Research on Information Encryption Algorithm under the Power Network Communication Security Model

ChunYan Yang1*, Ying Ling1, Xin Li1

1 Electric Power Research Institute of Guangxi Power Grid Co., Ltd, Guangxi, Nanning, China, 530023

*Corresponding author e-mail: yangchunyan1@eprigx.org

Abstract. With the continuous development of current high-tech, network communication is quickly popularized in power automation monitoring systems, and colleagues have also brought many hidden dangers in communication security. This paper proposes a model that adapts to the security of power network communication. Based on the information encryption algorithm, this model can fully guarantee the security of both ends of the data transmission and can be applied to other network communication modes. Based on the power network communication security model, this article can use high-strength information encryption algorithms to encrypt data in the network to prevent the data transmitted in the network from being stolen or modified. The power network communication security model studied in this article mainly includes information encryption and decryption algorithms, client environment, and an SSL-based information encryption transmission protocol. Through analysis, it can be understood that the encryption and decryption algorithm is to perform MD5 transformation on key data and key strings, and the other is to use DES as the encryption algorithm before transmission. The experimental research results show that in the construction of power network communication, the power communication network is one of the most basic facilities in the development of the power grid. It is necessary to ensure the safety and economic operation of the power grid, and to improve the information level of the power grid enterprises and the network security protection system.

Keywords: Power Network Communication, Communication Security Model, Information Encryption Algorithm, Power Communication System

1. Introduction

The power network communication security system is the foundation of the development of various industries in our country, and the information system is a branch of the power network communication security system, which is mainly responsible for the transmission of various data information [1]. Compared with the previous traditional models, the grid security model has played an important role in operational efficiency, management and control [2]. In order to ensure the stable transmission of
information systems, enterprises should formulate corresponding security index systems. The communication security of the power grid ultimately depends on the operation and control of the technical personnel. If the personnel's professional skills are insufficient, it will also cause various security risks. Regularly reviewing data information is helpful to the security management of information encryption [3]. Audit work needs to provide correct decision-making guidance and safety technology for managers under the scientific guidance of power enterprise managers [4].

Information encryption algorithms Typical information encryption algorithms include Data Encryption Standard (DES) algorithm and Public Key Algorithm (RSA). The following two information encryption algorithms are briefly summarized. Data Encryption Standard (DES) algorithm [5]. The encryption algorithm is also called an asymmetric key algorithm. It uses two pairs of keys, a public key and a private key. The user needs to ensure the security of the private key so that the public key can be released. The relationship between the public key and the private key is very close, because the public key can only be used to decrypt information, and vice versa [6]. Therefore, since the online key distribution algorithm is greatly simplified, no key management protocol is required. Public key encryption algorithms mainly include RSA, fertzza, elgama, etc. [7].

With the continuous development of grid communication, the security of data transmission will also affect the construction, development and operation of the smart grid communication security system to occupy a very important position [8]. As a result, the data transmission security of the smart grid communication security system has attracted great attention worldwide. With the development of information encryption algorithms, the current smart grid communication security system adopts multiple communication methods to coexist and all messages adopt a communication method based on information encryption algorithm transmission, making it more and more risky of various network attacks. The smaller [9]. In addition, the installation locations of various power distribution terminals of the smart grid communication security system are relatively scattered, and the operating environment is relatively dangerous. There are certain security risks in many areas when connecting to the power information network. At present, there are unresolved problems in the research on data security of smart grid. Therefore, in order to ensure the safe transmission of information in the smart grid system, this paper adopts efficient and reliable encryption measures to protect data [10].

2. Establishment and analysis of information encryption algorithm

2.1. Menezes-Vanstone algorithm

The Menezes-Vanstone algorithm is actually an implementation process based on the EIGamal algorithm on the elliptic curve. The difference from the original EIGamal is that one is implemented on the cyclic subgroup of the elliptic curve and the other is implemented on the finite field.

