Send Orders for Reprints to reprints@benthamscience.ae

Digital Watermark based Authentication for Intrusion Detection of Digital Substations

Zhao Ming and Sun Qiangqiang*

Shenzhen Power Supply Co., LTD, Information Department. Shenzhen, Guangdong, 518200, China

Abstract: The paper proposes the use of digital watermark based authentication for intrusion detection in IEC 61850-automated substations. The watermark can be embedded into the Least Significant Bits of the measurements without visible deterioration in precision. When Intelligent Electronics Devices gets measurements, the watermark in the measurement can be retrieved to determine whether it has been attacked and detect malicious intrusion. The proposed approach is appropriate for the time critical and resource constrained applications in substation automation system for its simplicity. Numerical simulation shows that the process latency and error incurred by watermarking is acceptable and will not impact performance of protective function in IEC 61850 automated substations.

Keywords: Digital watermark, intrusion detection, substation automation system.

1. INTRODUCTION

With the development of communication and information technology over past decades, broadband communication network has been prevalent in power systems. This moves automation networks from proprietary, closed networks to the more current area of Information & Communication Technology. The monitoring and controlling of the electric power infrastructure have migrated from classic isolated automatic systems to a network based automatic system [1]. The risk of cyber attack increases since the applications toward the usage of standardized components has broken down inherent security barriers that earlier created by proprietary solutions [2].

As critical installations in the electric power grid, electric substations are a prime target for malicious activity [3]. Unlike traditional substation automation system (SAS) where Intelligent Electronic Devices (IEDs) are hardwired linked to implement data acquisition and carry out their function, development of electronic instrument transformers (EITs) and prevalence of communication and information technology have led to a revolution in SAS using IEC 61850 protocol. Impact of potential attack scenarios and its countermeasures are evaluated in [4]. Since tripping signal and outputs of EITs (current and voltage measurements) are transmitted as numerical signals via broadband communication network in IEC61850 automated substations [2-4], the risk emerges in a form that a fake tripping signal or measurements accepted by protection system could lead to mis-operation.

In order to harden the IEC61850 automated substation against cyber attack, various approaches have been elaborated. The security domain and user management mechanism are adopted in IEC 61850 protocols to prevent unauthorized access and mitigate the potential impact of a successful intruder [5]. Since the highly intelligent malware, like stuxnet, could infect the physical isolated computer networks via USB drive [6], the second line of defense, intrusion detection system (IDS) is highly preferred [7]. ID is the process of monitoring the events occurring in a computer network to detect the malicious intruder, and hence, attempting to stop detecting possible incidents. A basic premise for intrusion detection is that when audit mechanisms are enabled to record system events, distinct evidence of legitimate activities and intrusions will be manifested in the audit data [7]. Because of the large amount of audit records and the variety of system features, various statistics or machine learning based intelligent algorithm have been developed to analysis and detect the anomaly efficiently [8, 9]. Since various data (such as relay setting, user credentials and application logs, traffic logs, and measurements) within a substation and among neighboring substations are temporal and/or spatial correlated, the feature could be utilized to detect anomaly within a substation or supervisory control and data acquisition (SCADA) in an efficient way [10, 11]. However, the protection of very-high-speed message such as tripping signal and (current and voltage) measurements are significantly different from the other for their stringent latency requirement. Since these real time data should be transmitted in normally less than 2 ms and be processed as soon as possible [12], the fake data sent by an intruder could cause unwanted operations of protective devices before it is identified by the IDS.

