2014 American Control Conference (ACC)
June 4-6, 2014. Portland, Oregon, USA

Security of Smart Distribution Grids: Data Integrity Attacks on Integrated Volt/VAR Control and Countermeasures

André Teixeira György Dán Henrik Sandberg
ACCESS Linnaeus Centre,
KTH Royal Institute of Technology,
Stockholm, Sweden
Email: {andretei,gyuri,hsan}@kth.se

Robin Berthier Rakesh B. Bobba Alfonso Valdes
Information Trust Institute,
University of Illinois Urbana-Champaign,
Urbana, IL, USA
Email: {rgb,rbobba,avaldes}@illinois.edu

***Abstract*— We examine the feasibility of an attack on the measurements that will be used by integrated volt-var control (VVC) in future smart power distribution systems. The analysis is performed under a variety of assumptions of adversary capability regarding knowledge of details of the VVC algorithm used, system topology, access to actual measurements, and ability to corrupt measurements. The adversary also faces an optimization problem, which is to maximize adverse impact while remaining stealthy. This is achieved by first identifying sets of measurements that can be jointly but stealthily corrupted. Then, the maximal impact of such data corruption is computed for the case where the operator is unaware of the attack and directly applies the configuration from the integrated VVC. Furthermore, since the attacker is constrained to remaining stealthy, we consider a game-theoretic framework where the operator chooses settings to maximize observability and constrain the adversary action space.**

I. Introduction

Electric power networks are critical infrastructures essential to modern societies. Due to the technological development in sensing, actuating, and communication technologies over the last decades, the monitoring and operation of power networks has changed paradigms [1]. While power tranmission networks are readily monitored and controlled remotely, at the distribution level Distribution System Automation (DSA) is emerging as a suite of smart grid applications, using Volt-VAR Control (VVC) with objectives to maintain voltage and power factor within acceptable ranges (95 to 105 % of nominal, and in particular above 95 % at line end), as well as achieving some conservation goal [2].

VVC is considered the most desired and cost-effective function of DSA [3]. The related function of conservation voltage reduction (CVR) [4] may be employed to achieve energy savings on the order of 3 %, by reducing distribution voltage to the lower end of the nominal range while maintaining appropriate performance of equipment at end-customer loads. Voltage regulation is achieved by means of a load tap changer (LTC), which selects from a discrete set of tap settings along the transformer coils to achieve the desired voltage. Similarly, capacitor banks are energized to regulate the reactive power (VAR) [2]. The optimal LTC and capacitor bank settings may be viewed as a discrete optimization problem, solved by a variety of heuristics or proprietary methods. These optimization methods are designed to minimize power loss while maintaining voltage and power factor in desired ranges.

Smart grid system models are envisioned to provide integrated VVC (IVVC), wherein the sensors on the line communicate to a centralized volt-var controller at a substation [5]. Based on these measurements, as well as pseudo-measurements in the form of historical or other estimates, the central controller executes an algorithm that seeks a (near-) optimum setting of LTC and capacitors for the distribution feeder as a whole. Settings significantly far from the optimum result in, among other effects, excessive loss of active and reactive power in the distribution feeder, as well as potential damage to end-customer equipment and excessive wear on LTC and capacitors.

However, the ubiquitous and pervasive use of communication networks and heterogeneous IT components from different vendors has made the overall power system more vulnerable to cyber threats [6], [7]. At the power transmission network, there has been a substantial work on analyzing the classes of undetectable data injection attacks [8], [9], [10], [11], their impact on the system operation [12], [13], and possible protective and countermeasures [14], [15], [16], [17]. As for the distribution network, privacy issues related to smart meters were addressed [18], as well as cyber-physical modeling and attack impact analysis [19], [20], [21], albeit not addressing data integrity attacks on voltage measurements or IVVC. Related to voltage control in distribution grids, a game-theoretic approach for choosing detection thresholds was proposed in [22] for non-stealthy adversaries.

In this paper, we study the vulnerabilities that may be introduced by the IVVC scheme when an adversary is able to inject false data measurements into the system. In the attack model considered, the adversary can compromise some of the communications between measurement devices and the central controller. He or she uses this to inject false data into the system, causing the controller to issue commands to LTC and capacitors that are suboptimal. The adversary does this in such a way as to be stealthy and maintain the

This work was supported in part by the U.S. Department of Energy (DE-OE0000097), the Illinois-Sweden Program for Educational and Research Exchange (INSPIRE) at the University of Illinois, Urbana-Champaign, and at KTH Royal Institute of Technology, by the Swedish Research Council (grant 2013-5523), and by the ACCESS Linnaeus Centre.

attack for a long time. As such, falsified measurements must be maintained within a range that do not trigger threshold or bad data detections at the controller or through some independent detection channel. We explore the impact to the system that the adversary can inflict within these constraints. Although one may at first assume that the impact in terms of, for example, power loss would be relatively modest, it may be economically significant to a distribution system operator who may be operating within tight economic margins.

A contribution of this paper is to state the necessary and sufficient conditions for undetectable data injection attacks, under varying operator conditions. Seemingly similar conditions have been stated for transmission grids [8], [9], but these *do not* apply here since the operator may switch the grid configuration in order to detect the attacks, or to decrease the operational costs. In our study, the goal of the adversary is to increase the economic costs of the operator, while remaining undetected. This can be achieved by fooling the operator into running the grid at an unnecessarily high voltage level, for example. To analyze such attacks, we introduce a novel game-theoretic model of the operator and the adversary. The model can be used to bound the possible economic losses incurred by the operator under the undetectable attacks.

