공학석사 학위논문

FALSE DATA INJECTION ATTACK BY VIRTUAL POWER PLANTS FOR CURTAILMENT MINIMIZATION

출력제어 최소화를 위한 가상 발전소 사업자의 허위정보주입공격

2023년 2월

서울대학교 대학원
전기정보공학부
정 윤 식

FALSE DATA INJECTION ATTACK BY VIRTUAL POWER PLANTS FOR CURTAILMENT MINIMIZATION

지도 교수 윤 용 태

이 논문을 공학석사 학위논문으로 제출함
2022년 12월

서울대학교 대학원
전기정보공학부
정 윤 식

정윤식의 공학석사 학위논문을 인준함
2022년 12월

위 원 장 _____ (인)
부위원장 _____ (인)
위　　원 _____ (인)

Abstract

Studies on false data injection attacks (FDIA) against state estimation were mainly conducted on the transmission system. However, recently, as entities such as distributed energy resources (DERs), virtual power plants (VPPs), energy storage systems (ESSs), and EV charging stations, that are vulnerable to cyber-attacks, began to appear in the distribution system, research on FDIA in the distribution system is being actively conducted. Among them, this paper deals with the FDIA that VPPs attempt in the distribution system. As the number of DERs in the distribution system increases, the curtailment for DERs owned by VPP increases. This paper proposes FDIA model by VPPs to avoid curtailment under the realistic conditions. In the model, VPPs can implement an FDIA that deceives the distribution system operator (DSO)' s state estimation with only information obtained from the DERs they own. To verify this, IEEE 33 test feeder was used and the result shows that the attack was successful without being caught in the DSO's bad data detection (BDD). This paper provides the basic concept of VPP' s FDIA and shows that future DSOs need algorithms to defend against VPPs FDIA.

주요어: DSO, VPP, false data injection attack, state estimation, bad data detection, curtailment

학 번: 2021-28681

Contents

List of Tables

List of Figures

1 Introduction

1.1 Research background and motivation

Penetration of Distributed Energy Resources (DERs) have been increasing in the power system as cost of the generation by the Renewables has fallen due to recent technological advances. Solar installation costs by year are shown in Figure 1.1 [1].

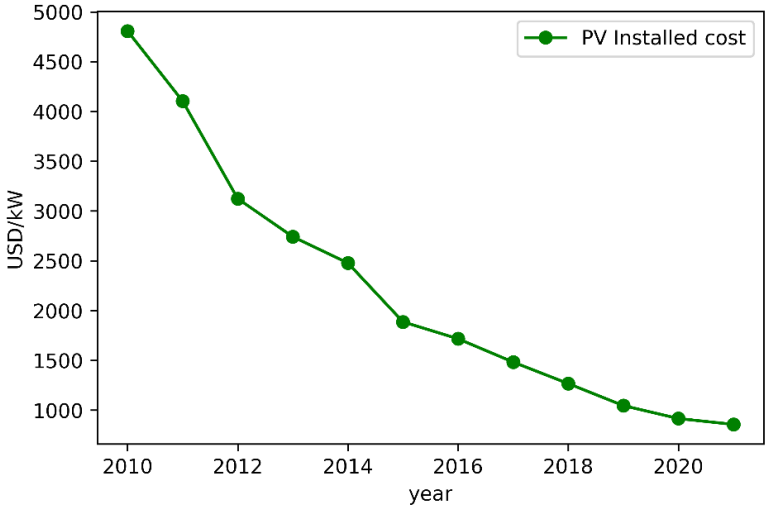

Figure 1.1 Global PV install cost, 2010-2020 [1]

These changes are fundamentally changing the structure of the power

system as shown in Figure 1.2. In the past, the power system was a centralized structure. Electric power produced by large-scale generators connected to the transmission system was delivered to consumers in one direction through the transmission and distribution network. On the other hand, the future power system including the present connects various types of distributed energy resources such as wind power, solar power, energy storage systems, and electric vehicles. As a result, a two-way power flow is occurring, and large variability is occurring due to the uncertain and intermittent characteristics of distributed energy resources [2].

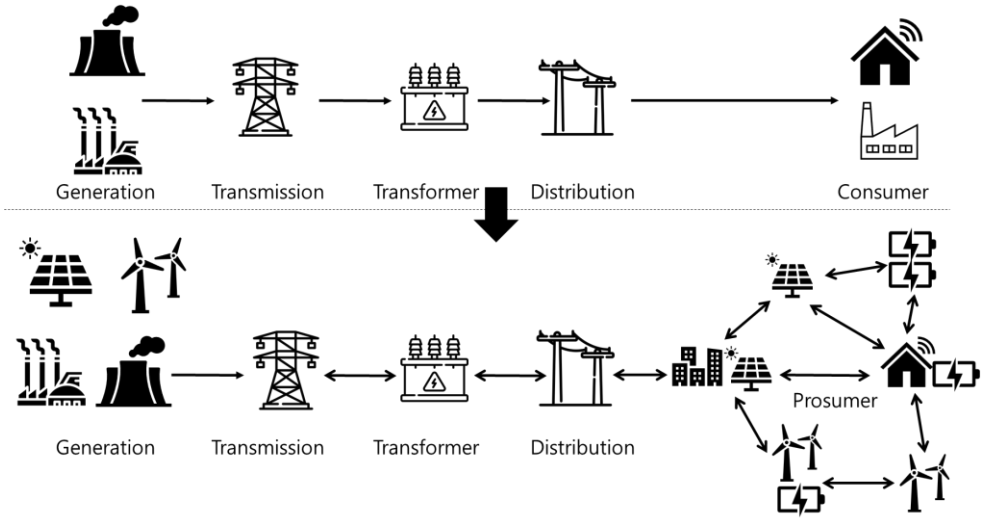

Figure 1.2 Comparison of the Conventional power system(up), Future power system(down) [2]

As a result, as participations from the DERs increased in the system, there have been technical issues related to the variability caused thereby such as overvoltage and congestions not only in transmission system but also

in distribution system. In an effort to mitigate such problem, locally centralized active operation by the distribution system operator (DSO) has been gaining greater attentions. The existing DSO’s role was limited to grid maintenance, repair and planning, power outage management, billing, and the role of connecting distributed energy sources to the grid. However, the role of the active DSO is extended to peak load management using distributed energy sources and distribution system line congestion management, reactive power supply, voltage maintenance, and technical validation for power market.

In the process of active operation of DSO, distribution system state estimation (DSSE) is essential because improper or inaccurate state estimation can excessively distort the profit of market players such as individual DERs or aggregators in the distribution system. Conversely, it is theoretically possible for profit-seeking entities with computation power such as virtual power plants (VPPs) to attempt to manipulate the curtailment of their DERs through a false data injection attack (FDIA) that passes through the DSO's bad data detection (BDD) embedded in the typical DSSE.

If VPP attempts and succeeds in FDIA to avoid curtailment, the future distribution system will become unstable and in the worst case may lead to system collapse. Therefore, it is necessary to simulate the FDIA that can occur in the distribution system in advance and study what results can be shown.

