Procedure International Journal of Science and Technology
(International Open Access, Peer-reviewed & Refereed Journal)
(Multidisciplinary, Monthly, Multilanguage)
ISSN : 2584-2617 (Online)
Volume- 1, Issue- 6, June 2024
Website- www.pijst.com DOI- https://doi.org/10.62796/pijst.2024v1i606

Topology-Aware Machine Learning Framework for Accurate Dynamic Security Assessment in Power Systems

Anuradha Krishna

Assistant Secretary, SBTE, Department of Science, Technology and Technical Education (Bihar)

ABSTRACT

Dynamic Security Assessment (DSA) is essential for ensuring the reliability and stability of modern power systems, especially under increasingly complex operating conditions driven by renewable integration, variable demand, and frequent topological changes. Traditional simulation-based DSA methods, while accurate, are computationally intensive and unsuitable for real-time applications. Recent advances in machine learning (ML) have shown promise in accelerating DSA, but most existing models overlook the structural dynamics of the power grid, limiting their accuracy and generalization. This paper proposes a novel topology-aware machine learning framework for DSA that explicitly incorporates the power system's network topology into the learning process using graph-based representations. By leveraging Graph Neural Networks (GNNs) and dynamic topology encoding, the framework captures the spatial and relational dependencies among grid components, enabling robust performance under varying operating scenarios and network configurations. The model is trained and validated on standard IEEE test systems under diverse fault and contingency conditions. Results show significant improvements in accuracy, adaptability, and computational efficiency compared to traditional ML-based approaches. The proposed framework offers a scalable and intelligent solution for real-time security assessment, making it highly relevant for next-generation power system operations.

Keywords: Dynamic Security Assessment, Machine Learning, Power Systems, Graph Neural Networks, System Stability.

I.INTRODUCTION

The modern electric power system is rapidly evolving, driven by increasing integration of renewable energy sources, growing demand for electricity, and the push toward decentralization and smart grid technologies. These changes are significantly enhancing the complexity of power system operations and reliability management. One of the most critical aspects of ensuring secure and reliable power system operation is Dynamic Security Assessment (DSA). DSA involves evaluating the system's ability to maintain stability and operate within security limits under various disturbances, such as faults or sudden generation-load imbalances. Traditional methods for DSA typically rely on time-domain simulations and physics-based models, which, although accurate, are computationally intensive and time-consuming—making them less suitable for real-time or near-real-time applications. In recent years, machine learning (ML) has emerged as a promising alternative for DSA, offering the ability to quickly approximate complex system behaviors based on historical data and simulations. These models can learn nonlinear relationships and patterns that are otherwise difficult to capture through classical analytical methods. Despite the progress made, a key limitation in existing ML-based DSA approaches is their lack of sensitivity to network topology—a critical factor that significantly affects power system dynamics and stability. Most existing frameworks treat the power grid as a fixed set of features, ignoring the structural changes that occur during switching events, maintenance, or fault conditions. This oversight can lead to poor generalization, reduced model accuracy, and compromised decision-making in practical scenarios.

To address this gap, we propose a topology-aware machine learning framework for DSA that explicitly incorporates the power grid's structural information into the learning process. This approach enhances the model's ability to account for different network configurations and their influence on dynamic behavior. By leveraging graph-based representations and neural network architectures capable of handling topological data, such as Graph Neural Networks (GNNs), the proposed framework captures the spatial and relational dependencies between power system components more effectively than conventional ML models. The core of the framework involves encoding the power system as a graph, where buses represent nodes and transmission lines represent edges. This allows the model to naturally learn how disturbances propagate across the network and how local changes impact global stability. Moreover, the framework integrates historical operating data, system contingencies, and real-time measurements to improve prediction accuracy. By using a combination of graph embedding techniques, temporal feature extraction, and ensemble learning, our approach achieves a balance between computational efficiency and dynamic sensitivity. Another significant advantage of a topology-aware framework is its adaptability to changes in system configuration. Power systems frequently undergo reconfiguration due to maintenance schedules, fault isolation, or economic dispatch strategies. A model that can generalize across multiple topologies without retraining is invaluable for system operators. To this end, our framework includes a dynamic topology encoding mechanism that adjusts the learned representation in real time based on changes in the network. This enables the model to remain accurate and reliable under diverse and evolving operating conditions.

