Load Margin Constrained Moving Target Defense against False Data Injection Attacks

Hang Zhang, Noah Fulk, Bo Liu, Lawryn Edmonds, Xuebo Liu, and Hongyu Wu
Mike Wiegers Department of Electrical and Computer Engineering
Kansas State University, Manhattan, Kansas 66506, USA

***Abstract*—Cyber physical security of power systems with high penetration of renewable generation has attracted attention from researchers. One critical issue is that cyber-physical attacks, disguised as uncertain renewable generation, can target conventional power system state estimation (SE). Moving target defense (MTD) is a promising defense strategy to detect stealthy false data injection (FDI) attacks against SE. However, all existing studies myopically perturb the reactance of transmission lines equipped with distributed flexible AC transmission system (D-FACTS) devices without adequately considering the system voltage stability. Exacerbated by the renewable generation uncertainty, existing MTD may cause voltage instability when the power grid is under stress. To address this issue, we propose a novel MTD framework that explicitly considers system voltage stability by using continuation power flow. We utilize the sensitivity matrix of power injection to line impedance, on which an optimization problem for maximizing load margin is formulated. This framework is validated on the IEEE 14-bus system and the IEEE 118-bus system, in which net load redistribution attacks are launched by sophisticated attackers. Steady-state simulations and dynamic simulations on PSS/E show the effectiveness of the proposed framework in circumventing the voltage instability while maintaining the detection effectiveness of MTD. The impact of the proposed method on attack detection effectiveness is also revealed.**

I. Introduction

The emerging renewable generation in modern power systems has increased the attack surface and provided adversaries with more opportunities to conduct highly structured and stealthy cyber-physical attacks. Smart grids with high penetration of renewable generation require decentralized control methods and sophisticated communication channels to ensure continuous and stable operation. Such reliance on communication reliability makes smart grids more vulnerable to cyber-attacks [1]. The concept of moving target defense (MTD) has been introduced in smart grids in the face of emerging cyber-physical attacks [2], [3]. MTD proactively perturbs the transmission line impedance using distributed flexible AC transmission system (D-FACTS) devices to invalidate attackers' knowledge about the power system configurations. Without knowing the true power system configuration, it is difficult for an attacker to construct stealthy false data injection (FDI) attacks against power system state estimation [4]–[9]. The recent proliferation of D-FACTS devices [10] has attracted increasing research attention due to their add-on cyber-physical security benefits via MTD.

The majority of MTD strategies in the literature are designed to detect FDI attacks against state estimation [6], [8], [9], [11]. Liu et al. [12] first propounded that there are two intertwined and essential problems associated with MTD, i.e., MTD planning and MTD operation. The MTD planning refers to optimally installing MTD devices (e.g., D-FACTS devices) on an appropriately identified subset of the system (e.g., transmission lines). The MTD operation determines how to optimally dispatch MTD device setpoints in real-time. A random MTD (RMTD) operation [11] was proposed to randomly change the reactance of D-FACTS equipped transmission lines without considering the detection effectiveness. An AC optimal power flow (AC-OPF) based optimized MTD strategy that minimizes the system loss is introduced in [5]. Liu et al. [13] defined the "hidden" MTD (HMTD) which optimally changes the branch reactance in AC network to minimize the system loss as well as line power flow differences. An HMTD is stealthy to attackers, even when the attackers are capable of checking the activation of D-FACTS [6]. In [14], Cui et al. proposed an HMTD strategy for three-phase unbalanced distribution systems. Lakshminarayana et al. [15] proposed to actively perform MTD, thus, the attacker's knowledge to mask the effects of the physical attack is outdated.

