IOP Conf. Series: Materials Science and Engineering **719** (2020) 012056 doi:10.1088/1757-899X/719/1/012056

Smart Grid Monitoring Systems based on Advanced Encryption Standard and Wireless Local Area Network

Chuankai Yang[1], Jingfeng Wu[1], Longyang Wang[2], Xiaolan Zhang[1], Liangshu Li[1], Shan Liu[2]

[1] State Grid Shaanxi Electric Power Research Institute, Xi'an, Shaanxi Province, China
[2] School of Electrical Engineering and Automation, Wuhan University, Wuhan, Hubei Province, China
Email: wanglongyang1994@163.com

Abstract. China's power grid is developing in the direction of informatization and increasingly large-scale at present. In view of the problems of optical cable interference and poor data security in the existing power grid detection system, a grid detection system based on wireless local area network (WLAN) and improved advanced encryption standard (AES) is proposed. Firstly, wireless local area network technology is introduced on the basis of the original power grid detection system to realize wireless transmission of power data. Then the newly-proposed system improves the S-BOX in the traditional AES encryption algorithm to improve the security of the algorithm. The improved AES encryption algorithm is applied to the grid detection system to realize the secure transmission of power data. Finally, the practical value of the grid detection system is verified by simulation.

1. Introduction

In recent years, the power grid equipment has potential safety hazards under heavy load due to the rapid growth of national electricity consumption. In order to ensure the normal operation of the grid equipment, the establishment of a safe and reliable high-efficiency smart grid is the development trend of the existing grid system [1]. Among them, the grid monitoring system is used to monitor the safety situation of the grid equipment as a problem finder in the power grid. It is an important component of the smart grid, and its normal operation directly affects the working condition of the entire grid. Therefore, the design of the grid monitoring system is of great significance for the construction of the grid. In order to ensure the safe and reliable operation of the grid monitoring system, actual and reliable monitoring of the information transmission process is one of the cores focuses when designing the system.

At present, some scholars have conducted relevant research on the power grid monitoring system. Chen Gang [2] designed the information transmission of the monitoring system which mainly used optical cable for wired transmission, which greatly improves the capacity of information transmission meaning it can transmit a large amount of information at the same time. However, the cable needs to be pre-laid and is affected by the transmission distance and the external environment. Li Min [3] analysed the characteristics of information networks in smart grids in order to overcome the information security issues that are increasingly prominent in smart grids, and established the importance of information network security to ensure the safe and efficient operation of smart grids. In order to pursue efficient and fast data transmission, Meikang Qiu et al. [4] used symmetric encryption algorithms such as DES algorithm and RC5 algorithm for data encryption. The encryption speed is accelerated and the energy loss is reduced, but the both sides of the communication use the same

decryption key, resulting in reduction of the security level in data transmissions. Zeng Fanyu [5] proposed combining AES encryption algorithm with ECC algorithm, combining the advantages of symmetric encryption algorithms and asymmetric encryption algorithms, and improving the security of encryption, but the encryption process is cumbersome and cannot achieve fast and efficient encryption.

Aiming at the limitations of wired transmission in the power grid, low data transmission efficiency and poor security, this paper proposes an improved power grid monitoring system. The system uses WLAN for data transmission and uses the improved AES encryption algorithm to improve the security of data transmission. Finally, the paper verifies the correctness and feasibility of the system through verification.

2. System Design

The main purpose of the grid monitoring system is to monitor the security situation of each station and send corresponding commands to the station according to the monitoring situation [6]. According to the above requirements, this paper divides the grid data monitoring system into separate layers: the sensing layer, the network layer and the application layer. Each layer has its own function. The overall framework of the grid monitoring system is shown in Figure 1.

