Impact of Topology Noise on Power Systems State Estimation Using a Temporal GCN Framework

Seyed Hamed Haghshenas
Department of Electrical Engineering
University of South Florida
Tampa, USA
seyedhamedhaghshenas@usf.edu

Mia Naeini
Department of Electrical Engineering
University of South Florida
Tampa, USA
mnaeini@usf.edu

***Abstract*—Graph Convolutional Networks (GCNs) have demonstrated great potential in analyzing energy data for learning the complex interactions and dynamics for supporting various functions within power systems including state estimation. However, these models are susceptible to noise in their underlying graph structure. In this paper, topology noise refers to the presence of a few additional or missing links in the power system graph model, caused by inaccurate information about the structure of the system and state of the lines or adversarial attacks on the graph's structure. The focus of this work is on evaluating the effects of topology noises or attacks and their location on the performance of a Temporal Graph Convolutional Network (TGCN) framework for power system state estimation.The results of this study demonstrate the TGCN framework's sensitivity in the presence of topology noises and attacks for state estimation in power systems. This study provides new insight regarding areas of vulnerability that could be exploited by such disturbances.**

***Index Terms*—Topology Noise, Poisoning Attacks, Smart Grids, State Estimation, Graph Convolutional Networks.**

I. Introduction

Power systems are being equipped with large number of monitoring and sensing devices generating large volume of data. The data collected from these system along with intelligent algorithms and machine learning (ML) approaches for analyzing them provide great opportunities for improving and supporting various critical functions in power systems. However, as the new approaches are being developed, it is essential to evaluate their sensitivity to various forms of deficiencies and vulnerabilities to attacks and misinformation.

State estimation is one of the critical functions in power systems that is essential for situational awareness and operation of the power systems. State estimation in power systems are traditionally performed using model-based techniques [1]; however, recent advances in the monitoring of power systems and large volume of energy data and intelligent data analytic techniques have provided new opportunities to support these important functions. Various ML techniques have been recently adopted for data-driven state estimation in power systems including neural network-based models [2]–[4]. The advantage of graph neural network (GNN) approaches in the state estimation problem in power systems and generally in analyzing the energy data is their capability in capturing the underlying interactions and structures within the data using a graph model [5]. In power systems, such interactions can be due to the physical structure of the system, physics of electricity and various operating rules governing the system. Such interactions can be captured in graphs, which have been extensively used in various analysis related to power systems. In many of such techniques, the physical structure of the power system (its physical components and their physical connections) are used as the graph model of the system. However, considering the large scale of the power systems and their stochastic dynamics, there may be scenarios in which the state of the whole system may not be fully observable and as such inaccuracies in the graph model of the system is possible. Moreover, adversarial topology attacks can also cause disruptions to the correct graph model for the system.

The focus of this paper is on topology noise, which refers to the presence of a small number of additional or missing links in the power system graph model. In this study, various topological disturbances, including topology attacks, are considered as instances of topology noises. It is shown in the literature that small graph noises or attacks can significantly affect the performance of the GNN models [6]. Understanding the effects of such noises or attacks on the performance of GCNs is crucial for reliable power system state estimation. Our primary objective is to evaluate the impact of topology noise and attacks on the performance of a Temporal Graph Convolutional Network (TGCN) framework for power system state estimation developed in our earlier work in [7]. By systematically introducing and varying the locations of topology noise, the goal is to gain insights into the sensitivity of the TGCN framework in the presence of these disturbances. The outcomes of this study are expected to provide valuable new insights into the behavior and vulnerabilities of the TGCN framework when confronted with topology noise or attacks during power system state estimation. Armed with this knowledge, decision-makers can make informed choices regarding the areas that require additional safeguards to mitigate the adverse effects of such disturbances.

In the subsequent sections of this paper, a detailed analysis of the experimental setup, methodology, and evaluation metrics employed to assess the performance of the TGCN framework under different scenarios of topology noise and attacks are presented. It is discussed that the obtained results

and drawn conclusions shed light on the sensitivity of the TGCN framework and its implications for state estimation in power systems.

