Information security defense method of electric power control system based on digital watermark

Chao Zhou, Yajuan Guo, Wei Huang, Haitao Jiang, Bin Li, Jinming Chen

State Grid Jiangsu Electric Power Research Institute, Nanjing 210000, China

Keywords: Cyber attack; Cyber security of power system; Verification based on digital watermark technology

Abstract: This paper presents a network attack authentication method based on digital watermark technology, CRC16 as watermark is added to the original data, combined with the simulation model of the method of performance analysis. It is proved that the method can detect false data in real time conditions, provide a new choice for information security. At the same time, the performance of digital watermarking is analyzed in detail through simulation, and the feasibility and superiority of the method of real-time data protection based on the watermark is further demonstrated. The current and voltage are obtained by the simple simulation model, and the current and voltage waveforms are almost coincident with the embedded watermark. Taking the impedance locus of distance protection as an example, it is observed that the embedding of digital watermark does not affect the normal operation of relay protection. This method provides a new way of thinking for the security protection of power information network, especially for digital and intelligent power system.

1. Introduction

Power system is a complex large nonlinear dynamic system. In modern society, all social activities and economic production are more or less with the power system associated, the modern grid electric energy production, transmission, distribution process accompanied by the uncertain factor for a large amount of information transfer, failure loss, power recovery [1]. Power system can be safe and stable operation of the relationship to the very serious social problems, and ensure safe operation of the power system is not only helpful to the improvement of the electric power enterprise's own profits, but also conducive to the normal operation of the whole national economic system [2-4].

Safety production and management is the core of the problem of power system security, in order to protect the power system production, safe management, we must a system master side can nip in the bud, risk problem in the final analysis is of various risk sources of power system caused by the influence of all kinds of risks exist in the power system. According to the definition of 1335-2004 ISO/IEC, risk is a designated threat, the use of an asset or a number of assets of the vulnerability, resulting in the possibility of damage or destruction of assets [5-7]. This definition gives the two most important aspects of the study of risk, namely, the probability of an event and the outcome of the event (damage or damage).

In view of the adverse effects of network attacks on power system control system, it should take the initiative to explore ways to mitigate or prevent the role of network attacks [8]. Power system mostly realizes the remote control and the communication between the main station and sub stations is critical and frequent cyber attacks will to power communication network caused great pressure, how to guarantee the security of data communication has been neglected [9-11]. This paper discusses the data transmission security of digital substation based on, how to improve the security of data transmission in the framework of the IEC61850 is the focus of discussion in this chapter, in view of the IEC61850 defines the protection mechanisms are transparent, easy to attack [12]. Author from the point of view of encryption of proposed a based on digital watermarking of real-time data transmission check method, this method has good real-time performance, high reliability and difficult to be found many advantages [13]. The simulation results show that is a feasible to deal with network attack power grid real-time data transmission scheme [14].

2. Data authentication based on digital watermarking

Conventional encryption algorithm is powerful and reliable, and has very rich in practical application, but because of the particularity of the digital substation data transmission protocol, transmission frame in each phase current and voltage acquisition amount takes up only a 16 bit data space, and each frame of data transmission time interval is very short, and does not allow occupy a bit more common encryption system, combined with encryption, decryption time is unable to meet the real-time requirement, the real-time data transmission encryption poses a great challenge. This paper proposes a digital watermarking algorithm based on digital watermarking, which can meet the requirements of real-time, reliability and so on. Digital watermarking technology is a technology of information hiding, he is through in the carrier (pictures, documents, etc.) and with recognition of identification information (digital watermarking) to achieve the identification of convenience.