However, MTD operations may deviate the steady-state operating point of a power system from the optimal one, causing massive economic and stability impacts [5]. The MTD-induced instability combined with the renewable generation uncertainty can further reduce the load margin and cause power flow Jacobian singularity [16]. It has been validated that a power flow singularity problem is equal to a voltage collapse problem [17]. In [18], the voltage stability is defined as the ability of a power system to maintain steady voltages at all buses in the system. Voltage magnitude violation may occur at peak hour if the system does not preserve capabilities of transmission network for power transfer. The action of MTD perturbation which changes the transmission line impedance may degrade the capability of the power transfer and cause voltage collapse during peak load period. Wang et al. [19] proposed an online line switching methodology for increasing load margins to static stability limit of a look-ahead power system. Cui et al. [20] proposed a voltage stability constrained OPF model utilizing a sufficient condition on power flow Jacobian nonsingularity. Wang et al. [21] proposed a voltage stability constrained OPF by using the minimum singular value of the power flow Jacobian as a voltage stability index. To the best of our knowledge, there is no research on MTD operation to detect FDI attacks while guaranteeing system stability. Fur-

thermore, even if existing MTD operational approaches [14], [15], [22] are proposed to follow some security constraints such as power flow limits and safe voltage boundaries, all those approaches consider a single-hour system load without taking into account forecasted load variations in look-ahead time periods. This might be plausible for AC OPF since it is frequently implemented, e.g., on an hourly basis. However, the frequency of the MTD can be several hours to a few days depending on the attacker's capabilities as well as how a system operator executes it (e.g., an event-based MTD strategy [23]). The lack of such look-ahead capabilities in existing MTD methods may cause system instability or even voltage collapse due to the reduction of load margin or voltage stability degradation between two consecutive MTD executions.

This paper aims to fill the gap by proposing a novel voltage stability constrained MTD framework against highly structured FDI attacks especially in the presence of stressful system conditions. One important consideration here is that the voltage-stability improvement ought to be minimally "invasive", meaning such an enhancement should not significantly degrade the attack detection effectiveness of the MTDs. In this paper, we develop a load margin-constrained method based on continuation power flow (CPF) [16] to ensure a sufficient load margin for system voltage stability at the most stressful time period. Then, we present a new MTD framework that seamlessly integrates the proposed voltage stability constrained method into the original MTD operational methods. Last, we run dynamic simulations on Power System Simulator for Engineering (PSS/E) to show the proposed load margin-constrained MTD framework can save the system from a myopic MTD induced voltage collapse. The real-time voltage responses are shown in the case study.

The rest of this paper is organized as follows. In Section II, we introduce the system formulation and the proposed framework. Case studies are in Section III and conclusions are drawn in Section IV.

II. Problem formulation

The background and the formulation for the load margin-constrained method is presented and proposed in this section. To distinguish the system operation point with or without MTD, we define hereinafter the D-FACTS operation point before MTD as *pre-MTD*, while the operation point after MTD as *post-MTD*. To facilitate the presentation, let subscript $orig$ denote an original post-MTD system state before implementing the proposed load margin-constrained method, and subscript new represent the new MTD state that is adjusted by using the load margin-constrained method.

A. Power system with conventional MTDs

The outer solid box in Fig. 1 shows an MTD-enabled power system measurement-control-loop in wide area monitoring, protection and control (WAMPAC). Attackers can eavesdrop the power system measurement data and inject the manipulated measurement back to the system. If the attackers have the knowledge of the system configuration, they can construct and inject stealthy FDI attack vector M_a into the supervisory control and data acquisition (SCADA) system. Attack vector M_a can bypass an AC state estimation based bad data detection (BDD) [24] if there is no MTD activated. The manipulated measurement (e.g., load $\hat{P}_d, \hat{Q}_d$) will be used in the applications of energy management systems, including the security constrained unit commitment and AC-OPF based economic dispatch P_G, Q_G. When an MTD is activated, the attacker's knowledge about the system configuration $h(\cdot)$ will be outdated and the injected attack vector that was constructed based on the outdated $h(\cdot)$ can be detected by BDD.

