This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

Time-Synchronization Attack Detection in Unbalanced Three-Phase Systems

Marguerite Delcourt, Ezzeldin Shereen, Gyrgy Dn, Jean-Yves Le Boudec, Mario Paolone

***Abstract*—Phasor measurement units (PMU) rely on an accurate time-synchronization to phase-align the phasors and timestamp the voltage and current phasor measurements. Among the symmetrical components computed from the phasors in three-phase systems, the standard practice only uses the direct-sequence component for state estimation and bad data detection (BDD). Time-synchronization attacks (TSAs) can compromise the measured phasors and can, thus, significantly alter the state estimate in a manner that is undetectable by widely used power-system BDD algorithms. In this paper we investigate the potential of utilizing the three-phase model instead of the direct-sequence model for mitigating the vulnerability of state estimation to undetectable TSAs. We show analytically that if the power system is unbalanced then the use of the three-phase model as input to BDD algorithms enables to detect attacks that would be undetectable if only the direct-sequence model was used. Simulations performed on the IEEE 39-bus benchmark using real load profiles recorded on the grid of the city of Lausanne confirm our analytical results. Our results provide a new argument for the adoption of three-phase models for BDD, as their use is a simple, yet effective measure for reducing the vulnerability of PMU measurements to TSAs.**

I. Introduction

Phasor Measurement Units (PMUs) constitute a key enabling technology for present and future power systems operation and control. Due to the high reporting rate supported by PMUs, usually in the range of tens of measurements per second, the situational awareness required by many smart grid applications can be improved. Such applications include power-oscillation monitoring [1], phase-angle monitoring [2], power-system linear state-estimation (LSE) [3], and protection and fault localization [4]. However, PMUs require precise time-synchronization over large geographical areas. To achieve time synchronization for PMUs, space-based time synchronization is typically used, where the precise time information is acquired through GPS satellites. An alternative solution is network-based time synchronization in which time information is transmitted through a network infrastructure from a *master* node, which is connected to an accurate time source and to several *slave* nodes, which could be the PMUs. The most widespread network-based time synchronization protocol is the Precision Time Protocol (PTP) [5] with its latest version PTPv2.1 published in 2020.

Nonetheless, both time-synchronization sources for PMUs have been shown to have vulnerabilites that could be exploited to perform time-synchronization attacks (TSAs) against multiple PMUs [6]. Civilian GPS signals are unauthenticated and thus vulnerable to spoofing attacks [7] [8], as an attacker can alter the time references sent by the GPS satellites to a PMU receiver. Similarly, PTP time references can be manipulated by modifying the synchronization messages after compromising software [9], or by physically introducing delays in the propagation of synchronization messages via the insertion of a delay box [10]. TSAs can have a devastating impact on many smart grid applications [11] [12] (e.g., phase angle monitoring, anti-islanding protection, and power oscillation damping), and thus they pose a serious threat to the security and reliability of power systems. Therefore, the detection and mitigation of TSAs is of utmost importance for power-system operators. Importantly, the existence of a TSA is hard to detect unless the TSA affects the system in a non-plausible way. In addition, TSAs are also a major threat to the security and reliability of other time-sensitive sensor-networks such as networks for mobile-source localization [13] or industrial collaborative robots [14].

In response to the severe threat of TSAs to power networks, many recent works have considered the problem of either mitigating or detecting TSAs. For space-based time synchronization, [15] proposes the detection of GPS spoofing by monitoring the carrier-to-noise-ratio of the GPS signal. For network-based time synchronization, [16] proposes the introduction of "guard clocks" in a PTP network to detect TSAs. An alternative approach for the detection of TSAs against PMUs, proposed in [17], relies on monitoring the correlation between adjustments made to the PMU clock frequency and changes in the phase angles measured by the PMU. Other works focus on the problem of mitigating TSAs. For example, [18] proposed authenticating GPS messages for mitigating GPS spoofing attacks against power systems. Similarly, the most recent standard of PTP (i.e., PTPv2.1) includes optional message authentication [9] in order to prevent the spoofing of PTP synchronization messages. However, the aforementioned works on detecting and mitigating TSAs either require hardware or software modifications to the PMUs, or propose the introduction of new network devices. Moreover, message authentication is not enough to detect advanced delay manipulations through delay-box insertion or through software compromise.

A promising alternative for detecting TSAs is to combine LSE with Bad Data Detection (BDD) schemes. Using the measurement residuals obtained with the weighted-least squares (WLS) state-estimator or the least-squares (LS) state-estimator, the BDD schemes are intended to detect the presence of erroneous or suspicious measurement data. State estimation can be performed using various models of the power system, including the direct-sequence model, the complete-sequence model and the three-phase model [19]. The relationship between the different models is discussed in Section II, and

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

we refer the reader to [20] for additional details on symmetrical components. However, due to unbalanced loads and untransposed transmission lines, a direct-sequence equivalent of the three-phase system will often be inaccurate, especially in distribution grids [21]. Therefore, a large body of research works has focused on developing accurate and efficient three-phase state estimators. Authors in [22] demonstrated the accuracy gain achieved through considering the three-phase model of a power system, using a hybrid state-estimator that utilizes both SCADA measurements and PMU measurements. Authors in [21] and [23] evaluated the robustness of three-phase state estimators to various sources of uncertainty in distribution grids. More recent works focus on creating a three-phase state estimator that relies only on PMU measurements. Authors in [24] present a real implementation of a three-phase linear state estimator that is only based on PMU measurements. Moreover, [25] considers the problem of finding an optimal placement of PMUs in a power system to achieve full observability in three-phase distribution grids. Their solution aims at minimizing the number of deployed PMUs, while maximizing state estimation accuracy. Authors in [26] focus on the computational efficiency of three-phase state estimators, by using modal transformation to leverage the linearity of the state estimation process when only PMUs are used. Lately, motivated by advances in machine learning, [27] proposes using artificial neural networks for three-phase state estimation on sparse PMU measurements, instead of the traditional WLS estimation, and finds that the estimator achieves high estimation accuracy while meeting real-time requirements. Yet, the majority of power-system operators today perform state estimation based on the direct-sequence model despite the advantages of three-phase state estimation, due to the lack of reliable three-phase grid component models, and due to the higher computational burden.

Unfortunately, recent work has shown that it is possible for an attacker to construct a TSA that can bypass the BDD schemes when using the direct-sequence model for state estimation, and, importantly, such undetectable TSAs were shown to have significant impact on the estimated power-flows on transmission lines [28]. The feasibility of such undetectable TSAs was also shown under practical implementation constraints [29], including an undetectable-attack strategy that requires no more than three vulnerable PMUs to be targeted simultaneously. General vulnerability conditions for mounting an undetectable TSA against vulnerable sites were provided in [30] and authors in [30] also showed that the grid can be secured by modifying the PMU allocation and by increasing the number of deployed PMUs. Although this measure does not require any changes to the hardware or to the software of deployed PMUs, it requires the introduction of additional measurement devices, which incurs increased cost. As an alternative, authors in [31] proposed to mitigate undetectable TSAs by upgrading network components to secure PTP at minimum cost.

In this work, we assess the benefits of using a three-phase state estimator as a simple tool to improve the detection of TSAs. Our proposal makes use of the three-phase measurements that should already be available to the control center of a power system. Note that the proposed approach is applicable irrespective of the method used by the attacker for compromising time synchronization. We make two important contributions. First, we provide an analytical characterization of the vulnerability of three-phase state estimation compared to state estimation based on a direct-sequence model. We show that in a balanced three-phase system the vulnerability conditions in the three-phase and in the direct-sequence representations are equivalent. However, if the system is unbalanced, we show that vulnerability in the direct-sequence representation does not imply vulnerability in the three-phase representation. These results indicate that three-phase state estimation is more resilient to TSAs. In practice, our findings imply that the use of the three-phase model improves the detectability of TSAs in unbalanced power systems (e.g., distribution systems). In contrast, when employed in balanced or nearly balanced systems (e.g., most transmission systems), a three-phase state estimator offers negligible advantages compared to a direct-sequence state estimator for detecting TSAs. Second, we provide empirical evidence that confirms the superiority of three-phase state estimation in detecting TSAs using extensive simulations on the IEEE 39-bus benchmark using real load profiles measured by PMUs installed on the 125 kV sub-transmission power grid of the city of Lausanne [32; 33].