The structure of the paper is as follows. In Section II, we derive models of distribution grids and the operator. In Section III, we obtain conditions for undetectable attacks and introduce the game-theoretic model. The new concepts are illustrated by means of an example. In Section IV, we perform a feasibility study of the attacks in a distribution grid simulation environment. Finally, in Section V, some concluding remarks are given.

II. Distribution System and Operator Models

Below we model distribution grids using guidelines from [23] and describe the IVVC scheme.

A. Distribution system model

Consider a distribution network similar to the one depicted in Fig. 1. The consumers are modeled as evenly distributed constant current loads along each line, as is commonly assumed [23]. A distribution line between nodes i and j is modeled by the total load consumed through that line, denoted as the complex variable $I_{ij} \in \mathbb{C}$, and the line impedance $Z_{ij} \in \mathbb{C}$. The current entering the line from i to j is denoted as the phasor $i_{ij} \in \mathbb{C}$ and the voltage at node i as $v_i \in \mathbb{C}$. The distribution network can then be modeled as follows.

Kirchoff's current law: The current leaving node i and flowing towards node j is

$$i_{ij} = I_{ij} + i_j + \sum_{k \in \mathcal{N}_j \setminus \{i\}} i_{jk}, \tag{1}$$

where $i_j = v_j / z_j$ is the current through the capacitor bank of impedance z_j at node j, and $\mathcal{N}_j$ is the set of nodes connected to node j. The impedance of capacitor bank j is determined by its setting $\sigma_j \in \{\text{ON}, \text{OFF}\}$, with the corresponding impedance $z_j \in \mathbb{C}$ with $|z_j| < \infty$ or $|z_j| = \infty$, respectively. Furthermore, we denote a given setting of all capacitor banks in the network as a *configuration* k with $C_k = \{\sigma_1, \ldots, \sigma_m\}$. The set of all possible configurations is denoted by $\mathcal{C}$.

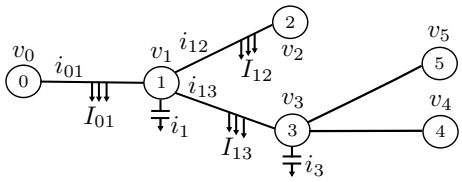

Fig. 1. Example distribution network topology.

Kirchoff's voltage law: The voltage drop between node i and j is modeled as

$$v_j = v_i - Z_{ij} \left(\frac{1}{2} I_{ij} + \sum_{k \in \mathcal{N}_j} i_{jk} + i_j \right).$$

Note the factor $1/2$ in front of I_{ij}, which accounts for the even distribution of I_{ij} along the line, see [23] for a derivation. Now, defining $\Gamma_{ij} = (1 + Z_{ij}/z_j)^{-1}$, the voltage drop can in general be rewritten as

$$v_j = \Gamma_{ij} v_i - \Gamma_{ij} Z_{ij} \left(\frac{1}{2} I_{ij} + \sum_{k \in \mathcal{N}_j} i_{jk} \right). \tag{2}$$

Example: For the particular grid illustrated in Fig. 1, the voltage drops are modeled as

$$\begin{aligned}
v_1 &= v_0 - Z_{01} \left(\frac{1}{2} I_{01} + i_{12} + i_{13} + i_1 \right), \\
v_2 &= v_1 - \frac{1}{2} Z_{12} I_{12}, \\
v_3 &= v_1 - Z_{13} \left(\frac{1}{2} I_{13} + i_{34} + i_{35} + i_3 \right), \\
v_4 &= v_3 - Z_{34} \left(\frac{1}{2} I_{34} \right), \quad v_5 = v_3 - Z_{35} \left(\frac{1}{2} I_{35} \right).
\end{aligned}$$

The resulting current flow equations for our example are

$$\begin{aligned}
i_{01} &= I_{01} + i_{12} + i_{13} + i_1, & i_{35} &= I_{35}, \\
i_{12} &= I_{12}, & i_1 &= \frac{v_1}{z_1}, \\
i_{13} &= I_{13} + i_{34} + i_{35} + i_3, & i_3 &= \frac{v_3}{z_3}. \\
i_{34} &= I_{34}, &
\end{aligned}$$

Throughout the paper, we assume that node 0 is connected to a transmission grid and thus the external power supply. Then the total complex power injected into the distribution network is

$$S = P + jQ = \frac{1}{2} v_0 i_{01}^*, \tag{3}$$

where P denotes active power and Q denotes reactive power.

B. Operator model

The main feeder voltage v_0 together with all the consumer loads I_{ij} together constitute a minimal state description of the distribution system [23]. That is, if these quantities are known, all other voltages and currents can be computed using

the equations above. In the following, we will assume that v_0 is directly measurable by the operator but that the consumer loads I_{ij} are uncertain. We therefore call

$$\mathbf{y} = \begin{pmatrix} I_{01} & I_{12} & \dots \end{pmatrix}^\top \in \mathbb{C}^n, \tag{4}$$

the (unknown) state of the distribution system, denoting n as the number of lines in the network.

In order for the operator to estimate $\mathbf{y}$, it needs to measure more quantities than just v_0. We therefore assume the operator can also accurately measure the complex power injection S, and a subset $\mathbf{v}$ of the other node voltages v_k. In this analysis, we assume the measurements are exact, *i.e.,* not subject to noise. This is of course a strong and unrealistic assumption. Nevertheless, it can still be used to derive some fundamental limitations since if an attacker is not detectable even with access to perfect measurements, adding realistic noise will not improve the situation. We also make the following assumption on the consumers.

