Topology Switching as Proactive Agility Against Adversarial Cyberattacks

Mohammad Zakaria Haider, Muhammad Nadeem, and Mohammad Ashiqur Rahman
Analytics for Cyber Defense (ACyD) Lab, Florida International University, USA
mhaid010@fiu.edu, mnadeem@fiu.edu, marahman@fiu.edu

***Abstract*—False data injection (FDI) attacks on power system state estimation exploit a fixed network model to satisfy stealth conditions and evade the classical anomaly detection process. This paper proposes a physics-based moving target defense (MTD) that leverages security-constrained topology switching to continually invalidate those conditions. In this work, we initially construct an offline library of switch-ready topologies by generating candidate spanning-tree configurations, enforcing power-flow convergence, security limits, and retaining only low-loss, stable operating points. Based on this, we design an online MTD scheduler that executes randomized, loss-aware switching actions, making it suitable for real-time operation. We demonstrate that topology switching alters the measurement matrix, disrupts topology-specific stealth, and fosters residual growth, which significantly enhances detection rates for the standard chi-square anomaly detection method. In addition, we demonstrate that the same switching strategy also enhances state-of-the-art machine learning-based anomaly detectors without requiring any architectural modifications. These results position security-constrained topology switching as a detector-agnostic, operationally feasible, agile mechanism against cyberattacks.**

***Index Terms*—Moving Target Defense, Cyber Security, False Data Injection Attack, Anomaly Detection, Smart Grid.**

I. Introduction

A. Motivation

According to the Threat Intelligence Index report, the energy sector was the fourth-most-attacked industry in 2022, accounting for 10.7% of overall cyberattacks [1]. The attackers behind the epic Triton/Trisis attack that in 2017 targeted and shut down a physical safety instrumentation system in a petrochemical plant in Saudi Arabia have now been discovered by probing the networks of dozens of US and Asia-Pacific electric utilities [2]. Furthermore, attacks like Stuxnet [3] and Dragonfly [4] necessitate the attacker to have complete access to real-time data in control centers and a comprehensive understanding of the system. The increasing use of advanced monitoring and anomaly detection faces a cybersecurity challenge in modern power grids. Adversaries can compromise measurement devices, sending malicious data to the control center and potentially causing physical damage. It is crucial to analyze cyber attack scenarios for power system safety. Studies on FDI attacks assume partial or full knowledge of the targeted system. Recent research, such as [5]–[7], focuses on injecting false data into load and power transmission measurements. FDI attacks aim to manipulate measurements to misguide control actions, thereby impacting automatic voltage regulation, load frequency control, and voltage variance control [8]–[11].

Stealthy false-data injection attacks exploit the fact that power-system state estimation is calibrated to a fixed network configuration [12]. Adversaries exploit static grids to craft stealthy attacks that evade conventional detection. To counter this, we employ topology-based MTD via scheduled breaker switching, rendering the attacker's knowledge stale. Unlike continuous parameter tweaks, topology changes are discrete and structural, altering measurement-state mappings. We demonstrate that this approach enhances detection sensitivity for both classical and learning-based methods

B. Related Works

Liu et al. demonstrated that adversaries with knowledge of H can craft attack vectors $a = Hc$ within the measurement column space, preserving the residual $J(r)$ distribution to evade detection [11]. Lakshminarayana et al. categorize MTD into network-based and physics-based approaches [10]. Physics-based MTD alters H via reactance or topology changes, shifting the null space to invalidate previously stealthy attack vectors. Reactance perturbation via D-FACTS is well-studied. Rahman and Bobba showed that dynamic adjustments ($\pm$10-20%) expose FDI attacks while maintaining grid observability [13]. Wu et al. optimized detection by maximizing the rank of $M = [H; H_0]$, where H_0 represents the attacker's assumed Jacobian [12]. Recent cyber-physical MTDs harden security by shifting the attack surface [14], [15], yet often operate independently of state estimation, potentially risking real-time observability. These approaches focus on dynamically changing the attack surface in both cyber and physical domains, making it increasingly difficult for attackers to maintain persistent access or execute coordinated attacks.

