Analyzing the Cyber Resilience of Distribution Systems with Vulnerable Inverter-Based Resources

Betelihem Ashebo, Anna Raymaker, Samuel Talkington, Richard Asiamah,
Animesh Chhotaray, Saman Zonouz, and Daniel K. Molzahn
Georgia Institute of Technology
{bashebo3,araymaker3,talkington,rasiamah3,achhotaray3,szonouz6,molzahn}@gatech.edu

Abstract

The proliferation of distributed energy resources (DERs), particularly solar photovoltaic (PV) systems, introduces new operational and security challenges for distribution networks. This paper presents a cyber-physical attack framework in which an adversary manipulates selected inverters to disrupt grid operations. To identify worst-case attacks, we formulate optimization problems that maximize steady-state voltage violations. The set of compromised inverters in these problems is constrained by an attack budget that is informed by vulnerabilities identified via our associated screening of Internet-connected inverters. The worst-case attack problems are formulated as Mixed-Integer Linear Programs (MILPs) that use the linearized DistFlow equations to model the impact of the attack on unbalanced three-phase distribution systems. The attack solutions obtained from the LinDist3Flow formulation are validated using AC power flow (ACPF) simulations with fixed attacked inverter setpoints. Numerical experiments on modified IEEE `13-bus`*,* `34-bus`*, and* `123-bus` *distribution test cases demonstrate that compromising between* $10\,\%$ *and* $25\,\%$ *of strategically selected inverters can induce voltage violations across multiple buses.*

Keywords: Cyber-physical Attacks, Distributed Energy Resources, Voltage Violations

1. Introduction

The power grid is undergoing a transformative evolution with the widespread integration of Distributed Energy Resources (DERs), including electric vehicles (EVs), solar photovoltaic (PV) systems, battery storage solutions, and smart home technologies. These resources enable decentralized energy production, storage, and consumption, marking a significant shift from the traditional centralized grid model. They introduce greater flexibility, efficiency, and resilience in the transition toward cleaner and more sustainable energy systems. However, their increasing digitization and connectivity have also expanded cyber-physical attack surfaces in electric power systems [1].

Among DER technologies, solar PV systems are of particular concern because of their rapid global adoption and reliance on Internet-connected smart inverters. Many of these inverters communicate via hosted management platforms or web interfaces that are directly reachable on the public Internet. Recent cybersecurity studies [2, 3] have shown that thousands of inverters, gateways, and data loggers are exposed online with weak authentication or outdated firmware. Malicious actors can potentially exploit these vulnerabilities and manipulate inverter settings to both interrupt local DER operations and propagate disturbances across the wider power system [4–11].

Building on the established insecurity of PV systems, prior research has largely examined how voltage related operational stresses in distribution networks can be aggravated under high PV penetration [12–23]. More recent publications have shown that coordinated cyber-physical attacks, including false-data injection and malicious inverter manipulation, can amplify voltage violations and compromise grid stability [24–27].

Prior literature has primarily examined the physical effects of high PV penetration and, more recently, the potential for cyber-physical attacks to worsen voltage problems in distribution networks. However, existing studies often assume an exogenous attack size, such as a fixed number of compromised solar PVs, rather than identifying which solar PVs an attacker would prioritize under limited attack resources. As a result, they do not fully capture the tradeoff between the effort required to compromise different solar PVs and the voltage impact that those compromised solar PVs can induce. In addition, over-voltage and under-voltage impacts are not always treated as equally important attack outcomes within a unified optimization framework. Analyses are frequently carried out on balanced or single-phase models as well. Finally, prior literature does not always use a full AC power-flow solution to validate the choice of which inverters to compromise.

To bridge these gaps, this paper develops a cyber-physical optimization framework to determine which

solar PVs an attacker would select, under a limited compromise budget, to induce the largest steady-state voltage violations in an unbalanced distribution network. Specifically, we formulate attack models for both under-voltage and over-voltage cases, in which the attacker chooses a subset of solar PVs to compromise and manipulates their real and reactive power setpoints to maximize voltage violations across the feeder. To make this selection problem tractable, we employ a linearized approximation of the DistFlow equations, which allows the optimization to include binary decision variables representing which solar PVs are compromised. The resulting formulation therefore identifies both the compromised solar PVs and the corresponding voltage violation outcome for a given budget. To verify that the LinDist3Flow based attack decisions remain physically meaningful, we validate the resulting voltage profiles and identify violations against nonlinear AC power flow (ACPF) solutions.

The remainder of the paper is organized as follows. Section 2 introduces the cyberattack vector, the attacked solar PV models, and the network model. Section 3 develops the voltage violation model. Section 4 presents the numerical results, including the experimental setup, implementation details, and voltage violation results. Finally, Section 5 concludes the paper and discusses future research.

2. Network and Solar PV Modeling

This section introduces our models for both the adversary and the physical system. We first detail the cyber threat model, which defines the attacker's capabilities, the criticality ranking of different vulnerabilities based on their cost and post-compromise impact, and the distribution of the vulnerability classes. We then present the network model used to represent the physical network, providing the basis for the attack formulations developed in subsequent sections.

2.1. Cyber Threat Model

A cyberattack on a power grid could take multiple forms. In this paper, we consider a remote, Internet-facing adversary who (i) has no insider or physical access to the grid, (ii) can perform large-scale Internet scanning and exploit development with commodity compute, and (iii) targets exposed solar PV systems. Although the same general attack model could apply to other distributed energy resources, we focus on solar PVs because they are the subject of our ongoing Internet-scanning research. In this setting, the attacker can compromise solar PVs depending on the communication and Internet infrastructure through which they are deployed.

1) *Vulnerability classes:* We categorize the attack surface into four vulnerability classes (also referred to as exposure classes) that capture the dominant, observable ways solar PVs appear on the public Internet, namely Modbus/TCP exposure (M), unauthenticated web interface (U), web interface with known vulnerabilities (C), and web interface with login (L).