II. Literature Review

The robustness and security of GNNs against adversarial topology attacks and topology noise have become critical concerns. Some of such work are focused on evaluating the vulnerability of the GNN model to topology attacks [6], [8], [9]. For instance, the authors in [8] investigated the vulnerability of GNNs to topology attacks and proposed a framework to generate adversarial examples. They demonstrated that targeted attacks, such as link addition or removal, can significantly degrade the performance of GNNs in tasks, such as node classification and link prediction.

Some of the related work focus on detecting the topology noise and attacks [10]. In addition, some efforts are focused on developing defense mechanisms against topology attacks [11]. In [12], the unexpected changes occurring in the graph topology are viewed as a noise in the structural information where a graph topology optimization method is proposed to improve the quality of structural information for the semi-supervised node classification tasks. Another related research [13] introduced a Parameterized Topological Denoising Network (PTDNet), which aims to enhance the performance and robustness of GCNs by eliminating edges that are not relevant to the task at hand. The authors in [14] introduced a noise-resistant GNN that can effectively denoise and densify the graph in a supervised approach, mitigating the negative impacts of noisy edges and promoting efficient message passing between labeled and unlabeled nodes. Transferability of topology attacks have also been studied in the literature. For instance, in [15], it was found that adversarial examples generated for one GNN model could also successfully deceive other GNN models, suggesting the existence of universal adversarial attacks against graph-based models.

While topology noise and attacks are prevalent in various domains and problems, they also pose a threat to models developed for power systems. For instance, the research presented in [16] examines the effects of topology poisoning attacks on the economic operation of smart grids, specifically focusing on the optimal power flow (OPF). One of the source of topology noise or attack in power systems is bad data injection attack to the system model. Several studies in the field of power grids have focused on detecting false data injection and their counter measures. For example, in the study presented in [17], a Temporal GNN model is proposed with the ability to locate and detect instances of false data injection attacks in smart grids. This model and similar ones, such as [18], assume that the grids' topology remains unaffected by malicious adversaries. In power system state estimation, the authors in [19] conducted one of the early studies of the graph topology attacks resulted from the man-in-the-middle attacks that modify data from specific meters and network switches to deceive the control center by providing incorrect network topology information. In another work [20], an Advanced Persistent Threat (APT) scenario is investigated where the attackers persistently and gradually manipulate the topology and structural configuration of the power grid to perturb the smart grid state estimation after successfully infiltrating the system. Recently, in [21] a Proactive Topology Obfuscation (ProTO) method is suggested to prevent active end-to-end topology attacks in network systems by adversaries, which aims to prevent them from obtaining the topology information of a target network. Finally, [22] introduces a GNN model for state estimation in smart grids. The model utilizes time-synchronized data from Phasor Measurement Units (PMUs) and effectively handles topology changes. The authors demonstrated the robustness of their GNN-based estimator in presence of non-Gaussian measurement noises and topology changes, respectively, by comparing it with a model-based Least Squares Estimator (LSE) and a regular Deep Neural Network-based State Estimator.

While many of the existing work in evaluating sensitivity analysis to topology noise and attacks are focused on the effects of systematically designed topology attacks and countermeasures for them in graph-empowered ML techniques, this work is focused on evaluating the effects of topology noise or attacks and their locations on the performance of a graph-empowered ML approach to state estimation in power systems. This study is an example study that can show vulnerable areas of power systems with respect to the ML models supporting their critical functions.

III. Methodology

A. Topology Noises and Attacks in Smart Grids

In the studies related to topology poisoning and edge perturbation in graph-empowered ML techniques, it is important to define the attack model on the structure or attributes of the edges and nodes of the graph. The assumption in such models is that the attacks are systematically designed to mislead the learning process for the largest impact on the performance. However, when it comes to topology noise, particularly in power system models, the inaccuracies in the graph structure and information may occur randomly due to missing and inaccurate information, or even false data injected by an attacker about the system structure. Specifically, the topology noise in power systems' models may occur due to the limited observability on certain parts of the system because of the large geographical scale of the system, limited or failed monitoring and measurement devices at certain areas, which can lead to unknown state of the components (e.g., a transmission line may have tripped but the system failed to record it), failures in the communication system responsible for transferring the data and more.

