Cybersecurity Resilient for Quartile-based Transformer Differential Protection Scheme

Het Bhalja[1], Bhaveshkumar R. Bhalja[2] and Pramod Agarwal[3]
Department of Electrical Engineering
Indian Institute of Technology Roorkee
Roorkee, India
het_b@ee.iitr.ac.in[1], bhavesh.bhalja@ee.iitr.ac.in[2] and pramod.agarwal@ee.iitr.ac.in[3]

***Abstract*— This paper proposes a new cybersecurity resilient technique utilizing two-layer feedforward neural network (2LFFNN). It is also able to predict the correct value of the altered SV packets. The performance of the proposed technique is evaluated in accordance with the quartile-based differential protection (87Q) scheme, which provides superior performance compared to the conventional transformer differential protection (87T) scheme. Nevertheless, as per the statistical analysis, 87Q scheme is more vulnerable against cyber security threats in IEC 61850 enabled substation. The attacker can easily attack the IEC 61850 process layer and gain access to the SV messages, which carry current and voltage information of the substation equipment to the process layer. To test the proposed cybersecurity resilient scheme, 51000 cases of synthetic data, used for training 2LFFNN, pertaining to different types of attack are generated by modeling 87Q scheme in PSCAD/EMTDC software package. After training the neural network, the performance of the proposed 2LFFNN is verified during the FDI attack and SV packet loss/delay. The simulation results indicate that the proposed scheme is not only capable to identify cyber-attacks but also able to mitigate using 2LFFNN.**

Keywords*— Cybersecurity, IEC 61850, Sampled value (SV) protocol, False data injection (FDI)

I. INTRODUCTION

A. Background

Automation and digitalization focus heavily on information and communication tools and computer-aided communication technology. The terms "Smart Grid" and "Smart Substation" rest a lot on how well the system can communicate and integrate computing and/or communication technology. Such an integration makes it more susceptible to cyber threats/attacks [1]. The protocols for substation automation and control are built on IEC 61850 standards [2]. The efficacy of the "smart substation" depends on how well and accurately each piece of equipment and component is capable of communicating with each other. The IEC 61850 is a standard for integration and communication of protection, automation, and control instruments in electrical power systems. It provides a standardised method for devices in power systems to communicate with each other, regardless of their manufacturer or technology [3].

B. Communication in Substation Automation System (SAS)

In SAS, the communication network is responsible for controlling, transmitting and distributing power as per IEC 61850. The IEC 61850 describes a number of services and protocols, such as the Manufacturing Message Specification (MMS), the sampled value (SV) messaging, and the Generic Object Oriented Substation Event (GOOSE) messaging. The SAS network has three levels namely (i) station level, (ii) bay level and (iii) process level. The MMS is used for exchanging information between two substation devices whereas the SV messages carry recorded sampled values of the currents and voltages on the process bus and connect the instrument transformer with IEDs. On the other hand, the GOOSE messages are used for performing communication between IEDs and switchgears of substations. The process bus connects IEDs and substation equipments or instrument transformers of individual component as per IEC 61850-9-2 over ethernet using IEC 8802-3 standards. The SAS utilizes several merging units (MUs), which convert voltages and currents of instrument transformers into IEC 61850-9-2 compatible SV messages and make them available on the process bus for further utilization of IEDs.

The SV and GOOSE messages are time-sensitive, due to which they are given higher priority in SAS. They are usually linked to the lower-level ethernet network using IEC 8802-3 [4]–[6]. Time-sensitive messaging may lead to data transmission problems and cyber threats, such as SV packet loss or delay, time delay, mistakes in a bit, bit reversal, false data injection (FDI) attacks, loss of communication channel/link, denial of service attacks, etc. Additionally, unlike GOOSE messages, the SV messages are not broadcasted repetitively. This makes SV message delivery more critical in case of cyberattack or SV packet loss/delay.