The rest of the paper is organized as follows. Section II presents the models considered for three-phase state estimation and for TSAs. Section III shows analytically that when the system has unbalances, the three-phase state estimator is more resilient to TSAs than the direct-sequence state estimator. Section IV presents extensive simulations confirming our analytical results. Finally, Section V concludes the paper.

II. System and Attack Models

We adapt the system model from [30] to three-phase systems, both in complex form and in rectangular coordinates. As explained in Section III, the former is used for the analysis of exact vulnerability conditions and the latter is used to measure the distance to vulnerability of sites that are not exactly vulnerable. We then introduce the attack model.

A. System Model in Complex Form

We consider a three-phase system with a total of n buses and $3m$ phasor measurements measured by PMUs. The complex measurement vector $z_{abc} \in \mathbb{C}^{3m}$ is linearly linked to the state vector $x_{abc} \in \mathbb{C}^{3n}$ via the complex measurement-to-state matrix $H_{abc} \in \mathbb{C}^{3m \times 3n}$ as

$$z_{abc} = H_{abc} x_{abc} + e_{abc}, \tag{1}$$

where $e_{abc} \in \mathbb{C}^{3m}$ is the complex measurement error. The LS estimate of the system's state is $\widehat{x}_{abc} = ((H_{abc})^{\dagger} H_{abc})^{-1} (H_{abc})^{\dagger} z_{abc}$, where $\dagger$ denotes the conjugate transpose. The difference r_{abc} between the estimated measurement vector $\widehat{z}_{abc} = H_{abc} \widehat{x}_{abc}$ and the observed measurement vector z_{abc} is called the residual vector. The residual can be computed as $r_{abc} = F_{abc} z_{abc}$, where the $3m \times 3m$ complex matrix $F_{abc} = H_{abc}((H_{abc})^{\dagger} H_{abc})^{-1}(H_{abc})^{\dagger} - Id$ is called the LS verification matrix, and where Id is the $3m \times 3m$

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

identity matrix. The transformation of the three-phase complex variables into their complex complete-sequence counterparts is explained in [26]. We present the corresponding transformations in rectangular coordinates in Section II-B. Specifically, the three-phase measurement vector can be transformed into its complete-sequence model counterpart as $z_{012} = T_Z z_{abc}$, where T_Z is the $3m \times 3m$ block diagonal matrix that has along its diagonal the 3×3 sequence transformation matrix

$$T = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{\frac{2j\pi}{3}} & e^{\frac{-2j\pi}{3}} \\ 1 & e^{\frac{-2j\pi}{3}} & e^{\frac{2j\pi}{3}} \end{bmatrix}.$$

Similarly, the three-phase state vector can be transformed into its complete-sequence model counterpart as $x_{012} = T_X^{-1} x_{abc}$, where T_X is the $3n \times 3n$ block diagonal matrix that has along its diagonal the 3×3 inverse sequence transformation matrix $T^{-1} = 3T^{\dagger}$, note that T is non-singular and therefore invertible. The measurement-to-state matrix in the complete-sequence model is obtained as $H_{012} = T_Z H_{abc} T_X$ and Eq.(1) in the complete-sequence model becomes

$$z_{012} = H_{012} x_{012} + e_{012},$$

where $e_{012} = T_X^{-1} e_{abc}$ is the complete-sequence measurement error. The verification matrix in the complete-sequence model is $F_{012} = H_{012}((H_{012})^{\dagger} H_{012})^{-1}(H_{012})^{\dagger} - Id$. The following lemma shows the relation between the verification matrix in the three-phase model and in the complete-sequence model.

Lemma 1. $F_{012} = T_Z F_{abc} T_Z^{-1}$.

Proof. We use the fact that $3T_Z^{\dagger} = T_Z^{-1}$.

$$\begin{aligned} F_{012} &= H_{012}(H_{012}^{\dagger} H_{012})^{-1} H_{012}^{\dagger} - Id \\ &= T_Z H_{abc} T_X (T_X^{\dagger} H_{abc}^{\dagger} T_Z^{\dagger} T_Z H_{abc} T_X)^{-1} T_X^{\dagger} H_{abc}^{\dagger} T_Z^{\dagger} - Id \\ &= 3T_Z H_{abc} T_X (T_X^{\dagger} H_{abc}^{\dagger} H_{abc} T_X)^{-1} T_X^{\dagger} H_{abc}^{\dagger} T_Z^{\dagger} - Id \\ &= 3T_Z H_{abc} T_X T_X^{-1} (H_{abc}^{\dagger} H_{abc})^{-1} (T_X^{\dagger})^{-1} T_X^{\dagger} H_{abc}^{\dagger} T_Z^{\dagger} - Id \\ &= 3T_Z H_{abc} (H_{abc}^{\dagger} H_{abc})^{-1} H_{abc}^{\dagger} T_Z^{\dagger} - Id \\ &= T_Z H_{abc} (H_{abc}^{\dagger} H_{abc})^{-1} H_{abc}^{\dagger} T_Z^{-1} - T_Z T_Z^{-1} \\ &= T_Z F_{abc} T_Z^{-1}. \end{aligned}$$

□

As mentioned previously, the standard practice only uses the direct-sequence component for state estimation and BDD. Let D be the $m \times 3m$ matrix that selects only the direct-sequence elements from the complete-sequence model. Specifically, D is a block diagonal matrix with $\begin{bmatrix} 0 & 1 & 0 \end{bmatrix}$ along its diagonal. Then the direct-sequence residuals are $F_1 z_1 = D F_{012} z_{012}$.

B. System Model in Rectangular Coordinates

The system model in complex form is a theoretical model that enables to identify closed-form vulnerability conditions. However, in practice the system model that is used in measurement systems is in rectangular coordinates. This is due to the fact that the use of the WLS estimator as state estimator is widespread and that it is linear over $\mathbb{R}$ and not over $\mathbb{C}$, because the covariance of the error is not linear over $\mathbb{C}$.

We now present an adaptation to three-phase systems of the system model in rectangular coordinates introduced in [30]. The $6m \times 1$ real three-phase measurement vector and the $6m \times 1$ real complete-sequence measurement vector in rectangular coordinates are denoted by $z_{\square,abc} = \left(\mathrm{Re}(z_{abc}^{[1]}), \mathrm{Im}(z_{abc}^{[1]}), \cdots, \mathrm{Re}(z_{abc}^{[3m]}), \mathrm{Im}(z_{abc}^{[3m]})\right)^T$ and $z_{\square,012}$, respectively; $z_{abc}^{[1]}$ denotes the measurement of index 1 of measurement vector z_{abc}. The measurement-to-state equation becomes $z_{\square,abc} = H_{\square,abc} x_{\square,abc} + e_{\square,abc}$, where $H_{\square,abc} \in \mathbb{R}^{6m \times 6n}$ is the three-phase measurement-to-state matrix in rectangular coordinates, $x_{\square,abc} \in \mathbb{R}^{6n}$ is the three-phase state vector in rectangular coordinates and $e_{\square,abc} \in \mathbb{R}^{6m}$ is the three-phase measurement error in rectangular coordinates. The $6m \times 6m$ real WLS verification matrix is $G_{\square,abc} = H_{\square,abc}(H_{\square,abc}^T C_{\square,abc}^{-1} H_{\square,abc})^{-1} H_{\square,abc}^T C_{\square,abc}^{-1} - Id$, where $C_{\square,abc}$ is the covariance matrix of the three-phase measurement error in rectangular coordinates. Therefore, the three-phase WLS residuals in rectangular coordinates are computed as $G_{\square,abc} z_{\square,abc}$.