3. Digital watermarking based on error correcting code

The hidden digital watermarking technique is a key method, what algorithm does not have substantial effects on the method, the digital watermarking is opaque, hidden in the original data, it will not affect the data are not vulnerable to the fact that attack. The algorithm though there will be a substantial effect, but the algorithm for computing the consuming time of the whole digital watermarking scheme has certain influence on the performance, algorithm for computing more rapidly, occupied memory space smaller will be more a conducive to enhance the performance of the proposed scheme. Data validation algorithm is not only the IEC61850 in the cyclic redundancy check (CRC) codes, including parity code and Hamming code and variety. Considering the various factors, the article also uses the CRC as the digital watermarking algorithm. The advantage of CRC is that it can detect the abrupt change of data bits at a low price, or the change of bit sequence. In short, it can be effectively detected if there is a change in the data bits. Unfortunately, this algorithm also has many defects, such as he and not error correction, only error detection alarm; secondly lack of authentication mechanism, any attacker also tamper protection data and CRC itself, to end and can't find any abnormality. CRC algorithm is not a one-way algorithm, so it can not be used as a digital signature. However, the CRC algorithm is simple and time consuming, and it has satisfied the requirement of this scheme, and it is a very mature algorithm, which has good stability. In this paper, the advantage of digital watermarking to make up the CRC of many defects, usually the attacker does not find the hidden CRC check code, and will be treated as a common data encoding.

4. Numerical simulation

4.1 Simulation setting

The simulation analysis of the outlet of 220kV substation is carried out. The lateral impedance of the power supply: 0.2+j4.5Ω; Line parameter settings are as follows: R1=R2= 0.027Ω/km, L1 = L2 = 0.86mH/km, C1 = C2 =0.0123μF/km; R0 = 0.1948Ω/km, L0 = 2.4mH, C0 = 0.0071μF/km. Bus exit at different distances of the single-phase, two-phase, three-phase short-circuit grounding, a unified set of 80 millisecond time to produce a fault, the simulation of the current and voltage waveforms drawn as shown in Figure 2 and figure 3. For the convenience of calculation, below with a photograph of initial sampling value 411.1664A, 121678.634V as an example, describes the specific implementation process of the watermark, and analysis add watermark verification code of the original data value caused by the error, or the analysis of the performance of digital watermarking algorithm.

Sending values for normal circumstances to end should be received, as shown in Figure 1, *A* process said current 269A add digital watermarking process, B said voltage 18123V add digital watermarking process. They respectively represent the method to add two kinds of digital watermarking algorithm in the extreme, the CRC1 and CRC7. B water prepress absolute error is 36V, the relative error is 0.1986% and transmitted to the second device conversion to the actual use of the range value to the original value of the absolute error for 147.705V, 0.15KV and relative error for 0.1214%, and a process more is 0 error phenomenon, visible watermark caused the error is very small, almost can be neglected.

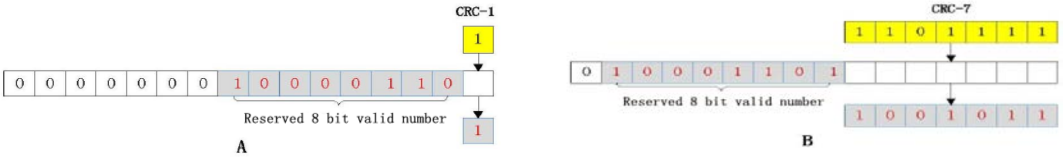

Fig. 1 An example of implementation process based on digital watermarking algorithm

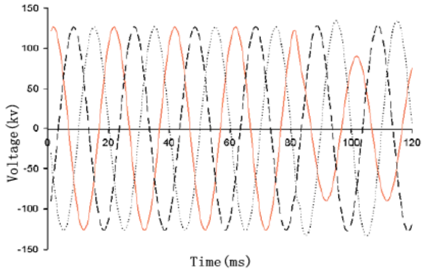

Fig. 2 A phase to ground short circuit simulation voltage waveform

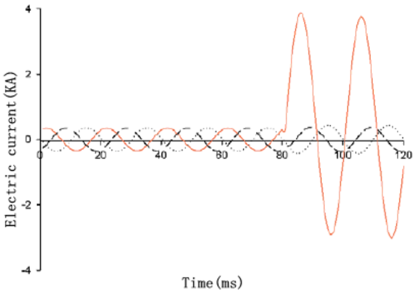

Fig. 3 A phase to ground short circuit simulation current waveform

As shown in Figure 2-3, A phase of single phase short circuit simulation waveforms of the voltage and current, vision without any difference and achieve the ideal effect of hiding and more fully shows that a malicious attacker undetectable communication data anomalies, therefore, to the digital watermarking hiding check of power electronic transformer data acquisition, if the check algorithm to select the appropriate, can achieve the desired effect.