One-time authentication signature, which can dramatically decrease the signing and verification times, has been

1874-1290/14

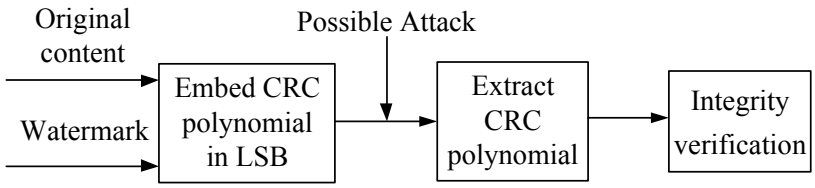

Fig. (1). Data process procedure.

proposed to guarantee integrity of sensitive data in electric power system [13]. With billions of one time signature stored in flash memory, the security of this scheme is independent of computer power and fits for resource constrained applications of IEDs, such as relays, RTUs, reclosers, PLCs, meters, and etc [14]. Moreover, once one time signature scheme is combined with IDS, attack on the authenticated data could be detected as anomaly, and hence, enhances performance of IDS. However, application of one time signature on measurements is not as desirable as on tripping signal due to reason as follows. Since measurements are sent at a frequency much higher than the tripping signal, it is difficult to implement precise synchronization of authentication signature between the sender and the receivers. Moreover, attaching 32 bits signatures on the former will increase communication load notably and sacrifice performance of communication. While attaching a 32 bits signatures on a tripping signal will have slim impact on an IEC61850 automated substation. Therefore, efficient and effective approach way to guarantee integrity of measurements is highly preferred. In [2], pattern identification based approach using probabilistic neural network is proposed to detect the fake malicious measurements online. In order to enhance precision and reduce process latency, similar approach such as evidence theory [15], support vector machine [16], and orthogonal least square based radial basis function neural network [17] has been investigated. However, these methods could not satisfy both latency and generalization requirement since state space complexity increases substantially for substations with complex diagram.

In order to guarantee the integrity of measurements in IEC61850 automated substations, a digital watermark based authentication for measurements of IEC 61850 automated substations is proposed in this paper. The paper is organized as follows. The watermark based authentication is introduced in Section 2. An error detecting code based watermark is developed in Section 3. Simulation configuration and Numerical simulation are given in Section 4. Section 5 concludes the paper.

2. DIGITAL WATERMARK BASED AUTHENTICATION

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, atop a dark background), caused by thickness or density variations in the paper [16]. Watermarks are commonly used as security features of banknotes, passports, postage stamps, and other documents to prevent counterfeiting. Digital watermark is similar to its predecessor. A watermark is embedded into a covertext (the digital contents to be protected), resulting in a watermarked signal called stegotext, which has no visible difference from the covertext [17]. The procedure of digital watermark can be described as Fig. (**1**).

The watermark can later be detected or extracted for the purpose of owner or author identification and integrity verification of tested data. The authentication process inserts a watermark into a digital content to produce a watermarked digital content. When the watermarked content is possibly attacked, authentication/verification process retrieves the embedded watermark. It is examined and compared with the watermark originally embedded into the digital content. If it is not identical to the original watermark, the watermarked digital content is determined to have been attacked.

The application of digital watermark is very broad. It is most frequently embedded into multimedia (audio, images, and video, etc.) By preserving perceptual quality of watermarked data for content authentication. A large variety of digital watermark algorithms utilizing spatial or frequency domain characteristics of multimedia data have been developed. Among them, Least Significant Bit (LSB) based watermark proposed in [18] is one of the most frequently used techniques. The watermark could be embedded in to the LSB of image pixels and the invisibility of the watermark is achieved since the LSB data are visually insignificant [19, 20]. The LSB based watermark can be utilized to authentication of measurement in IEC 61850 automated substations. The strategy seeks to embed the watermark in the least significant bit of the original measurement to provide an imperceptible watermark.

3. ERROR DETECTING CODE BASED WATERMARK

3.1. Digital Watermark of EITs' Measurement

The output of Electronics Current Transformer (ECT) and Electronics Voltage Transformer (EVT) are 2 bytes signed integer [21]. The first bit is the sign bit and the maximum Effective Number of Bit (ENOB) used for measurements is 15.

The output of protective ECT with rated current 200 ampere is 01CFH (decimal 463) [22] and the LSB of the current denotes 200/463=0.4320 ampere. Max output of protective ECT is 215 × 200 / 463 = 14.155kA, correspondingly. Output of EVT with rated voltage 220kV is 2D41H (decimal 11585) [14] and the LSB of voltage denotes 220000 / 11585=18.9901V. Max output of ECT is 2^{15} × 2.1598 = 622.267kV, correspondingly [15].

