The Impact of Load Altering Attacks on Distribution Systems with ZIP Loads

Sajjad Maleki, Shijie Pan, Elena Veronica Belmega, Charalambos Konstantinou, Subhash Lakshminarayana

The Impact of Load Altering Attacks on Distribution Systems with ZIP Loads

Sajjad Maleki*†, Shijie Pan§, E. Veronica Belmega‡†, Charalambos Konstantinou§, and Subhash Lakshminarayana*
* School of Engineering, University of Warwick, Coventry, United Kingdom
† ETIS UMR 8051, CY Cergy Paris Université, ENSEA, CNRS, F-95000, Cergy, France
‡Univ. Gustave Eiffel, CNRS, LIGM, F-77454, Marne-la-Vallée, France
§ CEMSE Division, King Abdullah University of Science and Technology (KAUST)
Email: sajjad.maleki@warwick.ac.uk, subhash.lakshminarayana@warwick.ac.uk

***Abstract*—Load-altering attacks (LAAs) pose a significant threat to power systems with Internet of Things (IoT)-controllable load devices. This research examines the detrimental impact of LAAs on the voltage profile of distribution systems, taking into account the realistic load model with constant impedance Z, constant current I, and constant power P (ZIP). We derive closed-form expressions for computing the voltages of buses following LAA by making approximations to the power flow as well as the load model. We also characterize the minimum number of devices to be manipulated in order to cause voltage safety violations in the system. We conduct extensive simulations using the IEEE-33 bus system to verify the accuracy of the proposed approximations and highlight the difference between the attack impacts while considering constant power and the ZIP load model (which is more representative of real-world loads).**

***Index Terms*—Cybersecurity, distribution system, load altering attack, voltage profile, ZIP load, IoT-controllable devices.**

I. Introduction

The increasing popularity and widespread adoption of Internet-of-Things (IoT)-controllable devices (e.g., smart air conditioners, electric vehicle chargers, etc.) have opened up new attack surfaces to target power grids. In particular, the vulnerability to load-altering attacks (LAAs) that rely on manipulating IoT-controllable appliances has become a significant concern [1], [2]. To launch LAAs, the attacker does not need to access any classified data about the power system but only needs to target the IoT-controllable loads, which have much less protection features as compared to supervisory control and data acquisition (SCADA) systems.

There has been a growing interest in understanding the impact of LAAs on power system operations in recent years. Reference [2] highlighted that large-scale LAAs can lead to significant disruptions in frequency, line failures, and increased operational costs. While the embedded protection schemes can enable power grids to withstand some adverse consequences, LAAs can still lead to controlled load shedding and bulk power partition [3]. LAAs can also be used to exploit congestion-based vulnerabilities in distribution systems and affect the energy market [4]. Authors of [5] conducted an analysis of the effects of LAAs under high renewable energy penetration conditions and showed that the adverse effects of LAAs are exacerbated due to the low inertia conditions.

While the works above analyze a one-time manipulation of the system load, reference [6] analyzed the effect of the so-called dynamic-LAAs (D-LAA) in which the attacker manipulates the system load over a period of time. They showed that such attacks can potentially destabilize the power grid's frequency control loop. In [7], the authors have provided an analytical framework to study the effects of D-LAAs and find the buses from which the attacker can launch the most effective LAA.

Recent works have also investigated detecting and mitigating LAAs. Reference [8] proposed a time-delay neural network to detect LAAs in smart grids by observing the grid's load profile, whereas [9] proposed a convolutional neural network approach to detect LAAs using phase angle and frequency measurements of phasor measurement units (PMUs). A novel economic dispatch approach was introduced in [10] to guarantee the stability of the system under LAA until the attack has been isolated. In [11], the authors introduce an optimal soft open point deployment to mitigate the effects of LAAs on distribution systems by controlling active and reactive power flows in critical normally-open points.

However, despite the growing literature on LAAs, the majority of the works in this area have focused on power balance in the transmission grid and the effects of LAA on the system frequency. In contrast, the impact of LAAs on the distribution grid has received little attention (with the exception of a few works such as [11]). More importantly, none of these works considers the effects of the load models while analyzing the impact of LAAs. It is important to note that real-life loads exhibit voltage-dependent characteristics that must be taken into consideration [12]. In this work, we address this research gap by studying the impact of LAAs on the voltage profile of distribution systems and conduct a comprehensive analysis considering the constant impedance Z, constant current I, and constant power P (ZIP) load model, which represents the voltage-dependency of loads.