Data transmission is based on binary coding, so the error caused by the digital watermark embedding of the original data is obvious and the original data size, the greater the raw data, watermark sequence is small, the error caused by the original data is smaller. In order to increase the influence of the watermark on the original data analysis, this paper also simulated the two cases of A/B two-phase grounding and A/B/C three-phase grounding, and observed the performance of digital watermarking under different conditions.

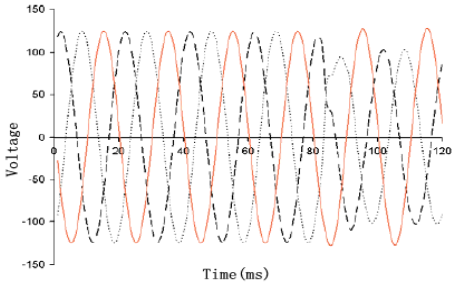

Fig. 4 Simulation voltage waveform of A/B two phase earth fault

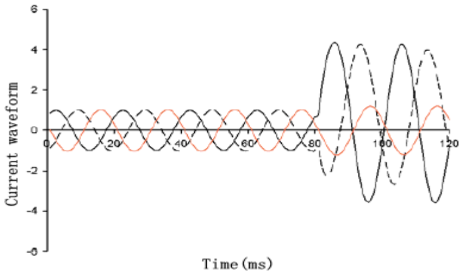

Fig. 5 Simulation current waveform of A/B two phase earth fault

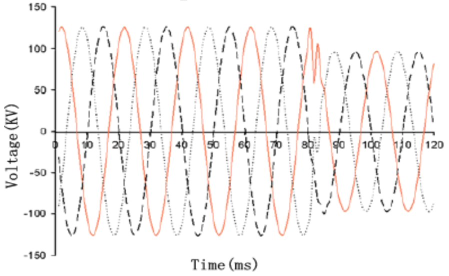

Fig. 6 A/B/C three phase grounding short-circuit simulation voltage waveform

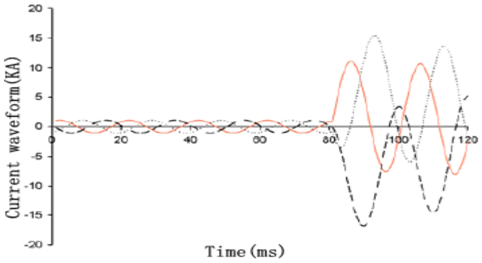

Fig. 7 A/B/C three phase grounding short circuit simulation current waveform

4.2 Digital watermarking efficiency analysis

In the simulation of the current, the voltage on the 8 bit keep the watermark to retain the relative error of the watermark, the signal is shown in Figure 8 and 9.

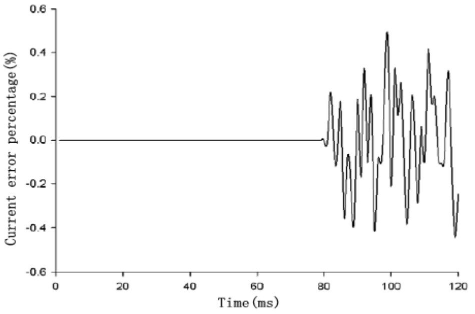

Fig. 8 Digital watermarking introduces the relative error of current data (A phase to ground fault)

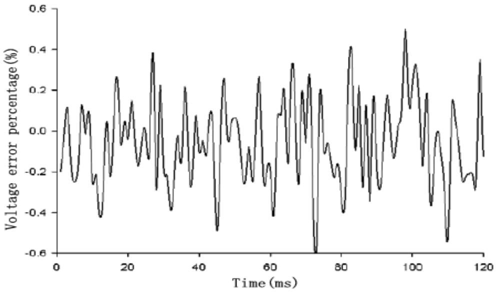

Fig. 9 Digital watermarking is introduced to the relative error of voltage data (A phase to ground fault).

