Journal of Mines, Metals and Fuels, *71(12A): 160-167; 2023. DOI: 10.18311/jmmf/2023/43177*

Print ISSN : 0022-2755

Journal of Mines, Metals and Fuels

Contents available at: *www.informaticsjournals.com/index.php/jmmf*

A Convolutional Neural Network based Pattern Classification Approach for Dynamic Security Assessment with Inadequate Energy Sources

Rituparna Mukherjee[1]*, Abhinandan De[2], Promit Kumar Saha[1], Susmita Dhar Mukherjee[1], Abhishek Dhar[1] and Saurabh Adhikari[1]

[1]Department of Electrical Engineering, Swami Vivekananda University, Kolkata – 700121, West Bengal, India; rituparnamukherjee@svu.ac.in

[2]Department of Electrical Engineering, Indian Institute of Engineering Science and Technology, Shibpur, Howrah - 711103, West Bengal, India

Abstract

The security-state categorization of complex power system networks based on "transient stability" is proposed in this research study as a "Convolutional Neural Network (CNN)" based pattern classification approach. The "pre- contingency operating states" of a "power system network" served as CNN's input. The focus was on predicting the system's post-contingency stability condition, so the Critical Clearance Time (CCT) was used as the primary metric for categorizing the "pre-contingency operational states" into "secure" and "insecure" classes. The recommended method was successfully applied to the "IEEE 39-bus system", and it was discovered that the CNN classifier can classify the power system's pre-contingency operational states based on an accurate forecast of the conditions that will lead to future post- contingency transient stability.

Keywords: *Classification, Convolutional Neural Network Dynamic Security, Power System Transient Stability*

1.0 Introduction

The synchronization of the spinning speeds of thousands of massive, interconnected producing units is necessary for the power system. In addition, regardless of variations in demand or potential generator failure, the operation requires all equipment to function within its physical limitations. Generator or backup power failures are frequent in a typical power system, which could alter the system's operational state. Power system security is the term used to describe the "degree of risk" that a power system poses in surviving potential disturbances like faults and contingencies without experiencing a substantial interruption in the delivery of electricity to consumers at any one time.

To ascertain how well-built a power system is in relation to a wide range of major conflicts that are likely to occur on a daily basis for any network, "security analysis" is therefore essential. For power system security investigations (DSA), there are two fundamental categories: "Static Security Analysis" (SSA) and "Dynamic Security Analysis" (DSA)[1]. It is essential that the power system returns to normal after a crisis because any catastrophe will inevitably cause the system's status to alter. According to the SSA, who assert that stable operations have been attained[2], the assessment mainly examines whether any physical or "security constraints" have been lifted in order to reach the "post- contingency steady state". However, a quick change to the steady-

*Author for correspondence

state operating point is highly doubtful in the event of any seriously upsetting events. This impossibility might lead to the system reaching a quasi-stable condition for a noticeably longer amount of time, which might further lead to the unintended activation of relays and circuit breakers that are used for system isolation and protection[3]. Finally, this phenomenon causes a series of critical systems and machinery to fail, endangering the system's security. Becausemost power generating units are built to function at or near their optimum efficiency, and because contemporary major power grids have improved, the possibility of instability in the competitive modern energy market has increased. specific research on dynamic security[4,5].

One of the most precise techniques for transient stability is nonlinear Time Domain Simulation (TDS)[1]. With the help ofsets of "time-domain non-linear algebraic equations", this technique simulates the behaviour of generators and other power system equipment. The equations are numerically solved in order to assess a system's dynamic behaviour underplausible perturbations and determine whether the perturbation would result in a loss of "transient stability". The fundamental drawback of TDS is that it cannot be used for online applications because it necessitates lengthy and resource-intensive numerical integrations[6]. TDS cannot beused to judge the "relative stability" of a power system, which is seen to be more significant than examining its "absolute stability". For instance, the only method to gauge the seriousness of a certain scenario is to assess how it will affect system security in comparison to other scenarios[7].

The direct technique employing transient energy function is an alternate method to the transient stability analysis for determining the post-contingency operating point[8]. The direct method's use of post contingency system reduced order modelling does not yield the same levels of accuracy. It is also not a viable strategy for "large-scale power systems", which need in-depth modelling.