C. Contribution

Topology switching is an alternative, physics-based, agile MTD strategy that reconfigures the network by opening or closing circuit breakers, fundamentally altering the power flow equations and the measurement matrix. The core contribution of this paper can be written as:

- We construct an offline library of switch-ready topologies by generating spanning trees via Kruskal's algorithm, enforcing AC power-flow convergence and security limits, and retaining only low-loss, stable variants.
- We design a proactive MTD scheduler that draws on a validated library to execute randomized, loss-aware, and

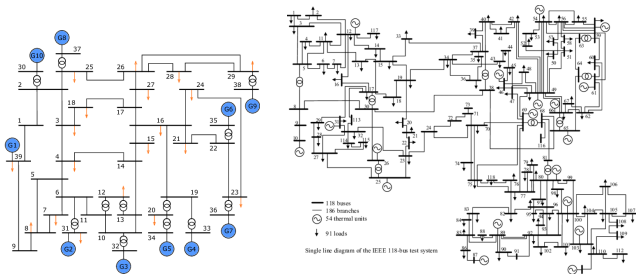
979-8-3315-8138-1

stability-preserving topology switches at regular intervals, suitable for real-time operation.
- Comparing identical FDI scenarios, we show that topology switching breaks stealth conditions, causing residual growth that significantly improves anomaly detection.
- We also demonstrated the effectiveness of topology switching in a state-of-the-art machine-learning-based anomaly-detection module.

The rest of the paper is organized as follows: we have discussed the technical overview of the system in Section II. Section III explains the testbed setup, test cases, and evaluation. We have concluded the paper in Section IV.

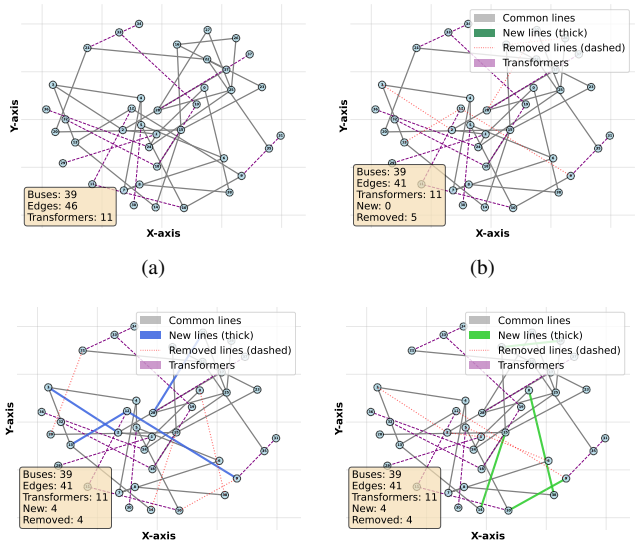
II. Technical Overview

A. Topology Optimization



(a) (b)

Fig. 1: (a) IEEE 39 bus (b) IEEE 118 bus



(a) (b) (c) (d)

Fig. 2: Demonstrating (a) base topology and (b)-(d) different generated topologies with distinction with base topology.

We formulate topology selection and switching for MTD as a constrained mixed-integer optimization that co-optimizes operational efficiency and cybersecurity. The optimizer chooses breaker statuses to produce discrete, structural changes in the network that (i) preserve connectivity and steady-state feasibility, (ii) respect frequency, voltage, security margins, and (iii) maximize *topology diversity* over time so that attacker knowledge becomes stale. The formulation integrates power-flow feasibility (via the Y-bus) and detection-theoretic impact (via the measurement Jacobian H), providing a closed-loop connection between switching actions and the performance of anomaly detection. Let L denote the set of transmission lines and $x_i \in \{0,1\}$ indicate the service status of line $i \in L$:

$$x_i = \begin{cases} 1, & \text{line } i \text{ in service,} \\ 0, & \text{line } i \text{ out of service.} \end{cases} \tag{1}$$

