False Data Injection Attacks on Smart Grid Voltage Regulation with Stochastic Communication Model

Yuan Liu, *Member, IEEE*, Omid Ardakanian, *Member, IEEE*, Ioanis Nikolaidis, *Member, IEEE*, Hao Liang, *Member, IEEE*

***Abstract*— With the growing adoption of electric vehicles (EVs) and advent of bidirectional chargers, EV aggregators, such as charging stations, will become a major player in electricity markets, providing voltage regulation (VR) or other services. We present a novel and practical VR scheme that takes advantage of the charging flexibility of EVs in charging stations that are connected to buses in a distribution grid. This VR scheme relies on real-time measurements, as well as estimates of the distribution system state and regulation capacity of each charging station. We then propose a novel false data injection attack (FDIA) against the VR capacity estimation process that exploits the uncertainty in EV mobility and network conditions. We show the attack vector with the largest expected adverse impact is the solution of a stochastic optimization problem, subject to a constraint that ensures it bypasses bad data detection. We determine this attack vector by solving a sequence of convex quadratically constrained linear programs. The case studies examined in a co-simulation platform, based on two standard test feeders, reveal the vulnerability of the VR capacity estimation process.**

***Index Terms*— Cyber attacks, distribution system state estimation, electric vehicles, stochastic optimization**

I. Introduction

THE growing penetration of distributed energy resources has created significant challenges for distribution system operators (DSOs), from increased chance of voltage limit violations to wide voltage fluctuations in the distribution system [1]–[3]. Traditional voltage regulation (VR) resources, such as on-load tap changers (OLTCs), are no longer sufficient to address these voltage fluctuations because they will need to make rapid, continuous adjustments [4], [5]. Compared to these VR resources, battery packs, like the ones in electric vehicles (EVs), are more advantageous due to their inexpensive operation and fast response [6]. The global EV stock is expected to reach 140 million vehicles with more than 550TWh of charging demand by 2030 [7]. These EVs can offer substantial VR capacity in smart distribution grids, reducing the cost associated with VR to a great extent [8]. With IEEE 802.11g, EVs can respond to control signals within four seconds, which is much faster than traditional VR resources [10].

A typical EV aggregator, such as an EV charging station (EVCS) with bidirectional chargers [9], can respond to VR commands issued by the DSO by coordinating charging of the connected EVs while still fulfilling their charging demand before they leave the station. However, owing to the uncertainty in EV mobility and charging demand, the VR capacity of an EVCS is variable and not readily known to the DSO. To facilitate the EVCS VR capacity estimation, prior work utilizes the supervisory control and data acquisition (SCADA) system for communications between the DSO and EVCS agents. Reliable communication is indeed required to send the sensor data for further analyses, such as distribution system state estimation (DSSE) and bad data detection (BDD) protecting DSSE [11]. For this reason, cyber attacks targeting the communication system are regarded as one of the major threats to the reliable operation of power system [12]. Examples of these attacks are false data injection attacks (FDIA), denial of service, and replay attacks. The FDIA is arguably more dangerous than other cyber attacks because it stealthier, enabling the attacker to disrupt the normal operation of the power system for a long time without being detected. Since first put forward in [13], such attacks have occurred several times, leading to long and catastrophic power outages. For example, in 2015, the attack launched against the Ukrainian power system's SCADA caused a power outage affecting more than two million customers for six hours [14].

Several efforts have been made to date to detect, locate, and mitigate FDIA against VR [15]–[17], yet they do not consider nontraditional VR resources, e.g., EV aggregators, and uncertainty in the communication network. In this work, we extend the commonly used VR scheme by incorporating the estimated VR capacity of every EVCS and a stochastic communication model. We then investigate the vulnerability of this VR scheme to a novel, carefully executed FDIA. The contributions of this paper are threefold:

- We propose a novel EVCS-assisted VR scheme. This scheme relies on the DSSE and BDD mechanism, which

This research was supported by funding from the Canada First Research Excellence Fund as part of the University of Alberta's Future Energy Systems research initiative. Grant Identification Number: CFREF-2015-00001. This work was also supported in part by a research grant from the Natural Sciences and Engineering Research Council of Canada.

Y. Liu (email: yuan17@ualberta.ca) and H. Liang (email: hao2@ualberta.ca) are with the Department of Electrical and Computer Engineering, University of Alberta, Canada.

O. Ardakanian (email: oardakan@ualberta.ca) and I. Nikolaidis (email: nikolaidis@ualberta.ca) are with the Department of Computing Science, University of Alberta, Canada.

we extend with linearized AC power flow.
- We develop an FDIA vector construction method under a stochastic communication model. The attack vector is guaranteed to bypass BDD even when the attacked measurements are partially received by the DSO. The proposed method solves a sequence of convex optimization problems to find the optimal attack vector.
- Through co-simulation, we demonstrate the vulnerability of the VR scheme to the proposed FDIA. Our case studies suggest that the proposed FDIA is potentially more harmful than the standard FDIA which utilizes an idealized communication model.

The plausibility of this FDIA calls for the development of more sophisticated BDD mechanisms that factor in stochastic network conditions. This is a direction for our future work.

The remainder of this paper is organized as follows. Section II surveys the related work and highlights the novelty of our work. Section III and IV introduce background information about VR and DSSE, and stochastic processes used to model EV mobility and data transmission. Section V presents the proposed attack vector construction method. Section VI describes the case studies and results. Section VII concludes the paper and presents avenues for future work.

II. Related Work

Prior work has investigated FDIAs against DSSE and proposed various detection methods [18], [19]. However, none of these studies accounts for the uncertainty of data communication. Since some of the false data injected by the attacker may not be received by the system operator in a timely fashion, existing FDIAs are not as stealthy as proved theoretically. In addition to misleading the DSSE process, the FDIA can affect ancillary services that rely on DSSE, such as VR [16], [20], [21]. In [16], the authors analyze how attackers can alter multiple field measurements in a coordinated manner to foil VR. Isozaki et al. [21] consider the impact of cyber attacks on VR in a distribution network with solar photovoltaics. An OLTC-induced FDIA against voltage regulation is investigated in [20]. It is shown that it can lead to a wrong OLTC tap position, causing serious under-voltage incidents. Zhuang et al. [22] analyze FDIA on battery energy storage installed in the distribution system, and show that the DSO can get wrong estimates of the battery energy content. To identify the attacker in various scenarios, a cooperative vulnerability factor framework is introduced in [15], where each agent can track voltage fluctuations to perform accurate detection. Moreover, a machine learning-based two-stage approach is developed for detecting attacks in [16]. In [17], a new method is proposed for the detection of FDIA in dc microgrids and the identification of the attacked unit, where the NARX neural networks are used for estimating dc voltages and dc output currents of all units in a dc microgrid. Abbaspour et al. [23] propose a Luenberger observer and a neural network-based approach to detect attacks against the load frequency control system.

Despite the vast literature in this area, there are still several challenges that are not fully addressed. First, most related work either relies on DC power flow, which is known to be less accurate than AC power flow in some distribution networks, or completely ignores the location of charging stations in the network. Second, the related work does not investigate the vulnerability of VR to FDIA when the DSO does not receive the attack vector completely. More specifically, an idealized communication model is adopted, ignoring the impact of packet losses on FDIA and BDD. Our work addresses this gap in the literature and is novel in that it presents a practical and accurate VR scheme that rely on EV charging stations, and develops a vector construction method for the FDIA against VR, considering the stochastic communication process.

III. Problem Statement and Assumptions

Fig. 1 shows a smart distribution network with various VR resources, such as battery energy storage system (BESS), OLTC, and EVCS with multiple bidirectional chargers. The distribution network is instrumented with a small number of distribution-level phasor measurement units (PMUs) in addition to smart meters that are installed at customers' premises. Each EVCS is also equipped with a car counting sensor, tracking the number of EVs parked in the station. We assume sensor measurements are time-synchronized and sent at regular intervals (every Δt) to the DSO control center located at the substation via a communication network. This network allows the DSO to remotely monitor the (partial) state of the distribution system or EVCSs in near real-time.

To maintain the voltage magnitude of each bus in the distribution system in a proper range, the DSO periodically observes or estimates the voltage magnitude of different buses and sends commands to VR resources to mitigate voltage limit violation problems. In particular, each VR cycle involves collecting sensor data, estimating the distribution system state, determining the contribution of VR resources using a VR scheme, and finally sending commands to the VR resources as depicted in Fig. 1. Due to random packet losses that could occur in the communication network and sparse deployment of PMUs, the DSO may have to use historical smart meter and PMU data to derive pseudo measurements. Together with real-time measurements, these pseudo measurements are used in the DSSE, the output of which is sent through a residual-based BDD mechanism to determine if it can be trusted [27]. Using BDD is essential because sensor measurements can be noisy or modified by an attacker. If the estimated state passes BDD, it will be utilized to issue VR commands. Otherwise, pseudo measurements are utilized to issue VR commands.