1.2 Research objective and contents

our research assumes a VPP that constructs an attack vector passing DSO’s bad data detection (BDD). In the previous literature, it was impractical to assume that the attacker installs additional metering devices to construct an attack vector. Thus, in this paper, we showed that the method VPP's local false data injection attack passing DSO's BDD can be implemented with only measurements from DERs that VPPs own. The proposed methodology is simulated based on the IEEE test feeder. The adverse effect on the distribution system and the additional profit obtained by the VPP is verified.

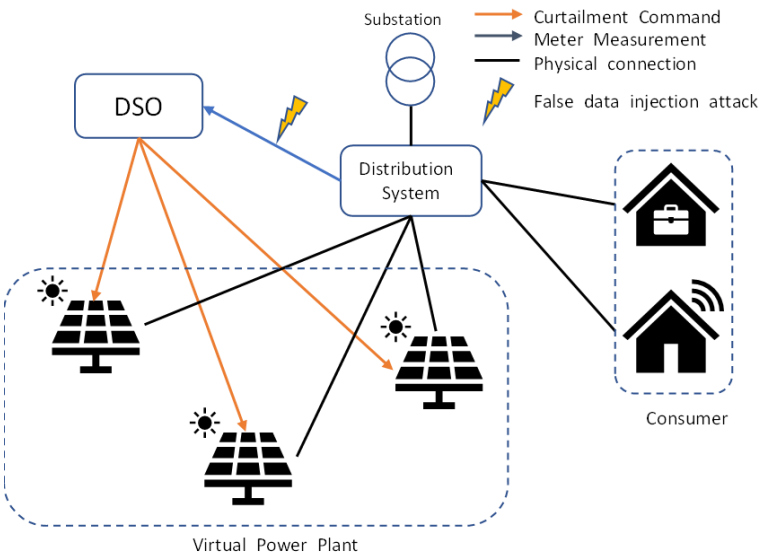

Figure 1.3 False data injection attack by virtual power plant

1.3 Research procedure

The remainder of this paper is organized as follows. In Chapter 2, research that have been conducted on false data injection attacks are review according to research purposes, results, and limitations, and in contributions, the differences between this study and previous studies are summarized. In chapter 3, theoretical background of this paper which describes the basic concept of state estimation, distribution system state estimation, bad data detection, false data injection attack is introduced. In chapter 4, based on the knowledge described in chapter 3, it is shown that how VPP can carry out an FDIA in future distribution system circumstances. In chapter 5, the VPP’s FDIA shown in chapter 4 is demonstrated in the IEEE 33 distribution system environment. In chapter 6, the further remarks and the conclusion of this paper are presented.

2 Literature review and contribution

2.1 Attempting false data injection attack in various condition

The concept of false data injection attack that can avoid bad data detection based on state estimation of the power system was first presented in [3]. In [3], Liu et al introduced the concept of a false data injection attack that can inject arbitrary errors into state variables without being caught by state estimation-based bad data detection. In addition, the probability of attack success according to the number of meters that can be compromised was presented. However, this paper has a limitation in that an attacker needs to know the parameters of all systems in order to create an attack vector, and it is based on DC state estimation that cannot be applied in the distribution system. In [4], Rahman and Mojsenian-Rad presented a method for creating a successful false data injection attack vector in a situation where DSO performs nonlinear AC state estimation, which is a more realistic condition. In [5], Deng et al showed that a false data injection attack can succeed even in the

distribution system under realistic conditions. To construct an attack vector that passes through the DSO's AC-based bad data detection (BDD), the attacker must know the state variables of all nodes due to the non-linearity of the power flow equation. However, Deng et al showed that, in relaxed condition, the local false data injection attack is possible only by using the local state variables. In [6], Wen and Liu demonstrated that data-driven FDIA is possible without knowing system measurement matrix. By proposing truncated singular value decomposition (SVD), they showed that attack vector can be constructed with computationally efficient way. In [7], Chen et al. proposed reinforcement learning-based FDIA to affect normal operation of automatic voltage controls (AVC). They showed that such attack is possible with only little knowledge of the whole power grid.

2.2 Impact of false data injection attack

In [8], Xie et al. suggested how the FDIA could affect the electricity market. It was shown that the attacker can manipulate the nodal price through FDIA, and that it can provide sufficient financial profit to the attacker through nodal price manipulation by virtual bidding. In [9], Yuan et al. showed that a load redistribution attack, a type of FDIA, is possible under realistic assumptions. In addition, the Yuan et al showed quantitatively how much the operation cost increases through the load redistribution attack.

2.3 Cyber-attack related to distributed energy resources

In [10], Isozaki et al. studied the impact of cyber-attack when photovoltaic (PV) is heavily connected to the distribution system. The authors showed that if an attacker manipulates the voltage measurement, it can affect the operation of the load ratio control transformers (LRTs) of the DSO and easily put the system into an undervoltage or overvoltage situation. In addition, using this, it was shown that if the PV has an overvoltage protection function, it can easily suffer from output power loss due to voltage attack. However, the attack proposed in this paper has a limitation in that it can be easily discovered when the DSO performs state estimation. In [11], Riggs et al. presented an algorithm to detect FDIA using artificial neural network (ANN). By comparing PV production data and global horizontal irradiance using ANN, it was shown that detection can be succeeded with 95% accuracy. In [12], Zhang et al. analysed the effect of FDIA on distributed load sharing of microgrids.

2.4 Contribution of this study

This study shows that FDIA is more likely to succeed when VPP owns many PVs in the distribution system. As the number of PVs owned by VPP increases, VPP can occupy an exclusive position in the distribution system due to the superiority of information in the distribution system. As far as the author is aware, this paper is the first paper to present a false data injection attack that VPP might perform in the distribution system. Therefore, by simulating an FDIA in which a VPP with a monopoly position can implement in the distribution system for its own benefit, it shows that the existing FDIA theory can occur in the future distribution system under realistic conditions. Also, it raises the awareness that future DSOs need an algorithm that can prevent such FDIA.

3 Theoretical background

In this section, the basic background knowledge required to understand VPP’s false data injection attack are presented.

3.1 State estimation

State estimation is used to estimate non-measurable state variables from measurable values and to reduce errors caused by measurement errors [13]. It is very important to continuously monitor current and voltage of the system to maintain system stability. However, transducers in power system measurements are very susceptible to errors [13]. If the measurement values with these errors are small, it will not have a great impact on power system operation, but if the number of errors increases, cumulated incorrect values are eventually sent to the system operator, leading power system operation in the wrong direction. In this case, the entire system may be at risk. For these reasons, state estimation has been mainly used to secure the stability and observability of the transmission system based on sufficient measurement sensors for decades.