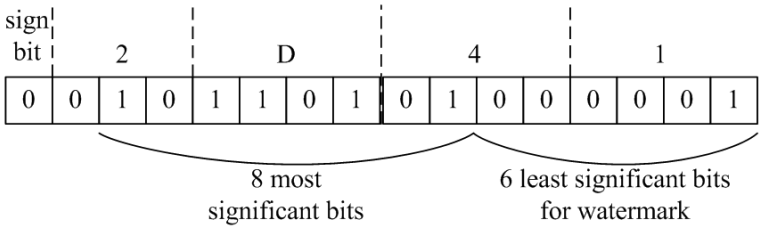

Fig. (2). Watermarked measurement of EVT with rated voltage.

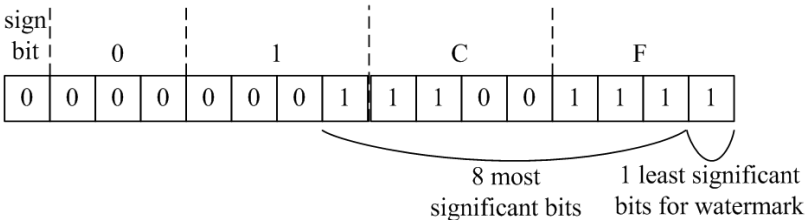

Fig. (3). Watermarked measurement of protective ECT with rated current.

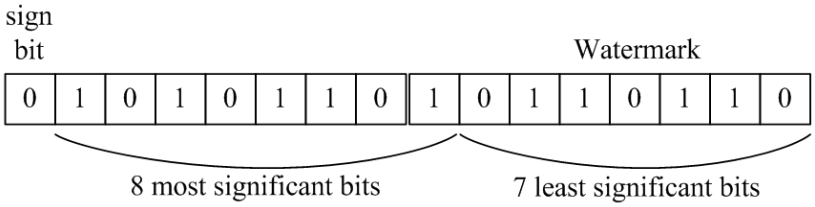

Fig. (4). 2 bytes watermarked measurements.

The percentage voltage (ratio) error of EVTs with class 1 and class 3 are ±1% and ±3% [22]. The ratio error of ECT with class 1 and class 3 are ±1% and ±3%, too. The accuracy of measurements is determined by the ENOB while the leading most significant bits (MSBs) play a more important role as compared to the least significant bits. Therefore, it is reasonable to embed watermark in the LSB. If the most significant 8 bits are preserved and the other LSBs are used for watermark as showed in Fig. (**2**), the max error incurred is $1/2^8 = 0.391\%$. For the watermarked measurement of EVT with rated voltage shown in Fig. (**2**), 6 least significant bits can be used for watermark. For the watermarked measurement of protective ECT with rated current shown in Fig. (**3**), only 1 least significant bit can be utilized to watermark. While when the primary system operates with short circuit fault present, at most 7 least significant bits can be used for watermark as showed in Fig. (**4**).

In the LSB scheme based application of the multimedia data, the watermark is usually one pseudo random sequence generated with encryption/decryption algorithm [18]. However, this is not appropriate for the computation resource constraint time critical application in IEC61850 automated substations [21].

3.2. Error Detection Code Based Watermark

Error detection code has been frequently used for error control in data communication. It uses the concept of redundancy, which means adding extra bits for detecting errors at the destination. These codes can detect single or multiple bit errors in the transmission of the data packet and are extremely helpful for detecting errors caused by electrical noise and other transmission errors. There are 3 types of redundancy checks are common in data communication.

- Parity check;
- Cyclic Redundancy Check (CRC)
- Checksum.

