IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 31, 2019, accepted March 9, 2019, date of publication March 14, 2019, date of current version April 1, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2904959

OLTC-Induced False Data Injection Attack on Volt/VAR Optimization in Distribution Systems

DARANITH CHOEUM, (Student Member, IEEE), AND DAE-HYUN CHOI, (Member, IEEE)
School of Electrical and Electronics Engineering, Chung-Ang University, Seoul 156-756, South Korea

Corresponding author: Dae-Hyun Choi (dhchoi@cau.ac.kr)

This work was supported in part by the Korea Electric Power Corporation under Grant R17XA05-75, and in part by the Korea Government (MSIP) through the National Research Foundation of Korea (NRF) under Grant 2018R1C1B6000965.

ABSTRACT This paper presents a new class of false data injection attacks (FDIAs) on volt/VAR optimization (VVO), which may result in abnormal voltage conditions along the radial medium voltage (MV) distribution feeder with an on-load tap changer (OLTC), capacitor banks (CBs), solar photovoltaic (PV) systems, and smart meters. In comparison with existing FDIAs against voltage control that do not consider the VVO process, we propose a new attack strategy with which the adversary can maliciously change the distribution feeder voltage profile by misleading the VVO function through stealthily injecting false data into smart meter measurements that are used for the VVO. The proposed attack strategy is formulated as a bilevel optimization problem using mixed integer linear programming (MILP). Injected false load data that raise or lower the tap position of the OLTC are calculated at the upper level while the VVO process is guaranteed to correctly operate with false data at the lower level. The bilevel optimization problem is finally reformulated to a single-level optimization problem based on Karush–Kuhn–Tucker conditions of the lower level optimization problem. A simulation study is carried out in an IEEE 33-bus distribution system with an OLTC, CBs, PV systems, and smart meters, and our results demonstrate the feasibility and capability of the proposed attack approach in terms of voltage level, attack effort, and PV penetration rate.

INDEX TERMS False data injection attack (FDIA), volt/VAR optimization (VVO), on-load tap changer (OLTC), smart meter, active distribution network.

NOMENCLATURE

A. VVO FORMULATION

N_t	Total number of prediction horizon steps.
N_d	Total number of nodes.
r_d	Resistance of the line from node d.
x_d	Reactance of the line from node d.
$P^{\text{line}}_{t,d}$	Real power flow from node d to $d+1$ at period t.
$Q^{\text{line}}_{t,d}$	Reactive power flow from node d to $d+1$ at period t.
$P^{\text{node}}_{t,d}$	Net real power consumption for node d at period t.
$Q^{\text{node}}_{t,d}$	Net reactive power consumption for node d at period t.
$P(Q)^{\text{lat}}_{t,d}$	Real(Reactive) power flow through the lateral branch from node d at period t.
$V_{t,d}$	Voltage magnitude for node d at period t.
$V^{\min(\max)}$	Minimum(Maximum) limit of the allowed voltage range for node d.
$\widehat{P}^{\text{PV}}_{t,d}$	Predicted PV real power output for node d at period t.
$Q^{\text{PV}}_{t,d}$	PV reactive power output for node d at period t.
$Q^{\text{CAP}}_{t,d}$	Reactive power output of CB for node d at period t.
$\widehat{P}^{\text{load}}_{t,d}$	Predicted real load consumption for node d at period t.
$\widehat{Q}^{\text{load}}_{t,d}$	Predicted reactive load consumption for node d at period t.
Tap^{OLTC}_{t}	Tap position of OLTC at period t.
a^{OLTC}	Step size of change in OLTC tap position.
$b^{\text{Cap}}_{t,d}$	Binary switch status of the capacitor for node d at period t; "1" for ON and "0" OFF.
$NTap^{\text{OLTC}}_{\max}$	Maximum switching operations of OLTC during the prediction horizon N_t.

The associate editor coordinating the review of this manuscript and approving it for publication was Zhitao Guan.

2169-3536 © 2019 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

B. ATTACK FORMULATION

$\widehat{P}^{\text{load},a}_{t,d}$	Manipulated real load consumption for node d at period t.
$\widehat{Q}^{\text{load},a}_{t,d}$	Manipulated reactive load consumption for node d at period t.
$\Delta P^{\text{load}}_{t,d}$	Injected false real load consumption data for node d at period t.
$\Delta Q^{\text{load}}_{t,d}$	Injected false reactive load consumption data for node d at period t.
$\delta^{D}_{t,d}$	Binary attack status for node d at period t; "1" with attack and "0" without attack.
τ	Limit factor for the magnitude of injected false real load consumption data.
ω	Weight for attack effort.
R	Maximum number of compromised smart meters.
M	Sufficient large positive constant.

I. INTRODUCTION

Volt/VAR optimization (VVO) is one of the key applications in distribution management systems (DMSs) for efficiently managing and controlling active distribution networks with distributed energy resources (DERs) (e.g., solar photovoltaic (PV) system and energy storage system (ESS)) [1]. In active distribution networks, VVO is carried out to determine optimal voltage levels along the distribution feeder under all loading conditions through the coordination of voltage regulators such as on-load tap changers (OLTCs) at substations and capacitor banks (CBs) and the smart inverters of DERs. Recently, advanced information and communication technology (ICT) such as advanced metering infrastructure (AMI) with smart meters provides voltage regulators with real-time loading and voltage measurements, consequently adjusting voltage profile more quickly and accurately [2].

However, as the coupling between the electric distribution system and ICT system becomes considerably stronger, the applications in DMS may become more vulnerable to potential cyber attacks through the ICT system. The 2015 Ukraine blackout [3] has been known as the first cyber attack against electric distribution systems wherein ICT networks and components were compromised, and it resulted in blackouts in three Ukrainian regions. This paper attempts to investigate the impact of cyber attacks on VVO in DMS.

The main objective of this paper is to propose a novel attack strategy with which the adversary malfunctions the operation of VVO by injecting false data into smart meter measurements that are used for VVO, consequently yielding the abnormal feeder voltage profile. Fig. 1 illustrates a two-layered framework that consists of cyber and physical layers, corresponding to an AMI/DMS and an electric distribution system, respectively. As shown in this figure, in the cyber layer the corrupted smart meter measurements due to false data injection from the adversary are, through the AMI network, fed into the VVO module in DMS, which in turn enables VVO to calculate the distorted optimal solutions of

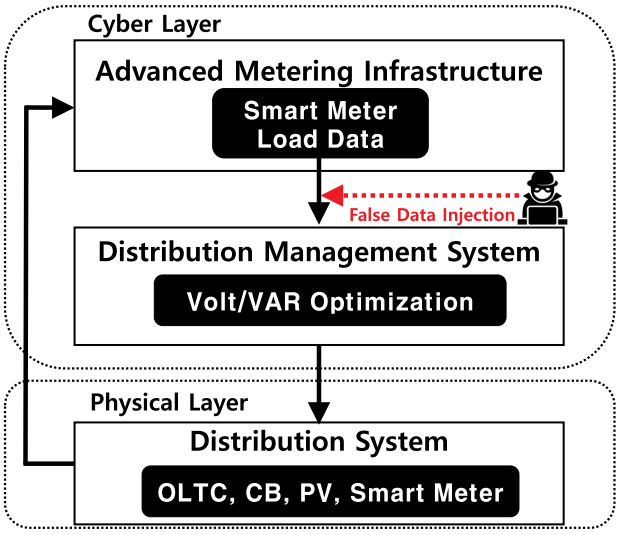

FIGURE 1. Cyber physical framework illustrating cyber attack on VVO.

voltage regulators and PV systems (e.g., incorrect tap positions of OLTC and wrong reactive power dispatch of PV systems). As a result, the distorted solutions lead to an abnormal feeder voltage profile and provide consumers with degraded voltage quality in the physical layer. This paper contributes to the following two aspects: (i) the proposal for a new class of false data injection attack (FDIA) strategies with which the adversary can distort the feeder voltage by misleading VVO to calculate the wrong OLTC tap positions through the injection of false data into smart meter measurements; and (ii) impact analysis of VVO subject to the proposed attacks.

In the power system engineering field, a first class of cyber data attack has been known as FDIA against DC model-based state estimation [4] where the adversary can maliciously change the estimate of the state of the transmission system while avoiding bad data detection in the energy management system (EMS). A more detailed review of the literature related to the subject of FDIA in electric power systems can be categorized into the following two parts:

- *Cyber attack on electric transmission system*: A large body of literature has been accumulated on the subject of FDIA in electric transmission system [5]–[14], ranging from attacks against AC state estimation [5], impact analysis of automatic generation control (AGC) attack [6], online static security and contingency analysis attack [7], [8], topology data attack through the manipulation of the status of circuit breaker and switch [9]–[12], load redistribution attack through the injection of malicious load data in a bilevel optimization problem [13] and a trilevel optimization problem [14] using mixed integer linear programming (MILP). While many studies have formulated new attack models and conducted their impact analysis in electric transmission systems from an adversary perspective, various defending strategies to mitigate the impact of cyber attack on electric power system operations, from a

system operator perspective, have been proposed. In [15], the least-budget dependent method against FDI attack was presented where securely protected sensors were determined by solving a mixed integer nonlinear programming (MINLP) problem based on Bender's decomposition. In [16], a bilevel MILP problem was formulated to determine the minimum number of measurements required to be protected. A new FDIA detection approach using load forecast data, generation schedules, and synchrophasor data was proposed in [17]. In [18], a framework for quantifying the impact of a cyber attack on bus and transmission line protection systems was developed where the expected load curtailment index was proposed to assess potential system loss from the attack. More recently, FDIA detection strategies based on various machine learning methods were presented where measurements can be categorized into non-attack events and attack events by using: temporal characteristics of FDIA using conditional deep belief network (CDBN) [19], semisupervised online learning method [20], and non-nested generalized exemplars (NNGE) through pre-processing of the state extraction method (STEM) [21]. A broader range of FDIA models and defending methods in the electric transmission system are summarized well in [22] and [23].

