Research and implementation of information security for intelligent distribution network

Wang Ning¹, Wu Yanli², Liu Guangxing³, Yao Ruizhe², Zhang Longfei²

¹ Associate Professor, Dalian University of Technology, Dalian, China
² Master student, Dalian University of Technology, Dalian, China
³ Assistant Engineer, Dongguan Power Supply Bureau, Dongguan, China
E-mail: 1922095560@qq.com

Abstract: The intelligent distribution network is an important hub for connecting power generation and users, and the security of its information is closely related to the stable operation of the power grid. In order to solve the contradiction between the security and real-time of information in intelligent distribution network according to Supplementary Provisions for Safety Protection of Medium and Low Voltage Distribution Network Automation System, an information security model of intelligent distribution network is proposed, after deeply studying AES encryption algorithm and SHA-256 authentication algorithm, using OPNET as simulation software for smart distribution network information to carry out transmission delay curve. FPGA is used as information security processing platform. We obtain the total delay, analyze the integrity and availability. The experiment proves that the intelligent distribution network information security processing solution satisfies the three elements of CIA information security, and has good confidentiality, integrity and availability.

1. Introduction

Driven by growth in energy and electricity demand, the power grid is experiencing a leap-forward development from traditional power grids to modern smart grids, from urban power grids to large-scale interconnected power grids across regions [1]-[2]. The smart grid includes three systems: power generation, intelligent power transmission and intelligent power distribution. As a key node in the smart grid, the smart distribution network is an important hub connecting power generation and users. Communication network is the key part of the realization of intelligent distribution network system, only by means of secure communication network can the distribution automation system transmit the commands of the control center to numerous remote terminal units accurately [3]. However, the communication network of intelligent distribution network brings many conveniences to the power system. Simultaneously, it also produces many lurking perils. Therefore, it is urgent to research the security of communication network in intelligent distribution network [4]-[5].

Based on the existing state of affairs that the information level of distribution network is constantly improving and the information defense system of intelligent distribution network is difficult to effectively withstand network attacks. According to Safety Protection Scheme for Secondary System of Distribution Network and General Scheme of Safety Protection for Secondary Power System of State Electricity Regulatory Commission, Notice on Strengthening the Safety Protection Work of Distribution Network Automation System and Supplementary Provisions for Safety Protection of Medium and Low Voltage Distribution Network Automation System were developed and released by grid organization, which stipulate the communication security protection requirements of distribution network. Intelligent distribution network communication must adopt security isolation such as APN.
and VPN, authentication encryption, access control. It must have the function of one-way authentication in distribution network communication system. Therefore, it is of great significance to research a safe and effective encryption authentication algorithm to ensure the safe and stable operation of smart distribution network [6]-[8].

Paper adopts XML encryption and XML authentication based on ARM processor [9]. Although XML encryption is the most prevalent technology for structuring data at present, it can ensure the security of data transmission between end-to-end, but it can not meet the real-time requirements of some data transmission in distribution network, and the author does not mention the time consumed by information encryption. Paper uses TEA encryption algorithm to calculate the security of distribution network information, and utilizes CRC check code to verify the integrity of information after decryption operation [10]. This method only takes 0.181ms to process the distribution network information, which meets the real-time requirement of the distribution network information. However, it does not use a special authentication algorithm, which leads to the lack of integrity, and it does not adopt the current mainstream encryption algorithm, it will enormously limit its versatility and compatibility. Paper proposes a GCM encryption authentication method, it meets real-time requirements, however, the information is only protected by authentication algorithm, therefore, the confidentiality of the information can not be guaranteed [11].

This paper introduces the AES algorithm to meet the real-time requirements of secure communication. and SHA-256 authentication algorithm is proposed to defend the intelligent distribution network information system from possible active attacks. Finally, the CIA test proves that the proposed method can meet the real-time requirements of information processing under the premise of effectively guaranteeing the security of data.

2. Intelligent distribution network communication security model establishment

In order to guarantee the communication safety of intelligent distribution network, the communication message ought to meet the three elements of communication security, CIA, which is Confidentiality, Integrity and Availability [12]. Generally, encryption is used to protect the confidentiality of information.