Given the reliance of DSSE on real-time measurements, an attacker can target PMUs and EV counters for false data injection to deceive the DSO into overestimating the VR capacity. Yet, to minimize the risk of being detected, it should account for the randomness of data communication that could result in pseudo measurements being used in lieu of real-time sensor measurements when they are not received by the time DSSE is run. We make the following assumptions in this work:

1) The DSO performs DSSE and sends VR commands at regular intervals;
2) EVs take precedence over other VR resources because of their responsiveness and low-cost operation;

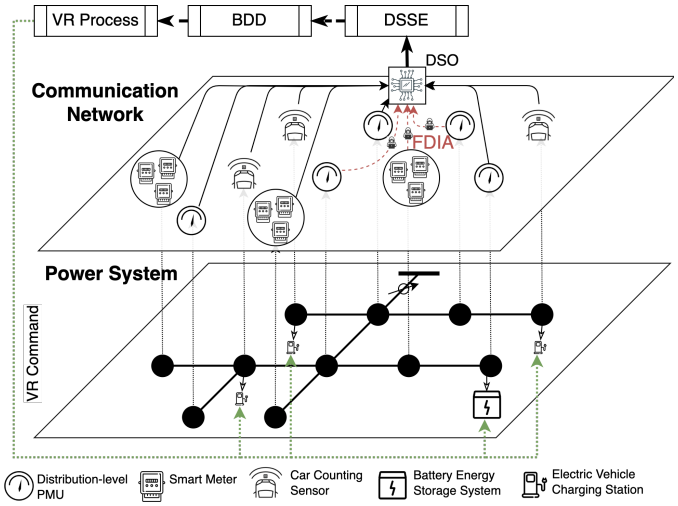

Fig. 1. Illustration of FDIA against the VR scheme in a distribution system with EVCS and traditional VR resources, e.g., battery energy storage (BESS). Red dashed lines show where the attacker injects false data.

3) EVs are keen to act as VR resources as long as their charging demands can be satisfied before departure;[1]
4) There is enough parking stalls in each EVCS so that all EVs are admitted upon arrival. But there might be a cap on the number of bidirectional chargers or the power that can be drawn simultaneously.[2] The remaining parking stalls are occupied by EVs that are waiting for service;
5) Car counting sensors installed at charging stations report the total number of EVs without error;
6) The attacker knows the distribution system model, and has access to real-time and historical PMU and smart meter data, and the number of EVs reported by each EVCS. They can inject false data into both PMU and EVCS measurements.

Next, we present the VR scheme, EVCS load model, stochastic communication model, DSSE, and residual-based BDD.

IV. Problem Formulation

To identify voltage issues and determine the contribution of VR resources, the DSO needs to collect real-time PMU and EVCS data to perform DSSE. In practice, this data may not be obtained accurately or in a timely fashion. It is imperative to develop a method for estimating the VR capacity of each EVCS considering the randomness of the communication network, EV mobility and charging demand. In this section, we discuss how to incorporate these random variables in the VR scheme, and present the modified DSSE and BDD.

A. Voltage Regulation in Distribution System

We consider a balanced three-phase distribution network with the set of nodes defined as $\mathbf{N} = \{1, \cdots, N\}$. We denote the voltage magnitude, phase angle, active power injection, and reactive power injection of node n at time t by $\mathbf{V}_t = \{v_{n,t}\}$, $\boldsymbol{\theta}_t = \{\theta_{n,t}\}$, $\mathbf{P}_t = \{p_{n,t}\}$, $\mathbf{Q}_t = \{q_{n,t}\}$, respectively. Suppose there is a subset of nodes $\mathbf{E} = \{1, \cdots, E\} \subseteq \mathbf{N}$ where the connected load is an EVCS. An EVCS at node $e \in \mathbf{E}$ can provide up-regulation capacity of $p^U_{e,t}$ and down-regulation capacity of $p^D_{e,t}$ at time t. We use the VR model described in [24]. Specifically, the goal is to keep the average nodal voltage magnitude within an acceptable range $[v^{\min}, v^{\max}]$ around some reference voltage v^R and preferably close to v^R. Hence, the VR objective function is formulated as the squared deviation from the reference voltage averaged over all nodes:

$$\min_{\{p'_{e,t}|e\in\mathbf{E}\}} \frac{1}{N}\sum_{n=2}^{N}(v^R - v_{n,t})^2 \tag{1a}$$

$$s.t. \quad p_{e,t} - p'_{e,t} \le p^D_{e,t}, e \in \mathbf{E} \tag{1b}$$

$$p'_{e,t} - p_{e,t} \le p^U_{e,t}, e \in \mathbf{E} \tag{1c}$$

$$v^{\min} \le v_{n,t} \le v^{\max}, n \in \mathbf{N} \tag{1d}$$

$$\mathbf{V}_t, \boldsymbol{\theta}_t = \text{PFA}(\mathbf{P}_t, \mathbf{Q}_t), \tag{1e}$$

where $p'_{e,t}$ is the active power contribution of EVCS e when participating in VR, and $\text{PFA}(\cdot)$ represents the set of power flow equations. Notice that not all the variables that appear in this problem are known to the DSO when it attempts to solve it. For example, due to random packet losses in the communication network, the DSO may need to utilize pseudo measurements to replace measurements that are not yet received, i.e., $p_{n,t}, q_{n,t}$. Moreover, it is difficult to collect the state of charge and charging demand of every EV in the EVCS. Thus, estimating the VR capacity of each EVCS, i.e., $p^U_{e,t}$ and $p^D_{e,t}$, requires solving a state estimation problem after taking into account the randomness of the communication process and EV mobility, and incorporating these estimates in the VR scheme. To further improve the accuracy of the proposed VR scheme, the impact of EVCS location on VR efficiency is taken into account. Since charging stations might be connected to different nodes in the distribution network, two charging stations that offer the same up- and down-regulation capacities may contribute differently in the VR scheme. Thus, we need to quantify the VR capacity of an EVCS based on its effect on the voltage magnitude of node n, which is given by

$$\Delta v(n) = g^V_n(\mathbf{P}_t, \mathbf{Q}_t, \mathbf{P}^D_t, \mathbf{P}^U_t), \tag{2}$$

where $\mathbf{P}^D_t = \{p^D_{1,t}, \cdots, p^D_{E,t}\}$, $\mathbf{P}^U_t = \{p^U_{1,t}, \cdots, p^U_{E,t}\}$ are the sets of up- and down-regulation capacities of all EVCSs, $g^V(\cdot)$ is a function representing the maximum difference in the voltage magnitude of node n that could be caused when the full VR capacity of each EVCS is utilized. This function is derived from power flow equations. Hence, the total VR capacity in the distribution network can be defined as

$$\Delta v = \sum_{n\in\mathcal{E}} \Delta v(n), \tag{3}$$

where $\mathcal{E} \subseteq \mathbf{N}$ is a subset of nodes in the distribution network that suffer from voltage limit violation problems. These nodes are typically at the end of distribution feeders.

[1]A fraction of the revenue generated from the EVCS participation in VR can be distributed among EVs to incentivize them to let the EVCS use their battery for voltage regulation. But, this is outside the scope of this paper.

[2]The upper limit is imposed by the utility to avoid transformer overloading.

B. Stochastic Process for Characterizing the Number of EVs

Suppose EVCS e has L_e charging points and EVs arrive at this charging station following a Poisson process with rate λ_e. Hence, the probability of having one arrival in a time slot of length τ is $q_a = \lambda_e\tau + o(\tau)$ and the probability of no arrival in that time slot is $q'_a = 1-\lambda_e\tau+o(\tau)$. Suppose the EV charging times are independent and identically distributed exponential random variables with mean $1/\mu_e$. Hence, the probability of having one departure from a specific active charger (i.e., charge service completion) in a time slot is $q_d = \mu_e\tau + o(\tau)$, and the probability of no departure from that charger in that time slot is $q'_d = 1 - \mu_e\tau + o(\tau)$. Note that $o(\tau)$ terms are negligible compared to τ when τ is sufficiently small; thus, they are ignored (infinitesimal asymptotics) [25].