Figure 9 and 8 are the voltage and current error caused by the watermark in the single phase to earth fault. By figure visible, A phase failure occurs, the current transformer output amplitude only 200 A, which converted into binary within the range of the current transformer is inadequate number of 8-bit effective bits, and non watermarked; After 80 milliseconds, the occurrence of a fault began to by watermarking the error introduced. Figure 13 - 10 is the A/B, A/B/C in two cases of the current, voltage to add a watermark after the error range.

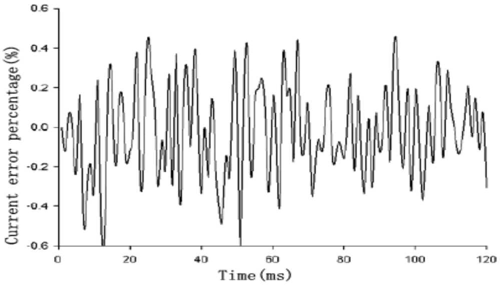

Fig. 10 Digital watermarking introduces relative error of current data (A/B two phase earth fault)

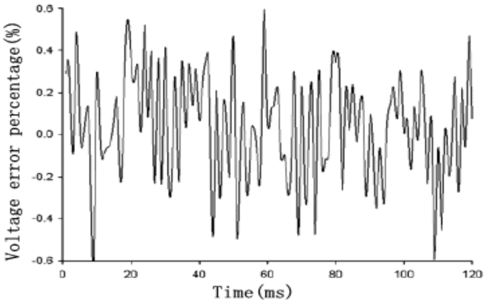

Fig. 11 Digital watermarking introduces relative error of voltage data (A/B two phase earth fault)

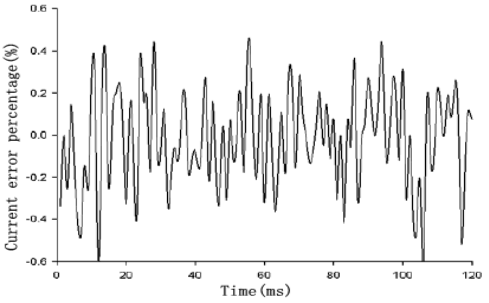

Fig. 12 Digital watermarking introduces relative error of current data (A/B/C two phase earth fault)

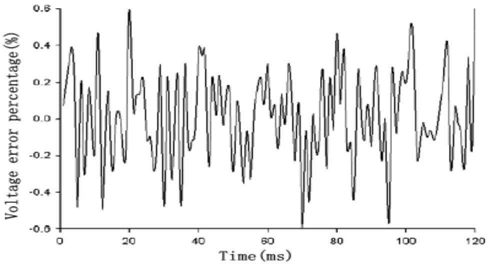

Fig. 13 Digital watermarking introduces relative error of voltage data (A/B/C two phase earth fault)

Microcomputer protection system is the key system to ensure the reliable operation of power system. IEEE Power System Relay Protection Committee issued a research report comprehensive systematically expounds the relay protection information security issues, this section to microcomputer distance protection analysis object, in a phase short circuit's simulation results based on, explore the performance of digital watermarking. According to the actual simulation results, the current and voltage data of the embedded watermark and the current voltage data of the watermark can be calculated to obtain the measured impedance at all times, and the connection line is drawn into the impedance locus. Visible from the figure, the two kinds of measurement impedance trajectory is difficult to detect some slight differences in the naked eye. In order to show the fine degree of the difference more intuitively, the impedance locus is enlarged into the stable region and the upper right corner of Figure 14 is enlarged. Visible from the graph, even if it is not visible to the embedded watermark in the impact of the impedance locus, it can be inferred that the 8 bits embedded in the premise of the watermark does not have a significant impact on the performance of distance protection.