DC-based State estimation is a process of estimating a state variable $\boldsymbol{x}$

from measurement $\boldsymbol{z}$ in which measurement error $\boldsymbol{e}$ exists. Their mathematical relationship can be expressed as follow:

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} \tag{3-1}$$

where $\boldsymbol{z} = (z_1, z_2, z_3, \dots, z_m)^T$ is the measurement vector, $\boldsymbol{x} = (x_1, x_2, x_3, \dots, x_m)^T$ is the state variable vector, $\boldsymbol{e} = (e_1, e_2, e_3, \dots, e_m)^T$ is the measurement error vector that follows distributions with zero means [14]. H is a constant $m \times n$ Jacobian matrix related to the type of measurement data, system topology, parameters.

In this paper, the most widely used state estimation method, weighted least squares (WLS), is used. The WLS based state estimation method is expressed as an optimization problem as follow:

$$\min_x J(x) = (\boldsymbol{z} - \boldsymbol{H}\boldsymbol{x})^T \boldsymbol{W} (\boldsymbol{z} - \boldsymbol{H}\boldsymbol{x}) \tag{3-2}$$

where W is the diagonal matrix representing measurement noise variance of the ith measurement sensor.

Equation (3-2) can be solved as below:

$$\nabla J(x) = -2[\boldsymbol{H}]^T \boldsymbol{W}\boldsymbol{z} + 2[\boldsymbol{H}]^T \boldsymbol{W}\boldsymbol{H}\boldsymbol{x} = \boldsymbol{0} \tag{3-2}$$

$$\hat{\boldsymbol{x}} = [[\boldsymbol{H}]^T \boldsymbol{W}\boldsymbol{H}]^{-1} \boldsymbol{H}^T \boldsymbol{W}\boldsymbol{z} \tag{3-3}$$

3.2 Distribution System State Estimation (DSSE)

As mentioned in 3.1, state estimation has been mainly used by transmission system operators (TSOs) to stably operate the transmission system. However, recently, as DERs which cannot exactly predict the amount of power generation are increasing in the distribution system, the need for distribution system state estimation (DSSE) is emerging for safe and reliable operation in the distribution system. However, from the technical perspectives, DSSE is difficult to be introduced due to the following reasons. First, since the distribution system covers broader areas than the transmission system, the measurement sensors cannot be sufficiently installed. Second, compared to the transmission system, the distribution system has a very low accuracy when performing DC state estimation because of high resistance/impedance ratio [13]. Therefore, it is possible to consider that the state estimation calculation is more complicated than the transmission system where DC-based state estimation can be used. Thus, in distribution system, AC-based state estimation should be applied. Due to the technical barriers mentioned, only very few utility companies tried to implement DSSE [15]–[17]. However, recently, with the spread of advanced metering infrastructure (AMI) and smart inverter attached to DERs, measurable data from the system that can be obtained from the distribution system are increasing

[18].

AC-based State estimation is a process of estimating a state variable x from measurement $\boldsymbol{z}$ in which measurement error $\boldsymbol{e}$ exists. Their mathematical relationship can be expressed as follow:

$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e} \tag{3-5}$$

where $\boldsymbol{z} = (z_1, z_2, z_3, \dots, z_m)^T$ is the measurement vector, $\boldsymbol{x} = (x_1, x_2, x_3, \dots, x_m)^T$ is the state variable vector, $\boldsymbol{e} = (e_1, e_2, e_3, \dots, e_m)^T$ is the measurement error vector that follows distributions with zero means [14]. h(x) is a nonlinear vector function relating measurements to states that depends on the type of measurement data, system topology, parameters. Active power, reactive power, active power flow, reactive power flow and voltage related $\boldsymbol{h}(\boldsymbol{x})$ are as follows:

$$h_i^p(x) = Real\left(V_i \sum_{j=1}^{n} Y_{ij} V_j\right) \tag{3-6}$$

$$h_i^q(x) = Imag\left(V_i \sum_{j=1}^{n} Y_{ij} V_j\right) \tag{3-7}$$

$$h_{ij}^p(x) = Real\left(V_i Y_{ij} V_j\right) \tag{3-8}$$

$$h_{ij}^q(x) = Imag\left(V_i Y_{ij} V_j\right) \tag{3-9}$$

$$h_i^v(x) = V_i \tag{3-10}$$

The WLS based state estimation method is expressed as an optimization problem as follow:

$$\min_{x} J(x) = \sum_{i=1}^{m} \frac{[z_i - h_i(x)]^2}{\sigma_i^2} \tag{3-11}$$

where σ_i is the measurement noise variance of the ith measurement sensor and m is the number of measurement data.

Equation (3-11) is computationally more complicated than DC-based state estimation because it has a nonlinear feature and must be solved in an iterative way.

3.3 Bad data detection (BDD)

Bad data detection (BDD) refers to the process of comparing estimated state variables and measured data and discriminating as 'bad data' if the difference is greater than a certain value [14]. The major reason for its consideration as the bad data, is due to the measurement errors, false data, compromised data, etc. Without BDD, the bad data affects the state estimation results, causing false system monitoring. Typically, the Largest normalized residual (LNR) method is used as the BDD algorithm. By using the estimated state variable $\hat{\boldsymbol{x}}$, normalized residual r_i can be calculated as follow:

$$r_i = \frac{[z_i - h_i(\hat{\boldsymbol{x}})]}{\sigma_i} \tag{3-4}$$

Then, the data whose residual exceeds a certain threshold are considered to be the bad data and deleted.

3.4 False data injection attack (FDIA)

A false data injection attack refers to compromising the state variable without getting caught in BDD by manipulating measurement data [3]. To achieve this goal, the attacker must carefully design the attack vector $\boldsymbol{a}$, which is added to measurements $\boldsymbol{z}$. Manipulated measurement data z_{bad} and compromised state variable $\hat{\boldsymbol{x}}_{\boldsymbol{bad}}$ can be expressed as follows:

$$\boldsymbol{z}_{\boldsymbol{bad}} = \boldsymbol{z} + \boldsymbol{a} \tag{3-5}$$

$$\hat{\boldsymbol{x}}_{\boldsymbol{bad}} = \hat{\boldsymbol{x}} + \boldsymbol{c} \tag{3-6}$$

where $\boldsymbol{c}$ represents the estimation error caused by the attacker. Substituting equation (3-13), (3-14) into BDD equation (3-12), the residual from $\boldsymbol{z}_{\boldsymbol{bad}}$, can be mathematically derived as equation (3-15) below.

$$\begin{aligned} \boldsymbol{r}_{\boldsymbol{bad}} &= \left[\frac{\boldsymbol{z}_{\boldsymbol{bad}} - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\boldsymbol{bad}})}{\boldsymbol{\sigma}}\right] \\ &= \left[\frac{\boldsymbol{z} + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\boldsymbol{bad}}) + \boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{h}(\hat{\boldsymbol{x}})}{\boldsymbol{\sigma}}\right] \\ &= \left[\frac{\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}}) + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\boldsymbol{bad}}) + \boldsymbol{h}(\hat{\boldsymbol{x}})}{\boldsymbol{\sigma}}\right] \end{aligned} \tag{3-7}$$