CRC proposed by Peterson, W. W. [22], is a single-burst-error-detecting cyclic code designed to detect accidental changes to digital data in computer networks. It is particularly easy to apply in hardware**,** therefore it is most frequently used in computation resource constraint and time critical application such as digital networks and storage devices to detect accidental changes to raw data. CRC code has been widely appended to the data packet transmitted in SAS and SCADA to ensure message integrity in the face of potentially noisy communication channels [21]. In this paper, it is inserted in the LSBs as a watermarked signature to ensure data integrity of MSB that has much significant impact on the value of the measurement. The procedure of CRC based authentication can be presented as Fig. (**5**).

Detailed discussions of CRC can be found in [22]. For the sake of completeness, we present a brief overview together with Fig. (**5**).

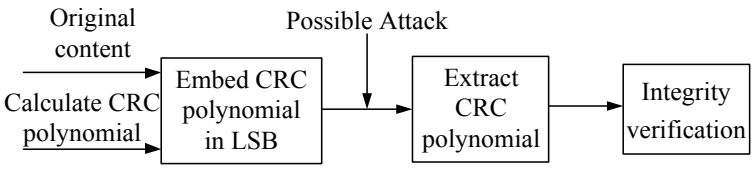

Fig. (5). Procedure of data authentication using CRC based watermark.

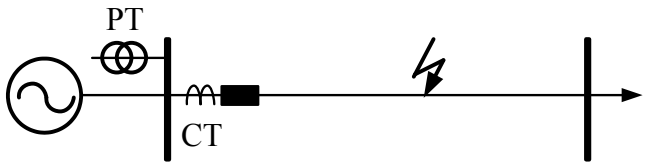

Fig. (6). Single line diagram of the simulated substation.

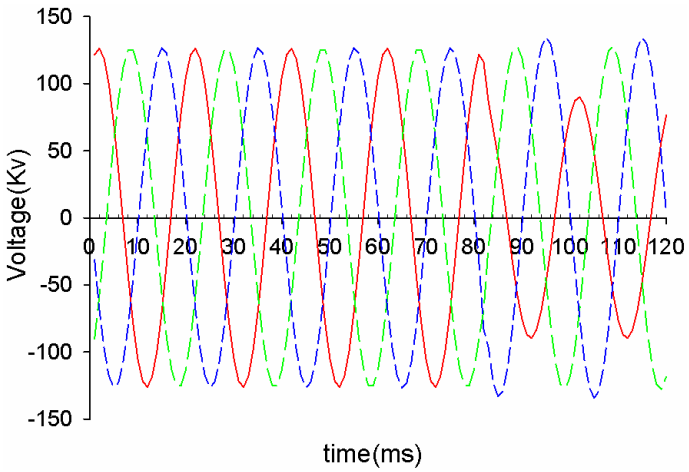

Fig. (7). Simulated busbar voltage with fault present.

The CRC is based on the binary division. A CRC code is formed by treating the original content to be covered as a polynomial of the form $m(x)=a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1x + a_0$, where $m(x)$ is a k bit long message block and a_i is the data value at the ith data position (a_{k-1} = MSB). For a CRC-r code, $m(x)$ is divided by the CRC generator polynomial $g(x)$ and the remainder of that division is appended to the end of $m(x)$ as the CRC value such that dividing any such resulting $n = k + r$ bit block by $g(x)$ will result in a remainder that has the same constant value regardless of the original value of $m(x)$. At the receiver, the original data is regarded as error-free if the division of the received data blocks ($m(x)$ and the CRC) yields this constant remainder. Otherwise, data corruption occurs during data transmission. r of CRC-r could be any positive integer while typical r is 8, or 16 or 32. The simplest CRC code, CRC-1, which uses the generator polynomial $x + 1$, is also known as parity bit. In this paper, the original context $m(x)$ denotes the first 8 MSBs of the effective bits of a measurement, while r = ENOB-8.