The Menezes-Vanstone algorithm is used to transform between encryption and decryption on a finite field. According to it, it can be concluded that the plain ciphertext space is:

$$Z_p^* \times Z_p^*$$  (1)

And its ciphertext space is:

$$E \times Z_p^* \times Z_p^*$$  (2)

Combining formula (1) and formula (2), it can be seen that the encryption algorithm is no longer a continuous finite domain space, but a set of discontinuous two-dimensional spaces E in a finite domain space. The algorithm is described as follows:

First select a prime number P that is large enough. E is the elliptic curve of $Z_P$ on the finite field, which is any point on E, and when the order of a is large enough, it makes the claimed cyclic discrete logarithm is the most difficult:

Randomly select an integer D, you can get:

$$1 \leq D \leq \text{ord}(a)$$  (3)

Calculate $\beta=Da$, where $a\beta$ is a public encryption key and D is a secret decryption key

$X=(X1, \ X2)$ in the plaintext form, $Z_p^* \times Z_p^*$ in the space, which is the same as the traditional
encryption algorithm meaning, secretly chooses an integer $K$, such that:
\[ 1 \leq K \leq \text{ord}(a) - 1 \]  

The form of the ciphertext is $y=(y_0, y_1, y_2)$, and the ciphertext space is: $E \times \mathbb{Z}_p^* \times \mathbb{Z}_p^*$

Encryption process: $Y_0=K\alpha$, coordinates $(c_1, c_2)=K\beta$, $y_1=c_1x_1 \mod p$, $y_2=c_2x_2 \mod p$

Decryption process: $(c_1, c_2)=dy_0$, where:
\[ x = (y_1c_1^{-1} \mod p, y_2c_2^{-1} \mod p) \]  

From the information encryption algorithm described above, it is obvious that the encryption algorithm on the elliptic curve greatly accelerates its encryption and decryption speed.

2.2. EIGamal signature algorithm

The EIGamal signature algorithm and the EIGamal signature algorithm were introduced at the same time. It is also a solution based on discrete logarithms. The specific description of the algorithm is as follows:

Select a public key as parameter $K$, and a private key parameter as $e$, among which the largest public prime numbers $a, p$, calculate the transformation $H(m)$ of the message, where:

\[ k = a^e \mod p \]  

Perform signature transformation:
\[ S(H(m)) = (E_1, E_2), \text{Among } X = a^m \mod p \]  
\[ Y = (H(m) - eX)^{-1} \mod (p - 1) \]  

Perform signature verification: If the following formula is made to be valid, it can be regarded as a valid signature.

\[ K^X Y^X = a^{H(m)} \mod p \]  

Therefore, after $K, X, Y$ can be substituted accordingly, the resulting expression is as follows:

2.3. Comparative analysis of the above two algorithms

The RSA signature algorithm is based on its own algorithm as the technical standard. It has become a de facto standard after getting a considerable range of applications. Because the EIGamal signature algorithm was discovered relatively late, and its predecessor was the Rabin signature algorithm, EIGamal has already had many forms of correction before this.

At present, the application of RSA algorithm is wider than that of DSA algorithm. In addition to the earlier application of RSA algorithm, the main reason is that DSA is slow, has not undergone sufficient security and analysis, and has a small application area.

2.4. The Secret Key Problem in the Security Mode of Electric Power Network Communication

The key problem in the power network communication security mode usually refers to the transmission and storage of the key used when using a symmetric cryptosystem to encrypt data. The problem of key transmission refers to how the two parties in communication can safely transmit the key to the other party, while ensuring that they are not known or modified or forged by various attackers during the transmission process. Although asymmetric ciphers do not need to transmit the key, their encryption speed is slow and cannot be suitable for most occasions; on the surface, although the key can be transmitted safely and not exposed, the imposter attack (also called man-in-the-middle attack) of the active attacker is There is no way. The transmission problem of the key also causes the problem of key distribution and storage. Assuming that in a network composed of $N$ users, each group of users needs to have a different key to encrypt and decrypt information, so that in the network There are a total of $\sum_{i=1}^{n} (i-1)! \cdot (i-1)!$ keys that need to be stored, and they are usually to ensure data security.