If the attacker designs the attack vector $\boldsymbol{a}$ as

$$\boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}}_{\boldsymbol{bad}}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) \tag{3-8}$$

Then (3-15) becomes as follows.

$$\begin{aligned} \boldsymbol{r}_{\boldsymbol{bad}} &= \left[\frac{\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}}) + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\boldsymbol{bad}}) + \boldsymbol{h}(\hat{\boldsymbol{x}})}{\boldsymbol{\sigma}}\right] \\ &= \left[\frac{\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}}) + \boldsymbol{h}(\hat{\boldsymbol{x}}_{\boldsymbol{bad}}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\boldsymbol{bad}}) + \boldsymbol{h}(\hat{\boldsymbol{x}})}{\boldsymbol{\sigma}}\right] \\ &= \left[\frac{\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})}{\boldsymbol{\sigma}}\right] \\ &= \boldsymbol{r} \end{aligned} \tag{3-9}$$

From (3-17), $\boldsymbol{r}_{\boldsymbol{bad}}$ and $\boldsymbol{r}$ become equal. From DSO' s perspective, there is no difference between bad data and original data. It means that the attacker can manipulate state variables without getting caught by BDD. However, for an attacker to create an attack vector $\boldsymbol{a}$ that manipulates all state variables, the attacker must be aware of all state variables.

4 VPP’ s local false data injection attack

As DERs are small and physically distributed, an entity called a virtual power plant (VPP) has emerged to integrate and operate them stably. However, the over generation caused by a number of DERs owned by VPPs in the distribution system can make the overvoltage problem [19]. In this situation, the DSO may issue a curtailment instruction to the DERs to resolve the overvoltage. For the VPPs, who make profits by selling the electricity produced by DERs, curtailment instruction directed to their DERs might cause a negative impact on their profitability. Therefore, to avoid such curtailment, it is possible for VPPs to try FDIA. The assumptions for the VPP attack scenario are as follows:

4.1 DSO assumptions

1) As the spread of AMI and smart inverters increases, measurable active power injection, reactive power injection, and voltage magnitude data are increasing. Thus, in this paper, it was assumed that DSO performed state estimation using active power injection $\boldsymbol{p}$, reactive power injection $\boldsymbol{q}$, and

voltage magnitude $|\boldsymbol{v}|$. Thus, equation (3-6), (3-7), (3-10) are used.

2) For the stability of the distribution system, it is recommended that the voltage magnitude be maintained between 0.95pu and 1.05pu [20]. Therefore, in the simulation, it was assumed that if the voltage magnitude exceeds 1.05pu, the DSO considers it as overvoltage and issues a curtailment instruction [21].

3) When the DSO instructs the curtailment, the DSO determines the amount of curtailment for each DER so that the total amount of curtailment is minimized based on voltage sensitivity [22]. This can be expressed mathematically as follows:

$$\begin{bmatrix} \Delta\boldsymbol{\theta} \\ \Delta|\boldsymbol{v}| \end{bmatrix} = \begin{bmatrix} \boldsymbol{J}_{p\theta}(x) & \boldsymbol{J}_{p|v|}(x) \\ \boldsymbol{J}_{q\theta}(x) & \boldsymbol{J}_{q|v|}(x) \end{bmatrix}^{-1} \begin{bmatrix} \Delta\boldsymbol{p} \\ \Delta\boldsymbol{q} \end{bmatrix} = \begin{bmatrix} \boldsymbol{Sens}_{p\theta}(x) & \boldsymbol{Sens}_{p|v|}(x) \\ \boldsymbol{Sens}_{q\theta}(x) & \boldsymbol{Sens}_{q|v|}(x) \end{bmatrix} \begin{bmatrix} \Delta\boldsymbol{p} \\ \Delta\boldsymbol{q} \end{bmatrix} \quad (4-1)$$

Where $\boldsymbol{J}$ denotes the Jacobian matrix, and $\Delta\boldsymbol{\theta} = [\Delta\theta_2, \dots, \Delta\theta_m]$, $\Delta|\boldsymbol{v}| = [\Delta|v|_2, \dots, \Delta|v|_m]$, $\Delta\mathbf{p} = [\Delta p_2, \dots, \Delta p_m]$, $\Delta\mathbf{q} = [\Delta q_2, \dots, \Delta q_m]$.

$Sens_{p\theta}(x), Sens_{p|v|}(x), Sens_{q\theta}(x), Sens_{q|v|}(x)$ are the sensitivity matrices of the voltage angle to the active power, the voltage magnitude to the active power, voltage angle to the reactive power, voltage magnitude to the reactive power. By using parameters obtained from equation (4-2) and state estimation, curtailment $\Delta\mathbf{p}$ for each DER can be obtained by solving the following optimization problem:

$$\min \sum_{i=2}^{m} \Delta p_i \tag{4-2}$$

$subject\ to$

$$[Sens_{p|v|}(x) \quad Sens_{q|v|}(x)] \begin{bmatrix} \Delta \mathrm{p} \\ \Delta q \end{bmatrix} \leq \boldsymbol{OV} \tag{4-3}$$

where $\boldsymbol{OV}$ is $|V|_i - 1.05pu$.

4.2 VPP assumptions

1) VPP can attain the active power $\boldsymbol{P}$, reactive power $\boldsymbol{Q}$, and voltage magnitude $|\boldsymbol{V}|$ data easily from their smart inverter of DERs.

2) The voltage angle $\boldsymbol{\theta}$, attacker needs to know to design the attacker vector $\boldsymbol{a}$, can be approximated as follows using the radiality of the distribution system [5].

$$S_i = V_i I_i^* \qquad \forall j \in \mathcal{N} \tag{4-4}$$

$$S_{ij} = V_i I_{ij}^* \qquad \forall \{i,j\} \in \mathcal{L} \tag{4-5}$$

$$I_{ij} = \sum_{k=j}^{n} I_k \qquad \forall \{i,j\} \in \mathcal{L} \tag{4-6}$$

$$V_j \approx V_i - \left(P_{ij} r_{ij} + Q_{ij} x_{ij}\right) \qquad \forall j \in \mathcal{N} \tag{4-7}$$

$$\frac{S_{ij}}{V_i} = \sum_{k=j}^{n} \frac{S_k}{V_k} \qquad \forall\{i,j\} \in \mathcal{L} \tag{4-8}$$

$$S_{ij} \approx \sum_{k=j}^{n} S_k \qquad \forall\{i,j\} \in \mathcal{L} \tag{4-9}$$

$$V_j = V_i - \sum_{k=j}^{n} \left(P_k r_{ij} + Q_k x_{ij}\right) \qquad \forall j \in \mathcal{N} \tag{4-10}$$

$$\theta_{ij} \approx P_{ij} x_{ij} - Q_{ij} r_{ij} \qquad \forall\{i,j\} \in \mathcal{L} \tag{4-11}$$

$$\theta_{ij} \approx \sum_{k=j}^{n} \left(P_k r_{ij} - Q_k x_{ij}\right) \qquad \forall\{i,j\} \in \mathcal{L} \tag{4-12}$$

Where $\boldsymbol{\mathcal{N}}$, $\boldsymbol{\mathcal{L}}$ are bus sets and line sets. S_k, P_k, Q_k are injection complex power, active power, and reactive power on bus k. S_{ij}, P_{ij}, Q_{ij} are complex power, active power , and reactive power flow between between i^{th} node and j^{th} node. θ_{ij} is voltage angle difference between i^{th} node and j^{th} node. r_{ij} and x_{ij} are line resistance and line impedance between i^{th} node and j^{th} node. From equation (4-4), (4-5), (4-6), we can derive equation (4-8). Also, equation (4-9) can be achieved because of the characteristic of distribution system. Using equation (4-7), (4-9), V_j can be approximated as shown in equation (4-10) [23]. From equation (4-9), (4-11), we can derive equation (4-12).