The three-phase measurement, state and error vectors and the three-phase measurement-to-state and verification matrices in rectangular coordinates can be transformed into their complete-sequence model counterparts using the block-diagonal transformation matrices $T_{\square,Z} \in \mathbb{R}^{6m \times 6m}$ and $T_{\square,X} \in \mathbb{R}^{6n \times 6n}$. $T_{\square,Z}$ has the following 6×6 matrix along its diagonal

$$\frac{1}{3}\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & \cos(\frac{2\pi}{3}) & -\sin(\frac{2\pi}{3}) & \cos(-\frac{2\pi}{3}) & -\sin(-\frac{2\pi}{3}) \\ 0 & 1 & \sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) & \sin(-\frac{2\pi}{3}) & \cos(-\frac{2\pi}{3}) \\ 1 & 0 & \cos(-\frac{2\pi}{3}) & -\sin(-\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) & -\sin(\frac{2\pi}{3}) \\ 0 & 1 & \sin(-\frac{2\pi}{3}) & \cos(-\frac{2\pi}{3}) & \sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{bmatrix}$$

and $T_{\square,X}$ has its inverse along its diagonal.

For the system model in complex form, the relation between the matrices in the three-phase and complete-sequence models becomes $H_{\square,012} = T_{\square,Z} H_{\square,abc} T_{\square,X}$ and $C_{\square,012} = T_{\square,Z} C_{\square,abc} T_{\square,Z}^{-1}$. The following lemma shows the relation between the WLS verification matrices in the three-phase and complete-sequence models.

Lemma 2. $G_{\square,012} = T_{\square,Z} G_{\square,abc} T_{\square,Z}^{-1}$.

Proof. The proof is very similar to the proof of lemma 1. By replacing $T_{\square,Z}^T = 3T_{\square,Z}^{-1}$, $T_{\square,X}^T = 3T_{\square,X}^{-1}$ and $C_{\square,012}^{-1} = 3T_{\square,Z} C_{\square,abc}^{-1} T_{\square,Z}^T$ in $G_{\square,012} = H_{\square,012}(H_{\square,012}^T C_{\square,012}^{-1} H_{\square,012})^{-1} H_{\square,012}^T C_{\square,012}^{-1} - Id$, we obtain $G_{\square,012} = T_{\square,Z} G_{\square,abc} T_{\square,Z}^{-1}$. □

As for the complex system model, we denote the direct-sequence verification matrix and measurement vector in rectangular coordinates by $G_{\square,1}$ and $z_{\square,1}$, respectively.

C. Attack Model

We consider an attacker that is able to manipulate the time reference of K sites, where each site is a group of buses where PMUs share the same time reference, as defined in [30]. A manipulation of the time reference of a site by d seconds induces a phase shift $\delta = 2\pi f d$ rad in the phasors measured by the PMUs of the attacked site, where f is the voltage frequency. Let S_k be the set of phasor indices measured at site

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

number k. If site k is attacked, then the attacked measurement vector at site k is $z_{abc}^{S_k\prime} = e^{j\delta} z_{abc}^{S_k}$: all the phases are shifted by δ and the magnitudes are unchanged. The values for other sites are unchanged:

$$(z'_{abc})_i = \begin{cases} e^{j\delta} z^i_{abc} & \text{if } i \in S_k \\ z^i_{abc} & \text{otherwise.} \end{cases}$$

Observe that the attacked measurement vector at site k in the complete-sequence model and in the direct-sequence model are subject to the same phase shift $z_{012}^{S_k\prime} = T_Z z_{abc}^{S_k\prime} = e^{j\delta} T_Z z_{abc}^{S_k} = e^{j\delta} z_{012}^{S_k}$ and $z_1^{S_k\prime} = D z_{012}^{S_k\prime} = e^{j\delta} D z_{012}^{S_k} = e^{j\delta} z_1^{S_k}$.

In order to identify and possibly remove anomalous measurements, state estimation in power grids is generally combined with bad data detection (BDD) algorithms. The most widely used techniques for BDD rely on the analysis of the measurement residuals obtained after state estimation, and are variants of either the largest normalized residual (LNR) test or the χ^2-test. The LNR-test checks the presence of unusually large residual values and the χ^2-test checks that the distribution of the sum of the residuals is plausible. Therefore, a TSA that does not modify the residuals is undetected by such BDD algorithms, which motivates the following definition.

Definition 1. *(Undetectable TSA) A TSA against a group of sites is undetectable under WLS if the residuals are not changed by the attack, i.e.,*

$$G_{\square,abc}\Delta z_{\square,abc} = 0, \text{ where } \Delta z_{\square,abc} = z'_{\square,abc} - z_{\square,abc},$$
$$G_{\square,012}\Delta z_{\square,012} = 0, \text{ where } \Delta z_{\square,012} = z'_{\square,012} - z_{\square,012},$$
$$G_{\square,1}\Delta z_{\square,1} = 0, \text{ where } \Delta z_{\square,1} = z'_{\square,1} - z_{\square,1},$$

depending on the chosen model.

Unfortunately, the computation of the WLS residuals is not linear over $\mathbb{C}$ but is linear over $\mathbb{R}$, whereas the computation of the LS residuals is linear over $\mathbb{C}$. The following lemma shows that despite this important difference, the vulnerability conditions are equivalent.

Lemma 3. *Consider the residuals under LS and under WLS, then*

$$G_{\square,abc} z_{\square,abc} = 0 \iff F_{abc} z_{abc} = 0,$$
$$G_{\square,012} z_{\square,012} = 0 \iff F_{012} z_{012} = 0,$$
$$G_{\square,1} z_{\square,1} = 0 \iff F_1 z_1 = 0.$$

Proof. The proof for the direct-sequence model is presented in [30]. The proofs for the three-phase and complete-sequence models are analogous to that of the direct-sequence model. □

As a consequence, we can perform the vulnerability analysis of three-phase state estimation using the complex LS verification matrix.

III. Vulnerability analysis of three-phase systems

In this section, we first show that the vulnerability conditions of a grid in the three-phase and complete-sequence models are equivalent. We then show that in the presence of unbalances, the three-phase model of the system is less vulnerable to undetectable attacks than the direct-sequence model of the system, and thus a three-phase state estimator is more recommended for LSE. Finally, we consider the case of attacks that only slightly modify the residuals, thus potentially remaining undetected by the BDD mechanisms, and we show that if the system is balanced then WLS using the direct-sequence model is at least as vulnerable as WLS using the complete-sequence model.

A. Exact Vulnerability Analysis

We first show that the vulnerability conditions for a group of sites are equivalent in the two considered three-dimensional models, i.e., the three-phase and complete-sequence models. Second, we show that if a TSA is feasible on a three-dimensional model of the system, then necessarily the one-dimensional model (i.e. only the direct sequence) can also be attacked. These results rely on the following characterization of the vulnerability conditions in the three-phase and in the complete-sequence models, for a group of sites $S = \cup_k S_k$. As a shorthand, for an index set S let us denote by F^S a submatrix of F formed by the columns indexed by S.

