Asian Journal of Information Technology 5(7): 772-777, 2006

Selective Hybrid Encryption Algorithms for Secure Transmission of Electrical Energy Data

Li Jing and He Yanxiang
Computer School, Wuhan University, Wuhan,430072, People of Republic China

Abstract: The encryption algorithms previously proposed usually encrypt every data of electrical energy in order to maintain security and safety. However, the quantity of electrical energy data to be transmitted is very large and a majority of them are encrypted, so the encryption algorithms previously proposed increase the burden of communications and reduce the transmission efficiency. In this study, A Selective Hybrid Encryption Algorithm for secure transmission of electrical energy data is presented. The algorithm is based on SSL (Secure Sockets Layer). It adopts Encryption Algorithm AES (Advanced Encryption Standard) to encrypt important data of electrical energy and uses SHA-1(Secure Hash Algorithm) to get message digest. At the same time, The algorithm make also use of ECC£¨Elliptic Curves Cryptography and AES to transmit data. With the method, the data of electrical energy encrypted can be transmitted highly active and safely.

Key words: Data of electrical energy, encryption algorithms, selective hybrid encryption, digital signature

INTRODUCTION

The date of electrical energy is a very important date under the operating mechanism in electric market. It is the bases for the economic balance among power plants and power grids, power grids and power grids, power plants and power plants. The date of electrical energy were gathered and got through the long-range communication of data collecting system of electric energy. It is consist of main station system, communication system, industry and resident Check meter system (Include the collector and electric energy meter). It can be used for collecting, treating, storing the electric energy and correlated data from power plant, distribution and substation, big consumers, every district etc. Moreover the statistics, analysis, calculations for the original gathered data can be made. The amount of transmission for the long-range electric energy data is very great and the transmission of the data must be safe, reliable, accurate, intact and real-time stated.

It includes seven kinds of information for the data from long-distance transmission:[1] voltage, current, power factor[2] obverse and reverse active power for time-sharing electricity energy, reactive power four quadrants for time-sharing electricity energy; [3] obverse and reverse max active power needs for time-sharing electricity energy and its happen time;[4] obverse and reverse max reactive power needs for time-sharing electricity energy and its happen time;[5] time of breaking off phase, times, power consumption during breaking off phase;[6] load diagram; [7] warning message. In these seven kinds of information, the second is the most important and also it is the date that is mostly likely to be juggled and intercepted.

The transmission of electrical energy data collecting system is usually based on SSL(Security Socket Layer), it set up encryption date passway between customer and user, plant uniform encryption algorithm into the application layer to guarantee security and dependability. However, the quantity of electrical energy data to be transmitted is very large and they are all encrypted, so the encryption algorithms previously proposed increase the burden of communications and reduce the transmission efficiency.

In this study, a selective hybrid encryption algorithm for secure transmission of electrical energy data is presented. The 2nd kind of secret data from the seven kinds of electricity energy data are encrypted with the high dependability algorithm. The data of (1),(3)~(7) which include a large number of unclassified data are carried on appropriate security treatment, thus the efficiency encryption and transmission is raised.

ELECTRICAL ENERGY DATA COMMUNICATION PROTOCOL AND SELECTIVE ENCRYPTION DATA LOCALIZATION

Electrical energy data communication protocol: According to Multi-function kWh meter communication procotol DL/T645-1997, the communication of electricity energy data adopts half-duplex operation way.[1] A main

Corresponding Author: Li Jing, Computer School, Wuhan University, Wuhan, 430072, People of Republic China

station is made of holding units or other data terminals. Slave stations are made of tariff devices. Every tariff devices has its coding address. Establishment and relieve of the communication link is controlled by the data frames from main station. Every frame is consisted of frame start symbol (1 byte: 68H), slave station address field (6 bytes:A0~A5, it can be Table number, capital number, user number, equipment number etc.), assistant start symbol(1 byte: 68H), control code(1 byte: C, definite the data transmission direction, station to exception symbol, following frame symbol, function of requirement and response etc.), data length(1 byte:L, means data domain byte number),data domain(2+m bytes: including identifications of data (2 bytes) and data block (m bytes), frame information portrait access code(1 byte: CS, all the byte mod 256 from frame start symbol to access code) and frame end symbol(1 byte:16H).