Because of their computational complexity, none of the standard methodologies for assessing the dynamic security ofelectric power networks can be used successfully in real-timeor online settings, according to a review of the methods nowin use. The majority of the electric power system's criticalpre-contingency states, which may result in widespread blackouts, are distinct, which adds to the problem'scomplexity. No single algorithm has been able to successfullydisclose such conditions quickly enough to be helpful in real- time security assessment. Therefore, it is vitally necessary todevelop a quick and reliable technique for real-time security monitoring and evaluation of the current security level of huge power systems. Several research findings from the late 1980s suggest that "Machine Learning" (ML) and "Artificial Intelligence" (AI) approaches can be utilized to solve this issue effectively[9,10]. Utilizing "machine learning" and "data mining approaches", attempts have been made toconstruct "very quick" and "intelligent" power system security assessment systems[11,12], with encouragingoutcomes. This was attributed to two particular features that may be effectively employed to determine the currentoperational health of a power system: their general ability torecognize "patterns" fast and their capacity to "learn through examples." These Artificial Intelligence (AI) techniques aimto demonstrate the organic connection between input (system operating scenarios) and the dynamic security status of the system (output). They can even predict emergency circumstances using certain system security indices byidentifying and tracking the pre-contingency operationalevents that would have contributed to system vulnerability. This article suggests an AI method for categorizing CNN- based big and complex power systems in order to conduct transient stability-based security evaluations. This methodmay inform the system operator of a potentially dangerous system operation in the event of significant interruptions andemergencies. By assessing the risk that the system wouldbecome briefly unstable in the case of plausible contingenciesand outages, it is possible to forecast and characterize the existing operational situations (pre-contingency) of a power system. To take into consideration this persistence, a Convolutional Neural Network based Security Classifier (CNNSC) that functions as a "dynamic security classifier" has been created. The suggested CNNSC may categorize the dynamic operating states of the power system into secure or insecure classes based on a conceivable future transient instability by providing it with a set of pre-contingency operating variables. Plans for emergencies have been madegiven the current loading conditions. Bus voltagemagnitudes, voltage angles, and power flow data weremeasured using a synchronized Phasor Measuring

Unit (PMU), and these measurements were then used as inputs to the CNNSC. The CNNSC outcome is "1" if the system's post- contingency operation is projected to be dangerous or "0" if it is assessed to be secure under a variety of reasonable assumptions.

1.1 The Concept of Convolution's Neural Network Based Dynamic Security State Classification

By assessing its capacity to momentarily destabilize the system in the event of a contingency in the future, the security classifier is intended to forecast and characterize the pre- contingency operational status of a power system. Convolution's Neural Network (CNN) has been taught to serve as a security classifier in order to do this (CNNSC). The system variables or features measured by PMUs during the pre-contingency operating scenario of the power system are the proposed CNNSC's inputs, and the CNNSC's output is a prediction of the system's dynamic security state[13]. The security classifier is designed to forecast and characterize thepre-contingency operational status of a power system by evaluating its potential to temporarily destabilize the system in the case of a contingency in the future. In order to do this,a Convolution's Neural Network (CNN) that serves as asecurity classifier has been trained (CNNSC). The dynamic security status of the system is predicted by the proposed CNNSC, and the system variables or characteristics measured by PMUs during the pre-contingency operating scenario of the power system serve as the CNNSC's inputs[13]. The criticality of the line faults was evaluated in this work using the CCT of various line faults[14]. The likelihood that a critical line fault will occur in a pre-contingency operating environment determines the criticality index for that fault.

To enhance the anticipated CNNSC's ability to assess the "degree of criticality" connected to various pre-contingency operating situations, off-line training was provided. Once trained, the CNNSC may be used online to forecast and categorize the power system's future dynamic security state into secure and insecure categories using just inputs from the PMU measurements in the pre-contingency operating scenario. Figure 1 shows the proposed CNNSC's conceptual diagram.