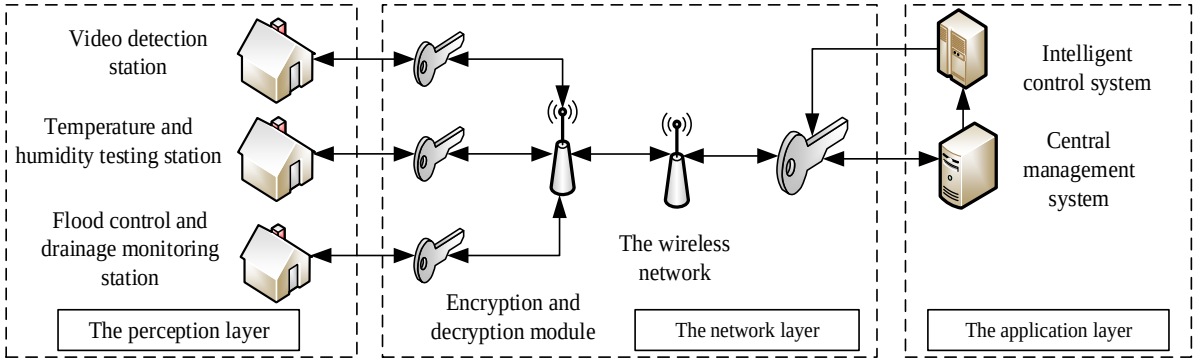

Figure 1. Grid monitoring system.

- Perceptual layer: mainly collects device data, including information in the video subsystem, temperature and humidity monitoring subsystem, flood control and drainage monitoring subsystem. They collect device data, and transfers the information to the central management system through the network transport layer;
- Network layer: mainly based on AES encryption algorithm to encrypt and decrypt data in WLAN. The collected data is encrypted by an improved encryption algorithm to improve the security and efficiency of data transmission;
- Application layer: mainly includes the central management system and intelligent control system. After receiving the encrypted data, the central management system decrypts, analyses and stores the encrypted data, and the intelligent control system uses the decrypted data to convey specific instructions to the power grid equipment to achieve control;

In the data transmission process of the power grid, the traditional wired communication needs to pre-lay the optical cable, the construction process is complicated, and has certain requirements concerning the transmission distance [7]. The system proposed in this paper uses wireless local area network for communication [8], which is not limited by distance. The WLAN established by WIFI technology is a combination of computer network and wireless communication technology. It mainly uses the open radio frequency (RF) technology of 2.4 GHz and 5.8 GHz bands instead of wired technology to form a local area network, which has all the functions of traditional wired LAN. The user can realize the broadband network access at anytime, anywhere and at random.

A schematic diagram of a grid monitoring system using a wireless local area network is shown in Figure 2 below.

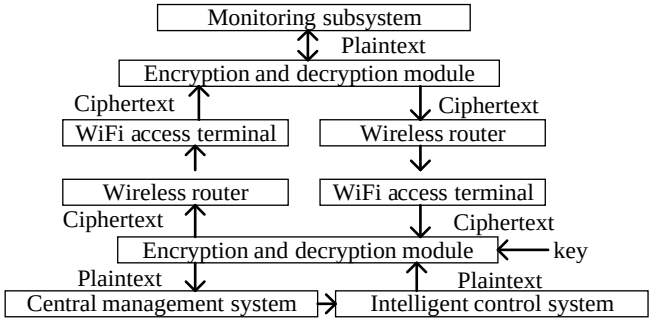

Figure 2. Schematic diagram of the grid monitoring system

The system information transmission is not limited by distance, and the information is encrypted before being sent out, which can effectively prevent the monitoring information from being stolen. After receiving the information, the receiving end decrypts the decrypted text, and the decrypted plaintext can directly perform subsequent processing, which can realize the high efficiency of monitoring information transmission.

3. Improved AES Encryption Algorithm

3.1. Analysis of AES Encryption Algorithm

In the process of data transmission, in order to protect the transmitted information, it needs to be encrypted. The commonly used encryption algorithms are RC4, RC5, etc. The system uses AES encryption algorithm. Advanced Encryption Standard (AES), also known as Rijndael encryption in cryptography, is a block encryption standard adopted by the US federal government. AES is the most common symmetric encryption algorithm, using the same key for encryption and decryption. In the encryption process, the key and the plaintext are operated in bytes [9].