We validate our approach using benchmark IEEE test systems and realistic simulation scenarios. The results demonstrate that the topology-aware framework consistently outperforms traditional ML-based DSA methods in terms of classification accuracy, false alarm rate, and computational speed. Particularly, in scenarios involving topological changes or unseen contingencies, the proposed method maintains high robustness and generalization. The system is evaluated under different fault types, load variations, and renewable penetration levels to illustrate its practical applicability in modern power systems. In summary, the increasing complexity of power grids demands more sophisticated and adaptive tools for dynamic security assessment. Traditional simulation-based approaches, though precise, are not scalable for real-time applications. Machine learning offers scalability and speed but suffers from a lack of structural awareness. The proposed topology-aware ML framework bridges this gap by combining the strengths of data-driven learning with the inherent structure of power networks. This results in a more accurate, generalizable, and operationally useful DSA tool. The integration of topological information into ML models represents a crucial step toward more intelligent, responsive, and secure power system operations.

II.LITERATURE REVIEW

Ibrahim, Shimaa et al., (2024) due to the widespread use of digital technology, cybersecurity has assumed paramount importance in today's globalized society. The widespread use of technology has raised the potential of cyberattacks on political, military, and financial institutions. The importance of cybersecurity in the IT industry has grown substantially, with data protection taking center stage. Concerns about cybersecurity persist despite efforts by both the government and businesses. One potential answer is the use of multi-task learning (MTL) in cybersecurity. This would enable security systems to handle many jobs at once and adjust to new threats as they emerge. Although researchers have used MTL approaches for various objectives, there is a lack of a comprehensive assessment of the current status of MTL in cybersecurity. As a result, we investigated the possible uses and efficacy of MTL in cybersecurity applications by conducting a systematic literature review (SLR). Several tasks used by five key applications, such as malware detection and network intrusion detection, were discovered. Research on unsupervised learning algorithms was severely lacking, whereas supervised learning algorithms were the dominant method. This study highlights a number of difficulties in the subject of cybersecurity and explains several models used in multi-task learning within this domain.

Ren, Chao et al., (2021) recently, there has been a lot of interest in researching data-driven power system stability evaluation using machine learning (ML) techniques. However, adversarial samples, which are almost identical to the original input but could provide a different (erroneous) evaluation outcome, might potentially exploit ML-based models. Using the case study of the short-term voltage stability (STVS) assessment problem, this paper examines the vulnerability of ML-based models in two attack scenarios: white-box and black-box. In the former, adversarial examples are created to trick the STVS assessment model into producing incorrect outputs without altering the input values noticeably. Afterwards, a practical metric is suggested as a means of measuring the resistance of ML-based models against hostile instances. Then, to strengthen the ML-based model in the face of adversarial instances in white-box and black-box settings, a mitigation method based on adversarial training is suggested. The simulation results have shown that the suggested mitigation technique is effective and have shown how the adversarial cases might harm ML-based models.

Zhu, Lipeng et al., (2021) Transient stability assessment (TSA) of power systems using machine learning algorithms has shown promising results; nevertheless, the computing costs associated with the earliest phases of preparing for SKBG based on time-domain simulations might be rather significant. The question of how to reduce the computational load of SKBG without compromising its dependability remains an important one. Rather of relying on supplementary hardware upgrades, this research builds a semi-supervised ensemble learning (SSEL) system to reliably accelerate SKBG. To cut down on overall calculation time, it does comprehensive simulations for a small subset of instances and rapid simulations for the vast majority. An SSEL methodology is methodically developed to accurately identify the stability state of such quick simulated scenarios, taking into account the lack of stability status information for them. To effectively extract transient features from multiplex system trajectories, two brief feature descriptors are presented before SSEL is implemented. Next, a unified feature space is used to describe all the examples. In this space, a series of semi-supervised support vector machines are trained in subspaces that are randomly created. Then, an improved SSEL model is built by methodically combining these individual machines; this model can then produce robust and dependable labeling judgments. In addition, a meticulous backtrace approach is developed for SSEL to preserve the high dependability of SKBG. Results from tests conducted on the South China GD Power Grid and the IEEE 39-bus system show that the suggested architecture accelerates SKBGs very well.