2.0 Convolutional Neural Network

A "Deep Learning" technique called a "Convolutional Neural Network (ConvNet/CNN)" may be able to take an input image, assign various objects and elements value

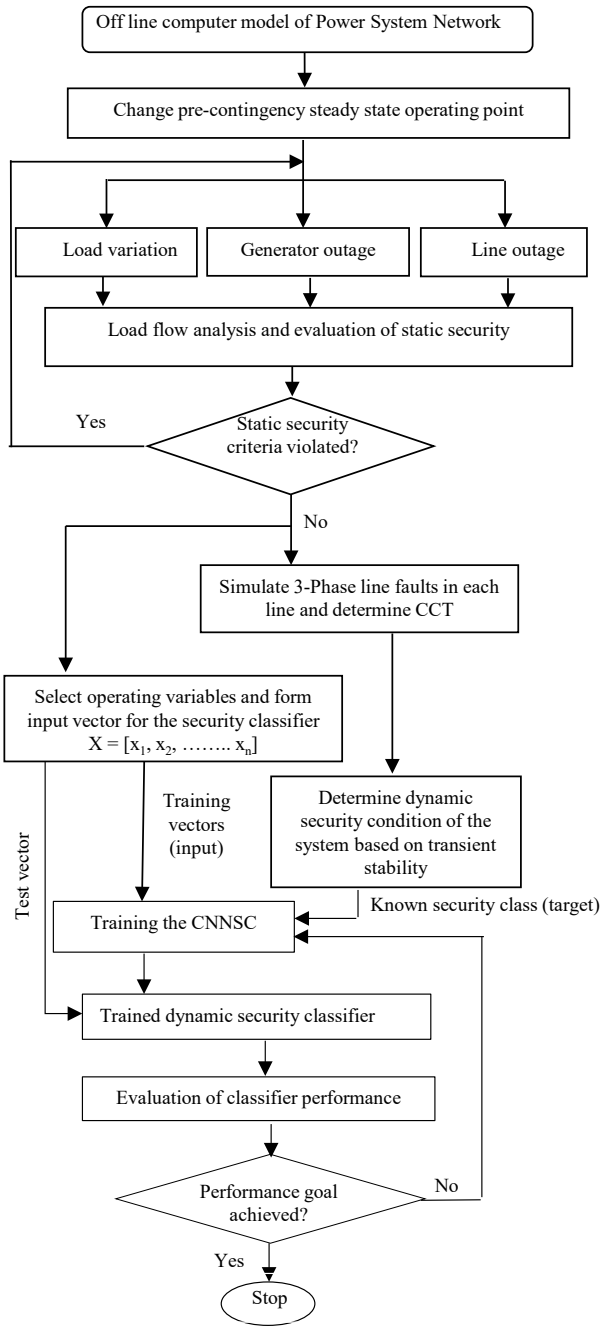

Figure 1. Conceptual diagram of the proposed CNNSC.

(learnable weights and biases), and be able to differentiate between them. Comparatively speaking, a ConvNet requires substantially less pre-processing than other classification methods. Contrary to earlier systems where filters had to be manually constructed, ConvNets are able to learn these filters and their attributes.

The construction of a ConvNet was influenced by the organization of the Visual Cortex and is comparable to the connecting network of neurons in the human brain. Individual neurons only respond to stimuli in the Receptive Field, a small area of the visual field. The complete visual field is made up of many overlapping fields like this. By using the appropriate filters, a ConvNet may be able to accurately capture the spatial and temporal dependencies in a picture. Because there are fewer parameters to take into account and the weights can be reused, the architecture enables a better fitting to the picture dataset. To better understand the complexity of the image, the network may be trained.

3.0 Off-Line Simulation of the Test System and Training the CNNSC

Because of its topological spread and complexity, the IEEE 39-bus system was selected as the optimal medium-sized system for all off-line research. The suggested online Fault Severity Ranking Scheme module is tested

