Application and Implementation of The Grounding Wire Information Management System Based on SM2

To cite this article: Jiajun Liu and Xueli Liu 2019 J. Phys.: Conf. Ser. 1168 062035

View the article online for updates and enhancements.
Application and Implementation of The Grounding Wire Information Management System Based on SM2

Jiajun Liu\(^1\) and Xueli Liu\(^1,a\)

\(^1\)Institute Of Water Resources And Hydro-Electric Engineering, Xi’an University of Technology, Xi’an, Shanxi, 710048, China

\(^a\) Corresponding author: 18292064383@163.com

Abstract. The intelligence and automation of grounding wire information management are improved by the grounding wire management system based on network communication in maintenance of catenary, but the security problem of information transmission existed in this system. For this reason, the SM2 algorithm is used to digitally sign the grounding wire information, and ensure it can not be tampered and non-repudiation. Under the C/S architecture, the grounding wire information management system with digital signature technology is established. The server realizes the information interaction between the grounding wire monitoring unit and the client. The client visually displays the status, location, and picture information of the grounding wire through the visual interface. The results show that the application of the SM2 digital signature technology for the grounding wire information management system insure the security of the grounding wire information.

1. Introduction

The catenary is a unique transmission network that supplies power to electric locomotives. And it is of no standby, complicated structure and outdoor layout[1], so it needs to be routinely overhauled to ensure safe and efficient operation of electric locomotives. In order to ensure the safety of workers and electrical equipment during the maintenance work of the catenary, it is essential to hang the grounding wire. Due to the manual reporting method used to monitor grounding wire in the maintenance of catenary at present, the method is cumbersome, complicated, inefficient, and prone to error, resulting in frequent safety accidents[2]. Liu et al.[3][4] used the GSM/4G communication technology to transmit the grounding wire information collected by the grounding wire monitoring unit, and the information is monitored, processed, and managed by the client in real time. The grounding wire management system based on network communication improves the intelligence and automation of grounding wire information management in maintenance of catenary. However, if the information illegally tampered by the third-party equipment during network transmission, the correctness of the grounding wire information monitored by the system cannot be guaranteed, which may still cause serious accidents such as the mistaken hanging, leakage hanging and leakage removing for grounding wire.

Therefore, the grounding wire information management system based on SM2 digital signature technology is established in the present paper, and the communication protocol is redesigned, as well as the management system is implemented under the C/S architecture, to ensure the secure transmission of grounding wire information.
## 2. Overview

The structure schematic diagram of the grounding wire information management system in catenary maintenance is shown in Figure 1, and it includes hardware and software parts.

![Figure 1. The structure frame of system](image)

The hardware part adopted the grounding wire monitoring unit based on 4G network communication introduced in Ref[5], which collects information through the GPS positioning module, the ultrasonic ranging module and the image acquisition module, and which uses 4G network communication technology to realize the transmission of status information, location information and image information for grounding wire. The software part is composed of the grounding wire management system base on the C/S architecture. The server realizes the information interaction between the grounding wire monitoring unit and the client, and accesses the data by operating the database. The client visually displays the status, location, and picture information of the grounding wire through the visual interface.

## 3. Application of SM2 digital signature technology

### 3.1 Overview of SM2

SM2 is an elliptic curve public key cryptography algorithm issued by the State Cryptography Administration in 2010 base on the ECC (Elliptic Curve Cryptography) algorithm, including a set of digital signature algorithm and public key cryptography algorithm[6]. As an asymmetric encryption algorithm, it adopts a more secure mechanism compared with the ECC. And it has shorter key string, faster encryption speed and higher efficiency under the same encryption strength compared with RSA[7][8]. Meanwhile, the SM2 algorithm can effectively avoid the backdoor trap problem that may exist in the international classic security algorithm. The schematic diagram of SM2 digital signature technology is shown in Figure 2.

![Figure 2. The schematic of SM2 digital signature technology](image)
3.2 Application of SM2 digital signature technology

The communication message in the grounding wire information management system is required to reflect all the services of the grounding wire monitoring unit. According to the characteristics of the grounding wire information, the communication message of this system adopts data frame mode. The protocol includes frame head, frame length, data type, data block, digital signature and frame trail.

Combined with the above-mentioned communication protocol and SM2 digital signature technology, the grounding wire monitoring unit implements the signature function, and the client implements the verification function. In the SM2 digital signature, the private key is $d_A$, the public key is $p_A$, the cryptographic hash function is $H_v$, and the hash value is $Z_A$. When the grounding wire monitoring unit sends the ground line information, firstly, the data type and data block should be extracted from the original message to be signed, and record them as signature to be signed $M$. Secondly, the $d_A$ is used to digitally signed the $M$, and then the generated digital signature $(r, s)$ is attached to the digital signature in the original message. Finally, the frame length is updated after generating digital signature, and form a composite message with the digital signature and send the composite message to the client. Therefore, in the grounding wire information management system, the specific flow chart of the generation algorithm for SM2 digital signature is shown in Figure 3.