Assumption 1 (Consumer behavior): The state $\mathbf{y}$ is independent of capacitor configuration $C_k \in \mathcal{C}$.

The assumption merely means that the consumers' current loads are not immediately affected if the operator changes the capacitor configuration. Using the model (2), the relation between the available measurements and the unknown state can be written in the compact form

$$\begin{bmatrix} \mathbf{v}^k - v_0^k \mathbf{f}_1(C_k) \\ (S^k/v_0^k)^* - v_0^k \mathbf{f}_2(C_k) \end{bmatrix} = \begin{bmatrix} H_v(C_k) \\ H_S(C_k) \end{bmatrix} \mathbf{y}, \tag{5}$$

for a particular configuration $C_k \in \mathcal{C}$, which is also signified by the superscript k on the measurement. The matrices H_v and H_S derive from (2), just as the scalings $\mathbf{f}_1$, $\mathbf{f}_2$. Often only a small subset $\mathbf{v}$ of the node voltages are measured, and it may not be possible to uniquely determine a state estimate $\mathbf{x}$ of the true state $\mathbf{y}$ from (5) only.

To improve the voltage levels and the power consumption in the network, the operator may decide to switch the capacitor configuration C_k, as discussed more below. Under Assumption 1, such switching does not immediately affect the state $\mathbf{y}$, but may still result in new independent measurements. Stacking all possible measurements and the relations (5), we obtain

$$\begin{bmatrix} \mathbf{v}^1 - v_0^1 \mathbf{f}_1(C_1) \\ \mathbf{v}^2 - v_0^2 \mathbf{f}_1(C_2) \\ \vdots \\ (S^1/v_0^1)^* - v_0^1 \mathbf{f}_2(C_1) \\ (S^2/v_0^2)^* - v_0^2 \mathbf{f}_2(C_2) \\ \vdots \end{bmatrix} = \begin{bmatrix} H_v(C_1) \\ H_v(C_2) \\ \vdots \\ H_S(C_1) \\ H_S(C_2) \\ \vdots \end{bmatrix} \mathbf{y} =: \underbrace{\begin{bmatrix} H_v(\mathcal{C}) \\ H_S(\mathcal{C}) \end{bmatrix}}_{H(\mathcal{C})} \mathbf{y}. \tag{6}$$

If the matrix $H(\mathcal{C})$ has full rank ($= n$), we can solve for a unique state estimate $\mathbf{x}$. We then say the *distribution system is observable*. Hence, switching the capacitor configuration may increase the operator's state awareness.

Integrated Volt-Var Control: The operator uses integrated VVC to minimize the the operation cost of the distribution network based on the system state estimate $\mathbf{x}$ available at the control center, which may be different from the true state $\mathbf{y}$ in the presence of an adversary or in an unobservable system. Moreover, the cost should be minimized while satisfying all operational constraints, such as voltage and power factor limits. We assume that some customers operate low cost over/undervoltage monitoring devices (*e.g.,* FNET Frequency Disturbance Recorders), and thus if voltage or power factor limits are violated, they would report the violation to regulators, who would notify the operator.

Among all capacitor bank configurations $\mathcal{C}$, let us denote by $\mathcal{C}_\mathcal{F}(\mathbf{x})$ the set of capacitor bank configurations that satisfy all operational constraints in system state $\mathbf{x}$. Under no attack, the optimal control policy for the operator is to choose a capacitor bank configuration $C^* \in \mathcal{C}_\mathcal{F}(\mathbf{x})$ that minimizes its cost, *i.e.,*

$$C^*(\mathbf{x}) = \arg \min_{C \in \mathcal{C}_\mathcal{F}(\mathbf{x})} V(\mathbf{x}, C), \tag{7}$$

for some pre-defined cost function V that could, for instance, correspond to the active power losses in the network. The optimization is constrained to configurations in $\mathcal{C}_\mathcal{F}(\mathbf{x})$, as otherwise some operational constraints might be violated.

III. Attack and Defense Strategies

Using the distribution network and operator models described in the previous section, below we model the stealthy adversary corrupting voltage measurements and propose a game-theoretic framework for choosing suitable defense strategies.

A. Adversary model

We make the following assumptions on the adversary.

Assumption 2 (Adversarial capabilities):

(i) The adversary may access the voltage node measurements $\mathbf{v}$, but not the power injection measurement S and the voltage measurement v_0 at the main feeder.

(ii) The adversary performs a one-shot modification to the measured voltages: $\mathbf{v} \to \mathbf{v} + \mathbf{a}$, where $\mathbf{a}$ is the attack vector.

We define stealth attacks as follows.

Definition 1 (C_k-stealth attack): The attack vector $\mathbf{a}$ is a C_k-stealth attack if and only if there exists a $\mathbf{\Delta y} \in \mathbb{C}^n$ such that

$$\mathbf{a} = H_v(C_k)\mathbf{\Delta y} \quad \text{and} \quad 0 = H_S(C_k)\mathbf{\Delta y}.$$

Definition 2 ($\mathcal{C}$-stealth attack): The attack vector $\mathbf{a}$ is a $\mathcal{C}$-stealth attack if and only if there exists (a single) $\mathbf{\Delta y} \in \mathbb{C}^n$ such that, for all $C_k \in \mathcal{C}$,

$$\mathbf{a} = H_v(C_k)\mathbf{\Delta y} \quad \text{and} \quad 0 = H_S(C_k)\mathbf{\Delta y}.$$

The motivation for Definition 1 is that

$$\begin{bmatrix} \mathbf{v}^k + \mathbf{a} - v_0^k \mathbf{f}_1(C_k) \\ (S^k/v_0^k)^* - v_0^k \mathbf{f}_2(C_k) \end{bmatrix} = \begin{bmatrix} H_v(C_k) \\ H_S(C_k) \end{bmatrix} (\mathbf{y} + \mathbf{\Delta y}), \tag{8}$$

and hence an operator cannot refute that the state is $\mathbf{x} := \mathbf{y} + \mathbf{\Delta y}$, if the attack is a C_k-stealth attack and the system is in configuration C_k and in the real state $\mathbf{y}$. Or put differently:

given the received (attacked) measurements and assuming an observable system, the operator has every reason to believe that the state is $\mathbf{x} := \mathbf{y} + \mathbf{\Delta y}$, when in fact it is $\mathbf{y}$.