We collect $x = \{x_i\}_{i \in L}$ as the *topology vector*. We adopt a bi-criteria objective that balances loss minimization and temporal diversity as below:

$$\min_{x \in \{0,1\}^{|L|}} \; J(x) \triangleq \alpha \, J_{\text{loss}}(x) \; + \; \beta \, J_{\text{div}}(x) \tag{2}$$

with weights $\alpha > 0$, $\beta > 0$. The loss surrogate uses line parameters as:

$$J_{\text{loss}}(x) \; = \; \sum_{i \in L} r_i \, l_i \, x_i \tag{3}$$

where r_i and l_i are the resistance (per km) and length (km) of line i. On the other hand, temporal diversity penalizes staying in similar configurations :

$$J_{\text{div}}(x) \; = \; -\sum_{i \in L} \left| x_i - x_i^{\text{prev}} \right| \; - \; \sum_{i \in L} \varepsilon_i \left| x_i - x_i^{\text{prev}} \right| \tag{4}$$

where x^{prev} is the last committed topology and $\varepsilon_i \sim \mathcal{U}(0.1, 0.5)$ is a small randomized tie-breaker to avoid cyclic pattern. Our approach was initially developed on the IEEE 39-bus system (Fig. 1(a)) and subsequently extended to the IEEE 118-bus system (Fig. 1(b)). We construct an offline library of switch-ready topologies by generating candidate spanning-tree configurations via Kruskal's algorithm, as illustrated in Fig.2(a)–Fig.2(d). Each candidate is retained only if it satisfies power-flow convergence and security limits, prioritizing low-loss, stable operating points. The offline library construction yielded up to 24 valid, security-constrained topologies for both systems, though this varies by system size (e.g., fewer for the IEEE 14-bus system). In the optimization objective (2), we assigned weights $\alpha = 0.4$ and $\beta = 0.6$, balancing minimal system losses (α) with sufficient topological diversity (β) to degrade attacker information. To ensure reliability, the offline generation acts as a strict filter; while our simulation focuses on steady-state limits, the framework allows operators to exclude topologies that violate N-1 criteria or desensitize protection. This ensures the MTD scheduler only utilizes pre-validated, operationally safe configurations for online optimization. Standard topology processors handle unexpected switching (e.g., faults), allowing the detector to adapt to the new Jacobian H or flag errors, ensuring MTD coexists with fault management. Since feasibility depends on real-time operating points, the online scheduler validates offline candidates against current load profiles before switching, ensuring voltage stability and thermal margins are maintained. Designed as an external SCADA/EMS application layer, the MTD framework minimizes online computational burden by offloading rigorous

topology validation to an offline process. This decoupled architecture ensures the lightweight scheduler does not compete with the real-time state estimation or contingency analysis for resources. Future implementations will extend this steady-state security model to include a transient stability assessment (TSA) module and adaptive protection coordination to address dynamic switching transients.

B. Topology Dependence of the Jacobian

Classical anomaly or bad-data detection in state estimation relies on hypothesis testing based on the chi-square (χ^2) distribution. The test statistic $J = r^\top R^{-1} r$, where r is the measurement residual, is compared against a threshold γ derived from the χ^2 distribution with $m-n$ degrees of freedom (m measurements, n state variables) . When $J > \gamma$, the anomaly is flagged. However, these approaches assume measurement errors follow a Gaussian distribution and cannot distinguish between stochastic noise and systematic attacks that preserve the residual structure. Our work builds on this foundation by evaluating whether MTD can restore the effectiveness of these methods against coordinated stealthy attacks.