3) If the voltage magnitude of the node connected to the DER owned by the VPP exceeds 1.05pu, VPP attempts a local false data injection attack described in section 3.4 to compromise it to under 1.05pu.

4) Upstream node is usually more robust to voltage false data injection

attack [24]. Thus, for VPP performs the false data injection attack on the downstream node.

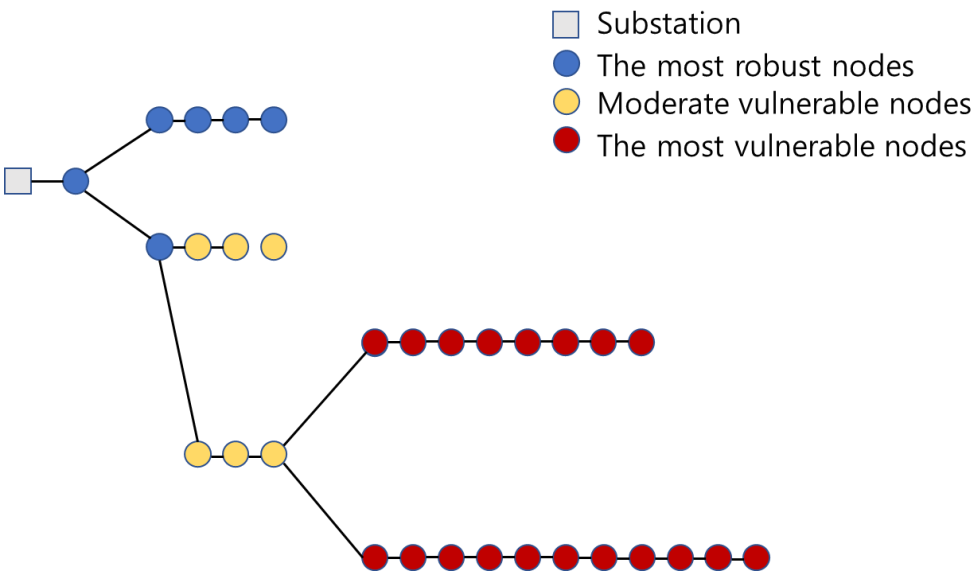

Figure 4.1 Vulnerable node of the IEEE 33 bus test system [24]

5) We assume that VPP performs a local FDIA that manipulates the state variable (voltage magnitude) of a specific node rather than the entire system. In order to avoid curtailment of all DERs that VPP has in the distribution system, FDIA requires all the state variables on the entire system. In general, system information is not disclosed, so it is practically difficult for VPP to attack the entire system. However, if the attacker's goal is to compromise only the state variable of a specific node, it is not necessary to know all the state variables. For example, if the attacker’s goal is to compromise only the voltage magnitude of the ith node, the

attacker can create an attack vector $\boldsymbol{a}$ even if the information for the attacker is available only for the state variable of the ith node and the state variables of the nodes adjacent to the ith node [5]. If that node adjacent to the ith node is j^{th} and k^{th} node, the data that VPP needs to know and manipulate to create an attack vector are shown in Table 4.1.

Table 4.1 Required data for successful FDIA

Measurements data to manipulate	State variable to know for attack vector
$P_j,\ P_i, P_k, Q_j, Q_i, Q_k, \lvert V_i \rvert$	$\lvert V_j \rvert, \lvert V_i \rvert, \lvert V_j \rvert, \theta_{ji}, \theta_{ik}$

6) It is assumed that there is only one VPP in the distribution system. This is because if multi-VPP exists in the distribution system and there are neighbouring solar power plants owned by different VPPs, the attack vector may overlap. Therefore, the attack model when multi-VPP exists is passed to future work.

5 Simulation Setting and Results

5.1 Simulation Environment

IEEE33 test feeder [25] was used to simulate the local false data injection attack of VPPs described in section 3. Detailed test feeder parameters are shown in Table 5.1. It was assumed that DERs belonging to the VPP was connected to nodes 15, 16, and 17 as shown in Fig 5.1. The active power generation of DERs connected to nodes 15, 16, and 17 at the time of the attack is 0.1MW, 0.8MW, and 1.3MW, respectively. The remaining load, generation system parameters are shown in Table 5.2.

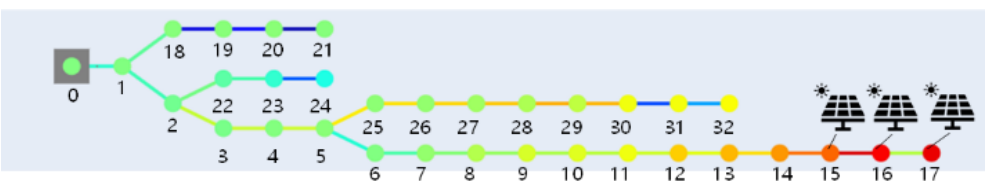

Figure 5.1 IEEE33 test feeder with DERs owned by VPP on nodes 15, 16, 17

Table 5.1 Parameters of test system: Line parameters

Line	From bus	To bus	R (ohm)	X (ohm)	S (MVA)	Line	From bus	To bus	R (ohm)	X (ohm)	S (MVA)
0	0	1	0.09	0.05	7.07	16	16	17	0.73	0.57	2.24
1	1	2	0.49	0.25	5.48	17	1	18	0.16	0.16	2.24
2	2	3	0.37	0.19	3.87	18	18	19	1.5	1.36	2.24
3	3	4	0.38	0.19	3.87	19	19	20	0.41	0.48	2.24
4	4	5	0.82	0.71	3.87	20	20	21	0.71	0.94	2.24
5	5	6	0.19	0.62	2.24	21	2	22	0.45	0.31	2.24
6	6	7	0.71	0.24	2.24	22	22	23	0.9	0.71	2.24
7	7	8	1.03	0.74	2.24	23	23	24	0.9	0.7	2.24
8	8	9	1.04	0.74	2.24	24	5	25	0.2	0.1	2.24
9	9	10	0.2	0.07	2.24	25	25	26	0.28	0.14	2.24
10	10	11	0.37	0.12	2.24	26	26	27	1.06	0.93	2.24
11	11	12	1.47	1.16	2.24	27	27	28	0.8	0.7	2.24
12	12	13	0.54	0.71	2.24	28	28	29	0.51	0.26	2.24
13	13	14	0.59	0.53	2.24	29	29	30	0.97	0.96	2.24
14	14	15	0.75	0.55	2.24	30	30	31	0.31	0.36	2.24
15	15	16	1.29	1.72	2.24	31	31	32	0.34	0.53	2.24