Let us denote the total number of charging and idling EVs in EVCS e by $c_{e,t} \leq L_e$. Hence, $\mathbf{C}_t = \{c_{1,t}, \cdots, c_{e,t}, \cdots, c_{E,t}\}$ is the set that contains the number of EVs that are in one of the E stations at time t. Assuming that there are $c_{e,t} = n$ EVs in EVCS e at t, we can derive the probability of having $n+i$ EVs in this EVCS at $t+1$ as follows:

$$P(c_{e,t+1} = n + i | c_{e,t} = n) = \tag{4}$$
$$\begin{cases} q_a {q'_d}^n & i = 1 \\ q'_a q_d^n & i = -n \\ \binom{n}{i} q'_a q_d^{-i} {q'_d}^{n+i} + \binom{n}{i+1} q_a q_d^{1-i} {q'_d}^{n+i-1} & -n < i < 1 \\ 0 & \text{otherwise} \end{cases}$$

where $\binom{n}{i}$ is a binomial coefficient. The DSO uses this probabilistic model to compute the most probable number of EVs in the EVCS, treated as the pseudo measurement, when it does not receive the real-time measurement of the respective EV counter by the time it performs DSSE.

Next we estimate the number of time slots in which an EV can participate in VR. Suppose an EV arrives at the EVCS at t with the initial SOC s^I, battery size e^B, charge (and discharge) power p^C, target SOC s^T and expected parking time t^P. The expected charging time for this EV would be:

$$t^C = \begin{cases} \frac{(s^T - s^I)e^B}{p^C}, & s^I < s^T \\ 0, & s^I \geq s^T \end{cases} \tag{5}$$

Naturally, EV owners seek to charge their battery to the target SOC before departure. Once the current SOC reaches the target SOC, the EVCS aggregator will be able to charge or discharge the EV battery to provide up- or down-regulation. In this case, the corresponding charge/discharge power contributes to the VR capacity of the EVCS. However, to compensate for the energy withdrawn from the EV battery in the VR scheme, the battery must be recharged to the target SOC before the EV departure. Thus, the number of time slots available for providing VR capacity are:

$$t^V = \begin{cases} \lfloor (t^P - t^C)/2 \rfloor, & t^C < t^P \\ 0, & t^C \geq t^P \end{cases}, \tag{6}$$

where $\lfloor \cdot \rfloor$ is the floor function. According to this expression, if the parking time t^P is smaller than t^C, there is not enough time for this EV to provide VR capacity. Otherwise, half of the remaining time can be effectively utilized for VR, assuming that the maximum charge and discharge power are the same. Note that if the time required to satisfy the energy demand of an EV is longer than its parking time, the EV will be charged until departure without providing any VR capacity. Since the expected charging time and parking, time are known in advance, the EVCS aggregator can opportunistically control the EV charging process. In other words, the t^V time slots can be utilized to provide the VR capacity when appropriate.[3]

The EVs that arrive at the EVCS can have various initial SOCs, battery sizes, and parking times. We denote the probability density function for the initial SOC and parking time by $f_S(\cdot)$ and $f_P(\cdot)$ respectively. Similarly, we denote the probability mass function for the battery size and maximum charge/discharge power by $\varrho_B(\cdot)$ and $\varrho_C(\cdot)$, respectively.

C. Stochastic Model for Data Transmission

In the ideal case, the DSO receives all sensor data on time, before it runs DSSE. However, due to the uncertainty of the communication network, packet losses might occur in the real world. When this happens, the DSO utilizes pseudo measurements in the DSSE process to replace the lost data. This suggests that the randomness of the communication process can directly influence the DSSE result. To build a practical VR scheme, a stochastic communication model is utilized in this paper. Suppose a total of U distribution-level PMUs are installed at nodes indexed by $\mathbf{U} = \{1, \cdots, U\}$ to monitor the voltage magnitude and phase angle. They send their measurements to the DSO at the end of each time slot, which are then used to carry out DSSE t time slots after the measurements are taken. The measurement packets that are not received by the control center after t time slots are deemed lost, and the respective pseudo measurements will be utilized in the DSSE process.

Following the Gilbert–Elliott model, we model changes in data transmission using a two-state Markov chain [26]. In this chain, the good state (G) represents successful transmission, and the bad state (B) represents unsuccessful transmission (i.e., the packet is not received after t time slots). The transition probability matrix of this chain is $\begin{bmatrix} 1-\kappa^{GB} & \kappa^{GB} \\ \kappa^{BG} & 1-\kappa^{BG} \end{bmatrix}$, where κ^{GB} is the probability of going from a good state to a bad state and κ^{BG} is the probability of going from a bad state to a good state. Thus, the stationary distribution of this Markov chain can be written as

$$\pi(G) = \frac{\kappa^{BG}}{\kappa^{GB} + \kappa^{BG}} \tag{7}$$

$$\pi(B) = \frac{\kappa^{GB}}{\kappa^{GB} + \kappa^{BG}}, \tag{8}$$

where $\pi(G)$ is the steady-state probability of being in a good state and $\pi(B)$ is the steady-state probability of being in a bad state. This implies that in the steady state, real-time PMU

[3]It might be the case that some EV owners only allow their battery to be used for VR after their original energy demand is supplied. In that case, the time slots available to provide the VR capacity are fixed. Even in that case, the method proposed in this work is applicable as discussed in Section V-B.

measurements are used in the DSSE process with probability $\pi(G)$ and pseudo measurements are used with probability $\pi(B) = 1 - \pi(G)$.

Based on the Gilbert-Elliott model, we can model the communication between sensors and the DSO control center as independent Markov processes. We use binary vectors $\boldsymbol{\phi}^U = [\phi_1^U, \cdots, \phi_U^U]$ and $\boldsymbol{\phi}^E = [\phi_1^E, \cdots, \phi_E^E]$ to collect the outcomes of data transmission in time slot t for all PMUs and EV counters. We use $\boldsymbol{\phi} = [\boldsymbol{\phi}^U, \boldsymbol{\phi}^E]^\top$ to compactly represent both vectors, the size of which is $U + E$.

D. DSSE with BDD

The DSSE problem concerns estimating the distribution system operating conditions given the measurement of a set of state variables [27], e.g., nodal voltage magnitude and phase angle, real and reactive power injection at nodes, and real and reactive power flow in branches. The relation between the measurement $\boldsymbol{z}$ and the system state $\boldsymbol{x}$ is given by:

$$\boldsymbol{z} = h(\boldsymbol{x}) + \boldsymbol{\varepsilon}, \tag{9}$$

where $h(\cdot)$ is a nonlinear function that relates the measurement to the system state, and $\boldsymbol{\varepsilon}$ is the measurement noise with covariance matrix $\boldsymbol{R}$. We note that $h(\cdot)$ depends on the distribution system structure and line parameters. Given $\boldsymbol{z}$, $h(\cdot)$, and $\boldsymbol{R}$, the system state $\boldsymbol{x}$ can be estimated by solving a weighted least squares (WLS) problem [28]:

$$\hat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x}} [\boldsymbol{z} - h(\boldsymbol{x})]^\top \boldsymbol{W} [\boldsymbol{z} - h(\boldsymbol{x})], \tag{10}$$

where $W = \text{diag}\{\boldsymbol{R}^{-1}\}$ and $[\cdot]^\top$ denotes matrix transposition. This optimization problem can be solved via an iterative approximation method, such as the Newton-Raphson method. However, nonlinearity of $h(\cdot)$ increases the computation overhead to a great extent. More importantly, its convergence cannot be guaranteed. Thus, this optimization problem is often simplified by linearizing the power flow equations. Consequently, $h(\cdot)$ is given by $h(\boldsymbol{x}) = \boldsymbol{H}\boldsymbol{x}$, where $\boldsymbol{H}$ is the measurement matrix obtained from the linearized power flow equations [29] (the Jacobian matrix can also be used). In this case, the estimate can be derived as follows:

$$\begin{aligned} \hat{\boldsymbol{x}} =& \arg\min_{\boldsymbol{x}} [\boldsymbol{z} - \boldsymbol{H}\boldsymbol{x}]^\top \boldsymbol{W} [\boldsymbol{z} - \boldsymbol{H}\boldsymbol{x}] \\ =& (\boldsymbol{H}^\top \boldsymbol{W} \boldsymbol{H})^{-1} \boldsymbol{H}^\top \boldsymbol{W} \boldsymbol{z}. \end{aligned} \tag{11}$$

In this context, the residual can be defined as the difference between the actual measurement $\boldsymbol{z}$ and the measurement that corresponds to the estimated system state, i.e., $\hat{\boldsymbol{z}} = \boldsymbol{H}\hat{\boldsymbol{x}}$. Then, by comparing the Euclidean norm of the residual $\boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}}$ against a threshold ϵ, false data or erroneous measurement can be detected following a residual-based BDD mechanism (if $\|\boldsymbol{r}\|_2 > \epsilon$). Otherwise, the estimated system state $\hat{\boldsymbol{x}}$ can be trusted. The value of ϵ is typically determined by a hypothesis test $\text{P}(\|\boldsymbol{r}\|_2 > \epsilon) < \tau$, where τ is the significance level.