3. Modeling method

3.1. Establishment of the power network communication security risk mod
The judgment of the power network communication security risk rating prediction model is a typical two-category model in the risk rating process. The probability can determine the storage risk level of the communication data according to whether the threshold is set.

$$\rho(Y = 1|X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n)}}$$  \hspace{1cm} (10)

The fitting effect of the rating model is expressed by the pseudo $R$-square statistic. It can be seen that:

$$\text{Cox}&\text{Snell} - R^2 = 1 - \frac{\ln(L_0)}{\ln(L)}$$  \hspace{1cm} (11)

The coverage ratio of the result is the actual rating sample, the correct rating proportion model is as follows:

$$\text{RESF} = \frac{TA}{TA + FA}$$  \hspace{1cm} (12)

The accuracy of the result is the actual rating sample, the correct rating proportion model is as follows:

$$\text{RESJ} = \frac{TA}{TA + FN}$$  \hspace{1cm} (13)

According to 30 synthesizable feature dimensions, in order to avoid information errors and omissions and increase the complexity of model calculation, it is necessary to expand feature selection to generate a relatively small and optimal feature set.

$$\text{WOE}_i = \ln\left(\frac{p_{yi}}{p_{yn}}\right)$$  \hspace{1cm} (14)

$$S = \sum (p_{yi} - p_{ni}) \cdot \text{WOE}_i$$  \hspace{1cm} (15)

The model describes the regression results between cloud data storage ratings and related indicators.

$$T_m(x): X \rightarrow \{-1, +1\}$$  \hspace{1cm} (16)

Second, calculate the classification error rate on this processor:

$$e_m = P(T_m(x_i) \neq y_i) = \sum_{i=1}^{N} w_{mi} \exp\left(-a_m y_i T_m(x_i)\right)$$  \hspace{1cm} (17)

Calculate the coefficient of $T_m(x)$:

$$a_m = \frac{1}{2} \log \frac{1 - e_m}{e_m}$$  \hspace{1cm} (18)

Update the probability distribution of the training data set:

$$D_{m+1} = (W_{m+1, 1}, \ldots, W_{m+1, i}, \ldots, W_{m+1, N})$$

$$w_{m+1, i} = \frac{w_m}{z_m} \exp\left(-a_m y_i T_m(x_i)\right), (i = 1, 2, \ldots, N)$$  \hspace{1cm} (19)

After completing the above steps, construct a linear combination of classifiers:

$$f(x) = \sum_{m=1}^{M} a_m T_m(x)$$  \hspace{1cm} (20)

The final data cloud processor obtained from the scientific research is:

$$T(x) = \text{sign}(f(x)) = \text{sign}\left[\sum_{m=1}^{M} a_m T_m(x)\right]$$  \hspace{1cm} (21)
4. Evaluation results and research

![Graph showing the measured change trend of information security model data based on information encryption algorithm.](image)

**Figure 1.** The measured change trend of information security model data based on information encryption algorithm

Figure 1 shows the measured change trend of the information security model data based on the information encryption algorithm. When other parameters remain unchanged, in the process of optimizing the power communication safety information system, changing the middle GBH715 height can flexibly adjust the fluctuations of the entire curve, especially when the safety performance deviation is large, the high-order loss coefficient is reflected, so the influence of high-order on the four-wave mixing effect can be ignored in the ultra-flat coefficient distribution; Therefore, it is necessary to design a power network information security model based on information encryption algorithms.