These classes differ in terms of the difficulty to exploit the vulnerability, i.e., the attacker's effort or cost, and also the post-compromise capability of an adversary that has successfully exploited a vulnerability. For example, while Modbus exposure (M) typically provides the lowest barrier to direct solar PV manipulation, login-only portals (L) have the highest barrier as they require an adversary to guess the credentials. Naturally, unauthenticated web interfaces (U) are easier to breach than those with known vulnerabilities (C). Using these insights, we use the following conservative ordering (highest $\rightarrow$ lowest) of vulnerability classes based on their criticality:

$$\mathrm{M} > \mathrm{U} > \mathrm{C} > \mathrm{L}. \tag{1}$$

Prior work has demonstrated that Internet-connected industrial and operational technology solar PV systems can be discovered at scale via Internet scanning, supporting the plausibility of finding exposed solar PVs in real deployments [28]. Additionally, public vulnerability reports document known vulnerabilities and incidents affecting widely deployed solar PV inverter models, underscoring the practical risks associated with exposure [3,29]. As shown in Figure 1, these exposure classes can be represented as entry points in an attack graph linking adversary actions to solar PV manipulations.

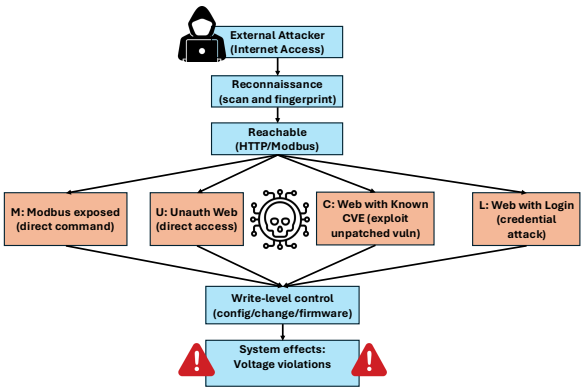


Figure 1. Attack graph for compromising smart inverters.

Using the Censys Internet-wide scanning platform, we identified representative examples of exposed solar PV systems. A screenshot in the appendix (Fig. 7) shows an exposed metering center served over an unauthenticated web interface that also exposes a Modbus/TCP

endpoint. For these exposed solar PV systems, once compromised, an attacker may be able to change active and reactive power setpoints, disable anti-islanding or other protective functions, upload malicious firmware, or issue commands that cause trips or other abnormal behavior.

2) Distribution of vulnerability classes: We assign each DER to a vulnerability class using the empirical exposure distribution measured by our companion Internet-scanning study [30]. Because a single host can exhibit more than one exposure (for example, an unauthenticated web interface that also advertises a Modbus endpoint), we map each DER to a single class corresponding to its most severe observed exposure, following the criticality ordering in (1): Modbus/TCP exposure (M) takes precedence, followed by unauthenticated web interface (U), web interface with known vulnerabilities (C), and login-protected web interface (L). This yields mutually exclusive classes whose prevalences across the exposed solar PV population are $p_{\mathrm{M}} = 10.45\%$, $p_{\mathrm{U}} = 18.75\%$, $p_{\mathrm{C}} = 7.84\%$, and $p_{\mathrm{L}} = 62.96\%$.

The vulnerability class assigned to a DER determines its *cost to compromise* c_s, which reflects the attacker effort required to gain write-level control through that exposure. We assign costs that increase by a unit step along the ordering in (1), namely $c_{\mathrm{M}} = 1$, $c_{\mathrm{U}} = 2$, $c_{\mathrm{C}} = 3$, and $c_{\mathrm{L}} = 4$. These are relative costs, so only their ratios affect the budget constraint in (2c). Each unit increment corresponds to an additional capability the attacker must acquire. Modbus/TCP exposure (M) is the lowest-cost path: it requires neither authentication nor an exploit, as the attacker connects to a standardized protocol and issues read or write commands directly to inverter registers. An unauthenticated web interface (U) likewise requires no credentials, but the attacker must first identify the device-specific control endpoints and interpret a non-standardized vendor interface rather than a uniform protocol, adding reconnaissance effort. A web interface with a known CVE (C) further requires obtaining or developing a working exploit for the disclosed vulnerability and applying it successfully, which is more effort than interacting with an already-open interface. Finally, a login-protected interface (L) requires defeating an explicit access control through default-credential testing, credential stuffing, or brute force, with no guarantee of success and the risk of lockout, making it the highest-cost path.

2.2. Attacked and Non-Attacked Solar PVs

We model the attacker's selection of which distributed generators (DGs) to compromise and how they are operated maliciously. Let $\mathcal{S} \subseteq \mathcal{N}$ denote the nodes with distributed generation, and let $u_s \in \{0, 1\}$ be a binary variable indicating whether the attacker controls a particular DG $s \in \mathcal{S}$, where

$$u_s = \begin{cases} 1 & \text{generator } s \text{ is compromised} \\ 0 & \text{otherwise.} \end{cases}$$

When a solar PV is compromised ($u_s = 1$), the attacker gains the ability to manipulate its power injections.

The relation in (2a) describes how the attacker can set the active power, P_s, to any value between zero and the inverter's full capability, P_s^*. If the solar PV is not compromised ($u_s = 0$), its output is fixed to the nominal setpoint, P_s^*. Likewise, (2b) models the attacker's ability to set the reactive power output within the solar PV's reactive power limits $\underline{Q}_s$ and $\overline{Q}_s$ when this generator is attacked ($u_s = 1$). Otherwise, the solar PV operates at a nominal reactive power setpoint Q_s^* (e.g., $Q_s^* = 0$ for unity power factor operation).

Finally, the attacker's actions are limited by a total attack budget, B, that models the effort that the attacker can allocate to compromising solar PV generators. As shown in (2c), this formulation ensures that the sum of the individual costs c_s for each compromised solar PV (where $u_s = 1$) does not exceed the budget. These relationships are:

$$P_s^*(1 - u_s) \le P_s \le P_s^*, \tag{2a}$$

$$Q_s^*(1 - u_s) + \underline{Q}_s u_s \le Q_s \le Q_s^*(1 - u_s) + \overline{Q}_s u_s, \tag{2b}$$

$$\sum_{s \in \mathcal{S}} c_s u_s \le B, \tag{2c}$$

$$u_s \in \{0, 1\}. \tag{2d}$$

for all solar PVs $s \in \mathcal{S}$.