Let $x \in \mathbb{R}^n$ denote the system state (voltage magnitudes and angles) and $z \in \mathbb{R}^m$ the measurement vector collected from SCADA/PMU channels. For an active network topology $\mathcal{T}$, the nonlinear measurement model can be written as:

$$z \;=\; h_{\mathcal{T}}(x) + e, \qquad e \sim \mathcal{N}(0, R) \tag{5}$$

where $R \succ 0$ is the measurement noise covariance. Linearizing (5) about an operating point $x^\star$ yields:

$$z \;\approx\; H_{\mathcal{T}}\, x + e, \qquad H_{\mathcal{T}} \;\triangleq\; \left.\frac{\partial h_{\mathcal{T}}(x)}{\partial x}\right|_{x^\star} \tag{6}$$

Weighted least squares (WLS) with $W \triangleq R^{-1}$ gives the estimator and the corresponding residual as:

$$\hat{x} \;=\; \left(H_{\mathcal{T}}^\top W H_{\mathcal{T}}\right)^{-1} H_{\mathcal{T}}^\top W z, \tag{7}$$

$$r \;=\; z - H_{\mathcal{T}}\hat{x} \;=\; \left(I - P_{\mathcal{T}}\right) z \tag{8}$$

Where $P_{\mathcal{T}} \;\triangleq\; H_{\mathcal{T}}\left(H_{\mathcal{T}}^\top W H_{\mathcal{T}}\right)^{-1} H_{\mathcal{T}}^\top W$. Under the null (benign) hypothesis with full-column-rank $H_{\mathcal{T}}$, the J can be written as:

$$J \;\triangleq\; r^\top W r \tag{9}$$

The topology $\mathcal{T}$ determines the bus-admittance matrix $Y_{\text{bus}}(\mathcal{T}) = G(\mathcal{T}) + jB(\mathcal{T})$, constructed by stamping active branches:

$$Y_{ii} = \sum_{k \in \mathcal{N}(i)} \left(y_{ik} + j b_{ik}^{\text{sh}}/2\right), \quad Y_{ij} = -\,y_{ij} \quad (i \neq j) \tag{10}$$

where $y_{ij} = 1/(r_{ij} + j x_{ij})$ for an energized line (i,j), and $\mathcal{N}(i)$ is the neighbor set of bus i. Measurement functions for bus injections and line flows, P_i, Q_i, P_{ij}, Q_{ij}, are smooth functions of $\{V_\ell, \theta_\ell\}$ with coefficients determined by $G(\mathcal{T})$ and $B(\mathcal{T})$ where ℓ represents the line index of the system. Consequently, the Jacobian $H_{\mathcal{T}}$ inherits explicit dependence on $\mathcal{T}$ and can be written as:

$$H_{\mathcal{T}} \;=\; \begin{bmatrix} \frac{\partial P}{\partial \theta} & \frac{\partial P}{\partial V} \\ \frac{\partial Q}{\partial \theta} & \frac{\partial Q}{\partial V} \\ \frac{\partial P_{ij}}{\partial \theta} & \frac{\partial P_{ij}}{\partial V} \\ \frac{\partial Q_{ij}}{\partial \theta} & \frac{\partial Q_{ij}}{\partial V} \end{bmatrix}_{\mathcal{T}}$$

Each block depends on $G(\mathcal{T})$ and $B(\mathcal{T})$ through terms such as:

$$\frac{\partial P_i}{\partial \theta_k} = \begin{cases} -V_i V_k\left(G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik}\right), & k \neq i \\ -Q_i - B_{ii}V_i^2, & k = i \end{cases} \tag{11}$$

$$\frac{\partial P_i}{\partial V_k} = \begin{cases} V_i\left(G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik}\right), & k \neq i \\ 2G_{ii}V_i + \sum_{\ell \neq i} V_\ell\left(G_{i\ell}\cos\theta_{i\ell} + B_{i\ell}\sin\theta_{i\ell}\right), & k = i \end{cases} \tag{12}$$

with $\theta_{ik} = \theta_i - \theta_k$. Energizing or de-energizing branches modifies G_{ik}, B_{ik}, and diagonals G_{ii}, B_{ii}, thus altering both diagonal and off-diagonal sensitivities in $H_{\mathcal{T}}$.