However, the non-linear power flow models and the voltage dependency pose significant difficulty in the analysis. To address this challenge, we introduce two approximations – (i) Linearized distribution flow (LinDistFlow) model to calculate the voltage profile of the system which neglects the power losses of lines [13] (ii) ZP approximation for ZIP load model [14]. The accuracy of the approximations in estimating the true voltages of the system under LAA is verified by conducting extensive simulations using the IEEE-33 bus system. To summarize, the key contributions of this paper are:

- Taking the voltage dependency of load demand into account

by implementing the ZIP load model in our analysis.
• Deriving closed-form expressions to calculate the voltage of buses following an LAA and characterizing the minimum number of devices to be compromised in order to cause voltage safety violations in the distribution system.
• Analyzing the effect of the location of LAA on the severity of its consequence on the voltage profile of distribution systems.

The rest of the paper is organized as follows. Section II presents the implemented introduces the system model. The effect of LAA on the voltage profile of distribution systems is analyzed in Section III, followed by the introduction of a closed-form approximation in Section IV for computing the voltage profile of the distribution system with ZIP loads. The numerical results and discussions are presented in Section V. Lastly, Section VI concludes the paper.

II. Preliminaries

In this section, we introduce the system model and describe the load models implemented in this work. Lastly, we delve into the discussion of the LAA model.

A. Power System Model

We use a connected directed graph $G = \{\mathcal{N}, \mathcal{L}\}$ to represent a distribution system, where $\mathcal{N} = \{1, 2, \ldots, N\}$ denotes the set of buses and $\mathcal{L}$ denotes the set of branches. The distribution system graph has a radial structure is hence a tree. Apart from bus 1 (the root), each bus is called the 'child' of its adjacent bus closer to bus 1 by one branch; the latter is called the 'parent' bus of the child. Thus, the set of branches is defined as $\mathcal{L} = \{(\pi_i, i) \mid \pi_i,\ i \in \mathcal{N}\}$, π_i is parent of i. In this system, bus 1 is the generator bus. Furthermore, for simplicity and to clearly illustrate our results, we assume that there is no distributed generation. We denote by $\mathcal{D}_k$ the set of buses which forms the unique path connecting bus 1 to bus k, excluding bus 1 and including bus k. The impedance and the power flow of the line $(\pi_i, i) \in \mathcal{L}$ is denoted by $z_{\pi_i,i} = r_{\pi_i,i} + j\ x_{\pi_i,i}$ ($r_{\pi_i,i}$ is the resistance and $x_{\pi_i,i}$ is the reactance of the line) and $S_{\pi_i,i} = P_{\pi_i,i} + j\ Q_{\pi_i,i}$ ($S_{\pi_i,i}$, $P_{\pi_i,i}$, and $Q_{\pi_i,i}$ stand for apparent, active, and reactive power flows of the line) respectively. The load of the bus $i \in \mathcal{N}$ is denoted by S_i^0 such that

$$S_i^0 = P_i^0 + jQ_i^0, \tag{1}$$

where S_i^0, P_i^0 and Q_i^0 represent the apparent, active and reactive power demands respectively.

B. Power Flow Model

1) Branch flow model: The branch flow model represents the full AC power flow and the equations describing the steady state of the system are given by (assuming no distributed generation) [13]:

$$\sum_{k:i\to k} S_{i,k} = S_{\pi_i,i} - z_{\pi_i,i}\ |I_{\pi_i,i}|^2 - S_i^0, \tag{2}$$

where $V_{\pi_i} - V_i = z_{\pi_i,i}\ I_{\pi_i,i}$, $S_{\pi_i,i} = V_{\pi_i}\ I^*_{\pi_i,i}$; while $I_{\pi_i,i}$ is the current flowing through the branch $(\pi_i, i) \in \mathcal{L}$, V_i and V_{π_i} are the voltages of the bus $i \in \mathcal{N}$ and of its parent bus respectively, and the superscript $(\cdot)^*$ denotes the conjugate of a complex number.