Lemma 4. *Consider the set of measurement indices S, then*

$$F_{012}^S z_{012}^S = T_Z F_{abc}^S z_{abc}^S.$$

Proof. Because T_Z and T_X are block diagonal matrices with T and T^{-1} along their diagonal, respectively, the complete-sequence model verification matrix has the following structure

$$F_{012} = \begin{bmatrix} TF_{abc}^{[1:3,1:3]}T^{-1} & \cdots & TF_{abc}^{[1:3,3m-3:3m]}T^{-1} \\ \vdots & & \vdots \\ TF_{abc}^{[3m-3:3m,1:3]}T^{-1} & \cdots & TF_{abc}^{[3m-3:3m,3m-3:3m]}T^{-1} \end{bmatrix}.$$

Hence, $F_{012}^S = T_Z F_{abc}^S (T_Z^{-1})^S$. Similarly, we can write $z_{012}^S = T_Z^S z_{abc}^S$ and we obtain

$$F_{012}^S z_{012}^S = T_Z F_{abc}^S (T_Z^{-1})^S T_Z^S z_{abc}^S = T_Z F_{abc}^S z_{abc}^S.$$

□

Theorem 1. *A group of sites is vulnerable to undetectable TSAs in the three-phase model if and only if it is vulnerable to undetectable TSAs in the complete-sequence model.*

Proof. Previous work from [30] showed that the analysis of the system vulnerability to TSAs reduces to the vulnerability analysis of every site and every pair of sites. We first show the equivalence for single sites. Theorem 4 of [30] states that a site measuring $p \geq 1$ phasors with indices in S_k, such that no measurement alone is critical and at least one measurement is not equal to 0, is vulnerable to undetectale TSAs if and only if $p \geq 2$ and z^{S_k} is in the null space of F^{S_k}. Hence, a site, with measurement indices in S_k, is vulnerable to TSAs in the three-phase model if and only if $F_{abc}^{S_k} z_{abc}^{S_k} = 0$, hence $T_Z F_{abc}^{S_k} z_{abc}^{S_k} = 0$ and thus by Lemma 4, $F_{012}^{S_k} z_{012}^{S_k} = 0$. Similarly, if the site is vulnerable to TSAs in the complete-sequence model, then $F_{012}^{S_k} z_{012}^{S_k} = 0$, hence $T_Z^{-1} F_{012}^{S_k} z_{012}^{S_k} = 0$ and thus by lemma 4, $F_{abc}^{S_k} z_{abc}^{S_k} = 0$.

We now show the equivalence for pairs of sites. Theorem 6 of [30] states that two sites measuring phasors with indices in S_i and S_k, respectively, such that $|S_i| + |S_k| = p$, no measurement is critical by itself, neither site is vulnerable to TSAs by itself and at least one measurement in each site is not

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

equal to zero, are vulnerable to TSAs if and only if $F^{S_i}z^{S_i}$ and $F^{S_k}z^{S_k}$ are colinear. Hence, a pair of sites, with measurement indices in S_i and S_k, is vulnerable to TSAs in the three-phase model if and only if $F^{S_i}_{abc}z^{S_i}_{abc}$ and $F^{S_k}_{abc}z^{S_k}_{abc}$ are colinear $\iff$ $\exists l \in \mathbb{C}^*$ such that $F^{S_i}_{abc}z^{S_i}_{abc} + lF^{S_k}_{abc}z^{S_k}_{abc} = 0$. By Lemma 4, this is equivalent to $T_Z F^{S_i}_{012}z^{S_i}_{012} + lT_Z F^{S_k}_{012}z^{S_k}_{012} = T_Z(F^{S_i}_{012}z^{S_i}_{012} + lF^{S_k}_{012}z^{S_k}_{012}) = 0$. Because T_Z is invertible, this is equivalent to $F^{S_i}_{012}z^{S_i}_{012} + lF^{S_k}_{012}z^{S_k}_{012} = 0$, i.e., $F^{S_i}_{012}z^{S_i}_{012}$ and $F^{S_k}_{012}z^{S_k}_{012}$ are colinear. □

Theorem 2. *If a group of sites is vulnerable to undetectable TSAs in the three-phase or complete-sequence model, then its direct-sequence representation is also vulnerable to undetectable TSAs. The converse is not always true.*

Proof. As for Theorem 1, we use the result from [30] which states that the analysis of the system vulnerability to TSAs reduces to the vulnerability analysis of every site and every pair of sites. We first show the relation for single sites. Recall that a site with measurement indices in S_k is vulnerable to TSAs in a three-dimensional model if and only if $F^{S_k}_{012}z^{S_k}_{012} = 0$. Hence, by definition, the direct-sequence residuals are $F^{S_k}_1 z^{S_k}_1 = DF^{S_k}_{012}z^{S_k}_{012} = 0$, where D is the matrix, defined in Section II-A, that selects only the direct-sequence elements from the complete-sequence model measurement vector.

Similarly, we show the relation for pairs of sites. Recall that a pair of sites, with measurement indices in S_i and S_k, is vulnerable to TSAs if and only if $F^{S_i}_{012}z^{S_i}_{012}$ and $F^{S_k}_{012}z^{S_k}_{012}$ are colinear vectors, which is equivalent to stating that there exists an $l \in \mathbb{C}^*$ such that $F^{S_i\cup S_k}_{012}\begin{bmatrix} z^{S_i}_{012} \\ lz^{S_k}_{012}\end{bmatrix} = 0$. Then, $F^{S_i\cup S_k}_1\begin{bmatrix} z^{S_i}_1 \\ lz^{S_k}_1\end{bmatrix} = DF^{S_i\cup S_k}_{012}\begin{bmatrix} z^{S_i}_{012} \\ lz^{S_k}_{012}\end{bmatrix} = 0$. Therefore, if $F^{S_i}_{012}z^{S_i}_{012}$ and $F^{S_k}_{012}z^{S_k}_{012}$ are colinear, then $F^{S_i}_1 z^{S_i}_1$ and $F^{S_k}_1 z^{S_k}_1$ are also colinear. Observe that D is not an invertible matrix, thus the converse is not always true. □

Theorem 2 shows that the set of vulnerabilities for the three-phase model is a subset of those for the direct-sequence model. In principle, the inclusion need not be strict, as shown by the next result.

Theorem 3. *For a balanced three-phase system, a group of sites is vulnerable to undetectable TSAs in the three-phase or complete-sequence model if and only if its direct-sequence representation is vulnerable to undetectable TSAs.*

Proof. Recall that by definition, when the system is balanced, $z_b = \alpha^2 z_a$ and $z_c = \alpha z_a$ with $\alpha = e^{2j\pi/3}$. Hence, when the system is balanced, $z_0 = z_2 = 0$ and $z_1 = z_a$. Also, when the system is balanced, the verification matrix in the three-phase model is of the form

$$F_{abc} = \begin{bmatrix} P_{11} & \cdots & P_{1m} \\ \vdots & & \vdots \\ P_{m1} & \cdots & P_{mm}\end{bmatrix}, \text{ where } P_{xy} = \begin{bmatrix} a_{xy} & b_{xy} & b_{xy} \\ b_{xy} & a_{xy} & b_{xy} \\ b_{xy} & b_{xy} & a_{xy}\end{bmatrix}$$

with $a_{xy},\ b_{xy} \in \mathbb{C}\ \forall 1 \le x, y \le m$. After transformation using T_Z, we obtain that the verification matrix in the complete-sequence model F_{012} is a block matrix with 3×3 blocks

$$Q_{xy} = \text{diag}(a_{xy} + 2b_{xy}, a_{xy} - b_{xy}, a_{xy} - b_{xy}).$$

Therefore, if the system is balanced, then $F^{S_k}_{012}z^{S_k}_{012} = F^{S_k}_1 z^{S_k}_1$ because the other values are equal to 0. Hence, $F^{S_k}_{012}z^{S_k}_{012} = 0$ if and only if $F^{S_k}_1 z^{S_k}_1 = 0$, where S_k is the set of measurement indices at bus k. Similarly for a pair of sites with measurement indices in S_i and S_k, we obtain ERR $\left[F^{S_i}_{012}z^{S_i}_{012}|F^{S_k}_{012}z^{S_k}_{012}\right] =$ ERR $\left[F^{S_i}_1 z^{S_i}_1|F^{S_k}_1 z^{S_k}_1\right]$. Hence, when the system is balanced, $F^{S_i}_{012}z^{S_i}_{012}$ and $F^{S_k}_{012}z^{S_k}_{012}$ are colinear if and only if $F^{S_i}_1 z^{S_i}_1$ and $F^{S_k}_1 z^{S_k}_1$ are colinear. Recall that the analysis of the system vulnerability to TSAs reduces to the vulnerability analysis of every site and every pair of sites. □