2.3. Network Model

We consider a distribution network modeled as an undirected graph $G = (\mathcal{N} \cup \{0\}, \mathcal{E})$, where $\mathcal{N}$ denotes the set of all nodes in the network except the source node. The set of phases present at a node i is denoted by $\Phi_i \subseteq \{a, b, c\}$. Each branch $(i, j) \in \mathcal{E}$ is characterized by its phase-impedance matrices, $\mathbf{R}_{ij} = [r_{\psi\psi'}]$ and $\mathbf{X}_{ij} = [x_{\psi\psi'}]$. The complex phase impedance matrix is given as $\mathbf{Z}_{ij} := \mathbf{R}_{ij} + \mathrm{j}\mathbf{X}_{ij}$.

The network operating point is characterized by $\mathbf{P}_{ij}$ and $\mathbf{Q}_{ij}$, the real and reactive power flowing from node i to node j; the squared voltage magnitudes at node i (with $v_i^\psi := |V_i^\psi|^2$); $\boldsymbol{\ell}_{ij}$, the squared current magnitudes on the line; and p_j^ψ, q_j^ψ, the net real and reactive power injections at node j on phase ψ.

1) AC DistFlow: We largely adopt the standard notation for the branch flow model (BFM); see [31] and [32, Sections 2.2, 2.3]. For each node $i \in \mathcal{N}$, let $V_i := [V_i^{\psi}]_{\psi \in \Phi_i}$ denote the vector of per-phase nodal voltages, and for each line $l \in \mathcal{E} : l \ni i$ incident on i, let $I_{ij} := [I_{ij}^{\psi}]_{\psi \in \Phi_i}$. The complex power flows in a three-phase unbalanced distribution network are fully described by the following set of equations.

1. Ohm's law:

$$V_j = V_i - \mathbf{Z}_{ij} I_{ij},$$

for each node $i \in \mathcal{N}$.

2. Definition of complex flows:

$$S_{ij} := V_i I_{ij}^{\mathsf{H}},$$

and the definition of square current magnitudes:

$$\ell_{ij} := \mathsf{diag}(I_{ij} I_{ij}^{\mathsf{H}}),$$

for each branch $(i, j) \in \mathcal{E}$. Here, $(\cdot)^{\mathsf{H}}$ denotes the complex conjugate transpose and $\mathsf{diag}(\cdot)$ denotes the extraction of the entries of the rank-one matrix $I_{ij} I_{ij}^{\mathsf{H}}$.

3. Power balance:

$$\sum_{i:i \to j} \mathsf{diag}(S_{ij} - \mathbf{Z}_{ij} \ell_{ij}) + s_j = \sum_{k:j \to k} \mathsf{diag}(S_{jk})$$

for all nodes $j \in \mathcal{N}$.

2) Linearized DistFlow (LinDist3Flow): The LinDist3Flow model [31, 33] simplifies the DistFlow formulation discussed in Section 2.3 by neglecting line losses and linearizing the voltage drop. This linearization is performed around an operating point of zero power injections and flows, yielding the following tractable, three-phase model:

$$P_{ij}^{\psi} + p_j^{\psi} = \sum_{k:j \to k} P_{jk}^{\psi}, \qquad \forall \psi \in \{a, b, c\}, \tag{3a}$$

$$Q_{ij}^{\psi} + q_j^{\psi} = \sum_{k:j \to k} Q_{jk}^{\psi}, \qquad \forall \psi \in \{a, b, c\}, \tag{3b}$$

$$\boldsymbol{v}_j = \boldsymbol{v}_i + \mathbf{M}_{P,ij} \mathbf{P}_{ij} + \mathbf{M}_{Q,ij} \mathbf{Q}_{ij}, \tag{3c}$$

where the matrices $\mathbf{M}_{P,ij}$ and $\mathbf{M}_{Q,ij}$ are defined for each line $(i, j) \in \mathcal{E}$ using the per-phase series resistances $r_{\psi\psi'}$ and reactances $x_{\psi\psi'}$ (for phases $\psi, \psi' \in \Phi$) as follows:

$$\mathbf{M}_{P,ij} = \begin{bmatrix} -2r_{aa} & r_{ab} - \sqrt{3}x_{ab} & r_{ac} + \sqrt{3}x_{ac} \\ r_{ba} + \sqrt{3}x_{ba} & -2r_{bb} & r_{bc} - \sqrt{3}x_{bc} \\ r_{ca} - \sqrt{3}x_{ca} & r_{cb} + \sqrt{3}x_{cb} & -2r_{cc} \end{bmatrix}, \tag{4a}$$

$$\mathbf{M}_{Q,ij} = \begin{bmatrix} -2x_{aa} & x_{ab} + \sqrt{3}r_{ab} & x_{ac} - \sqrt{3}r_{ac} \\ x_{ba} - \sqrt{3}r_{ba} & -2x_{bb} & x_{bc} + \sqrt{3}r_{bc} \\ x_{ca} + \sqrt{3}r_{ca} & x_{cb} - \sqrt{3}r_{cb} & -2x_{cc} \end{bmatrix}. \tag{4b}$$

3. Voltage Violation Attack

In this section, we formulate attack variants that maximize voltage violations. To model distinct adversarial strategies, we consider three variants of the attack, each defined by a different mathematical norm of the voltage violation vector, $\boldsymbol{\delta}$. Each variant corresponds to an optimization problem with a different attack objective. Specifically, we use the ℓ_0-norm to maximize the number of violating bus-phases (widespread disruption), the ℓ_∞-norm to target the single worst-case violation, and the ℓ_1-norm to maximize the total aggregate violation.

To formulate these objectives, we first define the individual elements of the violation vector $\boldsymbol{\delta}$. We introduce non-negative slack variables for each bus-phase pair (i, ψ) to represent the magnitude of over-voltage and under-voltage violations. The over-voltage violation, $\delta_{i,\psi}^{+}$, and the under-voltage violation, $\delta_{i,\psi}^{-}$, are defined as:

$$\delta_{i,\psi}^{+} := \max\left\{v_{i,\psi} - v_{i,\psi}^{\max},\, 0\right\}, \tag{5a}$$

$$\delta_{i,\psi}^{-} := \max\left\{v_{i,\psi}^{\min} - v_{i,\psi},\, 0\right\}, \tag{5b}$$

where $v_{i,\psi}$ denotes the squared voltage magnitude and $v_{i,\psi}^{\min}$ and $v_{i,\psi}^{\max}$ represent the lower and upper squared voltage magnitude limits for the corresponding bus and phase, respectively.