Table 5.2 Parameters of test system: Load and generation

Bus	Pd (MW)	Qd (MVAR)	Pg (MW)	Bus	Pd (MW)	Qd (MVAR)	Pg (MW)
0	0.000	0.000	-	17	0.060	0.020	-1.300
1	0.100	0.060	-	18	0.090	0.040	-0.940
2	0.090	0.040	-	19	0.090	0.040	-
3	0.120	0.080	-	20	0.090	0.040	-0.405
4	0.060	0.030	-	21	0.090	0.040	-
5	0.060	0.020	-	22	0.090	0.050	-
6	0.200	0.100	-	23	0.420	0.200	-
7	0.200	0.100	-	24	0.420	0.200	-
8	0.060	0.020	-	25	0.060	0.025	-
9	0.060	0.020	-	26	0.060	0.025	-
10	0.045	0.030	-	27	0.060	0.020	-
11	0.060	0.035	-	28	0.120	0.070	-
12	0.060	0.035	-	29	0.200	0.600	-
13	0.120	0.080	-	30	0.150	0.070	-1.300
14	0.250	0.010	-	31	0.210	0.100	-
15	0.300	0.020	-0.100	32	0.060	0.040	-0.675
16	0.060	0.020	-0.800	Sum	4.115	2.280	-5.520

The result of the power flow calculation is shown in Table 5.3. From Table 5.3, it is possible to confirm that voltages at the nodes 16 and 17 are 1.056pu and 1.061pu, due to the over-generation at the node 16 and 17.

Table 5.3 Parameters of test system: Power flow results

Bus	$\|V\|$ (p.u)	θ (°)	P (MW)	Q (MVAR)	Bus	$\|V\|$ (p.u)	θ (°)	P (MW)	Q (MVAR)
0	1.000	0.000	1.169	-2.474	17	1.061	6.357	-1.240	0.020
1	1.000	0.100	0.100	0.060	18	1.001	0.166	-0.850	0.040
2	0.997	0.522	0.090	0.040	19	1.001	0.296	0.090	0.040
3	0.998	0.845	0.120	0.080	20	1.001	0.346	-0.315	0.040
4	1.000	1.170	0.060	0.030	21	1.001	0.326	0.090	0.040
5	1.001	2.036	0.060	0.020	22	0.994	0.491	0.090	0.050
6	0.999	2.213	0.200	0.100	23	0.987	0.405	0.420	0.200
7	1.002	2.407	0.200	0.100	24	0.984	0.363	0.420	0.200
8	1.007	2.815	0.060	0.020	25	1.001	2.142	0.060	0.025
9	1.012	3.230	0.060	0.020	26	1.002	2.292	0.060	0.025
10	1.014	3.281	0.045	0.030	27	1.004	3.019	0.060	0.020
11	1.016	3.370	0.060	0.035	28	1.006	3.573	0.120	0.070
12	1.026	4.009	0.060	0.035	29	1.009	3.844	0.200	0.600
13	1.029	4.373	0.120	0.080	30	1.017	4.435	-1.150	0.070
14	1.034	4.661	0.250	0.010	31	1.018	4.500	0.210	0.100
15	1.042	5.005	0.200	0.020	32	1.019	4.617	-0.615	0.040
16	1.056	6.127	-0.740	0.020					

These voltages exceed the DSO’s overvoltage criterion of 1.05pu. Thus, if the VPP does not attempt any attacks, the DSO will issue a curtailment instruction based on voltage sensitivity to resolve the overvoltage. By solving the optimization problem described in DSO assumption 3, the calculated curtailment on each DER is as follows:

$$\Delta p_{17} = 0.199$$

As a result, the DSO will issue the curtailment instruction to the VPP to

reduce the output by the DERs connected to the 17 nodes by 0.199MW. To avoid this, the VPP implements FDIA.

5.2 Non−intelligent attack

First, let’s assume that the VPP tries to compromise node voltage by only changing the node voltage of 16,17 to 1.05pu. non-intelligent attack vector is shown in Table 5.4. In the case of such a non-intelligent attack, the measurement data obtained by the DSO may be affected because of compromised voltage magnitude measurement, but the state estimation result of voltage magnitude will not be changed. Thus, there will be a big difference between measurement values and state estimation values at the nodes 16 and 17 as shown in Table 5.5 and Fig 5.2. In other words, this non-intelligent attack cannot pass the BDD by the DSO.

Table 5.4 non−intelligent attack vector values of voltage magnitude, active power injection, reactive power injection

Bus	$\lvert V\rvert^{attack}$ (pu)
15	0.000
16	-0.006
17	-0.011

Table 5.5 Comparison of Measurement voltage magnitude and state estimated voltage magnitude in non-intelligent attack

Bus	Measurement $\|V\|$ (p.u)	State estimated $\|V\|$ (p.u)	Bus	Measurement $\|V\|$ (p.u)	State estimated $\|V\|$ (p.u)
0	1.000	1.000	17	1.050	1.061
1	1.000	0.999	18	1.001	1.000
2	0.997	0.997	19	1.001	1.000
3	0.998	0.998	20	1.001	1.001
4	1.000	0.999	21	1.001	1.000
5	1.001	1.000	22	0.994	0.993
6	0.999	0.999	23	0.987	0.987
7	1.002	1.002	24	0.984	0.983
8	1.007	1.006	25	1.001	1.001
9	1.012	1.012	26	1.002	1.002
10	1.014	1.013	27	1.004	1.004
11	1.016	1.016	28	1.006	1.006
12	1.026	1.025	29	1.009	1.009
13	1.029	1.029	30	1.017	1.017
14	1.034	1.034	31	1.018	1.017
15	1.042	1.041	32	1.019	1.018
16	1.050	1.055			

