Received: 28 November 2023 | Revised: 29 May 2024 | Accepted: 26 June 2024

IET Generation, Transmission & Distribution

DOI: 10.1049/gtd2.13217

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

CFDI: Coordinated false data injection attack in active distribution network

Yang Liu[1] | Chenyang Yang[2] | Nanpeng Yu[3] | Jiazhou Wang[1] | Jue Tian[4] | Hao Huang[5] | Yadong Zhou[2] | Ting Liu[1]

[1]School of Cyber Science and Engineering, MoE KLINNS Lab, Xi'an Jiaotong University, Xi'an, China

[2]School of Automation Science and Engineering, MoE KLINNS Lab, Xi'an Jiaotong University, Xi'an, China

[3]Department of Electrical and Computer Engineering, University of California at Riverside, Riverside, California, USA

[4]School of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an, China

[5]Electric Power Dispatch and Control Center of Guangdong Power Grid Co., Ltd., Guangzhou, China

Correspondence
Yadong Zhou, School of Automation Science and Engineering, MoE KLINNS Lab, Xi'an Jiaotong University, Xi'an 710049, China.
Email: ydzhou@xjtu.edu.cn

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 62293501, 62293502; Key Research and Development Program of Shaanxi, Grant/Award Number: 2024GX-ZDCYL-02-19; Science and Technology Project of China Southern Power Grid Corporation, Grant/Award Numbers: 030000KC23040079, GDKJXM20230394; China Postdoctoral Science Foundation, Grant/Award Number: 2020M683520; Fundamental Research Funds for the Central Universities

Abstract

The active distribution network (ADN) can obtain measurement data, estimate system states, and control distributed energy resources (DERs) and flexible loads to ensure voltage stability. However, the ADN is more vulnerable to cyber attacks due to the recent wave of digitization and automation efforts. In this article, false data injection (FDI) attacks are focused on and they are classified into two types, that is, type I attacks on measurement data and type II attacks on control commands. After studying the impact of these two FDI attacks on the ADN, a new threat is revealed called coordinated FDI attack, which can maximize the voltage deviation by coordinating type I and type II FDI attacks. From the attacker's perspective, the scheme of CFDI is proposed and an algorithm is developed to find the optimal attack strategy. The feasibility of CFDI attacks has been validated on a smart distribution testbed. Moreover, simulation results on an ADN benchmark have demonstrated that CFDI attacks could cause remarkable voltage deviation that may deteriorate the stability of the distribution network. Moreover, the impact of CFDI attacks is higher than pure type I or type II attacks. To mitigate the threat, some countermeasures against CFDI attacks are also proposed.

1 | INTRODUCTION

It is a global trend to facilitate the low-carbon transformation of energy structures by introducing large quantities of distributed energy resources (DERs) and flexible loads into smart grids [1]. With a high penetration rate of DERs and flexible loads, the distribution network is facing great security threats. For example, the uncertainty in photovoltaic and wind power generation has a great impact on the supply-demand balance of the power system [2], while uncoordinated plug-in electric vehicles (EVs) on a residential distribution grid can cause problems including power losses and voltage deviations [3]. To increase the distribution network's reliability and robustness, the active distribution network (ADN) is being developed rapidly, which can obtain measurement data, estimate system states, and make decisions to control DERs and flexible loads automatically via the supervisory control and data acquisition (SCADA) system [4, 5].

Yang Liu and Chenyang Yang contributed equally to this work.

Voltage stability is one of the most important security indicators for distribution networks. If the voltage exceeds the allowed deviation range, it can cause some electrical appliances to malfunction, decrease the torque and speed of electric motors, and affect the efficiency and quality of manufacturing activities [6]. In severe cases, it can cause generator failure or even voltage collapse [7]. To guarantee the voltage stability, researchers have revealed the principles of voltage regulation and proposed some voltage regulation methods using DERs and flexible loads [8–10]. Specifically, voltage regulation methods that utilize optimization algorithms for coordinated control of multiple DERs have emerged [11, 12], whose optimization objectives include optimal power flow, optimal power quality, and minimum power losses [13–15]. EV charging schedules are optimally coordinated to support voltage and energy regulation [10].

The deep coupling of cyber networks and power grids has expanded the attack surface, thus aggravating the threats of cyber-physical attacks. Specifically, attackers can launch false data injection (FDI) attacks from the cyber network, inject false commands or measurements to disturb the system operation, leading the power grid to an unstable operation state [16–19]. For instance, dynamic load altering attacks are introduced against smart grid demand response programs, which can make power system's frequency unstable [20]. A cyber-physical coordinated attack against protection relays is studied in [21], which can cause cascading failures via cyber-attacks on protection relays followed by physical attacks on the transmission line. Although FDI attacks have been well studied, most researchers focus on the security of the transmission network, while few researchers have considered the threat of FDI attacks in ADN. Moreover, the threat of compromising flexible loads and DERs on a large scale in ADN has not been thoroughly studied.

In this paper, we explore the impact of coordinated FDI (CFDI) attacks on the voltage security of ADNs, where voltage deviation is caused by both false measurements impacting DERs (i.e. type I FDI attack) and false commands on flexible loads like EVs (i.e. type II FDI attack). We present a method that can indirectly manipulate the reactive power output of DERs by injecting false measurement data into the SCADA system, thus misleading its control decision. Furthermore, we develop an iterative optimization algorithm to find the optimal CFDI attack strategy. Based on the voltage regulation timeline in ADNs, we propose an attack scheme that changes the active power of flexible loads and the reactive power of DERs synergistically. Results from simulation experiments demonstrate that, with limited attack resources, CFDI attacks could lead to larger voltage deviations when compared to pure type I or type II FDI attacks. We also propose some defense strategies against such attacks. Our main contributions are summarized as follows:

- We revealed the threat of CFDI, where attackers can leverage flexible loads and DERs via the optimal collaborative attack strategy, thus causing distinct voltage deviations by manipulating the active and reactive power in ADNs, respectively.
- We introduced an indirect control method where attackers can manipulate the reactive power output of DERs by influencing the SCADA system's state estimation and control decisions through FDI attacks on measurements.
- We have demonstrated the possibility of CFDI on a real smart distribution testbed, where FDI attacks could be launched to inject false commands and measurements.
- We validated the feasibility of CFDI through extensive simulation experiments and demonstrated its advantages compared to single-sided attacks. Moreover, several defense strategies are proposed based on the analysis of experimental results.

The remainder of this paper is organized as follows. Section 2 reviews relevant works in this field. Section 3 presents the algorithms for CFDI attacks. Section 4 validates the feasibility of CFDI attacks on the smart distribution testbed. Section 5 validates the proposed attack through simulation experiments and analyzes the influencing factors. Section 6 provides some defense strategies, and Section 7 concludes the paper.

2 | RELATED WORK

This section summarizes related works in the fields of ADN and FDI attacks based on the principles and methods of the proposed attacks.

In recent years, there has been a growing emphasis on the physical stability as well as network and data security of ADNs. ADNs have great potential in coordinating high penetration of renewable energy and improving the reliability of power supply. Compared to traditional distribution networks, ADNs have enhanced two-way communication and active control capabilities. SCADA system is one of the important technologies to achieve these functions, which performs optimization based on measurement data. Researchers have proposed many optimization models that leverage SCADA systems such as optimal power flow [14], optimal voltage regulation [15], and power losses minimization. Among them, the optimization of voltage quality has received widespread attention. In addition to traditional on-load tap changers (OLTCs) and reactive power compensators (RPCs), voltage regulation in ADNs can also be achieved by controlling the reactive power output of DERs. The linear relationship between DERs and distribution network voltages was explored and the voltage regulation calculation was simplified in [8, 9]. An intelligent method for voltage control in distribution networks using distributed generators was proposed in [22]. Multiple distributed generators were coordinated with conventional voltage control devices in a centralized system in [11] to optimize line losses while regulating voltage. The voltage control problem was decomposed into several local sub-problems using graph partitioning and ε-decoupling in [12, 23], reducing the dimensionality and system communication cost of the optimization problem. Taking into account the radial topology characteristics of distribution networks, the distributed generator management system was integrated

into the decentralized Volt/Var management system, and the distribution network was divided into regions with separate voltage regulation and reactive power support schemes in [24]. However, the SCADA system is vulnerable to malicious attacks in obtaining measurement data, performing state estimation, and achieving optimal control. Also, these voltage regulation methods are dispersed throughout the distribution network, allowing attackers to exploit the same principle to manipulate energy output and achieve reverse voltage regulation remotely. Obviously, these capabilities of ADN introduce new threat scenarios for security.

FDI attacks directly undermine the perception and control capability of SCADA systems, thereby affecting other functionalities. The FDI attack was first proposed in [25], allowing the constructed attack vector to bypass residue-based bad data detection of state estimation. The topology FDI attack was demonstrated in [26], which could cause misjudgment of the system topology. To make FDI attacks more realistic, some researchers modeled them as optimization problems that consider limited resources and covert attacks [27–30], and used solvers or heuristic algorithms to construct optimal attack vectors. Furthermore, researchers are also working on reducing the difficulty of designing FDI attacks and reducing reliance on complete power grid parameters. An FDI model that only requires the admittance of all lines connected to the target bus was presented in [31], and was further simplified to only require admittance in [32]. Using principal component analysis and geometric methods, the FDI attack that does not rely on network information was proposed in [33]. However, due to the DC approximation, it is unsuitable for launching attacks with large deviations. An approach that relies only on a few phase measurement units was introduced in [34], which enables FDI attacks against AC state estimation. FDI attacks that can bypass the distribution system state estimation (DSSE) program were discussed in [32, 35, 36], where attackers have to simultaneously compromise multiple measurements to remain undetectable [37]. However, these studies focus solely on the cyber network when analyzing the threats posed by FDI attacks. Also, they overlook the potential effects on the physical network and do not consider the possible impact of inaccurate decision-making by SCADA systems on ADN.