B. D-FACTS application: power injection to impedance sensitivity

D-FACTS devices are used to manage power flows and minimize system losses in the power system operation. The power injection to impedance sensitivity (PII) is originally proposed, as an intermediate step in the chain rule of calculus, to determine the relationship between the state variables and line impedance [25]. The potential of PII remains unexplored. In this paper, we utilize the PII to indicate how much the system power transfer capability can be improved due to the change in MTD setpoint, when the system is near the power transfer limit (i.e., CPF nose point). The PII is calculated as:

$$PII \triangleq \begin{bmatrix} \frac{\partial p}{\partial x_{ij}} \\ \frac{\partial q}{\partial x_{ij}} \end{bmatrix} \tag{1}$$

C. Load margin optimization

Load margin, L_M, is a metric for measuring the system voltage stability. It is defined as the maximum amount of load that the system can support given a system configuration. With a specific system configuration and peak load forecast, the load margin is calculated by CPF with a predictor-corrector method. The PII reveals the relationship between the line impedance change and the system load margin change $\Delta L_M = PII \times \Delta X$. With the revealed relationship, a linear programming problem can be formed to maximize the load margin of the system with the original MTD by re-dispatching the MTD setpoint. The optimization problem is shown below:

$$\max_{\Delta X} \quad \sum_{i=1}^{\mathcal{N}} \mu_i \times row_i(PII) \times \Delta X \tag{2}$$

$$\text{s.t.} \quad \Delta L_M \leq PII \times \Delta X \tag{2a}$$

$$\text{LB} \leq X_{\text{orig}} + \Delta X \leq \text{UB} \tag{2b}$$

Equation 2 maximizes the total incremental load margin of the system with the original MTD X_{orig}, where ΔX is the MTD setpoint adjustment which will be used to construct the new MTD $X_{\text{new}} = X_{\text{orig}} + \Delta X$. Parameter μ is the coefficient to balance the load margin increase on the load buses $i \in \mathcal{N}$, where $\mathcal{N}$ is the set of load buses. System operators can choose a large μ_i to increase more load margin on a critical load at bus i. For each load bus, the incremental load margin is $row_i(PII) \times \Delta X$. Constraint 2a ensures the MTD setpoint adjustment can provide the expected incremental load margin,