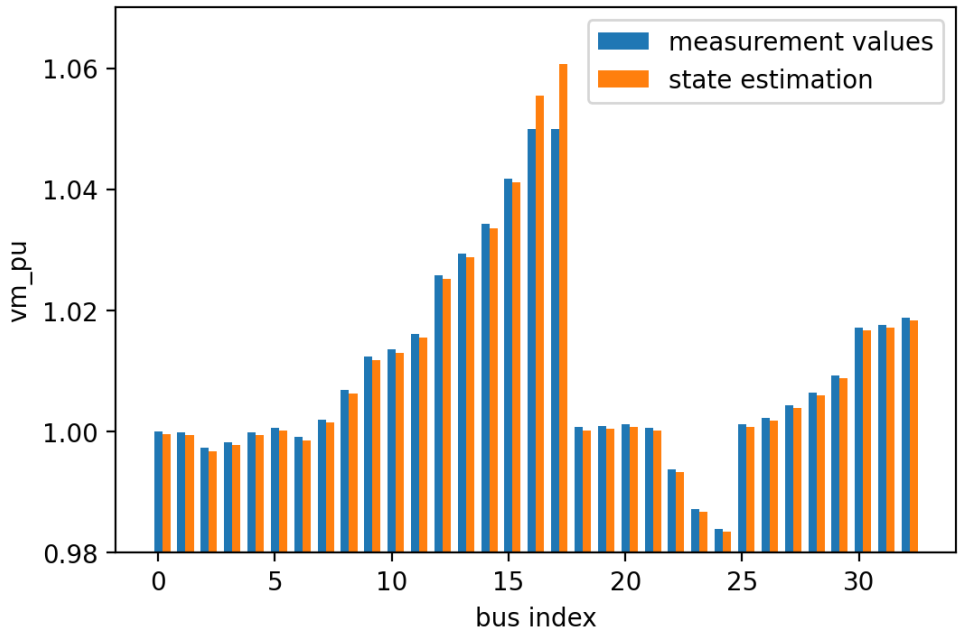

Figure 5.2 Measurement values and state estimation values by non-intelligent attack

5.3 Intelligent attack

Based on the assumption that the VPP designs an attack vector $\boldsymbol{a}$ using equation (3-16) and tries an intelligent attack, the VPP must know $|V_{15}|, |V_{16}|, |V_{17}|, \theta_{1516}, \theta_{1617}$ to create the attack vector. Voltage magnitude can be obtained by smart inverter and voltage angle can be approximated by using equation (4-12). Also, the VPP needs to manipulate P_{15}, P_{16}, $P_{17}, Q_{15}, Q_{16}, Q_{17}, |V_{16}|, |V_{17}|$measurements. From equations (3-6), (3-7), (3-10) and (3-16), calculated attack vector values are shown in Table 5.6.

Table 5.6 Intelligent Attack vector values of voltage magnitude, active power injection, reactive power injection

Bus	$\|V\|^{attack}$ (pu)	P^{attack} (MW)	Q^{attack} (MVAR)
15	0.000	-0.288	-0.378
16	-0.006	-0.467	-0.196
17	-0.011	0.766	0.585

If VPP manipulates $P_{15}, P_{16}, P_{17}, Q_{15}, Q_{16}, Q_{17}, |V_{16}|, |V_{17}|$ using attack vector from Table 5.6, the results can be seen in Fig 5.3. Both the measurement value and the state estimation value of node 16,17 are equal to 1.05pu. Therefore, it is possible to conclude that the attack passed the DSO's BDD. As a result, the DSO recognizes that overvoltage has not occurred and does not issue a curtailment instruction. Thus, the VPP can make additional profit by implementing intelligent FDIA.

Table 5.7 Comparison of Measurement voltage magnitude and state estimated voltage magnitude in intelligent attack

Bus	Measurement $\|V\|$ (p.u)	State estimated $\|V\|$ (p.u)	Bus	Measurement $\|V\|$ (p.u)	State estimated $\|V\|$ (p.u)
0	1.000	1.000	17	1.050	1.050
1	1.000	1.000	18	1.001	1.001
2	0.997	0.997	19	1.001	1.001
3	0.998	0.998	20	1.001	1.001
4	1.000	1.000	21	1.001	1.001
5	1.001	1.001	22	0.994	0.994
6	0.999	0.999	23	0.987	0.987
7	1.002	1.002	24	0.984	0.984

8	1.007	1.007	25	1.001	1.001
9	1.012	1.012	26	1.002	1.002
10	1.014	1.014	27	1.004	1.004
11	1.016	1.016	28	1.006	1.006
12	1.026	1.026	29	1.009	1.009
13	1.029	1.029	30	1.017	1.017
14	1.034	1.034	31	1.018	1.018
15	1.042	1.042	32	1.019	1.019
16	1.050	1.050			

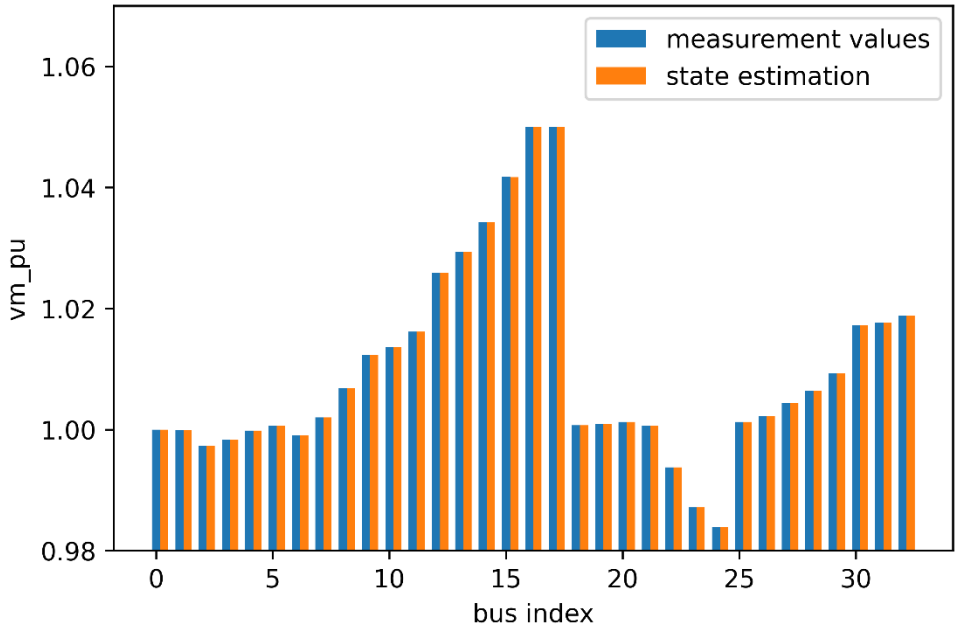

Figure 5.3 Measurement values and state estimation values by intelligent attack

6 Conclusion

In this paper, we investigated FDIA that VPP can try in the distribution system. This study demonstrated that the FDIA that deceives the DSO’s state estimation is technically feasible with only the information that the VPP can obtain from the DER it owns without the effort to install an additional sensor. To demonstrate and simulate this method, technical and mathematical background information for the state estimation, bad data detection, and false data injection attack was presented that was required to understand FDIA conducted by VPP. The method was simulated in the IEEE33 distribution system environment, and it was confirmed that the non-intelligent attack, which simply manipulated voltage, failed due to DSO's bad data detection, but an intelligent attack using an attack vector made with the theory presented was not detected by bad data detection. This paper assumes FDIA for the case where VPP owns only PV. However, if the VPP owns an energy storage system (ESS) that can control the amount of power, it is expected that more flexible attacks will be possible. Thus, for future work, further simulations on the advanced attacks in an environment with the VPP including the ESS, are required. In addition, research on algorithms that can defend against these flexible false data

injection attacks is also needed.