Overall, while the aforementioned studies have elaborated on the threats of FDI attacks to both the cyber and physical layers of ADNs, they have not revealed how threats on the cyber layer can affect the physical layer. To fill this knowledge gap, we have developed a CFDI attack strategy based on voltage regulation principles and, for the first time, proposed a method to indirectly manipulate the control command through FDI on measurements. This CFDI attack leverages the resources from both cyber and physical networks by launching two types of FDI attacks, and finally accumulates voltage deviations on a specific bus. Note that if the over-voltage and under-voltage relays have been deployed, they may cause load shedding and partial outage, which could be regarded as a subsequent result of a successful CFDI attack.

ALGORITHM 1 False measurement data injection in Type I FDI attacks.

Input: initial system state $\boldsymbol{x}_0$, control target $\boldsymbol{u}_{att}^{\mathrm{I}}$, threshold $\varepsilon_{\boldsymbol{u}}$

Output: $\boldsymbol{z}_{att}$

$\boldsymbol{u}_0 \leftarrow \boldsymbol{0}$, $\boldsymbol{x}_{att} \leftarrow \boldsymbol{0}$, $\boldsymbol{z}_0 \leftarrow \boldsymbol{j}^{-1}(\boldsymbol{x}_0)$
for $i = 1 : m_{iter}$ **do**
  $\boldsymbol{x}_i' \leftarrow \boldsymbol{j}^{-1}(\boldsymbol{z}_{i-1} + (\boldsymbol{u}_{att}^{\mathrm{I}} - \boldsymbol{u}_{i-1}))$
  $\boldsymbol{x}_i \leftarrow \boldsymbol{x}_{i-1} + \boldsymbol{x}_{i-1} - \boldsymbol{x}_i'$
  $\boldsymbol{u}_i \leftarrow \boldsymbol{h}(\boldsymbol{x}_i)$
  if $\|\boldsymbol{u}_{att}^{\mathrm{I}} - \boldsymbol{u}_i\| < \varepsilon_{\boldsymbol{u}}$ **then**
    $\boldsymbol{x}_{att} \leftarrow \boldsymbol{x}_i$
    break
  end if
  $\boldsymbol{z}_i \leftarrow \boldsymbol{j}(\boldsymbol{x}_i)$
end for
if $\boldsymbol{x}_{att} == \boldsymbol{0}$ **then**
  return NULL
end if
$\boldsymbol{z}_{att} \leftarrow \boldsymbol{j}(\boldsymbol{x}_{att})$
return $\boldsymbol{z}_{att}$

3 | COORDINATED FALSE DATA INJECTION ATTACK

In this section, we propose CFDI to cause voltage fluctuations by leveraging the variation of active and reactive power in ADN. First, we introduce the voltage regulation process and how to affect voltage by changing power. Second, we introduce the type I FDI attack (FDI Attack on Measurement data), and design Algorithm 1 to determine the target measurement data injection based on the desired change on reactive power. Third, we introduce the type II FDI attack (FDI Attack on Control Command) and illustrate how to conduct it for desired change on active power. Then, we propose CFDI and design Algorithm 2 to coordinate two types of attacks. Finally, we analyze the timeline of the CFDI attack during the periodic active voltage control process.

3.1 | Preliminaries

The process of voltage regulation by the SCADA system can be divided into two steps: i) state estimation based on measurement data, and ii) executing a voltage regulation algorithm based on the state to adjust the reactive power output of DERs.

In this article, we propose CFDI to cause distinct voltage deviations by manipulating the active and reactive power injection of the system. The relationship between these physical quantities can be described by the power flow equation in the form of polar coordinates as:

$$P_i = V_i \sum_{j \in \mathcal{A}(i)} V_j (G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij}), \tag{1}$$

ALGORITHM 2 Optimal CFDI attack strategy.

Input: system state $\boldsymbol{x}$, measurement data $\boldsymbol{z}$, target node i, voltage deviation target $\Delta \boldsymbol{V}_{target}$, threshold ε_V

Output: Attack strategy $\boldsymbol{u}_{att}$

$\Delta \boldsymbol{P}_{att} \leftarrow \boldsymbol{0}, \Delta \boldsymbol{Q}_{att} \leftarrow \boldsymbol{0}$
for $i = 1 : m_{iter}$ **do**
  $[\Delta \boldsymbol{P}, \Delta \boldsymbol{Q}] \leftarrow$ solve (14)
  if unsolvable **then**
    return NULL
  end if
  $\Delta \boldsymbol{P}_{att} \leftarrow \Delta \boldsymbol{P}_{att} + \Delta \boldsymbol{P}, \quad \Delta \boldsymbol{Q}_{att} \leftarrow \Delta \boldsymbol{Q}_{att} + \Delta \boldsymbol{Q}, \boldsymbol{z} \leftarrow \boldsymbol{z} + [\Delta \boldsymbol{P}, \Delta \boldsymbol{Q}]$
  $\boldsymbol{x} = [\boldsymbol{V}, \boldsymbol{\theta}] \leftarrow$ state estimation based on $\boldsymbol{z}$
  if $||V_{ref} - V_i| - \Delta V_{target}| < \varepsilon_V$ **then**
    $\boldsymbol{z}_{att} \leftarrow$ Run Algorithm 1 using $\boldsymbol{u}_{att}^{\mathrm{I}} \leftarrow \Delta \boldsymbol{Q}_{att}$
    $\boldsymbol{u}_{att}^{\mathrm{II}} \leftarrow \Delta \boldsymbol{p}_{att}$
    return $\boldsymbol{u}_{att} \leftarrow [\boldsymbol{z}_{att}, \boldsymbol{u}_{att}^{\mathrm{II}}]$
    break
  end if
end for

$$Q_i = V_i \sum_{j \in \mathcal{A}(i)} V_j (G_{ij} \sin \theta_{ij} - B_{ij} \cos \theta_{ij}), \tag{2}$$

where P_i, Q_i represent the active and reactive power injected into bus i, respectively. V_i represents the voltage magnitude of bus i. $\mathcal{A}(i)$ represents the set of adjacent buses of bus i. G_{ij}, B_{ij}, θ_{ij} represent the conductance, susceptance and phase difference between buses i and j, respectively.

Let $\boldsymbol{x} = [\boldsymbol{V}, \boldsymbol{\theta}]$ denotes system state, $\boldsymbol{z} = [\boldsymbol{P}, \boldsymbol{Q}]$ denotes measurement data. $\boldsymbol{z} = \boldsymbol{j}(\boldsymbol{x})$ holds when the measurement error is ignored. $\boldsymbol{j}(\cdot)$ is the power flow equation shown in (1) and (2).

As a high-dimensional non-linear system, the system state $\boldsymbol{x}$ and the power flow on transmission branches cannot be obtained analytically. Therefore, iterative methods are usually used to obtain the numerical solution of the power flow in a certain state. The Newton-Raphson method is one of the most used methods in power flow calculations. During the calculation process, it is iterated by linearizing the relationship between physical quantities. The linearized power flow equation is as follows:

$$\begin{pmatrix} \Delta \boldsymbol{P} \\ \Delta \boldsymbol{Q} \end{pmatrix} = \boldsymbol{J} \begin{pmatrix} \Delta \boldsymbol{\theta} \\ \Delta \boldsymbol{V} \end{pmatrix}, \tag{3}$$

where

$$\boldsymbol{J} = \begin{bmatrix} \dfrac{\partial \boldsymbol{P}}{\partial \boldsymbol{\theta}} & \dfrac{\partial \boldsymbol{P}}{\partial \boldsymbol{V}} \\ \dfrac{\partial \boldsymbol{Q}}{\partial \boldsymbol{\theta}} & \dfrac{\partial \boldsymbol{Q}}{\partial \boldsymbol{V}} \end{bmatrix}. \tag{4}$$

$\boldsymbol{J}$ is the Jacobian matrix, which is calculated by (7) and quantifies the impact of voltage changes on the power injection of the system in a given state. Since the voltage magnitude and voltage angle generally fluctuate within a small range, the relationship between voltage and power can be approximated as linear and its coefficients are the elements in the Jacobian matrix. Correspondingly, the impact of power changes on voltage can be expressed as:

$$\begin{pmatrix} \Delta \boldsymbol{\theta} \\ \Delta \boldsymbol{V} \end{pmatrix} = \wedge \begin{pmatrix} \Delta \boldsymbol{P} \\ \Delta \boldsymbol{Q} \end{pmatrix} = \begin{bmatrix} \wedge_{\theta P} & \wedge_{\theta Q} \\ \wedge_{VP} & \wedge_{VQ} \end{bmatrix} \begin{pmatrix} \Delta \boldsymbol{P} \\ \Delta \boldsymbol{Q} \end{pmatrix}, \tag{5}$$

where $\wedge$ is the sensitivity matrix, that is, the inverse matrix of $\boldsymbol{J}$. $\wedge$ can be split into four sub matrices. Each of them represents the relationship between corresponding physical quantities, for instance, $\wedge_{VP}$ represents the impact of active power changes on voltage magnitude.

3.2 | Type I FDI attack: FDI attack on measurement data

The SCADA system will directly and accurately control some power equipment in ADNs, such as DERs [38] and OLTCs [39]. The reactive power output of DERs is especially actively managed by the SCADA system to participate in voltage regulation. Therefore, we consider using type I FDI attacks to mislead the SCADA system's perception and decision-making through FDI attacks on measurement data, thereby indirectly manipulating the reactive power output of DERs.