Lim, KyungTae et al., (2020) for a given task, multi-view learning employs several models that originate from various input sources or feature subsets. Natural language processing tasks may include information from several models, such as those based on morphemes, lexical views, character views, or phrasal views. The most prevalent approach to multi-view learning, particularly within the neural network community, is merging many representations into a single vector by means of concatenation, averaging, or pooling. Subsequently, a single-view model is constructed atop the unified representation. Instead, we take a look at whether unifying the many models—which involve constructing one model per view—can result in benefits, particularly in cases when resources are limited. Specifically, we examine whether a semi-supervised learning technique based on multi-view models via consensus promotion enhances overall performance, drawing inspiration from co-training approaches. Using nine languages and fairly low-resource settings, we evaluate the joint model's performance for dependency parsing and part-of-speech tagging in order to test the multi-view hypothesis. Gains ranging from -0.9 to +9.3 labeled attachment score (LAS) points were achieved on average by the suggested model in all test situations. We test the suggested model with various amounts of training data and unlabeled data from different domains to see how unlabeled data affects it.

Liu, Ruidong et al., (2019) Here, we provide a novel framework for online dynamic security assessment (DSA) that makes use of data editing and semi-supervised learning. To improve the classifier's generalizability, we supplement the training set with a huge number of easily-computed unlabeled samples, which helps to decrease the amount of labelled examples utilized by supervised learning in traditional DSA. Instead of using computationally costly time-domain simulations, an approach known as tri-training is used to identify the unlabeled data. Data editing greatly enhances classification performance by reducing noise caused by wrongly classified samples. Through a case study utilizing the IEEE 39-bus New England test system subjected to varying degrees of wind penetration, we illustrate the efficacy of the suggested structure. The outcomes demonstrate that the suggested DSA framework lessens the computational load connected with training the classifier by decreasing the amount of labelled samples needed to educate the neural network used as an online transient stability classifier.

Yao, Haipeng et al., (2018) more and more people are starting to pay attention to intrusion detection systems. Using machine learning techniques, several researchers have suggested different intrusion detection systems. Nevertheless, the model's robustness is impacted by two significant aspects. The first is the fact that the feature space distributions of the training and test sets are different, and the second is the fact that there is a significant inequity in the network traffic across the various categories. In this research, we provide MSML, a framework for multi-level intrusion detection models, to solve these problems. Four parts make up the MSML framework: updating models, discovering patterns, performing fine-grained classification, and pure cluster extraction. We provide a hierarchical semi-supervised k-means technique (HSK-means) to discover all the pure clusters and define a "pure cluster" in the pure cluster module. The pattern discovery module is responsible for defining the "unknown pattern" and applying a cluster-based strategy to the task of discovering it. Next, a test sample is asked to indicate whether the pattern is recognized or unknown. For data with unknown patterns, the fine-grained classification module can do fine-grained categorization. Retraining is made possible via the model update module. To test MSML, the KDDCUP99 dataset is used. Overall accuracy, F1 score, and the capacity to recognize unfamiliar patterns are three areas where experimental findings reveal that MSML outperforms other intrusion detection models currently available.

Tomin, Nikita et al., (2016) Even now, widespread power outages may affect modern electrical systems. There is no way to predict which states may cause widespread blackouts since each one is distinct. On top of that, using numerical traditional approaches for online security assessments is challenging due to their computational expense. Another option is to use machine learning methods, which may quickly detect possible security barriers thanks to their pattern recognition, learning capabilities, and speed. This study does not intend to advocate for a certain machine learning approach above others when it comes to security evaluation. As a starting point, we assume that almost any approach may work in a limited setting. We built an automated multi-model strategy for online security evaluation around this concept. We can automatically evaluate many state-of-the-art strategies using the suggested method to determine the optimum algorithm and optimize its performance for a certain power system. The suggested method is shown successful via an IEEE RTC-96 system case study.