2) LinDistflow (LDF): LinDistflow (LDF) is a simplified form of the branch flow model in (2) that ignores the branch power losses [13]. Under this model, the voltage drop between two consecutive buses is given by

$$V_k = \sqrt{V_{\pi_k}^2 - 2\ r_{\pi_k,k}\ P_{\pi_k,k} - 2\ x_{\pi_k,k}\ Q_{\pi_k,k}}. \tag{3}$$

LDF makes it possible to obtain a linearized model for computing the voltages of buses by substituting $U_k = V_k^2$.

C. Load Models

1) Constant power load model: The constant power (CP) load model is described by (1), where the load is assumed to be independent of the bus voltages.

2) ZIP load model: Real-world loads are voltage-dependent and the ZIP load model is used to show this dependency [12]. Under this model, the load at node $i \in \mathcal{N}$ as a function of V_i is given by

$$S_i^{ZIP}(V_i) = P_i^0(\alpha_p + \beta_p V_i + \gamma_p V_i^2) + jQ_i^0(\alpha_q + \beta_q V_i + \gamma_q V_i^2), \tag{4}$$

where $\alpha_k,\ \beta_k$, and γ_k, $k \in \{p, q\}$ are the coefficients of the ZIP model for constant power, constant current, and constant impedance respectively; and they are obtained experimentally in [15]. Also we have $\alpha_k + \beta_k + \gamma_k = 1$.

In this work, we focus on LAAs in which an attacker with access to a cluster of IoT-controllable devices simultaneously turns them on or off, causing an abrupt change in the load demand. We focus on static LAAs, which are one-time manipulations of the demand. If the attack occurs in bus $a \in \mathcal{N}$ and the additional load demand arising from LAA, (i) considering CP load is given by $S_a^A = P_a^A + jQ_a^A$, and (ii) considering ZIP load is given by

$$S_a^{A_{ZIP}} = P_a^A(\alpha_p + \beta_p V_a + \gamma_p V_a^2) + jQ_a^A(\alpha_q + \beta_q V_a + \gamma_q V_a^2). \tag{5}$$

In distribution systems, arguably the most undesirable consequence of LAAs is the alteration of the voltage profile, which will be the main focus of this work. In particular, the objective of this work is to highlight the difference in the impact of LAAs considering realistic ZIP load model as opposed to the CP model used in several prior works.

We note that the impact of a malicious load alteration on the distribution network voltages can be determined by solving the power flow equations described in (2). Nevertheless, this approach makes it hard to obtain analytical insights about how the effects of various attacks differ. In what follows, we derive analytically tractable expressions to quantify the impact of LAAs using simplified models that nevertheless provide an accurate estimate of the true impact in practice.

III. Quantified Analysis of the Effect of LAA on the Voltage Profile

The impact of LAAs in the distribution network depends on two key factors (among others) that are the primary focus of this work:

1. Dependence on the underlying load model.

2. Dependence on the location (i.e., the bus index) where the LAA occurs.

In this section, we will examine how these two factors affect the voltage profile of the distribution system. Our aim is to obtain closed-form expressions to gain an analytical understanding. To end this, we make two simplifying assumptions: (i) We use the LDF model to approximate the distribution system bus voltages following the LAA; and, (ii) We use an approximate model for ZIP loads called ZP [14]. We start by analyzing the impact of LAAs under the CP load model.

A. Constant Power Loads

This subsection illustrates how to compute the voltages of buses while there is an LAA in the system. First, using (3), we can write the voltage of any bus $k \in \mathcal{N}$ in terms of the generator bus voltage as

$$V_k = \sqrt{V_1^2 - 2\sum_{i\in\mathcal{D}_k}(r_{\pi_i,i}P_{\pi_i,i} + x_{\pi_i,i}Q_{\pi_i,i})}. \quad (6)$$