- *Cyber attack on electric distribution system*: In comparison with extensive research on the FDIA problem at the transmission system level, studies about the FDIA problem at the distribution system level are relatively few. In [24], a least-effort FDIA against three-phase balanced distribution system state estimator was proposed where the adversary can reduce his/her effort with only the information of local state obtained by approximating the entire system state using a small number of power flow or injection measurements. The possibility of a cyber threat on a distribution automation system (DAS) was first addressed in [25] and [26], where the attack impact assessment model [25] that consists of a terminal device level and control center server level was developed, and an efficient secret key distribution protocol without requiring much computation of encryption algorithm [26] was proposed. More recently, a unified attack model and security assessment framework for active distribution systems was developed based on limited stochastic Petri net (LSPN) graph theory, and the index that quantify the attack performance and the system robustness was proposed in [27]. A considerable amount of literature has been published recently on the attack model and impact analysis in voltage control [28]–[34], including the manipulation of the OLTC tap position [28], [29], attack on Volt-VAR control (VVC) under different capacitor bank configurations [30], the voltage change due to the malfunction of DERs through the injection of false generation setpoint signal [31] and reactive current measurement [32], an event tree-based impact assessment framework [33], and a denial-of-service attack mitigation framework [34].

Although extensive research has been carried out on the subject of the FDIA problem at both the transmission and distribution system levels, to the best of our knowledge, no research has been conducted to present FDIA against VVO and investigate the impact of such an attack on the voltage level along the distribution feeder. In prior work, Isozaki *et al.* [28], Anwar *et al.* [29], Teixeira *et al.* [30], Shelar and Amin [31], Teymouri *et al.* [32], Langer *et al.* [33], and Cameron *et al.* [34] considered an attack scenario where the adversary can attack against voltage control algorithms without the VVO process being considered. The main contributions of this paper are suggested as follows:

1) We propose two types of FDIAs on VVO. The adversary stealthily raises or lowers the tap position of OLTC by misleading the VVO process by injecting false data into smart meter measurements that are used for VVO, consequently leading to the abnormal voltages along the distribution feeder.
2) We formulate the proposed attack approach in a bilevel mixed integer linear programming (MILP) optimization problem that consists of upper and lower level optimization problems. The former calculates injected false data for the OLTC tap position to stealthily increase or decrease while the adversary spends the least attack effort. The latter enables VVO to operate correctly even with the injected false data. The bilevel optimization problem is then transformed to a single-level MILP optimization problem using Karush-Kuhn-Tucker (KKT) conditions of the lower level optimization problem.
3) We quantify the performance of the proposed attacks in the IEEE 33-bus distribution system in terms of: i) the OLTC tap position; ii) voltage magnitude along the feeder; and iii) attack effort as a function of the magnitude of injected false data and a maximum number of compromised smart meters. Furthermore, we study the impact of the proposed attacks with varying amount of PV penetration as well as with different number of prediction horizon in the VVO on the voltage profile.

The rest of this paper is organized as follows. Section II provides an overview of the VVO model and the KKT conditions of the optimization problem. Section III states the attack problem and elaborates the formulation of the proposed VVO attack strategies using a bilevel and single-level MILP optimization programming. The simulation results for the proposed attack approach are provided in Section IV, and the conclusions are given in Section V.

II. BACKGROUND

The main notations used throughout this paper are summarized in the nomenclature section. Bold symbols represent vectors. Hat symbols represent estimates of true parameter value. The other undefined symbols in the nomenclature section are explained in the text.

A. VOLT/VAR OPTIMIZATION MODEL

For each node d with a scheduling period t and prediction horizon N_t, the VVO problem is generally formulated as follows:

$$\min J = \sum_{t=1}^{N_t}\sum_{d=1}^{N_d} |V_{t,d} - V^{\text{nom}}| \tag{1}$$

$$s.t.\ \boldsymbol{\alpha} : P^{\text{line}}_{t,d+1} = P^{\text{line}}_{t,d} - P^{\text{node}}_{t,d+1} - P^{\text{lat}}_{t,d+1} \tag{2}$$

$$\boldsymbol{\chi} : Q^{\text{line}}_{t,d+1} = Q^{\text{line}}_{t,d} - Q^{\text{node}}_{t,d+1} - Q^{\text{lat}}_{t,d+1} \tag{3}$$

$$\boldsymbol{\lambda} : V_{t,d+1} = V_{t,d} - \left(\frac{r_d P^{\text{line}}_{t,d} + x_d Q^{\text{line}}_{t,d}}{V_0}\right) \tag{4}$$

$$\boldsymbol{\theta} : V_{t,1} = V^{\text{nom}} + a^{\text{OLTC}} Tap^{\text{OLTC}}_t \tag{5}$$

$$\boldsymbol{\gamma} : P^{\text{node}}_{t,d} = \widehat{P}^{\text{load}}_{t,d} - \widehat{P}^{\text{PV}}_{t,d} \tag{6}$$

$$\boldsymbol{\nabla} : Q^{\text{node}}_{t,d} = \widehat{Q}^{\text{load}}_{t,d} - Q^{\text{PV}}_{t,d} - Q^{\text{CAP}}_{t,d} \tag{7}$$

$$\boldsymbol{\beta} : Q^{\text{CAP}}_{t,d} = b^{\text{CAP}}_{t,d} Q^{\text{CAP,nom}}_{d} \tag{8}$$

$$b^{\text{CAP}}_{t,d} \in \{0, 1\} \tag{9}$$

$$\sum_{t=1}^{N_t} |Tap^{\text{OLTC}}_t - Tap^{\text{OLTC}}_{t-1}| \le NTap^{\text{OLTC}}_{\max} \tag{10}$$

$$Tap^{\text{OLTC}}_t \in \{-16, \ldots, -1, 0, 1, \ldots, 16\} \tag{11}$$

$$\boldsymbol{\kappa} : -c^{\text{PV}} \widehat{P}^{\text{PV}}_{t,d} \le Q^{\text{PV}}_{t,d} \le c^{\text{PV}} \widehat{P}^{\text{PV}}_{t,d} \tag{12}$$

$$\boldsymbol{\Phi} : V^{\min} \le V_{t,d} \le V^{\max}. \tag{13}$$

In this formulation, the objective function is to minimize the total deviation of voltages from the nominal voltage for all nodes during the prediction horizon in (1). Equations (2)–(4) represent the linearized distribution real power flow, reactive power flow, and voltage for node d at the scheduling period t, respectively [35]. Equation (5) represents the substation voltage, which can be determined by the OLTC tap position Tap^{OLTC}_t, along with the step size for changing tap positions a^{OLTC}. For each node d, the nodal real and reactive power balance equations can be expressed in terms of the real and/or reactive power of the load, CBs, and PVs in (6) and (7). Equation (8) represents the reactive output that is supported by the CB for node d at scheduling period t. Here, $Q^{\text{CAP,nom}}_d$ is the size of the capacitors and $b^{\text{CAP}}_{t,d}$ is a binary decision variable that determines the switch status of the capacitors in (9). During the prediction horizon N_t, the total number of switching operations for the OLTC is limited by its corresponding switching threshold $NTap^{\text{OLTC}}_{\max}$ in (10) along with the integer position of the OLTC tap in (11). Equation (12) represents the reactive power capability of the PV system at node d, which can be described in terms of the predicted PV real power output $\widehat{P}^{\text{PV}}_{t,d}$ and its coefficient c^{PV} defined as

$$c^{\text{PV}}_d = \sqrt{\frac{1 - (PF^{\text{PV,min}}_d)^2}{(PF^{\text{PV,min}}_d)^2}}$$

where $PF^{\text{PV,min}}_d$ is the minimum power factor of the PV system at node d. The range of allowable voltages for all nodes can be expressed in (13) where $V^{\min}$ and $V^{\max}$ are selected to be 0.95 p.u. and 1.05 p.u. The decision variable vectors from the VVO problem are denoted as $\mathbf{V}$, $\mathbf{P}^{\text{line}}$, $\mathbf{Q}^{\text{line}}$, $\mathbf{P}^{\text{node}}$, $\mathbf{Q}^{\text{node}}$, $\mathbf{Q}^{\text{CAP}}$, $\mathbf{Q}^{\text{PV}}$, $\mathbf{Tap}^{\text{OLTC}}$, and $\mathbf{b}^{\text{CAP}}$.