To model such scenarios, in this work, the original/correct graph of the system is denoted by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with the set of N vertices denoted by $\mathcal{V}$ representing the buses in the power system and the set of edges, denoted by $\mathcal{E}$, representing the power lines in the power system. The noisy topology is denoted by $\mathcal{G}' = (\mathcal{V}, \mathcal{E}')$, in which the set of edges is different from the original set of edges $\mathcal{E}$ in few extra or missing links enabling the modeling of different kind of inaccuracies and

attacks discussed earlier. While in a more general model, nodes as well as the attributes associated with the nodes and links may get noisy or be target of attacks, in this work the focus is on the noise/attack affecting the edges of the topology. To be specific, e_{ij}^{EN} denotes the case in which an extra edge between nodes i and j from $\mathcal{V}$ is present in the topology by mistake. Similarly, e_{ij}^{MN} denotes the case in which an edge between nodes i and j from $\mathcal{V}$ existed in the original graph $\mathcal{G}$, which is missing in the considered topology by mistake.

Note that the presented graph model $\mathcal{G}$ is one of the key inputs to the TGCN model, which allows capturing the structure of interactions in the binary $N \times N$ adjacency matrix of the model A, which is directly derived from $\mathcal{G}$ by considering zero when two nodes are not connected and one when they are. The topology noise will alter the adjacency matrix to a noisy one A', misleading the information sharing, message passing and graph convolutional functions in many of the GNN models. In this work, the effects of both missing and extra links in the power system graph model on the state estimation performance using the TGCN are studied. Next, the TGCN model adopted in this work from [7], is briefly reviewed.

B. TGCN Model for State Estimation

This study builds upon the TGCN framework, which was first introduced in [7]. In this section, a brief overview of the model is presented to set the stage for the following sections, where we delve into the effects of topology noise on the system state estimation within this framework.

The TGCN model in [7] utilizes a message-passing framework that is based on message passing and sharing information among neighboring nodes in the model. This model leverages neighbor information to estimate the state of unobservable nodes. Unobservable nodes here refer to the nodes that are not directly monitored using measurement devices, such as phasor measurement units (PMUs), due to lack or failure of such devices or communication failure to collect the data from such devices. Additionally, the model incorporates one-step ahead prediction by capturing both temporal and spatial interactions among the measurements. In other words, this TGCN model exploits both the temporal and spatial information (through the adjacency matrix of the system) to estimate the state of the whole system both at current time t and next time instant $t+1$. Here the electrical attributes, such as voltage magnitude V_n and phase angle θ_n at the buses of the system define the state of the components. The measurement vector for bus n at time t is denoted by $Z_{n,t} := [V_{n,t}, \theta_{n,t}]^T$. The state of the system at time t is defined as $X_t := [V_t, \theta_t]^T \in \mathbb{R}^{2N}$. The goal of the TGCN model is to learn the relationship between the observations and the state of all the nodes as well as learning the relationship between the past measurements and future state of the system. These two relationships can be captured through two non-linear functions, namely f_1 and f_2, to be learnt using the neural network model. A non-linear aggregation function f_1, combines the measurement information from the neighbors of the node to estimate the state of the unobservable nodes. This can be denoted as $Z_t = f_1(.)X_t$. The non-linear function f_2 captures the temporal relationships between the state and measurements, which can be denoted as $X_{t+1} = f_2(.)X_t$. Combining these two will show the process of the TGCN in the form of $X_{t+1} = F(Z_t, X_t)$, where $F(\cdot)$ represents the aggregated function responsible for estimating the system's state by capturing both the spatial and temporal information in the measurements.