Based on (6), if there is an LAA in bus a, the voltage of bus k (V_k^a) can be obtained as

$$V_k^a = \sqrt{V_1^2 - 2\Delta_k - 2P_a^A r_{k,a} - 2Q_a^A x_{k,a}}, \quad (7)$$

where $\Delta_k = \sum_{i\in\mathcal{D}_k}(r_{\pi_i,i}P_{\pi_i,i} + x_{\pi_i,i}Q_{\pi_i,i})$, $r_{k,a} = \sum_{i\in\{\mathcal{D}_a\cap\mathcal{D}_k\}} r_{\pi_i,i}$, and $x_{k,a} = \sum_{i\in\{\mathcal{D}_a\cap\mathcal{D}_k\}} x_{\pi_i,i}$. From Δ_k, we notice that, generally, an LAA at the leaf buses results in a higher drop in the voltage profile of the distribution system since the values of $r_{k,a}$ and $x_{k,a}$ will be higher (notice that when a is a leaf bus, the set $\mathcal{D}_a$ has more elements). In other words, an LAA targeting leaf buses has a more severe impact on the system.

Using (7), we can obtain an expression to find the number of devices (e.g., air conditioners) the attacker needs to turn on simultaneously in order to cause system voltage safety violations. Let us denote V_{th} as the voltage safety threshold, P_D and Q_D as the active and reactive powers of each device. Then, using (7), and following straightforward simplifications, we obtain (assuming $V_1 = 1$ p.u.)

$$P_a^A = \frac{U_{th} - 1 + 2\Delta_k}{-2(r_{k,a} + \frac{Q_D}{P_D}x_{k,a})}, \quad (8)$$

where $U_{th} = V_{th}^2$. Using (8), P_a^A/P_D gives the number of devices that should be simultaneously switched on/off to achieve the attacker's objective.

B. ZIP Loads

In this subsection, we conduct a similar analysis considering the ZIP load model. The key difference, in this case, is that as the voltage of the system drops due to the LAA, the loads will consume less power [15]. As a result, we expect to obtain a better voltage profile (and a lower voltage drop) under the ZIP model. Using (7) and (5), we obtain the following voltage in bus $k \in \mathcal{N}$ when the LAA takes place in bus a

$$V_k^a = \sqrt{V_1^2 - 2\Delta_k^{ZIP} - 2P_a^{A_{ZIP}} r_{k,a} - 2Q_a^{A_{ZIP}} x_{k,a}}, \quad (9)$$

where

$$\Delta_k^{ZIP} = \sum_{i\in\mathcal{D}_k}\left(r_{\pi_i,i}P_{\pi_i,i}^{ZIP} + x_{\pi_i,i}Q_{\pi_i,i}^{ZIP}\right), \quad (10)$$
$$P_{\pi_i,i}^{ZIP} = P_{\pi_i,i}(\alpha_p + \beta_p V_i + \gamma_p V_i^2),$$
$$Q_{\pi_i,i}^{ZIP} = Q_{\pi_i,i}(\alpha_q + \beta_q V_i + \gamma_q V_i^2),$$
$$P_a^{A_{ZIP}} = P_a^A(\alpha_{p_a} + \beta_{p_a} V_a + \gamma_{p_a} V_a^2),$$
$$Q_a^{A_{ZIP}} = Q_a^A(\alpha_{q_a} + \beta_{q_a} V_a + \gamma_{q_a} V_a^2).$$

We note that in this case, the bus voltages cannot be obtained in closed form because the above load values depend quadratically on the voltages. Thus, we use an iterative algorithm in which to calculate the voltages. This iterative method is based on the backward-forward sweep (BFS) method [16] with an additional iteration feature, which updates the loads values in each step based on the previous step calculated voltage. The full description of the algorithm is omitted here because of the lack of space. We note once again that the iterative algorithm despite its effectiveness does not yield any analytical insights (which is the main objective of this paper). We address this issue in the following section by introducing one more approximation.

IV. Closed-form Approximation of Voltages Under the ZIP Model

In this section, we propose an alternative solution for computing the bus voltages with the ZIP model in one shot or closed form (instead of the iterative procedure) by introducing an additional approximation.