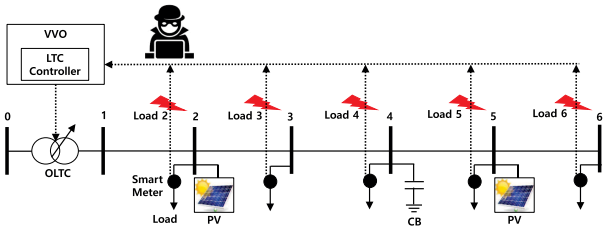

FIGURE 2. Illustration of VVO attack manipulating smart meter data.

In this paper, we convert the mixed-integer nonlinear programming (MINLP)-based VVO algorithm into a MILP optimization problem. To this end, the nonlinear equations for the objective function (1) and the constraints for the number of switching operations for the OLTC (10) are linearized as, respectively,

$$\Delta V_{t,d} = |V_{t,d} - V^{\text{nom}}| \tag{14}$$

$$\mathbf{J}^- : \Delta V_{t,d} \ge V_{t,d} - V^{\text{nom}} \tag{15}$$

$$\mathbf{J}^+ : \Delta V_{t,d} \ge V^{\text{nom}} - V_{t,d} \tag{16}$$

and

$$\mathbf{U}^- : NTap^{\text{OLTC}}_t \ge Tap^{\text{OLTC}}_t - Tap^{\text{OLTC}}_{t-1} \tag{17}$$

$$\mathbf{U}^+ : NTap^{\text{OLTC}}_t \ge Tap^{\text{OLTC}}_{t-1} - Tap^{\text{OLTC}}_t \tag{18}$$

$$\boldsymbol{\xi} : \sum_{t=1}^{N_t} NTap^{\text{OLTC}}_t \le NTap^{\text{OLTC}}_{\max}. \tag{19}$$

Furthermore, the binary and integer decision variables in (9) and (11) are relaxed with continuous variables as the following linear constraints:

$$\boldsymbol{\zeta} : 0 \le b^{\text{CAP}}_{t,d} \le 1 \tag{20}$$

$$\boldsymbol{\rho} : -16 \le Tap^{OLTC}_t \le 16. \tag{21}$$

In this paper, the linear programming (LP)-based VVO problem through the relaxation above needs to be formulated in order to develop our attack strategy illustrated in the following section. It is noted that the proposed attack strategy includes the KKT conditions of the VVO problem, however, no KKT conditions of the MILP optimization problem exist.

In the LP-based VVO formulation, all variable vectors ($\boldsymbol{\alpha}$, $\boldsymbol{\chi}$, $\boldsymbol{\lambda}$, $\boldsymbol{\theta}$, $\boldsymbol{\gamma}$, $\boldsymbol{\nabla}$, $\boldsymbol{\beta}$, $\boldsymbol{\kappa}$, $\boldsymbol{\Phi}$, $\mathbf{J}$, $\mathbf{U}$, $\boldsymbol{\zeta}$, and $\boldsymbol{\rho}$) corresponding to the equality/inequality constraints are the Lagrangian multipliers that have non-negative values. In particular, the Lagrangian multiplier vector associated with its inequality constraint consists of two types of Lagrangian multiplier subvectors, corresponding to the upper and lower limit of inequality constraints, respectively (e.g., $\boldsymbol{\kappa} = [\boldsymbol{\kappa}^+, \boldsymbol{\kappa}^-]$ in (12)).

B. KKT CONDITIONS

A general optimization problem with linear equality and inequality constraints is formulated as follows:

$$\min_{\mathbf{x}} \; J(\mathbf{x}, \mathbf{a}) \tag{22}$$

$$s.t. \; \boldsymbol{\lambda} : \mathbf{F}\mathbf{x} = \mathbf{a}, \tag{23}$$

$$\boldsymbol{\kappa} : \mathbf{G}\mathbf{x} \leq \mathbf{a}, \tag{24}$$

Here, $\mathbf{x}$ and $\mathbf{a}$ are the vectors for decision variables and parameters, respectively. $\mathbf{F}$ and $\mathbf{G}$ are linear matrices associated with the equality and inequality constraints, respectively.

Given the Lagrangian function ($\mathcal{L}(\mathbf{x}, \mathbf{a}) = J(\mathbf{x}, \mathbf{a}) - \boldsymbol{\lambda}(\mathbf{F}\mathbf{x} - \mathbf{a}) + \boldsymbol{\kappa}(\mathbf{G}\mathbf{x} - \mathbf{a})$), the KKT conditions are written as

1) $\nabla_{\mathbf{x}}\mathcal{L}(\mathbf{x}, \mathbf{a}) = \mathbf{0}$
   $\Rightarrow \nabla_{\mathbf{x}} J(\mathbf{x}, \mathbf{a}) - \boldsymbol{\lambda}\nabla_{\mathbf{x}}(\mathbf{F}\mathbf{x} - \mathbf{a}) + \boldsymbol{\kappa}\nabla_{\mathbf{x}}(\mathbf{G}\mathbf{x} - \mathbf{a}) = \mathbf{0}$,
2) $\mathbf{F}\mathbf{x} = \mathbf{a}$,
3) $\mathbf{G}\mathbf{x} \leq \mathbf{a}$.
4) $\boldsymbol{\kappa}(\mathbf{G}\mathbf{x} - \mathbf{a}) = \mathbf{0}, \boldsymbol{\kappa} \geq \mathbf{0}$,

where the first conditions are the first-order optimal conditions, the second and third conditions are the primal feasibility conditions, and the fourth conditions are the dual feasibility or the complimentary slackness conditions.

In this paper, we apply the KKT conditions to a bilevel optimization attack problem where the LP VVO problem at a lower level is replaced by its KKT conditions.

III. FORMULATION OF VOLT-VAR OPTIMIZATION ATTACK

A. STATEMENT OF THE PROPOSED ATTACK PROBLEM

In this paper, we consider a closed-loop VVO architecture where load measurements from smart meters are periodically fed into the VVO module through AMI networks as shown in Fig. 2. We assume that the VVO algorithm is executed in a medium voltage (MV) distribution system that is equipped with voltage regulators (e.g., OLTC and CBs), PV systems, and smart meters. In this environment, as shown in Fig. 2, the primary goal of the adversary is to stealthily move the tap position of the OLTC by injecting false data into smart meter measurements, consequently leading to changes in voltage along the MV distribution feeder. The proposed attacks are classified into the following two types:

- Attack I: The tap position of the OLTC is switched upward as much as possible in order to increase the voltage profile.
- Attack II: The tap position of the OLTC is switched downward as much as possible in order to decrease the voltage profile.

A higher voltage level caused by attack I can increase consumer energy consumption and decrease the distribution system efficiency owing to increasing power loss. On the other hand, a lower voltage level caused by attack II can have a detrimental impact on voltage stability and lead to voltage collapse with the violation of the minimum voltage limit.

Prior to the proposed attack, the adversary is required to have the following capabilities:

(R1) The adversary can compromise smart meters by observing and manipulating their measurements.
(R2) The adversary has the capability to execute the VVO having the knowledge of distribution system topology including the line parameters and the location of voltage regulating devices, PV systems and smart meters.
(R3) The adversary has the knowledge of operating parameters for voltage regulators (e.g., the range of the OLTC tap position and the size of CB) and the prediction value of the PV generation output with the power factor of the PV systems.

B. BILEVEL OPTIMIZATION PROBLEM FOR THE PROPOSED ATTACKS

Based on the aforementioned attack assumptions, the two proposed attack strategies are formulated as a bilevel MILP optimization problem as follows:

$$\text{Attack I: } \max \left\{ Tap_t^{\text{OLTC}} - \omega \sum_{d=1}^{N_d} \delta_{t,d}^{D} \right\} \tag{25}$$

or

$$\text{Attack II: } \min \left\{ Tap_t^{\text{OLTC}} + \omega \sum_{d=1}^{N_d} \delta_{t,d}^{D} \right\} \tag{26}$$

$$s.t. \sum_{d=1}^{N_d} \Delta P_{t,d}^{\text{load}} = 0 \tag{27}$$

$$\sum_{d=1}^{N_d} \Delta Q_{t,d}^{\text{load}} = 0 \tag{28}$$

$$\Delta P_{t,d}^{\text{load}} \neq 0 \Leftrightarrow \delta_{t,d}^{D} = 1 \tag{29}$$

$$-\tau \widehat{P}_{t,d}^{\text{load}} \leq \Delta P_{t,d}^{\text{load}} \leq \tau \widehat{P}_{t,d}^{\text{load}} \tag{30}$$

$$\sum_{d=1}^{N_d} \delta_{t,d}^{D} \leq R \tag{31}$$

$$-c_d^{\text{load}} \Delta P_{t,d}^{\text{load}} \leq \Delta Q_{t,d}^{\text{load}} \leq c_d^{\text{load}} \Delta P_{t,d}^{\text{load}} \tag{32}$$

$$\min \sum_{t=1}^{N_t} \sum_{d=1}^{N_d} \Delta V_{t,d} \tag{33}$$

$$s.t. \; \boldsymbol{\gamma} : P_{t,d}^{\text{node}} = \widehat{P}_{t,d}^{\text{load},a} - \widehat{P}_{t,d}^{\text{PV}} \tag{34}$$