C. Stealthy FDI and Effect of MTD

We focus on topology-aware FDI attacks because they represent the worst-case benchmark for detection systems. These adversaries leverage knowledge of the static Jacobian matrix H to craft attack vectors that are mathematically invisible to residual-based detectors. Demonstrating detection against this sophisticated class of attacks confirms the robustness of the MTD strategy. We can consider an additive FDI attack, $a \in \mathbb{R}^m$ and so the attacked measurement is $z^{\text{atk}} = z + a$. With topology $\mathcal{T}$, the WLS residual becomes:

$$r_{\mathcal{T}}^{\text{atk}} \;=\; \left(I - P_{\mathcal{T}}\right)(z + a) \;=\; r_{\mathcal{T}}^{\text{benign}} \;+\; \underbrace{\left(I - P_{\mathcal{T}}\right)a}_{\text{attack component}} \tag{13}$$

where $r_{\mathcal{T}}^{\text{benign}} = (I - P_{\mathcal{T}})z$. Stealthy attacks for topology $\mathcal{T}_0$ needs to satisfy :

$$a \in \mathcal{R}(H_{\mathcal{T}_0}) \;\iff\; \exists\, c \text{ s.t. } a = H_{\mathcal{T}_0} c \;\implies\; \left(I - P_{\mathcal{T}_0}\right)a = 0 \tag{14}$$

so that $r_{\mathcal{T}_0}^{\text{atk}} = r_{\mathcal{T}_0}^{\text{benign}}$ and the chi-square statistic remains nominal. Let MTD switch the topology from $\mathcal{T}_0$ to $\mathcal{T}_1$, changing the projector from $P_{\mathcal{T}_0}$ to $P_{\mathcal{T}_1}$. The same $a = H_{\mathcal{T}_0} c$ generally fails to lie in $\mathcal{R}(H_{\mathcal{T}_1})$, and the post-switch residual includes a non-vanishing attack component:

$$r_{\mathcal{T}_1}^{\text{atk}} - r_{\mathcal{T}_1}^{\text{benign}} \;=\; \left(I - P_{\mathcal{T}_1}\right) H_{\mathcal{T}_0} c. \tag{15}$$

The corresponding increase in the chi-square statistic can be :

$$\begin{aligned} \Delta J \;\triangleq\; \left(r_{\mathcal{T}_1}^{\text{atk}} - r_{\mathcal{T}_1}^{\text{benign}}\right)^\top W \left(r_{\mathcal{T}_1}^{\text{atk}} - r_{\mathcal{T}_1}^{\text{benign}}\right) \;=\; \\ c^\top H_{\mathcal{T}_0}^\top \underbrace{\left(I - P_{\mathcal{T}_1}\right)^\top W \left(I - P_{\mathcal{T}_1}\right)}_{=:\,\Pi_{\mathcal{T}_1}} H_{\mathcal{T}_0}\, c \end{aligned} \tag{16}$$

which is strictly positive unless $H_{\mathcal{T}_0} c \in \mathcal{R}(H_{\mathcal{T}_1})$. Thus, any stealthy FDI tailored to $\mathcal{T}_0$ becomes detectable after a switch to $\mathcal{T}_1$ provided the column spaces differ. We can write the Jacobian difference as $\Delta H \triangleq H_{\mathcal{T}_0} - H_{\mathcal{T}_1}$. When the switch

is not infinitesimal, the attack component in (15) can be expressed as:

$$\big(I-P_{\mathcal{T}_1}\big)H_{\mathcal{T}_0}c \;=\; \big(I-P_{\mathcal{T}_1}\big)\big(H_{\mathcal{T}_1}+\Delta H\big)c \;=\; \big(I-P_{\mathcal{T}_1}\big)\Delta H\, c \tag{17}$$