The total violation at each bus-phase pair, $\delta_{i,\psi}$, constitutes the elements of the violation vector $\boldsymbol{\delta}$. Formally, the total violation is defined as the sum of these over- and under-voltage components

$$\delta_{i,\psi} = \delta_{i,\psi}^{+} + \delta_{i,\psi}^{-} \tag{6}$$

for each node $i \in \mathcal{N}$ and each phase $\psi \in \Psi_i$. As these components are complementary, with at most one being non-zero for any given bus and phase, their sum effectively captures the magnitude of whichever violation is active. We also define the binary indicator $\phi_{i,\psi} := \phi_{i,\psi}^{+} + \phi_{i,\psi}^{-}$, which equals 1 when bus-phase (i, ψ) lies outside its operational bounds.

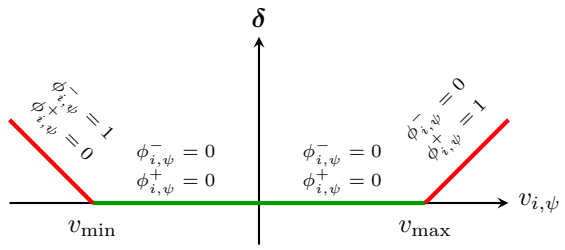


Figure 2. An indicator function for voltage violations where $\phi_{i,\psi} \in \{0,1\}$ is 1 when $v_{i,\psi}$ lies outside its operational bounds and 0 otherwise, while δ measures the size of the violation.

In addition to the solar PV model constraints from Section 2.2, the following constraints define the variables used to measure voltage violations. The formulation employs binary indicators $\phi^+_{i,\psi}$ and $\phi^-_{i,\psi}$ to show whether the voltage lies outside its operational bounds, as illustrated in Fig. 2. We do not enforce voltage bounds as hard constraints; instead, we use them to measure how far the voltages move outside the admissible range, and then maximize that measured violation through the chosen attack objective. The resulting problem remains a mixed-integer linear program, which allows us to solve it with standard solvers such as Gurobi and makes the approach scalable.

The relationship in Figure 2 is formalized by the following big-M constraints for each bus i and phase ψ. First, for each over-voltage variable $\delta^+_{i,\psi}$ and under-voltage variable $\delta^-_{i,\psi}$, we impose non-negativity:

$$\delta^+_{i,\psi} \geq 0, \qquad \delta^-_{i,\psi} \geq 0, \tag{7}$$

and apply the following upper bounds

$$\delta^+_{i,\psi} \leq \left(v_{i,\psi} - v^{\max}_{i,\psi}\right) + M\left(1 - \phi^+_{i,\psi}\right), \tag{8a}$$

$$\delta^+_{i,\psi} \leq M\phi^+_{i,\psi}, \tag{8b}$$

$$\delta^-_{i,\psi} \leq \left(v^{\min}_{i,\psi} - v_{i,\psi}\right) + M\left(1 - \phi^-_{i,\psi}\right), \tag{8c}$$

$$\delta^-_{i,\psi} \leq M\phi^-_{i,\psi}, \tag{8d}$$

for all nodes $i \in \mathcal{N}$ and all corresponding phases $\psi \in \Psi_i$. Similarly, for each of the aforementioned variables, we also apply the following lower bounds

$$\delta^+_{i,\psi} \geq -M\left(1 - \phi^+_{i,\psi}\right) + \left(v_{i,\psi} - v^{\max}_{i,\psi}\right), \tag{9a}$$

$$\delta^+_{i,\psi} \geq -M\phi^+_{i,\psi}, \tag{9b}$$

$$\delta^-_{i,\psi} \geq -M\left(1 - \phi^-_{i}\right) + \left(v^{\min}_{i,\psi} - v_{i,\psi}\right), \tag{9c}$$

$$\delta^-_{i,\psi} \geq -M\phi^-_{i,\psi}, \tag{9d}$$

for all nodes $i \in \mathcal{N}$ and all corresponding phases $\psi \in \Psi_i$. Lastly, each of the indicator variables $\phi^+_{i,\psi}$ and $\phi^-_{i,\psi}$ must satisfy

$$\phi^+_{i,\psi} + \phi^-_{i,\psi} \leq 1, \qquad \phi^+_{i,\psi},\, \phi^-_{i,\psi} \in \{0,1\} \tag{10}$$

for all nodes $i \in \mathcal{N}$ and all corresponding phases $\psi \in \Psi_i$. When the constraints (7), (8), (9), and (10) are jointly satisfied, we achieve the piecewise linear voltage violation function depicted in Fig. 2.

We consider two separate attack cases. In the under-voltage case, the attacker maximizes violations of the lower voltage bound, so the objective is built from the under-voltage terms $\delta^-_{i,\psi}$. In the over-voltage case, the attacker maximizes violations of the upper voltage bound, so the objective is built from the over-voltage terms $\delta^+_{i,\psi}$. The three objectives introduced in (11) are applied separately within each of these two cases.

Using the violation variables defined in (5), we define the three attack objectives as

$$\|\boldsymbol{\delta}\|_0 \;:=\; \sum_{(i,\psi)} \phi_{i,\psi}, \tag{11a}$$

$$\|\boldsymbol{\delta}\|_1 \;:=\; \sum_{(i,\psi)} \left(\delta^+_{i,\psi} + \delta^-_{i,\psi}\right), \tag{11b}$$

$$\|\boldsymbol{\delta}\|_\infty \;:=\; \max_{(i,\psi)} \left(\delta^+_{i,\psi} + \delta^-_{i,\psi}\right), \tag{11c}$$

respectively.

The voltage violations $\boldsymbol{\delta}$ are a direct consequence of the attacker's power setpoint decisions, as the resulting power flows determine the bus voltages via Section 2.3.