Because of the high real-time requirement of distribution network, it is necessary to consider the speed of the algorithm when selecting the encryption algorithm. Symmetric encryption algorithm is much faster than asymmetric encryption algorithm. AES owns higher speed, higher resource utilization efficiency and more secure. Therefore, this paper selects AES algorithm to encrypt distribution network information [13]-[14].

On the basis of guaranteeing the confidentiality of communication message, the integrity and availability should be satisfied at the same time. Accordingly, this paper presents an information security model of intelligent distribution network as shown in Figure 1. The monolithic construction of the model includes: information generation module, key generation module, AES encryption module, AES decryption module, SHA authentication module, parameter verification module, real-time verification module and data output module.
When the initial signal of encryption and authentication is input into the information security communication system of distribution network. Firstly, using SHA authentication system to generate authentication code $MAC$, The AES encryption module encrypts the information $M$ by using the required key $K$ to generate the ciphertext $C$, and attaches the $MAC$ to the end of the ciphertext.

After the decryption check start signal inputting to the message secure communication system, above all, the AES decryption is performed on the $C_1$ of the smart distribution network information. Generating authentication code $MAC_1$ through SHA authentication module. If $MAC_1$ is consistent with $MAC$ and the parameters are checked correctly, the message is not attacked. When the real-time nature of the test also past muster, the original text, the authentication label, and the completion signal are output.

3. The implementation of intelligent distribution network communication security

3.1. The implementation of confidentiality

In order to guarantee the confidentiality and real-time of the message, this paper encrypt information by AES. Mainkey is the 128bits key which is negotiated between the receiver and the sender in advance; Plaintext is the input of the encryption part of AES algorithm, that is, the distribution network communication information sent by the information sender. Ciphertext is the output encrypted by AES, which is n 128bits ciphertext blocks generated.

The design of encryption module of AES algorithm is shown in Figure 2. Using the Mainkey to perform the AES encryption operation on the Plaintext. After an XOR operation between Mainkey and Plaintext, it is necessary to complete 10 times of S-Box module, 10 rounds of Shift-Row modules, 9 columns of mixed Mix-Column modules, Ciphertext is completed by 10 times round XOR operation.. Here, each round key addition operation needs to generate a set of round keys according to Mainkey to complete the round key addition operation. Decryption is the inverse of encryption.
3.2. The implementation of integrity

The integrity module of the intelligent distribution network information security model designed in this paper is implemented by the secure hash algorithm SHA-256 authentication algorithm. SHA-256 authentication algorithm can convert input compression with data length of 264 bits into message digest with 256 bits [15]. SHA-256 authentication algorithm is used to protect the information against active attacks such as deletion, insertion and tampering brought by attackers. The design of the SHA-256 authentication algorithm module is shown in Figure 3.

![SHA-256 algorithm implementation](image)

Figure 3. SHA-256 algorithm implementation

4. Information security model CIA test

4.1. Confidentiality analysis

The AES algorithm completes the correlation test at the beginning of the development. Due to the design advantages of the S-box and the algorithm, AES algorithm exhibits a good irrelevance [16]. However, the authentication code, in this paper, is generated by the AES algorithm in plaintext, and the AES algorithm ciphertext is also produced by plaintext. The ciphertext and the authentication code are simultaneously intercepted by the attacker. If there is some correlation between the authentication code and the AES algorithm ciphertext, the attacker may guess the plaintext through statistical analysis. Based on this, this paper tests the correlation between ciphertext and authentication code. Therefore, this paper attacks ciphertext with different degrees of tampering, and uses statistical methods to analyze the correlation between ciphertext and authentication code. The specific operation is: tampering test for the information of length 1326 bytes, fifty bytes of ciphertext are tampered with at a time until it is completely tampered with completely, we test the number of changes in the authentication code after the ciphertext has been falsified. Relevance analysis between tamper cipher digits and authentication code change digits by excellent statistical tool R software. It shows the change-digit curve of authentication code in Figure 4. Figure 5 is the correlation analysis of four groups of altered digits of authentication codes subjected to tampering attacks by R software.
Due to the limitation of input length of SHA-256 authentication algorithm, one-time authentication cannot complete the authentication operation of message limit length, so this paper uses four parallel SHA-256 to complete the operation. Since four parallel operations are not allowed to correlate with each other, the graph line should be shown in Figure 4, which shows a step-by-step rise, the smaller the correlation of data between each step, the safer the data will be. Based on this, this paper uses the powerful statistical analysis software R to analyze the data correlation between each step. As can be seen from Figure 5, the correlation coefficients of the four groups are 0.3278858, 0.3720288, -0.4157705, -0.1432037. After taking the absolute value, it is 0.3278858, 0.3720288, 0.4157705, 0.1432037, which is weak correlation. Therefore, the correlation between the ciphertext and the authentication code is poor, which can effectively resist the correlation analysis of the attacker after the tampering attack.