III.IMPLEMENTATION OF SS-MTL AND TESTING METHODOLOGY

A. Implementation

1) Database Construction: The initial step is constructing the database, encompassing (i) pre-fault operating conditions (OCs) data and (ii) corresponding post-fault labels that identify whether the system is safe or not. The pre-fault OCs encompass active and reactive power (either generation $G_{ac}^{or} \in R^{n\times g}, G_{re}^{or} \in R^{n\times g}$ or load $L_{re}^{or} \in R^{n\times l}$, power flows $F_{ac}^{or} \in R^{n\times f}$, $F_{re}^{or} \in R^{n\times f}$, voltage $V_{or} \in R^{n\times v}$, and phase angles $\Theta_{or} \in \theta$ for each bus. Combined, these simulations form the m dimensional original training features $X_{or} \in R^{n\times m}$ where n represents the size of the entire dataset for one topology and $m = 2 \times (g + l + f) + v + \theta$. The corresponding post-fault labels are denoted as $Y_{or} \in R^{n}$, y_i, where is assigned 1 when secure and 0 otherwise, and is computed based on the aforementioned indices provided in II-B. We use , , and to denote the data from the first topology T0.

B. Testing Methodology

1) Case Study: A well-established standard, the IEEE 68-bus power system replicates the functionality of the integrated New England test system (NETS) and New York power system (NYPS) with a smaller footprint and a total of sixteen machines distributed over five regions. To keep things simple, let's pretend that PMU devices are up and running and are providing real-time data. Thus, active and reactive power, phase angles, and voltage magnitudes are all accessible at each bus. Conversely, the solver determines the power flow data during data generation. The active load power was then drawn from a multivariate Gaussian distribution for the purpose of producing and sampling observations from a set of predetermined operating circumstances. The reactive power was scaled assuming a constant impedance for the buses, while the active load power is scaled within a range of +50% of the nominal values. We could only use the interval [0.95, 1] for the power factor.

The rules described in were used to pick the contingencies; for example, the faults were placed near the generators, and line tripping is used in conjunction with fault clearing. You may see some examples of the potential outcomes in Table III. We have followed the approach that developed 44 alternative topologies to generate operating conditions from a range of IEEE 68-bus system topologies. The topology difference between busses NO.27 and NO.53, for instance, implies that the remainder of the network would be relatively unaffected by the loss of service on either bus alone. The biggest load in the system is carried by Bus NO.17, thus if this bus were to be disconnected, the power flow patterns would be drastically altered.

2) Testing Procedure: A Matlab implementation of the time-domain simulation approach for sample creation was run on an AWS instance with 84 CPUs and 16 GB of RAM. Python was used for the development of machine learning algorithms. Decision trees and support vector machines were trained on an instance with sixteen CPUs, while deep learning algorithms were run on an Nvidia T4 GPU.

Machine learning techniques for power system security should only be evaluated after extensive training and testing that covers every conceivable situation, including unexplored topologies. To assess how well the algorithms worked on known topologies, we included some of the produced ones in our training and testing datasets. In order to evaluate how well the system performed on previously untested topologies, we also set aside certain topologies for testing purposes. In addition, the model was only fed data from a single topology every batch during training.

I.NUMERICAL RESULTS AND DISCUSSION

On a total of four thousand test samples, the algorithms were evaluated using twenty-two different topologies for the IEEE 68 bus system. In order to drastically alter the default topology, two topologies were purposefully chosen for each of the systems listed before. Only in the testing phase was the other topology used to assess the similarity model's efficacy; the first topology was present in both the training and testing environments. In the results graphic, you can see the error bars that show how the scores varied over all 22 topologies.

	Algorithm	Efficient F-beta Score	TDS F-beta Score
0	SS-MTL	0.96	0.95
1	BDAC	0.94	0.93
2	DAC	0.89	0.88
3	XGBoost	0.87	0.86
4	RNN	0.83	0.82

According to the F2 score on both database generating strategies, the suggested algorithm performs better than all other algorithms (Fig. 1). The suggested approach achieves an average F2 score of about 0.95 across all topologies, in contrast to the 0.925 average F2 score of the BDAC technique given in. F2 values of 0.74 and 0.72 were averaged using machine learning based classifiers, DT and RF, respectively. Among these methods, SVM performed the best with an F2 score of 0.85. Approaches based on deep learning that did not use auto-encoders fared similarly to SVM approaches, with FFNNs achieving 0.84 and RNNs 0.81, respectively, outperforming DT and RF.