In the VR scheme, the real-time system state is defined as $\boldsymbol{x} = [\mathbf{P}_t, \mathbf{Q}_t, \mathbf{P}_t^D, \mathbf{P}_t^U]^\top$ and the measurement vector is denoted by $\boldsymbol{z} = [\mathbf{V}_t, \boldsymbol{\theta}_t, \mathbf{C}_t]^\top$. The vectors $\mathbf{V}_t$, $\boldsymbol{\theta}_t$, and $\mathbf{C}_t$ collect real-time measurements and pseudo measurements according to the communication result.

V. Stochastic FDIA on Voltage Regulation

In the previous section, we augmented the system state with the variables that are necessary for VR, namely up-regulation capacity, down-regulation capacity, and EV counts. Given this new definition, a modified DSSE framework would be needed for the DSO to estimate the system states. In this section, we first develop an optimization-based method for FDIA vector construction assuming an idealized communication model. We then present a new framework for DSSE that takes the VR variables into account. Based on this framework, we formulate an optimization problem for FDIA vector construction under a stochastic communication model.

A. FDIA against VR under Idealized Communication Model

Under the idealized communication model, sensor data is guaranteed to be received before running DSSE, hence pseudo measurements are never used. In this case, the attacker's objective to perturb measurements such that the adverse impact on the distribution network is maximized. We define the impact of an FDIA by comparing the VR capacity in the network before and after this attack, given by

$$\psi_{\boldsymbol{\phi}}(\boldsymbol{\alpha}) = \Delta v_{\boldsymbol{\phi}}^A - \Delta v_{\boldsymbol{\phi}}, \tag{12}$$

where $\boldsymbol{\phi}$ is a 1-vector here because all packets must be received on time under the idealized model, $\Delta v_{\boldsymbol{\phi}}$ is defined in (3), and $\Delta v_{\boldsymbol{\phi}}^A$ is the same quantity under FDIA. The optimal FDIA vector can be determined by solving the optimization problem below:

$$\max_{\boldsymbol{\alpha}} \ \psi_{\boldsymbol{\phi}}(\boldsymbol{\alpha}) \tag{13a}$$

$$s.t. \ \ \boldsymbol{z}^A = \boldsymbol{z} + \boldsymbol{\alpha} \tag{13b}$$

$$\hat{\boldsymbol{x}}^A = \Omega \boldsymbol{z}^A \tag{13c}$$

$$\boldsymbol{r}^A = \boldsymbol{z}^A - \mathbf{H}\hat{\boldsymbol{x}}^A \tag{13d}$$

$$\|\boldsymbol{r}^A\|_2 \leq \epsilon \tag{13e}$$

$$z^{\min} \leq z \leq z^{\max} \qquad \forall z \in \boldsymbol{z}^A \tag{13f}$$

Here $\boldsymbol{\alpha}^U = [\alpha_1^U, \cdots, \alpha_U^U]$ and $\boldsymbol{\alpha}^E = [\alpha_1^E, \cdots, \alpha_E^E]$ are the attack vectors concerning PMUs and EV counters (in charging stations); $\boldsymbol{\alpha} = [\boldsymbol{\alpha}^U, \boldsymbol{\alpha}^E]^\top$ is the combined attack vector; $\boldsymbol{z}^A$ represents the modified measurements; the range $[z^{\min}, z^{\max}]$ is the range of valid measurement values of each sensor; $\Omega = (\mathbf{H}^\top \boldsymbol{W} \mathbf{H})^{-1} \mathbf{H}^\top \boldsymbol{W}$ is the estimation matrix obtained from (11). The objective function is linear because we have linearized the power flow equations (similar to [29]) and estimation function.

B. Modified DSSE with VR Variables

Conventionally in DSSE, $h(\cdot)$ is obtained through power flow analysis to calculate the voltage magnitude and phase angle measurements given the real and reactive loads. But when the VR variables are added to the state, a new function must be derived to estimate the VR capacity according to the extended system state, i.e., $\boldsymbol{z} = [\mathbf{V}_t, \boldsymbol{\theta}_t, \mathbf{C}_t]^\top$. In this section, we first obtain the inverse of $h(\cdot)$ which relates the EV counts

to VR capacity. Knowing the inverse function, we derive $h(\cdot)$ at the end of this section.

Suppose one EV is parked at stall ℓ in EVCS e in time slot t. This EV can be represented using a vector $[t_0, t^P, t^C, s^I, p^C, b^E]$, where $t_0 \leq t$ is the arrival time slot and we have a constraint that $t - t_0 \leq t^P$. Given $p_{e,t}$, which denotes the active load of EVCS e obtained from the power flow analysis, we can estimate the expected number of charging EVs in this station at time t (see Section II-B):

$$c^C_{e,t} = \frac{p_{e,t}}{\sum_{\forall p^C} p^C \cdot \varrho_C(p^C)}. \tag{14}$$

Accordingly, the expected number of idling EVs in this station can be calculated from $c^I_{e,t} = c_{e,t} - c^C_{e,t}$.

If up-regulation capacity is needed when an EV is being charged and this EV has sufficient laxity (i.e., $t^P > T^C$), it can stop charging and immediately discharge its battery to provide the up-regulation capacity of $2\,p^C$ (since it will discharge at p^C instead of charging at p^C) and continue charging afterwards. Otherwise, no VR capacity can be provided. Besides, an idling EV with charging demand satisfied can provide both up- and down-regulation capacity:

$$p^U_{e,\ell,t} = \begin{cases} 2\,p^C, & t^P > t^C, \quad \text{charging EV} \\ p^C, & t^P > t - t_0, \quad \text{idling EV} \\ 0, & \text{otherwise} \end{cases} \tag{15}$$

$$p^D_{e,\ell,t} = \begin{cases} p^C, & s^I + p^C \Delta t \leq s^T, \quad \text{idling EV} \\ 0, & \text{otherwise} \end{cases} \tag{16}$$

where the condition $t^P > t - t_0$ ensures there is enough time to compensate the discharged energy, and the condition $s^I + p^C \Delta t \leq s^T$ ensures the EV is not fully charged.

Given the probability density and mass functions, i.e., $f_S(\cdot)$, $\varrho_B(\cdot)$, $\varrho_C(\cdot)$, and $f_P(\cdot)$, we can derive the cumulative distribution function of t^C and t^V. Then, the expected VR capacity of an EV can be derived based on the conditional probabilities as follows:

$$\bar{p}^{ID}_{e,\ell,t} = p^C \frac{P(t^C < t - t_0, s^I + p^C \Delta t \leq s^T)}{P(t^C < t - t_0)}, \tag{17}$$

$$\bar{p}^{CD}_{e,\ell,t} = 0, \tag{18}$$

$$\bar{p}^{IU}_{e,\ell,t} = p^C \frac{P(t^V > 0, t^C < t - t_0)}{P(t^C < t - t_0)}, \tag{19}$$

$$\bar{p}^{CU}_{e,\ell,t} = p^C \frac{P(t^V > 0, t^C < t - t_0)}{P(t^C < t - t_0)} + 2p^C \frac{P(t^V > 0, t^P > t^C \geq t - t_0)}{P(t^C < t - t_0)}. \tag{20}$$

where $\bar{p}^{ID}_{e,\ell,t}$ and $\bar{p}^{IU}_{e,\ell,t}$ represent the down- and up-regulation capacities of an idling EV, and $\bar{p}^{CD}_{e,\ell,t}$ and $\bar{p}^{CU}_{e,\ell,t}$ represent the same quantities for a charging EV. Putting it all together, the total VR capacity of an EVCS can be estimated using a linear function of the total number of charging and idling EVs in that station:

$$\bar{p}^D_{e,t} = \bar{p}^{ID}_{e,\ell,t} c^I_{e,t} + \bar{p}^{CD}_{e,\ell,t} c^C_{e,t}, \tag{21}$$

$$\bar{p}^U_{e,t} = \bar{p}^{IU}_{e,\ell,t} c^I_{e,t} + \bar{p}^{CU}_{e,\ell,t} c^C_{e,t}. \tag{22}$$

Recall that the voltage magnitude and phase angle of each node can be calculated given the linear power flow equations. Thus, the inverse of $h(\cdot)$ is a linear function of measurement z, and can be written in matrix form. This enables us to write $h(\cdot)$ in matrix form too.