$$\boldsymbol{\eta} : \widehat{P}_{t,d}^{\text{load},a} = \widehat{P}_{t,d}^{\text{load}} + \Delta P_{t,d}^{\text{load}} \tag{35}$$

$$\boldsymbol{\nabla} : Q_{t,d}^{\text{node}} = \widehat{Q}_{t,d}^{\text{load},a} - Q_{t,d}^{\text{PV}} - Q_{t,d}^{\text{CAP}} \tag{36}$$

$$\boldsymbol{\mu} : \widehat{Q}_{t,d}^{\text{load},a} = \widehat{Q}_{t,d}^{\text{load}} + \Delta Q_{t,d}^{\text{load}} \tag{37}$$

$$\text{Eqn. (2)} - \text{(5)}, \text{Eqn. (8)} \tag{38}$$

$$\text{Eqn. (12)} - \text{(21)} \tag{39}$$

In the upper level (25)–(32), the adversary computes false load data ($\Delta P_{t,d}^{\text{load}}$, $\Delta Q_{t,d}^{\text{load}}$) that are injected into smart meters in order to maximize (attack I) or minimize (attack II) the OLTC tap positions and minimize the attack effort simultaneously while maintaining the undetectable condition along

with the limited attack capability. The multi objective function (25) or (26) for attack I or attack II consists of two terms, corresponding to the OLTC tap position and a total number of injected false load data where $\delta^D_{t,d}$ equals to one when smart meter at node d is attacked, otherwise $\delta^D_{t,d}$ equals to zero. In the second term for the objective function, ω represents a penalty weight for the attack effort. A larger ω yields a smaller number of $\delta^D_{t,d} = 1$ along with a reduced false data magnitude, and hence, it saves the attack effort; yet, it prevents the adversary from manipulating the OLTC tap position significantly. Equations (27) and (28) guarantee that the injected false data are undetected by system operators. The number of injected false data are counted in (29), which is equivalent to the following constraints:

$$\Delta P^{\text{load}}_{t,d} + \tau\ P^{\text{load}}_{t,d}\delta^D_{t,d} \geq 0 \tag{40}$$

$$\Delta P^{\text{load}}_{t,d} - \tau\ P^{\text{load}}_{t,d}\delta^D_{t,d} \leq 0 \tag{41}$$

$$\delta^D_{t,d} \in \{0, 1\}. \tag{42}$$

Equations (30) and (31) represent the limit for the magnitude and the number of injected false data, respectively. In (32), the injected false reactive power data are bounded by the limit in terms of the injected false real power data and the following coefficient c^{load}_d in terms of the power factor (PF^{load}_d) at node d

$$c^{\text{load}}_d = \sqrt{\frac{1-(PF^{\text{load}}_d)^2}{(PF^{\text{load}}_d)^2}}.$$

On the other hand, the lower level (33)–(39) represents the VVO problem that is illustrated in subsection II-A. Only the difference from the previous VVO formulation is that the VVO problem at the lower level includes the modified nodal real and reactive power balance equations (34)–(37), which are expressed as a function of the injected false data delivered from the upper level.

C. SINGLE-LEVEL OPTIMIZATION PROBLEM FOR THE PROPOSED ATTACKS

In this paper, the bilevel MILP optimization-based attack strategy is converted into an equivalent single-level optimization problem. To this end, the lower level optimization problem is replaced by its KKT equations, which are classified into four types of conditions as follows:

■ The first-order optimality conditions

Given the Lagrangian function of the VVO problem at the lower level, which is illustrated in subsection II-B, the first-order optimality conditions can be derived as

$$1 - J^-_{t,d} - J^+_{t,d} = 0 \tag{43}$$

$$-\lambda_{t,d-1} + \lambda_{t,d} - \Phi^-_{t,d} + \Phi^+_{t,d} + J^-_{t,d} - J^+_{t,d} - \theta_t = 0 \tag{44}$$

$$-\frac{\lambda_{t,d} r_d}{V^{\text{nom}}} - \alpha_{t,d-1} + \alpha_{t,d} = 0 \tag{45}$$

$$-\frac{\lambda_{t,d} x_d}{V^{\text{nom}}} - \chi_{t,d-1} + \chi_{t,d} = 0 \tag{46}$$

$$-\nabla_{t,d} - \beta_{t,d} = 0 \tag{47}$$

$$-\nabla_{t,d} - \kappa^-_{t,d} + \kappa^+_{t,d} = 0 \tag{48}$$

$$\beta_{t,d} Q^{\text{CAP,nom}}_d - \zeta^-_{t,d} + \zeta^+_{t,d} = 0 \tag{49}$$

$$\gamma_{t,d} - \eta_{t,d} = 0 \tag{50}$$

$$\nabla_{t,d} - \mu_{t,d} = 0 \tag{51}$$

$$-\alpha_{t,d-1} - \gamma_{t,d} = 0 \tag{52}$$

$$-\chi_{t,d-1} - \nabla_{t,d} = 0 \tag{53}$$

$$a^{\text{OLTC}}\theta_t - \rho^-_t + \rho^+_t + U^-_t - U^-_{t+1} - U^+_t + U^+_{t+1} = 0 \tag{54}$$

$$-\xi_t - U^-_t - U^+_t = 0. \tag{55}$$

■ The primal feasibility conditions

The primal feasibility conditions are all equality and inequality constraints for the lower level optimization problem:

$$\text{Eqn. (34)} - \text{(39)} \tag{56}$$

■ The complimentary conditions

The complimentary conditions are expressed as the multiplication of all inequality constraints and their Lagrangian multipliers.

$$J^-_{t,d}\left(-V_{t,d} + V^{\text{nom}} - \Delta V_{t,d}\right) + J^+_{t,d}\left(V_{t,d} - V^{\text{nom}} - \Delta V_{t,d}\right) = 0 \tag{57}$$

$$\kappa^-_{t,d}\left(-Q^{\text{PV}}_{t,d} - c^{\text{PV}}\widehat{P}^{\text{PV}}_{t,d}\right) + \kappa^+_{t,d}\left(Q^{\text{PV}}_{t,d} - c^{\text{PV}}\widehat{P}^{\text{PV}}_{t,d}\right) = 0 \tag{58}$$

$$U^-_t\left(-NTap^{\text{OLTC}}_t - Tap^{\text{OLTC}}_{t-1} + Tap^{\text{OLTC}}_t\right) + U^+_t\left(-NTap^{\text{OLTC}}_t + Tap^{\text{OLTC}}_{t-1} - Tap^{\text{OLTC}}_t\right) = 0 \tag{59}$$

$$\xi_t\left(\sum_{t=1}^{N_t} NTap^{\text{OLTC}}_t - NTap^{\text{OLTC}}_{\max}\right) = 0 \tag{60}$$

$$\Phi^-_{t,d}\left(-V_{t,d} + V_{\min}\right) + \Phi^+_{t,d}\left(V_{t,d} - V_{\max}\right) = 0 \tag{61}$$

$$\zeta^-_{t,d}\left(-b^{\text{CAP}}_{t,d}\right) + \zeta^+_{t,d}\left(b^{\text{CAP}}_{t,d} - 1\right) = 0 \tag{62}$$

$$\rho^-_{t,d}\left(-Tap^{\text{OLTC}}_t - 16\right) + \rho^+_{t,d}\left(Tap^{\text{OLTC}}_t - 16\right) = 0. \tag{63}$$

It is noted that the complimentary conditions above are nonlinear owing to the multiplication of two continuous decision variables. Thus, to formulate the attack method in an MILP optimization problem, the nonlinear complimentary conditions can be relaxed as the linear constraints with additional binary decision variables ($\delta^{J^-}_{t,d}$, $\delta^{J^+}_{t,d}$, $\delta^{\kappa^-}_{t,d}$, $\delta^{\kappa^+}_{t,d}$, $\delta^{U^-}_t$, $\delta^{U^+}_t$, $\delta^{\xi^+}_t$, $\delta^{\Phi^-}_{t,d}$, $\delta^{\Phi^+}_{t,d}$, $\delta^{\zeta^-}_{t,d}$, $\delta^{\zeta^+}_{t,d}$, $\delta^{\rho^-}_t$, and $\delta^{\rho^+}_t$) as follows:

$$\begin{cases} J^-_{t,d} - M\delta^{J^-}_{t,d} \leq 0 \\ -V_{t,d} + V^{\text{nom}} + \Delta V_{t,d} \leq M(1 - \delta^{J^-}_{t,d}) \\ J^+_{t,d} - M\delta^{J^+}_{t,d} \leq 0 \\ V_{t,d} - V^{\text{nom}} + \Delta V_{t,d} \leq M(1 - \delta^{J^+}_{t,d}) \end{cases} \tag{64}$$