In the voltage regulation process, the control command $\boldsymbol{u} = [\Delta \boldsymbol{P}, \Delta \boldsymbol{Q}]$ is determined by $\boldsymbol{x}$ as:

$$\boldsymbol{u} = \boldsymbol{h}(\boldsymbol{x}), \tag{6}$$

where $\boldsymbol{h}$ is the voltage regulation algorithm. After regulation, the measurement data will be shifted to $\boldsymbol{z}_{new} = \boldsymbol{z} + \boldsymbol{u}$. Accordingly, the system state $\boldsymbol{x}$ will reach a new state $\boldsymbol{x}_{new}$ and could be estimated using the least square method as:

$$\boldsymbol{x}_{new} = \boldsymbol{j}^{-1}(\boldsymbol{z} + \boldsymbol{u}). \tag{7}$$

The safe domain of the system state is denoted as $\mathbb{K}_s$, which is the set of all states where the voltage remains within the operation limits. Thus, the control command u is determined to make $\boldsymbol{x}_{new} \in \mathbb{K}_s$. Since the voltage magnitude of the power system is mainly related to reactive power, the indirect manipulation for DERs uses the desired control command $\boldsymbol{u}_{att}^{\mathrm{I}} = \Delta \boldsymbol{Q}_{att}$ as input to obtain the measurement data injection $\boldsymbol{z}_{att}$. From (6) and (7), we can obtain:

$$\boldsymbol{z}_{att} = \boldsymbol{j}(\boldsymbol{x}_{att}) = \boldsymbol{j}\left(\boldsymbol{h}^{-1}\left(\boldsymbol{u}_{att}^{\mathrm{I}}\right)\right), \tag{8}$$

where

$$\boldsymbol{j}^{-1}\left(\boldsymbol{z}_0 + \boldsymbol{u}_{att}^{\mathrm{I}}\right) \notin \mathbb{K}_s, \tag{9}$$

$$\boldsymbol{j}^{-1}\left(\boldsymbol{z}_{att} + \boldsymbol{h}\left(\boldsymbol{j}^{-1}\left(\boldsymbol{z}_{att}\right)\right)\right) \in \mathbb{K}_s, \tag{10}$$

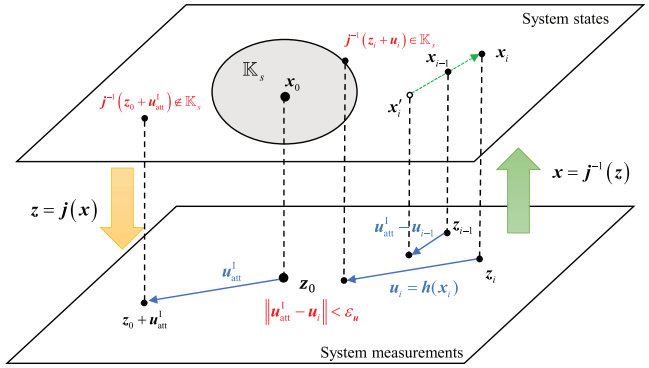


FIGURE 1 The i-th iteration of Algorithm 1. Two blue arrows are control command vectors. Black dashed lines represent the mutual conversion between vector spaces of $\boldsymbol{x}$ and $\boldsymbol{z}$. The green dashed arrow indicates that the points at both ends are symmetrical about the midpoint. The i-th iteration starts from $\boldsymbol{z}_{i-1}$ and reach $\boldsymbol{x}_i'$ along the direction of the arrow according to Line 3 of Algorithm 1. Then, it finds $\boldsymbol{x}_i$ in the direction of the green arrow according to Line 4 of Algorithm 1. According to (9), (10) and (11), $\boldsymbol{z}_i$ can be the final result if $j^{-1}\left(z_0+u_{att}^{I}\right)\notin\mathbb{K}_s$, $j^{-1}\left(z_i+u_i\right)\in\mathbb{K}_s$, and $\|u_{att}^{I}-u_i\|<\varepsilon_u$.

$$\left\|\boldsymbol{u}_{att}^{\mathrm{I}}-\boldsymbol{h}\left(\boldsymbol{j}^{-1}\left(\boldsymbol{z}_{att}\right)\right)\right\|<\varepsilon_{\boldsymbol{u}}. \tag{11}$$

Therefore, after conducting the type I FDI attack by injecting $\boldsymbol{z}_{att}$ according to these formulations, we can ensure that: (a) The real voltage after attack is out of the safe domain according to (9); (b) The voltage regulation algorithm would think it has regulated the voltage back to the safe domain under the misguided system state $\boldsymbol{j}^{-1}(\boldsymbol{z}_{att})$ according to (10); (c) The regulation output $\boldsymbol{h}(\boldsymbol{j}^{-1}(\boldsymbol{z}_{att}))$ is close to the desired control command $\boldsymbol{u}_{att}^{\mathrm{I}}$ according to (11).

However, it is hard to solve (8) directly as the voltage regulation algorithm $\boldsymbol{h}$ is usually an optimization problem and $\boldsymbol{h}^{-1}$ cannot be explicitly expressed in a closed form. To address this issue, we propose Algorithm 1 to determine $\boldsymbol{z}_{att}$ that satisfies (11), whose main idea is illustrated in Figure 1. Specifically, two planes in the figure represent the space of system states and system measurements, respectively. In the (i-1)-th iteration, $\boldsymbol{x}_{i-1}, \boldsymbol{z}_{i-1}, \boldsymbol{u}_{i-1}$ are obtained. If there is still a gap between $\boldsymbol{u}_{i-1}$ and $\boldsymbol{u}_{att}^{\mathrm{I}}$, we perform the i-th iteration beginning from $\boldsymbol{z}_{i-1}$. First, assume that control command $\boldsymbol{u}_{att}^{\mathrm{I}}-\boldsymbol{u}_i$ is exerted on the system and calculate the corresponding state $\boldsymbol{x}_i'$ at Line 3. Then, we find $\boldsymbol{x}_i$ that is the symmetry point of $\boldsymbol{x}_i'$ about $\boldsymbol{x}_{i-1}$ at Line 4. These two steps could make $\boldsymbol{u}_i=\boldsymbol{h}(\boldsymbol{x}_i)$ closer to $\boldsymbol{u}_{att}^{\mathrm{I}}$ than $\boldsymbol{u}_{i-1}$. The iteration is terminated when $\|\boldsymbol{u}_{att}^{\mathrm{I}}-\boldsymbol{u}_i\|<\boldsymbol{\varepsilon}_{\boldsymbol{u}}$ at Lines 6-9. If $\boldsymbol{u}_i$ doesn't converge to $\boldsymbol{u}_{att}^{\mathrm{I}}$ within m_{iter} iterations, then we consider that $\boldsymbol{u}_{att}^{\mathrm{I}}$ can not be reached at Lines 12-14.

3.3 | Type II FDI attack: FDI attack on control command

As the integration of intermittent DERs introduces greater variability and uncertainty, more flexible loads are introduced as demand response (DR) resources [40, 41] and controlled by automatic response technologies like OpenADR [42]. Therefore, attackers could launch type II FDI attacks to change the power output of flexible loads by injecting false control commands.

The most promising flexible loads for demand response regulation include EVs, aggregated thermostatic loads and energy storage etc. [43, 44], which may also be exploited by attackers. The simplest attack is to plug in and out a considerable number of flexible loads like EVs by injecting false control commands simultaneously. This could be easily achieved if the relevant load aggregators or cloud controllers are compromised [45]. Among those flexible loads, EVs are interruptible loads with great threats from cyber attacks on charging piles, charging stations or load aggregators. In addition, as the penetration rate increases gradually, EVs will have a greater impact on the distribution network [3]. Although changes in active power have a smaller impact on voltage magnitude than reactive power, the centralized switching of large-scale controllable loads can still have a considerable shock on voltage magnitude. Thus, we can choose the active power of EVs charging as the attack target. According to (5), the deviation of voltage caused by the change of active power $\boldsymbol{u}_{att}^{\mathrm{II}}=\Delta\boldsymbol{P}_{att}$ is $\wedge_{VP}\cdot\Delta\boldsymbol{P}_{att}$. To cause a non-trivial impact on the voltage magnitude, $\boldsymbol{u}_{att}^{\mathrm{II}}=\Delta\boldsymbol{P}_{att}$ in the type II attack should satisfy

$$\boldsymbol{V}+\wedge_{VP}\cdot\boldsymbol{u}_{att}^{\mathrm{II}}=\boldsymbol{V}+\wedge_{VP}\cdot\Delta\boldsymbol{P}_{att}\notin\mathbb{K}_s. \tag{12}$$

3.4 | Strategy of CFDI attack

To maximize the voltage deviation with limited attack resources, we propose an optimization method to obtain the optimal CFDI attack strategy. The schematic diagram of the overall attack is shown in Figure 2. Since both types of FDI attacks regulate voltage by changing power injection, we can build an optimization model by quantitatively analyzing the impact of power changes on voltage.

As the elements reflecting the impact of node j on node i may not necessarily lie in the i-th row and j-th column of the sensitivity matrix, let the mappings $e(i)$ and $g(j)$ represent the rows and columns representing nodes i and j, respectively. The voltage variation at node i can be approximated by

$$\Delta V_i=\sum_j\left(\alpha_{e(i),g(j)}\Delta P_j+\beta_{e(i),g(j)}\Delta Q_j\right), \tag{13}$$

where $\alpha_{e(i),g(j)}$ and $\beta_{e(i),g(j)}$ are impact coefficients representing the elements in the $e(i)$-th row and $g(j)$-th column of Λ_{VP} and Λ_{VQ}, respectively. With limited resources, attackers need to determine whether attacking node i is worth it and derive the optimal coordinated attack strategy. To address this, we use an optimization model to describe the problem and get the solution as follows:

$$\min\ w_P\Sigma_j\Delta P_j+w_Q\Sigma_k\Delta Q_k,\ j\in\boldsymbol{L},\ k\in\boldsymbol{S}, \tag{14a}$$

$$\text{s.t. } \Sigma\Delta N_j\le N^{max}-\Sigma N_j, \tag{14b}$$

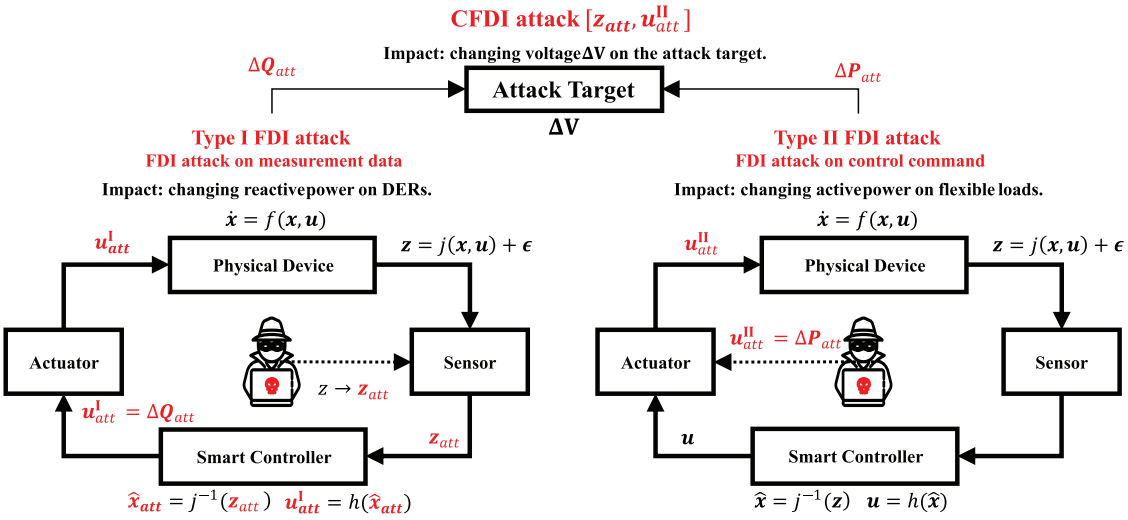


FIGURE 2 The CFDI attack consists of type I and type II FDI attacks. Type I FDI attacks can change reactive power ΔQ on DERs, while type II FDI attacks can change active power ΔP on flexible loads, DERs etc. Finally, the coordinated change of active power ΔP and reactive power ΔQ can cause significant voltage deviation ΔV on the target node.