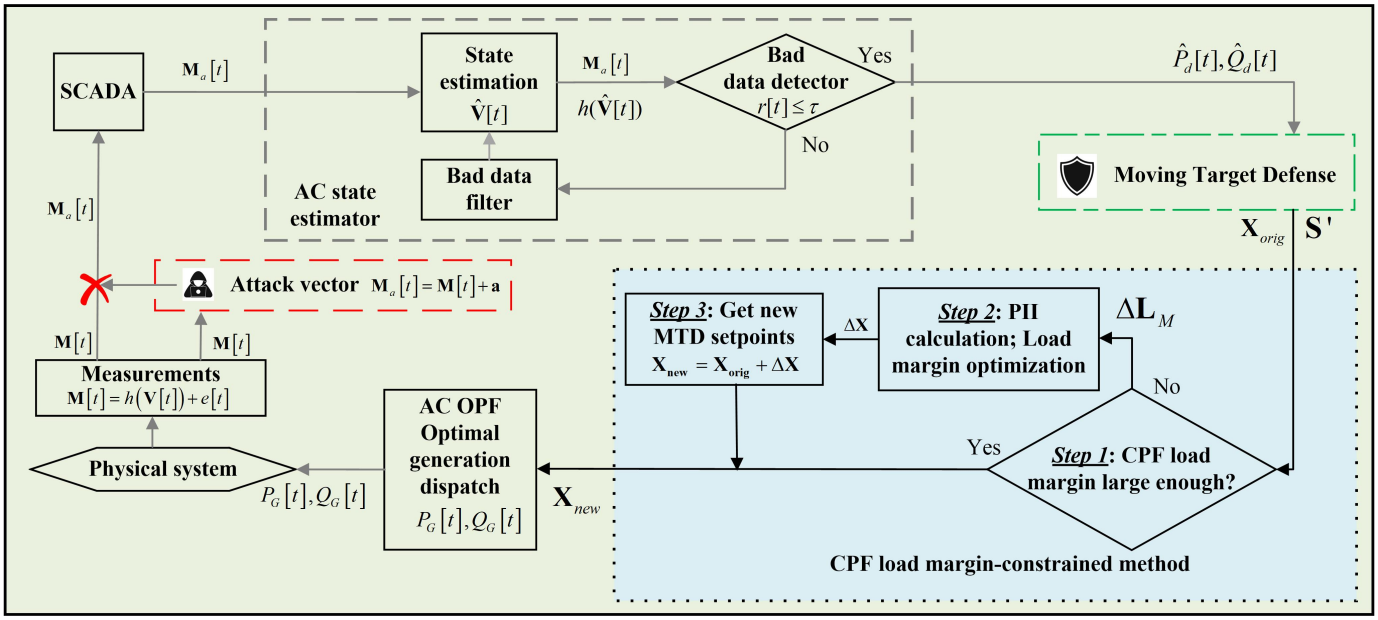


Fig. 1. Flowchart of the new MTD framework with the proposed load margin-constrained method.

Algorithm 1 load margin-constrained method

Input: X_{orig}, S'
Output: X_{new}

```
Solve CPF problem to get load margin L_M of X_orig
if S' ≤ L_M then (as they satisfy the load margin constraint for the most critical condition)
    return X_orig
else
    Calculate the expected load margin increase ΔL_M
    Compute the PII from (1)
    Solve the optimization problem (2)
    X_new = X_orig + ΔX
end if
return X_new
```

ΔL_M. The determination of ΔL_M is discussed in Section II-D. Constraint 2b ensures the total impedance change after the adjustment is within the physical capacity of D-FACTS devices. UB and LB are the upper and lower rated capacity of D-FACTS devices, where UB and LB are equal to $\pm 20\%$ of the transmission line impedance which is generally used in MTD [5], [6], [8], [9], [11], [13].

D. Load margin-constrained MTD framework

As previously discussed, all existing MTD methods fail to consider the system load margin that is very likely to degrade by MTDs. Without look-ahead capability, the degraded load margin may not be capable of supporting the most critical forecasted load $S' = max([S_{t_1}, S_{t_2}, S_{t_3}, ..., S_{t_N}])$, where t_1 to t_N are the time indices of the look-ahead time periods within an MTD window. This motivates us to develop a load margin-constrained MTD method as a post-MTD method to increase the load margin of the original MTD at S'. The proposed method is demonstrated in the dotted box in Fig. 1, the steps of which are shown in Algorithm 1. In this algorithm, the expected incremental load margin $\Delta L_M = S' - L_M$ is the difference between the forecast peak load and the load margin of the unconstrained MTD operation. In addition, the load margin-constrained MTD setpoints are calculated by adding ΔX to the original unconstrained MTD setpoints, i.e., $X_{\text{new}} = X_{\text{orig}} + \Delta X$.

III. Case Study

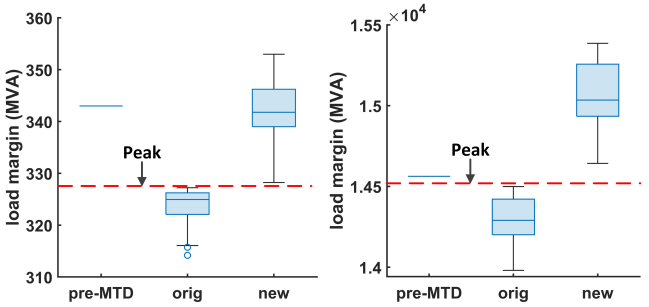
In this section, we present the case study and computational results on the proposed load margin-constrained MTD framework. The load margin-constrained method is implemented by using the CPF toolbox in MATPOWER [26]. We use the IEEE 14-bus system and IEEE 118-bus system as the test systems. The average execution time of the proposed algorithm in IEEE 14-bus and 118-bus systems are 0.012 seconds and 0.043 seconds, respectively. The computing environment for the simulations is a desktop with an Intel Core i5 processor and 8 GB RAM.