A. No Attack

To this aim we exploit the approximate ZP model for the ZIP model introduced in [14]. This eliminates the βV_i term of the load model in (4) and the resulting load is

$$S_i^{ZP}(V_i) = P_i^0(\alpha_p' + \gamma_p' V_i^2) + jQ_i^0(\alpha_q' + \gamma_q' V_i^2), \quad (11)$$

where $\alpha_p' = \alpha_p + \frac{\beta_p}{2}$,$\alpha_q' = \alpha_q + \frac{\beta_q}{2}$,$\gamma_p' = \gamma_p + \frac{\beta_p}{2}$, and $\alpha_q' = \gamma_q + \frac{\beta_q}{2}$. Implementing the ZP model in (6) we obtain

$$V_k = \sqrt{V_1^2 - 2\sum_{i\in\mathcal{D}_k}\left(r_{\pi_i,i}P_{\pi_i,i}^{ZP} + x_{\pi_i,i}Q_{\pi_i,i}^{ZP}\right)}, \quad (12)$$

where $P_{\pi_i,i}^{ZP} = P_{\pi_i,i}(\alpha_p' + \gamma_p' V_i^2)$, $Q_{\pi_i,i}^{ZP} = Q_{\pi_i,i}(\alpha_q' + \gamma_q' V_i^2)$. Then, a variable change ($U_k = V_k^2$) results in a set of linear equations which can be depicted as matrix form as follows

$$\mathbf{U}_{(N-1)\times 1} = \Omega_{(N-1)\times N}\begin{bmatrix}1\\ \mathbf{U}\end{bmatrix}_{N\times 1}, \quad (13)$$

where $\mathbf{U}$ is the vector of squares of voltages, and $\Omega_{(N-1)\times N}$ is the matrix of entries:

$$\omega_{i,1} = 1 - \sum_{m\in\mathcal{D}_i}(2r_{\pi_m,m}P_{\pi_m,m}^0\alpha_p' + 2x_{\pi_m,m}Q_{\pi_m,m}^0\alpha_q'), \quad (14)$$

$$\omega_{i,k} = \begin{cases}\sum_{c=2}^{i} -2r_{\pi_c,c}P_k^0\gamma_p' - 2x_{\pi_c,c}Q_k^0\gamma_q', & \text{if } i \in \mathcal{D}_k\\ \omega_{\pi_i,k}, & \text{otherwise,}\end{cases} \quad (15)$$

where $P^0_{\pi_m,m}$ and $Q^0_{\pi_m,m}$ are active and reactive powers flowing in the branch $(\pi_m, m) \in \mathcal{L}$ while $V_m = 1$ p.u., also $2 \leq i \leq N$ and $2 \leq k \leq N$. To solve the system of linear equations in (13), we can re-write it as follows:

$$\left(\mathbf{I}_{(N-1)\times(N-1)} - \Omega'_{(N-1)\times(N-1)}\right) \mathbf{U}_{(N-1)\times 1} = \Omega''_{(N-1)\times 1}, \tag{16}$$

where $\Omega''_{(N-1)\times 1} = [\omega_{2,k}]$, $\Omega'_{(N-1)\times(N-1)} = [\omega_{i,k}]$ for $i = \{3, 4, ..., N\}$, and $k \in \mathcal{N}$. To sum up, our closed-form or one-shot approximation of the bus voltages is: $\mathbf{U}_{(N-1)\times 1} = (\mathbf{I}_{(N-1)\times(N-1)} - \Omega'_{(N-1)\times(N-1)})^{-1}\, \Omega''_{(N-1)\times 1}$, assuming that $\det(\mathbf{I}_{(N-1)\times(N-1)]} - \Omega'_{(N-1)\times(N-1)}) \neq 0$, which seems to be always the case in our setting given the relatively small values of $\omega_{i,j} \ll 1$ obtained numerically.

B. Under LAA

Introducing LAA into the distribution system will lead to changes in the coefficients of the proposed closed-form approximation. Here, we can also re-write the voltages in equation (7) as: $\mathbf{U}^A_{(N-1)\times 1} = \Omega^A_{(N-1)\times N} \begin{bmatrix} 1 \\ \mathbf{U}^A \end{bmatrix}_{N\times 1}$. The new coefficients of the matrix Ω^A are denoted by $\omega^A_{i,k}$, which comprises two parts: $\omega_{i,k}$ representing the calculated coefficients for normal operation circumstances, and $\omega^a_{i,k}$ representing the additional part resulting from LAA. Considering an LAA in bus a, the additional load resulting from the LAA is given by $S^{A_{ZP}}_a = P^{A_0}_a(\alpha'_p + \gamma'_p U_a) + jQ^{A_0}_a(\alpha'_q + \gamma'_q U_a)$.