The operation in the AES encryption process needs to be performed in the S-box. The iteration period of the traditional S-box on the GF(2^8) domain is too short, which affects the algebraic nature of the S-box and the anti-attack capability of the algorithm. Since the packet keys of AES is generated by initial key expansion, there is inevitably a certain degree of correlation between each packet key. Correlation can lead to two bad results. One is to increase the possibility of the initial key being compromised, affecting the security of encryption; the second is to make the errors in the transmission spread ferociously once occurred, reducing the accuracy of encryption and decryption. Therefore, the use of improved S-box and elimination of correlation between packet keys is crucial to improving the security and accuracy of the AES algorithm.

3.2. Improvement of S-box

In the AES encryption algorithm, the SubByte operation is its only non-linear part. It is implemented by the pre-calculating table S-box, so the quality of the S-box has a significant impact on the performance of the algorithm [10]. The complexity of the S-box algebraic equation is one of the important indicators reflecting its security, which is related to the ability of the S-box to resist attacks. The traditional S-box algebra equation only has 9 items [11], so the traditional S-box algebraic equation is not complex enough and is lacking in security.

In this paper, the two operations of modifying the affine transformation pair and adjusting the S-box calculation order are applied to the encryption algorithm of the grid monitoring system, which can significantly increase the iteration period of the S-box, enhance the algebraic nature of the S-box, and improve the security of the information transmission of the grid monitoring system[12]. A new affine transform pair ('A7', '6F') is used, and the following three steps are used to calculate a new S-box. (1) An affine transformation is performed on affine transformation pair ('A7', '6F'). (2) Find the multiplicative inverse element. (3) The affine transformation pair ('A7', '6F') is subjected to affine transformation again, and achieving output result. The operation of the inverse S-box is the same as that of the S-box, and the affine transformation pair is ('D0', '35'). The new S-box iterative output

period and affine transformation pair period are longer, and the number of algebraic equation items of S-box and inverse S-box is also increased from 9 to 255, which greatly improves the complexity of S-box.

3.3. Improvement of Key

In the traditional AES encryption algorithm, each round of encrypted key is obtained by a key expansion algorithm, and the 4-word initial key is expanded into a 44-word round key for ten rounds of encryption operation [13]. Due to the reversibility of the extended algorithm, the round key and the initial key can be calculated from each other, and therefore, the correlation between the traditional round keys is strong. The attacker can easily obtain all the key content after obtaining a partial key, and the security is low.

This paper proposes to apply the stream cipher idea to the information transmission process of the grid monitoring system, and generate a random sequence by using a pseudo-random algorithm to generate a random key. A pseudo-random sequence can satisfy the non-speculative needs in cryptographic operations under certain conditions. Commonly used pseudo-random number column generation algorithms include square-to-square algorithm and BBS algorithm. In this paper, the pseudo-random algorithm used is the linear congruence algorithm [14]. The flow of generating pseudo-random numbers is shown in Figure 3 below.

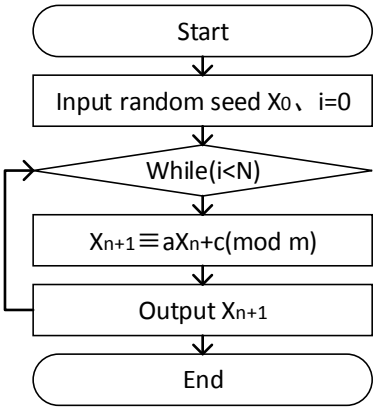

Figure 3. Pseudo-random number generation process

This is a widely used pseudo-random number generation algorithm whose recursion formula is $X_{n+1} = (aX_n + c) mod\ m,\ n$=1、2、3...$n$. he linear congruence algorithm has the advantages of fast generation speed and long sequence period of generation, making it an ideal pseudo-random number generation algorithm.