Theorem 3 implies that in a balanced three-phase system, the three-phase and direct-sequence models are equally vulnerable to TSAs. However, in an unbalanced three-phase system, three-phase state estimation is less vulnerable to undetectable TSAs than state estimation based on the direct-sequence model. In other words, a site or a pair of sites whose direct-sequence representation is vulnerable to TSAs may not be vulnerable using a three-phase representation. Intuitively, if the three-phase measurements are all taken into account, an attack at a site shifts three times more phasors than in the direct-sequence representation, making it harder to remain undetected.

B. Approximate Vulnerability Analysis

A group of sites that is not vulnerable to undetectable TSAs could potentially be vulnerable to attacks that only slightly change the residuals. In what follows we analyze the potential vulnerability of sites and pairs of sites to such attacks. Unlike for undetectable TSAs for which Lemma 3 allowed us to focus on the LS verification matrix, due to the change of the residuals we have to perform the potential vulnerability analysis of three-phase state estimation using the WLS verification matrix in rectangular coordinates.

For the purpose of measuring the distance to vulnerability we rely on and extend vulnerability metrics introduced in [30] for a single site and for a pair of sites. It is sufficient to consider these two metrics as the analysis of the system vulnerability to TSAs can be reduced to the vulnerability analysis of every site and every pair of sites, as shown in [30]. Let us first recall the metrics for the direct-sequence model.

Definition 2. *[30] The direct-sequence vulnerability metric for*

- *a site k is defined as $\|R^{S_k}_1 z^{S_k}_1\|$,*
- *a pair of sites (i,k) is defined as $1 - ERR(\left[R^{S_i}_1 z^{S_i}_1|R^{S_k}_1 z^{S_k}_1\right])$,*

where $R_1 \in \mathbb{C}^{2m\times m}$ and $G_{\square,1} \in \mathbb{R}^{2m\times 2m}$ are given by

$$R_1 = \frac{1}{2}\begin{bmatrix} G^1_{\square,1} - jG^2_{\square,1} \\ G^3_{\square,1} - jG^4_{\square,1}\end{bmatrix} \text{ and } G_{\square,1}z_{\square,1} = \begin{bmatrix} G^1_{\square,1} & G^2_{\square,1} \\ G^3_{\square,1} & G^4_{\square,1}\end{bmatrix}\begin{pmatrix} Re(z_1) \\ Im(z_1)\end{pmatrix},$$

and ERR *is the effective rank ratio.*

The effective rank ratio (ERR) of a matrix is the ratio of the largest singular value in absolute value to the sum of all singular values in absolute value. The closer the metrics are to 0, the more vulnerable is the site or the pair of sites. If the metric is equal to 0 then the site or the pair of sites is in fact vulnerable to undetectable TSAs, while if the metric is close

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

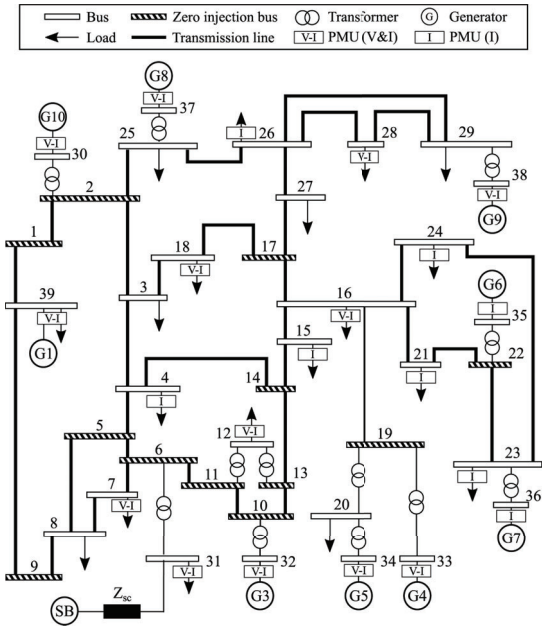

Fig. 1: PMU deployment on the IEEE 39-bus benchmark system.

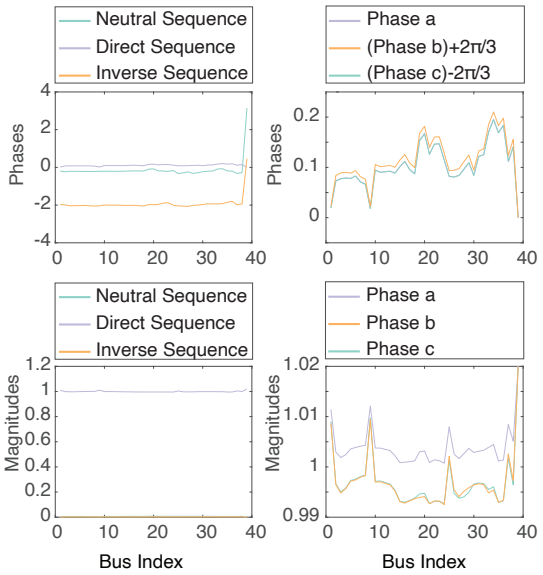

Fig. 2: Voltage phasors in a balanced system, phase representation and symmetric components, obtained after load-flow calculation at a single time instant

to 0 then an attacker may be able to compute an attack that could potentially remain undetected by the BDD algorithms. For three-phase analysis we propose to adapt Definition 2 as follows.

Definition 3. *The three-dimensional vulnerability metric in the three-phase model (resp. complete-sequence model) for*

- *a site k is defined as $\|R^{S_k}_{abc} z^{S_k}_{abc}\|$ (resp. $\|R^{S_k}_{012} z^{S_k}_{012}\|$),*
- *a pair of sites (i,k) is defined as $1 - ERR(\left[R^{S_i}_{abc} z^{S_i}_{abc} | R^{S_k}_{abc} z^{S_k}_{abc}\right])$ (resp. $1 - ERR(\left[R^{S_i}_{012} z^{S_i}_{012} | R^{S_k}_{012} z^{S_k}_{012}\right])$),*

where $R_{abc} \in \mathbb{C}^{6m \times 3m}$ (resp. $R_{012} \in \mathbb{C}^{6m \times 3m}$) is defined from blocks of $G_{\square,abc}$ (resp. $G_{\square,012}$).

Since the covariance matrix affects the structure of the WLS verification matrix, it is not possible to establish an equivalence result similar to that of Theorem 3 for the approximate vulnerability metrics, not even if the system is balanced. Nevertheless, in what follows we show that if the system is balanced then WLS using the direct-sequence model is at least as vulnerable as WLS using the complete-sequence model.