$$\Delta N_j \le N_j^{max} - N_j, \tag{14c}$$

$$\Delta P_j = (N_j + \Delta N_j) P^{unit}, \tag{14d}$$

$$Q_k^{min} \le Q_k + \Delta Q_k \le Q_k^{max}, \tag{14e}$$

$$V_{ref} - V_i + \Delta V_i \ge \Delta V_{target}, \tag{14f}$$

where w_P and w_Q are weight coefficients representing the cost of manipulating the active power and reactive power, respectively. $\boldsymbol{L}$ represents the set of load nodes. $\boldsymbol{S}$ represents the set of buses with DERs. ΔN_j represents the increased number of controlled EV charging operations at bus j. N^{max} represents the total number of EV charging stations that the attacker can control. N_j^{max} represents the maximum number of EVs that can be compromised at bus j. N_j represents the number of EVs currently being charged at bus j. ΔV_{target} represents the target voltage deviation for the attacker and $V_{ref} = 1$ p.u. represents the reference voltage. The objective function (14a) is the cost of manipulating the power. Equations (14b) and (14c) describe the upper limit of EVs that can be compromised in the whole system and at bus j, respectively. Equation (14d) describes the relationship between the number of EVs and their charging power, where P^{unit} represents the charging power of each EV. Equation (14e) limits the reactive power generated by DER, where Q_k^{min} and Q_k^{max} represent the lower and upper limits at bus j, respectively. Equation (14f) ensure that the voltage deviation could at least reach ΔV_{target}. It is worth noting that the threat of voltage deviation is manifested on the load side, so the attacked bus i should also be included in the set $\boldsymbol{L}$.

Since the sensitivity matrix is a linear approximation, the solution to the above equation does not guarantee that the attack will achieve the target voltage deviation. Therefore, we use an iterative method to obtain an attack strategy that can accurately achieve the target voltage deviation. The algorithm is depicted in Algorithm 2. In the body of the loop, Lines 3–6 solve (14) and obtain the attack strategy $[\Delta \boldsymbol{P}, \Delta \boldsymbol{Q}]$ of each iteration, and if (14) is unsolvable, we deem that the attack cannot reach the target. Then we update $\Delta \boldsymbol{P}_{att}$, $\Delta \boldsymbol{Q}_{att}$ and $\boldsymbol{z}$ to execute power flow calculation for new system parameters in Lines 7 and 8. The calculated voltage deviation is compared with the target ΔV_{target}. If the target value is not reached, another iteration is performed. If the algorithm converges as described in Line 9 within m_{iter} iterations, we can obtain the attack strategy as $\boldsymbol{u}_{att} = [\boldsymbol{z}_{att}, \boldsymbol{u}^{II}_{att}]$ in Lines 10–12, which are the attacks on measurement data and control commands, respectively. Otherwise, we also regard that the attack cannot reach the target, which indicates that the bus is not worth attacking.

3.5 | Timeline of CFDI attack

The existing control strategy of the active distribution network is mainly based on quasi-real-time optimization, and the interval between two consecutive active regulations is usually more than 10 min [46]. Let t_n denote the time of the system's n-th active voltage regulation, and Δt represents the interval between two consecutive active regulations. The timeline for a sample CFDI attack is illustrated in Figure 3. The n-th CFDI attack executes around t_n. Type I FDI attack can be launched with counterfeit data at any moment between t_{n-1} and t_n, and consequently lets the system perceive a false state based on the counterfeit data and make false control decisions for the reactive power of DERs at t_n. After t_n, the type II FDI attack is initiated by manipulating the active power of flexible loads in the power grid, and the effects of both types of attacks on the voltage will add up and continue until t_{n+1}. When the occurrence of the type II attack is close to t_n, the duration of CFDI's attack effect reaches the maximum value of nearly Δt.

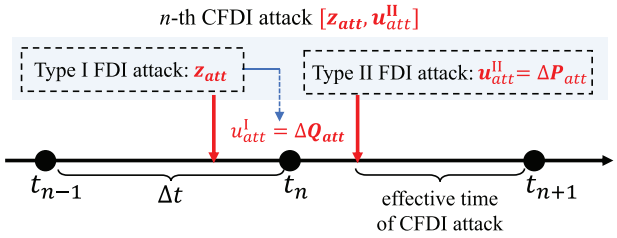


FIGURE 3 Timeline of the CFDI attack. The active voltage regulation is performed every Δt. For the n-th CFDI attack, the change of reactive power ΔQ_{att} is introduced by the active voltage regulation at t_n, which has been misled by the type I FDI attack z_{att} conducted before t_n. Meanwhile, the change of active power ΔP_{att} is directly introduced by the type II FDI attack u^{II}_{att} conducted after t_n.

4 | FEASIBILITY ANALYSIS ON DISTRIBUTION NETWORK TESTBED

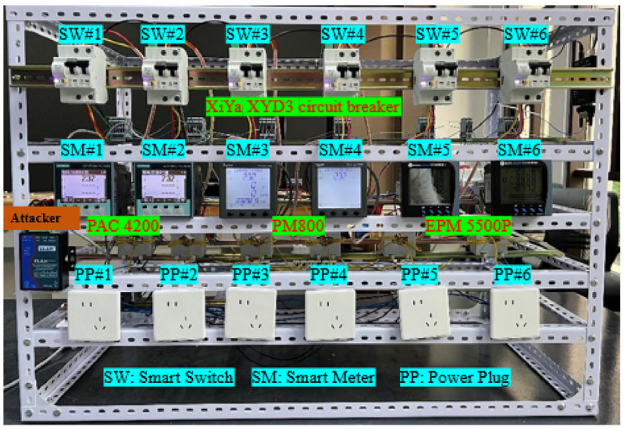
The requirements for a successful FDI attack are as follows.

- **Network access rights**: Attackers should have access to the target network, so that attackers can eavesdrop on the network and inject false data accordingly. The network access right can be obtained via either network penetration [47], near-source penetration [48] or physical intrusion [49].
- **Detailed device information**: Attackers should get the information about measurement devices and control devices, which could be obtained from device scanners like Shodan, Censys, ZoomEye [50], or through comparing eavesdropped data with known devices' signature database.
- **Devices' security vulnerabilities**: Attackers should know devices' vulnerabilities before exploiting them for launching FDI attacks. These vulnerabilities could be obtained from published common vulnerabilities and exposures (CVE) records [51], or dug by fuzzing technologies [52].

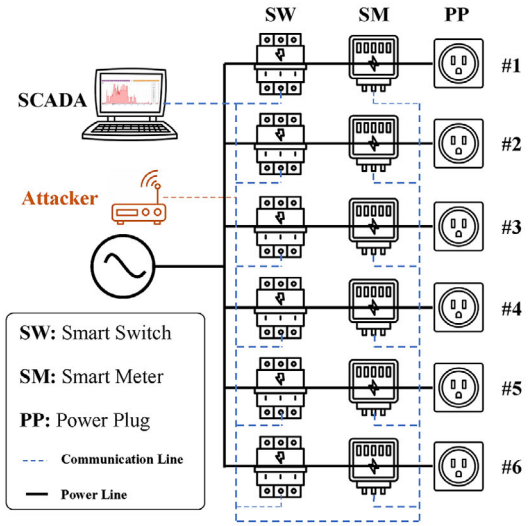
To validate the feasibility of CFDI attacks, we have built a smart distribution testbed with six circuit branches. As shown in Figure 4, for each branch, the SCADA system monitors the energy consumption via the smart meter and turns the circuit on/off via the smart switch. An illegal device is attached to the communication fieldbus network and controlled remotely by the attacker, which can eavesdrop on the network and launch FDI attacks. This illegal device is an off-the-shelf wireless serial port transmission device [53, 54], which could convert serial data in the serial communication line to TCP data from/to the wireless receiver (i.e. the attacker). With this device, attackers could eavesdrop on the communication line and inject false data remotely. With this testbed, we will validate the feasibility of type I and type II FDI attacks by analyzing devices' vulnerabilities, and CFDI attacks could be conducted via their combination.

4.1 | Feasibility analysis for type I FDI attack

There are three types of smart meters, that is, Siemens PAC4200, Schneider PM810 and GE EPM5500P, all of which communicate using the Modbus protocol. All three meters have a password field to protect the system, and a four-digit password (0,000-9,999) is required to enter the parameter setting mode. After exploration, we have found several security flaws on their password protection mechanisms as follows:



(a) Picture of smart distribution network testbed.



(b) Diagram of smart distribution network testbed.

FIGURE 4 A smart distribution network testbed with six circuit branches, each containing a smart switch, a smart meter and a power plug, respectively. All smart devices are monitored and controlled by the SCADA system via the RS485 communication line.

