Covert Distribution Load Tripping Attacks

Betelihem Kebede Ashebo, Samuel Talkington, Saman Zonouz, and Daniel K. Molzahn
School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, USA
{bashebo3, talkington, szonouz6, molzahn}@gatech.edu

***Abstract*—The increasing integration of distributed energy resources (DERs), particularly solar photovoltaic (PV) systems, has introduced new cybersecurity challenges in distribution networks. This paper presents a data-driven attack model that examines how an adversary can exploit direct load control (DLC) mechanisms to selectively disconnect downstream loads during periods of high solar generation. Such targeted load tripping forces excess PV output to flow back toward the substation transformer, potentially causing power imbalances and transformer overloading. We model both PV output and load demand as multivariate Gaussian distributions to capture their inherent temporal and spatial uncertainties. A probabilistic power imbalance metric is defined to quantify the extent of reverse flow under compromised conditions. To identify the most impactful combinations of load disconnections and timing, we employ a multi-armed bandit approach based on the Upper Confidence Bound (UCB) algorithm. Simulation results demonstrate the feasibility and effectiveness of the attack strategy under realistic variability in solar output and demand.**

***Index Terms*—Distributed Energy Resources, Cybersecurity, Transformer Overloading, Multivariate Gaussian Modeling, Upper Confidence Bound**

I. Introduction

Distributed Energy Resources (DERs) enhance the flexibility, efficiency, and resilience of modern power grids, supporting the broader transition to sustainable energy systems. DERs encompass decentralized, small-scale generation and storage technologies such as solar photovoltaics (PV), wind turbines, and battery energy storage systems that are typically deployed near the point of consumption, enabling localized energy production and reducing reliance on centralized infrastructure.

Among the various DER technologies, solar photovoltaics (PV) have experienced the most significant growth, driven by rapid cost reductions, supportive policy measures, and the global shift toward decarbonization. Rooftop PV installations, in particular, have become increasingly prevalent in both residential and commercial sectors [1]. According to the U.S. Energy Information Administration (EIA), the United States added 26.3 GW of new PV capacity in 2023, raising the cumulative installed capacity to approximately 137.5 GW [2].

Despite their operational benefit, DERs also introduce new cybersecurity concerns, particularly as these systems become increasingly integrated with communication and control networks [3]. The National Institute for Standards and Technology (NIST) has highlighted that the incorporation of advanced technologies into the electric grid increases the system's exposure to cyber threats [4].

One potential vulnerability arises from the Direct Load Control (DLC) infrastructure widely implemented in demand response programs. Through DLC, utilities or aggregators remotely manage customer loads such as air conditioning units, water heaters, and pool pumps to balance supply and demand during peak periods. Although designed to enhance flexibility, this control mechanism presents a potential entry point for adversaries. By compromising DLC command signals, an attacker can selectively disconnect downstream loads [5]–[8]. When this occurs during periods of increased levels of PV generation, local demand is significantly reduced, forcing surplus solar power to flow upstream. Such reverse power flow can exceed transformer ratings, potentially causing equipment overloads and service interruptions [9]–[13].

A substantial body of research has explored the operational impacts of photovoltaic (PV) systems on distribution networks. For instance, Walling et al. [14] examined how rooftop PV influences local power flows and voltage profiles. Manito et al. [15] demonstrated that high levels of PV penetration exacerbate thermal stress and accelerate degradation in distribution transformers. Sharma et al. [16] and Hajeforosh et al. [17] investigated the conditions under which reverse power flow resulting from PV generation can lead to transformer overloading. Other research has focused on load-altering attacks, where adversaries manipulate control commands to disrupt demand profiles [18].

While these studies provide valuable insights into the physical and operational effects of PV integration, they often rely on deterministic assumptions that do not fully capture the stochastic nature of real-world grid conditions. In particular, few works address the joint uncertainties in PV generation and load demand during adversarial events [19].

To bridge this gap, this paper contributes a probabilistic modeling framework for load-tripping attacks in DER-integrated distribution networks. Our approach represents both PV output and load demand as correlated multivariate Gaussian random variables, enabling the analysis of variability across time and location. We define a probabilistic overload condition to estimate the likelihood that reverse power flow exceeds transformer capacity. To further guide effective attack strategy selection under uncertainty, we adopt a multi-armed bandit formulation using the Upper Confidence Bound (UCB) algorithm [20]–[22].