The selective of the encryption data from electricity energy data can be confirmed by the data identification code, data identification code (DI_0,DI_1) define data type and attribute of the data frame. When the high 4 bits of the second byte from the data identification code DI_{1H} = 1001, it can be selected as the electricity energy data to be encrypted. Large number of data frame from data identification code DI_{1H}≠1001 need not be encrypted.

Selective encryption data localization: The process of long-distance transmission for electricity energy data is sending out request of reading data from main station to slave stations and slave stations respond main station. According to the data identification code of electricity energy, the block and form of data frame is chose from stations. The data can be located selectively for the electricity energy data to be encrypted. Fig. 1(a) and (b) show the form of the reading data request frame which main station send to station and normal reply no follow-up data frame from station.

In Figure1b, it shows no follow-up data frame when the controlling code C = 81H;data length: L = 02H+m (data length); N1, …, Nm is respectively m electricity energy data

68H	A0	...	A5	68H	C	L	DI_0	DI_1	CS	16H

Fig. 1a: Form of reading data request frame which main station send to station

68H	A0	...	A5	68H	C	L	DI_0	DI_1	N_1	...	N_m	CS	16H

Fig.1b: Form of normal reply data frame from station

In Fig. 1(b),it shows no follow-up data frame when the controlling code C=81H;data length:

L=02H+m(data length); N1,…,Nm is respectively m electricity energy data

- The location of encrypted data block from no follow-up data frame: The data blocks N1,…,Nm in which the high 4 bits of data identifier DI1H£½1001.
- The first bit of encrypted data : The 13rd byte of normal responding data frame of station.
- The end bit of encrypted data : The 13 + m-1 byte of normal responding data frame of station.

It can locate like the form of the data frame which is adopted when it has no follow-up data frame.

THE DESIGN OF SELECTIVE HYBRID ENCRYPTION ALGORITHMS

Some interrelated encryption standard, algorithms and agreement

Advanced encryption standard[2]: In 1997. The American government start to collect new data encryption standard algorithms (AES) publicly to take place of the data encryption standard which is abolished in 1998. After three turn filter, American government choose the encryption algorithm "RIJNDAEL" which the Belgium cryptogram expert Joan Daemen and Vincent Rijmen bring forward for the AES. American government issue AES for the national standard publicity. RIJNDAEL algorithms is a grouping iteration encryption algorithm which the length of data block and private key can change. The length of the data block and private key can respectively be 128 bits, 192 bits, 256 bits. In the overall construction, this algorithm adopt circle function, which is consist of non-linear level, the linear mix level, the key superimposed layer, it replace of replacement network, multi- circles iteration.

AES is very safe, the algorithm design is simple, it has concision and precision mathematical algorithm inside and encryption data can be got across once. AES private key can be installed fast, encrypt and decipher fast, need a little memory space, run well in the all platform, support parallel processing and it also can resist all known attack. So we choose AES to encrypt the original data in this study.

Elliptic curves cryptography (ECC): Elliptic Curves Cryptography is a public key cryptography and it is bring forward by Koblitz[3] and Miller in 1980s. The private key and public key of users are created, based on that the

elliptical curve point is the definition of the separated groups of a few knotty problems. The public key of the user can be found in the public private key base, private key is held by user. When transmitting data, transmission side first encrypt data by the public key from the receiving side, then receiving side decipher data by its private key when it receives data, it can be allowed to guarantee the security of the data and need not transmit key.

Elliptic Curves Cryptography has some characteristics like safe, short key, light calculating amount, run fast, the realization of software is in small scale, the realization circuit of hardware save electricity etc.

Secure hash function: Secure hash algorithm(SHA)[4], is designed by National Institute of Standards and Technology (NIST) and issued in 1993(FIPS PUB 180) and it issue FIPS PUB 180-1 in 1995, usually called SHA-1. The length of input data is not more than 264 bits (binary system), output is 160 bits information digest.