$$\begin{cases} \kappa^-_{t,d} - M\delta^{\kappa^-}_{t,d} \leq 0 \\ Q^{\text{PV}}_{t,d} + c^{\text{PV}}\widehat{P}^{\text{PV}}_{t,d} \leq M(1 - \delta^{\kappa^-}_{t,d}) \\ \kappa^+_{t,d} - M\delta^{\kappa^+}_{t,d} \leq 0 \\ -Q^{\text{PV}}_{t,d} + c^{\text{PV}}\widehat{P}^{\text{PV}}_{t,d} \leq M(1 - \delta^{\kappa^+}_{t,d}) \\ \delta^{\kappa^-}_{t,d} + \delta^{\kappa^+}_{t,d} \leq 1 \end{cases} \tag{65}$$

$$\begin{cases} U_t^- - M\delta_t^{U^-} \le 0 \\ NTap_t^{\mathrm{OLTC}} + Tap_{t-1}^{\mathrm{OLTC}} - Tap_t^{\mathrm{OLTC}} \le M(1-\delta_t^{U^-}) \\ U_t^+ - M\delta_t^{U^+} \le 0 \\ NTap_t^{\mathrm{OLTC}} - Tap_{t-1}^{\mathrm{OLTC}} + Tap_t^{\mathrm{OLTC}} \le M(1-\delta_t^{U^+}) \end{cases} \tag{66}$$

$$\begin{cases} \xi_t^+ - M\delta_t^{\xi^+} \le 0 \\ -\sum_{t=1}^{N_t} NTap_t^{\mathrm{OLTC}} + NTap_{\max}^{\mathrm{OLTC}} \le M(1-\delta_t^{\xi^+}) \end{cases} \tag{67}$$

$$\begin{cases} \Phi_{t,d}^- \le M\delta_{t,d}^{\Phi^-} \\ V_{t,d} - V_{\min} \le M(1-\delta_{t,d}^{\Phi^-}) \\ \Phi_{t,d}^+ \le M\delta_{t,d}^{\Phi^+_{t,d}} \\ -V_{t,d} + V_{\max} \le M(1-\delta_{t,d}^{\Phi^+}) \\ \delta_{t,d}^{\Phi^-} + \delta^{\Phi^+} \le 1 \end{cases} \tag{68}$$

$$\begin{cases} \zeta_{t,d}^- \le M\delta_{t,d}^{\zeta^-} \\ b_{t,d}^{\mathrm{CAP}} \le M(1-\delta_{t,d}^{\zeta^-}) \\ \zeta_{t,d}^+ \le M\delta_{t,d}^{\zeta^+} \\ -b_{t,d}^{\mathrm{CAP}} + 1 \le M(1-\delta_{t,d}^{\zeta^+}) \\ \delta_{t,d}^{\zeta^-} + \delta_{t,d}^{\zeta^+} \le 1 \end{cases} \tag{69}$$

$$\begin{cases} \rho_t^- \le M\delta_t^{\rho^-} \\ Tap_t^{\mathrm{OLTC}} + 16 \le M(1-\delta_t^{\rho^-}) \\ \rho_t^+ \le M\delta_t^{\rho^+} \\ -Tap_t^{\mathrm{OLTC}} + 16 \le M(1-\delta_t^{\rho^+}) \\ \delta_t^{\rho^-} + \delta_t^{\rho^+} \le 1. \end{cases} \tag{70}$$

■ The dual feasibility conditions

All the non-negative Lagrangian multipliers belong to the dual feasibility conditions as follows:

$$[\boldsymbol{\alpha}; \boldsymbol{\chi}; \boldsymbol{\lambda}; \boldsymbol{\theta}; \boldsymbol{\gamma}; \boldsymbol{\nabla}; \boldsymbol{\eta}; \boldsymbol{\mu}; \boldsymbol{\beta}; \boldsymbol{\kappa}; \boldsymbol{\Phi}; \mathbf{J}, \mathbf{U}, \boldsymbol{\xi}, \boldsymbol{\zeta}, \boldsymbol{\rho}] \ge 0. \tag{71}$$

Finally, using the aforementioned KKT conditions, the proposed attack strategy can be formulated as the following single-level optimization problem:

$$\text{Attack I: } \max \left\{ Tap_t^{\mathrm{OLTC}} - \omega \sum_{d=1}^{N_d} \delta_{t,d}^D \right\} \tag{72}$$

or

$$\text{Attack II: } \min \left\{ Tap_t^{\mathrm{OLTC}} + \omega \sum_{d=1}^{N_d} \delta_{t,d}^D \right\} \tag{73}$$

$$s.t. \text{ Eqn. } (27) - (32) \tag{74}$$

$$\text{Eqn. } (43) - (56),\ (64) - (71)$$

$$\text{(KKT conditions).} \tag{75}$$

IV. SIMULATION RESULTS

A. SIMULATION SETUP

In this section, we assess the performance of the proposed attack approach in the modified IEEE 33-bus distribution test system [35], which is illustrated in Fig. 3. In this test system, the base MVA is set to 100 MVA. The modified IEEE 33-bus system includes one OLTC, nine CBs, four PV systems and

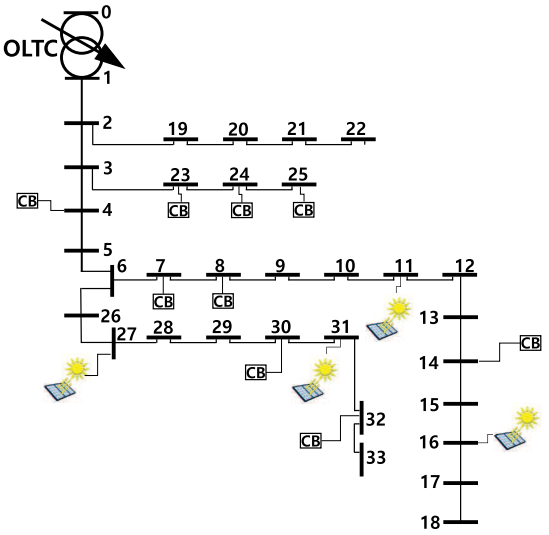

FIGURE 3. Modified IEEE 33-bus system with OLTC, CBs, and PV systems.

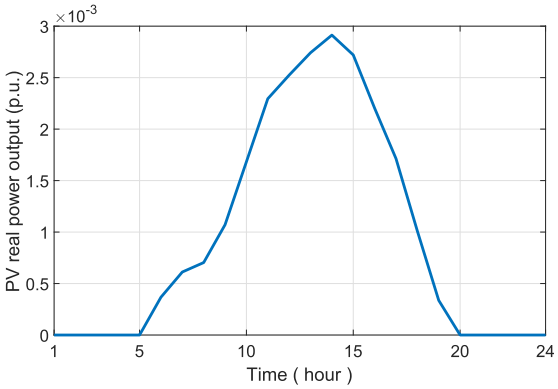

FIGURE 4. Profile of the predicted value with a resolution of 1 h for PV real power output.

32 smart meters. The smart meters are located from node 2 to node 33. An integer tap position of OLTC at the substation ranges from -16 to 16 with its step change $a^{\mathrm{OLTC}} = 0.003$. The maximum number of tap changes for OLTC during the predicted horizon is set to $NTap_{\max}^{\mathrm{OLTC}} = 3$. The CBs are connected to nodes 4, 7, 8, 14, 23, 24, 25, 30, and 32, and the maximum output of each CB is $Q_d^{\mathrm{CAP,nom}} = 30\mathrm{kVAr}$. The PV systems are installed at nodes 11, 16, 17, and 31. The profiles for the predicted PV real power output and load coefficient are shown in Fig. 4 and Fig. 5, respectively. For simplicity, the predicted PV real power output and load coefficient are assumed to be identical for all nodes. The scheduling period is 1 h for VVO with a predicted horizon $N_t = 1$. The comparison of the attack performance for VVO with different predicted horizons between $N_t = 1$ and $N_t = 4$ is conducted in the following subsection. Initially, the parameters for the attack optimization problem are given as follows: the limit for injected real load attack measurement $\tau = 0.5$, maximum number of compromised smart meters $R = 25$, and large positive constant for the relaxation $M = 10^5$. The proposed attack model is implemented in computer

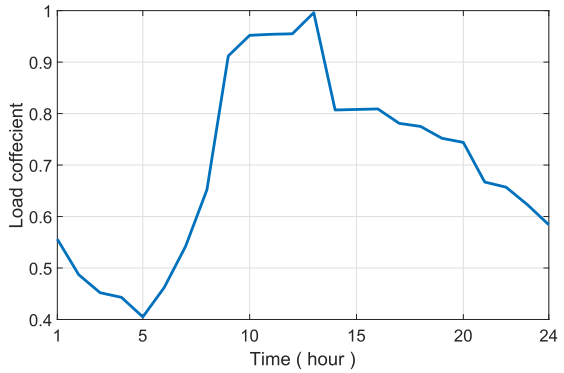

FIGURE 5. Profile of the predicted value with a resolution of 1 h for load coefficient.

(IntelCore i7-4790 CPU clocking at 3.6 GHz and 4 GB of RAM) using the optimization toolbox in MATLAB R2018a.