The rest of this paper is organized as follows. Section II formulates the adversarial load-tripping problem, introducing

This material is based upon work supported by the U.S. Department of Energy, Office of Science, Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The work of S. Talkington is supported by the National Science Foundation Graduate Research Fellowship.

Reproducibility: The code for this paper is publicly available at this link.

a probabilistic framework that jointly models the variability in photovoltaic output and load demand. This section also outlines the design of a data-driven attack strategy based on the Upper Confidence Bound (UCB) algorithm, which systematically identifies high-impact load disconnections. Section III describes the simulation setup based on a modified IEEE 13-bus test feeder, incorporating load and solar PV data from the SMART-DS Greensboro Area dataset. Section IV presents and interprets the numerical results, highlighting the conditions under which reverse power flow and transformer overloading are most likely to occur. Finally, Section V concludes the paper and discusses directions for future research.

II. Problem formulation

We consider an adversary who trips downstream loads to force excess DER generation back into the substation transformer, in order to induce overload or equipment failure. The adversary's strategy is defined by two principal decisions: the selection of loads to disconnect and the timing of their disconnection. Rather than shedding all loads, we assume that the adversary incurs some cost when compromising individual loads, or alternatively, seeks to avoid revealing the full extent of their capabilities for potential use in future attacks. Tripping the entire set of controllable loads at once would result in a sudden, large-scale disruption that would likely immediately trigger alarms and attract operator attention, undermining the attack's stealth.

Instead, the adversary strategically selects a subset of at most $k < n$ loads whose disconnection maximizes the net surplus of DER generation over the remaining demand, thereby inducing the greatest reverse power flow toward the substation transformer. The adversary does this carefully at discrete, spaced out time intervals, or *rounds*, to maintain a level of subtlety that delays detection. Equally important is the decision of when to act: the attacker schedules their load tripping at strategically chosen times based on the underlying stochastic process that governs the solar output and the demand.

Concretely, the attacker wishes to *learn the underlying distribution* of the customers' behavior and strategically time a select, potentially very small number of power outages. This targeted load selection coupled with precise timing enables the adversary to impose maximum stress on the substation transformer while minimizing the number of curtailed loads, and avoiding detection. This natural threat model is described very naturally as a multi-armed bandit algorithm.

A. Uncertainty model

Let $\boldsymbol{g}, \boldsymbol{d} \in \mathbb{R}^n_+$, be random active power generation and demand vectors in a lossless n-bus distribution network model with a single transformer. We emphasize that *the entries of these vectors do not need to be independent, nor do they need to be identically distributed.* The first and second moments of the random demand and generation vectors are

$$\mathsf{E}\left[\boldsymbol{d}\right] := \boldsymbol{\mu}_d, \qquad \mathsf{E}\left[\boldsymbol{d}\boldsymbol{d}^\top\right] := \boldsymbol{\Sigma}_d,$$
$$\mathsf{E}\left[\boldsymbol{g}\right] := \boldsymbol{\mu}_g, \qquad \mathsf{E}\left[\boldsymbol{g}\boldsymbol{g}^\top\right] := \boldsymbol{\Sigma}_g,$$

respectively. We analyze the difference between these two vector-valued stochastic processes—the random net power injection vector, defined as $\boldsymbol{p} := \boldsymbol{g} - \boldsymbol{d}$. Under the lossless assumption, the flow through the transformer is $S := \mathbf{1}^\top \boldsymbol{p}$. For simplicity, we adopt the simplifications of Assumption 1.

Assumption 1. The attacker has compromised all devices in the network, the power factors of all nodes are unity (i.e., reactive power is invariably zero), the network is lossless, and the random active power demands are bounded as $\mathbf{0} \leq \boldsymbol{d} \leq \overline{\boldsymbol{d}}$, almost surely.

Under Assumption 1, it can be shown that the net power injection vector is a sub-Gaussian random vector, allowing us to readily apply the theory of multi-armed bandits.