- **Protection missing in remote access**: For Schneider PM810 and GE EPM5500P meters, the password is only effective when we want to change the critical parameters locally on the device panel. If we access PM810 and GE EPM5500P through the communication interfaces remotely, the critical parameters (even including the password field) can be changed directly.
- **Unsecure communication during authentication**: For the Siemens PAC4200 meter, we need to provide the password when we want to change critical parameters. As the password is transmitted in plain text using the Modbus protocol, it can be easily eavesdropped by attackers.

TABLE 1 Register settings of CT ratio and PT ratio in three smart meters.

Smart meter brand	Register name	Register address	Range	Default value
Siemens PAC4200	PT Pri.	50005	1-99,999	400
	PT Sec.	50007	1-690	400
	CT Pri.	50011	1-99,999	50
	CT Sec.	50013	1, 5	5
Schneider PM800	PT Pri.	3205	1-32,767	120
	PT Sec.	3207	100, 110, 115, 120	120
	CT Pri.	3201	1-32,767	5
	CT Sec.	3202	1, 5	5
GE EPM5500P	PT Pri.	105 and 106	100-500,000	100
	PT Sec.	107	100-400	100
	CT Pri.	108	5-10,000	5
	CT Sec.	/	5	5

* 'Pri.' and 'Sec.' are short for 'Primary' and 'Secondary', respectively. CT ratio = CT Pri./CT Sec., PT ratio = PT Pri./PT Sec.

- **Weak password without brute force attack prevention**: The four-digit password for Siemens PAC4200 can be cracked easily, as there are no measures against the brute-force attack. Specifically, we tested the Siemens PAC4200 meter in the testbed and found that all 10,000 possible passwords could be tried exhaustively within 78 s.

After cracking the password protection mechanism, attackers can compromise them with malicious firmware via online updates. Alternatively, attackers can inject false data by changing the parameter settings. For example, we can change the CT ratio (i.e. CT Primary/CT Secondary) and PT ratio (i.e. PT Primary/PT Secondary) to manipulate the data. The relevant registers for these meters are shown in Table 1. Specifically, If we change the CT ratio from 25:5 to 250:5, the current readings in the meter would be magnified tenfold (e.g. switched from 1A to 10A). Accordingly, all the measurements related to the current readings (e.g. active power, reactive power etc.) would be affected. Thus, for the type I FDI attack (i.e. FDI attack on measurement data), attackers can inject false measurement data via these compromised smart meters.

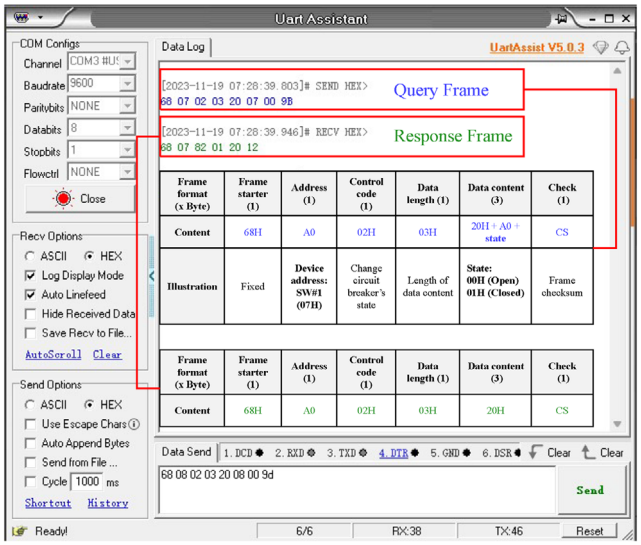


FIGURE 5 Query and response frames for open smart switch#1. The frame checksum is the sum of all bytes from the frame starter to the data content, truncated to lowest 8 bits.

4.2 | Feasibility analysis for type II FDI attack

The smart switch in the testbed communicates using a simple private protocol, and the commands for controlling the smart switch are transmitted in plain text. For example, for switch#1 (device address:07H), the query commands for open and close circuit#1 are as follows.

- **Turn off circuit#1**: 68H 07H 02H 03H 20H 07H **00H** 9BH
- **Turn on circuit#1**: 68H 07H 02H 03H 20H 07H **01H** 9CH

Note that the only difference between these two commands is at the penultimate byte, which represents the desired state of open (00H) or close (01H) for the specified switch. The detailed illustration of each byte from the query and response frames for open switch#1 can be found in Figure 5. As all bytes are transmitted in plain text, it is easy for attackers to capture and replay these control commands. Thus, for the type II FDI attack (i.e. FDI attack on control command), attackers can inject false control commands to compromised smart switches via eavesdropping and replay attacks.

5 | EVALUATION

In this section, we evaluate the threat of CFDI attacks on distribution networks through simulation experiments. First,

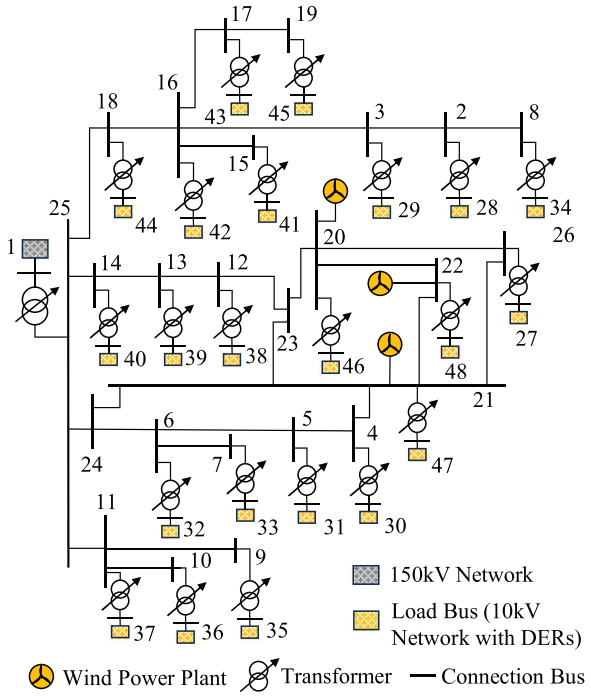


FIGURE 6 The topology of DTU-ADN.

we confirm that attacks can be successfully launched on the experimental system and achieve attack objectives under certain load/generation conditions. Then, we compared them with unilateral attacks to demonstrate that the attack capabilities of CFDI attacks are significantly higher than those of ordinary unilateral FDI attacks. Finally, we conducted multiple experiments by changing the experimental parameters to analyze the factors influencing the effectiveness of the attacks.

5.1 | Simulation setup

The simulation experiments are conducted on the DTU-7k Bus ADN (DTU-ADN) [55]. As shown in Figure 6, DTU-ADN utilizes the topology and parameters of a real Nordic grid at the 60kV level, and lots of DERs are connected at 10 kV buses. Bus 1 is the substation bus, buses 20, 21 and 22 are DER buses connected with controllable wind power plants, buses 27-48 are load buses containing loads and uncontrollable DERs, and the rest are connection buses. The simulations are implemented in MATLAB on a PC with 1.10-GHz Intel(R) Core(TM) i7-10710U CPU and 16 GB of RAM. The MILP subproblem is modeled and solved by Gurobi. The major simulation parameters are chosen as follows.

- We choose 2,000 different load/generation conditions from actual hourly load and generation data for about three months [55]. For each condition, 22 load buses can be regarded as the attack target separately, resulting in a total of 44,000 different CFDI attacks.
- Based on the installed capacity of the wind power plants in the case study, we constrained the reactive power output of each DER bus within ±12 MVar.

TABLE 2 Feasibility of Algorithm 2 for DERs under different ΔV_{target}.

ΔV_{target}	n_{att}	n_{succ}	Success rate
8%	3234	3212	99.3%
10%	652	652	100%
12%	191	189	99.0%

- Considering the limitation on attack resources, we assumed that only a portion of EVs could be compromised. That is there are up to 500 compromised EVs in total and at most 100 compromised EVs per load bus, and each EV's charging power is set to 50 kW.
- m_{iter} is set to 10 to ensure low latency of attack strategy generation. Considering that the control command will converge to a region instead of a point as mentioned in Section 3.2, we set ε_u to 0.01MVA. And ε_V is set to 0.0001p.u. to ensure an accuracy of 1%.
- The typical voltage deviation limitation is ±5% [56], and motors may stop working when the voltage deviation is beyond ±10% [57]. Therefore, we set the target of voltage deviation ΔV_{target} as 8%, 10% and 12% in most experiments, respectively.

5.2 | Feasibility verification

Section 4 has already demonstrated the feasibility of carrying out CFDI attacks. In addition, the algorithms and strategies used in CFDI attacks also need to be verified. In this subsection, we analyze the ability of Algorithm 1 in type I FDI attack to indirectly control DERs and the feasibility of Algorithm 2 in optimal CFDI attack strategy.

The purpose of type I FDI attack is to falsify the system state $\boldsymbol{x}_{att}$ such that the system control command $\boldsymbol{u}$ is misled to attack target $\boldsymbol{u}_{att}$. However, in Algorithm 1, $\boldsymbol{u}_i$ does not necessarily converge to $\boldsymbol{u}_{att}$, resulting in the inability to obtain $\boldsymbol{x}_{att}$ and thus unable to implement the attack in practice. Therefore, we use the percentage of cases of successfully obtaining $\boldsymbol{x}_{att}$ to demonstrate the feasibility of this algorithm. Let n_{att} represent the total number of conditions in which attack strategies can be obtained for the 22 load buses, and let n_{succ} represent the total number of conditions in which $\boldsymbol{x}_{att}$ can be successfully obtained. The success ratio for different target attack voltages ΔV_{target} is shown in Table 2. From the table, type I FDI can successfully implement attacks according to the attack strategies in most conditions, indicating that this algorithm has a high level of feasibility.