In case of conventional transformer differential protection (87T), the time-synchronised SV messages are required which utilize precision time protocol (PTP) as per IEEE 1588 standards. As the said scheme needs reliable SV packet transfer, loss/delay of SV packet may lead to the mal-operation of 87T [7]. Many researchers have tried to evaluate the performance of the IEC 61850-based bus and distance protection scheme and suggested corrective measures in case of SV packet loss or delay [8]– [9]. In [10], FDI attacks are detected for renewable-based power systems using machine learning (ML)/deep learning (DL) methods. A generative adversarial network (GAN) is adopted in [11] to detect FDI attacks on wide-area monitoring systems that focus on communication between substations and/or control centres. A least square fitting-based method is utilized in [12] for detection of FDI attacks in PMU data and provides a mitigation technique that helps in power system state estimation. Though the aforementioned three papers have carried out FDI attacks on control centres and power system operators, they have not considered attacks on the SAS level.

Then, various anomaly detection algorithms are developed by tracking the digital footprints of the attacker in the SAS network [13]–[14]. Further, the specification-based intrusion detection system (IDS) is developed for IEDs placed at SAS [15]. Though this IDS is designed for GOOSE and SV messages, they do not provide any mitigation technique at the protection algorithm level. Subsequently, methods based on ML and DL have utilized for mitigation of FDI attacks on the PMU data [10], [16]–[19].

979-8-3503-9678-2/23/$31.00 ©2023 IEEE

In this paper, a preventive framework is developed using 2LFFNN which can effectively predict falsely injected data and packet loss/delayed data. The main contribution of the proposed work are as follows:

1) The proposed algorithm is capable to detect as well as predict falsely injected data and packet loss/delay.
2) The developed framework can be retrofitted in the existing IEDs as a pre-processing mechanism, which enhances security of IEC 61850 enabled sub-station against cyber-attacks.
3) The suggested algorithm enhances the security of the existing 87Q against FDI attacks and SV packet loss/delay.

The manuscript is organized as follows. In section II, layout of the SAS, quartile-based differential protection scheme and various cyber-attack scenarios are discussed. The proposed 2LFFNN based method is explained in the section III. In section IV, the performance of the proposed scheme on different FDI attacks and SV packet loss/delay is discussed. The section V concludes the paper.

II. Layout of the SAS for Transformer Protection and Considered Cyberattack Scenarios

A. Layout of Transformer Protection in IEC 61850 enabled Substation

The typical layout of the substation having SAS in accordance with IEC 61850 along with power transformer are shown in Fig. 1. The rating of the transformer is given in Appendix. The dedicated station MUs are installed for measuring currents and voltages from instrument transformers and broadcast them on the process level of the SAS in terms of SV packets as per IEC 61850-9-2 and IEEE 1588. As per IEC 61850, the MU needs to send the SV packet information with a sampling rate of 80 samples/cycle for protection application and 256 samples/cycle for power quality application. The IEDs (based on quartile-based differential protection scheme) can access the data that are available in terms of SV packets from MUs. Based on the SV packet information, IEDs will take decisions and notify the intended operation in the form of GOOSE messages to MUs. The MUs are capable to communicate with the switchgear of the substation and perform necessary actions. It is to be noted that IEDs can communicate at any level of SAS. Further, the attacker may enter to process, bay and station level. Fig. 1 also shows the layout of different levels of SAS where the intruder can attack the information.

B. Quartile-based differential protection scheme

The quartile-based differential protection scheme is presented in [20]. It is a statistical method, which divides any ordered dataset into 4 equal parts using quartiles (lower quartile (Q1), median quartile (Q2) and upper quartile (Q3)). According to IEC 61850, 80 samples/cycle data will be available at the process level. These data are utilized to calculate differential current samples (ID) and superimposed differential current (SID) samples for a duration of one cycle as per (1).

$$\mathrm{SID}\,(t) = \mathrm{ID}\,(t) - \mathrm{ID}\,(t - \mathrm{T}) \tag{1}$$

where, ID is the differential current of the particular winding of the transformer, T is the total number of samples in a cycle.