since $\big(I-P_{\mathcal{T}_1}\big)H_{\mathcal{T}_1}=0$. Substituting (17) into (16) yields :

$$\Delta J \;=\; \|\Delta H\, c\|^2_{\Pi_{\mathcal{T}_1}} \;\triangleq\; (\Delta H\, c)^\top \Pi_{\mathcal{T}_1}(\Delta H\, c) \tag{18}$$

making explicit that the detectability gain scales with the component of $\Delta H c$ orthogonal (in the W-metric) to $\mathcal{R}(H_{\mathcal{T}_1})$. Because $H_{\mathcal{T}}$ is a smooth function of $(G(\mathcal{T}), B(\mathcal{T}))$, and these in turn are stamped from the energized line set, ΔH reflects both diagonal sensitivity shifts (self-admittance) and off-diagonal changes (bus couplings) induced by topology switching. Under benign operation after the switch, J in (9) remains approximately χ^2_d. With an FDI designed for $\mathcal{T}_0$ but evaluated under $\mathcal{T}_1$, the noncentrality parameter becomes:

$$\lambda \;=\; \mathbb{E}[\,\Delta J\,] \;\approx\; \|\Delta H\, c\|^2_{\Pi_{\mathcal{T}_1}} \tag{19}$$

so that J is approximately $\chi^2_d(\lambda)$. For a fixed false-alarm level α, the decision threshold $\tau = \chi^2_{d,1-\alpha}$ satisfies :

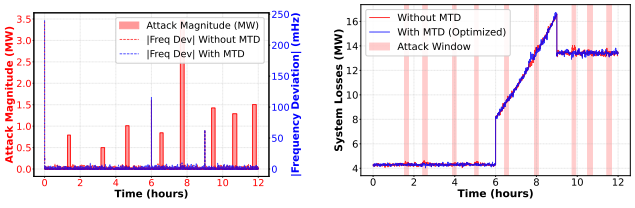
$$\mathbb{P}(J>\tau \mid \text{attack}) \;=\; 1-F_{\chi^2_d(\lambda)}(\tau) \tag{20}$$

which increases monotonically with λ. Hence, any MTD policy that yields a sufficiently large $\|\Delta H\, c\|_{\Pi_{\mathcal{T}_1}}$ improves detection against attacks crafted for the pre-switch topology.

III. Evaluation

A. Implementation

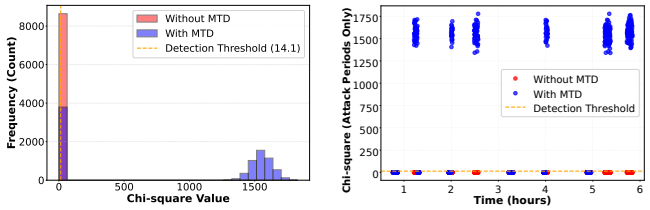
We implemented the framework using pandapower [16] on the IEEE 39-bus and 118-bus systems, ensuring network-agnostic compatibility. The topology-selection problem is formulated as a mixed-integer linear programming (MILP) and solved using the pyomo library with a deterministic solver cascade: $GLPK$, followed by CBC, $ECOS$, and $SCIP$ if necessary. A topology is accepted into the library only if it satisfies rigorous operational constraints, i.e., the AC power flow must converge, bus voltage magnitudes must remain within $\pm 5\%$ of nominal values (0.95–1.05 p.u.), and line flows must remain within thermal limits. This ensures that every proactive switch maintains the grid's steady-state stability.



(a) (b)

Fig. 3: (a) False data injection attack with frequency deviation and (b) comparative system loss during simulation.