B. Threat model

The set of all attack strategies available to the adversary, or action space, is the set of all possible ways the adversary can trip off at most k loads. We can rigorously describe this action space as the n-dimensional *hyper-simplex* of radius k:

$$\mathcal{A} := \left\{\boldsymbol{a} \in \{0,1\}^n \ : \ ||\boldsymbol{a}||_1 \leq k\right\}. \tag{1}$$

The action space of the attacker, (1), is equivalent to the set of all binary vectors with at most k non-zero entries.

Suppose the attacker has compromised all devices in the network, and wishes to carefully choose a configuration of load tripping configurations over the course of a finite sequence of attack times. At each attack time, or *round* $t = 1, \dots, T$, the attacker chooses a load tripping attack $\boldsymbol{a}_t \in \mathcal{A}$, and observes the flow through the transformer $S : \mathcal{A} \to \mathbb{R}$, which takes the form

$$S(\boldsymbol{a}_t) := \mathbf{1}^\top \left(\boldsymbol{g}_t - \boldsymbol{A}_t \boldsymbol{d}_t\right) = \sum_{i=1}^n g_{ti} - d_{ti} \cdot \mathbb{1}\left\{a_{ti} = 1\right\}.$$

Here, $\boldsymbol{A}_t := \mathsf{diag}(\mathbf{1} - \boldsymbol{a}_t) \in \{0,1\}^{n \times n}$ is a binary diagonal matrix encoding the attack strategy at time t, where

$$(\boldsymbol{A}_t)_{ii} = 1 - (\boldsymbol{a}_t)_i = \begin{cases} 0, & i \in A_t \ (\mathsf{tripped}), \\ 1, & \mathsf{otherwise}. \end{cases} \tag{2}$$

In the attack matrix (2), we set $A_t \subseteq \{1, \dots, n\}$ to be the set of all loads that the attacker chooses to trip at time t.

C. Confidence bound analysis

To identify the most impactful combinations of load disconnections and time intervals for inducing reverse power flow toward the substation transformer, we employ the Upper Confidence Bound (UCB) algorithm; for a detailed description, see [22, Ch. 7].

Note that the net generation term $\mathbf{1}^\top \boldsymbol{g}_t$ is independent of the attack term $\boldsymbol{A}_t \boldsymbol{d}_t$. Thus, *maximizing the reward is equivalent to choosing the k loads with the highest demand* (in expectation) to trip. Each load i can therefore be treated as an independent "arm" with unknown mean demand $\mu_i := \mathsf{E}[d_i]$. A standard upper confidence bound (UCB) rule for each arm, followed by selecting the TopK UCB scores, gives an optimal strategy.

Thus, at each time step t, the attack strategy $A_t := \mathsf{TopK}_t \subseteq \{1, \ldots, n\}$ is the indices of the k largest UCBs. Let N_i be the number of times the attacker has tripped load i, and define the attacker's sample mean estimator for each load i:

$$\hat{\mu}_i := \frac{1}{N_i} \sum_{\tau \in [t]} d_{\tau i} \cdot \mathbb{1}\{i \in A_\tau\}. \tag{3}$$

Appealing to Hoeffding's inequality, the UCB score of load i at time step t is then

$$\mathsf{UCB}_t(i) := \hat{\mu}_i + c_t \cdot \sqrt{\frac{2\log(t)}{\max(1, N_i)}}, \tag{4}$$

where $c_t > 0$ is some time-varying exploration coefficient.

D. Algorithm

The covert load tripping strategy employed by the attacker is described in Alg. 1. This online UCB algorithm seeks to estimate the first moment of the loads $\mathsf{E}[\boldsymbol{d}]$ and maximizes the flow through the transformer by picking the K largest of them.