Assumption 1 *The attack model is formulated as a single-period deterministic snapshot. Load and solar PV operating conditions are treated as fixed, and non-compromised solar PVs are assumed to remain at their nominal setpoints during the attack. Consequently, the formulation does not capture uncertainty, time-varying behavior, or corrective responses from non-compromised solar PVs or system operators.*

Under Assumption 1,[1] we evaluate the voltage impact of a coordinated solar PV attack at a fixed operating point. For each objective, the attack optimization problem is formulated as

$$\begin{aligned} &\text{maximize} && \|\boldsymbol{\delta}\|_k \\ &\text{subject to:} && (2), (3), \\ &&& (7), (8), (9), (10), \end{aligned} \tag{12}$$

[1] As discussed in Section 5, our ongoing work includes extending the formulation to generalize beyond these assumptions.

for $k \in \{0, 1, \infty\}$.

After solving (12) for a given attack budget and objective, the optimization identifies the compromised solar PVs and the associated malicious real- and reactive-power setpoints. These attacked setpoints are then used to compute the resulting voltage profile and the corresponding violation metrics through the ℓ_0, ℓ_1, and ℓ_∞ norms of the voltage violation vector. Because the attack optimization is performed using the LinDist3Flow approximation, the resulting operating point is subsequently validated using a nonlinear AC power flow (ACPF) model with the same attacked solar PV setpoints. The comparison between the LinDist3Flow and ACPF results provides a consistency check on both the predicted voltage magnitudes and the identified violation locations.

4. Numerical Results

In this section, we first describe the modified test feeders and the numerical implementation used in our study. We then present the attack results across the three systems under different budgets and for both the under-voltage and over-voltage cases.

4.1. Test Systems

We evaluate the performance of the proposed attack algorithm using modified versions of the standard IEEE `13-bus`, `34-bus`, and `123-bus` distribution test feeders [34]. In our implementation, all delta-connected loads in the original feeder data are converted to equivalent grounded-wye loads before the LinDist3Flow analysis. Additionally, since the original test cases lack DERs, we augment each system by placing PV generators at load buses. For a given penetration level, the rated active power of each PV generator is set proportional to the local real-power demand. This placement strategy gives 14 PV units totaling 2,650 kW, with individual ratings between 100 kW and 300 kW, on the `13-bus` feeder, 34 solar PV units totaling 1,769 kW on the `34-bus` feeder, and 50 solar PV units totaling 1,885 kW on the `123-bus` feeder.

4.2. Implementation Details

We implement the voltage violation optimization problems in the Julia programming language using the JuMP package [35]. The three-phase LinDist3Flow network model is formulated using the `PowerModelsDistribution.jl` package [36], and the resulting mixed-integer problems are solved with the `Gurobi Optimizer` [37]. Internally, `PowerModelsDistribution` introduces auxiliary

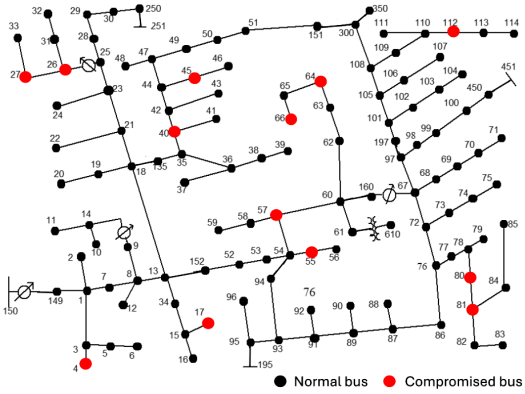


Figure 3. Modified IEEE 123-bus distribution feeder showing the compromised buses selected by the budget constrained attack under the ℓ_0-objective. Red and black markers denote compromised and uncompromised buses, respectively.

buses, such as `xfm1`, `reg1`, and distinct substation transformer buses, to represent transformers and voltage regulators. Since these auxiliary nodes do not correspond to physical feeder buses, we exclude them from the analysis. Accordingly, voltage violations are evaluated only at the physical feeder buses of each network. Gurobi solved the under-voltage attack problem ($B = 30$) for the IEEE `123-bus` feeder in 10.86 seconds. This shows that our LinDist3Flow MILP formulation scales well and remains computationally efficient in our experiments.

4.3. Voltage Violations

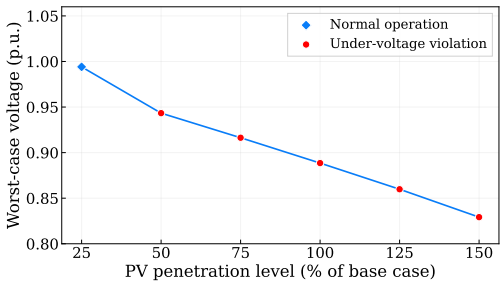
We apply the voltage violation formulation in Section 3 to all three test feeders under both under-voltage and over-voltage attack scenarios. By varying the attack budget, we evaluate how the voltage profile changes and how the number of violated buses and phases varies as the attacker's budget increases. Each PV is assigned a distinct compromise cost according to the formulation in Section 2.1.

For the IEEE `13-bus` feeder, Fig. 4 shows the impact of increasing PV penetration on under-voltage behavior. As shown in Fig. 4(a), the worst-case bus voltage decreases steadily with the PV penetration level, falling from approximately 1.00 p.u. at 25 % penetration to about 0.83 p.u. at 150 %. The voltage drops below the 0.95 p.u. threshold at 50 % penetration.

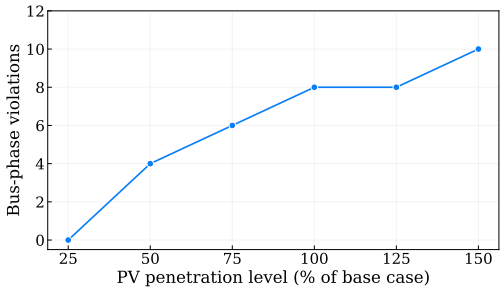
Fig. 4(b) shows that the number of violated bus-phases also increases with penetration level, rising from zero at 25 % penetration to 10 at 150 %.