Theorem 4. *For a balanced three-phase system,*

- *the direct-sequence vulnerability metric of a site k is no more than its three-dimensional counterpart: $\|R^{S_k}_{012} z^{S_k}_{012}\| \geq \|R^{S_k}_1 z^{S_k}_1\|$,*
- *the direct-sequence vulnerability metric of a pair of sites i and k is no more than its three-dimensional counterpart: $1-ERR([R^{S_i}_{012} z^{S_i}_{012} | R^{S_k}_{012} z^{S_k}_{012}]) \geq 1-ERR([R^{S_i}_1 z^{S_i}_1 | R^{S_k}_1 z^{S_k}_1])$.*

Proof. As previously, $z_0 = z_2 = 0$ if the system is balanced, therefore, $R^{S_k}_{012} z^{S_k}_{012}$ is equal to the product of the submatrix of $R^{S_k}_{012}$ consisting of only the direct-sequence columns, with the direct-sequence measurement vector $z^{S_k}_1$. Hence, $R^{S_k}_1 z^{S_k}_1$ is a subvector of vector $R^{S_k}_{012} z^{S_k}_{012}$, i.e., $R^{S_k}_{012} z^{S_k}_{012}$ is equal to $R^{S_k}_1 z^{S_k}_1$ concatenated with more values. As a result, $\|R^{S_k}_{012} z^{S_k}_{012}\| \geq \|R^{S_k}_1 z^{S_k}_1\|$. With a similar reasoning, we obtain that matrix $[R^{S_i}_{012} z^{S_i}_{012} | R^{S_k}_{012} z^{S_k}_{012}]$ corresponds to matrix $[R^{S_i}_1 z^{S_i}_1 | R^{S_k}_1 z^{S_k}_1]$ with added rows, thus $\text{rank}([R^{S_i}_{012} z^{S_i}_{012} | R^{S_k}_{012} z^{S_k}_{012}]) \geq \text{rank}([R^{S_i}_1 z^{S_i}_1 | R^{S_k}_1 z^{S_k}_1])$. Observe that the ERR is equal to 1 if and only if the matrix is of rank equal to 1 and decreases as the rank increases. Therefore, we obtain that $\text{ERR}([R^{S_i}_{012} z^{S_i}_{012} | R^{S_k}_{012} z^{S_k}_{012}]) \leq \text{ERR}([R^{S_i}_1 z^{S_i}_1 | R^{S_k}_1 z^{S_k}_1])$. □

IV. Numerical Results

We use simulations based on measurements from the Lausanne power grid to illustrate our results, thus demonstrating the superiority of the three-phase model in detecting TSAs.

A. Electrical Model

We perform the evaluation on the IEEE 39-bus benchmark system. We consider a PMU allocation in which 21 PMUs are deployed in the system, as shown in Figure 1. Among the 21 PMUs, 13 PMUs measure both voltage phasors and injected current phasors at buses {7, 12, 16, 18, 28, 30, 31, 32, 33, 34, 37, 38, 39}, and 8 PMUs measure only injected current phasors at buses {4, 15, 21, 23, 24, 26, 35, 36}. We assume that the PMUs are able to measure the three phases of several phasors simultaneously. Moreover, we consider that the set of buses {1, 2, 5, 6, 9, 10, 11, 13, 14, 17, 19, 22} are zero-injection buses. We mentioned previously that groups of buses that share the same time clock are called sites. Throughout our simulations, we consider that the time reference of every bus can be compromised individually, i.e., sites consist of single buses.

We obtained active and reactive three-phase power measurements measured by 15 PMUs installed in the 125 kV grid of the city of Lausanne, recorded in 2016. Some of the PMUs monitor 1 power line and others monitor 2 power lines, resulting in a total of 22 available measurement points. We

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

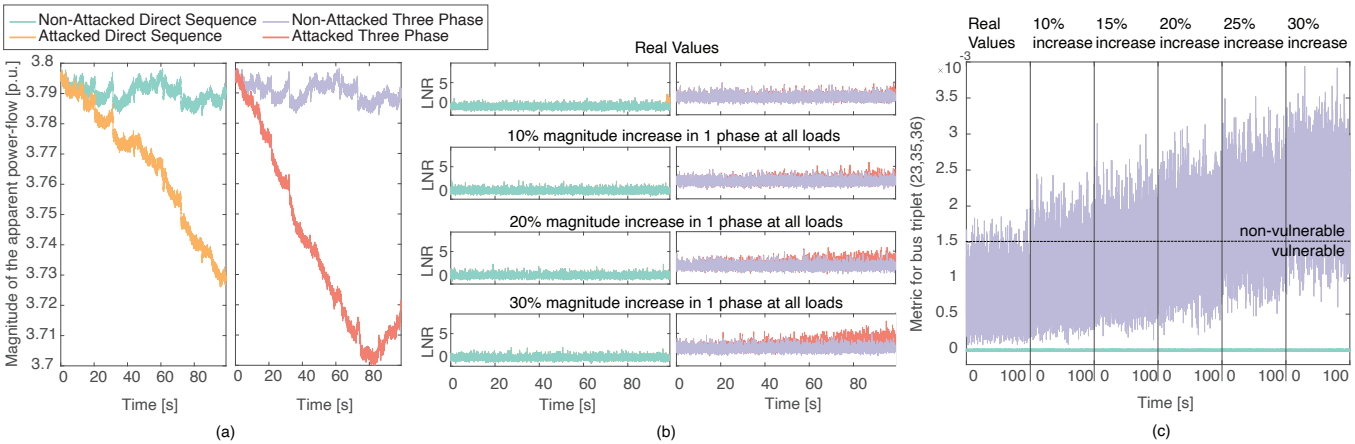

Fig. 3: Balanced measurements, attack on $\{23,35,36\}$: (a) Magnitude of the power-flow on the line between buses 21 and 22, with and without an attack on the direct-sequence and three-phase measurements; (b) LNR values with and without an attack with increasing unbalances: the attacked and non-attacked LNR values of the direct-sequence measurements are indistinguishable, whereas they are increasingly distinguishable for the three-phase measurements; (c) Vulnerability metric with increasing unbalances:the direct-sequence metric is constant at 0 (i.e. vulnerable) and the three-phase metric increases as the unbalances increase.

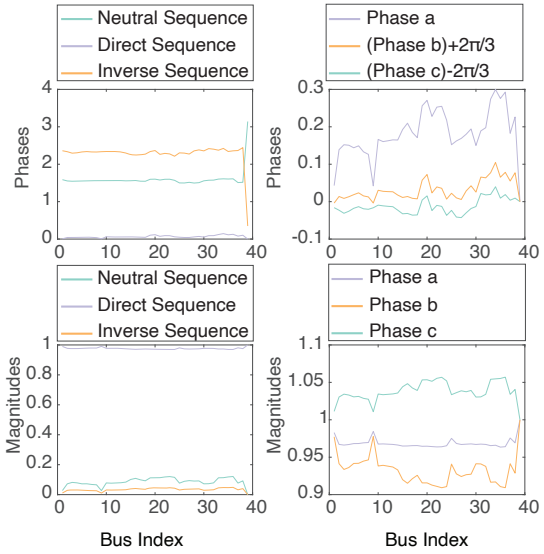

Fig. 4: Real unbalanced voltage phasors after the load flow at one time-instant according to the complete-sequence and three-phase models.

assigned one set of three-phase PMU measurements to each of the 19 loads of the IEEE 39-bus benchmark. After running the load flow, we obtained three-phase voltage phasors for each bus. These voltages are considered as state values. We then created the measurements by adding noise in their phase and magnitude according to the level of noise of 0.1-class PMUs. We consider that the frequency with which we obtain measurements is $50Hz$. All presented attacks are computed using the output constrained PI-controller clock servo aware (OCPI) attack strategy presented in [29]. This attack strategy takes into account the presence of a clock servo in each PMU, used for controlling the clock adjustment rate. The attack strategy targets a minimum of three buses simultaneously, since an attack targeting less than three non-critical buses is always detectable [29]. Attacks targeting more than three buses have been shown to be successful in [29], but in this paper we present TSAs targeting a triplet of buses for the sake of simplicity. The BDD algorithm used to illustrate the detectability of an attack is the LNR test on the WLS residuals [26; 28; 29].