Algorithm 1 Covert Load Tripping Attack

Require: Attack horizon T, attack budget K

Initialize: $\boldsymbol{a} \leftarrow \mathbf{0}_n$, $N_i \leftarrow 0$, $\quad \widehat{\mu}_i \leftarrow 0 \quad i = 1, \ldots, n$.
for each round $t = 1$ to T **do**
  $\mathsf{UCB}_t(i) \leftarrow \hat{\mu}_i + \alpha\sqrt{\frac{2\log(t)}{\max\{1, N_i\}}}$
  Select: $A_t \leftarrow \mathsf{TopK}(\mathsf{UCB}_t(i),\, i = 1, \ldots, n)$
  Execute attack: $(\boldsymbol{a})_i = 0$ for all $i \in A_t$,.
  for each tripped node $i \in A_t$ **do**
    Update trip count: $N_i \leftarrow N_i + 1$,
    Update sample estimator: $\widehat{\mu}_i \leftarrow \widehat{\mu}_i + \frac{d_{it} - \widehat{\mu}_i}{N_i}$
  end for
  Observe imbalance: $S(\boldsymbol{a}_t) \leftarrow \frac{1}{S_{\max}} \mathbf{1}^\top (\boldsymbol{g}_t - \boldsymbol{a}_t \circ \boldsymbol{d}_t)$
end for
return Optimal configuration: $\boldsymbol{a}_\star \leftarrow \boldsymbol{a}_T$

III. Experimental Description

A. Regret analysis

Throughout our experiments, we analyze the *cumulative regret*, which is a common metric used to analyze online learning algorithms. Given a sequence of load tripping actions at time t, $\{\boldsymbol{a}_\tau\}_{\tau=1}^t \subseteq \mathcal{A}$, we define the cumulative regret of the adversary at time t as

$$R_t := \mathsf{E}\left[\max_{\boldsymbol{a} \in \mathcal{A}} \sum_{\tau \in [t]} S_\tau(\boldsymbol{a}) - S_\tau(\boldsymbol{a}_t)\right], \tag{5}$$

where $[t] := \{1, \ldots, \tau, \ldots, t\}$. In words, the regret (5) measures the average difference between how large the attacker could have caused the power flow to be, and what was actually done by the sequence of actions taken by the attacker.

B. Dataset description

We use a lossless formulation for a modified IEEE 13-bus test case [23] integrated with the open-source SMART-DS Greensboro Area synthetic dataset [24], which is available at [25]. In particular, our simulations use load and solar PV time-series data selected from the `urban_suburban` feeder, and we select the `solar high_batteries_none_timeseries` scenario, which represents a high-penetration solar deployment without battery storage. This choice allows us to isolate the effects of solar generation on feeder dynamics without the confounding influence of local energy storage.

The time-series data in the SMART-DS dataset includes real power consumption at 15-minute resolution. Load profiles are drawn from the NREL ResStock model for residential buildings. PV generation data is derived from the National Solar Radiation Database (NSRDB) and similarly interpolated to 15-minute intervals. Each PV unit is associated with a time-series file indicating power output scaled to its inverter capacity.

This setup reflects a realistic urban feeder with temporal variability in both demand and generation. It enables us to evaluate the system's response to targeted cyber-physical disruptions under high DER penetration, particularly under peak solar generation conditions.

IV. Results

For the exploratory work described in this paper, we implemented the Upper Confidence Bound (UCB). While the attacker is theoretically capable of exploring all $2^{13} - 1 = 8191$ feasible load combinations, we adopt a key simplification: the attacker's action space is constrained to shutting off at most k loads at each time step.

An important consideration is the statistical correlation between local PV generation and customer load consumption. Due to this correlation, the impact of disconnecting specific loads varies significantly. Loads closely aligned with PV production contribute disproportionately to net surplus injections at the substation and thus represent strategic targets for the adversary.

Under baseline (non-attacked) conditions, the power imbalance at the substation modeled as a Gaussian random variable exhibits a mean of $\mathbb{E}[S] = -1.50$ p.u. and a standard deviation of $\sigma[S] = 3.426$ p.u.. The negative mean indicates that, on average, the substation draws power from the upstream grid to meet local demand, confirming its role as a net importer of energy. The standard deviation reflects natural fluctuations in net demand arising from temporal variability in both load consumption and PV generation.

The UCB algorithm identified an optimal strategy involving the simultaneous disconnection of different residential loads. This targeted action resulted in a significant net power surplus of $|S(k_t)| = 5.0605$ p.u., reversing power flow direction and marginally exceeding the transformer's rated capacity. Specifically, this induced an overload of approximately 1.2% above its rated limit.

