Research on Data Security Encryption Based on Extracting Evaluation Index from Multiple Angles

Pan Hu, Nan Hu, Chuanming Jiao, Fuliang Zhang and Ruiting Qu*
Information and Communication Branch, State Grid Liaoning Electric Power Co., LTD., shenyang, Liaoning, 110006, China
*Corresponding E-mail: caoguoqiang@sgepri.sgcc.com.cn

Abstract. In order to solve the problem of low accuracy of ciphertext analysis in traditional power system data encryption methods, this paper presents and designs a power system data encryption method based on multi-angle evaluation index. Firstly, the C/S architecture of security protection is established, and the information node of the management information database is supplemented with the multi-level management system. Then the 3DES encryption algorithm is introduced to balance the weights of the two factors according to the scaling assignment, to increase the data confidentiality, and the embedded terminal is used to assist decryption. The experimental results show that the decryption result of the design method has a high precision, which verifies the effectiveness of the design method in improving the precision of ciphertext.

1. Introduction
The development of network and communication technology has penetrated into every field of society, and mankind has already stepped into the information age formally[1-2]. The most outstanding characteristic of the information age is that it can make full use of the information and data resources. From the point of view of hardware, encrypted gateway is a common way of data encryption in power system, but encrypted gateway is only suitable for data transmission node in distribution network. In reference [3], a digital lightweight shape-preserving encryption method is proposed to realize symmetric encryption for specific data types, that is, the key can be encrypted and decrypted. However, this encryption method needs to issue digital certificates, which leads to low encryption efficiency and is not suitable for the current large distribution network. A real-time encryption method for wide-area measurement data based on Storm is proposed in reference [4], but the Storm framework in this method is difficult to resist the attack of data tampering, resulting in poor resistance. The traditional power system sampling encryption method after encrypted transmission, the accuracy of ciphertext analysis is low, so a power system data encryption method based on multi angle extraction evaluation index is designed.

2. Power System Data Security Encryption Method for Extracting Evaluation Indexes from Multiple Angles

2.1. Establish the safety protection system of power system
Using computer system to establish security protection C/S architecture, install local security agent on client side, adopt security agent server on server side, add security transport layer through protocol stack on both sides of communication, and ensure data security to a certain extent [5].
Based on the architecture of electric power information system, it is a multi-level security management system, which can be represented as a visual layered model [6]. This model is a non-peer communication protocol model for both sides of communication, including three planes with different functions. The agent management plane contains the management module of the logical database nuclear management station of all the agent stations, and mainly deals with the communication information between the security agent and the agent [7]; the mode management plane is used to distinguish the communication modes, including UDP/TCP, B/S, C/S and other different communication protocols; the security agent plane is used to realize the authentication, key management, data signature and other functions for users according to the choice of TCP/UDP encryption mode in the mode management plane. For the security agent in the model, it needs to be managed, in essence, it is to manage the TCP/IP network and terminal devices. The service primitive of security agent management can borrow the service primitive of SNMP [8].

Through the establishment of power system security protection system, security agent is used to integrate many functions and achieve the management of security agent.

2.2. Encryption algorithm introduced

Encryption algorithm is essentially a function to provide authentication for power system data, to ensure the integrity, confidentiality and availability of information. This paper uses 3DES algorithm, which is generated after three polling on the basis of DES algorithm [9].

In the 3DES algorithm flow, DES uses shift, XOR, S box and other operations, plaintext through IP replacement, through several iterations, to achieve the sampling data encryption, the function can be expressed as follows:

\[
\begin{align*}
R_n &= L_{(n-1)} \otimes f\left(R_{(n-1)}, k_{(n-1)}\right) \\
L_n &= R_{(n-1)}
\end{align*}
\]

Where \(\otimes\) stands for XOR processing; \(f\) is a 32-bit output function with \(R_{(n-1)}\) as variable, including IP expansion permutation, S-box, etc.; \(k_{(n-1)}\) is a 48 bit key input to layer N. The performance of encryption algorithms requires high encryption strength, fast operation speed and low resource consumption, but the higher the algorithm complexity, the slower the operation speed, and the greater the resource consumption. Therefore, under fixed conditions, the importance of factors is determined by pairwise comparison, and the comparison judgment matrix is shown as follows:

\[
A = \begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1j} \\
a_{21} & a_{22} & \cdots & a_{2j} \\
\vdots & \vdots & \ddots & \vdots \\
a_{i1} & a_{i2} & \cdots & a_{ij}
\end{bmatrix}
\]

(2)