Nevertheless, if the operator switches from C_k to say C_l, it may be that the attack vector $\mathbf{a}$ is not a C_l-stealth attack, and hence the measurements should raise suspicion. Even if the attack vector $\mathbf{a}$ is also a C_l-stealth attack, it may require a different $\mathbf{\Delta y}$ to be explained. This should also raise the suspicion of the operator, remembering from Assumption 1 that capacitor switches do not incur changes in the load.

Therefore, a malicious adversary may want to take his attack one step further and look for an attack that is stealthy for all possible configurations $\mathcal{C}$. This is the background for Definition 2. If $\mathbf{a}$ is a $\mathcal{C}$-stealth attack, the operator cannot refute that the state is $\mathbf{y} + \mathbf{\Delta y}$, no matter how he switches between the configurations.

The stealth attacks for a distribution power network are completely characterized in the following two theorems.

Theorem 1: Let the columns of the matrix $B_k \in \mathbb{C}^{n\times(n-1)}$ form an arbitrary basis of $\mathcal{N}(H_S(C_k))$. Then $\mathbf{a}$ is a C_k-stealth attack if and only if there exists an $\alpha \in \mathbb{C}^{n-1}$ such that

$$\mathbf{a} = H_v(C_k)B_k\alpha.$$

The corresponding non-refutable state bias is $\mathbf{\Delta y} = B_k\alpha$.

Theorem 2: Let the columns of the matrix $B_{\mathcal{C}} \in \mathbb{C}^{n\times m}$ form an arbitrary basis of the nullspace $\mathcal{N}\left(\begin{bmatrix}\Delta H_v(\mathcal{C}) \\ H_S(\mathcal{C})\end{bmatrix}\right)$, where

$$\Delta H_v(\mathcal{C}) = \begin{bmatrix} H_v(C_1) - H_v(C_2) \\ H_v(C_2) - H_v(C_3) \\ \vdots \end{bmatrix}, \quad H_S(\mathcal{C}) = \begin{bmatrix} H_S(C_1) \\ H_S(C_2) \\ \vdots \end{bmatrix}.$$

Then $\mathbf{a}$ is a $\mathcal{C}$-stealth attack if and only if there exists an $\alpha \in \mathbb{C}^m$ such that $\mathbf{a} = H_v(C_1)B_{\mathcal{C}}\alpha$. The corresponding non-refutable state bias is $\mathbf{\Delta y} = B_{\mathcal{C}}\alpha$.

Remark 1: Note that if $\mathbf{a}$ is a $\mathcal{C}$-stealth attack, then $\mathbf{a} = H_v(C_1)B_{\mathcal{C}}\alpha = H_v(C_k)B_{\mathcal{C}}\alpha$ for all $C_k \in \mathcal{C}$.

B. Example: Stealth attacks

Let us study the introduced definitions in the network shown in Fig. 1. We assume the five node voltages are measured, i.e, $\mathbf{v} = \begin{pmatrix} v_1 & \dots & v_5 \end{pmatrix}^\top$, and are all possible for the adversary to corrupt. We assume the line impedances are (in per-unit system) $Z_{01} = 0.21 + 0.43j$ pu, $Z_{12} = 2.57 + 5.27j$ pu, $Z_{13} = 1.29 + 2.63j$ pu, and $Z_{34} = Z_{35} = 0.64 + 1.32j$ pu.

The four capacitor configurations are

$$\begin{aligned} C_1: &\quad z_1 = -0.28j \text{ pu} && z_3 = -1.66j \text{ pu} \\ C_2: &\quad z_1 = \infty \text{ pu} && z_3 = -1.66j \text{ pu} \\ C_3: &\quad z_1 = -0.28j \text{ pu} && z_3 = \infty \text{ pu} \\ C_4: &\quad z_1 = \infty \text{ pu} && z_3 = \infty \text{ pu} \end{aligned}$$

First we characterize the C_1-stealth attacks. Using Theorem 1, we compute a basis for all the C_1-stealth attacks $\mathbf{a}$ as

$$H_v(C_1)B_1 = \begin{pmatrix} 0.00 & 0.00 & 0.05 + 0.03j & 0.10 + 0.01j \\ 1.00 & 0.00 & 1.00 & -0.40 + 0.59j \\ 0.00 & 0.00 & -0.82 + 0.43j & 1.00 \\ 0.00 & 1.00 & -0.80 + 0.32j & 0.96 - 0.19j \\ 0.25 & -1.00 & -0.80 + 0.32j & 0.91 + 0.40j \end{pmatrix}.$$

Using Theorem 2, we can also compute a basis for all the $\mathcal{C}$-stealth attacks $\mathbf{a}$. It turns out that the two first columns of $H_v(C_1)B_1$ given above is a basis for the $\mathcal{C}$-stealth attacks. (Of course, the $\mathcal{C}$-stealth attacks must lie in a subspace of the C_1-stealth attacks.) It is interesting to notice that an adversary that adds an arbitrary voltage a to the measurement v_4 and subtracts a from v_5 is stealthy in all capacitor configurations. The same holds for an attack that adds a to v_5 and simultaneously adds $4.00a$ to v_2, for example. It is also interesting to notice that an adversary that manipulates the measurements v_1 or v_3 can always be detected by an operator by proper switching of the capacitors. This may be expected, since these are the voltage nodes being connected to the controllable capacitors.