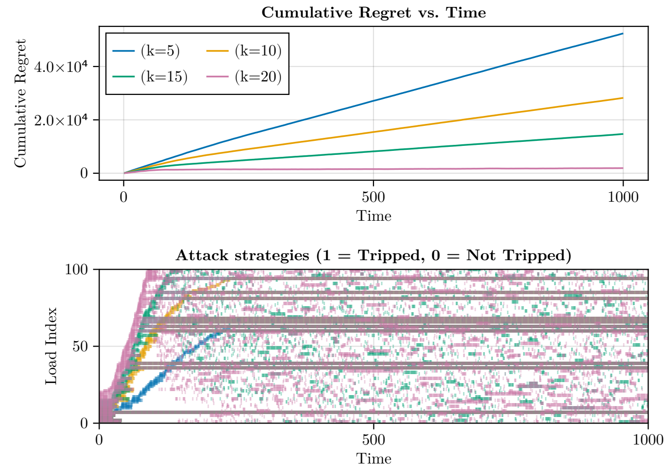

Fig. 1. Performance of Algorithm 1 on the proposed random test dataset with $n = 100$ nodes, and 10 nodes i that follow the vulnerable distribution. We show the results output by Alg. 1 with tripping budgets $k \in \{5, 10, 15, 20\}$.

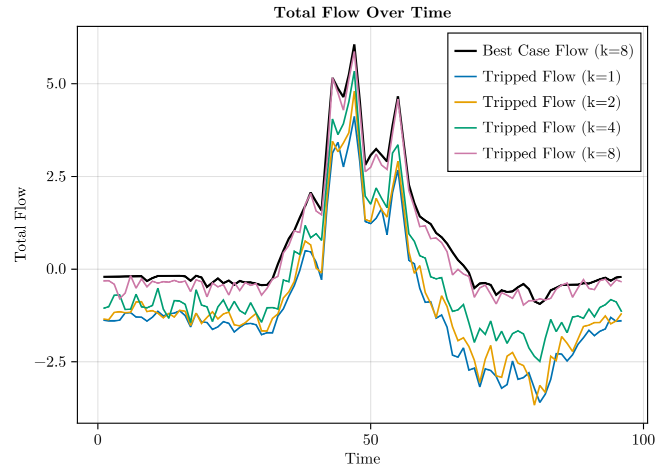

Fig. 2. Flow through the transformer vs. time when applying the load tripping strategy in Alg. 1 to realistic data. The data are sourced 13 nodes taken from urban-suburban feeder within the SMART-DS Greensboro test case [25] with attack budgets $k \in \{1, 2, 4, 8\}$.

A. Synthetic data

We first demonstrate the results of the covert load tripping algorithm on synthetic data. The experiments depicted in this section are fully reproducible and are publicly available at the following link:

Link to reproducible Julia code

Fig. 1 shows the results of the load tripping Alg. 1 on $t = 1, \ldots, T = 1000$ iid copies of the following random vectors:

1) generation: $(\boldsymbol{g}_t)_i \sim \mathcal{N}(\mu, 1)$, and
2) demand: $\boldsymbol{d}_t$, where each entry is one of the following Gaussian random variables: d^{typ} or d^{vuln}, where
   - $d^{\mathsf{typ}} \sim \mathcal{N}(\frac{1}{2}\mu, 1)$ is a "typical" load and
   - $d^{\mathsf{vuln}} \sim \mathcal{N}\left((\frac{1}{2} + \xi) \cdot \mu, 1\right)$, $\xi \sim \mathsf{Uniform}(0, 1)$ is a "vulnerable" demand, with a potentially much larger mean, making these nodes ripe for a cyberattack.

The results on the synthetic data in Fig. 1 demonstrate the typical logarithmic regret behaviors for UCB algorithms. In fact, it is possible to show that UCB is provably good for this problem, and that it is not possible to do better.

Although quantitatively small, the observed overload underscores a critical finding: strategically timed, minimal interventions such as the disconnection of a carefully selected subset of residential loads can effectively challenge, and even momentarily surpass, the operational thresholds of distribution infrastructure. This highlights the disproportionate impacts that low-effort, targeted actions can have on device overloads.