\(a_{ij}\) in the above matrix is the scale of two factors, and the explanation between the assignment and definition of the scale is shown in Table 1.

| Assignment of scale \(a_{ij}\) | Definition |
|---------------------|----------|
| 1 \(\frac{1}{a_{ji}}\) | Factor \(i\) is as important as factor \(j\) |
| 3 \(a_{ij}\) | Factor \(i\) and factor \(j\) are slightly important |
| 5 \(a_{ij}\) | Factor \(i\) and factor \(j\) are |
more important
7 Factor \( i \) and factor \( j \) are very important
9 Factor \( i \) and factor \( j \) are absolutely important

When the scale is assigned 2, 4, 6, or 8, it falls between the above criteria. Under the precondition of data confidentiality, the delay should be satisfied as far as possible and the consumption of resources should be reduced [10]. Where the business data requirements establish the business matrix as follows:

\[
A_0 = \begin{bmatrix}
1 & 3 & 3 \\
\frac{1}{3} & 1 & 5 \\
\frac{1}{5} & \frac{1}{3} & 1 \\
\end{bmatrix}
\] (3)

The expressions for weight vector \( W_0 \) and consistency check \( CR \) that can be obtained are:

\[
W_0 = \begin{bmatrix}
0.681 \\
0.225 \\
0.094
\end{bmatrix} \\
CR = 0.0042
\] (4)

When encrypting the sampled data of power system, the weight of the two factors is balanced by the assignment of the scale of the encryption algorithm, and the data confidentiality is increased.

2.3. Design encryption expansion card
The need for decryption of large volumes of data in power information systems cannot be met by separate encryption algorithms, and embedded terminal protection is required to assist in decryption. Embedded terminal protection is embedded in the terminal security encryption chip, the use of hardware encryption, with the network test to achieve authentication and data encryption.

Based on the original data acquisition and metering unit, the embedded terminal adds the encryption expansion card, which has a good effect on the large flow data load requiring encryption and ensuring the reliability and real-time of data communication. The embedded cipher computing chip in the cipher expansion card of the data sampling terminal can be responsible for communication authentication, encryption, decryption and other information security work. Figure 1 is the design of the hardware encryption expansion card of the power system sampling terminal:

![Encryption Expansion Card](image)

Figure 1 Design of Encryption Expansion Card for Data Acquisition Terminal of Power System

In Figure 1 above, the CPU is SamSung (SC4510B), the main frequency is 50MHz, the SDRAM model is HY57V641620, the specification is 1×4M×8, the dual-port RAM is CYPress (CY7C026), the specification is 16k×16, the ROM is ATMFL (AT29C010A), and the * 2 means composed of two
pieces, the specification is 128k×16. The processor will transfer the processed data to the security encryption expansion card, which stores the encryption algorithm, and choose different algorithms to encrypt the data according to the actual needs. After processing, the data will be transmitted to the security access platform, and finally sent to the company intranet to improve the accuracy of data decryption.

2.4. Data Encryption under ECC-AES Combined Algorithm
Data encryption is aimed at perceptual data, can directly lead to data failure, and the attack process is faster. Therefore, ECC-AES is used to combine the parallel mode of the algorithm to further improve the speed of data encryption.

After matrix transformation, column obfuscation is performed on the plaintext after matrix transformation as follows:
① Suppose a data in the matrix is $x$;
② The result of $x \times 01$ is $x$ itself;
③ In $x \times 02$ operation, the binary of $x$ is shifted one unit to the left and 0 to the right. If the highest bit of $x$ is 1, it will be different again;
④ Operation $x \times 03$, the result is $x \times 02 + x$, and the calculation method is the same as above;
⑤ Complete the column confusion calculation in turn until the result of $x \times x$ is obtained.

At the receiving end, according to the reverse process of encryption and the corresponding authentication signature, the ciphertext is decrypted to ensure the security of data transmission in the distribution network. So far, the research of power system data encryption method based on multi angle extraction evaluation index is completed.