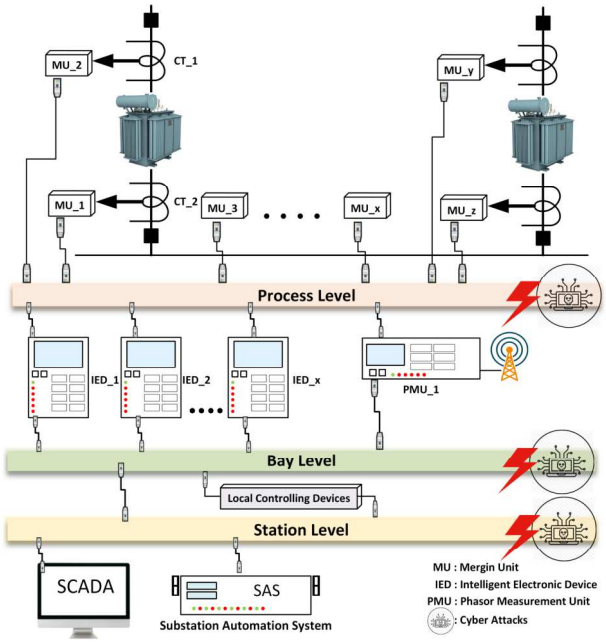

Fig. 1. Typical layout of IEC 61850 enabled substation

After calculating SID, the data are arranged in ascending order and the lower (Q1), median (Q2) and upper (Q3) quartiles are calculated as per (2). Further, the inter-quartile range (IQR) and pre-detection index (PDI) are calculated as per (3) and (4), respectively.

$$\mathrm{Q}(1/2/3)(t) = \mathrm{SID}\,(n) + p\left(\mathrm{SID}(n+1) - \mathrm{SID}(n)\right) \tag{2}$$

where, p and l are the floor and fraction part of (T/4), (T/2) and (3T/4) for Q = 1, 2 and 3, respectively.

$$\mathrm{IQR}\,(t) = \mathrm{Q3}\,(t) - \mathrm{Q1}\,(t) \tag{3}$$

$$\mathrm{PDI}\,(t) = \left(\mathrm{Q1}\,(t)/\mathrm{Q3}\,(t)\right) \times \left(\mathrm{Q2}\,(t) - \mathrm{Q1}\,(t)\right)^2 \tag{4}$$

Further, to discriminate between internal fault and abnormal operating conditions of the transformer, a separate fault detection index (FDI), which is the ratio of PDI to IQR, is calculated as per (5).

$$\mathrm{FDI}\,(t) = \left(\mathrm{PDI}\,(t) \,/\, \mathrm{IQR}\,(t)\right) \times 100\% \tag{5}$$

The value of threshold (th) is compared phase-wise to detect an internal fault. The value of th is selected as 4% by rigorous simulation study and real field data [20]. Here, any kind of FDI attack is possible which can change the ordered data set and may lead to incorrect selection of quartile which in turn may lead to the mal-operation of the technique.

C. Various cyberattack scenarios

The intruder can take access to any information if he/she connects at any level of the SAS. The MUs of the substation will continuously send the voltage and current information in terms of SV packets. The IEDs will read the SV packets and finally decide occurrence of a fault. If an intruder is present at any level of the SAS, it can access the information of the transmitting SV packet messages. In such a situation, the intruder can put false information in the SV packet messages. In this situation, the IED will not be able to discriminate between original data and falsely injected data. Hence, the quartile-based differential protection scheme may observe the non-fault condition as a fault condition due to FDI attacks. Further, the MUs of all the substation equipment put their data on the process level. As the IEC 61850's process level has a

lot of data, it may lead to data loss or delay. The SV packet data loss/delay of one side of the transformer winding may lead to the unnecessary generation of ID and SID of the particular phase. The IED may treat this condition as a fault and may mal-operate.