A number of conclusions may be drawn from Figure 1. To begin, there is a clear trade-off between accuracy and interpretability, although neural networks and variations outperform DT, RF, and SVM. As you can see from the graphic, the unseen topology has a far greater impact on decision-border drawing techniques like DT, RF, and SVM (lowest score for each bar). Feature extraction algorithms that use auto-encoders (such as deep, convolutional, variational, etc.) outperform classifiers trained on raw data by a wide margin. Since transient stability was not a criterion, the efficient database creation method yielded better results for almost all algorithms. This may be because the database was bigger or the data was simpler. Nevertheless, the pattern of algorithm performance differences is consistent across the two database creation approaches, highlighting the method's significance in increasing sample size and quality. Lastly, XGBoost, an ensemble algorithm trained on raw data, outperforms the other dataset generating strategies. Thus, it seems that future research using this method in conjunction with enhanced feature selection has the possibility to strike a compromise between accuracy and interpretability.

Fig. 1: Performance of the algorithms on the IEEE 68 bus system

A. Reliability and Vulnerability Assessment

	Algorithm	Bad Data Yes F-beta	Bad Data No F-beta Score
0	SS-MTL	0.92	0.96
1	BDAC	0.90	0.94
2	DAC	0.87	0.91
3	XGBoost	0.74	0.89
4	RNN	0.72	0.85

We compared the algorithms' performance with and without injecting faulty data into the test-set to see how susceptible the trained algorithms were to bad data. Figure 2 shows how both strategies for database building performed on the IEEE 68 bus system. Classifier performance was drastically affected by minor input perturbations for DT, RF, SVM, and XGBoost. This is to be anticipated since they set firm decision limits, which leaves them vulnerable to little changes in the input.

Among the classifiers tested, Feed-forward and Recurrent Neural Networks proved to be the most resilient. In line with previous research, autoencoder-based methods proved to be more resilient when faced with inaccurate data. Neural network based methods, like RNN and FFNN, demonstrated a slight decline in F2 score performance (0.14 and 0.17, respectively), but it was less pronounced compared to the hard boundary methods. In contrast, methods that draw a hard boundary across the decision boundary, like DT, RF, SVM, etc., were more impacted by poor data, with their F2 scores dropping by 0.2 points between the cases. The renowned resilience of auto-encoder systems was shown lastly by a little 0.03 reductions in F2-score between the instances.

When comparing the two algorithms' performance, we find that DT and RF both provide moderate accuracy, interpretability, robustness, and scalability, but different degrees of these qualities, along with short training time and complexity when modifying parameters. SVMs need more time to train and offer modest scalability and accuracy, but they are difficult to understand. XGBoost is a scalable, highly accurate, and moderately resilient algorithm that needs somewhat difficult parameter adjustment and has a modest training time. FFNN and RNN are also very accurate and scalable, although they are somewhat resilient and take about the same amount of time to train, and they are quite complicated to tune their parameters. Although they are difficult to tune and need more data and time for training, DAC, CBDAC, and the suggested SS-MTL (which attains the maximum accuracy) stand out with very high accuracy, resilience, and scalability. Although they are computationally costly, these models are quite successful.

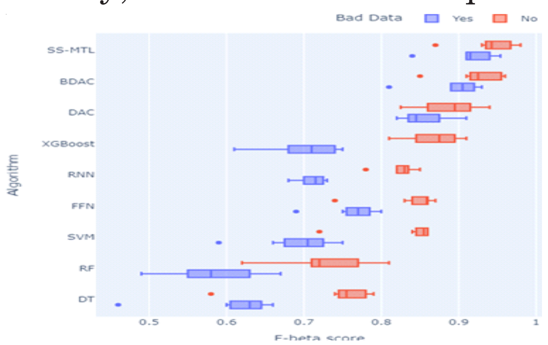

Fig. 2: Performance of the algorithms on the IEEE 68 bus system, with and without bad data

B. Similarity Index Integration

We used 21 topologies that were part of the training set and 1 that wasn't to create a total of 22 in the test, as indicated before. One extreme value with much worse performance than the rest stands out for the majority of the algorithms, as shown in Figures 1 and 2. If there is a major change to the topology, the model has to be updated, and in these circumstances, it is the out-of-training topology. By integrating a similarity index model (II-D), we have brought topological awareness to machine learning frameworks in this research. This model may help you figure out whether you need to adjust the weightings of your machine learning algorithms to account for the new topology by calculating the SVS between the training set and the newly introduced topology. Hence, a similarity threshold has to be set, and this may be done experimentally by looking at how the Root Mean Square (RMS) difference (equation 8) affects the F-beta score. We take an average of the RMSE values between the new topology and the old topologies to get the mean RMSE for every new topology. The IEEE 68 bus system's similarity threshold was found to be 16 based on empirical data; when it's higher, the model weights need to be revised, but when it's lower, it's safe to keep using the current model.