C. FDIA against VR under Stochastic Communication Model

Due to stochastic packet drops in the communication network, measurement data sent by PMUs may not be received by the DSO when it attempts to run DSSE, causing the respective pseudo measurements to be used instead. Let us denote the measurement vector utilized by the DSO in DSSE by

$$\boldsymbol{z}^R = \boldsymbol{\phi}\boldsymbol{z} + (\mathbf{1} - \boldsymbol{\phi})\boldsymbol{z}^P, \tag{23}$$

where $\mathbf{1}$ is the 1-vector, $\boldsymbol{\phi}$ is a binary vector that indicates sensor measurements that are successfully received by the DSO, and $\boldsymbol{z}^P$ is the pseudo measurement vector. Similarly, we define the measurement utilized in DSSE when FDIA is performed as follows:

$$\boldsymbol{z}^{AR} = \boldsymbol{\phi}\boldsymbol{z}^A + (\mathbf{1} - \boldsymbol{\phi})\boldsymbol{z}^P. \tag{24}$$

We write the joint probability distribution of the communication results as

$$P(\boldsymbol{\phi}) = \prod_{\{i|\boldsymbol{\phi}_i=1\}} \pi(G) \prod_{\{j|\boldsymbol{\phi}_j=0\}} \pi(B), \tag{25}$$

and the probability of receiving measurement vector $\boldsymbol{z}^R$ as

$$P(\boldsymbol{z}^R) = \sum_{\{\boldsymbol{\phi}|\boldsymbol{z}^R=\boldsymbol{\phi}\boldsymbol{z}+(\mathbf{1}-\boldsymbol{\phi})\boldsymbol{z}^P\}} P(\phi). \tag{26}$$

Hence, the probability of obtaining a state estimate $\hat{\boldsymbol{x}}$ from DSSE given the measurement $\boldsymbol{z}^R$ is

$$P(\hat{\boldsymbol{x}}) = \sum_{\{\boldsymbol{z}^R|\Omega\boldsymbol{z}^R=\hat{\boldsymbol{x}}\}} P(\boldsymbol{z}^R), \tag{27}$$

and the corresponding residual is

$$\boldsymbol{r} = \boldsymbol{z}^R - \hat{\boldsymbol{z}} = \boldsymbol{z}^R - \mathbf{H}\Omega\boldsymbol{z}^R. \tag{28}$$

Finally, the probability distribution over the residuals would be given by

$$P(\boldsymbol{r}) = \sum_{\{\boldsymbol{z}^R|\boldsymbol{z}^R-\mathbf{H}\Omega(\boldsymbol{z}^R)=\boldsymbol{r}\}} P(\boldsymbol{z}^R). \tag{29}$$

Recall that the total VR capacity can be calculated in terms of voltage magnitude differences according to (3). The up- and down-regulation capacities themselves are linear functions of EV counts as shown in (21) and (22). Thus, the Δv term in (3) is a linear function of the DSSE result, $\hat{\boldsymbol{x}}$, and can be written as $\Delta v = \mathcal{V}\Omega\boldsymbol{z}$, where $\mathcal{V}$ can be derived from (3), (21), and (22). This yields a probability distribution over the VR capacity $P(\Delta v) = \sum_{\{\hat{\boldsymbol{x}}|\hat{\boldsymbol{x}}=\Delta v\}} P(\hat{\boldsymbol{x}})$. Following the same approach, we can obtain the DSSE result given an attack vector $\boldsymbol{\alpha}$. We add A to the subscript to mark the variables related to FDIA.

We formulate an optimization problem for the FDIA vector construction under the stochastic communication model as

follows:

$$\max_{\boldsymbol{\alpha}} \Psi(\boldsymbol{\alpha}) \tag{30a}$$

$$s.t. \quad \Psi(\boldsymbol{\alpha}) = \sum_{\{\boldsymbol{\phi}\}} \eta_{\boldsymbol{\phi}}(\boldsymbol{\alpha}) P(\Delta v_{\boldsymbol{\phi}}^{A}) \psi_{\boldsymbol{\phi}}(\boldsymbol{\alpha}) \tag{30b}$$

$$\hat{\boldsymbol{x}}_{\boldsymbol{\phi}}^{A} = \Omega \boldsymbol{z}_{\boldsymbol{\phi}}^{AR} \qquad \forall \boldsymbol{\phi} \tag{30c}$$

$$\Delta v_{\boldsymbol{\phi}}^{A} = \mathcal{V} \hat{\boldsymbol{x}}_{\boldsymbol{\phi}}^{A} \qquad \forall \boldsymbol{\phi} \tag{30d}$$

$$\boldsymbol{r}_{\boldsymbol{\phi}}^{A} = \boldsymbol{z}_{\boldsymbol{\phi}}^{AR} - \mathbf{H} \hat{\boldsymbol{x}}_{\boldsymbol{\phi}}^{A} \qquad \forall \boldsymbol{\phi} \tag{30e}$$

$$\eta_{\boldsymbol{\phi}} = \begin{cases} 1, & \|\boldsymbol{r}_{\boldsymbol{\phi}}^{A}\|_2 \leq \epsilon \\ 0, & \text{otherwise} \end{cases} \qquad \forall \boldsymbol{\phi} \tag{30f}$$

$$z \in [z^{\min}, z^{\max}], \qquad \forall z \in \boldsymbol{z}^{AR} \tag{30g}$$

where $\eta_{\boldsymbol{\phi}}(\boldsymbol{\alpha})$ is the BDD result associated with attack vector $\boldsymbol{\alpha}$ and communication result $\boldsymbol{\phi}$. The optimal point of this problem is the attack vector that has the largest expected adverse impact on VR. Notice that, for a specific communication result $\boldsymbol{\phi}$, $P(\Delta v_{\boldsymbol{\phi}}^{A})$ is constant and $\psi_{\boldsymbol{\phi}}(\boldsymbol{\alpha})$ is a linear function of the attack vector $\boldsymbol{\alpha}$. Since $\eta_{\boldsymbol{\phi}}$ depends on both the attack vector $\boldsymbol{\alpha}$ and the communication result vector $\boldsymbol{\phi}$, all possible combinations of BDD results must be taken into consideration when solving this problem[4]. For example, in a distribution network with $E+U$ sensors, including PMUs and EV counters, there are 2^{E+U} possible communication results, each resulting in a specific $\boldsymbol{z}^{AR}$. As a result, there are $2^{2^{E+U}}$ possible BDD results (i.e., $\boldsymbol{\eta}$ vectors) because each $\boldsymbol{z}^{AR}$ either passes BDD or it does not.

Observe that the objective function $\Psi(\boldsymbol{\alpha})$ of (30) is the weighted sum of several $\psi_{\boldsymbol{\phi}}(\boldsymbol{\alpha})$ terms, each being similar to the objective function of (13) but for a specific $\boldsymbol{\phi}$. Thus, if the values of $\eta_{\boldsymbol{\phi}}(\boldsymbol{\alpha})$ elements are fixed, the objective function $\Psi(\boldsymbol{\alpha})$ becomes a linear function of $\boldsymbol{\alpha}$ and (30f) can be converted to an inequality constraint for each ϕ in the form of $\|\boldsymbol{r}_{\boldsymbol{\phi}}^{A}\|_2 \leq \epsilon$. Thus, the feasible set is the intersection of 2^{E+U} ellipsoids which are obtained by squaring the constraints. Hence, for each vector $\boldsymbol{\eta}$, the optimization problem is a convex quadratically constrained linear program (QCLP). It can be further shown that this QCLP is a special case of a second order cone program (SOCP) and can therefore be solved efficiently by an interior point method [30].

Algorithm 1 describes how (30) is solved by iterating over the set of $\boldsymbol{\eta}$ vectors and solving the resulting QCLP in each case. The maximum adverse impact $\Psi(\boldsymbol{\alpha})$, attained at the solutions of these problems, determines the solution of the original stochastic optimization problem. Note that in Line 4, we check whether the feasible set is empty and discard η if it is the case. This is because an empty feasible set indicates that no attack vector can lead to this specific combination of BDD results under an arbitrary communication result.

VI. Case Studies

In our case study we use an open-source co-simulation platform described in [36] to simulate the VR scheme involving stochastic communication, DSSE, and BDD. In this platform,

[4]Each possible combination of BDD results is a unique binary vector $\boldsymbol{\eta} = \{\eta_{\boldsymbol{\phi}}\}_{\forall \boldsymbol{\phi}}$, which results in a different objective function.