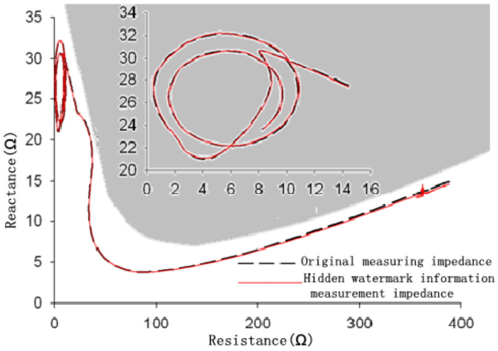

Fig. 14 Comparison of measured impedance locus

5. Conclusion

With the popularization and application of computer and network communication technology in power system, network attack will gradually become the number one threat to the power system. In recent years consecutive LAN attacks on sensitive infrastructure, network information usually data reflected, security number according to the secure communication is a very important work. This paper presents a network attack authentication method based on digital watermark technology, choose the CRC16 as watermark is added to the original data, combined with the simulation model of the method of performance analysis. It is proved that the method can detect false data in real time conditions, provides a new choice for information security. At the same time, the performance of digital watermarking is analyzed in detail through simulation, and the feasibility and superiority of the method of real-time data protection based on the watermark is further demonstrated. The current and voltage are obtained by the simple simulation model, and the current and voltage waveforms are almost coincident with the embedded watermark. Taking the impedance locus of distance protection as an example, it is observed that the embedding of digital watermark does not affect the normal operation of relay protection. This method provides a new way of thinking for the security protection of power information network, especially for digital and intelligent power system.

References

[1] Massimino P. System and method of adding a watermark to a JPEG image file: , US 8989432 B2[P]. 2015.

[2] Hou J U, Ji S K, Lee H K. Fast Watermark Synchronization Based on Complementary Templates[J]. Journal of Computer & Communications, 2014, 02(04):58-65.

[3] Qin J, Shi J, Sun C. Communication Scheme Selection of Distribution Automation System for County Distribution Grid. Jiangsu Electrical Engineering, 2014, 33: 44-47.

[4] Yan A, Pei C, Zha S, Qin H. Analysis of Jiangsu Distribution Automation Planning. Jiangsu Electrical Engineering, 2015, 34: 35-38.

[5] Radouane M, Nadia I, Rochdi M, et al. A Method of LSB substitution based on image blocks and maximum entropy[J]. International Journal of Computer Science Issues, 2013, 10(1).

[6] Eschbach R, Maltz M S, Chapman E. Method of creating non-patterned security elements: US, US8928948[P]. 2015.

[7] Delp E J, Lin E T. Synchronization of digital watermarks: US, US8370635[P]. 2013.

[8] Bitaghsir S A, Karimi N, Azizi S, et al. Stereo image watermarking method based on binocular just noticeable difference[C]// Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on. IEEE, 2014:33-38.

[9] Su S, Wang Y, Long Y, et al. Cyber attack impact on power system blackout[C]// Reliability of Transmission and Distribution Networks (RTDN 2011), IET Conference on. IET, 2011:1-5.

[10] Mcmillin B. Complexities of information security in Cyber-Physical Power Systems[C]// Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES. IEEE, 2009:1-2.

[11] Sgouras K I, Birda A D, Labridis D P. Cyber attack impact on critical Smart Grid infrastructures[C]// Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES. IEEE, 2014:1-5.

[12] Zhang Y, Wang L, Sun W. Investigating the impact of cyber attacks on power system reliability[C]// Cyber Technology in Automation, Control and Intelligent Systems (CYBER), 2013 IEEE 3rd Annual International Conference on. IEEE, 2013:462-467.

[13] Kundur D, Feng X, Liu S, et al. Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid[C]// Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on. IEEE, 2010:244-249.

[14] Bruno C, Guidi L, Lorite-Espejo A, et al. Assessing a Potential Cyberattack on the Italian Electric System[J]. IEEE Security & Privacy Magazine, 2015, 13(5):42-51.