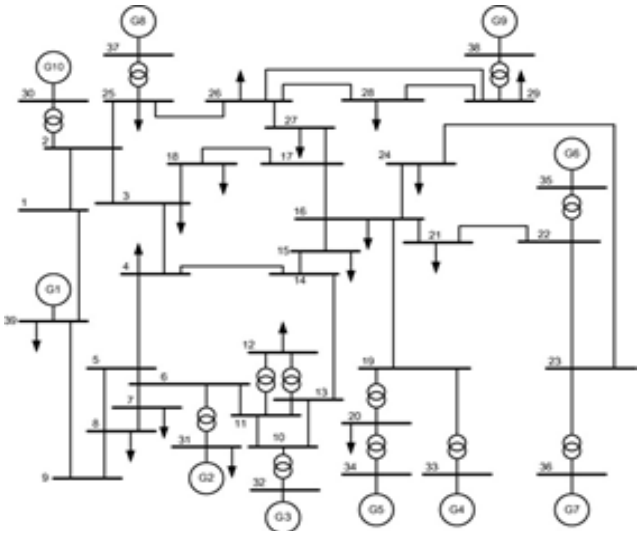

Figure 2. IEEE 39-bus test system.

on the IEEE 39-bus. This system consists of 10 machines, 10 generators, 34 transmission lines, 12 transformers, 29 load buses, and 2 shunt capacitors. A single-line schematic representation of the system is shown in Figure 2.

Numerous load-flow simulations in the IEEE 39-bus test system with variable initial starting conditions, such as generation and load variations, and changed operating scenarios, such as generator and line outages and their combinations (OCs), were successful in producing a large number of diverse and evenly distributed pre-contingency steady-state operating scenarios. We modelled the most accurate operating circumstances by simulating simultaneous load changes in about one-third of the system load buses at a time. Any arbitrary 10 buses were randomly chosen at a time as candidates for load variation in 5 steps outof the total 29 load buses (0.5, 0.75, 1.0, 1.25 and 1.5 p.u. of thebase load of the buses).

The following 10 arbitrary buses were used in the same manner, and so on. All of the system load buses were covered after 20 iterations of the operation. This resulted in the development of 5×20 = 100 unique, evenly spaced, and yet extremely plausible loading scenarios. Then, single-generator outage conditions were added to each of the aforementioned 20 loading scenarios. With the IEEE 39 bus system's 10 number generators and the additional case of "no generator Visual Cortex is structured. The Receptive Field, a restricted region of the visual field, is the only place where individual neurons respond to inputs. The complete visual field is madeup of many overlapping fields like this. By using the appropriate filters, a ConvNet may be able to accurately capture the spatial and temporal dependencies in a picture. Because there are fewer parameters to take into account and the weights can be reused, the architecture enables a better fitting to the picture dataset. To better understand the complexity of the image, the network may be trained. outage," a total of 100x11 = 1100 different load-generation-generator outage scenarios were simulated. Multiple generator outages were not taken into considerationsince they would vastly increase the number of operational situations that are significantly less credible in real-time operation and would therefore be of little use as training examples. Based on the same concept, single line-outage cases were seen as another form of variation in OC. For the test system's 34 lines, 100 load-generation patterns

were paired with 34 single line-outage scenarios and the additional condition of "no line-outage" in order to duplicate 3500 mutually exclusive load-generation-line outage combinations. Thus, a total of 1100+3500 = 4600 unique yet realistic initial steady-state OCs were simulated in order to provide a thorough representation of the whole operating areaof the IEEE 39-bus test system.

3.1 Selection of Input Variables and Formation of Input Pattern Vector

The choice of input information is crucial when training the CNNSC. The CNNSC input data was picked for training beginning with the choice of PMU measurable operating variables, also known as "primary variables," which were believed to be reflective of the dynamic characteristics of the system and closely correlated with the post-contingency system security. The 146 major variables used for the IEEE 39-bus test system are listed in Table 1. These variables subsequently make up the CNNSC's "input vector". The created input vector has the following form: X = [VBk, δBk, PLin x-y, QLin x-y], where k denotes the kth system bus and x-y denotes the transmission line that connects bus x and bus y. In order to create a comprehensive set of input pattern vectors, X was determined for each of the previously described 4600 typical Operating Scenarios (OCs). These vectors were then transmitted to the CNNSC for classification of the OCs based on transient stability.

3.2 Classification of Training Samples by CNNSC

Off-line CNNSC training was accomplished via cross-validation with CCT of the line faults. The training set was developed using a random sampling of 3000 out of the 4600 pre-contingency operating situations defined in section 4 (about 2/3 of the total data). One-third of the total data, or the remaining 1600 cases, were kept as test samples. The simulation produced about 16% of unsecured pre- contingency Operating Scenarios (OCs), while the other 84% were secure OCs. Table 2 summarises the distribution of the secure and insecure OCs in the training and testing dataset.