Fig. 2 shows the total power flow (in p.u.) under coordinated attacks. The colored lines correspond to the attack strategy in Algorithm 1 which selects and trips k loads at each time step, where k denotes the number of loads tripped by the attacker. As k increases, the magnitude of the reverse power flow becomes more significant, particularly during midday hours when the solar generation is high.

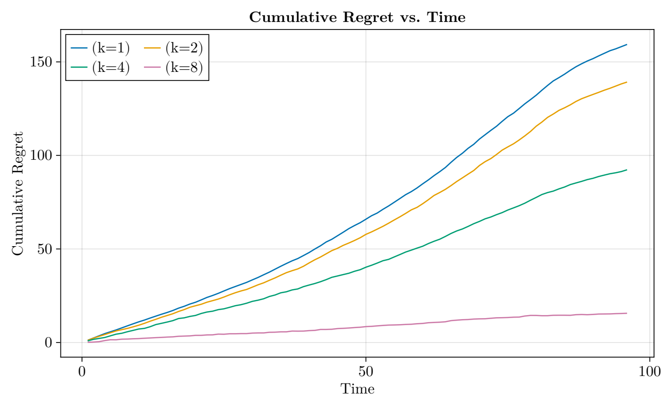

Fig. 3. Cumulative regret vs. time when applying the load tripping strategy in Alg. 1 to realistic data. The data are sourced 13 nodes taken from urban-suburban feeder within the SMART-DS Greensboro test case [25] with attack budgets $k \in \{1, 2, 4, 8\}$.

Fig. 3 presents the cumulative regret over time for different values of k. As shown, smaller values of k result in higher cumulative regret, indicating that the attack policy is less effective at approximating the most extreme impact. In contrast, larger values such as $k = 8$ achieve much lower cumulative regret, which shows that the attack strategy in Alg. 1 more closely approximates the optimal tripping policy as more loads are allowed to be compromised.

V. Conclusion

We analyzed an online attack algorithm that exposes vulnerabilities in power distribution networks by strategically disconnecting downstream loads, thereby inducing reverse power flow and potentially overloading substation transformers. Operating under uncertainty, the adversary employs a Gaussian statistical model capturing the variability of solar

PV generation and customer load demand. By leveraging the Upper Confidence Bound (UCB) algorithm, the attacker identifies an optimal subset of loads to disconnect at carefully selected times, maximizing stress on the substation transformer with minimal and targeted intervention.

Our findings demonstrate that this type of attack is both plausible and effective. Even under conservative assumptions, strategically timed, limited-scale load disconnections can trigger transformer overloads, highlighting a significant vulnerability in feeders with high DER penetration. Although our analysis adopts an adversarial perspective, the insights gained can directly inform the development of proactive detection methods and mitigation strategies, underscoring the critical need for enhanced situational awareness and resilience planning in DER-integrated grids.

Future work will extend this framework by integrating models of the power flow equations and empirical variance estimates, thereby providing a more detailed assessment of voltage violations and potential cascading effects under attack scenarios. In addition, we will focus on developing real-time detection algorithms capable of identifying anomalous shifts in power flows and load patterns consistent with adversarial activities, even with limited observability and uncertainty in DER outputs. To support broader applicability, future work will also address the scalability of the proposed approach to accommodate larger distribution networks.

References

[1] P. Jahangiri and D. C. Aliprantis, "Distributed volt/var control by PV inverters," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3429–3439, 2013.

[2] National Renewable Energy Laboratory (NREL), "Spring 2024 solar industry update," U.S. Department of Energy, Tech. Rep. NREL/PR-6A20-90042, 2024. [Online]. Available: https://www.nrel.gov/docs/fy24osti/90042.pdf

[3] M. R. Maghami, A. G. O. Mutambara, and C. Gomes, "Assessing cyber attack vulnerabilities of distributed generation in grid-connected systems," *Environment, Development and Sustainability*, pp. 1–27, 2025.

[4] V. Pillitteri and T. Brewer, "Guidelines for smart grid cybersecurity," NIST Interagency/Internal Report (NISTIR 7628 Revision 1), Tech. Rep., September 2014.

[5] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[6] P. Xun, P. dong Zhu, S. Maharjan, and P. Cui, "Successive direct load altering attack in smart grid," *Computers & Security*, vol. 77, pp. 79–93, 2018.