Then, using equation (7) we obtain the following matrix coefficients for $i \geq 2$ and $k \geq 2$:

$$\omega^a_{i,1} = \sum_{c\in\{\mathcal{D}_i \cap \mathcal{D}_a\}} -2P^{A_0}_a \alpha'_p r_{\pi_c,c} - 2Q^{A_0}_a \alpha'_q x_{\pi_c,c}, \tag{17}$$

$$\omega^a_{i,k} = \begin{cases} -2r_{\pi_i,i} P^{A_0}_a \gamma'_p - 2x_{\pi_i,i} Q^{A_0}_a \gamma'_q, & \text{if } i \in \mathcal{D}_a \\ \omega^A_{\pi_i,k}, & \text{otherwise.} \end{cases} \tag{18}$$

Finally, we obtain $\omega^A_{i,k} = \omega_{i,k} + \omega^a_{i,k}$, for $i \geq 2$ and $k \geq 1$. $\Omega^A_{(N-1)\times N} = [\Omega^{A''}_{(N-1)\times 1}\ \Omega^{A'}_{(N-1)\times(N-1)}]$ is formed by the new coefficients and the new bus voltages can be derived as

$$\mathbf{U}^A_{(N-1)\times 1} = (\mathbf{I} - \Omega^{A'})^{-1}\Omega^{A''}. \tag{19}$$

Solving (19) enables calculating the voltages of buses by solving a system of linear equations for a system with LAA.

C. Number of Devices Required for LAA

In this subsection, we wish to determine the minimum number of targeted devices in the LAA at leaf buses that are required to cause a voltage drop below the acceptable voltage nadir (V_{th}). For this, we utilize the (19) in Subsection IV-B. In these equations, the voltage value at the leaf bus under attack is known to be V_{th}, while the values of $P^{A_0}_a$ and $Q^{A_0}_a$ are unknown. Consequently, we have $Q^{A_0}_a = \frac{Q_D}{P_D} P^{A_0}_a$.

Since the voltage value at the leaf bus under attack is known, the linear system allowing us to compute the other bus voltages and $P^{A_0}_a$ will change as follows. The new coefficients of the Ω^d matrix are:

$$\omega^D_{i,1} = \begin{cases} \omega_{i,1} + V^2_{th}\omega_{i,a}, & \text{if } i \neq a, \\ \omega_{i,1} + V^2_{th}(\omega_{i,a} - 1), & \text{if } i = a, \end{cases} \tag{20}$$

$$\omega^D_{i,k} = \begin{cases} \sum_{c\in\mathcal{D}_i} -2r_{\pi_c,c}\alpha'_p - 2\frac{Q_D}{P_D} x_{\pi_c,c}\alpha'_q, \\ \qquad \text{if } k = a, i \in \mathcal{D}_a, \\ \omega^D_{\pi_i,k}, \quad \text{if } k = a, i \notin \mathcal{D}_a, \\ \omega_{i,k}, \quad \text{otherwise.} \end{cases} \tag{21}$$

We define $\mathbf{X}$ as a vector with the same dimension as $\mathbf{U}$. All of the elements of this vector are the same as $\mathbf{U}$ except for one, where $\mathbf{X}$ contains $P^{A_0}_a$ instead of U_a (since we already know $U_a = V^2_{th}$). We can then obtain the matrices $\Omega^d = [\Omega^{d''}\Omega^{d'}]$. At last, by solving the linear system of equations

$$(\mathbf{I}' - \Omega^{d'})\mathbf{X} = \Omega^{d''}, \tag{22}$$

where $\mathbf{I}'$ is an identity matrix but the a^{th} element of the main diagonal is zero. we obtain the bus voltages as well as the required P^{A0}_a. Then, Q^{A0}_a can be calculated based on this.