The optimal attack strategy is designed to generate significant voltage deviations in CFDI attacks. We set the target voltage deviation ΔV_{target} as 8%, 10% and 12%, respectively, and conduct optimal CFDI attack strategies in Algorithm 2 under 2000 different load/generation conditions. The number of success conditions on each load bus is shown in Figure 7. Specifically, when $\Delta V_{target} = 8\%$, successful attacks could be launched in many conditions on most buses. When $\Delta V_{target} = 10\%$, successful attacks can be achieved under certain conditions. When $\Delta V_{target} = 12\%$, attacks can still be completed in a few

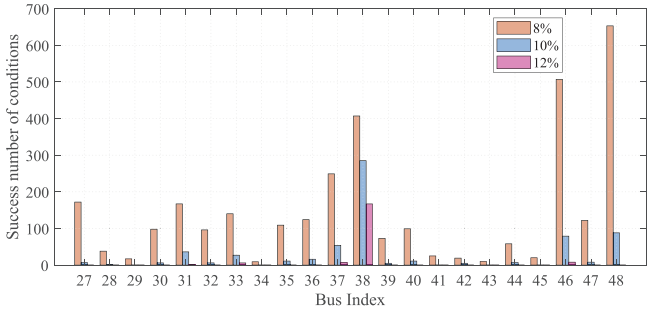
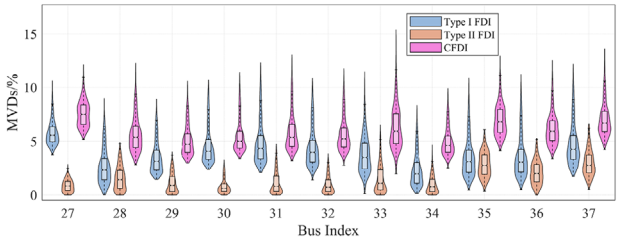
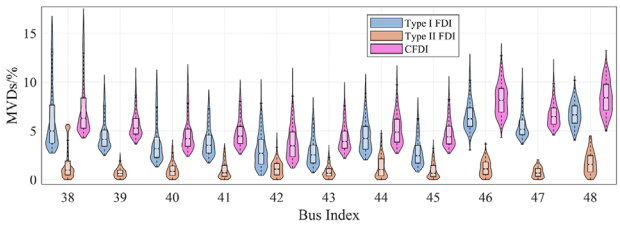


FIGURE 7 The number of success CFDI attacks that could be conducted on each load bus in 2000 conditions.



(a) The distribution of MVDs on buses 27-37.



(b) The distribution of MVDs on buses 38-48.

FIGURE 8 Violin plots of MVDs caused by FDI attacks on 22 load buses. The Violin plot is a hybrid of a box plot and a kernel density plot, depicting summary statistics and the density of each variable.

conditions and on a small number of buses. Thus, this attack could cause significant damage to the distribution system.

5.3 | Comparison of threats posed by different attacks

In this subsection, we compared the threats posed by type I FDI attacks, type II FDI attacks, and CFDI attacks in 2,000 conditions, and the distribution of maximum voltage deviations (MVDs) on each bus is shown by the violin plot. As shown in Figure 8, the overall distributions of MVDs caused by coordinated attacks are higher than those of unilateral attacks on all 22 load buses, indicating that coordinated attacks can cause greater voltage deviations. Moreover, under the same ΔV_{target}, the violin shapes of MVDs caused by coordinated attacks are wider on all buses, indicating that coordinated FDI attacks have less stringent requirements on the load/generation conditions.

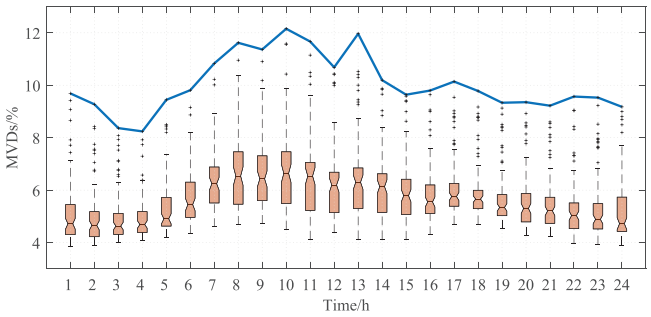


FIGURE 9 Box plots of MVDs over the 24-h period corresponding to 80 days. The line at the top of the figure represents the change in maximum value of MVDs.

5.4 | Changes of threats on different time periods

Typically, the changes of loads and DERs within 24 h cause the network states to show certain regularity over time. For example, the power of photovoltaic generation reaches its peak around 12:00 a.m. (noon time) and is 0 at night; residents' power consumption reaches its peak from 7:00 p.m. to 11:00 p.m. This leads to varying levels of vulnerability for ADN at different times of the day. We analyzed the experimental results corresponding to the first 80 days in Section 5.3 according to time periods. The distribution of the MVDs caused by attacks on all buses in different time periods is shown in Figure 9. It is clear that the distribution from 7:00 a.m. to 13:00 a.m. is generally higher than that of other time periods, and is the lowest at night.

5.5 | Impact of RPC and OLTC on CFDI attacks

In ADN, there are still some passive voltage regulation devices which are regulated by local controllers for Volt/Var control. In this section, we consider some local RPCs and OLTC as passive voltage regulation devices and evaluate their impact on CFDI attacks under different regulating abilities. Without loss of generality, we choose the MVD on bus 38 as the evaluation metric.

First, we consider the impact of local RPCs on CFDI attacks. On some vulnerable buses, we placed RPCs and varied the total regulation capacity from 0 to 3 MVar. The variation of MVDs on bus 38 under different capacities of RPCs is shown in Figure 10. From the figure, although the MVD caused by CFDI attacks could be alleviated by local PRCs, a significant voltage deviation (11%) still exists when the capacity of 3 MVar is exhausted.

Second, we test the OLTC's impact on CFDI attacks. To ensure that the ADN can regulate itself within the allowable range of voltage deviation, we increase the gear of OLTC from -1% to 6%. The variation of MVDs with the gear of OLTC is shown in Figure 11. From the figure, the OLTC can effectively alleviate CFDI attacks, limiting its MVD to around 7%. However, the number of OLTC operations is limited considering

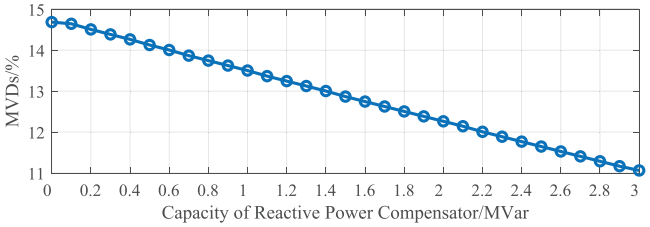


FIGURE 10 MVD on bus 38 under different total capacity of RPCs.

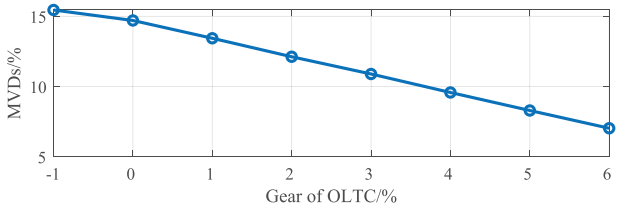


FIGURE 11 MVDs on bus 38 under different gears of OLTC.

the operation cost and equipment wear [11]. Hence, the OLTC cannot meet the regulatory requirements if CFDI attacks are conducted frequently.

5.6 | Influential factor

In the first two experiments, we found that some buses are more vulnerable to attacks, meaning they can achieve the target voltage deviation or reach a higher voltage deviation on a higher number of load/generation conditions. To develop some prevention and defense methods, we analyzed the factors that influence the magnitude of coordinated attack threats on different buses. It is obvious that the amount of attack resources and the load condition (heavy load/light load) are important influencing factors, but they are not the causes of the differences between buses. By analyzing the topology of the system and simulation results of the experimental cases, we identified some key influential factors. The following discussions are conducted separately on type I and type II FDI attacks.

Type I FDI attacks are based on active control of DERs. Therefore, we adjusted the position of DER buses and only performed type II FDI attacks to observe and compare the magnitude of attack threats on each load bus. We found that the distance between the attacked bus and the DER buses is an important factor. If we consider the topology of the distribution network as an unweighted graph, the distance between two buses is the length of the shortest path in the graph. Let D_{ij} represent the distance between bus i and DER bus j, and ΔV_i represent the average of MVDs on 2,000 conditions. The correlation coefficients between $\boldsymbol{D} = \{\sum_{j \in S} \frac{1}{D_{ij}} | i \in \boldsymbol{L}\}$ and $\Delta \boldsymbol{V} = \{\overline{\Delta V_i} | i \in \boldsymbol{L}\}$ under different DERs' location cases are shown in Table 3, indicating that the MVD has a strong positive correlation with the average of the distances' reciprocal.

Type II FDI attacks rely on controlling EVs' charging on a large number of load buses, which are often distributed throughout the entire distribution network. However, by analyzing the attack strategy mentioned in Section 5.2, we found that the manipulated load buses of which the active power is changed are often concentrated in a few fixed buses irrespective of operation conditions and which bus is attacked, as shown in Figure 12. This indicates that the load fluctuations on these buses have a stronger impact on the voltage level of the entire network and are not significantly affected by changes of operation conditions. Additionally, as shown in Figure 8, some buses are less vulnerable to FDI attacks and remain in a relatively secure state under most operation conditions.

In conclusion, for the type I attack, the threat of each DER bus on the load bus will decrease as the distance between them increases. For the type II attack, the threat of flexible loads on each load bus is affected by the mutual influence between load buses, which is mainly determined by the network topology and parameters of the ADN and has little relation to load/generation conditions.

TABLE 3 The correlation coefficients between $\boldsymbol{D}$ and $\Delta \boldsymbol{V}$ under different connection points of DERs.

Buses connected with DERs	Correlation coefficient
20, 21, 22	0.92
2, 6, 11	0.66
2, 15, 17	0.87

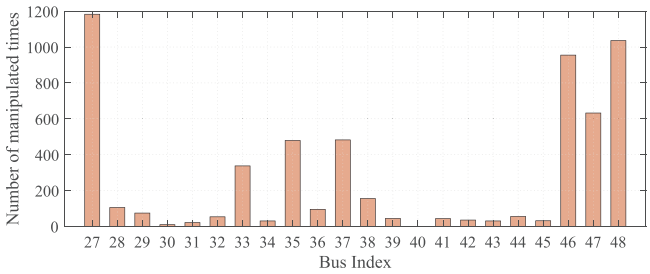


FIGURE 12 The number of manipulated times by CFDI attackers on 22 load buses in 2000 conditions.