III. The Proposed Approach

A. Two-layer Feedforward Neural Network (2LFFNN)

A two-layer feedforward neural network is a type of artificial neural network that consists of an input layer, a hidden layer, and an output layer. The 2LFFNN is a fully connected neural network and it is also known as a multilayer perceptron (MLP). The hidden layer (one with a layer size of 10 is used in this approach) performs a non-linear transformation of the input layer data. The main advantage of 2LFFNN is that it can learn complex non-linear relationship between input and output data, making it useful for the prediction of affected SV packets in case of FDI attacks or SVs packet loss/delay. The output can be visualised as per (6).

$$O_j = g\left(\sum_h wout_{j,h} + b_2\left(g\left(\sum_i win_{h,i}\, X_i + b_1\right)\right)\right) \quad (6)$$

where, '*win'* and *'wout'* is the weight function of the input and output layer, respectively, 'b_1' and 'b_2' is the biasing of the hidden layer and output layer, respectively, '*i'* is the size of the input data, '*h*' is the size of hidden layers and '*j*' is the size of the output. Here, values of '*i*' and '*j'* are taken as 80 and the value of '*h'* is considered as 10.

The architecture of the proposed 2LFFNN is shown in Fig. 2. The input layer will have SV packets, which are available through the process level of IEC 61850-9-2. The incoming SV packets and past received SV packets (stored in buffer of the IED) are used together for input of the proposed 2LFFNN. The proposed 2LFFNN utilizes 80 samples as input and gives 80 samples as output. The size of the input and output weight matrix is 10 × 80 and 80 × 10, respectively. The size of the hidden layer is considered as 10. In case of a FDI attack, the IED will receive manipulated SV packet instead of the original packet. Hence, before processing the

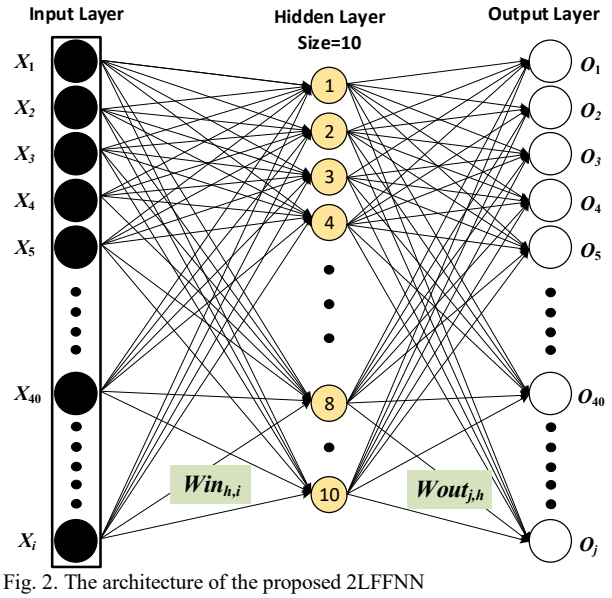

Fig. 2. The architecture of the proposed 2LFFNN

TABLE I. Considered Scenario for Generation of Training Data

False Data Injection (FDI) attack			
Affected SV packet numbers	**No. test cases**	**Affected SV packet numbers**	**No. test cases**
1	1500	6	2500
2	1500	7	3500
3	1700	8	3500
4	1800	9	3500
5	2000	10	4000
Total data for FDI attacks **(A)**			**25500**
SV packet loss/delay			
Affected SV packet numbers	**No. test cases**	**Affected SV packet numbers**	**No. test cases**
1	1500	6	2500
2	1500	7	3500
3	1700	8	3500
4	1800	9	3500
5	2000	10	4000
Total data for SV packet loss/delay **(B)**			**25500**
Total data generated (A+B)			**51000**

manipulated SV packet, it is passed through the 2LFFNN network. The other SV packets will be used from the stored buffer of the IED. Using these SV packets, the proposed 2LFFNN will sense the intrusion in the incoming SV packet. It performs the corrective measure and predicts the value of the original packet based on the past information of the received SV packets.