V. Numerical Results and Discussion

All the simulations have been carried out in MATPOWER using the IEEE-33 bus system. For simulations, P^0_i and Q^0_i are 50% of default values in MATPOWER case files. The ZIP load coefficients of all the buses which are set to the residential loads-type F [15]. To integrate the LAAs, we employ (17) - (19) using $n_{atk}P^0$ and $n_{atk}Q^0$ as $P^{A_0}_a$ and $Q^{A_0}_a$ respectively, in which n_{atk} is the number of attacked devices. Note that each device has unique P^0, Q^0 and ZIP coefficients and according to the type of attacked devices, they all are altered based on [15]. Further, we set $V_{th} = 0.95$ p.u. In what follows, we present results on the accuracy of approximations introduced in Sections II-B and IV-A and find the critical load to be manipulated under the LAA to cause safety violations in the bus voltages.

A. Accuracy of the Approximations

First, we examine the accuracy of the approximations in computing the bus voltages considering the ZIP load model and ignoring the LAAs. Note that the BFS method provides the true voltages since it considers the full AC power flow model in (2). Considering V^{BFS}_i as the true value for the voltage, the maximum error, $e_i = \frac{|V^{BFS}_i - V_i|}{V^{BFS}_i} \times 100$, (over all the buses) for the voltages computed using (16), and represented in Fig. 1 was 1.07% (for a base voltage of 0.97 p.u.), which is a relatively small value and justifies the use of the approximations.

B. Impact of LAAs

Next, we evaluate the impact of the location of LAA and the load model under consideration in three scenarios – (i) no LAA, (ii) LAA at bus 3, and (iii) LAA at bus 18. Based on the configuration of the test system, bus 18 is a leaf bus. For both scenarios with LAA, the victim appliances are chosen to be 800 air conditioners. To evaluate the attack impact, we compute the voltages using the iterative method.

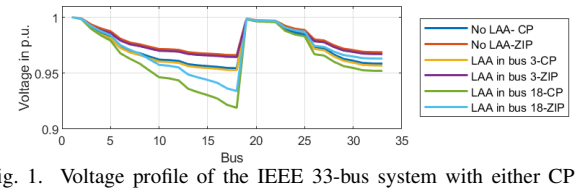

Fig. 1. Voltage profile of the IEEE 33-bus system with either CP or ZIP loads under an LAA manipulating 800 air conditioners.

TABLE I
ADDITIONAL LOAD DEMAND CAUSED BY LAAS WITH ZIP LOADS.

LAA Bus	Additional P (kW)	Additional Q(kVAR)
3	395.53	97.58
18	386.09	80.20

Fig. 1 illustrates that launching an LAA at a leaf bus has a more severe impact on the voltage profile. However, when we consider the ZIP model, the negative impact of the LAA is reduced while two factors contribute to the distinct voltage profiles observed in the system. The first factor is the location of the LAA, in which case we observe an effect similar to the case of CP loads (i.e., an attack at the leaf bus has a more severe impact). On the other hand, a second factor includes the dependency of the load on the nodal voltages.

Table I represents the additional net load demand resulting from LAA in two different attack scenarios. We note that the net load demand considering the voltage dependency is lower when the attack occurs at the leaf buses. Thus we can conclude that the voltage dependency of loads will alleviate the effect of the first factor to some extent.

C. Critical Attacks

Finally, we compute the least number of appliances to be compromised to cause system voltage safety violation. Equation (8) determines the critical device count for the system with CP loads, while (22) calculates it for the system with ZIP loads. The results are summarized in Table II where we inject LAAs at different leaf buses in the system (one at a time). We observe that launching an LAA at bus 18 requires the least number of compromised devices. This also confirms the results observed in Fig. 1, where we similarly observe that launching an LAA at bus 18 is most detrimental to the system.

In Fig. 2, the voltage profile (computed using the model in Subsection IV-B) of the system is depicted in the presence of an LAA at bus 18. According to this figure, based on the closed-form approximation, launching LAA on 282 air conditioners, 163 resistive heaters, or 151 copiers in bus 18 is sufficient to cause voltage constraint violation.