3. Analysis of experimental results

3.1. Build test environment
It is necessary to implement and test the method under the condition of supporting energy storage technology. The experimental parameters of power system data encryption method based on energy storage technology are as follows:

| Serial number | Project          | Parameter                      |
|---------------|------------------|--------------------------------|
| 1             | Hardware platform| QEMU virtual hardware platform |
| 2             | Operating system | Mac OS High Sierra             |
| 3             | Browser          | Internet Explorer 8 and above |
| 4             | Network bandwidth| 200Mbps                        |
| 5             | Physical machine | MacBook Air (MQDCH/A)          |

3.2. Experimental results and analysis
In the above experimental environment, the electrification test is carried out, and the process of data encryption and decryption is shown on the display screen. The results of this experiment intercept the results of the first six experiments of the two methods, as shown in Tables 3 and 4:

| Experimental serial number | Encrypted results | Decryption result |
|----------------------------|-------------------|-------------------|
|                            | Plain writing     | Ciphertext       | Plain writing     | Ciphertext       |
| 1                          | 16 1D 13          | 2D 23 SF         | 2D 23 SF         | 15 1D 13         |
| 2                          | 1A 16 C3          | 34 F5 6E         | 34 F5 6E         | 1A 16 C3         |
| 3                          | 12 AC 1F          | 1R S3 62         | 1R S3 62         | 12 AC 23         |
| 4                          | 1T 23 6P          | 19 W3 1F         | 19 W3 1F         | 1T 2C 6P         |
According to the test results in Tables 3 and 4, the results of plaintext and ciphertext are similar in the process of encrypting power system data using the traditional method and the method in this paper. In the process of decryption, the plaintext is changed into a series of ciphertext, the decryption result of the traditional method is biased, the decryption result of this method is lower, the decryption result of this method is higher, which proves the effectiveness of this method in improving the precision of ciphertext. The specific parsing accuracy is compared as shown in Figure 2:

![Figure 2 Analysis accuracy comparison results of different methods](image_url)

It can be seen from Figure 2 that after the experiment, the accuracy of the data encryption method based on energy storage technology in this paper is always above the standard value, and its accuracy is higher, but the accuracy of the traditional method is lower. The reason is that the security protection system is established in the process of power system data encryption, and the security transmission layer is added in the protocol stack of the two ends of communication.

4. Conclusions

With the rapid development of wind power generation, photovoltaic power generation and energy storage technology, the proportion of new energy in the future power system will be more and more. According to the different subjects and purposes of the evaluation, the multi-angle evaluation index system of the wind-photovoltaic combined power system is established. However, due to the limitation of individual ability and time, the evaluation index system established is still insufficient. With the development of technology, new safety problems will appear in the use of telecom information collection system. The safety protection construction should be advanced and forward-looking, and the corresponding safety protection strategy should be formulated in time for the new problems to ensure that the safety protection strategy can continuously and effectively play its role.
Acknowledgment
The study was supported by “State Grid Liaoning Electric Power Co., LTD. Science and Technology Project (Project No: 2020YF-73)".

References
[1] Babacan O, Abdulla A, Hanna R, et al. (2018) Unintended Effects of Residential Energy Storage on Emissions from the Electric Power System[J]. Environmental Science and Technology, 52(22):13600-13608.
[2] Itraj, Bombale, Patil, et al. (2020) Performance analysis of 802.11n-based cognitive wireless system with joint rate and power adaptation[J]. International Journal of Electronics, 107(11):1887-1911.
[3] Liu B T, Peng C G, Wu R X W, et al. (2019) Lightweight Format-Preserving Encryption Algorithm Oriented to Number[J]. Journal of Computer Research and Development, 56(7):1488-1497.
[4] ZHANG S M, SUN J, WANG B Y. (2016) Storm Based Real-time Data Encryption in Wide Area Measurement System of Smart Grid[J]. Automation of Electric Power Systems, 40(21):123-127+167.
[5] Bilil H, Gharavi H. (2018) MMSE-Based Analytical Estimator for Uncertain Power System With Limited Number of Measurements[J]. IEEE Transactions on Power Systems, 33(5):1-9.
[6] Shabani, Masoume, Mahmoudimehr, et al. (2018) Techno-economic role of PV tracking technology in a hybrid PV-hydroelectric standalone power system[J]. Applied energy, 15(59):69-75.
[7] Eltamaly A M, Abd Elghaffar A N. (2018) Modeling of distance protection logic for out-of-step condition in power system[J]. Electrical Engineering, 588(1):1891-1899.
[8] Pablo Fernández-Porras, Panteli M, Jairo Quirós-Tortós. (2018) Intentional Controlled Islanding: When to Island for Power System Blackout Prevention[J]. IET Generation Transmission & Distribution, 12(14):3542-3549.
[9] Haisong J, Tao P, Jilin Z, et al. (2018) Semi-quantum noise randomized data encryption based on an amplified spontaneous emission light source[J]. Optics Express, 26(9):11587.
[10] Rocking-chair Na-ion hybrid capacitor: (2019) a high energy/power system based on Na3V2O2(PO4)2F@PEDOT core–shell nanorods[J]. Journal of Materials Chemistry A, 7(3):1030-1037.