SHA is a type of data encryption algorithm. Being developed and improved by encryption experts for many years, it has been considered as one of the safest hash algorithm, which is completed day by day. The step is like that: Receive a section proclaimed in writing, then change it into one section (usually smaller) Cipher text in an irreversible way; also can be regarded as a series of input code. (called map or information) and change it into output series which is short, fixed digit, namely the process of hashed value(also called digest of information or authentication of message code). The value of hashed function can be regarded as a verifiable "fingerprint" or "digest" to proclaimed in writing, so the digital signature of hashed value can be regarded as the digital signature to the proclaimed in writing.

Since the algorithm is completed day by day through the development and improvement by the encryption expert for many years, now it is called one of the recognized safest hash algorithm and be widely used, so it adopt this algorithm to verify the digest of data from electricity energy in this study.

SSL secure protocol: Secure Sockets Layer (SSL) protocol was first designed and exploited by Netscape Communication Company and it is mainly used to enhance the safety coefficient of the data among the application. SSL. The whole concept of SSL protocol can be summarized like this: It is a protocol of affairs safety between the users who guarantee to install SSL and server and it refers to all TC/IP implication.

SSL is a protocol which guarantee the computer communication security, protect the process of communication. For instance, when a client is connected to a host computer, first initialize shaking protocol and set up SSL protocol will encrypt the whole process of communication and check the integrality till interlocution finished.

Since the transmission issue to be solved in this study only refers to transmit side and receive side and SSL protocol has the characteristics like it can realize the equipment simply, mature and safe technology and be fit for two sides communication, so this scheme choose SSL protocol.

Selective hybrid encryption algorithms composition: SSL secure protocol is consist of AES algorithm, SHA-1 algorithm and ECC algorithm which Selective Hybrid Encryption Algorithms proposed in the study base on. First check the electricity energy data. Encrypt the data of active power obverse, reverse time-sharing electricity energy, reactive power four quadrants time-sharing electricity energy with AES algorithm, then calculate information dig of electricity energy data to be transmitted with SHA-1 algorithm, Combine ECC and AES to realize the function of encryption, decryption, digital signature and verification for the electricity energy data.

SELECTIVE HYBRID ENCRYPTION ALGORITHMS IMPLEMENTATION PROCEDURE

Selective Encryption for electricity energy data: It includes seven kinds of information for the date from long-distance transmission. Among these seven kinds of information, the 2nd kind data is the most important data, also it is the date that is mostly likely to be juggled and intercepted so this kind of data should be chosen to encrypt with high reliability algorithm from electricity energy data in order to keep safe.

The procedure of Selective and encryption electricity energy data:

- Check data identification of data frame from station response
- DL1 ∧ 11110000B=10010000B
- If it equal to 10010000B,then jump to (4);
- if not, then jump to (5)
- Encrypt and output the data from13th bit to the end of 13+m-1 bit of current data frame with AES.
- Do not deal with the data frame, output directly.

Electricity energy data transmit process: With the process of selective encryption above, the party of electrical energy data to be encrypted can be encrypted