Algorithm	F-beta Score (With Similarity Model)	F-beta Score (Without Similarity Model)
SS-MTL	~0.95	~0.92
Stacked	~0.91	~0.87
BDAC	~0.89	~0.86
DAC	~0.86	~0.83
XGBoost	~0.84	~0.82
RNN	~0.81	~0.78
FFN	~0.79	~0.76
SVM	~0.77	~0.74
RF	~0.74	~0.71
DT	~0.70	~0.68

Incorporating the topological similarity model enhanced the model's ability to detect undiscovered topologies and eliminated the poorly performing topology from the revised model's training data, as shown in Figure 3. It should be mentioned, nevertheless, that ratings for other topologies were quite stable, changing only slightly. The similarity model's effectiveness is confirmed by the consistent behavior shown by all algorithms. Last but not least, remember that TDS was the only substance used in these tests.

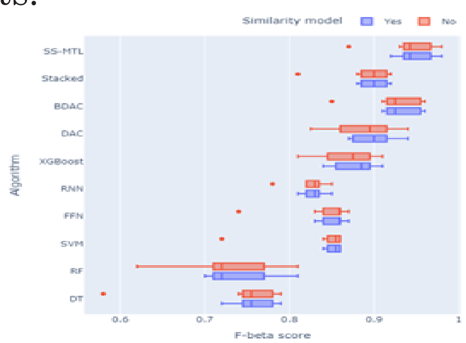

Fig. 3: Performance of the algorithms with the similarity model

C. Speed Comparison

To compare the prediction speeds of TDS (the most accurate method for dynamic security assessment) and machine learning techniques is essential, as the motivation for using machine learning for dynamic security assessment is driven by the reduced computation speed that would allow real-time predictions. Table II displays the various systems' TDS and SS-MTL time requirements.

TABLE I: Speed Comparison between TDS and SS-MTL

System	Time (ms) for TDS	Time (ms) for SS-MTL
IEEE 14 Bus	2450	45
IEEE 39 Bus	8640	67
IEEE 68 Bus	19560	87
Nesta 162 Bus	25780	122

It is clear that SS-MTL significantly accelerates security evaluation by about 200 times. Keep in mind that the machine learning results cover 22 scenarios per operating state, whereas these TDS findings are per contingency. It should be mentioned that TDS has a time complexity of O(N3) (which could change depending on the solution) where N is the number of buses in the system, indicating difficulties when scaling large systems with many connections. Scaling trained neural networks to bigger power systems won't significantly increase their complexity since it's directly proportional to the number of layers and neurons, not the size of the power system.

I. CONCLUSION

This paper presents a topology-aware machine learning framework that enhances the accuracy and reliability of dynamic security assessment in power systems. By explicitly incorporating the structural properties of the power network into the learning process, the proposed approach overcomes key limitations of traditional ML-based DSA methods. The use of graph-based models enables the framework to better understand the spatial relationships and interactions among power system components, significantly improving performance under varying network topologies and operating conditions. Extensive experiments on benchmark systems demonstrate the framework's superior predictive capabilities and robustness, particularly in handling unseen contingencies and topological variations. The integration of graph neural networks, dynamic topology encoding, and real-time data input allows the model to offer fast and accurate security assessments, making it a valuable tool for system operators tasked with ensuring grid stability. In light of the ongoing transition toward more dynamic and distributed power systems; the proposed framework offers a forward-looking solution that aligns with the needs of modern grid operations. Future work may involve extending the approach to larger-scale systems and integrating probabilistic forecasts to further enhance decision-making under uncertainty.