The specific process of encrypting by using a pseudo-random number is as follows: a random sequence is generated by a pseudo-random number generation algorithm, then the random sequence produces a key stream sequence, and the plaintext and the key stream are packet-encrypted according to a certain length. The byte replacement operation in the encryption process uses the improved S-box described above. For the cryptanalyst, even if a sufficient number of plaintext and ciphertext pairs are intercepted, the entire key sequence cannot be inferred because the encryption keys of each packet are not correlated.

4. Simulation and Analysis of Improved AES Encryption Algorithm

4.1. Encryption and Decryption Simulation of Improved AES Encryption Algorithm

The improved AES encryption algorithm proposed in this paper is based on C++ programming, and a palindrome is selected as plaintext for independent encryption simulation. The X_0 of the generated random sequence is 167, and the seed key is randomly selected in the pseudo-random number column,

and the packet length is 128 bits. The number of encryption and decryption rounds is 10, and the generated key stream sequence is 1408 bits in total. The encryption and decryption simulations were performed twice using the same plaintext, and the results are shown in Tables 1 below.

Table 1. Data and results of encryption and decryption simulation.

FIRST	**Plaintext**	123456abccba654321
	Ciphertext	de,99,1d,20,68,90,85,44,f3,ed,77,a2,d5,8,h7,e0,3b,53
	Decryption result	123456abccba654321
SECOND	**Plaintext**	123456abccba654321
	Ciphertext	2a,4e,35,7a,19,h6,31,d0,55,fc,c6,ad,4e,3h,5c,ea,1,40
	Decryption result	123456abccba654321

The traditional AES encryption algorithm obtains the same ciphertext by independently encrypting the same plaintext multiple times, and since the packet key is expanded by the original seed key, the correlation between the ciphertexts of each packet is stronger. In this paper, the simulation is performed independently using the same plaintext. The decrypted result is the same as the plaintext, and the correctness of the improved AES encryption algorithm is verified. However, in these two simulations, the ciphertext is completely different. This is because the key in the improved AES algorithm is a random sequence obtained by the linear congruence algorithm using the stream cipher idea. Therefore, the keys used for each encryption are different. Even if the same plaintext is independently encrypted multiple times, the keys are different each time, and the ciphertext obtained each time changes.

4.2. Security Analysis of Improved AES Encryption Algorithm

In the process of improving the AES encryption algorithm, the affine transformation pair of the S-box is firstly modified, the calculation order of the S-box is adjusted, the iteration period of the S-box is increased, and the algebraic property of the S-box is enhanced. After changing the key generation method, instead of using the key expansion of the traditional AES algorithm, a pseudo-random algorithm is selected to obtain a random key stream sequence. Therefore, the improved AES encryption algorithm is a hybrid encryption algorithm combining packet cipher and sequence cipher, which is more secure than the algorithm using packet cipher or sequence cipher alone.

In the improved key, a random number sequence is generated using the function $X_{n+1} = (aX_n + c) mod\ m,\ n=1、2、3...n$. This function is a one-way function [15], which is a function that is easy to solve in the forward direction and is difficult or impossible to solve in the reverse direction. Therefore, when one or more random numbers in a random sequence are known, it is extremely difficult to detonate the entire sequence or seed key. Each time a different seed key is used for encryption, the random sequence generated each time is different, so that each encryption and decryption use a different key stream. Since the key stream sequence is not generated by key expansion, there is no correlation between the packet keys. The cryptanalyst cannot infer the key stream sequence even if a certain number of plaintext and ciphertext pairs are intercepted. The unpredictability of the key greatly increases the difficulty of the algorithm being compromised, so it can be considered that the improved AES encryption algorithm is more secure.