TABLE I

SIMPLIFIED AVERAGE PAYOFF MATRIX FOR THE REPEATED GAME.

$U_{2,*} \geq U_{3,*} \geq 0$

		BR	Mixed(ω)
$\neg A$	NA	$U_{1,*} = 0$ 0	$-U_{1,\omega}$ 0
A	NA	$U_{1,*} = 0$ 0	$-U_{1,\omega}$ $U_{1,\omega}$
	BRP	$-U_{2,*}$ $U_{2,*}$	$-U_{2,\omega}$ $U_{2,\omega}[-V_d]$
	MP	$-U_{3,*}$ $U_{3,*}$	$-U_{3,\omega}$ $U_{3,\omega}$

C. A game theoretic approach to defense strategies

For a particular configuration C let us denote the difference from the optimal objective function (7) by

$$\Delta V(\mathbf{x}, C) = V(\mathbf{x}, C) - V(\mathbf{x}, C^*(\mathbf{x})) \geq 0, \qquad (9)$$

which is the payoff of the adversary if the operator chooses configuration C. If a configuration $C \in \mathcal{C}_{\mathcal{F}}(\mathbf{x}) \setminus \mathcal{C}_{\mathcal{F}}(\mathbf{y})$ is chosen by the operator then an operational constraint is violated and the adversary will be possible to discover. For example, unhappy customers may report that the voltage level is lower than promised. A discovered attack results in a loss of future payoffs for the adversary.

This problem can be modeled as a cheap talk signaling game [24], *i.e.,* a game with incomplete information between the operator and the adversary. In this model the *type* of the attacker is determined by the actual state of the system, the operator's decision determines the payoff of both players, but the operator only knows the system's state indirectly, as told by the attacker through corrupted measurements. The horizon of the game depends on the players' strategies: the game terminates when the adversary is discovered.

The action set $\mathcal{A}_o$ of the operator is the set $\mathcal{C}$ of configurations. The information available to the operator is the potentially attacked system state $\mathbf{x} = \mathbf{y} + \mathbf{\Delta y}$, where $\mathbf{\Delta y}$ is a state bias that satisfies Theorem 2, but the operator is not

aware of whether or not there is an attacker and thus, whether or not the oberved system state $\mathbf{x}$ is actually attacked. We therefore consider that the operator only chooses configurations $C_k \in \mathcal{C}_{\mathcal{F}}(\mathbf{x})$ with positive probability. We denote by A the event that there is no attacker, and the belief of the operator that there is an attacker by p_A. We model the case of no attacker ($\neg A$) by an attacker with uniformly zero payoff, as shown in the first row of Table I.

In the following, for brevity, we provide a qualitive analysis of the game, for which it suffices to focus on two strategies of the operator. First, the pure strategy that in every round chooses $C^*(\mathbf{x})$, which we call the *best response (BR)* strategy. Second, the *mixed* strategy ω on $\mathcal{C}_{\mathcal{F}}(\mathbf{x})$, which plays some (or all) configurations $C_k \in \mathcal{C}_{\mathcal{F}}(\mathbf{x}) \setminus \{C^*(\mathbf{x})\}$ with a small probability $\omega_k > 0$, and plays the best response $C^*(\mathbf{x})$ otherwise.

We consider three strategies of the adversary. First, the adversary can choose *not* to manipulate any measurement data, *i.e.,* $\mathbf{x} = \mathbf{y}$, which we call *no attack (NA)*. Under *NA* the adversary's *average* payoff is $U_{1,*} = 0$ if the operator plays the *BR* strategy and it is $U_{1,\omega} \geq 0$ if the operator plays the *mixed* strategy. Second, the adversary can choose to perform an attack $\mathbf{x}$ that maximizes the operator's loss under the assumption that the operator always chooses the *BR* strategy. When choosing $\mathbf{x}$ the adversary has to ensure that the operational constraints would not be violated under the configuration chosen by the operator, therefore we can write

$$\mathbf{x}_{BRP} = \arg \max_{\mathbf{x}:\mathbf{C}^*(\mathbf{x}) \in \mathcal{C}_{\mathcal{F}}(\mathbf{y})} V(\mathbf{y}, C^*(\mathbf{x})) - V(\mathbf{y}, C^*(\mathbf{y})). \tag{10}$$

We call this the *best-response-proof (BRP)* attack strategy. The *BRP* strategy provides average payoff $U_{2,*} \geq 0$ to the adversary if the operator plays the *BR* strategy. Nevertheless, if the operator plays the *mixed* strategy then it might choose a configuration C_k under which some operational constraints are violated, and the adversary would be detected. If detected, the adversary is subject to a penalty $-V_d$, and the game terminates.