B. Training of the 2LFFNN

To avoid overfitting, it is necessary to generate enough data set for training of the neural network. This can be achieved by simulating different operating condition scenarios of the transformer in PSCAD/EMTDC software package. The data pertaining to various scenarios are collected in MATLAB environment. Various FDI attacks and SV packet loss/delay, generated by modeling various scenarios of transformer in PSCAD/EMTDC, are utilized to train the neural network. The same is depicted in Table-I. The Levenberg–Marquardt (LM) method is used to train the neural network [21] as it offers flexibility, reliability and faster convergence. Additionally, the mean square error (MSE) is used to measure the efficacy of the trained neural network. The entire dataset (as depicted in Table-I) is randomly divided into three parts namely (i) training (60%), (ii) validation (20%), and (iii) testing (20%). Further, the neural network was trained on the computer having Intel Xeon Gold 6226R CPU with (16×2 Cores), 1024 GB of RAM and 16 GB NVIDIA RTX A4000 GPU with 6144 CUDA cores. The trained neural network has an MSE of 0.0012 and a Pearson correlation coefficient (PCR) of 0.9997, which indicate effective training and correctness of the proposed 2LFFNN.

IV. Performance Evalution

The performance of the proposed 2LFFNN is checked for various FDI attack and SV packet loss/delay scenarios. Further, its performance is also checked in conjunction with quartile-based differential protection scheme. At last, points to be considered during hardware implementation of the proposed algorithm are also discussed.

A. FDI attacks on the convention scheme

Fig. 3 (a) shows a FDI attack on the current signal acquired from the conventional scheme and transmitted as SV packets. It is observed from Fig. 3 (a) that five SV packets are falsely injected. Fig. 3 (b) shows the performance of the 2LFFNN during the said FDI attack. It is observed from Fig. 3 (b) that the proposed approach is not only able to detect intrusion but also capable of predicting and replacing the false data as a preventive measure.

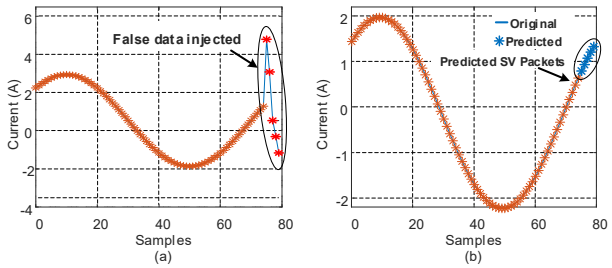

Fig. 3. (a) FDI attack in the form of current signal with 5 altered SV packets and (b) Response of the proposed approach.

B. Impact of FDI attack on 87Q

Fig. 4 (a) shows waveform of current signal acquired from 87Q based protection scheme with 10 altered SV packets. Due to falsely injected data, as observed from Fig. 4 (b), the 87Q based protection scheme initiates unwanted tripping commend as the value of FDI exceeds threshold value (*th*).

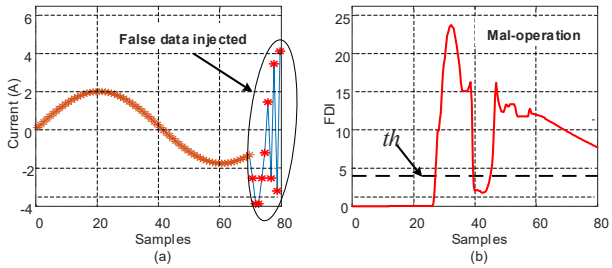

Fig. 4. (a) FDI attack on current signal with 10 altered SV packets and (b) Response of the 87Q based protection scheme

C. Mitigation of FDI attack by the proposed framework on 87Q

Fig. 5 (a) shows the response of the proposed framework on the current signal with 10 altered SV packets (as shown in Fig. 4 (a)). Further, the response of 87Q based protection scheme with the predicted signal given by the proposed framework, as depicted in Fig. 5 (a), is shown in Fig. 5 (b). The above discussion clearly indicates that the proposed framework is able to predict the falsely injected data. It also prevents the mis-operation of 87Q based protection scheme due to accurate reconstruction of the attacked signal.