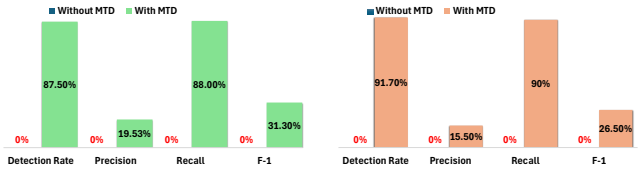
By maintaining the stealth condition mentioned in (14), we have generated false load measurement values that are injected into the automatic generation control unit. Fig. 3(a) shows the injected load amount and corresponding frequency deviation for the IEEE 39 Bus system, and the comparative system loss is shown in Fig. 3(b). It is important to note the operational cost of this defense. Because the optimizer prioritizes low-loss configurations (α in Eq. 2), the relative increase in system losses for MTD topologies was restricted to an average of 5%-10% compared to the baseline static topology. This confirms that the loss penalty incurred for enhanced security remains within acceptable economic limits for transmission operation. When the system switches its topology from $\mathcal{T}_0$ to $\mathcal{T}_1$ or $\mathcal{T}_n$ to $\mathcal{T}_m$ it impacts the chi-square distribution and based on this difference the system can identify the anomaly. Fig. 4(a)-Fig. 4(b) shows the comparative difference of chi-square probability distribution and values between MTD and without MTD conditions. In this work, we selected a model ranking essentially unchanged and yields only marginal shifts in overall discrimination, indicating limited benefit for the mechanical wear-and-tear constraints of high-voltage circuit breakers [10]. While faster switching increases agility, the hourly interval aligns with standard dispatch schedules and ensures operational stability. However, we have kept the discussion of the optimal switching interval and its impact for future exploration.



(a) (b)

Fig. 4: Representation of chi-square distribution for MTD and without MTD scenario.

B. Numerical Analysis



(a) (b)

Fig. 5: Performance of chi-square anomaly detection between MTD and without MTD scenario for (a) IEEE 39 bus and (b) IEEE 118 bus.

For both the IEEE 39-bus and 118-bus systems, the baseline (without MTD) fails, as shown in Fig. 5(a) and Fig. 5(b), indicating that stealthy FDI attacks remain entirely undetected. Introducing topology-based MTD fundamentally changes this behavior. For the 39-bus system, MTD raises the detection rate from 0% to 87.50%, with recall reaching 88.00% and F1 improving to 31.30%. Similarly, on the 118-bus system, the detection rate increases from 0% to 91.70%, recall increases

to 90.00%, and F1 increases to 26.50%. These gains show that MTD successfully converts previously stealthy attacks into detectable events across both networks. The relatively low precision (19.53% for 39-bus and 15.50% for 118-bus) indicates a higher false-alarm rate, reflecting an operational trade-off in which MTD substantially improves attack visibility and coverage at the cost of noisier alarms. To mitigate this, we propose a topology-aware adaptive threshold that dynamically adjusts τ or employs a post-switch filtering window. Even if adversaries possess the full topology library, MTD remains effective due to temporal uncertainty; attackers must synchronize injection with the active configuration. Randomized switching forces a prediction, where any mismatch between the attack vector and the current measurement subspace exposes the intrusion.

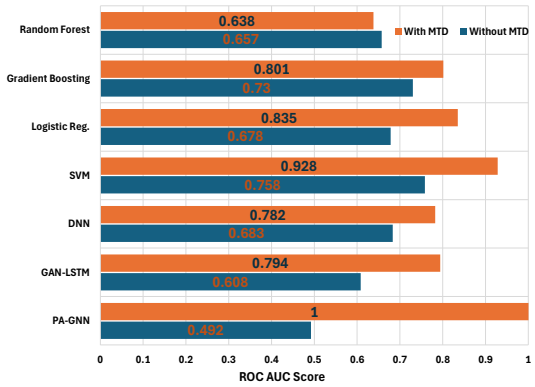


Fig. 6: Demonstrating state-of-the-art machine learning based anomaly detection performance between without MTD and with MTD scenarios for the ROC AUC score.