6 | COUNTERMEASURES

Extensive research has been conducted on defense methods against FDI attacks. However, most defense methods pertain to transmission systems, and few have considered FDI attacks in distribution systems. Moreover, CFDI attacks utilize some new features of ADNs, which may render traditional methods ineffective. Therefore, based on the experimental analysis presented earlier and the functionalities of SCADA systems, this paper offers insights into the prevention, detection, and mitigation strategies for CFDI attacks.

System hardening and data protection: With strategies such as encryption and continuous monitoring [58, 59], we can identify critical buses that need enhanced monitoring and provide pre-incident plans for the operation of distribution

networks. In addition, it is also important to strengthen the distribution grid with effective detection methods for complicated cyber attacks. Moreover, attacks on physical systems usually require attackers to have comprehensive information about the system [60]. Therefore, methods such as data obfuscation can disrupt attackers' access to information [61]. Furthermore, existing works propose intrusion detection methods for fieldbus networks [62], which can help prevent SCADA systems from being eavesdropped and deceived.

Proactive detection strategy: The efficacy of CFDI attacks heavily depends on the attacker's knowledge of the system (e.g. network topology, lines' impedance). Recently, the concept of moving target defense (MTD) has been introduced into the power system security field. This approach involves dynamically perturbing lines' impedance [63, 64] or encoded meter outputs [65] to impede the attacker's ability to acquire up-to-date system knowledge. Recently, the application of MTD within distribution systems has garnered significant interest. Leveraging the substantial presence of flexible AC transmission devices within the grid, this method can detect most FDI attacks at a very low cost.

System resistance improvement: This approach consists of two aspects: (1) Enhancing system's resilience. CFDI attacks often require significant changes in several buses' power. Therefore, limiting the power injection and fluctuation of buses would be an effective measure [66]. Also, reactive power compensation devices like RPCs can be added at the load bus to replace the reactive power output of partial distributed energy supply, and convert part of the voltage regulation capability of active control into passive control. (2) Reducing the impact of attacks on critical loads. If the attack cannot be completely eliminated, securing critical loads can indirectly enhance the system's resilience to attacks. It is pointed out in Section 5.6 that the degree to which a bus is threatened by attacks is negatively correlated with the distance to the DER bus. Therefore, some important loads can be placed in safety regions that are far away from the DER bus and are not susceptible to active load fluctuations. Similarly, when placing DERs in ADN, the DER buses should be located at a small distance from each other. This will help enlarge security regions and reduce the impact of attacks on the entire network. We conducted the following experiments to confirm this recommendation. We connect DERs into the network with 100 different location cases, and then calculate the average distance between the three DERs and the average value of the MVDs on 2000 conditions. The relationship is shown in Figure 13. Obviously, as the concentration degree of DERs increases (i.e. the average distance of DERs increases), the average value of MVD decreases in the entire network, making ADN face a less severe attack threat.

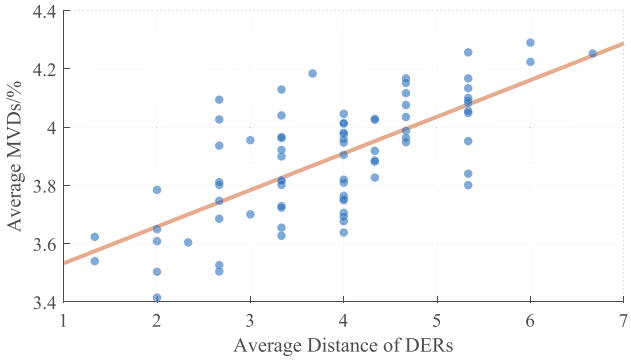


FIGURE 13 Location of DERs' impact on the voltage deviation threat.

7 | CONCLUSION AND FUTURE WORK

In this paper, we propose a coordinated FDI attack that induces significant voltage deviations in ADNs. This attack exploits the impact of power change from DERs and flexible loads on voltage deviation, which can be achieved through two types of FDI attacks, that is, type I attack on measurement data and type II attack on control commands. For the type I attack, we also present a method for indirectly controlling the reactive power output of DERs by false measurements. To enhance the attack capability, we propose an algorithm to generate the optimal coordinated attack strategy under limited attack resources. Experimental results on the DTU-ADN benchmark demonstrate that the CFDI attack can cause significant voltage deviation and is stronger than pure type I or type II FDI attack. Finally, we analyze the influential factors on CFDI attacks and propose countermeasures against CFDI attacks.

In the future, we will further investigate the CFDI attack in two directions. First, we will consider the impact of indeterminate factors like charging behaviors of EVs and the power fluctuation of DERs on attack resources, and study the threat under these factors. Second, we will explore the threat when information, including network topology, parameters, and regulation strategies, is incomplete.

AUTHOR CONTRIBUTIONS

Yang Liu: Conceptualization; supervision; visualization; writing—original draft; writing—review and editing. **Chenyang Yang**: Methodology; software; validation; visualization; writing—original draft. **Nanpeng Yu**: Investigation; validation; writing—review and editing. **Jiazhou Wang**: Validation; visualization; writing—review and editing. **Jue Tian**: Conceptualization; formal analysis; validation; writing—review and editing. **Hao Huang**: Data curation; funding acquisition; investigation; resources. **Yadong Zhou**: Conceptualization; project administration; supervision; writing—review and editing. **Ting Liu**: Conceptualization; funding acquisition; project administration; resources; supervision.

ACKNOWLEDGEMENTS

This work was partially supported by National Natural Science Foundation of China (62293501, 62293502), Key Research and Development Program of Shaanxi (2024GX-ZDCYL-02-19), Science and Technology Project of China Southern Power Grid Corporation (No. 030000KC23040079 [GDKJXM20230394]), China Postdoctoral Science Foundation (2020M683520), Fundamental Research Funds for the Central Universities.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Yang Liu https://orcid.org/0000-0002-4075-1971

REFERENCES

1. Meegahapola, L., Mancarella, P., Flynn, D., Moreno, R.: Power system stability in the transition to a low carbon grid: A techno-economic perspective on challenges and opportunities. Wiley Interdiscip. Rev.: Energy Environ. 10(5), e399 (2021)
2. Xie, S., Nazari, M.H., Yin, G., Chen, W., et al.: Impact of stochastic generation/load variations on distributed optimal energy management in DC microgrids for transportation electrification. IEEE Trans. Intell. Transp. Syst. 23(7), 7196–7205 (2021)
3. Clement Nyns, K., Haesen, E., Driesen, J.: The impact of charging plug-in hybrid electric vehicles on a residential distribution grid. IEEE Trans. Power Syst. 25(1), 371–380 (2010)
4. Kong, X., Zhang, X., Zhang, X., Wang, C., Chiang, H.D., Li, P.: Adaptive dynamic state estimation of distribution network based on interacting multiple model. IEEE Trans. Sustainable Energy 13(2), 643–652 (2021)
5. Zhang, Z., Dong, Z.Y., Yue, D.: Multiple time-scale voltage regulation for active distribution networks via three-level coordinated control. IEEE Trans. Ind. Inf. 20(3), 4429–4439 (2024)
6. von Jouanne, A., Banerjee, B.: Assessment of voltage unbalance. IEEE Trans. Power Delivery 16(4), 782–790 (2001)
7. Simpson Porco, J.W., Dörfler, F., Bullo, F.: Voltage collapse in complex power grids. Nat. Commun. 7(1), 10790 (2016)
8. Ayres, H., Freitas, W.,De Almeida, M., Da Silva, L.: Method for determining the maximum allowable penetration level of distributed generation without steady-state voltage violations. IET Gener. Transm. Distrib. 4(4), 495–508 (2010)
9. Rogers, K.M., Klump, R., Khurana, H., Aquino Lugo, A.A., Overbye, T.J.: An authenticated control framework for distributed voltage support on the smart grid. IEEE Trans. Smart Grid 1(1), 40–47 (2010)
10. Escobar, F., Víquez, J.M., García, J., Aristidou, P., Valverde, G.: Coordination of DERs and flexible loads to support transmission voltages in emergency conditions. IEEE Trans. Sustainable Energy 13(3), 1344–1355 (2022)
11. Viawan, F.A., Karlsson, D.: Coordinated voltage and reactive power control in the presence of distributed generation. In: 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–6. IEEE, Piscataway (2008)
12. Baran, M.E., El Markabi, I.M.: A multiagent-based dispatching scheme for distributed generators for voltage support on distribution feeders. IEEE Trans. Power Syst. 22(1), 52–59 (2007)
13. Preiss, R., Warnock, V.: Impact of voltage reduction on energy and demand. IEEE Trans. Power Appar. Syst. PAS-97(5), 1665–1671 (1978)
14. Yuan, H., Li, F., Wei, Y., Zhu, J.: Novel linearized power flow and linearized OPF models for active distribution networks with application in distribution LMP. IEEE Trans. Smart Grid 9(1), 438–448 (2016)
15. Sekhavatmanesh, H., Cherkaoui, R.: Analytical approach for active distribution network restoration including optimal voltage regulation. IEEE Trans. Power Syst. 34(3), 1716–1728 (2018)
16. Kosut, O., Jia, L., Thomas, R.J., Tong, L.: Malicious data attacks on the smart grid. IEEE Trans. Smart Grid 2(4), 645–658 (2011)
17. Yang, Q., Yang, J., Yu, W., An, D., Zhang, N., Zhao, W.: On false data-injection attacks against power system state estimation: Modeling and countermeasures. IEEE Trans. Parallel Distrib. Syst. 25(3), 717–729 (2013)
18. Choeum, D., Choi, D.H.: Vulnerability assessment of conservation voltage reduction to load redistribution attack in unbalanced active distribution networks. IEEE Trans. Ind. Inf. 17(1), 473–483 (2020)
19. Chen, X., Hu, S., Li, Y., Yue, D., Dou, C., Ding, L.: Co-estimation of state and fdi attacks and attack compensation control for multi-area load frequency control systems under fdi and dos attacks. IEEE Trans. Smart Grid 13(3), 2357–2368 (2022)
20. Amini, S., Pasqualetti, F., Mohsenian Rad, H.: Dynamic load altering attacks against power system stability: Attack models and protection schemes. IEEE Trans. Smart Grid 9(4), 2862–2872 (2016)
21. Lai, K., Illindala, M., Subramaniam, K.: A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment. Appl. Energy 235, 204–218 (2019)
22. Vovos, P.N., Kiprakis, A.E., Wallace, A.R., Harrison, G.P.: Centralized and distributed voltage control: Impact on distributed generation penetration. IEEE Trans. Power Syst. 22(1), 476–483 (2007)
23. Yu, L., Czarkowski, D., De León, F.: Optimal distributed voltage regulation for secondary networks with DGs. IEEE Trans. Smart Grid 3(2), 959–967 (2012)
24. Barr, J., Majumder, R.: Integration of distributed generation in the volt/var management system for active distribution networks. IEEE Trans. Smart Grid 6(2), 576–586 (2014)
25. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Security (TISSEC) 14(1), 1–33 (2011)
26. Liu, X., Li, Z.: Local topology attacks in smart grids. IEEE Trans. Smart Grid 8(6), 2617–2626 (2016)
27. Jin, M., Lavaei, J., Johansson, K.: A semidefinite programming relaxation under false data injection attacks against power grid AC state estimation. In: 2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 236–243. IEEE, Piscataway (2017)
28. Nayak, J., Al Anbagi, I.: Modelling false data injection attacks against nonlinear state estimation in AC power systems. In: 2020 8th International Conference on Smart Grid (icSmartGrid), pp. 37–42. IEEE, Piscataway (2020)
29. Sawas, A., Farag, H.E.: Two-fold intelligent approach for successful FDI attack on power systems state estimation. In: 2018 IEEE Electrical Power and Energy Conference (EPEC), pp. 1–6. IEEE, Piscataway (2018)
30. Liu, C., Liang, H., Chen, T.: Network parameter coordinated false data injection attacks against power system AC state estimation. IEEE Trans. Smart Grid 12(2), 1626–1639 (2020)
31. Liu, X., Li, Z.: False data attacks against AC state estimation with incomplete network information. IEEE Trans. Smart Grid 8(5), 2239–2248 (2016)
32. Deng, R., Liang, H.: False data injection attacks with limited susceptance information and new countermeasures in smart grid. IEEE Trans. Ind. Inf. 15(3), 1619–1628 (2018)
33. Chin, W.L., Lee, C.H., Jiang, T.: Blind false data attacks against AC state estimation based on geometric approach in smart grid communications. IEEE Trans. Smart Grid 9(6), 6298–6306 (2017)
34. Du, M., Pierrou, G., Wang, X., Kassouf, M.: Targeted false data injection attacks against ac state estimation without network parameters. IEEE Trans. Smart Grid 12(6), 5349–5361 (2021)
35. Ayad, A., Farag, H., Youssef, A., El Saadany, E.: Cyber–physical attacks on power distribution systems. IET Cyber-Phys. Syst.: Theor. Appl. 5(2), 218–225 (2020)
36. Zhuang, P., Deng, R., Liang, H.: False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems. IEEE Trans. Smart Grid 10(6), 6000–6013 (2019)
37. Sreeram, T., Krishna, S.: Graph-based assessment of vulnerability to false data injection attacks in distribution networks. IEEE Trans. Power Syst. 39(2), 4510–4520 (2024)
38. Zhang, B., Dou, C., Yue, D., Park, J.H., Xie, X., Yuan, D., et al.: Transmission and decision-making co-design for active support of region frequency regulation through distribution network-side resources. IEEE Trans. Circuits Syst. I Regul. Pap. 70(10), 4204–4217 (2023)