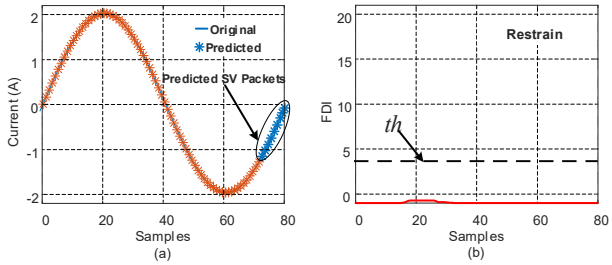

Fig. 5. (a) Response of the proposed framework on current signal with 10 altered SV packets and (b) Response of the 87Q based protection scheme

D. SV packet loss/delay

Fig. 6 (a) shows the current signal in which eight SV packet loss/delay occurred. In such a situation, the corresponding sample is assumed to be zero. Hence, 87Q based protection scheme will get SV packets from one side of the transformer whereas on the other side SV packets will be delayed/lost due to which unwanted trip commands may be initiated. This can be mitigated by the proposed 2LFFNN-based approach. Its response is shown in Fig. 6 (b). It is observed from Fig. 6 (b) that the proposed approach can predict the SV samples, which are lost/delayed due to process level traffic of the IEC 61850.

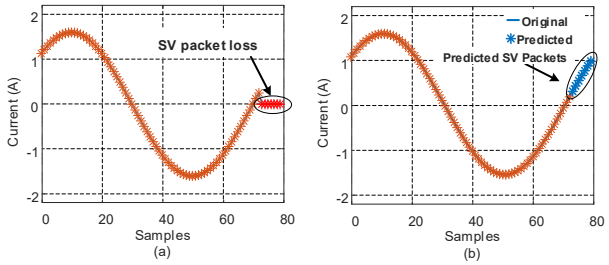

Fig. 6. (a) SV packet loss/delay on the acquired current signal with 8 SV packet loss/delay and (b) Response of the proposed framework

E. Implementation of the 2LFFNN

The proposed 2LFFNN uses 2-layer feedforward fully connected neural network. Due to a single hidden layer with its small size (only 10), the computational complexity is lower than other ML/DL-based methods. This computational complexity plays a crucial role in the implementation of the preventive framework on the existing IEDs in IEC 61850 enabled sub-station as a pre-processing mechanism. Enough computational time should be available between two consecutive incoming SV packets so that the preventive framework (as suggested in this paper). This will also help the protection algorithm to complete its task and taking appropriate decisions based on the available packets. As the proposed method can be easily implemented/retrofitted together with the existing IEDs installed in IEC 61850 enabled sub-station, it will reduce process-level threats. The proposed framework can be easily implemented on the hardware using the TMS320F28xx series-based digital signal processor (DSP) [22]/ Xilinx 7 series-SPARTAN 7-based field programmable gate array (FPGA)[23].

V. Conclusion

The proposed 2LFFNN can handle FDI attacks and SV packet loss/delay as per IEC 61850-9-2. Its performance is checked for quartile-based differential protection scheme which is highly vulnerable against cyberattacks. The proposed 2LFFNN can be placed ahead of the protection scheme in the IEDs of SAS so that all incoming traffic of IEDs can be passed through it. This will lead to the detection of any intrusion/discrepancy in the data and preventive action can be taken. The results indicate that the proposed 2LFFNN can easily detect FDI attacks and compensate for the SV message packet loss/delay. At the same time, it also prevents mal-operation of the existing quartile-based differential

protection in case of FDI attacks or SV packet loss/delay. Due to less computational complexity, the proposed 2LFFNN can easily be implemented at IEDs and the upcoming traffic should pass from 2LFFNN to identify and mitigate cyber-threat.

APPENDIX

Power Transformer data: 3-phase, 315 MVA, 50 Hz, 400 kV/220 kV, Yd1, Reactance in terms of per phase: 12.5 %, Inrush current in terms of percentage of rated current: 0.1%

ACKNOWLEDGEMENT

This work was supported by Central Power Research Institute as a research program under grant CPRI/R&D/TC/Trans/2022.

REFERENCES

[1] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," IEEE Transactions on Power Delivery, vol. 25, no. 3, pp. 1501–1507, 2010.

[2] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," ." International Journal of Electrical Power & Energy Systems, vol. 99, pp. 45–46, 2018.