These results show that higher PV penetration makes

the feeder more vulnerable to coordinated manipulation, since the most severe voltage drop becomes progressively worse and the resulting under-voltage violations spread across a larger portion of the feeder.



(a) Worst-case bus voltage.



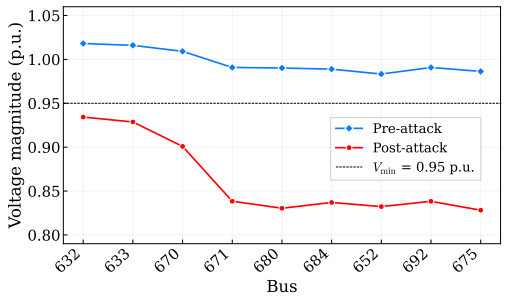
(b) Number of bus-phase violations.

Figure 4. Effect of PV penetration on the under-voltage case in the IEEE 13-bus feeder under an attack budget of $B = 4$.

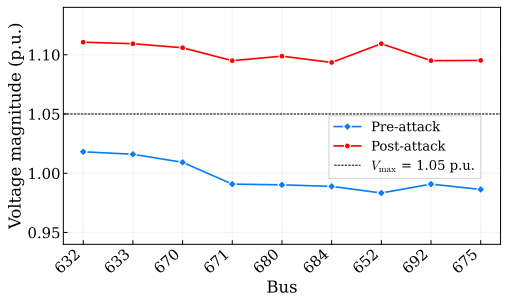
Fig. 5 compares the pre-attack and post-attack voltage profiles across the IEEE `13-bus` feeder for both attack objectives. In the under-voltage case shown in Fig. 5(a), the pre-attack voltages remain above 0.95 p.u. at all buses. After the attack, the voltage profile shifts downward across much of the feeder, with the largest drops occurring at buses 680, 652, and 675. These buses are located downstream of bus 671, farther from the substation along the feeder segment between buses 632 and 671. Once the attacker manipulates the selected PV setpoints, the cumulative voltage drop becomes most severe at these downstream locations.

In the over-voltage case shown in Fig. 5(b), the pre-attack voltages stay below 1.05 p.u. across the feeder. After the attack, bus voltages increase across nearly the entire feeder, and several buses exceed the upper limit. The highest post-attack voltages occur at bus 652, which again lies far downstream.

In both attack cases, coordinated manipulation of solar PV setpoints can push otherwise acceptable operating points into either under-voltage or over-voltage conditions, with the largest deviations concentrated at downstream buses that are farther from the substation and more sensitive to upstream setpoint changes.



(a) Under-voltage case.



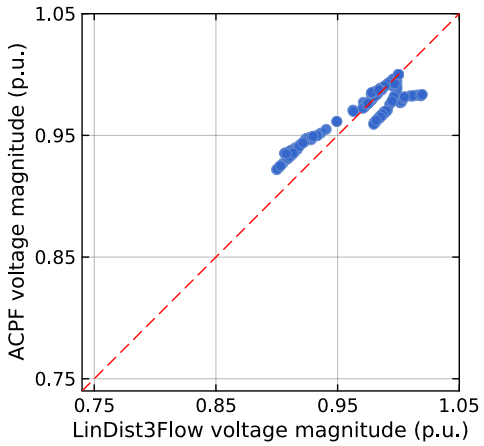
(b) Over-voltage case.

Figure 5. Pre-attack and post-attack voltage profiles for the IEEE 13-bus feeder under an attack budget of $B = 8$.

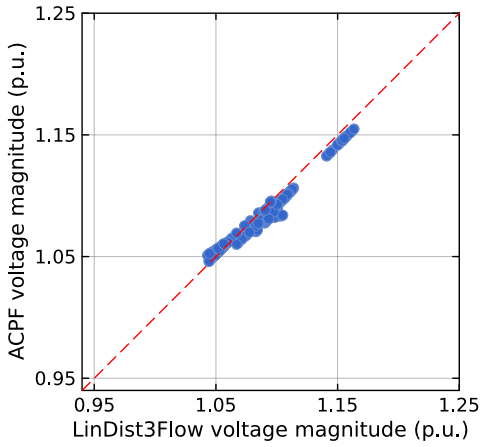
Fig. 6a compares the LinDist3Flow and ACPF voltage magnitudes for the under-voltage case in the IEEE 123-bus feeder. Most points remain close to the line of perfect agreement, which indicates that the linearization error introduced by LinDist3Flow is small in this case. The points stay tightly clustered around the diagonal over nearly the full voltage range, and the linear approximation tracks both the severity and the spread of the voltage drop with only small deviations from the ACPF solution.

Fig. 6b shows the corresponding comparison for the over-voltage case. Here again, most points lie near the diagonal, indicating that LinDist3Flow captures the main voltage-rise behavior with relatively small linearization error. The voltage increase pattern is reproduced well across most buses and phases, although small deviations remain at higher voltage magnitudes.

Across both cases, this close agreement suggests that the attack solution we obtained from the linearized optimization problem in (12) is consistent with the ACPF validation. This provides a degree of empirical evidence that the solar PV compromise decisions, represented by the binary variables in (2), are likely to be close to those that would be obtained from the corresponding mixed-integer nonlinear formulation based on the AC power



(a) Under-voltage case.



(b) Over-voltage case.

Figure 6. Parity plots comparing LinDist3Flow and ACPF voltage magnitudes for the IEEE 123-bus feeder for under-voltage and over-voltage attack cases.

flow equations.

Tables 1 and 2 show the attack outcomes for the three IEEE test feeders in the under-voltage and over-voltage cases, respectively. For each feeder, the results are shown at multiple budget levels and separated by adversarial objective.

A clear pattern across all three feeders is that a larger attack budget allows the attacker to cause more severe violations, although the added damage becomes smaller at the higher budget levels. Under the ℓ_1-objective, for example, the total under-voltage violation in the IEEE 13-bus feeder increases from 0.957 p.u. at $B = 4$ to 1.666 p.u. at $B = 12$. The over-voltage case shows the same behavior, with the ℓ_1-value increasing from 1.551 p.u. to 2.011 p.u. over the same budget range. The IEEE 34-bus and IEEE 123-bus feeders follow the same pattern, but on a larger scale.