Algorithm 1: FDIA Vector Construction

Input: $\mathbf{H}$, $\mathbf{W}$, $\boldsymbol{z}$, $\boldsymbol{z}^{P}$, Ω, $\mathcal{V}$, ϵ, $\pi(G)$, $\pi(B)$
Output: $\boldsymbol{\alpha}^{*}$

1 $\alpha_{\boldsymbol{\eta}}^{*} \leftarrow 0$ **for** *each vector* $\boldsymbol{\eta}$ **do**
2 Solve the respective convex QCLP;
3 **if** *Optimal point (denoted* $\boldsymbol{\alpha}_{\boldsymbol{\eta}}'$*) exists* ***and*** $\Psi(\boldsymbol{\alpha}_{\boldsymbol{\eta}}') > \Psi(\boldsymbol{\alpha}_{\boldsymbol{\eta}}^{*})$ **then**
4 $\boldsymbol{\alpha}_{\boldsymbol{\eta}}^{*} \leftarrow \boldsymbol{\alpha}_{\boldsymbol{\eta}}'$;
5 **end**
6 **end**
7 Return $\boldsymbol{\alpha}_{\boldsymbol{\eta}}^{*}$

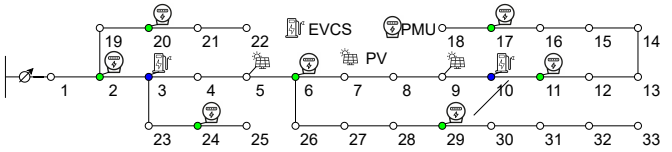

Fig. 2. IEEE 33-bus test feeder topology

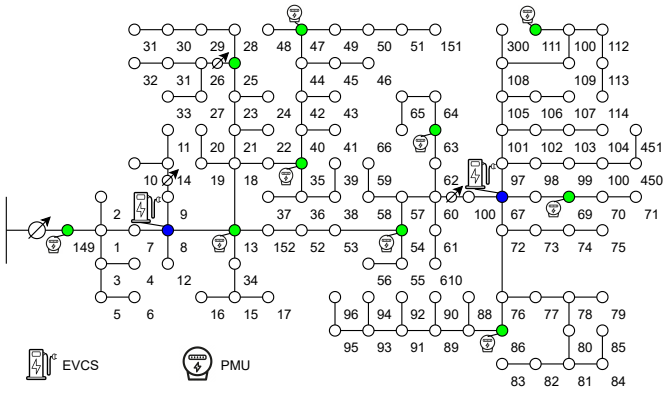

Fig. 3. IEEE 123-bus test feeder topology

OpenDSS is utilized for power flow analysis and a network simulator component is used to capture the communication bit error rate. The bit error rate is set to 0.01, the communication involves small frames with a payload of 32 bits, and framing overhead is considered negligible. The communication network topology is assumed to be a star, with the DSO at the center of the star.

To investigate the impact of stochastic communication on the FDIA performance and the vulnerability of the distribution system VR scheme to this attack, we evaluate the proposed FDIA on the IEEE 33-bus test feeder [31] and a simplified version of the IEEE 123-bus test feeder [32]. Fig. 2 and 3 depict where charging stations and distribution-level PMUs are installed in these systems.

There are 2 charging stations in each distribution system, each station is equipped with an EV counter. It is assumed that EV counters send their readings to the DSO via the same communication network that is used to transmit PMU data. We use real data to generate the initial SOC, charging demand, and parking time of EVs that visit an EVCS. Specifically, the charging demand is approximated based on the product

of trip distance, in the NHTS dataset [38], and the average energy consumption per mile together with the battery size and corresponding maximum driving mileage are obtained from [39]. The charging power and parking times are pulled from the EVnetNl dataset [40]. A log-normal distribution with expected value of 0.6848 and standard deviation of 0.9353 is fitted to the empirical distribution of parking times. The charging power is divided into 23 discrete levels from 1 to 23 kW, and the empirical probability mass function is obtained from the dataset. The initial SOC of EVs is generated given the battery size and daily trips. In each EVCS, 50 parking stalls are assumed to be equipped with bidirectional chargers that support (dis)charge powers ranging from 1 to 23 kW.

To evaluate the proposed FDIA in under-voltage and over-voltage scenarios, we add two photovoltaic (PV) systems to the IEEE 33-bus test feeder as shown in Fig.2. They are connected to Bus 5 and Bus 9, respectively. The solar generation data is obtained from the NREL dataset [37]. To guarantee accurate state estimation, the minimum number of PMUs should be between 1/5 and 1/3 of the total number of buses [33]. Thus, we consider a total of 7 PMUs in IEEE 33-bus test feeder and 10 PMUs in the simplified IEEE 123-bus test feeder. The pseudo measurement of PMUs can be obtained from the historical data if needed. The pseudo measurement of EVCS counters are obtained from the EVCS queuing model presented in Section IV-B. Following [22], we set the error of magnitude and phase angle measurements to be an additive white Gaussian noise, $N(0, 0.01)$ and $N(0, 0.005)$, respectively. The base loads and PMU pseudo measurements are generated according to [34], and the pseudo measurement error is assumed to be an additive white Gaussian noise $N(0, 0.09)$ [35].

We run our experiments on a laptop computer with an Intel Core i7-10875 CPU @2.30GHz. We use CVX [41] to model and solve Problem (30). The average time to solve the optimization problem for each time slot is respectively 17.68 and 57.79 seconds in IEEE 33-bus and 123-bus test feeders.

In the first case study, we compare the efficacy of FDIA with idealized communication (IC) model [20] with the proposed FDIA with stochastic communication (SC) in the IEEE 33-bus test feeder, where an attack vector is computed in every time slot (10 min) and the total duration of our simulation is one day. Fig. 4 shows the VR estimation error caused by the FDIA vectors that bypass the BDD. The VR estimation error is not drawn when the FDIA does not bypass BDD. We can see that FDIAs can cause a noticeable VR capacity estimation error, i.e., $\psi(\boldsymbol{\alpha})$. Compared to FDIA with IC, the proposed FDIA (with SC) can effectively mislead the DSO, resulting in similar VR capacity estimation errors with higher BDD pass rate.[5] In particular, the FDIA with SC increases the mean absolute percentage error (MAPE) of the VR capacity estimation to 427% and the FDIA with IC increases it to 433%, which is slightly higher but results in a much higher detection rate.

In addition to the increased VR capacity estimation error, the negative impact of FDIAs on the voltage profiles is also more pronounced. As shown in Fig. 5, both constructed FDIA vectors can result in under-voltage incidents (voltage dropping below $0.95pu$). This is while there is no under-voltage incidents without FDIA because the DSO can accurately estimate the EVCS VR capacity and the insufficient capacity is met by other VR resources. However, the DSO issues an erroneous VR request under FDIA. Since the EVCS VR capacity is

[5]There are many more blue markers than red markers which indicates that more attack vectors did not pass BDD in the case of FDIA with IC.

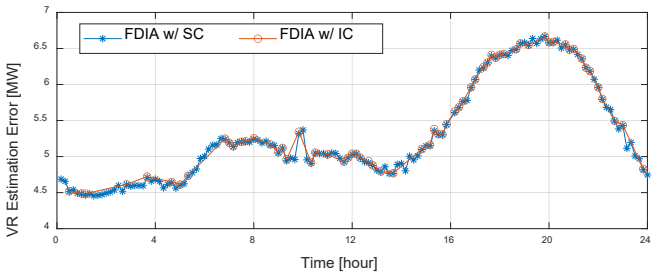

Fig. 4. Comparison of VR capacity estimation error in the IEEE 33-bus system. Note that a dot/marker is drawn only when the attack vector bypasses BDD.

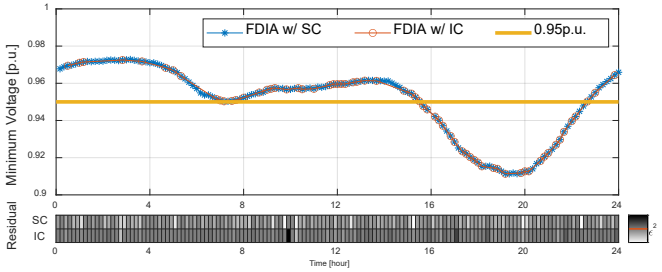

Fig. 5. Comparison of minimum voltage magnitude and BDD pass rate in the IEEE 33-bus system. The heatmaps below this figure show the value of $\|\boldsymbol{r}_{\boldsymbol{\phi}}^{\boldsymbol{A}}\|_{\boldsymbol{2}}^{\boldsymbol{2}}$ and the horizontal (red) line in the colorbar marks the color intensity of $\boldsymbol{\epsilon^2}$. Thus, any point that is painted with a lighter gray color corresponds to an attack that has bypassed BDD.

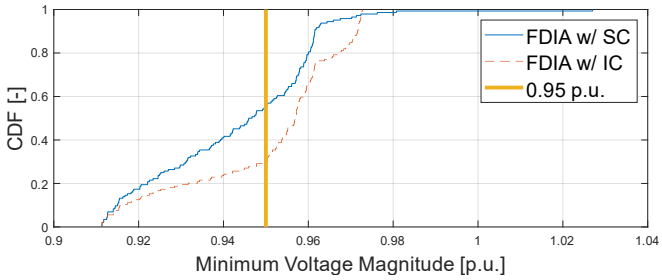

Fig. 6. Cumulative distribution function of the minimum voltage magnitude in the IEEE 33-bus system.