**Figure 4.** Changing the Digit Curve of Authentication Code

**Figure 5.** Correlation Analysis

### 4.2. Integrity analysis

The integrity of secure communication means that the information is not allowed to be falsified during the transmission of information [17]. To ensure the integrity of information, the model should have the function of responding to active attacks such as tampering, deletion and insertion. Therefore, on the integrity test platform of Figure 6, we simulate an assailant's attack on the information, according to the response of the platform, we can test whether the model can detect the active attack.
The four digital tubes on the left show the number of ciphertext changes in Figure 6. It can be seen from the figure that the attacker tampering with the data of 100 bits; The four digital tubes on the right show the number of changes in the authentication code, that is to say, the tampered authentication code changed 238 bits of data compared with the unassailed authentication code. Through experiments, we can see that the model designed in this paper can detect information being attacked actively and respond to it, thus ensuring the integrity of the information.

4.3. Usability test
Usability of secure communication means that when legitimate users need lawful use of information, they should be guaranteed to get it in a timely manner, that is, to ensure the real-time nature of information [18]. Supplementary Provisions for Safety Protection of Medium and Low Voltage Distribution Network Automation System is the most stringent criterion for real-time information. Its standard is: part of the information is completed within 4ms from the sender to the receiver. Therefore, the communication scheme proposed in this paper guarantees the security of distribution network information, but the crux is whether the communication delay can meet the real-time requirement of less than 4ms.

There are two parts of communication delay time: the one is the processing time of the algorithm, including the encryption time of the sender, \( t_{AES_{\text{encrypt}}} \), and the decryption time of the receiver, \( t_{AES_{\text{decrypt}}} \); the another is the network transmission time of the information, \( t_{\text{net\_delay}} \). As shown in formula (1).

\[
 t = t_{AES_{\text{encrypt}}} + t_{AES_{\text{decrypt}}} + t_{\text{net\_delay}} 
\]

This paper achieves the operation AES encryption, decryption based on FPGA. Figure 7 is a hardware experiment platform for FPGA. The 1st, 2nd and 3rd digital tubes on the left of the peripheral of the FPGA display the time of hardware implementation in microseconds. As can be seen from the figure, this information security processing time is 210μs.
Figure 8 shows the data sampling waveform of the Saleae Logic16 logic analyzer operating in 100Mbits/s dual channel mode. The acquisition is the start signal flag bit and the output completion flag bit of the FPGA. Its time length is set to 2s, the data precision is 10ns. Channel 0 collects the start signal, and Channel 1 gather the end signal. Channel 1 has two up-and-down signals in Figure 8. This is because the first Up-edge is the completed encryption and authentication signal, and the information is decrypted and authenticated at 90ns after the encryption is completed. The start time of the encryption authentication in the FPGA is 985.77996ns, and the end time of it is 985.85798ns. After 90ns delay, the time to start decryption authentication is 985.85807ns, and the time to end of it is 985.98988ns. The total time for a secure operation is 209.92μs, where the encryption authentication time is 78.02μs, the interval is 0.09μs, and the decryption authentication time is 131.81μs. The total time of the information security operation is consistent with the operation processing time displayed by the digital tube in Figure 10, which proves that the real-time display program of the hardware circuit is correct. According to the hardware experiment of real-time test, even in the case of maximum data transmission delay, the total delay time of the model is 1.3992ms, which meets the real-time requirements of intelligent distribution network data transmission specified by IEC 61850 standard, and has 65.02% of margin.