![Figure 3. The signature generation algorithm](image)

When the receiving end receives the composite message from the grounding wire monitoring unit, firstly, the received information $M'$ and the to-be-verified signature $(r', s')$ are extracted according to the frame length in the communication protocol. Secondly, the public key $p_A$ and $s'$ are used to regenerate the signature $R'$ for the $M'$. If $R'=r'$, the signature verification is successful; otherwise, the verification failures, that is, the sender belongs to an unknown source or the communication message has been tampered with. In the grounding wire information management system, the specific flow chart of the verification algorithm for SM2 digital signature is shown in Figure 4.

The grounding wire information management system adopts SM2 digital signature technology, which can achieve security objectives such as information source confirmation, information integrity verification and non-repudiation, and can effectively prevent third-party from maliciously tampering with the grounding wire information.
4. The implementation of system

4.1 The function modules of server

According to the overall design of the grounding wire information management system, the server is the communication intermediary between the grounding wire monitoring unit and the client, and its main functional modules include the monitoring unit communication part, the client communication part, and the database interaction module. The diagram of function modules for the server is shown in Figure 5.

The server listens to the special port and receives the grounding wire information with digital signature sent by the grounding wire monitoring unit. Firstly, digital signature verification is performed. Secondly, different data blocks are split, decoded and restored according the data type after verification passed, and then interacts with the database to classify and store information into the corresponding data table. At the same time, the server sends corresponding response to the monitoring unit for different data packets, and response as a feedback to achieve closed-loop monitoring. The analysis algorithm of the server for the grounding wire information is shown in Figure 6.

A long connection between the server and the client is established and maintained. After splitting the grounding wire information, the multi-threading technology is used to synchronously push it to the client for visualization display in real time.

Figure 4. The signature verification algorithm
4.2 The function modules of client

In the grounding wire information management system, the client mainly realizes the functions of visual display of grounding wire information, data viewing and safe power transmission detection. The diagram of function modules for the client is shown in Figure 7.

Except for the attribute information of catenary, the grounding wire information also contains...
spatial location information, such as the position of the tower and the line. Therefore, Baidu map and MapXtreme can be used to bind the spatial data to attribute data[9], so that one can manage the catenary grounding wire in a visual geographical background. The visual display of the status information for the grounding wire by MapXtreme, and the visual display of the location information for the grounding wire by the Baidu map in the client. It is shown in the Figure 8.

Figure 8. The visualization of status and location information

When the maintenance of catenary is completed, the working status of all the grounding wires that collected by the client in the section is counted to determine whether the safe power transmission requirement is met before one issue the power transmission order. If there are still grounding elements on the electronic map, that is, there are grounding wire still hang on the scene, the tower number corresponding to the grounding elements is obtained. The main interface pops up the window and prompts the alarm, sends a warning message to the person in charge of the work site, and arranges the staff to check the grounding wire state of the corresponding tower. The specific algorithm is shown in Figure 9. The detection provides an effective basis for safe power transmission, which can avoid major accidents such as power transmission with grounding wire.
5. Conclusion
In this paper, aiming at the possible security problems in the information transmission of the grounding wire information management system based on network communication, a grounding wire information management system which is based on SM2 digital signature technology is established under the C/S architecture. In addition, combined with the current technical means, this system realizes the whole-process visual monitoring of the grounding wire in the maintenance operation by virtue of baidu map API technology and MapXtreme technology, which is more compatible with the daily management requirements of the grounding wire. By testing, the grounding wire information management system has good application effect and higher security, which can guarantee the information security in network transmission, and has certain application prospect and engineering value.

References
[1] Hongcai Liu. Research on the improvement of catenary maintenance mode. China Academy of Railway Sciences.(2016)
[2] Lijuan Yang, Zhouxun Lu. Remote monitor system of the power earth lines status based on GSM network. Control & Automation, 09:149-150(2005)
[3] Jiajun Liu, Mengna Liu, Yuan An. Design and implementation of grounding wire networked information management system based on GIS in overhead contact system maintenance operation. Power System Protection and Control, 44(07):134-139(2016)
[4] Kai Zhang. The research of the grounding line management system of catenary operation based on internet. Xi’an University of Technology.(2018)
[5] Jiajun Liu, Rui Wang. The research of grounding wire monitoring device of contact network based on 4G communication. Power System and Clean Energy, 34(02):17-22 (2018)
[6] Zhao Luo, Jihua Xie, Wei Gu. Development of power grid information security support platform based on SM2 cipher system. Automation of Electric Power Systems, 38(6):68-74 (2014)
[7] Walter, Colin D. Simple power analysis of unified code for ECC double and add. International Workshop on Cryptographic Hardware and Embedded Systems, 3156:191-204 (2004)
[8] Zhao Luo, Tong Yan, Jihua Xie, Junpeng Zhu. Application of SM2 encrypted system in telecontrol communication for smart substation. Automation of Electric Power Systems, 40(19):127-133 (2016)
[9] Bin Yang, Xiumei Gu. Research and application of water resources optimal scheduling management based on GIS. IEEE International Conference on Waste Recycling, ecology and Environment, 848-851 (2011)