The adversary can hedge against the *mixed* strategy played by the operator by considering only attacks $\mathbf{x}$ that allow the same set of configurations to be chosen as for the real system state $\mathbf{y}$, that is,

$$\mathbf{x}_{MP} = \arg \max_{\mathbf{x}:\mathcal{C}_{\mathcal{F}}(\mathbf{x}) \subseteq \mathcal{C}_{\mathcal{F}}(\mathbf{y})} V(\mathbf{y}, C^*(\mathbf{x})) - V(\mathbf{y}, C^*(\mathbf{y})). \tag{11}$$

We call this the *mixed-proof (MP)* attack strategy. If the operator plays the *BR* strategy, then the adversary's payoff is no more than that under the *BRP* strategy, *i.e.,* $U_{2,*} \geq U_{3,*} \geq 0$. Nevertheless, the *MP* attack strategy provides average payoff $U_{3,\omega}$ to the adversary if the operator plays the *mixed* strategy, without the possibility of detection. The payoff matrix of the game is shown in Table I.

Let us consider now the equilibrium strategies. If there is an attacker but the operator's belief is $p_A = 0$ and the attacker knows this belief, then the perfect Bayesian equilibrium is (BRP, BR). If, however, the operator's belief is $p_A > 0$ then (BRP, BR) is not an equilibrium, because the operator could decrease its long-term cost by playing the *mixed* strategy for some mixed strategy ω for which $U_{2,*} \geq U_{2,\omega}$, which would eventually lead to the discovery of the adversary. Thus, if V_d is finite then in equilibrium the operator will play its *mixed* strategy with ω chosen based on the belief p_A and based on the estimated costs, and the adversary plays a possibly mixed strategy. If V_d is infinite then at equilibrium the operator plays *mixed* so that $U_{3,\omega} < U_{1,\omega}$ and the adversary plays a mixed strategy over *NA* and *MP*. If there is no such ω then, interestingly, there is no equilibrium under $p_A < 1$.

TABLE II

TRUE POWER INJECTIONS AND VOLTAGE LEVELS (IN PER-UNIT, $v_0 = 1.0\,\text{pu}$).

	C_1	C_2	C_3	C_4
P	1.30	0.92	1.17	1.00
$\lvert v_1 \rvert$	0.56	0.41	0.63	0.60
$\lvert v_2 \rvert$	1.90	1.57	1.83	1.69
$\lvert v_3 \rvert$	0.90	0.63	0.88	0.78
$\lvert v_4 \rvert$	0.88	0.64	0.91	0.81
$\lvert v_5 \rvert$	0.88	0.64	0.91	0.81

D. Example: Attack and defense strategies

To illustrate the strategies discussed above, we return to the example from Section III-B. Let us assume that the cost function that the operator wants to minimize is simply the injected power from the transmission grid, *i.e.,* $V = P$, and the only operational constraint is to maintain the voltage level at node 2 between $1.4\,\text{pu}$ and $1.75\,\text{pu}$. We set the true state of the system to $\mathbf{y} = (1.38 \cdot (1-j) \quad 0.48 \quad 0.05 \quad 0.05 \quad 0.05)^\top$ pu. How the voltage levels and the injected power depend on the capacitor configuration C in the true state is given in Table II. In the true system state $\mathbf{y}$ the optimal configuration satisfying the constraint is clearly C_2, where $V = P = 0.92\,\text{pu}$, which is also the base configuration chosen by the operator. Note that configuration C_4 is feasible and more expensive, but that C_3 and C_1 are infeasible choices.

We assume the adversary has access to the voltage measurements at nodes 2 and 5 and stages the $\mathcal{C}$-stealth attack $\mathbf{a} = (0 \quad a \quad 0 \quad 0 \quad 0.25a)^\top$ pu, for a specific a of increasing magnitude. In Fig. 2, the voltage level as perceived by the operator under attack is plotted. Observe that the attacker here tries to fool the operator into believing the voltage level is lower than it actually is.

Let us first consider the scenario where the operator plays the *BR* strategy, *i.e.,* always chooses the best feasible configuration $C^*(\mathbf{x})$. Then as $|a|$ reaches about $0.17\,\text{pu}$, it would switch to configuration C_4. This increases cost, $\Delta V = 0.08\,\text{pu}$, which is also the payoff to the adversary. If the attack increases even more to about $0.29\,\text{pu}$, the operator would switch to C_3 leading to an increased cost $\Delta V = 0.25\,\text{pu}$. Note, however, that the true voltage is the one given at $|a| = 0$, hence the customers at node 2 would experience that their voltage level has raised to $1.83\,\text{pu}$; they

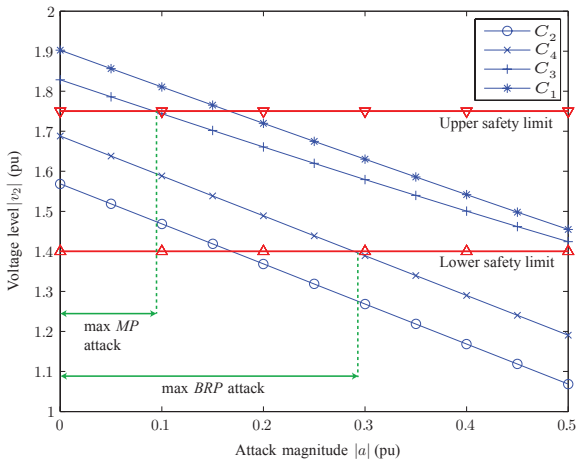

Fig. 2. The voltage level in node 2 as perceived by the operator under different configurations, as a function of the attack magnitude. Note that the *true* voltages are given for $|a| = 0$, and if the operator chooses C_3 or C_1 safety constraints are violated in the real system.

may report this safety violation to the operator, and the attack thus becomes detectable at this point. Hence, the largest *BRP* attack has a magnitude between $0.17\,\mathrm{pu}$ and $0.29\,\mathrm{pu}$ and a cost of $\Delta V = 0.08\,\mathrm{pu}$.