39. Caldon, R., Coppa, M., Sgarbossa, R., Turri, R.: A simplified algorithm for OLTC control in active distribution mv networks. In: AEIT Annual Conference 2013, pp. 1–6. IEEE, Piscataway (2013)
40. Siano, P.: Demand response and smart grids—A survey. Renewable Sustainable Energy Rev. 30, 461–478 (2014)
41. Yang, H., Wang, L., Ma, Y., Zhang, D., WU, H.: Optimization strategy of price-based demand response considering the bidirectional feedback effect. IET Gener. Transm. Distrib. 15(11), 1752–1762 (2021)
42. Herberg, U., Mashima, D., Jetcheva, J.G., Mirzazad Barijough, S.: OpenADR 2.0 deployment architectures: Options and implications. In: 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 782–787. IEEE, Piscataway (2014)
43. Xu, Z., Callaway, D.S., Hu, Z., Song, Y.: Hierarchical coordination of heterogeneous flexible loads. IEEE Trans. Power Syst. 31(6), 4206–4216 (2016)
44. Liu, Y., Tian, J., Yuan, X., Ye, B., Sang, Z., Yao, X., et al.: Real-time pricing response attack in smart grid. IET Gener. Transm. Distrib. 16(12), 2441–2454 (2022)
45. Sajeev, A., Rajamani, H.S.: Cyber-attacks on smart home energy management systems under aggregators. In: 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), pp. 1–5. IEEE, Piscataway (2020)
46. Liu, A., Wang, S., Liang, S., Zhu, C., Zhang, N.: Research and application of key technologies for active distribution network in industrial parks. Distrib. Util. 34(07), 21–27 (2017)
47. Chen, L., Yue, D., Dou, C., Chen, J., Cheng, Z.: Study on attack paths of cyber attack in cyber-physical power systems. IET Gener. Transm. Distrib. 14(12), 2352–2360 (2020)
48. Ruan, Z., Yang, Y., Chen, L.: Near-source attack for isolated networks with covert channel transmission. In: 2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 59–64. IEEE, Piscataway (2023)
49. Wang, X., Liu, Y., Jiao, K., Liu, P., Luo, X., Liu, T.: Intrusion device detection in fieldbus networks based on channel-state group fingerprint. IEEE Trans. Inf. Forensics Secur. 19, 4012–4027 (2024)
50. Li, R., Shen, M., Yu, H., Li, C., Duan, P., Zhu, L.: A survey on cyberspace search engines. In: Cyber Security: 17th China Annual Conference, CNCERT 2020, Revised Selected Papers 17, pp. 206–214. Springer, Singapore (2020)
51. Zhao, B., Ji, S., Lee, W.H., Lin, C., Weng, H., Wu, J., et al.: A large-scale empirical study on the vulnerability of deployed iot devices. IEEE Trans. Dependable Secure Comput. 19(3), 1826–1840 (2020)
52. Yoo, H., Shon, T.: Grammar-based adaptive fuzzing: Evaluation on scada modbus protocol. In: 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 557–563. IEEE, Piscataway (2016)
53. Shanghai ZLAN: Ethernet transparent transmission protocol in serial device server (2010). http://www.zlmcu.com/en/document/ethernet_transparet_transfer.html
54. PUSR: How to realize transparent transmission between serial to ethernet converters/serial device servers? (2020). https://www.pusr.com/support/faq/669-iot-news.html
55. Baviskar, A., Das, K., Koivisto, M., Hansen, A.D.: Multi-voltage level active distribution network with large share of weather-dependent generation. IEEE Trans. Power Syst. 37(6), 4874–4884 (2022)
56. Code for Design of Power Supply and Distribution System (gb50052-95). Ministry of Machinery Industry of the People's Republic of China, Shanghai (1996)
57. National Electrical Manufacturers' Association: Ansi/nema mg 1-2021—Motors and generators (2021). https://www.nema.org/standards/view/motors-and-generators
58. Bobba, R.B., Rogers, K.M., Wang, Q., Khurana, H., Nahrstedt, K., Overbye, T.J.: Detecting false data injection attacks on DC state estimation. In: Preprints of the first workshop on secure control systems, CPSWEEK, pp. 1–9. ACM, New York (2010)
59. Kim, T.T., Poor, H.V.: Strategic protection against data injection attacks on power grids. IEEE Trans. Smart Grid 2(2), 326–333 (2011)
60. Wei, Z., Yuan, X., Wang, Z., Zhang, T., Xing, Z., Liu, Y., et al.: Topology consistency verification in power system based on data inference. In: 2023 3rd International Conference on Energy Engineering and Power Systems (EEPS), pp. 787–791. IEEE, Piscataway (2023)
61. Tonyali, S., Cakmak, O., Akkaya, K., Mahmoud, M.M., Guvenc, I.: Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid AMI networks. IEEE Internet Things J. 3(5), 709–719 (2015)
62. Liu, P., Liu, Y., Wang, X., Bao, Y., Yang, D., Wang, W., et al.: A reflection-based channel fingerprint to locate physically intrusive devices in ICS. IEEE Trans. Ind. Inf. 19(4), 5495–5505 (2022)
63. Tian, J., Tan, R., Guan, X., Liu, T.: Enhanced hidden moving target defense in smart grids. IEEE Trans. Smart Grid 10(2), 2208–2223 (2018)
64. Wang, J., Tian, J., Liu, Y., Yang, D., Liu, T.: Mmtd: Multi-stage moving target defense for security-enhanced d-facts operation. IEEE Internet Things J. 10(14), 12234–12247 (2023)
65. Liu, C., Deng, R., He, W., Liang, H., Du, W.: Optimal coding schemes for detecting false data injection attacks in power system state estimation. IEEE Trans. Smart Grid 13(1), 738–749 (2021)
66. Ju, P., Lin, X.: Adversarial attacks to distributed voltage control in power distribution networks with DERs. In: Proceedings of the Ninth International Conference on Future Energy Systems, pp. 291–302. ACM, New York (2018)

How to cite this article: Liu, Y., Yang, C., Yu, N., Wang, J., Tian, J., Huang, H., Zhou, Y., Liu, T.: CFDI: Coordinated false data injection attack in active distribution network. IET Gener. Transm. Distrib. 18, 2556–2569 (2024). https://doi.org/10.1049/gtd2.13217