The ℓ_0-objective shows that widespread disruption is possible even at the lower budget levels. In the IEEE 13-bus feeder, for example, 10 out of 14 buses are violated at $B = 4$ in the under-voltage case, while 13 out of 14 buses are violated at the same budget in the over-voltage case. This indicates that the attacker does not need a larger budget to affect a substantial portion of the feeder.

Table 1. Under-Voltage Violation Attack Outcomes by Adversarial Objective

Feeder	Budget (B)	ℓ_∞-Norm Worst-Case (p.u.)	ℓ_1-Norm Total Viol. (p.u.)	Spatial Extent (ℓ_0)	
				Viol. Buses (Count)	Viol. Phases (Count)
IEEE 13	4	0.137	0.957	10/14	11/35
	12	0.206	1.666	11/14	11/35
IEEE 34	18	0.136	7.194	46/53	106/129
	28	0.152	7.908	44/53	101/129
IEEE 123	30	0.069	4.543	91/128	91/268
	50	0.071	4.545	91/128	91/268

Table 2. Over-Voltage Violation Attack Outcomes by Adversarial Objective

Feeder	Budget (B)	ℓ_∞-Norm Worst-Case (p.u.)	ℓ_1-Norm Total Viol. (p.u.)	Spatial Extent (ℓ_0)	
				Viol. Buses (Count)	Viol. Phases (Count)
IEEE 13	4	0.072	1.551	13/14	32/35
	12	0.113	2.011	12/14	23/35
IEEE 34	18	0.293	12.829	45/53	84/129
	28	0.293	12.845	45/53	84/129
IEEE 123	30	0.113	11.646	126/128	247/268
	50	0.114	11.647	126/128	247/268

5. Conclusion

The increasing penetration of distributed energy resources (DERs) introduces new cyber-physical risks in distribution networks. In particular, an attacker who compromises inverter-interfaced PV systems may manipulate both active and reactive power setpoints, enabling coordinated actions that can stress grid assets and violate operational limits. In this paper, we consider a DER-rich feeder under an adversarial model in which compromised

PV inverters are controllable within their operating capabilities. To capture heterogeneous attacker effort, we assign each PV a *cost of compromise* that quantifies the resources required to gain control, and evaluate the resulting voltage violations under constrained attacker budgets.

Our results show that budget constrained attacks on compromised solar PVs can produce severe and widespread voltage violations across the feeder. As the attack budget increases, the overall severity of the violations also increases, although the rate of increase slows at higher budget levels. The comparison between LinDist3Flow and ACPF further shows that the linearized model captures the main voltage behavior under attack with reasonable accuracy. While formulated from an adversarial standpoint, our analysis provides useful insights for designing proactive defense mechanisms and mitigation protocols. Our findings further highlight the importance of improving situational awareness and grid resilience in systems with high DER penetration.

Our future work will extend the framework in two directions. First, we will incorporate stochastic models for distributed generation and demand to study how variations in solar output and load affect coordinated DER attacks. Second, we will model the distribution system operator's response to examine how operator actions can limit voltage violations during an attack.

Appendix

We used the Censys Internet-wide scanning platform to identify devices relevant to our threat model. As detailed in our companion measurement study [30], this approach discovered over 66,000 Internet-exposed solar DER hosts worldwide. Figure 7–8 provides a representative screenshot that illustrates the kind of exposed interface observed in the wild and the capabilities attackers gain when such interfaces are reachable over the public Internet. This example is not exhaustive, but it underscores how even routine maintenance or monitoring portals, when misconfigured, can act as direct cyber-physical entry points into distributed energy systems. Many of these exposed endpoints, associated with solar inverters, energy meters, and gateway controllers, offered configuration, firmware, or data access without authentication. By examining this real-world example, we demonstrate the feasibility of adversarial actions such as remote firmware manipulation, password resets, and data tampering, which form the basis for the attack vectors outlined in Section 2.1.

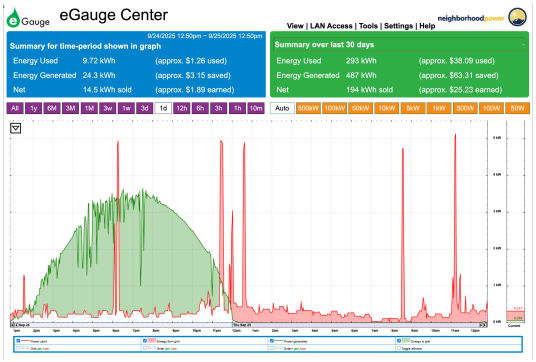


Figure 7. Exposed eGauge metering center reachable over the public Internet without authentication. The interface exposes `Tools` and `Settings` tabs that permit remote firmware upload and credential changes, giving an attacker write-level configuration control.

Figure 8. "Firmware Upgrade" tab under the "Tools" tab in the public eGauge interface. This tab exposes remote firmware update functionality; without authentication, such functionality can enable an attacker to install arbitrary firmware or malicious code.

References

[1] U.S. Department of Energy, CESER & EERE, "DOE cybersecurity report provides recommendations to secure distributed clean energy on the nation's electricity grid," https://www.energy.gov/ceser/articles/doe-cybersecurity-report-provides-recommendations-secure-distributed-clean-energy, 2022, accessed: 2025-10-15.

[2] DER Security Corp, "Solar energy under attack," https://dersec.io/solar-energy-under-attack/, 2025, accessed: 2025-10-15.

[3] Forescout Research – Vedere Labs, "The security risks of Internet-exposed solar power systems," https://www.forescout.com/blog/the-security-risks-of-internet-exposed-solar-power-systems/, 2025, accessed: 2025-10-15.

[4] C. Masters, "Voltage rise: The big issue when connecting embedded generation to long 11 kV overhead lines," *Power Engineering Journal*, vol. 16, no. 1, pp. 5–12, 2002.

[5] R. A. Shayani and M. A. G. de Oliveira, "Photovoltaic generation penetration limits in radial distribution systems," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1625–1631, 2010.