Let us next consider the scenario where the operator plays a mixed strategy ω, and chooses among all the feasible configurations with some nonzero probability. At an attack magnitude of $|a| \approx 0.09\,\mathrm{pu}$ the configuration C_3 appears as feasible to the operator. Nevertheless, as soon as the operator selects C_3 the attack may be detected. Thus an attacker that plays the *MP* strategy would not choose attacks larger than about $0.09\,\mathrm{pu}$, but in the example at this attack magnitude $C^*(\mathbf{x}) = C^*(\mathbf{y})$, hence the impact of the attack is rather limited. As an example, if the operator plays $\omega_{C^*(\mathbf{x})} = \omega_{C_2} = 0.99$ and $\omega_{C_4} = 0.01$ then $U_{3,\omega} = 0.0008\,\mathrm{pu}$. We see that the *mixed* strategy of the operator may significantly decrease the size and the cost of $\mathcal{C}$-stealth attacks, but of course at a slightly increased cost should there be no attack.

IV. Feasibility Study

The preceding derivation gives an algebraic description of stealthy data injections available to an adversary for a given H, which we have defined as dependent on a specific capacitor setting C. In this section, we undertake a preliminary evaluation of the impact of data injection attacks on the VVC, to verify that the studied attacks are feasible in a realistic system.

We used GridLab-D [1], a power distribution system simulation and analysis tool developed by PNNL, for our evaluation. In particular we use a subset of the modified IEEE 13 node feeder model (See Fig. 3) with voltage regulated link (link between nodes 632 and 650) and a capacitor bank (at node 684) that is included with the GridLab-D distribution. GridLab-D has a built-in volt-var optimization module that implements the algorithm proposed by Borozan *et al.,* [5].

[1] `http://www.gridlabd.org`

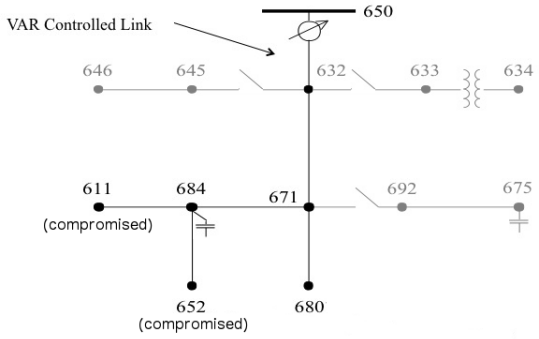

Fig. 3. Subset of the modified IEEE 13 Node Distribution System in GridLab-D. Parts greyed-out have been disconnected and measurements from two end-of-line meters have been compromised (node 611 and node 652).

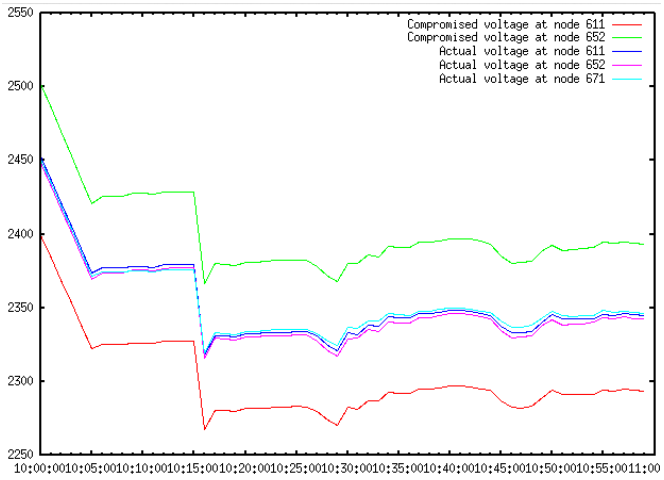

Fig. 4. Voltage measurements at three nodes for an hour of simulation. Two of the nodes have been compromised to report $+50$ and -50 volts. The VVC was configured to keep voltage at 2300 volts (common high-side voltage level in American distribution grids).

This algorithm uses end of the line (EOL) voltage measurements from nodes 652 and 611 in controlling the voltage level using the voltage regulator and the capacitor bank. GridLab-D uses a forward-backward sweep algorithm [23] to analyze distribution systems so the H matrix is never explicitly computed. Furthermore, the actual impedances on the lines are obtained from the type of line and length.

Thus for this preliminary evaluation, we used GridLab-D as a black box. Based on the intuition obtained from the example in Section III-B, voltage measurements at nodes 652 and 611 are modified by adding 50 volts to the voltage measurement at node 652 and subtracting 50 volts from the voltage measurement at node 611. Note that the lines between node 684 and nodes 652 and 611 are set to be identical so they have the same impedance. Simulation results with the injection attack and without the attack are shown in Figs. 4 and 5, respectively. Compromising the measurements has a direct impact on the ability of the VVC to maintain proper voltage at nodes 671, 652 and 61, as seen by comparing the actual voltage in both graphs. Specifically, without the attack

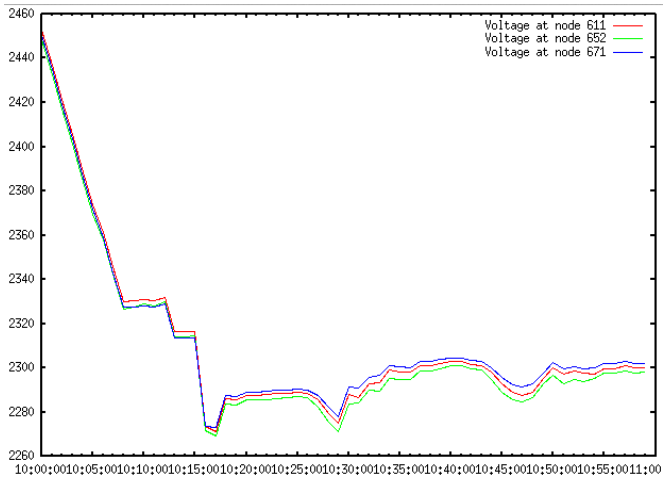

Fig. 5. Voltage measurements at three nodes for an hour of simulation, without data injection attack. The VVC was configured to keep the voltage at 2300 volts.