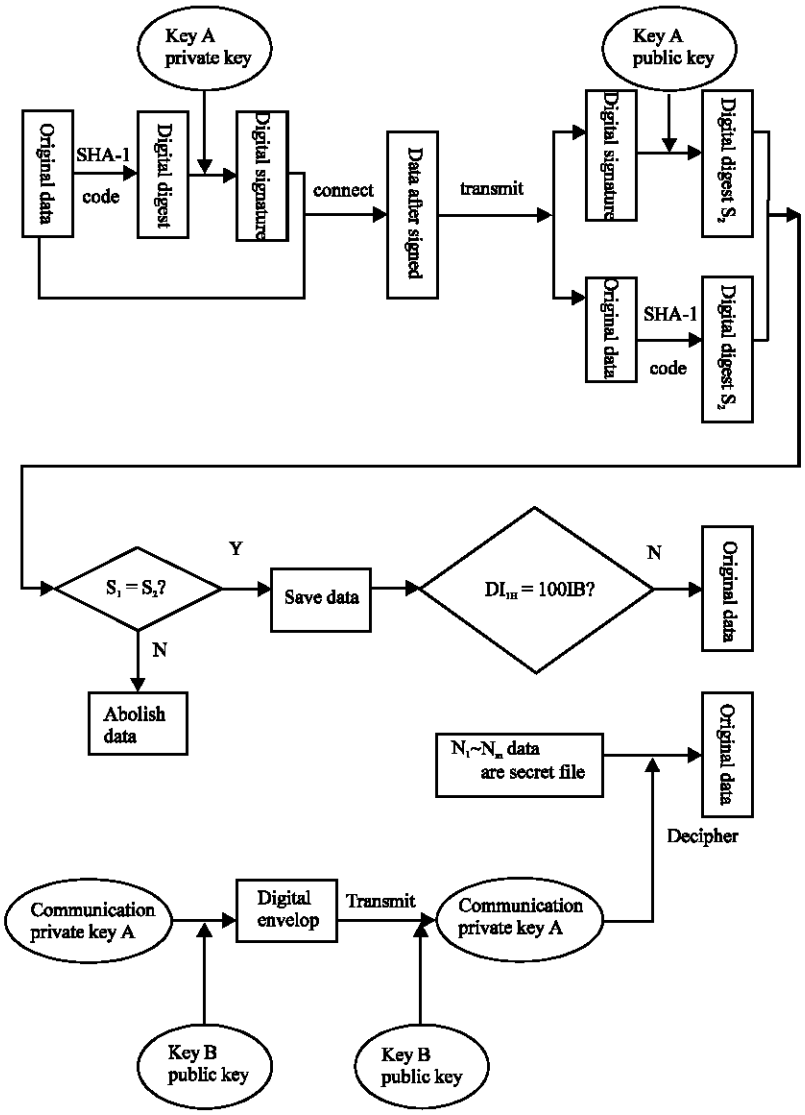

Fig. 2: Transmission process

by the high reliability encryption algorithm[6]. Then transmit the data to the receiving side after dealing with the output data.

The transmit process is shown in Fig. 2.

concrete steps:

- Transmit side A code original data with SHA-1 function, then produce a section of fixed length digital digest.
- Transmit side A encrypt digest with its private key (Key A) to form digital signature[5], enclose it in back of original data from sending information.
- Transmit side A encrypt its communication key with public key (Key B) of receive side B, then transmit to receive side B. This step make use of the effete of digital envelop.
- Receive side B receive encrypted communication key, then decipher it with its private key to get communication key of transmit side A.
- Receive side B decipher digital signature with public key of transmit side A to get digest; mean while code original data with SHA-1 function to produce another digest.
- Compared two digests by receive side B, if they are identical, it means the information is not destroyed or distorted, or discard.
- Receive side B judge the high 4 bits of the 12th byte from correct data: If it is 1001, encrypt N1~Nm

important electricity energy data, then decipher it with AES algorithm by communication key received from A to become original data; If not, data is original data, it can be used directly.

The advantage of Selective Hybrid Encryption Algorithms for Secure Transmission of Electrical energy data: Compared with routine encryption method of electricity energy data transmission, the method brought forward in this study has characteristics follows:

High efficiency of electrical energy data encryption: The routine electrical energy encryption scheme encrypt all the data completely, but in practical application, the amount of electricity energy data is very great and most data need not be encrypted, for instance: A main station long-distance communication collect data of 50 tariff devices (collector), a collector collect data of 8 electrical energy meters, there are 40 kinds of data in an electrical energy meter, a kind of data is described by 4 bytes, every electrical energy meter save a group of data per 5 minute (40 kinds), the amount of long-distance collected communication data from main station every day is: The data of 50×8×40×4×24×60/5=18,432,000 bytes. If encrypt every data, it will be 18432000 data. With the selective encryption algorithm proposed in this study, encrypt the active power obverse, reverse time-sharing electrical energy, reactive power four quadrants time-sharing electricity energy, only about 50×8×4×4×24×60/5 = 1,843, 200 bytes data need be encrypted. The amount of selectively encryption data is a tenth of the whole. It can improve the efficiency of electricity energy data encryption greatly, reduces the amount of data communication, enhances the efficiency of main station long-distance communication collecting.