Bibliography

[1] IRENA, “Renewable power generation costs in 2021,” 2021.

[2] IRENA, “Future role of distribution system operators – Innovation Landscape Brief,” 2019.

[3] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011, doi: 10.1145/1952982.1952995.

[4] M. A. Rahman and H. Mohsenian-Rad, “False data injection attacks against nonlinear state estimation in smart power grids,” in *2013 IEEE Power & Energy Society General Meeting*, Vancouver, BC, 2013, pp. 1–5. doi: 10.1109/PESMG.2013.6672638.

[5] R. Deng, P. Zhuang, and H. Liang, “False Data Injection Attacks Against State Estimation in Power Distribution Systems,” *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019, doi: 10.1109/TSG.2018.2813280.

[6] F. Wen and W. Liu, “An Efficient Data-Driven False Data Injection Attack in Smart Grids,” in *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*, Shanghai, China, Nov. 2018, pp. 1–5. doi: 10.1109/ICDSP.2018.8631857.

[7] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, “Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control,” *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019, doi: 10.1109/TSG.2018.2790704.

[8] L. Xie, Y. Mo, and B. Sinopoli, “False Data Injection Attacks in Electricity Markets,” *2010 First IEEE Int. Conf. Smart Grid Commun.*, p. 6.

[9] 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, doi:

10.1109/TSG.2011.2123925.

[10] 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, doi: 10.1109/TSG.2015.2427380.

[11] H. Riggs, S. Tufail, M. Khan, I. Parvez, and A. I. Sarwat, "Detection of False Data Injection of PV Production," in *2021 IEEE Green Technologies Conference (GreenTech)*, 2021, pp. 7–12. doi: 10.1109/GreenTech48523.2021.00012.

[12] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed Load Sharing Under False Data Injection Attack in an Inverter-Based Microgrid," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1543–1551, Feb. 2019, doi: 10.1109/TIE.2018.2793241.

[13] A. J. Wood, B. F. Wollenberg, and G. B. Sheble, *Power Generation, Operation, and Control, Third Edition*. Wiley-Interscience, 2013.

[14] M. Ahmad, *Power System State Estimation*. Artech House, 2013.

[15] N. Katic, L. Fei, G. Svenda, and Zhou Yongji, "Distribution State Estimation field testing," in *2012 China International Conference on Electricity Distribution*, Shanghai, China, Sep. 2012, pp. 1–4. doi: 10.1109/CICED.2012.6508731.

[16] D. L. Lubkexnan and R. H. Jones, "Field results for a distribution circuit state estimator implementation," *IEEE Trans. Power Deliv.*, vol. 15, no. 1, pp. 399–406, Jan. 2000, doi: 10.1109/61.847280.

[17] Z. J. Simendic, V. C. Strezoski, and G. S. Svenda, "In-field verification of the real-time distribution state estimation," in *18th International Conference and Exhibition on Electricity Distribution (CIRED 2005)*, Turin, Italy, 2005, vol. 2005, pp. v3-33-v3-33. doi: 10.1049/cp:20051129.

[18] A. Primadianto and C.-N. Lu, "A Review on Distribution System State Estimation," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3875–3883, Sep. 2017, doi: 10.1109/TPWRS.2016.2632156.

[19] P. Barker, "Overvoltage considerations in applying distributed resources on power systems," in *IEEE Power Engineering Society Summer Meeting*, Chicago, IL, USA, 2002, vol. 1, pp. 109–114. doi: 10.1109/PESS.2002.1043188.

[20] A. Teixeira, G. Dan, 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 *2014 American Control*

Conference, Portland, OR, USA, Jun. 2014, pp. 4372–4378. doi: 10.1109/ACC.2014.6859265.

[21] H. S. Moon, Y. G. Jin, Y. T. Yoon, and S. W. Kim, "Prequalification Scheme of a Distribution System Operator for Supporting Wholesale Market Participation of a Distributed Energy Resource Aggregator," *IEEE Access*, vol. 9, pp. 80434–80450, 2021, doi: 10.1109/ACCESS.2021.3085002.

[22] Q. Zhou and J. W. Bialek, "Generation curtailment to manage voltage constraints in distribution networks," *IET Gener. Transm. Distrib.*, vol. 1, no. 3, p. 492, 2007, doi: 10.1049/iet-gtd:20060246.

[23] M. E. Elkhatib, R. El-Shatshat, and M. M. A. Salama, "Novel Coordinated Voltage Control for Smart Distribution Networks With DG," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 598–605, Dec. 2011, doi: 10.1109/TSG.2011.2162083.

[24] A. Anwar, A. N. Mahmood, and Z. Tari, "Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid," *Inf. Syst.*, vol. 53, pp. 201–212, Oct. 2015, doi: 10.1016/j.is.2014.12.001.

[25] E. B. Mesut and F. W. Felix, "Network reconfiguration in distribution sysyems for loss reduction and load balancing," *IEEE Trans. Power Deliv.*, vol. 4, no. 2, pp. 1401–1407, 1989, doi: 10.1109/61.25627.

초록

상태추정에 대한 허위정보주입공격 연구는 주로 송전계통을 대상으로 연구되어 왔다. 하지만 소규모 분산 자원, 가상 발전소, 에너지 저장장치, 전기차 충전소 등 가상공격에 취약한 자원들이 배전계통에 등장하면서 배전계통에 대한 허위정보주입공격 관련 연구가 최근 활발히 연구되고 있다. 그 중, 이 연구는 가상 발전소 사업자가 배전계통 내에서 시도할 수 있는 허위정보주입공격을 다룬다. 배전계통 내 태양광 발전소와 같은 소규모 분산자원들이 증가하면서 가상 발전소 사업자가 소유한 태양광 발전소에 내려지는 출력제어 조치가 함께 증가하고 있다. 이 연구는 현실적인 조건하에 가상 발전소 사업자가 출력제어 조치를 피하기 위해 시도할 수 있는 허위정보주입공격 모델을 제시한다. 이 공격모델은 가상 발전소 사업자가 자신들이 소유한 태양광 발전소에서 얻는 정보만으로 배전계통 운영자의 상태추정을 속이는 공격이 가능함을 보인다. 이를 증명하기 위해, IEEE 33 테스트 계통을 사용해 본 모델이 배전계통 운영자의 거짓정보감지를 우회할 수 있음을 보였다. 본 연구는 미래에 발생할 수 있는 가상 발전소 사업자의 허위정보주입공격에 대한 기본 개념을 제시하고 미래 배전계통 운영자가 본 연구에 제시한 허위정보주입공격을 방어할 수 있는 알고리즘이 필요함을 보인다.

주요어: DSO, VPP, false data injection attack, state estimation, bad data detection, curtailment

학 번: 2021-28681