B. Practically Balanced Measurements and Increasing Unbalances

In the real data obtained from the Lausanne grid, we found some periods of time in which the three phases of the loads are very close to being balanced. Figure 2 shows the phase and magnitude of the state voltage values at each bus at one time-instant. We observe that the phases are almost the same shifted by $\frac{-2\pi}{3}$ and $\frac{2\pi}{3}$ and that the magnitudes are almost the same centered around 1. We also observe that the neutral-sequence and inverse-sequence components are very close to 0 in magnitude.

We simulated an attack on the direct-sequence measurements of the triplet of buses $\{23,35,36\}$, with the goal of minimizing the estimated power-flow on the line between buses 21 and 22, during a time interval of 100s (i.e. 5000 measurements) during which the system is practically balanced. We chose to attack this triplet because, as shown in Figure 3c, its direct-sequence vulnerability metric is equal to 0, which means that it is vulnerable to TSAs. We then applied the same attack on the three-phase measurements. Figure 3a shows the non-negligible effect of the attack on the magnitude of the estimated power-flow, with respect to the direct-sequence (left) and the three-phase measurements (right). The LNR values for the direct-sequence (left) and the three-phase (right) measurements are shown in the first row of Figure 3b. Notice that in both cases, the attacked and non-attacked LNR values are indistinguishable. In other words, the attack is undetectable whether the BDD algorithms take as input the direct-sequence measurements or the three-phase measurements. The first column of Figure 3c shows that the vulnerability metric computed for the triplet of buses with the direct-sequence measurements is equal to 0 during the entire simulation and is around $0.75e-3$ in the three-phase model. In both cases the metric is very low, showing that TSAs can be performed undetectably. Note that in Section III-B, the vulnerability metric was introduced for pairs of sites but in the simulations, we chose to target three sites simultaneously.

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

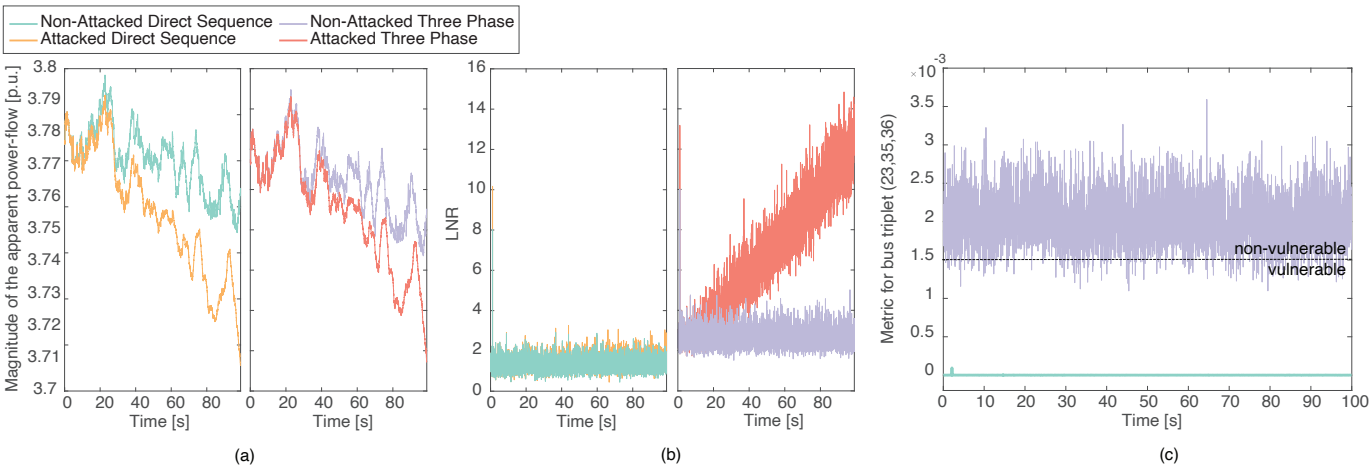

Fig. 5: Unbalanced system, attack on {23,35,36}: (a) Magnitude of the power-flow on the line between buses 21 and 22, with and without an attack on the direct-sequence and three-phase measurements; (b) LNR values with and without an attack: the attack is undetected using the direct-sequence model but is detected with three-phase estimation; (c) Vulnerability metric: the direct-sequence metric shows vulnerability and the three-phase metric is above the triplet-vulnerability threshold.

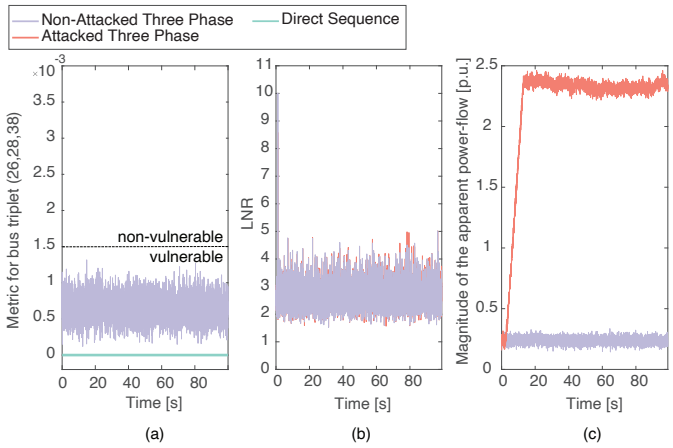

Fig. 6: Undetectable attack on the three-phase unbalanced measurements of buses {26,28,38}: (a)Vulnerability metric: both metrics are always below the triplet-vulnerability threshold; (b) Results of the LNR test with and without the attack are hardly distinguishable; (c) The attack results in a one order of magnitude misestimation of the magnitude of the power-flow on the transmission line between buses 26 and 28.

The metric computed is the same metric generalized to three sites: $1 - \text{ERR}(\left[R^{S_{23}} z^{S_{23}} | R^{S_{35}} z^{S_{35}} | R^{S_{36}} z^{S_{36}}\right])$. The closer the latter is to 0, the more vulnerable the triplet of buses is.

We investigate the level of unbalance required to create a discrepancy in the detectability of attacks applied to the direct-sequence and the three-phase measurements, by introducing unbalance in the power-flow measurements from the Lausanne grid. Generally, unbalances can have various sources, including different amounts and types (inductive and capacitive) of loads, and line parameters. For clarity, we chose to use one source of unbalance: we gradually increased the magnitude of the loads on one phase by 10%, 15%, 20%, 25% and 30%. For each considered level of unbalance we computed an undetectable attack in the direct-sequence model, which we then applied to the three-phase model. Figure 3b shows that the LNR values of the attacked and non-attacked direct-sequence measurements are always indistinguishable, which means that the attack on the direct sequence remains undetected as the unbalance increases. In contrast, Figure 3b shows that between the 10% and 30% magnitude increase, the LNR values of the attacked and non-attacked three-phase measurements are increasingly distinguishable. Hence, the attack on the three-phase measurements is becoming easier to detect. As expected, Figure 3c shows that the vulnerability metric remains unchanged for the direct-sequence measurements and gradually increases for the three-phase measurements. Depending on the LNR detectability threshold that we want to set, we can find the corresponding vulnerability metric threshold. For example, it is reasonable to say that an attack with the LNR values obtained with the 20% or 25% magnitude increase, can be easily detected. Therefore, a reasonable choice for the triplet-vulnerability threshold would be $1.5e-3$, as shown in Figure 3c.

C. Unbalanced Measurements

Next, we focus on actual unbalanced measured data from the Lausanne grid. Figure 4 shows the phase and magnitude of the voltage phasors at each bus at one time instant. We observe that both the angles and the magnitudes are quite different across phases, and that the latter is not always close to 1. We also observe, as a sign of unbalance, that the neutral-sequence and inverse-sequence components are distinguishable from 0. We used this real dataset to compute TSAs targeting the same triplet of buses as previously {23,35,36} with the same objective of reducing the estimated power-flow on the line between buses 21 and 22.