We validated MTD against state-of-the-art ML detectors using receiver operating characteristic–area under the curve (ROC–AUC) scores. (Fig. 6), chosen for their robustness to class imbalance. In anomaly detection, it is particularly informative because it is threshold-independent and robust to class imbalance, making it well-suited for scenarios where attacks are rare but critical to detect. The results show that MTD consistently improves the discrimination of these models. The largest gain is observed for the physics-aware graph neural network (PA-GNN), whose ROC–AUC increases from 0.492 to 1.000, indicating near-perfect separation between attack and benign samples under MTD. Notable improvements are also seen for the generative adversarial network with long short-term memory (GAN-LSTM) ($0.608 \rightarrow 0.794$), support vector machine (SVM) ($0.758 \rightarrow 0.928$), logistic regression ($0.678 \rightarrow 0.835$), deep neural network (DNN) ($0.683 \rightarrow 0.782$), and gradient boosting ($0.730 \rightarrow 0.801$). Random forest is the only method that exhibits a slight decrease ($0.657 \rightarrow 0.638$), suggesting that MTD benefits are generally positive across both classical and learning-based architectures.

IV. Conclusion

In summary, this paper demonstrates that agility with MTD via periodic, security-constrained topology switching can significantly enhance the detection of stealthy FDI attacks in power systems. By continually invalidating the attacker's assumed network model, MTD improves detection performance for both classical chi-square and state-of-the-art anomaly detection methods. Our framework validates this approach through synchronized attack scenarios, addressing practical trade-offs such as switching frequency and false-alarm tolerance. Future work will target adaptive adversaries with online learning capabilities, investigate joint optimization with economic and reliability objectives, and develop real-time adaptive thresholding strategies.

Acknowledgement

This work is supported by the Department of Energy (DOE) (Award# DE-CR0000046). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the DOE's views.

References

[1] J. Gregory, "Today's biggest threats against the energy grid," 2023. https://securityintelligence.com/articles/, accessed 2025-09-20.

[2] K. Jackson, "Triton attackers seen scanning us power grid networks," 2019. https://www.darkreading.com/perimeter/, accessed 2025-09-20.

[3] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *Proc. IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, pp. 4490–4494.

[4] A. Hesseldahl, "Hackers infiltrated power grids in u.s., spain," 2014. https://www.vox.com/2014/7/1/11628504/hackers-infiltrated-power-grids-in-us-spain, accessed 2025-09-20.

[5] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[6] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, 2012.

[7] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

[8] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.

[9] W. Luo and L. Xiao, "Reinforcement learning based vulnerability analysis of data injection attack for smart grids," in *Proc. 2021 40th Chinese Control Conference (CCC)*, pp. 6788–6792.

[10] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense against cyber-physical attacks in power grids via game theory," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5244–5257, 2021.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, June 2011.

[12] Q. Wang, S. Wu, Z. Wu, J. Hu, Q. He, Y. Ye, and Y. Tang, "Topology switching-based moving target defense against false data injection attacks on a power system," *International Journal of Electrical Power Energy Systems*, vol. 163, p. 110350, 2024.

[13] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proceedings of the First ACM Workshop on Moving Target Defense*, MTD '14, (New York, NY, USA), p. 59–68, Association for Computing Machinery, 2014.

[14] J. Giraldo, A. Cardenas, and R. G. Sanfelice, "A moving target defense to detect stealthy attacks in cyber-physical systems," in *2019 American Control Conference (ACC)*, pp. 391–396, 2019.

[15] Y. Hu, P. Zhu, P. Xun, B. Liu, W. Kang, Y. Xiong, and W. Shi, "Cpmtd: Cyber-physical moving target defense for hardening the security of power system against false data injected attack," *Computers Security*, vol. 111, p. 102465, 2021.

[16] "pandapower." https://www.pandapower.org/, accessed on 11-16-2025.