B. IMPACT OF THE PROPOSED ATTACKS ON VOLTAGE PROFILE

In this subsection, we conduct an impact analysis of voltage conditions along the distribution feeder subject to the proposed attacks I and II. We consider two types of voltages belonging to different layers as shown in Fig. 1: 1) voltage in cyber layer; and 2) voltage in physical layer. The former represents the optimal voltage schedule that is calculated by the VVO. The latter represents the voltage value that involves the actual operating condition of the distribution system. Voltage in the physical layer is computed by distribution system power flow analysis [36]. In this paper, voltages in the cyber layer and in the physical layer are denoted by the cyber voltage and the physical voltage, respectively.

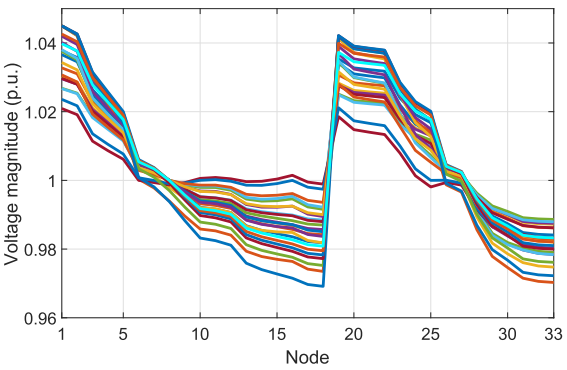

FIGURE 6. Voltage profile for 33 nodes during 24 h without attack.

Figs. 6, 7 and 8 show cyber voltage profiles for all nodes during 24 h without attack, with attack I, and with attack II, respectively. Fig. 6 provides a performance benchmark for the proposed attack strategies where the voltages are maintained within their acceptable limits [0.95 p.u., 1.05 p.u.]. Compared to Fig. 6, we observe from Figs. 7 and 8 that attacks I and II tend to increase or decrease feeder voltages, respectively, while the voltages are still maintained at their

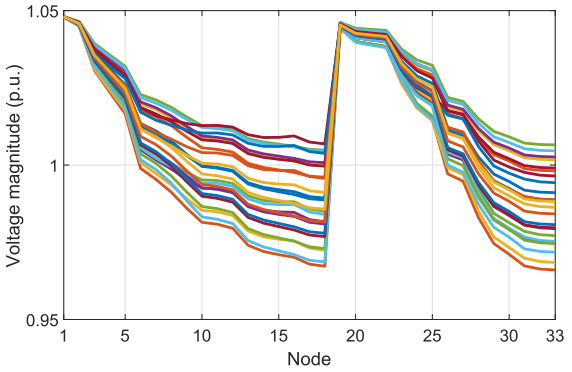

FIGURE 7. Voltage profile for 33 nodes during 24 h with attack I.

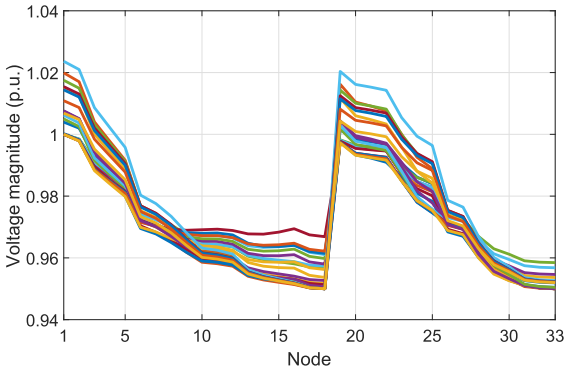

FIGURE 8. Voltage profile for 33 nodes during 24 h with attack II.

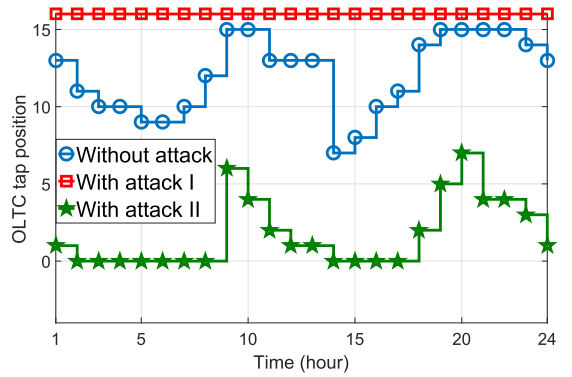

FIGURE 9. Comparison of three different tap positions of OLTC during 24 h among without attack and with attacks I and II.

acceptable levels. This observation is due to the fact that the OLTC tap position becomes higher or lower by the adversary that successfully constructs and injects the false load attack vector into the VVO module, respectively, consequently distorting the normal voltage profile. Fig. 9 compares the OLTC tap positions between without attack and with attacks I and II. In the case of no attack, we observe from Fig. 9 that the OLTC tap position ranges from 7 to 15 where a lower tap position is associated with a higher amount of PV generation (2 p.m.∼4 p.m.) and a higher tap position with a lower amount of PV generation (7 p.m.∼11 p.m.). As expected, compared to the tap positions of OLTC without

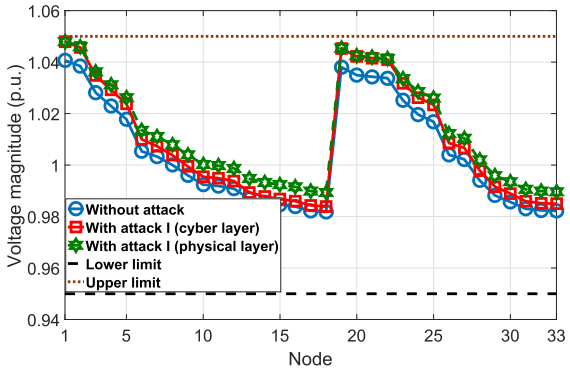

FIGURE 10. Comparison of three different voltage profiles at 8 a.m.: (i) without attack, (ii) with attack I (cyber layer), and (iii) with attack I (physical layer).

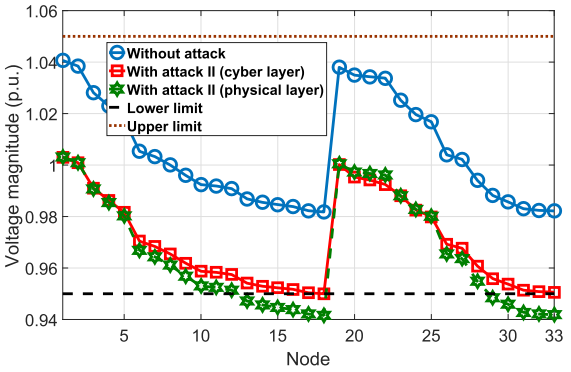

FIGURE 12. Comparison of three different voltage profiles at 8 a.m.: (i) without attack, (ii) with attack II (cyber layer), and (iii) with attack II (physical layer).

attack, they increase or decrease owing to attacks I and II, respectively, as shown in Fig. 9. However, it is observed from this figure that the OLTC tap position has the maximum value at any scheduling time during attack I. This observation may be regarded as an abnormal operation of the OTLC by system operators. In this case, the adversary needs to wait another day when the schedule that has different OLTC tap positions at some nodes can be obtained from attack I.

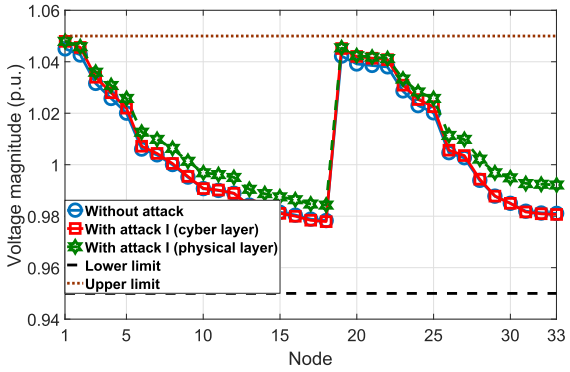

FIGURE 11. Comparison of three different voltage profiles at 10 p.m.: (i) without attack, (ii) with attack I (cyber layer), and (iii) with attack I (physical layer)

Next, we evaluate the impact of the proposed attacks on the physical voltage at two randomly selected scheduling time slots. Figs. 10 and 11 show two cyber voltages without attack and with attack I along with one physical voltages with attack I at 8 a.m. and 10 p.m., respectively. We can observe from these figures that both cyber and physical voltages remain within the allowable range and are listed in the decreasing order of their magnitudes, as follows: the physical voltage with attack > the cyber voltage with attack > the cyber voltage without attack. We verify from this result that the adversary with attack I successfully increases the physical voltage through the manipulation of the OLTC tap position without being detected by system operators in the cyber layer.

We also observe from Figs. 10 and 11 that attack I has no detrimental impact on voltage quality because no physical voltage violation occurs after the attack. However, it is noted that a higher voltage operating condition requires more power supply from the substation, and hence, it has a detrimental impact on system efficiency.

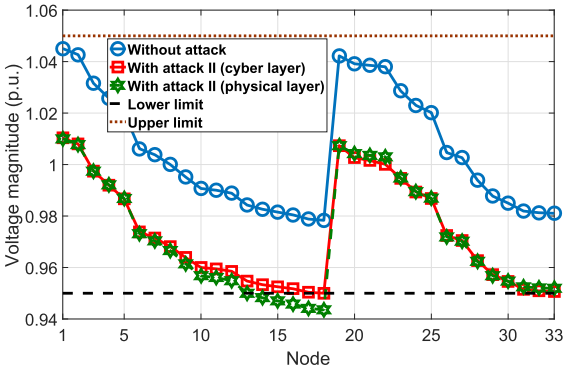

FIGURE 13. Comparison of three different voltage profiles at 10 p.m.: (i) without attack, (ii) with attack II (cyber layer), and (iii) with attack II (physical layer).