The TGCN framework comprises two layers. The first layer is a graph convolution layer that utilizes a message passing framework to effectively capture the system's structure and interactions among its components. The graph convolution layer can be formulated as $\mathcal{H}^{l+1} = \sigma(\tilde{D}^{-\frac{1}{2}}\tilde{A}\tilde{D}^{-\frac{1}{2}}\mathcal{H}^l\mathcal{W}l)$, where $\tilde{A} := A + I_N$, with A representing the adjacency matrix and I_N being the identity matrix of size N. Additionally, $\tilde{D} := I_N \sum j\tilde{A}_{i,j}$ serves as the degree matrix. Here, $\sigma(\cdot)$ denotes the sigmoid activation function, and $\mathcal{H}^l$ represents the output of layer l with weights $\mathcal{W}_l$. The second layer of the TGCN framework is a Gated Recurrent Unit (GRU) layer, which is responsible for capturing temporal dependencies within the time-series data. The TGCN process can be summarized as $F(Z_t, A) = \sigma(\hat{A}\text{ReLU}(\hat{A}Z_t\mathcal{W}_0)\mathcal{W}_1)$, where $\hat{A} := \tilde{D}^{-\frac{1}{2}}\tilde{A}\tilde{D}^{-\frac{1}{2}}$. $\mathcal{W}_0 \in \mathbb{R}^{\beta\times\delta}$ and $\mathcal{W}_1 \in \mathbb{R}^{\delta\times\tau}$ are the model weights with β, δ, and τ representing the batch size, hidden units, and prediction length, respectively. More detailed information about the model's parameters, including the reset gate, update gate, memory unit, hidden state, and model bias, can be found in [7].

IV. Performance Evaluation Under Topology Noise

This section presents the performance evaluation of the state estimation using the TGCN framework under various scenarios of topology noise including missing and extra edges in the topology at different locations in the system.

To perform this evaluation, the IEEE 118 bus system has been utilized to generate a large dataset of synthesized PMU time-series through simulation using MATPOWER [23]. Following the methodology described in [7], the dynamics and temporal aspects are incorporated into the simulations by considering load profiles obtained from the New York Independent System Operator (NYISO) [24] sampled at a frequency of 30Hz. The recorded state variables in this simulation consist of time-series data for bus voltage magnitudes and angles. The IEEE 118 bus system consists of 186 transmission lines, including 7 dual links connecting the buses. Treating each dual link as individual link, the total number of links in the system becomes 179.

In order to better understand the effects of the location of topology noise, the missing and extra edge locations are organized as following: (1) Incorrect Missing Edge Scenario: In each scenario one node (bus in the power system) is considered as the target location of the noise and the lines connected to it are removed one by one in the graph model to form the $\mathcal{G}'$. The performance of the state estimation using TGCN with the generated $\mathcal{G}'$ for each node is averaged

over the missing line scenarios at that node. This scenario is examined at every bus of the system. (2) Incorrect Extra Edge Scenario: In each scenario one node is considered as the target location of the noise and one line is added at a time between the target bus and nearby buses within a predetermined radius, $\mathcal{R}$, which is selected to ensure the presence of at least one neighboring bus in close proximity to the target bus. This proximity is necessary to add the deceptive lines between them, which results in a new $\mathcal{G}'$ for each extra added line. In this work, the radius is selected to be $\mathcal{R} = 500$ based on the geographical coordinates of the buses shown in Fig. 2. Using this approach, 406 new links were considered to be added into the original graph of the system, $\mathcal{G}$. The performance of the state estimation using TGCN with the generated $\mathcal{G}'$ for each node is averaged over the extra line scenarios at that node. This scenario is examined at every bus of the system.