The confusion matrix in Table 3 illustrates the CNNSC's training performance. It is discovered that

Table 1. The initial pre-selected primary system variables

Primary System Variables	Symbolused	Number of variables
"Voltage magnitude of all bus"	VB	39
"Voltage angle of all bus"	∂B	39
"Line active power flow"	PLin	34
"Line reactive power flow"	QLin	34
Total		146

Table 2. Training and test data for the CNNSC

Dataset	Count	%
Total no of OCs	4600	100%
No of insecure OCs	736	16%
No of secure OCs	3864	84%
No of training OCs	3000	65%
No of test OCs	1600	35%

Table 3. "Confusion Matrix" of the CNNSC for 3000 training cases

		Predicted		
		Secure	**Insecure**	
Actual	**Secure**	TP = 2240	FN = 35	TP + FN = 2275
	Insecure	FP = 10	TN = 715	FP + TN = 725
		TP + FP =2250	FN + TN =750	N = 3000

training accuracy is high. Ten of the 725 unsecured OCs in the training set were incorrectly classified as secure OCs, while the remaining 715 OCs were correctly classified as insecure OCs. While the remaining 2275 secure OCs were accurately classified as secure OCs, 35 of the 2275 secure OCs were incorrectly classified as insecure OCs. In Table 3: "TP represents True positive FP represents False Positive FN represents False Negative and TN represents True Negative"

4.0 Performance Evaluation of the CNNSC in the Unseen Test Cases

Using 1600 never-before-seen test operational scenarios, the CNNSC's classification accuracy was assessed after it had successfully undergone training. Table 4 displays the findings of the confusion matrix's security state classification for the 1600 unseen OCs. With only 16 misclassifications, the CNNSC was able to classify the unseen cases effectively. A variety of criteria were created and applied to judge the effectiveness of the planned CNNSC. The accuracy 'a' of the classifier was defined as the probability of performing a correct classification, which is the ratio of the number of correct classifications to the total number of exemplars: $a = \frac{\sum G_{ij}}{N}$ where G_{ij} is the i^{th} diagonal element of the confusion matrix. N is the number of exemplars.

The probability of classifying anything incorrectly was determined to be e = 1-a, or the misclassification rate. A variety of metrics have been employed to assess the effectiveness of the classifier, including:

"Classification Accuracy" = $(TP + TN)/N$
"Positive misclassification rate (PMR)" = $FP/FP + TP$
"Negative misclassification rate (NMR)" = $FN/FN + TN$

Other well-known classification algorithms as the "Random Forest method" (RF)[15], "Support Vector

Table 4. "Confusion matrix" of the CNNSC for 1600 randomtest cases

		Predicted		
		Secure	**Insecure**	
Actual	**Secure**	TP = 1189	FN = 38	TP + FN =1227
	Insecure	FP = 11	TN = 362	FP + TN =373
		TP + FP =1200	FN + TN =400	N = 1600

Table 5. Comparison of "classification accuracy" of different classifiers

Data set	Metrics	CNN	RF	SGB	SVM	MLS
Test set	Classification Accuracy (%)	97	92	82	89	86
	Composite Misclassification rate	0.03	0.08	0.18	0.11	0.14
	Positive Misclassification rate	0.01	0.13	0.22	0.19	0.18
	Negative Misclassification rate	0.09	0.1	0.29	0.2	0.24

Machine" (SVM) [16], and "Method of Least Squares" (MLS)[17] were also examined in order to compare the prediction accuracy of the CNN approach. Table 5 displays the relative effectiveness of the various classification techniques. The outcomes show that the CNN-based classifier outperforms other approaches in terms of classification performance.

5.0 Conclusion

The research presented a pattern recognition approach for assessing the security of power system networks based on transient stability. A powerful Convolution's Neural Network based Security Classifier (CNNSC) was created and trained to predict and categorize the operating states of the power system prior to a contingency into secure and insecure classes using PMU-based measured typical system variables like voltage, voltage-angle, and power flow. The CNNSC was trained off-line using the results of the dynamic security computation using the Critical Clearance Time (CCT) of line-faults as a measure of transient stability. The proposed method was evaluated using the IEEE 39 bus test system and yielded encouraging results. The IEEE evaluation of the developed CNNSC's performance contrasted its performance with that of other related classifiers, such as MLS, RF, SGB.