Fast and security of encryption and decipher: In traditional encryption scheme, it usually encrypt data with DES, but it appear some effective attack method which aim at DES and encryption and decipher speed of these two kinds of encryption algorithms is slow. so symmetrical encryption algorithm AES is used in this scheme, so as to make full use of its characteristics of high security, fast encryption and decipher. Thanks to Selective Hybrid Encryption Algorithms, the amount of encryption data reduce by nine tenths, so the speed of encryption and decipher enhance greatly.

The integrality of original text and fast signature: Traditional information digest algorithm mainly base on Message Digest (MD5) Algorithm, but with the development of calculate ability and hash code analysis, security and popularity of these two kinds of algorithms drop to some extent, so a new hash algorithm----SHA-1 is adopted in this study. First change the original data into digest, it is equivalent to a fingerprint characteristic of the original data, any modification of the original data can all be detected by receive side B, so as to satisfy the demand of integrality; then the private key encryption digest of transmit side public algorithms(ECC), it can overcome the shortcoming of low speed when public key algorithm is encrypted the original text directly[5].

Security of private key: It utilize the theory of digital envelop in the course of users key transmission, encrypt symmetry private key of transmit side A by public key of receive side B, which can make up shortage of symmetry private key transmit hard. This kind of technology is very safe. combine the advantage of symmetry encryption technology (AES) and public key technology (ECC), encrypt on two levels, to get the flexibility of key technology and efficiency of the symmetrical key technology.

Secrecy: In the 4th step, the symmetry key of transmit side A is encrypted and transmitted by public key of receive side B, since nobody knows the private key of B, so only B can decipher this encryption file, so as to satisfy demand of security.

Authentication and Resisting the denying: In the last 3 steps, receive side B decipher the digital signature by the public key of transmit side A, meanwhile authenticate the file signing transmitted by A. since nobody has the private key of transmit side A, only transmit side A can create signature which can be deciphered by its public key, so transmit side A can not deny once signing the file.

CONCLUSION

Algorithms of encryption and digital signature and security protocol etc. in this study are all be chosen after compare, fully consider the characteristic of electricity energy data transmission and combine the actual conditions of the current electricity energy data transmission system, it is both superiority and feasibility. Selective hybrid encryption algorithms base on Secure Sockets Layer(SSL) protocol, organic combine, low cost of symmetry key AES algorithm, effective of dissymmetry key ECC algorithm and security of new hash algorithm SHA-1 to satisfy the request that the electricity energy data communication system to transmit the data secretly, safely and fast.

REFERENCES

1. The standard of the Ministry of Power Industry of China DL/T 645-1997. Peking: China Power Publishing Company.
2. Zhang Huan-gou and Liu Yu-zhen, 2003. Introduction of cryptography: Wuhan University publishing company.
3. Koblitz, N., 1987. Elliptic Curve Crytosystem. Mathematics of Computation, 48: 203-209.
4. Jia Jun-Mian, Wang Ji-Qing and Kong Yin-Hui, 2005. The research on text secure transmission plan in the system of electron market. Electric Power System Communication, 26: 33-35.
5. Harn L. and G. Guang, 1999. Elliptic Curve Digital Signatures and Accessories. Cryptographic Algorithms and E-Commerce. City University of H.K. Press, 126-130.
6. Alattar, A.M., G.I. Al-Regib and S.A. Al-Semari, 1999. Improved selective encryption techniques for secure transmission of MPEG video bit-streams. Image Processing, 1999. ICIP 99. Proceedings. International Conference on 4: 24-28, 256 - 260.