VVC is able to bring the voltages down from $2,450$ volts to $2,300$ volts and maintain them there. But with the data injection while the VVC is still able to bring the voltages down from 2450 volts, it is only able to bring them down to $2,350$ volts. In fact, an observing operator will believe that the voltage at node 611 is at the desired level of $2,300$ volts, at node 671 to be at $2,350$ volts, and at node 652 to be at $2,400$ volts. These initial results indicate that an attacker can indeed cause the VVC to function in a suboptimal manner.

V. Conclusions

In this paper, we have explored the problem of data integrity attacks on a distribution grid operated by IVVC. In particular, the distribution network's physical model was used to characterize stealthy data integrity attacks on voltage measurements under different capacitor bank configurations. Supposing that the adversary wishes to remain stealthy, we characterized the attack impact on the distribution network's operation cost and formulated a game between the stealthy adversary and the operator, from which possible countermeasures can be derived to detect and mitigate the attack. Additionally, we undertook a preliminary evaluation of data integrity attack strategies on an actual distribution model using GridLab-D. The experiments show that such attacks, computed using simplified models, can indeed disrupt the distribution grid operation.

References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *Power and Energy Magazine, IEEE*, vol. 7, no. 2, pp. 52–62, Mar.-Apr. 2009.

[2] E. Jauch, "Volt/VAR management–an essential "SMART" function," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, Seattle, WA, USA, Mar. 2009, pp. 1–7.

[3] I. Roytelman and V. Landenberger, "Real-time distribution system analysis - integral part of DMS," in *IEEE/PES Power Systems Conference and Exposition, PSCE '09.*, Mar. 2009, pp. 1–6.

[4] K. Schneider, J. Fuller, and D. Chassin, "Evaluating conservation voltage reduction: An application of GridLAB-D: An open source software package," in *IEEE Power and Energy Society General Meeting*, Jul. 2011, pp. 1–6.

[5] V. Borozan, M. Baran, and D. Novosel, "Integrated Volt/VAR control in distribution systems," in *IEEE Power Engineering Society Winter Meeting*, vol. 3, Columbus, OH, USA, 2001, pp. 1485–1490.

[6] T. Kropp, "System threats and vulnerabilities: An EMS and SCADA security system overview," *IEEE Power and Energy Magazine*, vol. 4, no. 2, pp. 46–50, Mar.-Apr. 2006.

[7] S. Amin, "Securing the electricity grid," *The Bridge, quarterly publication of the US National Academy of Engineering*, vol. 40, no. 1, pp. 13–20, 2010.

[8] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. on Computer and Communications Security*, Chicago, IL, USA, Nov. 2009.

[9] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweden, April 2010.

[10] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proceedings of the 50th IEEE Conference on Decision and Control*, Orlando, FL, USA, Dec. 2011.

[11] G. Hug and J. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[12] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. of the First IEEE Int. Conf. on Smart Grid Communications*, Gaithersburg, MD, USA, Oct. 2010.

[13] A. Teixeira, H. Sandberg, G. Dán, and K. H. Johansson, "Optimal power flow: Closing the loop over corrupted data," in *Proc. American Control Conference*, Montreal, Canada, Jun. 2012.

[14] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. of the First IEEE Int. Conf. on Smart Grid Communications*, Gaithersburg, MA, USA, Oct. 2010.

[15] R. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on DC state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweden, April 2010.

[16] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. of the First IEEE Int. Conf. on Smart Grid Communications*, Gaithersburg, MD, USA, Oct. 2010.

[17] O. Vukovic, K. C. Sou, G. Dán, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1108–1118, Jul. 2012.

[18] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proc. of the 10th annual ACM workshop on Privacy in the electronic society*, Chicago, IL, USA, 2011, pp. 49–60.

[19] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. Wang, "Impact of cyber-security issues on smart grid," in *2nd IEEE PES Int. Conf. and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*, Dec. 2011, pp. 1–7.

[20] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *Int. J. Secur. Netw.*, vol. 6, no. 1, pp. 2–13, Apr. 2011.

[21] A. Giacomoni, M. Amin, and B. Wollenberg, "A control and communications architecture for a secure and reconfigurable power distribution system: An analysis and case study," in *Proc. of the 18th IFAC World Congress*, Milano, Italy, Aug.-Sep. 2011.

[22] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for voltage control in smart grid," in *50th Annual Allerton Conference on Communication, Control, and Computing*, Allerton, IL, USA, Oct. 2012, to appear.

[23] W. H. Kersting, *Distribution System Modeling and Analysis, Second Edition (Electric Power Engineering Series)*, 2nd ed. CRC Press, Nov. 2006.

[24] I.-K. Cho and D. M. Kreps, "Signaling games and stable equilibria," *The Quarterly Journal of Economics*, vol. 102, no. 2, pp. 179–221, May 1987.