Smart Grid Security Situational Awareness Based on Large Data Analysis

Hesong Ye[1], Jun Xu[2], Zhijie Zhu[2]

[1]State Grid Jiangxi Electric Power Co., Ltd.Jiiujiang Power Supply Branch, Jiujiang, China

[2]State Grid Jiangxi Electric Power Co., Ltd, Nanchang, China

Keywords: distribution network communication; security; digital signature; power grid security situation

Abstract: Aiming at the security problem of message information exchange in intelligent distribution network, a security algorithm based on digital signature is proposed in this paper. An intelligent distribution network security algorithm based on public key mechanism is proposed. The unified format of message suitable for intelligent distribution network is discussed. The specific implementation method of message security for intelligent distribution network based on digital signature is studied. The performance characteristics of the algorithm are measured and analyzed on the current intelligent distribution network platform. The validation results show that the algorithm meets the requirements of communication security in intelligent distribution network and has very high practical value.

1. Introduction

Communication system is the core of operation, maintenance, control and management of intelligent distribution network. All kinds of intelligent electronic devices in distribution network realize information sharing through network interconnection to achieve safe and stable operation of the system. On the one hand, the main control station of the intelligent distribution network needs to communicate with all kinds of measuring equipment distributed in the distribution network to obtain real-time measurement and realize the monitoring of the system state. Similarly, all kinds of protection and control equipment receive commands from the main control station to realize all kinds of remote control operation, and timely remove faults to ensure system safety.

2. Security analysis

As an important part of the construction of intelligent distribution network, the basic requirements of communication security include integrity, effectiveness and non-repudiation.

Integrity: It is necessary to ensure the original information of data in order to maintain the characteristics of data that cannot be modified, destroyed or lost in the process of transmission and exchange.

Effectiveness: Refers to the information needed to prevent denial of access and ensure authorized access. When authorized entities need to access information, they can access and provide authenticated access. Denial of service, disruption of network and normal operation of system in network environment are all valid attacks. The effectiveness of communication system should consider the objective fault factors and human factors such as virus and illegal intrusion.

Non-repudiation: Strengthen the management of various acts to prevent denial of acts that have occurred or to confirm that no acts have occurred. Mainly for the emergence of security issues to provide a queriable basis and means.

Based on the security requirement of intelligent distribution network, the research on message security has been carried out in the field of distribution network. Documents [3] and [4] have studied how to add hash authentication code in message to realize the authenticity and data integrity of data sources in distribution automation communication. There are many types of intelligent electronic equipment in distribution network, which belong to different manufacturers and operation companies. Symmetric key method is widely used in the current research of information security in

  DOI: 10.25236/aisct.2019.078

distribution network, which can not realize the security of key and the certainty and non-repudiation of the source of message.

It is noted that most of the schemes proposed in the field of smart distribution network security only focus on one aspect of the information security of distribution network. It is difficult to meet the three requirements of accessibility, confidentiality and integrity of distribution network at the same time, and there is a general lack of in-depth research into the specific application of distribution network message level.

Therefore, this paper proposes an intelligent distribution network security algorithm based on public key mechanism, discusses the unified format of message for intelligent distribution network, studies the specific implementation method of message security for intelligent distribution network based on digital signature, and tests and analyses the performance characteristics of the algorithm on the current intelligent distribution network platform.

3. Digital Signature

Digital signature, also known as public key digital signature, is a digital information authentication method using public key encryption and digital digest technology, similar to handwritten signature used to prove the authenticity and validity of paper documents. The basic concept is that each user publishes a public key to verify the signature, and at the same time saves a private key to generate the signature. That is to say, the signature of the message depends on the message itself and the user's private key, and the signature can be verified by using the user's public key.

A digital signature involves a hash function value, the sender's public key, and the sender's private key. As shown in the figure, when sending a message, the sender generates a message digest from the text of the message with a hash function, and then encrypts the digest with its own private key. The encrypted digest will be sent to the receiver as the digital signature of the message and the message together, with the receiver as the head. First, the message digest is calculated from the received original message with the same hash function as the sender, then the additional digital signature of the message is decrypted with the sender's public key. If the digest is the same, the receiver can confirm that the digital signature is the sender, otherwise the message is discarded.

Digital signature adopts public key mechanism, which solves the key management problem of intelligent electronic equipment of different types and manufacturers in distribution network, and provides a basis for message security of intelligent distribution network communication network. At present, there is no uniform format for communication message in distribution network, and it is difficult to exchange information effectively in various self-defined message forms. Firstly, the message format suitable for the intelligent distribution network is studied. The message format of the intelligent distribution network should consider both universality and efficiency, so that the message can be flexibly adapted to various complex situations of the distribution network with high efficiency. Messages are composed of message receiver address, sender address, message type and length, message specific content APDU, time and security authentication code and so on. Time and security authentication code are optional, and the last position of message is placed. These two options can be ignored in distribution network messages without time record or security algorithm. It does not affect the whole message structure.

The public key mechanism of digital signature simplifies the key distribution method by adding a public key management function to the existing distribution network system. Each intelligent electronic device in the distribution network registers its own public key in the key management system of the distribution network, keeps its own private key not to leak out, at the same time, obtains the public key of the intelligent electronic device which needs to communicate in the key management system of the distribution network.