4. NUMERICAL SIMULATION

4.1. Simulation Configuration

A 220kV transmission system used for simulation is constructed as Fig. (**6**). The line parameters and other relevant data considered for simulation study are as follows: source impedance of power source parameter: 0.2+j4.5Ω per phase, positive and negative sequence line parameters: R1 = R2 = 0.027Ω/km, L1 = L2 = 0.86mH/km, C1 = C2 = 0.0123μF/km; zero-sequence line parameters: R0 = 0.1948Ω/km, L0 = 2.4mH, C0 = 0.0071μF/km. Distance protection subscribes output of EITs. A three phase short circuit fault is initiated at 80 milliseconds at 8 kilometers away from the busbar. The simulated current and voltage are showed as Fig. (**7**) and Fig. (**8**).

It can be observed that there is no watermarking incurred error in the output of ECT when the system operates with no fault present. The cause might be the maximum load current is 150 amperes (binary 11100111, 7 bits), which takes up

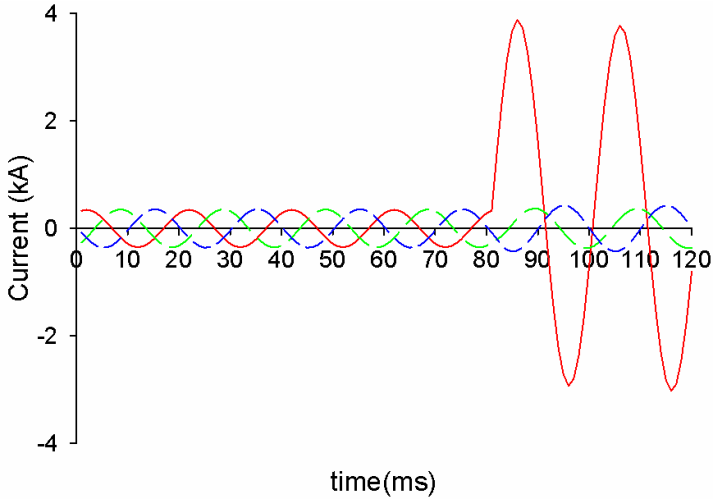

Fig. (8). Simulated line current with fault present.

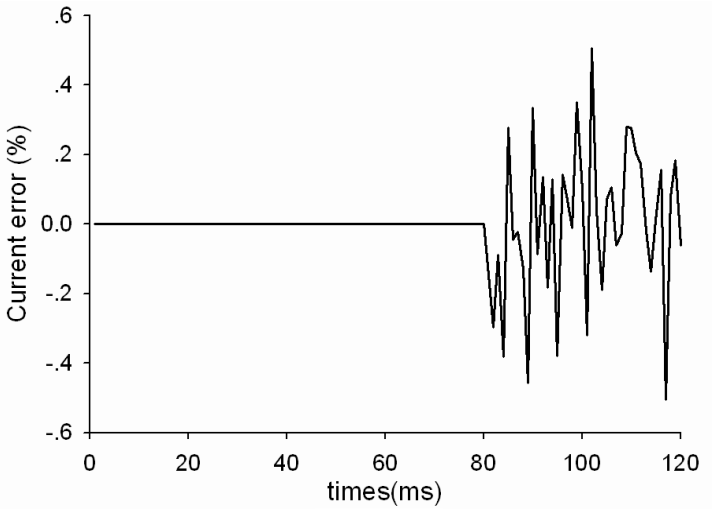

Fig. (9). Current error of Phase A incurred by digital watermark.

less than 8 MSBs. The watermark is embedded in measurement of ECT with short circuit fault current present. Since variation in the magnitude of the voltage incurred by the short circuit fault is not significant, the error incurred by the watermark is not notable, correspondingly.

4.2. Impact of Watermarking

The watermark is embedded with 8 MSBs persevered, that is, data are watermarked to guarantee data integrity at the cost of 0.391% error. The incurred error of EVT and ECT is plotted as showed in Fig. (**9** and **10**).

The measuring impedances with/without watermark are calculated and the impedance trajectory is plotted as Fig. (**11**). It can be observed that there is only imperceptible visual difference between the two impedance trajectories calculated with original/watermarked measurements. Difference between the two impedance trajectories remain visually imperceptible, which indicate the error incurred by the watermark preserving 8 MSBs will not have impact on the performance of distance protection.