[7] E.-N. S. Youssef, F. Labeau, and M. Kassouf, "Adversarial dynamic load-altering cyberattacks against peak shaving using residential electric water heaters," *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 2073–2088, 2023.

[8] A. Ebtia, D. E. Rebbah, M. Debbabi, M. Kassouf, M. Ghafouri, A. Mohammadi, and A. Soeanu, "Spatial-temporal data-driven model for load altering attack detection in smart power distribution networks," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 5, pp. 7414–7427, 2024.

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[10] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.

[11] F. Ebe, B. Idlbi, J. Morris, G. Heilscher, and F. Meier, "Evaluation of PV hosting capacities of distribution grids with utilisation of solar roof potential analyses," *CIRED 24*, vol. 2017, no. 1, pp. 2265–2269, 2017.

[12] I. B. Majeed and N. I. Nwulu, "Impact of reverse power flow on distributed transformers in a solar-photovoltaic-integrated low-voltage network," *Energies*, vol. 15, no. 23, p. 9238, 2022.

[13] W. A. Jabbar, S. Annathurai, T. A. A. Rahim, and M. F. M. Fauzi, "Smart energy meter based on a long-range wide-area network for a stand-alone photovoltaic system," *Expert Systems with Applications*, vol. 197, p. 116703, 2022.

[14] R. Walling, R. Saint, R. C. Dugan, J. Burke, and L. A. Kojovic, "Summary of distributed resources impact on power delivery systems," *IEEE Transactions on Power Delivery*, vol. 23, no. 3, pp. 1636–1644, 2008.

[15] A. R. Manito, A. Pinto, and R. Zilles, "Evaluation of utility transformers' lifespan with different levels of grid-connected photovoltaic systems penetration," *Renewable Energy*, vol. 96, pp. 700–714, 2016.

[16] V. Sharma, S. M. Aziz, M. H. Haque, and T. Kauschke, "Effects of high solar photovoltaic penetration on distribution feeders and the economic impact," *Renewable and Sustainable Energy Reviews*, vol. 131, p. 110021, 2020.

[17] S. Hajeforosh, A. Khatun, and M. Bollen, "Enhancing the hosting capacity of distribution transformers for using dynamic component rating," *International Journal of Electrical Power & Energy Systems*, vol. 142, p. 108130, 2022.

[18] S. Maleki, S. Pan, S. Lakshminarayana, and C. Konstantinou, "Survey of load-altering attacks against power grids: Attack impact, detection and mitigation," *IEEE Open Access Journal of Power and Energy*, 2025.

[19] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2015.

[20] W. Macready and D. Wolpert, "Bandit problems and the exploration/exploitation tradeoff," *IEEE Transactions on Evolutionary Computation*, vol. 2, no. 1, pp. 2–22, 1998.

[21] P. Auer, "Using confidence bounds for exploitation-exploration trade-offs," *Journal of Machine Learning Research*, vol. 3, pp. 397–422, November 2002.

[22] T. Lattimore and C. Szepesvari, *Bandit Algorithms*. Cambridge University Press, July 2020.

[23] D. M. Fobes, S. Claeys, F. Geth, and C. Coffrin, "PowerModels-Distribution.jl: An open-source framework for exploring distribution power flow formulations," *Electric Power Systems Research*, vol. 189, no. C, November 2020, presented at *21st Power Systems Computation Conference (PSCC)*, June 2020.

[24] B. Palmintier, T. Elgindy, C. Mateo, F. Postigo, T. Gómez, F. de Cuadra, and P. D. Martinez, "Experiences developing large-scale synthetic US-style distribution test systems," *Electric Power Systems Research*, vol. 190, p. 106665, November 2021, presented at *21st Power Systems Computation Conference (PSCC)*, June 2020.

[25] B. Palmintier, C. Mateo Domingo, F. E. Postigo Marcos, T. Gomez San Roman, F. de Cuadra, N. Gensollen, T. Elgindy, and P. Duenas, "SMART-DS Synthetic Electrical Network Data OpenDSS Models for SFO, GSO, and AUS," 2020. [Online]. Available: https://data.openei.org/submissions/2981