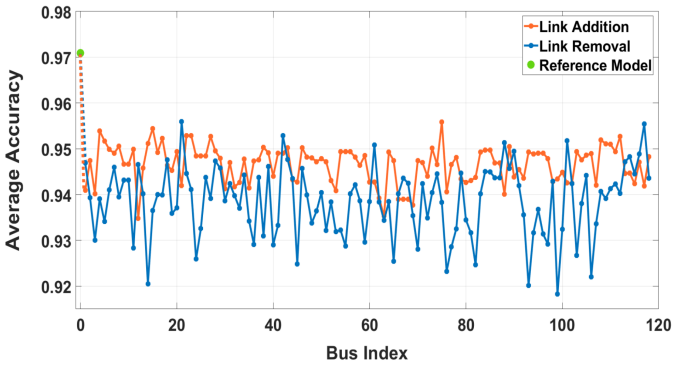

Fig. 1: Average accuracy of the TGCN framework as a function of topology noise/attack in the form of link removal and link addition at different buses of the IEEE 118 bus system. Note that the first data point represents the accuracy for the model with original topology $\mathcal{G}$

The TGCN model's performance is evaluated via RMSE and accuracy metrics and is shown in Fig. 1. This figure illustrates the average accuracy of the TGCN framework for the cases of incorrect missing edge scenario, referred to as Link Removal and incorrect extra edge scenario, referred to as Link Addition. While the results shown in Fig. 1 seem to exhibit a random pattern as they are organized by the location of the noise, i.e., bus index, there are some key observations to pay attention to. First, the drop in the performance of the TGCN framework for state estimation is more in the case of link removal as some essential topology information is lost due to the noise. Moreover, both in the case of link removal and link addition, the location of the noise/attack plays a key role in determining the severity of the impact. While the performance is minimally affected in certain locations, there are few locations that show more drops in the performance of the state estimation. This may suggest the need for improving the protection and monitoring services in such locations to prevent noise or attacks in more sensitive locations.

While these are important observations, the results presented in Fig. 1 do not offer insights into why certain locations could be more sensitive to topology noise and attacks. As such, more investigation is necessary in understanding the relation

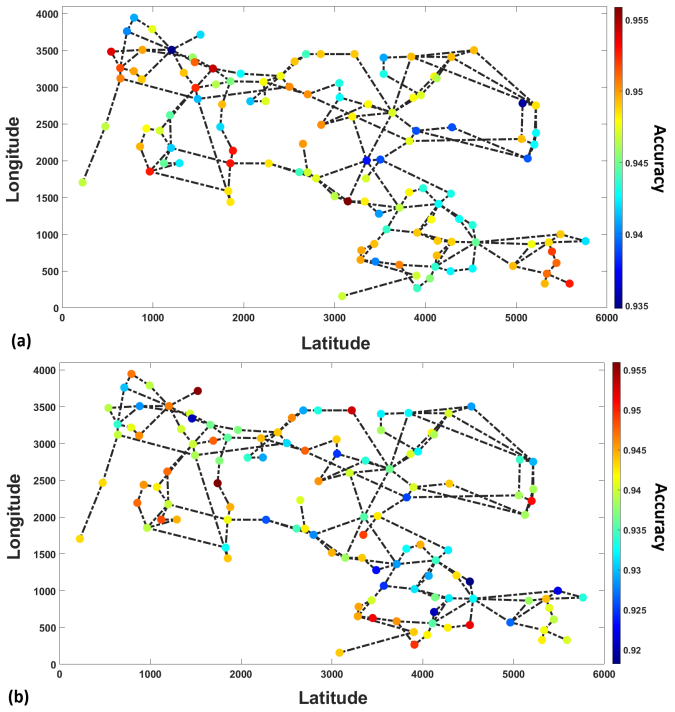

Fig. 2: Color-mapped representation of the IEEE 118 bus system topology illustrating the average accuracy of the TGCN framework when the noise in the topology is localized in one-hop vicinity of each bus. The state estimation accuracy is displayed under (a) link addition and (b) link removal scenarios.

between the noise sensitivity and the structure of the system. Figure 2 displays the IEEE 118 bus system topology in which the average accuracy of the state estimation under link addition (Fig. 2-a) and link removal (Fig. 2-b) scenarios are shown using a color-mapped over the buses of the system. This figure reveals that while certain locations are more sensitive to link removal, they are less sensitive to link addition. However, it is still not clear how the topology noise is related to the features of the system as clearly there is no correlation between the performance and the geographical location of the buses.