VI. CONCLUSIONS

In this paper, we have investigated the impact of load altering attacks (LAAs) on the voltage profile of distribution systems with ZIP loads. Our analysis highlighted the impact of the location of LAA for two different load models (CP and ZIP). We proposed a closed-form method to compute the bus voltages with the ZIP load model which has a reduced complexity but suffers from an accuracy loss, because assumptions needed to obtain the closed-form expressions. Our future research will focus on investigating the impact of LAAs in more complex systems that also contain distributed generation (e.g., solar panels). Additionally, we will devise strategies to mitigate the adverse effects of the LAAs.

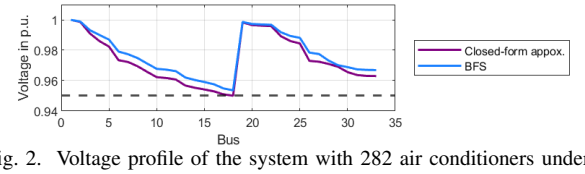

Fig. 2. Voltage profile of the system with 282 air conditioners under LAA in bus 18 obtained by proposed closed-form approximation and BFS.

TABLE II
REQUIRED NUMBER OF DEVICES TO BE MANIPULATED IN DIFFERENT LEAF BUSES TO CAUSE A VOLTAGE DROP BELOW 0.95 P.U.

Bus	ACs		Resistive heater		Copiers	
	CP	ZIP	CP	ZIP	CP	ZIP
18	100	282	66	163	59	151
22	3998	6127	2713	3169	2428	2884
25	3433	5251	2068	2441	2003	2270
33	327	1177	214	481	193	447

REFERENCES

[1] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[2] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium*, 2018, pp. 15–32.

[3] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against iot demand attacks," in *USENIX Security Symposium*, 2019, pp. 1115–1132.

[4] O. G. M. Khan, E. F. El-Saadany, A. Youssef, and M. F. Shaaban, "Cyber security of market-based congestion management methods in power distribution systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8142–8153, 2021.

[5] S. Lakshminarayana, J. Ospina, and C. Konstantinou, "Load-altering attacks against power grids under covid-19 low-inertia conditions," *IEEE Open Access J. Power Energy*, vol. 9, pp. 226–240, 2022.

[6] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2018.

[7] S. Lakshminarayana, S. Adhikari, and C. Maple, "Analysis of iot-based load altering attacks against power grids using the theory of second-order dynamical systems," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4415–4425, 2021.

[8] E.-N. S. Youssef, F. Labeau, and M. Kassouf, "Detection of load-altering cyberattacks targeting peak shaving using residential electric water heaters," *Energies*, vol. 15, no. 20, p. 7807, 2022.

[9] H. Jahangir, S. Lakshminarayana, C. Maple, and G. Epiphaniou, "A deep learning-based solution for securing the power grid against load altering threats by iot-enabled devices," *IEEE Internet Things J.*, 2023.

[10] Z. Chu, S. Lakshminarayana, B. Chaudhuri, and F. Teng, "Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch," *IEEE Trans. Smart Grid*, 2022.

[11] Z. Liu and L. Wang, "A robust strategy for leveraging soft open points to mitigate load altering attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1555–1569, 2021.

[12] T. Van Cutsem and C. Vournas, *Voltage stability of electric power systems*. Springer Science & Business Media, 2007.

[13] M. Baran and F. F. Wu, "Optimal sizing of capacitors placed on a radial distribution system," *IEEE Trans. Power Del.*, vol. 4, no. 1, pp. 735–743, 1989.

[14] F. U. Nazir, B. C. Pal, and R. A. Jabr, "Approximate load models for conic opf solvers," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 549–552, 2020.

[15] A. Bokhari, A. Alkan, R. Dogan, M. Diaz-Aguiló, F. De Leon, D. Czarkowski, Z. Zabar, L. Birenbaum, A. Noel, and R. E. Uosef, "Experimental determination of the zip coefficients for modern residential, commercial, and industrial loads," *IEEE Trans. Power Del.*, vol. 29, no. 3, pp. 1372–1381, 2013.

[16] D. Shirmohammadi, H. W. Hong, A. Semlyen, and G. Luo, "A compensation-based power flow method for weakly meshed distribution and transmission networks," *IEEE Trans. Power Syst.*, vol. 3, no. 2, pp. 753–762, 1988.