[6] M. Rylander, J. Smith, D. Lewis, and S. Steffel, "Voltage impacts from distributed photovoltaics on two distribution feeders," in *IEEE Power & Energy Society General Meeting (PESGM)*, 2013.

[7] D. Shelar and S. Amin, "Security assessment of electricity distribution networks under DER node compromises," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 23–36, 2016.

[8] A. M. Nour, A. Y. Hatata, A. A. Helal, and M. M. El-Saadawi, "Review on voltage-violation mitigation techniques of distribution networks with distributed rooftop PV systems," *IET Generation, Transmission & Distribution*, vol. 14, no. 3, pp. 349–361, 2020.

[9] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2364–2383, 2022.

[10] M. Lundberg, O. Samuelsson, and E. Hillberg, "Local voltage control in distribution networks using PI control of active and reactive power," *Electric Power Systems Research*, vol. 212, p. 108475, 2022.

[11] K. R. Babu and D. K. Khatod, "Smart inverter-based distributed volt/var control for voltage violation mitigation of unbalanced distribution networks," *IEEE Transactions on Power Delivery*, vol. 39, no. 3, pp. 1481–1490, 2024.

[12] Y. T. Tan and D. S. Kirschen, "Impact on the power system of a large penetration of photovoltaic generation," in *IEEE Power Engineering Society General Meeting (PESGM)*, 2007.

[13] Y. Hanai, Y. Hayashi, J. Matsuki *et al.*, "Voltage control for a loop distribution system with renewable energy sources," in *International Conference on Renewable Energies and Power Quality (ICREPQ)*, 2010.

[14] M. E. Elkhatib, R. El-Shatshat, and M. M. Salama, "Novel coordinated voltage control for smart distribution networks with DG," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 598–605, 2011.

[15] H. E. Farag, E. F. El-Saadany, and R. Seethapathy, "A two-way communication-based distributed control for voltage regulation in smart distribution feeders," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 271–281, 2011.

[16] M. A. Mahmud, M. Hossain, and H. R. Pota, "Analysis of voltage rise effect on distribution network with distributed generation," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 14 796–14 801, 2011.

[17] X. Liu, A. Aichhorn, L. Liu, and H. Li, "Coordinated control of distributed energy storage system with tap changer transformers for voltage rise mitigation under high photovoltaic penetration," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 897–906, 2012.

[18] R. Tonkoski, D. Turcotte, and T. H. El-Fouly, "Impact of high PV penetration on voltage profiles in residential neighborhoods," *IEEE Transactions on Sustainable Energy*, vol. 3, no. 3, pp. 518–527, 2012.

[19] A. P. Kenneth and K. Folly, "Voltage rise issue with high penetration of grid-connected PV," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 4959–4966, 2014.

[20] T. Aziz and N. Ketjoy, "PV penetration limits in low voltage networks and voltage variations," *IEEE Access*, vol. 5, pp. 16 784–16 792, 2017.

[21] X. Hu, Z.-W. Liu, G. Wen, X. Yu, and C. Liu, "Voltage control for distribution networks via coordinated regulation of active and reactive power of DGs," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4017–4031, 2020.

[22] K. A. Makinde, D. O. Akinyele, and A. O. Amole, "Voltage rise problem in distribution networks with distributed generation: A review of technologies, impact and mitigation approaches," *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 9, no. 3, pp. 575–600, 2021.

[23] Y. Li, Y. Sun, K. Li, J. Zhuang, Y. Liang, and Y. Pang, "Analysis and suppression of voltage violation and fluctuation with distributed photovoltaic integration," *Symmetry*, vol. 13, no. 10, p. 1894, 2021.

[24] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, 2015.

[25] N. G. A. Aysheh, T. Khattab, and A. Massoud, "Cyber-attacks against voltage profile in smart distribution grids with highly-dispersed PV generators: Detection and Protection," in *IEEE Electric Power and Energy Conference (EPEC)*, 2020.

[26] A. Farooq, K. Shahid, Y. Gui, and R. L. Olsen, "Impact of cyber-attack on coordinated voltage control in low voltage grids," *IET Renewable Power Generation*, vol. 17, no. 11, pp. 2887–2894, 2023.

[27] E. Naderi and A. Asrari, "Mitigating voltage violations in smart city microgrids under coordinated false data injection cyberattacks: Simulation and experimental insights," *Smart Cities*, vol. 8, no. 1, p. 20, 2025.

[28] R. Pickren, A. Chhotaray, F. Li, S. Zonouz, and R. Beyah, "Release the hounds! Automated inference and empirical security evaluation of field-deployed PLCs using active network data," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2024.

[29] J. Johnson, "Public history of solar energy cyberattacks and vulnerabilities," https://dersec.io/reports/DERSec-Solar-Vulnerability-Summary-v2.0-Final.pdf, 2024.

[30] Anonymized authors for the sake of double-blind review, "Grid trouble in paradise: Uncovering vulnerable distributed energy resources and their grid-level risks," *under review*, 2026.

[31] L. Gan and S. H. Low, "Convex relaxations and linear approximation for optimal power flow in multiphase radial networks," in *18th Power Systems Computation Conference (PSCC)*, 2014.

[32] A. Dubey, S. Paudyal *et al.*, "Distribution system optimization to manage distributed energy resources (DERs) for grid services," *Foundations and Trends in Electric Energy Systems*, vol. 6, no. 3-4, pp. 120–264, 2023.

[33] D. B. Arnold, M. Sankur, R. Dobbe, K. Brady, D. S. Callaway, and A. Von Meier, "Optimal dispatch of reactive power for voltage regulation and balancing in unbalanced distribution systems," in *IEEE Power & Energy Society General Meeting (PESGM)*, 2016.

[34] W. H. Kersting, "Radial distribution test feeders," *IEEE Transactions on Power Systems*, vol. 6, no. 3, pp. 975–985, 1991.

[35] I. Dunning, J. Huchette, and M. Lubin, "JuMP: A modeling language for mathematical optimization," *SIAM Review*, vol. 59, no. 2, pp. 295–320, 2017.

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

[37] Gurobi Optimization, LLC, *Gurobi Optimizer Reference Manual*, 2023, https://www.gurobi.com.