There are two key issues for the watermark based data authentication proposed in the paper.

- Process time incurred by CRC based watermark

The watermarking and integrity verification can be implemented by either hardware or software. Were it implemented with hardware, the process time is negligible. Numerical simulation on a HP notebook with Intel dual-core 1.73GHz CPU and 1G memory shows that process time for watermarking is 8.1687 μs while process time for integrity verification is 0.5721 μs, which are acceptable to the protection system.

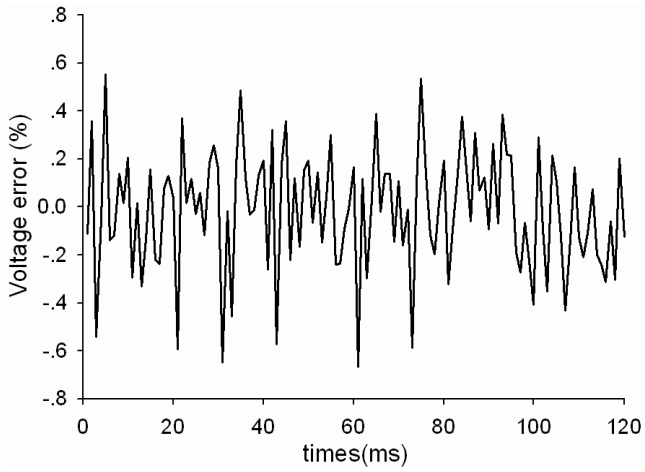

Fig. (10). Voltage error of Phase A incurred by digital watermark.

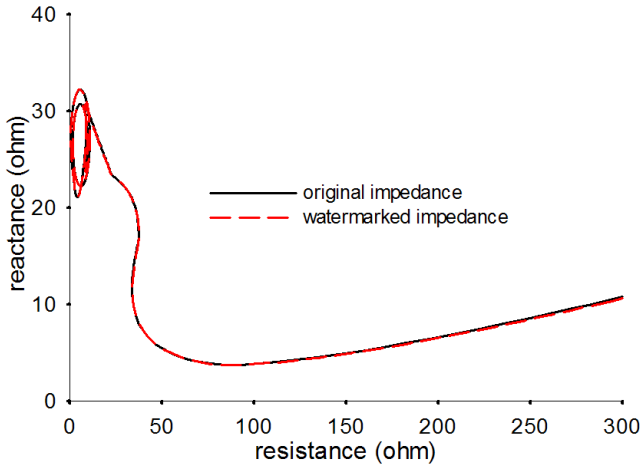

Fig. (11). Comparison of measuring impedance with/without digital watermark.

- Probability of undetected error

The undetected error probability relies on length of CRC code. The undetected error probability approaches $1/2^p$ for any CRC code of length p [22]. Therefore, a long length of CRC code is preferred to lower the undetected error probability. The essential of the LSB based watermark is to assure data integrity at the cost of precision. Since ratio error increases with longer watermark and the preserved ENOB and the number of bits used for watermark add up to 15, a major problem on LSB based watermark is to determine the tradeoff among the distortion between the original measurement and watermarked data.

Were 7 or 6 MSBs of effective bits preserved, the error incurred becomes 0.781% and 1.562%, respectively. In order to show its' impact on distance relay, the trajectories of measuring impedance with/without watermark are plotted in Fig. (**12**) and Fig. (**13**). It can be observed that there is visually detectable difference between trajectories of measuring impedance calculated with/without watermark. Since the largest number of bits used for watermark is 7, 8, and 9 for the measurements preserving 8, 7, and 6 MSBs of effective bits, the largest likelihood of undetected error are 0.781%, 0.391%, and 0.195%, respectively.