A. Impact on voltage stability

Figure 2 depicts a box plot of load margin in the two systems before and after implementing the proposed load margin-constrained method. The load margin of the pre-MTD system with no MTD operation is also shown as a baseline. In each box, the central mark indicates the median, and the bottom and top edges suggest the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points excluding outliers, and the outliers are plotted individually. Three system states are compared including the pre-MTD state, the original MTD state, and the new MTD state. According to Algorithm 1, this method only makes adjustment if the system cannot support the forecasted peak load. Therefore, Fig. 2 only shows the original MTDs that fail to do so, which is why the body of

the box plot of the original MTD is lower than the forecasted peak load. In the IEEE 14-bus system, the forecasted peak load is 327.2 MVA labeled by a horizontal red line. In Fig. 2(a), the load margin of the pre-MTD state is 343 MVA, which is greater than the forecasted peak load. Hence, the pre-MTD system state is capable of supporting the forecasted peak load. For all RMTDs whose original load margin is less than the forecasted peak load, Lines 5-10 in Algorithm 1 are executed. It is seen in the new MTD box that the proposed load margin-constrained method significantly brings up the load margin of those RMTDs. As a result, the load margin of all new MTDs are equal to or greater than the forecasted peak load. Similar plots for the IEEE 118-bus system are displayed in Fig. 2(b). The results in Fig. 2 demonstrate that the proposed load margin-constrained method can significantly increase the load margin of original MTDs and ensure ample load margins to support the forecasted peak load.

PSS/E simulations are further carried out on the IEEE 14-bus system. The dynamic voltage responses of this system under the original MTDs and the proposed load margin-constrained MTDs are compared in Fig. 3. As seen at the beginning of the simulation, the system is at an off-peak load without any MTDs. At 1s, both RMTD and the load margin-constrained MTD are implemented. Compared with the RMTD, the load margin constrained MTD decreases the impedance on 11 transmission lines and increases the line impedance on the rest 9 transmission lines. The voltage is stable in both cases after the MTD operations. However, this is not the case when it comes to the peak load (the total load increases by 60% instantaneously) starting from 4s. The system with the original MTD undergoes drastic and short spikes of voltage oscillations and the voltage collapses at 4.6s. Such oscillations indicate that the system generators strive to increase their generation to prevent the system from voltage collapse, but unfortunately they fail to do so due to the insufficient power transfer capability of the transmission lines. In contrast, the system with the load margin-constrained MTD undergoes a smaller voltage drop right after the load increase due to the power mismatch, but the system voltage remains stable at around 0.75 p.u.. Although the voltage magnitude does not meet the ANSI requirement, the proposed method still shows a much better dynamic voltage response, which,



(a) IEEE 14-bus (b) IEEE 118-bus

Fig. 2. Load margin before and after implementation of the load margin-constrained method.

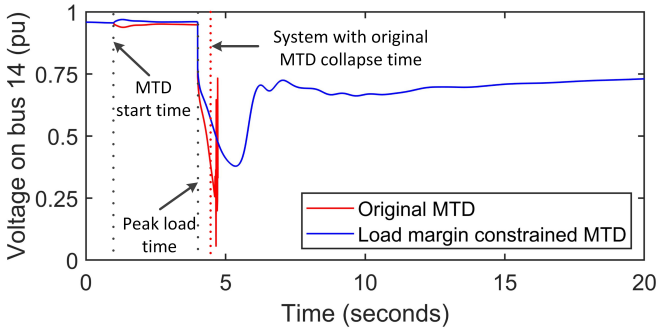
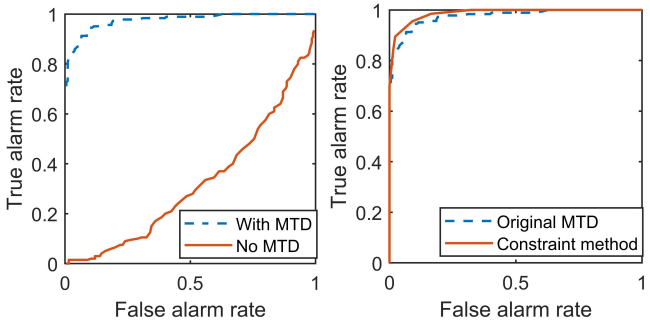