Figs. 12 and 13 illustrate the impact of attack II on both cyber and physical voltages at 8 a.m. and 10 p.m.. Compared to the result from Figs. 10 and 11 without voltage violation, we verify from Figs. 12 and 13 that the adversary with attack II causes physical voltage violations below the minimum voltage limit at some nodes while the cyber voltage with attack at any node still remains within the allowable range. We observe from Figs. 12 and 13 that the physical voltage violations occur at two groups of nodes at 8 a.m., {nodes 13∼18} and {nodes 29∼33}, whereas the physical voltage violations does at 10 p.m. at only {nodes 13∼18}. This observation derives from the fact that due to no available PV reactive power injection at 10 p.m., the PV systems do not contribute to increased voltages above the minimum limit, which in turn results in raising the OLTC tap position.

C. IMPACT OF PV ON THE VVO ATTACK

In this subsection, we quantify the impact of three different amounts of PV real power output on the performance of

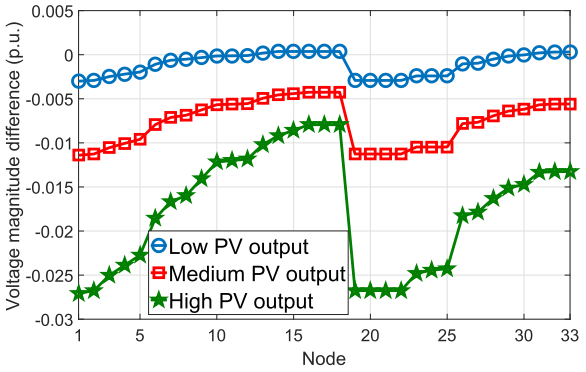

FIGURE 14. Impact of three different PV penetration rates on voltage magnitude differences between without attack and with attack I.

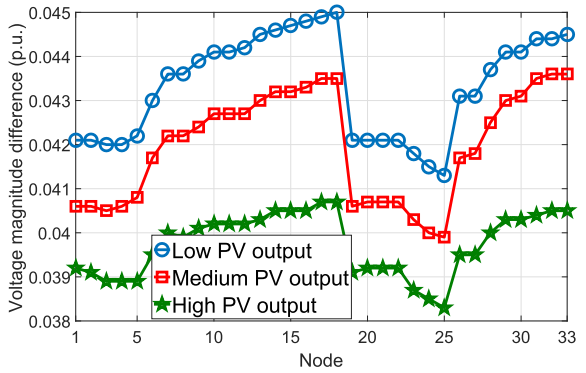

FIGURE 15. Impact of three different PV penetration rates on voltage magnitude differences between without attack and with attack II.

the proposed attacks, corresponding to different scheduling time slots: (1) low PV generation at 6 p.m.; (2) medium PV generation at 11 a.m.; and (3) high PV generation at 2 p.m. Figs. 14 and 15 show the comparison of voltage magnitude differences among different PV penetration rates when attacks I and II occur, respectively. Here, the voltage magnitude difference is defined as the deviation of physical voltage with attack from cyber voltage without attack. We observe from Fig. 14 that the adversary using attack I can cause more negative voltage deviation from the normal voltage level with a higher PV penetration rate. This phenomenon is due to the fact that the voltage level at the substation is lower at a high PV penetration than at low PV generation, and hence, the adversary can obtain more room to maximize the OLTC tap position for increasing the voltage level at any node. Compared to Fig. 14, Fig. 15 demonstrates that the adversary using attack II can have a more significant impact on positive voltage deviation at low PV penetration than at a high PV penetration rate. It is noted that low PV penetration causes a higher OLTC tap position than high PV penetration. As a result, low PV penetration provides more room for the adversary using attack II to minimize the OLTC tap position and decrease voltages eventually.

D. IMPACT OF THE ATTACK EFFORT ON THE VVO ATTACK

In this subsection, we investigate the impact of the attack effort on the performance of the proposed attacks.

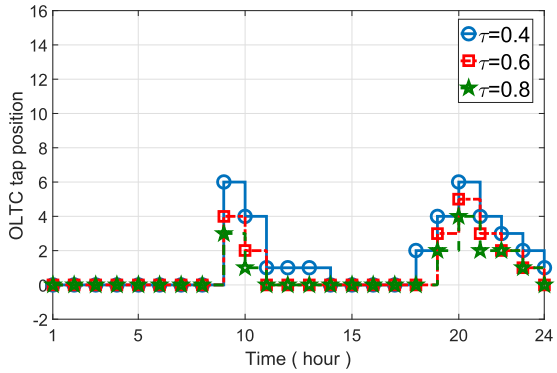

FIGURE 16. Tap positions of OLTC with three different attack limit factors τ.

Here, the attack effort is defined as two attack limit factors, τ and R, for: (1) the magnitude of injected false load data τ; and (2) the maximum number of injected false load data R, respectively. For the simulation study, three different values of the attack effort are selected with $\tau = 0.4$, 0.6 and 0.8 and $R = 5$, 15 and 25. In this simulation, the impact assessment of attack II subject to varying attack effort is conducted. Fig. 16 shows the OLTC tap positions during 24 h after the attack with varying τ. Along with the result from Fig. 16, it is observed that the increase of value of τ results in a lower OLTC tap position at some scheduling time slots, which consequently lead to an increase in the physical voltage magnitude difference at any node as shown in Fig. 17.

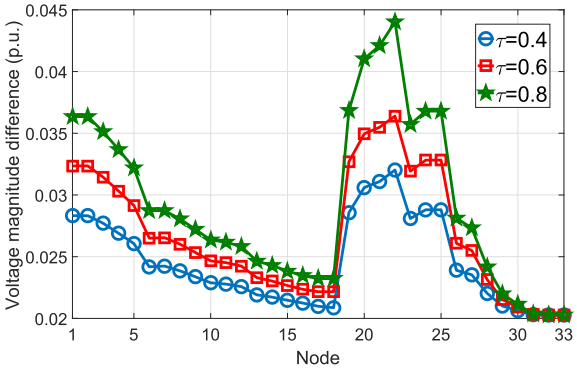

FIGURE 17. Voltage profiles with three different attack limit factors τ.

Fig. 18 shows the OLTC tap positions during 24 h after the attack with varying R. Similar to the result from Fig. 16, it is observed from Fig. 18 that the OLTC tap positions at some scheduling time slots become lower with increasing R. As shown in Fig. 19, it is also observed that the voltage magnitude differences fluctuate further with a larger value of R.

In addition, with different values of R, the location of nodes with the attacked smart meters (i.e., load measurements) are summarized as follows: {node 11, node 23, nodes 28∼30} for $R = 5$, {node 4, node 6, node 14, node 16, node 18, node 21, node 23, nodes 25∼32} for $R = 15$, and {nodes 4∼9, nodes 14∼32 for $R = 25$. It is noted from this result that,

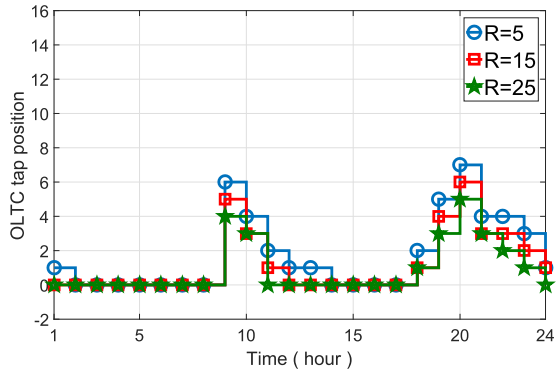

FIGURE 18. Tap positions of OLTC with three different attack efforts R.

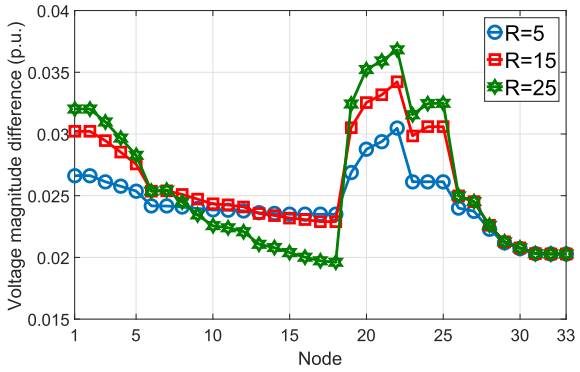

FIGURE 19. Voltage profiles with three different attack efforts R.

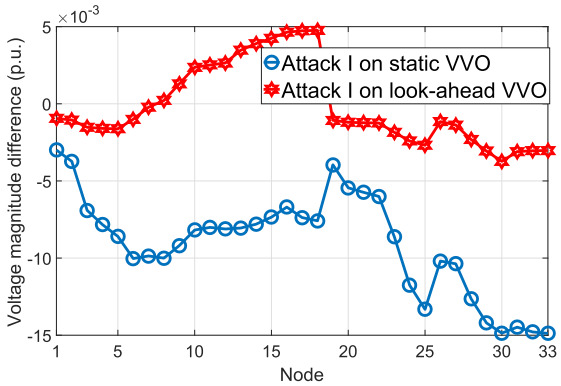

FIGURE 20. Comparison of attack I performance between static VVO and look-ahead VVO at 10 a.m.