4. Algorithm and flow chart

Based on the sender of intelligent electronic equipment in distribution network, the message is

organized according to the unified format of the message in the above-mentioned intelligent distribution network. As a sender of intelligent electronic equipment, according to the requirements of the information exchange range of intelligent distribution network, by setting the receiving address in the uniform format of message in intelligent distribution network, it can flexibly transmit message information to one or more (multicast) intelligent electronic equipment.

After all the communication participants in the intelligent distribution network have determined the required password and the same elliptic curve parameters, they only need to extract the specific content of the organized message at a time, and carry out the Elliptic Curve Digital Signature Algorithms (ECDSA) for the extracted information.

For message sender: firstly, extract the specific content m in APDU segment of distribution network communication message, then use HASH algorithm, such as SHA1, to calculate the HASH value h of m, and then use the private key of sender to encrypt h to obtain the sender's digital signature s by ECC algorithm. S is filled in the frame check area of the communication message in the distribution network, the sender's digital signature process is completed, and the message can be sent to the receiver.

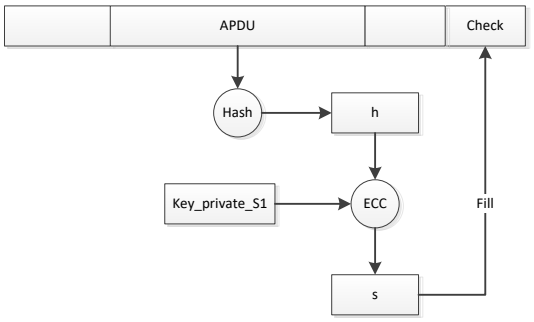

Figure 1 Digital Signature Procedure for Message Sender

For the message receiver: after receiving the communication message containing digital signatures, first extract the content M'in the APDU domain of the communication message, and then calculate the HASH value h', based on the pre-agreed HASH algorithm; then extract the content s', and decrypt the ECC content h', based on the public key. Consistent with h', the digital signature is validated.

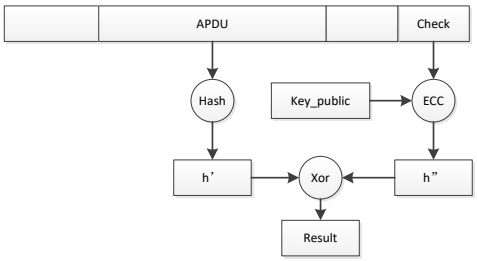

Figure 2 Digital Signature Procedure for Message Receiver

5. Example Messages and Time-consuming

In order to verify the actual performance of ECDSA algorithm in distribution network communication, this paper tests ECDSA algorithm on different intelligent electronic equipment platforms. Typical normalized telemetry message is selected as the test message. The length of the test message is 87Byte. After Hash operation, the elliptic curve digital signature algorithm is implemented. The specific time-consuming is as follows:

Table 1 Elliptic Curve Digital Signature Algorithms

	ATmega256RFR2(16MHz)	C6748(300MHz)
ECDSA sign time (ms):	555	55.59
ECDSA verify time (ms):	590	60.57

The measured delay shown in the figure above shows that the encrypting and decrypting time of ECDSA algorithm running on the same platform is comparatively close, which helps to balance the

load of intelligent electronic devices at both sending and receiving ends. The chip architecture and operating frequency of the controller used in intelligent electronic devices have a great influence on the time-consuming of the algorithm. The total time consumed by this algorithm is about 116ms on the C6000 series DSP platform, which can meet the real-time requirement of general information exchange in intelligent distribution network.

6. Conclusion

Aiming at the security problem of message information exchange in intelligent distribution network, a security algorithm based on digital signature is proposed in this paper. Based on hash function and asymmetric encryption algorithm with the strongest security performance under certain key length, elliptic curve digital signature algorithm can effectively guarantee the integrity, validity and non-repudiation required by the security of distribution network communication. After proving the security and validity of the algorithm, the proposed security algorithm is verified on the embedded platform. The verification results show that the algorithm meets the requirements of the security of distribution network communication, and has a very high practical value for ensuring the increasingly severe security of distribution network communication.

References

[1] Yijiu Zhao, Shuangman Xiao. Sparse Multiband Signal Acquisition Receiver with Co-prime Sampling, IEEE Access. vol.6, pp. 25261-25269, 2018.

[2] Hanxin Chen,Yunfei Shang,Kui Sun, Multiple fault condition recognition of gearbox with sequential hypothesis test, Mechanical system and signal processing, 2013, Vol.40, pp.469-482.

[3] He, Yi-Bin; Zeng, Ya-Jun; Chen, Han-Xin; Xiao, San-Xia; Wang, Yan-Wei; Huang, Si-Yu, Research on improved edge extraction algorithm of rectangular piece, International Journal of modern physics C, 2018,Vol.29(1), DOI: 10.1142/S0129183118500079.

[4] Liu Yang, Hanxin Chen, Fault diagnosis of gearbox based on RBF-PF and particle swarm optimization wavelet neural network, Neural computing and applications, doi.org/10.1007/s00521-018-3525-y.

[5] Zeng, Li; Shi, Jun; Luo, Jingli; Chen, Hanxin. Silver sulfide anchored on reduced graphene oxide as a high -performance catalyst for CO2 electroreduction，Journal of Power Sources, 2018, Vol.398, pp.83-90.

[6] D. Zhou, A. Al-Durra, K. Zhang, A. Ravey, F. Gao, “Online Remaining Useful Life Prediction of Proton Exchange Membrane Fuel cells using a Novel Robust Methodology,” Journal of power sources, Vol. 399, Issue. 30, Pages 314-328, 2018.