Fig. 3. Dynamic voltage magnitude response simulated by PSS/E.



(a) MTD impact (b) Proposed method impact

Fig. 4. ROC curves of BDD residual in IEEE 118-bus system.

in turn, can provide the system operator with sufficient time to implement AC-OPF or dispatching other voltage supporting devices [27], [28]. However, this is out of the scope of this paper and will be studied in our subsequent efforts.

B. Impact on attack detection effectiveness

In addition, simulations are carried out to test the MTD effectiveness against net load redistribution [29] attacks using AC state estimation-based BDD. One thousand RMTD strategies are constructed as a defense pool to test the attack detection effectiveness. The measurement noise is assumed to be Gaussian distributed with zero mean and the standard deviation as 1% of the actual measurement. We construct 1,000 net load redistribution attack vectors to form an attack pool. Figure 4 shows the receiver operating characteristic (ROC) curves of BDD residuals under different MTD scenarios. These ROC curves are created by plotting the true positive rate versus the false positive rate at various BDD thresholds. We run the BDD tests with the measurements from attacked cases and non-attacked cases. The true alarm rate indicates the probability that the BDD alarms when the system is under attack. The false alarm rate indicates the probability that the BDD alarms when there is no attack. Figure 4(a) compares the attack detection effectiveness of the BDD with and without the help of original MTDs. As seen, the ROC curve without MTD passes through the bottom right of the graph, leading to the smaller area under the curve (AUC) than the scenario with MTDs. A smaller AUC indicates a worse performance in attack detection effectiveness. The results in Figure 4(a) demonstrate: 1) the net load redistribution attack is stealthy against AC state estimation-based BDD; 2) instead of

increasing the BDD residual, the net load redistribution attack decreases the residual [29], leading to a smaller true positive rate than the false positive rate at a given threshold.

Further, we test the impacts of the proposed method on the attack detection effectiveness of the original MTD in Fig. 4(b). It is seen that the load margin-constrained method will maintain similar attack detection effectiveness as the original RMTD. A slightly larger AUC than the original MTD emerges under the load margin-constrained MTD case. This can be explained by examining the line impedance change in percentage induced by an MTD, which is indicative of the average absolute MTD magnitude. The average absolute MTD magnitude of the load margin-constrained MTDs is 10.42% which is larger than that of the original MTDs, i.e., 9.80%. Here, the observation that the attack detection effectiveness increases with the MTD magnitude is consistent with other MTD works [7], [30]. The results in Fig. 4(b) indicates that the proposed method can maintain similar attack detection effectiveness as the original MTD.

IV. Conclusion

In this paper, we address a voltage instability issue that is induced by existing myopic MTDs. The proposed load margin-constrained method, is developed based on CPF to ensure the load margin is beyond the forecast peak load and thus keeps the system voltage stable at peak time. Furthermore, we propose a new MTD framework that seamlessly integrates the load margin-constrained method. The case study shows that the proposed load margin-constrained method can improve the system load margin and save the system from an original MTD induced voltage collapse at the peak load hour. Meanwhile, the load margin-constrained MTD can maintain similar attack detection effectiveness as the original MTD. Our future work will explore implementing the proposed MTD load margin-constrained method under other advanced MTD strategies including inverter-based MTDs to equivalently change system configurations. In addition, the PII sensitivity matrix in this paper is calculated by using linear approximation. To maintain higher accuracy, we will use machine learning methods such as deep neural network and support vector regression to replace the linear PII sensitivity matrix.