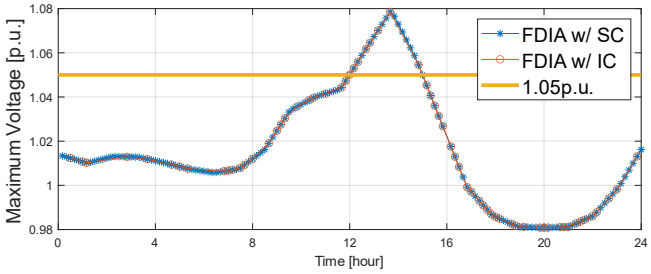

Fig. 7. Comparison of maximum voltage magnitude in the IEEE 33-bus system.

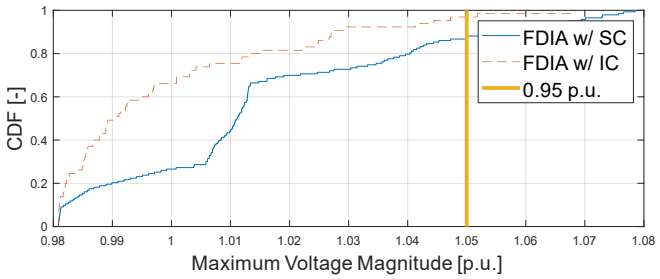

Fig. 8. Cumulative distribution function of the maximum voltage magnitude in the IEEE 33-bus system.

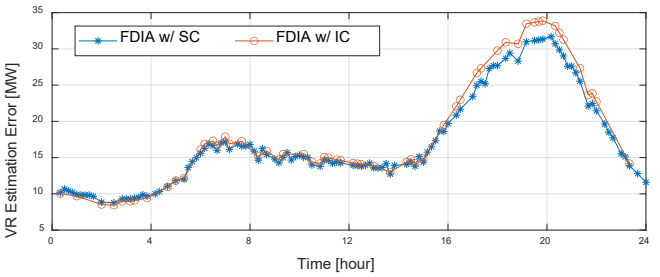

Fig. 9. Comparison of VR capacity estimation error in the IEEE 123-bus system. Note that a dot/marker is drawn only when the attack vector bypasses BDD.

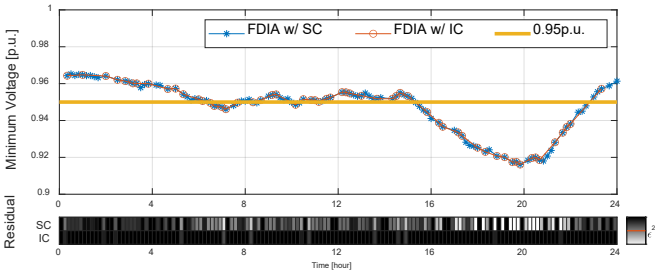

Fig. 10. Comparison of minimum voltage magnitude and BDD pass rate in the IEEE 123-bus system. The heatmaps below this figure show the value of $\|\boldsymbol{r}_{\phi}^{\boldsymbol{A}}\|_{\boldsymbol{2}}^{\boldsymbol{2}}$ and the horizontal (red) line in the colorbar marks the color intensity of $\boldsymbol{\epsilon^2}$. Thus, any point that is painted with a lighter gray color corresponds to an attack that has bypassed BDD.

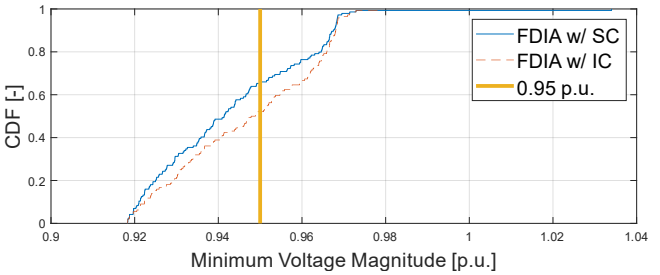

Fig. 11. Cumulative distribution function of the minimum voltage magnitude in the IEEE 123-bus system.

overestimated and the actual VR capacity is not enough to satisfy the VR request, serious damages can be inflicted on the power system. Moreover, considering the randomness of the communication process, the proposed FDIA with SC causes 41 under-voltage incidents during one day, which is approximately twice the number of incidents seen in the case of FDIA with IC. This can be attributed to the higher number of modified measurements that manage to go past BDD as can be seen in the bottom subplot of Fig. 5 (the two heatmaps). Recall that not all injected false data can be received by the DSO in time for VR optimization due to the stochastic packet drops that occur in the communication network. Thus, the attack vector that bypasses BDD mechanisms in theory might be actually detected. By considering the packet drop probability, the proposed FDIA can increase the BDD pass rate from 45% to 99.3% (i.e., one under-voltage incident in 144 time slots); this greatly increases the stealthiness of FDIA. We conclude from Fig. 6 that the proposed FDIA is more likely to create under-voltage incidents than FDIA with IC. Next, we consider the over-voltage scenario in the IEEE 33-bus test feeder, where the power generated by the PVs is so high that the local voltage magnitude exceeds the upper limit. As shown in Fig. 7, both constructed FDIA vectors can cause over-voltage incidents (voltage rising above 1.05pu). In both cases, the attacker misleads the DSO into overestimating the down-regulation capacity of EVCSs; thus, the insufficient VR capacity leads to the over-voltage incidents. Nevertheless, thanks to the use of the stochastic communication model, the BDD pass rate of the proposed FDIA is higher. Consequently, the proposed FDIA can cause over-voltage incidents with a higher probability, which is indicated in Fig. 8.

We now turn our attention to the case study that involves the IEEE 123-bus test feeder. The goal is to show that in a large distribution system, the performance of the proposed FDIA does not fall apart. As it can be seen in Fig. 9, the MAPE of VR capacity estimation caused by FDIA with SC is 674%, which is on par with the 691% relative error caused by FDIA with IC. We witness that FDIA with IC results in a higher error than FDIA with SC (especially from 16:00 to 22:00), but this comes at the cost of being detected more often. As shown in Fig. 10, the FDIA with IC causes 26 under-voltage incidents, while the proposed FDIA causes 47 incidents. By inspecting the BDD pass ratio and the corresponding under-voltage incidents, it is evident that the attacker can also achieve a better performance when it accounts for the stochasticity of the communication network. The greater potential of the proposed FDIA to cause more detrimental under-voltage incidents in larger distribution systems is also depicted in Fig. 11.

VII. Conclusion and Future Work

We presented an efficient VR scheme that takes advantage of the estimated VR capacity of charging stations that have V2G support and are connected to buses in the distribution network. We then proposed a novel FDIA against this VR scheme, which considers potential delays and packet losses in the communication network and the stochastic mobility pattern and charging demand of an EV fleet, to maximize its expected adverse impact on the distribution system over time. We carried out simulation on two standard test feeders using a co-simulation platform to showcase the greater potential of this FDIA to inflict damage compared to the state-of-the-art FDIA attack that relies on an idealized communication model. Our result highlights the vulnerability of the existing BDD mechanism that protects the DSSE process.

In future work, we intend to develop a new BDD mechanism to address this vulnerability. The DSO can consider various communication results in a network simulator to decide if the received measurement can be trusted. For example, the DSO can utilize redundant measurements and randomly replace the real-time measurements with pseudo measurements. Hence, the measurements used for DSSE are different from the attacker's estimate based on communication randomness. This can help to improve the detection rate and complicate the attack vector construction process, thereby preventing the attacker from solving it in a timely fashion. We also plan to develop a probabilistic model for the participation of EVs as economic resources in the VR scheme. This model will capture the battery degradation cost and incorporate incentives that will be provided to individual EVs to participate in VR.

REFERENCES

[1] L. Leon et al., "Devices and control strategies for voltage regulation under influecnce of photovoltaic distributed generation. a review," *IEEE Latin Am. Trans.*, vol. 20, no. 5, pp. 731-745, Jan. 2022.

[2] H. Sun et al., "eview of challenges and research opportunities for voltage control in smart grids," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp.2790-2801, Feb. 2019.

[3] J. Lai et al., "Distributed voltage regulation for cyber-physical microgrids with coupling delays and slow switching topologies," *IEEE Trans. Syst. Man Cybern. -Syst.*, vol. 50, no. 1, pp. 100-110, Jul. 2019.

[4] S. Wang et al., "Deep reinforcement scheduling of energy storage systems for real-time voltage regulatio in unbalanced LV networks with high PV penetration," *IEEE Trans. Sustain. Energy*, vol. 12, no. 4, pp. 2342-2352, Oct. 2021.