It should be pointed out that in a strict sense, encryption/decryption algorithm based cryptographic authentication mechanisms or watermarking should be used for applications requiring protection against cyber attacks. However, computation loads and process latency associated may not be acceptable for the time critical and resource constraint applications in substation automation systems. Although CRCs can be used as a watermark to identify tampering of measurement, they are not designed for protecting against intentional alteration of data. For example, once the way to produce an error detection code based LSB watermark is known to an attacker, he can edit a measurement and re-compute the error detection code without the substitution being detected [17]. Therefore, the proposed approach cannot be used as a general solution. However, since there are numerous varieties of CRCs and other error detecting code [22], they can be used

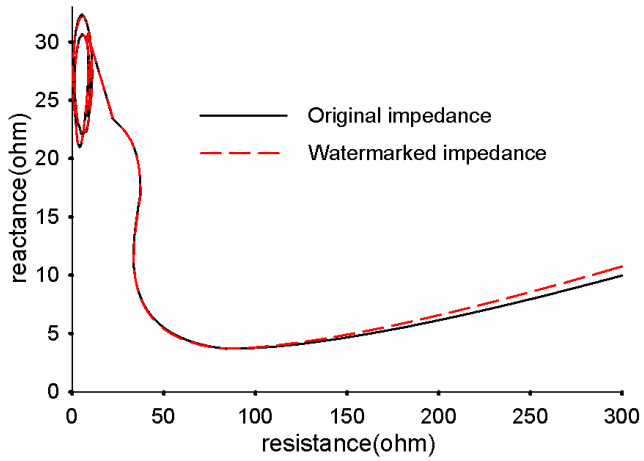

Fig. (12). Measuring impedance with measurements preserving 7 MSBs.

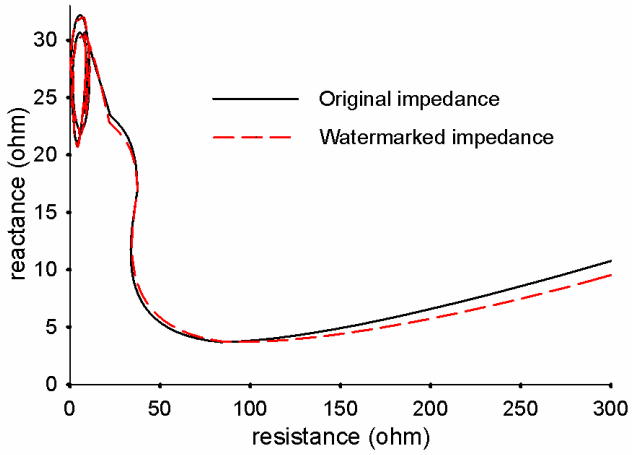

Fig. (13). Measuring impedance with measurements preserving 6 MSBs.

for watermarking as a proprietary approach for intrusion detection system of a specific substation. Therefore, the tampering measurement can be identified to prevent misoperation of the protection system, and the malicious intruder can be isolated to counter cyber attack.

CONCLUSION

As critical installations in the electric power grid, electric substations are a prime target for malicious cyber attackers. The cyber security defense of substation automation system has unique requirement for its time critical and resource constraint environment. This paper proposes the use of a LSB based watermark for data authentication. The watermark can be generated using any error detection code to detect tampered measurement, and hence, the malicious intruder can be identified and isolated by the IDS. Numerical simulation of a CRC based watermark shows that the proposed approach fit for the IEDs with limited process power and it has slim impact on performance of the protective system.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the funding support of the GuangDong electric power corporation and ShenZhen Electric Power Corporation for providing the resources and facilities.

REFERENCES

[1] Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino, A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in SCADA systems," IEEE Trans. Industrial Informatics, vol. 7, no. 2, pp. 179-186, May 2011.

[2] Su Sheng, W.L. Chan, K.K. Li, Duan Xianzhong, "Context information based cyber security defense of substation," IEEE Trans. Power Del., vol.22, no.3, pp. 1477-1481, July 2007.

[3] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, Jian-Cheng Tan, "Security analysis and auditing of IEC61850-based automated substations," IEEE Trans. Power Delivery, vol. 25, no. 4, pp. 2346-2355, Oct. 2010.