![Figure 8. Hardware real-time test chart](image)

5. Conclusion
In order to ensure the security, availability and integrity of information in intelligent distribution network, this paper presents an encryption and authentication algorithm of AES_WITH_SHA256. In this paper, Quartus II software is used for synthesis while the smart distribution network star network model is selected as the background. Taking FPGA as a security information processing chip, a secure information processing platform has been built. Through experimental testing, the encryption and decryption processing time and communication network delay time can be calculated. The total delay time required for the secure processing method proposed in this paper is within 1.3992ms, which meets the real-time requirement. As a result, the model reaches the three elements of CIA information security.

6. References
[1] Zhang Yachun. Static Stability Evaluation of Power Grid Based on Response Information [D]. Jilin: Northeast Electric Power University, 2016.
[2] Li Zhongwei, Tong Weiming, Jin Xianji. Construction of Information Security Defense System and Information Security Testing System for Smart Grid[J]. Automation of Electric Power Systems, 2016, 40(8): 147-151.
[3] Ma Yaning. Research on Security Mechanism of Distribution Automation Communication System Based on EPON[D]. North China Electric Power University(Beijing), 2011.
[4] Liu Dichen, Peng Sicheng, Liao Qingfen, et.al. Prospects for the Future Integrated Distribution System Configuration Oriented to Energy Internet[J]. Power Grid Technology, 2015, 39(11): 3023-3034.
[5] Ma Zhao, Zhou Xiaoxin, Shang Yuwei, et al. Future Distribution System Form and Development Trend[J]. Journal of Electrical Engineering of China, 2015, 35(06): 1289-1298.

[6] Mu Hongtao. Research and implementation of security interactive gateway for distribution network based on national secret algorithm[D]. Beijing: North China Electric Power University, 2017.

[7] Zhu Jianfeng. Application of Asymmetric Encryption Algorithm in Distribution Automation System[J]. Automation & Information Engineering, 2014(50): 35-38.

[8] Wang Lidong. Study on the construction plan and strategy of distribution automation in Lu'an area[D]. Beijing: North China Electric Power University, 2017.

[9] Balasubramanya Raju, Ashwin Krishna, Geetishree Mishra. Implementation of an efficient dynamic AES algorithm using ARM based SoC[C]. Mathura, India: International Conference on Electrical, Computer and Electronics, 2017: 39-43.

[10] Wang Zhidong, Wang Gang, Li Yongchang, et al. Encryption method of IEC 61850-9-2LE based on micro encryption algorithm[J]. Automation of Electric Power Systems, 2016, 40(4): 121-127.

[11] Wang Baoyi, Wang Min’an, Zhang Shaomin, et al. A GCM-based intelligent transmission method for intelligent substation messages[J]. Automation of Electric Power Systems, 2013, 37(3): 91-96.

[12] He Lei. Getting Started with IEC 61850[M]. Beijing: China Electric Power Press, 2014: 260-313.

[13] Deng Yuanqing, Gongjing. Cryptography Concise Course[M]. Beijing: Tsinghua University Press, 2013.

[14] Dai Xichang. Research on Data Transmission Security of Intelligent Distribution Network[D]. East China Jiaotong University, 2015.

[15] Qin Chuanhong. Research on real-time and security of intelligent substation communication network[D]. Dalian: Dalian University of Technology, 2013.

[16] Prakhar Kaushik, Rana Majumdar. Timing attack analysis on AES on modern processors[D]. Noida, India: International Conference on Reliability, Infocom Technologies and Optimization: 2017: 462-465.

[17] Liu Yixian, Mu Dejun. Research on network security assessment method based on CIA attribute[J/OL]. Computer Technology and Development, 2017.

[18] Tong Xiaoyang, Wang Xiaoru. Thoughts on Network Attacks and Grid Information Security Prevention Caused by U.S. Power Outages[J]. Automation of Electric Power Systems, 2016, 40(7): 144-148.