Acknowledgment

This material is based upon work supported in part by the U.S. National Science Foundation under Grant No. 1929147 and No. 2146156, and in part by the U.S. Department of Energy under Award No. DE-EE0008767.

References

[1] A. Ayad, H. E. Farag, A. Youssef, and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using recurrent neural networks," in *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2018, pp. 1–5.

[2] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 342–347.

[3] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2012, pp. 2104–2113.

[4] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29 641–29 659, 2021.

[5] B. Liu and H. Wu, "Optimal D-FACTS placement in moving target defense against false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4345–4357, 2020.

[6] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2208–2223, 2018.

[7] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting stuxnet-like attacks," *IEEE transactions on smart grid*, vol. 11, no. 1, pp. 291–300, 2019.

[8] B. Liu, H. Wu, A. Pahwa, F. Ding, E. Ibrahim, and T. Liu, "Hidden moving target defense against false data injection in distribution network reconfiguration," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2018, pp. 1–5.

[9] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using d-facts devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, 2019.

[10] "A Mobile Unit Tours Europe, Smart Wires in India and More." [Online]. Available: https://www.smartwires.com/portfolio-item/8245/

[11] 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*, 2014, pp. 59–68.

[12] B. Liu and H. Wu, "Systematic planning of moving target defence for maximising detection effectiveness against false data injection attacks in smart grid," *IET Cyber-Physical Systems: Theory & Applications*, 2021.

[13] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 763–776, 2018.

[14] M. Cui and J. Wang, "Deeply hidden moving-target-defense for cyber-secure unbalanced distribution systems considering voltage stability," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 1961–1972, 2021.

[15] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense for detecting coordinated cyber-physical attacks in power grids," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019, pp. 1–7.

[16] V. Ajjarapu and C. Christy, "The continuation power flow: a tool for steady state voltage stability analysis," *IEEE Transactions on Power Systems*, vol. 7, no. 1, pp. 416–423, 1992.

[17] Y. Wang, L. Da Silva, W. Xu, and Y. Zhang, "Analysis of ill-conditioned power-flow problems using voltage stability methodology," *IEE Proceedings-Generation, Transmission and Distribution*, vol. 148, no. 5, pp. 384–390, 2001.

[18] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1387–1401, 2004.

[19] L. Wang and H.-D. Chiang, "Toward online line switching for increasing load margins to static stability limit," *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 1744–1751, 2015.

[20] B. Cui and X. A. Sun, "A new voltage stability-constrained optimal power-flow model: Sufficient condition, SOCP representation, and relaxation," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5092–5102, 2018.

[21] C. Wang, B. Cui, Z. Wang, and C. Gu, "SDP-based optimal power flow with steady-state voltage stability constraints," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4637–4647, 2018.

[22] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2320–2335, 2020.

[23] M. Higgins, K. Mayes, and F. Teng, "Enhanced cyber-physical security using attack-resistant cyber nodes and event-triggered moving target defence," *arXiv preprint arXiv:2010.14173*, 2020.

[24] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.
[25] K. M. Rogers and T. J. Overbye, "Some applications of distributed flexible AC transmission system (D-FACTS) devices in power systems," in *2008 40th North American Power Symposium*, 2008, pp. 1–8.
[26] 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," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.
[27] R. Faranda, A. Pievatolo, and E. Tironi, "Load shedding: A new proposal," *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 2086–2093, 2007.
[28] C. Mozina, "Undervoltage load shedding," in *2007 Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources*, 2007, pp. 39–54.
[29] H. Zhang, B. Liu, and H. Wu, "Net load redistribution attacks on nodal voltage magnitude estimation in ac distribution networks," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 2020, pp. 46–50.
[30] B. Liu and H. Wu, "Optimal planning and operation of hidden moving target defense for maximal detection effectiveness," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.