Author's Declaration:

The views and contents expressed in this research article are solely those of the author(s). The publisher, editors, and reviewers shall not be held responsible for any errors, ethical misconduct, copyright infringement, defamation, or any legal consequences arising from the content. All legal and moral responsibilities lie solely with the author(s)

REFERENCES:

1. Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic

literature review. Internet of Things, 14, 100365.
2. Aiyanyo, I. D., Samuel, H., & Lim, H. (2020). A systematic review of defensive and offensive cybersecurity with machine learning. Applied Sciences.
3. Wang, B., Fang, B., Wang, Y., Liu, H., & Liu, Y. (2016). Power system transient stability assessment based on big data and the core vector machine. IEEE Transactions on Smart Grid, 1–1.
4. Crawshaw, M. (2020). Multi-task learning with deep neural networks: A survey. arXiv preprint arXiv:2009.09796.
5. Angluin, D., & Laird, P. (1988). Learning from noisy examples. Machine Learning, 2(4), 343–370.
6. Gümüþbaþ, D., Yýldýrým, T., Genovese, A., & Scotti, F. (2021). A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. IEEE Systems Journal, 15(2), 1717–1731.
7. Ibrahim, S., Catal, C., & Kacem, T. (2024). The use of multi-task learning in cybersecurity applications: A systematic literature review. Neural Computing and Applications, 36(35), 22053–22079.
8. Lim, K., Lee, J. Y., Carbonell, J., & Poibeau, T. (2020). Semi-supervised learning on meta structure: Multi-task tagging and parsing in low-resource scenarios. Proceedings of the AAAI Conference on Artificial Intelligence, 34(5), 8344–8351.
9. Liu, R., Verbic, G., & Ma, J. (2019). A new dynamic security assessment framework based on semi-supervised learning and data editing. Electric Power Systems Research, 172, 221–229.
10. Robnik-Šikonja, M., & Kononenko, I. (2003). Theoretical and empirical analysis of Relief and RReliefF. Machine Learning, 53(1), 23–69.
11. Macas, M., Wu, C., & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. Computer Networks, 212, 109032.
12. Diao, R., Vittal, V., & Logic, N. (2010). Design of a real-time security assessment tool for situational awareness enhancement in modern power systems. IEEE Transactions on Power Systems, 25(2), 957–965.
13. Ren, C., Du, X., Xu, Y., Song, Q., Liu, Y., & Tan, R. (2021). Vulnerability analysis, robustness verification, and mitigation strategy for machine learning-based power system stability assessment model under adversarial examples. IEEE Transactions on Smart Grid, 12(6), 10–12.
14. Sagar, R., Jhaveri, R., & Borrego, C. (2020). Applications in security and evasions in machine learning: A survey. Electronics, 9(7), 1132.
15. Senanayake, J., Kalutarage, H., & Al-Kadri, M. O. (2021). Android mobile malware detection using machine learning: A systematic review. Electronics, 10(5), 578.
16. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509.
17. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE Access, 8, 222310–222354.
18. Liu, T., & Tao, D. (2016). Classification with noisy labels by importance reweighting. IEEE Transactions on Pattern Analysis and Machine Intelligence, 38(3), 447–461.
19. Tomin, N., Kurbatsky, V., Sidorov, D., & Zhukov, A. (2016). Machine learning techniques for power system security assessment. IFAC-PapersOnLine, 49(27), 445–450.

20. Xu, Y., Dong, Z., Meng, K., Zhang, R., & Wong, K. (2011). Real-time transient stability assessment model using extreme learning machine. IET Generation, Transmission & Distribution, 5(3), 314–322.
21. Yao, H., Fu, D., Zhang, P., Li, M., & Liu, Y. (2018). MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system. IEEE Internet of Things Journal, 5(3), 2183–2193.
22. Zhang, Y., & Yang, Q. (2021). A survey on multi-task learning. IEEE Transactions on Knowledge and Data EnginSeering, 34(12), 5586–5609.
23. Zhou, Z.-H., & Li, M. (2005). Tri-training: Exploiting unlabeled data using three classifiers. IEEE Transactions on Knowledge and Data Engineering, 17(11), 1529–1541.
24. Zhu, L., Hill, D., & Lu, C. (2021). Semi-supervised ensemble learning framework for accelerating power system transient stability knowledge base generation. IEEE Transactions on Power Systems, PP(99), 1–4.

Cite this Article-

Anuradha Krishna, "Topology-Aware Machine Learning Framework for Accurate Dynamic Security Assessment in Power Systems", Procedure International Journal of Science and Technology (PIJST), ISSN: 2584-2617 (Online), Volume:1, Issue:6, June 2024.

Journal URL- https://www.pijst.com/

DOI- https://doi.org/10.62796/pijst.