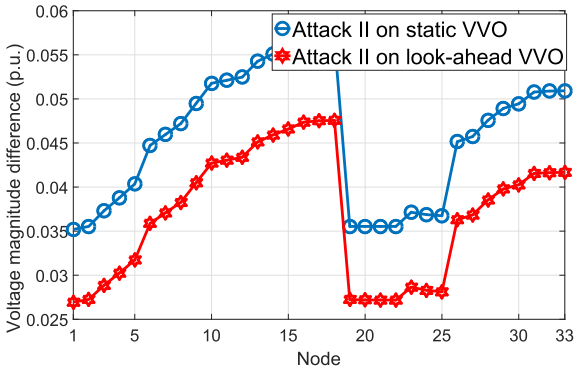

FIGURE 21. Comparison of attack II performance between static VVO and look-ahead VVO at 10 a.m.

to achieve the desired attack result, in general the adversary injects false data into smart meters that are further away from the substation. For a secure VVO operation against false data injection attacks, this may provide some practical guideline wherein smart meters installed around the end node of the distribution system need to be protected with a higher priority.

E. IMPACT OF THE NUMBER OF PREDICTION HORIZON ON THE VVO ATTACK

This subsection evaluates the impact of the proposed attacks on VVO with different number of prediction horizon N_t. In this paper, we define VVO with a one-step prediction interval (i.e., $N_t = 1$) as static VVO, otherwise as look-ahead VVO with multi-step prediction intervals. In comparison with the static VVO approach, the benefit of the look-ahead VVO approach lies in that during the multi-step prediction horizon, look-ahead VVO allows OLTC, CB, and PV systems with inter-temporal constraint to reserve their capacities and operate efficiently, thus operating the VVO process more effectively along with the reduction of the total cost (i.e., the deviation of optimal voltage from nominal voltage) of VVO. To fairly compare the attack performance between static VVO and look-ahead VVO, we assume that identical smart meters for both VVO methods are attacked.

Figs. 20 and 21 show voltage magnitude differences of static VVO ($N_t = 1$) and look-ahead VVO ($N_t = 4$) at 10 a.m. due to attack I and attack II, respectively. We observe from these figures that the voltage magnitude difference in static VVO is larger than in the look-ahead VVO. We can conjecture from this observation that in view of robustness to cyber attack, look-ahead VVO still outperforms static VVO.

Finally, the main observations from the simulation studies can be summarized as follows:

- The proposed attacks I and II are undetectable because the cyber voltages remain within the allowable range after the attack.
- Attack I increases cyber voltage and physical voltage where the latter is larger than the former. However, no voltage violation at any node in physical layer occurs.
- Attack II decreases cyber voltage and physical voltage where the latter is less than the former. Voltage violations in physical layer are identified at some nodes.
- Attack I has a more detrimental impact on physical voltage profile with a higher PV penetration whereas attack II does with a lower PV penetration.
- The increase of attack effort in terms of the magnitude and the number of injected false load data leads to more voltage deviation from the normal voltage level.
- Static VVO with one-step prediction interval is more susceptible to attacks I and II than look-ahead VVO with multi-step prediction intervals.

V. CONCLUSIONS

In this paper, we presented a novel false data injection attack that causes changes in voltage profile along a distribution feeder by misleading VVO through false load data injection into smart meters and manipulating tap positions of an on-load tap changer. We first formulated two attack strategies that increase or decrease the tap position of an on-load tap changer in a bilevel optimization problem where the upper level and lower level correspond to the construction of attack vector and the VVO operation with attack vector, respectively. Then, we reformulated the bilevel optimization-based attack method into a single-level optimization problem using Karush-Kuhn-Tucker conditions of the lower level optimization problem. Numerical examples simulated in the IEEE 33-bus distribution system demonstrated that the proposed attack approach can stealthily result in an abnormal feeder voltage profile in both the physical and the cyber layers.

In the future, we will extend the proposed attack model to a more practical attack in a realistic unbalanced three-phase distribution system with a voltage-dependent load model. Another interesting direction for future research is to develop an effective mitigation strategy to protect distribution systems from false data injection attacks against VVO.

REFERENCES

[1] L. Wang, F. Bai, R. Yan, and T. K. Saha, "Real-time coordinated voltage control of PV inverters and energy storage for weak networks with high PV penetration," *IEEE Trans. Smart Grid*, vol. 33, no. 3, pp. 3383–3395, May 2018.

[2] T. V. Dao, S. Chaitusaney, and H. T. N. Nguyen, "Linear least-squares method for conservation voltage reduction in distribution systems with photovoltaic inverters," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1252–1263, May 2017.

[3] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, Nov. 2009, pp. 21–32.

[5] W.-L. Chin, C.-H. Lee, and T. Jiang, "Blind false data attacks against ac state estimation based on geometric approach in smart grid communications," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6298–6306, Nov. 2018.

[6] R. Tan *et al.*, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

[7] J. Chen *et al.*, "Impact analysis of false data injection attacks on power system static security assessment," *J. Modern Power Syst. Clean Energy*, vol. 4, no. 3, pp. 496–505, 2016.

[8] J.-W. Kang, I.-Y. Joo, and D.-H. Choi, "False data injection attacks on contingency analysis: Attack strategies and impact assessment," *IEEE Access.*, vol. 6, pp. 8841–8851, 2018.

[9] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[10] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3820–3829, Jul. 2018.

[11] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.

[12] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2016–2025, Jul. 2016.

[13] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[14] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 720–729, Mar. 2017.

[15] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[16] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.

[17] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018.

[18] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580, Mar. 2017.

[19] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[20] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[21] U. Adhikari, T. H. Morris, and S. Pan, "Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 3928–3941, Sep. 2018.

[22] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[23] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[24] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, to be published.

[25] X. Ye, J. Zhao, Y. Zhang, and F. Wen, "Quantitative vulnerability assessment of cyber security for distribution automation systems," *Energies*, vol. 8, pp. 5266–5286, Jun. 2015.

[26] I. H. Lim *et al.*, "Security protocols against cyber attacks in the distribution automation system," *IEEE Trans. Power Del.*, vol. 25, no. 1, pp. 448–455, Jan. 2010.

[27] R. Fu, X. Huang, Y. Xue, Y. Wu, Y. Tang, and D. Yue, "Security assessment for cyber physical distribution power system under intrusion attacks," *IEEE Access*, to be published.

[28] 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.

[29] A. Anwar, A. N. Mahmood, and M. Ahmed, "False data injection attack targeting the LTC transformers to disrupt smart grid operation," in *Proc. Int. Conf. Secur. Privacy Commun. Netw.*, Beijing, China, Sep. 2014, pp. 252–266.

[30] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/var control and countermeasures," in *Proc. Amer. Control Conf. (ACC)*, Portland, OR, USA, Jun. 2014, pp. 4372–4378.

[31] D. Shelar and S. Amin, "Security assessment of electricity distribution networks under DER node compromises," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 23–36, Mar. 2017.

[32] A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, "Cyber security risk assessment of solar PV units with reactive power capability," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Washington, DC, USA, Oct. 2018, pp. 2872–2877.

[33] L. Langer, P. Smith, M. Hutle, and A. Schaeffer-Filho, "Analysing cyber-physical attacks to a smart grid: A voltage control use case," in *Proc. Power Syst. Comput. Conf. (PSCC)*, Genova, Italy, Jun. 2016, pp. 1–7.

[34] C. Cameron, C. Patsios, P. Taylor, and Z. Pourmirza, "Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes," *IEEE Trans. Smart Grid*, to be published.

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

[36] W. H. Kersting, *Distribution System Modeling and Analysis*. New York, NY, USA: CRC Press, 2017.

DARANITH CHOEUM (S'19) received the B.E. degree in electrical and electronics engineering from the Institute of Technology of Cambodia, Phnom Penh, Cambodia, in 2017. He is currently pursuing the master's degree with the School of Electrical and Electronics Engineering, Chung-Ang University, Seoul, South Korea. His research interests include cyber security and data attack on smart grids.

DAE-HYUN CHOI (S'10–M'19) received the B.S. degree in electrical engineering from Korea University, Seoul, South Korea, in 2002, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from Texas A&M University, College Station, TX, USA, in 2008 and 2014, respectively. From 2002 to 2006, he was a Researcher with Korea Telecom (KT), Seoul, South Korea, where he was involved in designing and implementing home network systems. From 2014 to 2015, he was a Senior Researcher with LG Electronics, Seoul, South Korea, where he developed home energy management systems. He is currently an Assistant Professor with the School of Electrical and Electronics Engineering, Chung-Ang University, Seoul, South Korea. He has received the Best Paper Award from the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm) in Tainan, Taiwan. His research interests include power system state estimation, electricity markets, the cyber-physical security of smart grids, and the theory and applications of cyber-physical energy systems.