Next, the performance of the model is evaluated with respect to the location of the topology noise as a function of a topological feature of the buses, namely their degree (i.e., number of connection to adjacent buses in $\mathcal{G}$). In Fig. 3, the link removal and link addition scenarios, shown in Fig. 1, are sorted based on the degree of the buses. It can be observed that the state estimation model is less sensitive to topology noise at buses with lower degrees compared to those with higher degrees. In both scenarios of link removal and addition, up to the degree value of six, the accuracy of the state estimation decreases as the degree increases. However, for buses with higher degrees, there is no distinguished pattern in the model's performance although the accuracy in such cases are less than the topology noise at buses with less degree. Although the decreasing pattern does not fully capture the overall trend in the presented results in Fig. 3, it can be observed that topology noises at higher degree buses can impact the performance

more.

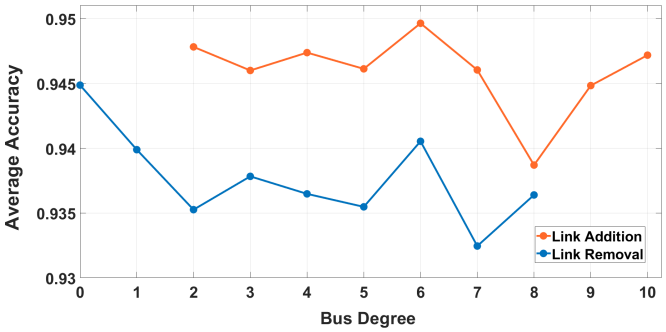

Fig. 3: Accuracy of TGCN framework for state estimation in the IEEE 118 bus system to reflect the impact of topology noise/attacks through link removal and addition as a function of target bus degree.

V. Conclusion

The vulnerability of the Graph Neural Network models to noise in the underlying graph structure is a concern, especially when the model is supporting critical functions, such as state estimation, in critical systems, such as power systems. Our study aimed to evaluate the effects of topology noise, which refers to the presence of additional or missing links in the power system graph model due to inaccurate information or deliberate adversarial attacks, and their location on the performance of a Temporal Graph Convolutional Network (TGCN) framework for power system state estimation. Through our analyses, it was discovered that topology noise in the form of missing links in the graph have more severe impact on average compared to topology noise in the form of incorrect extra edges in the graph. Moreover, it was observed that the degree of a bus, representing the number of connections it has with other buses, plays a crucial role in the network's response to topology noises. By understanding the sensitivity of the TGCN framework to topology noise or attacks, informed decisions can be made and appropriate measures can be taken to enhance the robustness and security of power systems in the face of potential threats.

VI. Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant No. 2118510.

References

[1] F. F. Wu, "Power system state estimation: a survey," International Journal of Electrical Power Energy Systems, vol. 12, no. 2, pp. 80–87, 1990.

[2] Z. Wu, Q. Wang and X. Liu, "State Estimation for Power System Based on Graph Neural Network", 2022 IEEE 5th International Electrical and Energy Conference (CIEEC), pp. 1431-1436, 2022.

[3] X. Wu, H. Zhang, S. Guo and J. Cao, "State Estimation of Energy Internet Using SCADA and PMU Data Based on Graph Convolutional Networks", 2021 IEEE International Conference on Energy Internet (ICEI), pp. 102-106, 2021.

[4] S. Stock, M. Dressel, D. Babazadeh and C. Becker, "Application of Physics-based Graph Convolutional Network in Real-time State Estimation of Under-determined Distribution Grids", 2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pp. 1-5, 2022.

[5] F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner and G. Monfardini, "The Graph Neural Network Model", Journal of IEEE Transactions on Neural Networks, vol.20, no.1, pp.61-80, 2009.

[6] D. Zügner, O. Borchert, A. Akbarnejad, and S. Günnemann, "Adversarial Attacks on Graph Neural Networks: Perturbations and their Patterns", ACM Transactions on Knowledge Discovery Data 14, vol. 5, Article 57, 2020.