**Table 1.** Comparison of measured data of different types of information encryption algorithms

| Algorithm name       | Route trend 1 | Route trend 2 |
|----------------------|--------------|--------------|
| RSA signature algorithm | 121.33       | 23.15        |
| ElGamal              | 255.12       | 212          |
| Menezes-Vanstone     | 215.12       | 339          |
| Method prediction    | 205.37       | 212          |

The measurement data in Table 1 shows that this method is more accurate when the degree of the inscribed triangle is small. When the link distance increases to 227km, Menetes Vanstone can accurately estimate the scattering loss, the error of nb101 is only 3, but the error of the correlation angle measurement data has a much greater impact on the calculation result.
As shown in Figure 2, the actual application performance analysis of three different information encryption algorithms is to compare different actual effects. The three information encryption algorithms RSA, ElGamal and Menezes Vanstone were tested and analyzed. Elm, SVM and KNN use 22, 22 and 19 functions respectively. Figure 2 shows the performance analysis diagram of three different information encryption algorithms in practical applications.

5. Conclusion
With the current rapid development of industrialization in my country, problems such as power shortages during peak power consumption of smart grids have become more and more prominent. The occurrence of such problems has caused certain problems on the production efficiency of enterprises and the daily lives of ordinary residents. Adverse effects. Therefore, improving the management level of the power demand side of the smart grid and strengthening the research of related monitoring terminal equipment are effective measures to enable the efficient operation of my country's smart grid. The security model system uses the SSL information encryption protocol algorithm to ensure that the information communicated between the two parties is encrypted through the encryption algorithm. encryption. And confirm the identity of both parties through digital signature technology, which not only guarantees the security of information transmission, but also confirms that the information will not be maliciously attacked and forged. Project practice has proved that the modified model can be used in power communication and can be extended to a wider range of Network communication application system.

References
[1] Kong P Y . Cost Efficient Data Aggregation Point Placement With Interdependent Communication and Power Networks in Smart Grid[J]. Smart Grid, IEEE Transactions on, 2019, 10(1):74-83.
[2] Moussa B , Akaber P , Debbabi M , et al. Critical Links Identification for Selective Outages in Interdependent Power-Communication Networks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(2):472-483.
[3] Zhao D , Qin H , Song B , et al. A Reinforcement Learning Method for Joint Mode Selection and Power Adaptation in the V2V Communication Network in 5G[J]. IEEE Transactions on Cognitive Communications and Networking, 2020, 6(2):452-463.
[4] Kong P Y . Cost Efficient Data Aggregation Point Placement With Interdependent Communication and Power Networks in Smart Grid[J]. Smart Grid, IEEE Transactions on, 2019, 10(1):74-83.
[5] Zhang Z , Niu Y , Cao Z , et al. Security Sliding Mode Control of Interval Type-2 Fuzzy Systems Subject to Cyber Attacks: The Stochastic Communication Protocol Case[J]. IEEE Transactions on Fuzzy Systems, 2020, PP(99):1-1.
[6] Zhou C, Liao X, Wang Y, et al. Capacity and Security Analysis of Multi-mode Orbital Angular Momentum Communications[J]. IEEE Access, 2020, PP(99):1-1.

[7] Verma P K, El Rifai M, Chan K W C. [Signals and Communication Technology] Multi-photon Quantum Secure Communication || Preliminary Security Analysis of the Multi-stage Protocol[J]. 2019, 10.1007/978-981-10-8618-2(Chapter 7):119-130.

[8] Chai X, Zheng X, Gan Z, et al. An image encryption algorithm based on chaotic system and compressive sensing[J]. Signal Processing, 2018, 148(jul.):124-144.

[9] Qin Y, Wang Z, Wang H, et al. Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container[J]. Optics and Lasers in Engineering, 2018, 105(JUN.):118-124.

[10] Yang F, Mou J, Sun K, et al. Lossless image compression-encryption algorithm based on BP neural network and chaotic system[J]. Multimedia Tools and Applications, 2020, 79(1–2).