6.0 References

1. Kundur P. Power System Stability and Control. McGraw-Hill Education; 1994.
2. Kundur P, Paserba J, Ajjarapu V, Andersson G, Bose A, Canizares C, Hatziargyriou N, Hill D, Stankovic A, Taylor C, Van Cutsem T, Vittal V. Definition and classification of power system stability IEEE/CIGRE joint task force on stabilityterms and definitions. IEEE Trans Power Syst. 2004; 19(3):1387–401. https://doi.org/10.1109/TPWRS.2004.825981
3. Sauer PW, Pai MA. Power System Dynamics and Stability. Prentice-Hall, New Jersey; 1998.
4. Laufenberg MJ, Pai MA. A new approach to dynamic security assessment using trajectory sensitivities. IEEE Transactions on Power Systems. 1998; 13(3). https://doi.org/10.1109/59.709082
5. Chiang HD, Wang CS, Li H. Development of BCU classifiers for on-line dynamic contingency screening of electric power systems. IEEE Trans on Power Systems. 1999; 14(2):660-6. https://doi.org/10.1109/59.761895
6. Zhang R, Xu Y, Dong Z, Wong PK. Post-disturbance transient stability assessment of power systems by a self- adaptive intelligent system. IET Generation, Transmission and Distribution. 2015; 9(3):296–305. https://doi.org/10.1049/iet-gtd.2014.0264
7. Morteza S, Wu N, Bay SJ. Transient stability assessment of large lossy power systems. IET Generation, Transmission and Distribution. 2018; 12(8):1822-30. https://doi.org/10.1049/iet-gtd.2017.0864
8. James QJ, Hill JD, Lam SYA, Gu J, Li KOV. Intelligent time-adaptive transient stability assessment system. IEEE Transactions on Power Systems. 2017; 33(1):1049-58. https://doi.org/10.1109/TPWRS.2017.2707501

9. Fouad A, Vittal V. Power system transient stability analysis using the transient energy function method. International Journal of Electrical Power and Energy System. 1988; 10(4):233-146. https://doi.org/10.1016/0142-0615(88)90011-7
10. Hiskens IA, Hill DJ. Energy functions, transient stability and voltage behaviour in power systems with nonlinear loads. IEEE Transactions on Power Systems. 1989; 4(4):1525-33. https://doi.org/10.1109/59.41705
11. Vu TL, Turitsyn K. Lyapunov functions family approach to transient stability assessment. IEEE Transactions on Power Systems. 2016; 31(2):1269-77. https://doi.org/10.1109/TPWRS.2015.2425885
12. Rituparna M, Abhinandan D. Development of an ensemble decision tree-based power system dynamic security state predictor. IEEE Systems Journal. 2020; 14(3):3836-43. https://doi.org/10.1109/JSYST.2020.2978504
13. Rituparna M, Abhinandan D. Real-time dynamic security analysis of power systems using strategic PMU measurements and decision tree classification. Electrical Engineering, Springer; 2020. https://doi.org/10.1007/s00202-020-01118-z
14. Ren LY, Tian F, Yan JF, Yu Z, Su H, Wu T. Online application and fast solving method for critical clearing time of three-phase short circuit in power system. International Journal of Smart Grid and Clean Energy. 2013; 2(1). https://doi.org/10.12720/sgce.2.1.93-99
15. Tin Kam H. The random subspace method for constructing decision forests. IEEE Transactions on Pattern Analysis and Machine Intelligence. 1998; 20(8):832-44. https://doi.org/10.1109/34.709601
16. Gomez FR, Rajapakse AD, Annakkage UD, Fernando IT. Support vector machine-based algorithm for post- fault transient stability status prediction using synchronized measurements. IEEE Transactions on Power Systems. 2011; 26(3):1474-83. https://doi.org/10.1109/TPWRS.2010.2082575
17. Lilley RW. Demonstration of MLS advanced approach techniques. IEEE Aerospace and Electronic Systems Magazine. 1990; 5(5):41-6. https://doi.org/10.1109/62.54625