5. Conclusion

This paper optimizes the data transmission process in the grid detection system, by improving the traditional AES encryption algorithm, S-box and keys, it also simulates and analyses the improved algorithm. The conclusions are as follows:

- Data transmission using wireless local area network solves the problem that the optical cable in the traditional wired communication is limited by the distance and the pre-laying process is complicated. Wireless transmission is not limited by distance and has a higher degree of transmission liberty, which provides great convenience for power grid monitoring;

- In the process of data transmission, the widely used AES encryption algorithm is adopted. In the improvement process of the S-box and the key, the complexity of the S-box and the unpredictability of the key are significantly improved, and the anti-attack capability of the AES encryption algorithm is improved.
- After the simulation, it is found that the plaintext before encryption is the same as the plaintext after decryption, but the ciphertext is different. The correctness and the feasibility of the improved AES encryption algorithm is verified.

The power grid monitoring system designed in this paper can carry out long-distance transmission of monitoring data safely and efficiently, and realize the protection of the power grid.

6. Acknowledgments

This work was supported by the Science and Technology Project of State Grid Corporation of China under Project of “Research on the third generation substation auxiliary system” with NO. 520530180015.

7. References

[1] Farhangi, and H. "The path of the smart grid." IEEE Power & Energy Magazine 8.1(2010):18-28.
[2] Chen Gang, and Wang Xiaoshan. "Design and implementation of optical cable intelligent distribution monitoring system for regional electric power communication network." Modern Electronics Technique 09(2017):174-176+180.
[3] Li Min, et al. "The Information Security Risk Analysis of Smart Grid." NORTH CHINA ELECTRIC POWER1(2017):62-65.
[4] Qiu Meikang, et al. "Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System." IEEE Transactions on Smart Grid 2.4(2011):715-723.
[5] Zeng Fanjing, and Liu Xiaodong. "The research of AES algorithm based on the WLAN encryption." Electronic Design Engineering 05(2017):119-122.
[6] Zhai Hucheng. "Research and Analyze the Operating Condition Monitoring Technology of Transmission Line under Smart Grid." Science and Technology & Innovation 24(2015):96-96.
[7] Fang Yuesheng, Chen Hao, and Zeng Fanxing. "Development of Optical Fiber Technology and Its Application in Electric Power Communication." ELECTRIC POWER ICT 12.8(2014):20-26.
[8] Fan Yulin. "Review of Wireless Local Area Networks." Modern Information Technology v.03; No.9(2019):60-61+64.
[9] Mohammad, Omer K. Jasim, et al. "Innovative Method for Enhancing Key Generation and Management in the AES-Algorithm." Computer Science 4.4(2015):14-20.
[10] Shreenivas, Pai N, et al. "Logic optimization of AES S-Box." International Conference on Automatic Control & Dynamic Optimization Techniques IEEE, 2017.
[11] Das, Suman, U. Z. J. K. M. Sadique, and R. Ghosh. "Study of Randomness in AES Ciphertexts Produced by Randomly Generated S-Boxes and S-Boxes with Various Modulus and Additive Constant Polynomials." Journal of the Institution of Engineers (India): Series B 97.2(2016):193-208.
[12] Shen Xiaochen, Han Meng. "Improved S-box Based on Strict Avalanche Distance Criterion." Microelectronics & Computer v.35; No.6(2018):92-96.
[13] Fan Lichen, and Wang Guihai. "Research and Improvement on the Key Expansion of Encryption Algorithm AES." Information Technology and Information 03(2015):82-84.
[14] Zhang Dawei, Shao Yinghai, and Zuo Lei. "Pseudo random number generation algorithm based on linear congruence method." Journal of Eastern Liaoning University (Natural Science Edition)v.25; No.99.03(2018):55-60.
[15] Zhang, Xiaomin. "Verifiable multi-secret sharing scheme based on linear one-way function." Journal of Computer Applications 33.5(2013):1391-1393.