[7] M. J. Hossain and M. Rahnamay–Naeini, "State Estimation in Smart Grids Using Temporal Graph Convolution Networks", 2021 North American Power Symposium (NAPS), pp. 01-05, 2021.

[8] K. Xu and H. Chen and S. Liu and P.Y. Chen and T.W. Weng and M. Hong and X. Lin, "Topology Attack and Defense for Graph Neural Networks: An Optimization Perspective", arXiv, 2019.

[9] A. Liu, B. Li, T. Li, P. Zhou and R. Wang, "AN-GCN: An Anonymous Graph Convolutional Network Against Edge-Perturbing Attacks", in IEEE Transactions on Neural Networks and Learning Systems, 2021.

[10] S. Xu, Y. Yao, L. Li, W. Yang, F. Xu and H. Tong , "Detecting Topology Attacks against Graph Neural Networks", arXiv, 2022.

[11] X. Zhang and M. Zitnik, "GNNGuard: Defending Graph Neural Networks against Adversarial Attacks", Advances in Neural Information Processing Systems, 2020.

[12] C. He, G. Kou, H. Zhang and Z. Hu,"Graph Topology Noise Aware Learning by Feature Clustering and Pseudo-labels Generator", 2022 International Joint Conference on Neural Networks (IJCNN), pp. 1-8, 2022.

[13] D. Luo, W. Cheng, W. Yu, B. Zong, J. Ni, H. Chen, and X. Zhang, "Learning to Drop: Robust Graph Neural Network via Topological Denoising", In Proceedings of the 14th ACM International Conference on Web Search and Data Mining (WSDM '21), 779–787. 2021.

[14] E. Dai, W. Jin, H. Liu and S. Wang, "Towards Robust Graph Neural Networks for Noisy Graphs with Sparse Labels", Association for Computing Machinery, pp. 181-191, 2022.

[15] A. Bojchevski, S. Günnemann, "Adversarial attacks on node embeddings via graph poisonings," Proceedings of the 36th International Conference on Machine Learning, 2019.

[16] M. A. Rahman, E. Al-Shaer and R. Kavasseri, "Impact Analysis of Topology Poisoning Attacks on Economic Operation of the Smart Power Grid", 2014 IEEE 34th International Conference on Distributed Computing Systems, pp. 649-659, 2014.

[17] S. H. Haghshenas, M. A. Hasnat and M. Naeini, "A Temporal Graph Neural Network for Cyber Attack Detection and Localization in Smart Grids", 2023 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp.1-5, 2023.

[18] O. Boyaci et al., "Graph Neural Networks Based Detection of Stealth False Data Injection Attacks in Smart Grids," in IEEE Systems Journal, vol. 16, no. 2, pp. 2946-2957, June 2022.

[19] J. Kim and L. Tong, "On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures", in IEEE Journal on Selected Areas in Communications, vol. 31, no. 7, pp. 1294-1305, 2013.

[20] A. Jolfaei and K. Kant, "On the Silent Perturbation of State Estimation in Smart Grid", in IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4405-4414, 2020.

[21] T. Hou, T. Wang, Z. Lu and Y. Liu, "Combating Adversarial Network Topology Inference by Proactive Topology Obfuscation", in IEEE/ACM Transactions on Networking, vol.29, no.6, pp.2779-2792, 2021.

[22] S. Moshtagh, A. Islam Sifat, B. Azimian and A. Pal, "Time-Synchronized State Estimation Using Graph Neural Networks in Presence of Topology Changes", arXiv, 2022.

[23] R. D. Zimmerman, C. E. Murillo-Sánchez and R. J. Thomas, "MATPOWER: Steady-State Operations,Planning,and Analysis Tools for Power Systems Research and Education", in IEEE Transactions on Power Systems, vol.26, no.1, pp.12-19, 2011.

[24] The New York Independent System Operator, Inc[US]. https://www.nyiso.com/