[3] "IEEE Recommended Practice for Implementing an IEC 61850-Based Substation Communications, Protection, Monitoring, and Control System," IEEE Std 2030.100-2017, pp.1-67, 19 June 2017.

[4] H. D. Ngo and H. S. Yang, ''Latency and traffic reduction for process-level network in smart substation based on high-availability seamless redundancy, IEEE Transactions on Industrial Electronics, vol. 63, no. 4, pp. 2181–2189,Apr. 2016.

[5] D. M. E. Ingram, F. Steinhauser, C. Marinescu, R. R. Taylor, P. Schaub, and D. A. Campbell, "Direct evaluation of iec 61850-9-2 process bus network performance," IEEE Transactions on Smart Grid, vol. 3, no. 4, pp. 1853–1854, 2012.

[6] H. D. Ngo and H. S. Yang, "Latency and traffic reduction for process-level network in smart substation based on high-availability seamless redundancy," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 4, pp. 2181–2189, 2016.

[7] R. He, H. Peng, Q. Jiang, L. Zhou, and J. Zhu, "Performance analysis and threshold quantization of transformer differential protection under sampled value packets loss/delay," *IEEE Access*, vol. 7, pp. 55 698–55 706, 2019.

[8] D. M. E. Ingram, P. Schaub, R. R. Taylor, and D. A. Campbell, "Performance analysis of IEC 61850 sampled value process bus networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1445–1454, 2013.

[9] M. G. Kanabar, T. S. Sidhu, and M. R. D. Zadeh, "Laboratory investigation of iec 61850-9-2-based busbar and distance relaying with corrective measure for sampled value loss/delay," *IEEE Transactions on Power Delivery,* vol. 26, no. 4, pp. 2587–2595, 2011.

[10] F. Almutairy, L. Scekic, R. Elmoudi, and S. Wshah, "Accurate detection of false data injection attacks in renewable power systems using deep learning," *IEEE Access*, vol. 9, pp. 135 774–135 789, 2021.

[11] R. Jiao, G. Xun, X. Liu, and G. Yan, "A new ac false data injection attack method without network information," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5280–5289, 2021.

[12] E. Hallaji, R. Razavi-Far, M. Wang, M. Saif, and B. Fardanesh, "A stream learning approach for real-time identification of false data injection attacks in cyber-physical power systems," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3934–3945, 2022.

[13] C. W. Ten, J. Hong, and C. C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 865-873, Dec. 2011.

[14] J. Hong, C. C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Transactions on Smart Grid*, vol. 5,no. 4, pp. 1643-1653, April 2014.

[15] Hong, and C. C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems" *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 271–281, Jan. 2019.

[16] A. Chawla, P. Agrawal, B. K. Panigrahi, and K. Paul, "Deep-learning-based data-manipulation attack resilient supervisory backup protection of transmission lines" *Neural Computing & Application*, vol. 35, no.7, pp. 4835–4854, June 2021.

[17] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[18] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2017.

[19] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2218–2234, 2020.

[20] A. M. Shah, B. R. Bhalja, R. M. Patel, H. Bhalja, P. Agarwal, Y. M. Makwana, and O. P. Malik, "Quartile based differential protection of power transformer," *IEEE Transactions on Power Delivery,* vol. 35, no. 5, pp. 2447–2458, 2020.

[21] B. M. Wilamowski and H. Yu, "Improved computation for levenberg–marquardt training," *IEEE Transactions on Neural Networks*, vol. 21, no. 6, pp. 930–937, 2010.

[22] "TMS320F2837xD Dual-Core Microcontrollers Technical Reference Manual", Texas Instruments Inc., September 2019. [Online]. Available:https://www.ti.com/lit/ug/spruhm8i/spruhm8i.pdf?ts=1677742831509&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FTMS320F28379D

[23] "DS180 - 7 Series FPGAs Data Sheet: Overview (DS180) (v2.6.1)," Xilinx, 2020. [Online]. Available: https://docs.xilinx.com/v/u/en-US/ds180_7Series_Overview