[5] F. Bai et al., "An excessive tap operation evaluation approach for unbalanced distribution networks with high PV penetration," *IEEE Trans. Sustain. Energy*, vol. 12, no. 1, pp. 169–178, Jan. 2021.

[6] S. Amamra and J. Marco, "Vehicle-to-grid aggregator to support power grid and reduce electric vehicle charging cost," *IEEE Access*, vol. 7 , pp. 178528 – 178538, Dec. 2019.

[7] "Global EV Outlook 2020," *Int. Energy Agency*, Paris, France, Rep., Jun. 2020. [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2020.

[8] M. Rahman et al., "A vehicle-to-microgrid framework with optimization-incorporated distributed EV coordination for a commercial neighborhood," *IEEE Trans. Ind. Inform.*, vol. 16, no. 3, pp. 1788-1798, Mar. 2020.

[9] K. Reddy and S. Meikandasivam, "Load flattening and voltage regulation using plug-in electric vehicle's storage capacity with vehicle prioritization using ANFIS," *IEEE Trans. Sustain. Energy*, vol. 11, no. 1, pp. 260-270, Jan. 2020.

[10] A. Bilh, K. Naik, and R. Ei-Shatshat, "Evaluating electric vehicles' response time to regulation signals in smart grids," *IEEE Trans. Ind. Inform.*, vol. 14, no. 3, pp. 1210-1219, Mar. 2018.

[11] "Literature review on false data injection attack against power system," in *Prof. IEEESoutheastCon'20*, pp. 1-5, Mar. 2020.

[12] X. Cai et al., "Review of cyber-attacks and defense research on cyber physical power systems," in *Proc. IEEE iSPEC'19*, pp. 487-492, Nov. 2019.

[13] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 21-32, Jun. 2011.

[14] G. Liang et al., "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317-3318, Jul. 2017.

[15] S. Sahoo et al., "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.,* vol. 34, no. 8, pp. 8162-8174, Nov. 2018.

[16] N. Bhusal et al., "Detection of cyber attacks on voltage regulation in distribution systems using machine learning," *IEEE Access*, vol. 9, pp. 40402-40416, Mar. 2021.

[17] M. Habib et al., "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 9, no. 5, pp. 5294-5310, Jan. 2020.

[18] X. Yin, Y. Zhu, and J. Hu, "A subgrid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids," *IEEE Trans. Ind. Inform.*, vol. 18, no. 3, pp. 1957-1968, Mar. 2022.

[19] M. Jorjani, H. Seifi, and A. Varjani, "A graph theory-based approach to detect false data injection attacks in power system AC state estimation," *IEEE Trans. Ind. Inform.*, vol. 18, no. 3, pp. 2465-2476, Apr. 2021.

[20] D. Choeum and D. Choi, "OLTC-induced false data injection attack on Volt/VAR optimization in distribution systems," *IEEE Access*, vol. 7, pp. 34508-34520, Mar. 2019.

[21] Y. Isozaki et al., "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1824-1835, Jul. 2016.

[22] P. Zhuang and H. Liang, "False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2566-2577, May. 2021.

[23] A. Abbaspour et al., "Resilient control design for load frequency control system under false data injection attacks," *IEEE Trans. Ind. Electron.*, vol. 67, no. 9, pp. 7951–7962, Sep. 2020.

[24] K. Mehmood et al., "A real-time optimal coordination scheme for the voltage regulation of a distribution network including an OLTC, capacitor banks, and multiple distributed energy resources," *Int. J. Electr. Power Energy Syst.*, vol. 94, pp. 1-14, Jan. 2018.

[25] Shortle, John F., et al., *Fundamentals of queueing theory*, 4th ed. John Wiley & Sons, 2018.

[26] D. Ding et al., "Recursive secure filtering over Gilbert-Elliot channels in sensor networks: the distributed case," *IEEE Trans. Signal Inf. Proc. Netw.*, vol. 7, pp. 75-86, Dec. 2020.

[27] P. Zhuang, R. Deng, and H. Liang, "False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6000-6013, Nov. 2019.

[28] C. Liu et al., "Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1468-1478, Mar. 2020.

[29] H. Yuan et al., "Novel linearized power flow and linearized OPF models for active distribution networks with application in distribution LMP," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 438-448, Jan. 2018.

[30] S. Boyd and S. P. Boyd, "Convex optimization," Cambridge University, Mar. 2004.

[31] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Tran. Power Deliv.*, vol. 4, no. 2, pp. 1401-1407, Apr. 1989.

[32] S. Bolognani and S. Zampieri, "On the existence and linear approximation of the power flow solution in power distribution networks," *IEEE Trans. Power Syst.*, vol. 31, no. 1, pp. 163-172, Jan. 2016.

[33] T. Baldwin et al., "Power system observability with minimal phasor measurement placement," *IEEE Trans. Power Syst.*, vol. 8, no. 2, pp. 707-715, May 1993.

[34] E. Wilson, "Commercial and residential hourly load profiles for all TMY3 locations in the United States," National Renewable Energy Laboratory, Nov. 2014. [Online]. Available: https://data.openei.org/submissions/153.

[35] R. Singh, B. Pal, and R. Vinter, "Measurement placement in distribution system state estimation," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 668-675, May 2009.

[36] E. Souza, O. Ardakanian, and I. Nikolaidis, "A co-simulation platform for evaluating cyber security and control applications in the smart grid," in *Proc. IEEE ICC'20*, pp. 1-7, Jul. 2020.

[37] National Renewable Energy Laboratory. 2006 Solar Power Data for Integration Studies, U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. [Online] Available: https://www.nrel.gov/grid/solar-power-data.html.

[38] Federal Highway Administration. 2017 National Household Travel Survey, U.S. Department of Transportation, Washington, DC. [Online] Available: https://nhts.ornl.gov.

[39] "Useable battery capacity of full electric vehicles," *Electric Vehicle Database*. [Online] Available: https://ev-database.org/cheatsheet/useable-battery-capacity-electric-car.

[40] "ElaadNL open EV charging transactions," Jan. 2020. [Online]. Available: https://platform.elaad.io/download-data/.

[41] M. Grant and S. Boyd., "CVX: Matlab software for disciplined convex programming, version 2.0 beta." [Online] Available: http://cvxr.com/cvx.

Yuan Liu (S'16-M'21) is a postdoctoral research fellow in the Department of Electrical and Computer Engineering at University of Alberta, Canada. He received his Ph.D. degree from the Department of Electrical and Computer Engineering at the University of Alberta, Canada, in 2020, and received the B.Sc degree in Control Science and Engineering from Zhejiang University, China, in 2014. His current research interests include smart grid, electric vehicle, cyber security, and quantum computing.

Omid Ardakanian.jpg (M'15) is an Assistant Professor in the Department of Computing Science at the University of Alberta, Canada. He received his B.Sc. from Sharif University of Technology in 2009, and M.Math. and Ph.D. from the University of Waterloo in 2011 and 2015, respectively. From 2015 to 2017, he was an NSERC Postdoctoral Fellow at the University of California, Berkeley and the University of British Columbia. His research focuses on the design and implementation of networked systems. He served as Guest Editor for a special issue of IEEE Transactions on Smart Grid (2018-2019), and is currently serving as Area Editor for ACM SIGENERGY Energy Informatics Review.

Ioanis Nikolaidis (M'93) received his BSc from the University of Patras, Greece, in 1989, and his MSc and PhD from Georgia Tech in 1991 and 1994 respectively. He worked as a Research Scientist for ECRC GmbH (1994-1996) and joined the Department of Computing Science at the University of Alberta in 1997, where he is (since 2008) a Full Professor. Dr. Nikolaidis is conducting research in the area of data networking protocols, protocol performance, and wireless sensor networks. He served as Area Editor for Computer Networks, Elsevier ('00-'10), and as Editor ('99-'13) and Editor-in-Chief ('07-'09) for the IEEE Network magazine.

Hao Liang (S'09-M'14) is an Associate Professor and Canada Research Chair in the Department of Electrical and Computer Engineering at the University of Alberta, Canada. He received his Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2013. From 2013 to 2014, he was a postdoctoral research fellow in the Broadband Communications Research (BBCR) Lab and Electricity Market Simulation and Optimization Lab (EMSOL) at the University of Waterloo. His current research interests are in the areas of smart grid, cyber-physical systems, wireless communications, and wireless networking. He is a co-recipient of the IEEE Power Energy Society (PES) Prize Paper Award 2018 and the Best Student Paper Award from the IEEE 72nd Vehicular Technology Conference (VTC Fall-2010), Ottawa, ON, Canada. He was the System Administrator of IEEE Transactions on Vehicular Technology (2009-2013).