[4] G. Dondossola, J. Szanto, M. Masera, I. N. Fovino, "Effects of intentional threats to power substation control systems," International Journal of Critical Infrastructures, vol.4, no.1/2, pp. 129 – 143, 2008.

[5] Göran N. Ericsson, Åge Torkilseng, "Management of information security for an electric power utility-on security domains and use of ISO/IEC17799 Standard," IEEE Trans. Power Del., vol.20, no.2, pp. 683-690, Apr. 2005.

[6] Chen-Ching Liu, Alexandru Stefanov, Junho Hong, Patrick Panciatici. "Intruders in the grid," IEEE Power & Energy Magazine, vol.10, no.1, pp.58-66, Jan./Feb. 2012.

[7] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, Jian-Cheng Tan, "An intrusion detection system for IEC61850 automated substations," IEEE Trans. Power Delivery, vol. 25, no. 4, pp. 2376-2383, Oct. 2010.

[8] Karen Scarfone, Peter Mell. NIST Guide to Intrusion Detection and Prevention Systems, NIST Special Publication 800-94, Feb. 2007.

[9] Tal Ben-Zvi, J. V. Nickerson, "Intruder detection: an optimal decision analysis strategy," IEEE Trans. Systems, Man, and Cybernetics—Part C: Applications and Reviews, vol.42, no.2, pp. 249-253, March 2012.

[10] Shingo Mabu, Ci Chen, Nannan Lu, Kaoru Shimada, Kotaro Hirasawa, "An intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming," IEEE Trans on Systems, Man, and Cybernetics—Part C: Applications and Reviews, vol. 41, no. 1, pp.130-140, Jan. 2011.

[11] Sooyeon Shin, Taekyoung Kwon, Gil-Yong Jo, Youngman Park, Haekyu Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," IEEE Trans Industrial Informatics, vol.6, no.4, pp. 744-757, Nov. 2010.

[12] Chee-Wooi Ten, Govindarasu Manimaran, Chen-Ching Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," IEEE Trans. on Systems, Man, and Cybernetics—Part A: Systems and Humans, vol. 40, no. 4, pp. 853-865, July 2010.

[13] Chee-Wooi Ten, Junho Hong, Chen-Ching Liu, "Anomaly detection for cybersecurity of the substations," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 865-873, Dec. 2011.

[14] Chee-Wooi Ten, Chen-Ching Liu, Govindarasu Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," IEEE Trans. Power Systems, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[15] IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation, IEEE Standard 1646, Feb. 2005.

[16] Qinghua Li, Guohong Cao, "Multicast authentication in the smart grid with One-Time signature," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 686-696, Dec. 2011.

[17] T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, K. Sekiguchi, "Information-theoretic approach to authentication codes for power system communications," in Proc. 2010 IEEE PES Transmission and Distribution Conference and Exposition, pp.1-7.

[18] Zhu Lin, Duan Xianzhong, Su Sheng, Li Yinhong, "Evidence theory based fault tolerant method for protective relays in digital substations," Transaction of China Electrotechnical Society (in Chinese), vol. 26, no.1, pp. 154-161, Jan. 2011.

[19] Su Sheng, "Research on issues of digital power system," Ph.D. dissertation, Dept. Electrical & Electronics Eng., Huazhong University of Science and Techlogy, Wuhan, China, 2009.

[20] Su Sheng, Duan Xianzhong, W.L. Chan, Li Zhihuan., "Erroneous measurement detection in substation automation system using OLS based RBF neural network," Electrical Power and Energy Systems, vol. 31, no. 6/7, pp. 351–355, June 2009.

[21] http://en.wikipedia.org/wiki/Watermark - cite_ref-0Biermann, Christopher J. Handbook of Pulping and Papermaking. San Diego, USA: Academic Press, 1996, p. 171.

[22] Wei Sun, "Joint compression and digital watermarking: information-theoretic study and algorithms development," Ph.D. dissertation, Dept. Electrical & Computer Eng., Univ. Waterloo, Waterloo, Canada, 2006.

Received: October 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014