulse or the square-wave of certain frequency and peak-to-peak value after the power-on. Because in the square pulse includes the rich higher harmonic, thus is called for the multi-vibrator. To analyze the stability of the system, we should firstly model the corresponding system as the formula 5.

\[
\begin{align*}
\tilde{x} &= f(x) \\
y &= Cx
\end{align*}
\] (5)

**The Communications Security Enhancement Mode.** The confidentiality of the communication process between nodes is mainly achieved through the transmission of encrypted information. In the implementation of inter-node communication information encryption transmission, usually can use asymmetric encryption technology to achieve the information encryption, such as the RSA public key encryption technology; also can use symmetric encryption technology, such as RC5, DES and so on. In view of the inherent open nature of the computer communication network, it is necessary to take effective security measures to ensure the security of computer communication network. Under this condition, we should consider the listed aspect to achieve the systematic optimal solution.
• The function of network encryption technology is to prevent public or privatization information from being intercepted and stolen in the network and is the network security core. With the network encryption technology, it carries on the encryption and seal to the IP package that in public network transmits realizes secrecy and integrity of data transfer.

• The network planning mainly solves or alleviates some security problems in the networking scheme, including security plane division, border consolidation and protection at different security plane boundaries, IP address planning, different networks and services, As well as the necessary expansion and so on. Secure network planning mitigates or eliminates the general proliferation of the threats and the stress that large flows place on the system and makes the network easier to manage.

• Firewall protection intranet not by the attack of the exterior network, but it to intranet the monitoring of some illegal activities is imperfect as IDS is the reasonable supplement of firewall, it positive has provided on own initiative and harms the real-time protection of the operation to the internal attack and exterior attack receives to harm beforehand interception and response invasion in the network system that improves the information security.

Conclusion

In this paper, we conduct research on the security enhancement model of the communication system based on chaotic encryption and the analytic hierarchy process. Because of the chaos mapping has the ergodicity, unpredictability and to the characteristics that the parameter and starting value sensitivity and traditional cryptology are similar, it suits for the basic password design. The chaotic cryptosystem usually uses the initial value, system parameter and iteration number of the chaotic map to encrypt/decrypt the chaotic map. The algorithm of this paper tries to make the maximum value of the above three parameters in each iteration step by step and the output feedback to dynamically change these parameters. The designed system is novel and effective, in the future, we will conduct ore theoretical analysis to test the further effectiveness of the methodology.

References