Figure 5a shows the non-negligible effect of the attack on the magnitude of the estimated power flow on the line between buses 21 and 22. The attacked and non-attacked LNR values presented in Figure 5b are indistinguishable for the direct-sequence measurements (left), whereas they are clearly distinguishable for the three-phase measurements (right). As expected, Figure 5c shows that the vulnerability metric computed for the direct-sequence measurements is always very low, close to 0, and that the vulnerability metric computed for the three-phase measurements is always above the triplet-vulnerability threshold $1.5e-3$, which we empirically established in Section IV-B. Therefore, the use of the three-phase

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

measurements as input to the BDD algorithms enables the detection of the attack, which is not the case if we use only the direct-sequence measurements.

D. Undetectable Attack on Three-Phase Measurements

In this section we consider an attacker that mounts its attack on the three-phase unbalanced measurements instead of on the direct-sequence measurements only. We show that even though employing a three-phase state estimator significantly reduces the vulnerability of power-system state estimation to TSAs, undetectable TSAs may be possible despite using a three-phase state estimator. The measurements used in this section are the unbalanced measurements used in Section IV-C. For the PMU deployment shown in Figure 1 we found that the triplet of buses $\{26, 28, 38\}$ has a low three-phase vulnerability metric value, as shown in Figure 6a. We observe that both the direct-sequence and the three-phase metrics are below the triplet-vulnerability threshold, and hence we expect that we can perform an undetectable attack against this triplet.

Figure 6b shows the results of the LNR test on the attacked and non-attacked three-phase measurements. We observe that the LNR values obtained with and without the attack are indistinguishable. Notably, Figure 6c shows that the TSA results in a very large (one order of magnitude) overestimation of the apparent power flow on the transmission line between buses 26 and 28. This scenario shows that even though a three-phase state estimator is harder to attack, it might still be vulnerable to undetectable TSAs.

E. Vulnerability Analysis of Different PMU Deployments

The previous results demonstrate the potential of a three-phase state estimator in detecting TSAs against the IEEE 39-bus system for the PMU deployment shown in Figure 1. We now extend our analysis to other PMU deployments.

Random PMU deployment on the IEEE 39-bus system: to assess the impact of the number of PMUs on the vulnerability to TSAs, we considered random PMU deployments with a total of M phasor measurements, consisting of M_v voltage phasor measurements and M_i current-injection phasor measurements. We did not deploy PMUs on zero-injection buses (12 buses), only on the $b_m = 27$ measurable buses. We choose $M_v \sim \mathcal{U}(M - b_v, b_v)$ and $M_i = M - M_v$, where $\mathcal{U}$ is the discrete uniform distribution. We considered deployments that ensure grid observability, and have no critical measurement. For each deployment we compute the vulnerability metric for all pairs of PMUs, both for the direct-sequence model and for the three-phase model. Figure 7 shows the average number of vulnerable PMU pairs as a function of the number of measurements M in the system, along with 95% confidence intervals. Each point on the curves is the average over 1000 deployments of M phasor measurements. A PMU pair was considered vulnerable if the computed vulnerability metric (either for the direct sequence or the three-phase model) was below 10^{-5}. This value was chosen instead of 0, in order to account for computation approximations. The figure shows that the number of vulnerable pairs is significantly higher in the direct-sequence model than in the three-phase model, but vulnerable pairs of measurements exist in the three-phase model too. These results confirm our observations made for the deployment shown in Figure 1.

Fig. 7: Comparison between the vulnerability of various PMU deployments in the direct-sequence model and the three-phase model.

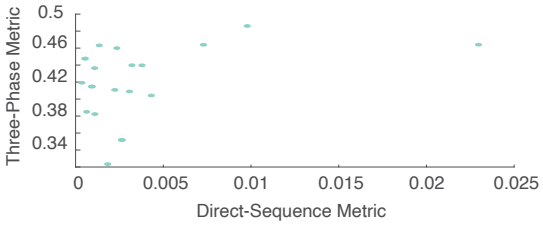

Fig. 8: Metric values for all pairs of buses of the 7-bus grid of the city of Lausanne. See [33] for further details. 6 pairs have a metric very close to 0 in the direct-sequence model and all metric values are far from 0 in the three-phase model.

All PMUs measure voltages and branch currents on the IEEE 39-bus system: we also considered a scenario where every PMU can measure the bus voltage as well as the bus incident branch currents. Given this constraint, we found that the PMU allocation with the smallest number of PMUs such that the IEEE 39-bus system is observable contains 16 PMUs, placed at buses $\{3, 8, 12, 15, 20, 21, 23, 27, 29, 30, 31, 32, 33, 35, 37, 39\}$. With this allocation, we found that 24 pairs of buses are vulnerable to TSAs in the direct-sequence model, while there is no vulnerable pair of buses in the three-phase model. A PMU pair was considered vulnerable if the computed vulnerability metric was below 10^{-5}. The vulnerable pairs are: $(4, 23)$, $(4, 27)$, $(7, 23)$, $(7, 27)$, $(16, 23)$, $(16, 27)$, $(18, 23)$, $(18, 27)$, $(23, 24)$, $(23, 25)$, $(23, 26)$, $(23, 28)$, $(23, 29)$, $(23, 34)$, $(23, 36)$, $(23, 38)$, $(24, 27)$, $(25, 27)$, $(26, 27)$, $(27, 28)$, $(27, 29)$, $(27, 34)$, $(27, 36)$, $(27, 38)$.

Analysis on the 7-bus grid of the city of Lausanne: we tested our method on the real 7-bus grid of Lausanne, where all PMUs measure the bus voltage and the branch currents of all connected lines. A description of the grid can be found in [33]. This grid has an untransposed line, thus the sources of unbalance are both coming from the loads and from the line parameters. We had access to the following data: measurement values, admittance matrix and the noise covariance matrix. We computed our metric for all pairs of buses, and we show the results at a particular time instant in Figure 8. We observe that 6 pairs of buses have dangerously small metric values below 0.001 in the direct-sequence model. In contrast, we observe that all pairs of buses have high metric values above 0.32 in the three-phase model, which means that the 6 vulnerable pairs in the direct-sequence model are not vulnerable in the three-phase model.

V. Conclusion

In this paper we analyzed the benefits of using a three-phase state estimator as a tool for detecting TSAs. We showed that in a balanced three-phase system the vulnerability conditions of the three-phase and the direct-sequence state estimators are equivalent. In contrast, we proved that in an unbalanced system the vulnerability of direct-sequence state estimation does not

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3078104, IEEE Transactions on Smart Grid

imply the vulnerability of three-phase state estimation, which shows that three-phase state estimators can be used for detecting a larger set of TSAs than traditional direct-sequence state estimators. Our simulations performed with real load profiles on an IEEE test system confirmed these results and showed that as the unbalance grows, undetectable TSAs on the direct-sequence measurements may become detectable if three-phase state estimation is used. Results obtained on the 7-bus grid of Lausanne also confirm these observations. Although the use of a three-phase state estimator enables to detect more TSAs, our simulations also showed that it is not always sufficient for completely securing the grid. A promising extension of our work would be to consider a non-linear system model that includes SCADA measurements for hybrid state estimation, but we leave this to be a topic of future work.

ACKNOWLEDGEMENT

This work is carried out within the frame of the Swiss Centre for Competence in Energy Research on the Future Swiss Electrical Infrastructure (SCCER-FURIES) with the financial support of the Swiss Innovation Agency (Innosuisse - SCCER program).

E. Shereen and G. Dán were partly supported by the Swedish Civil Contingencies Agency (MSB) through the Cerces project, by the Swedish Research Council through project 2020-03860, and by the Swedish Foundation for Strategic Research (SSF) through the CLAS project.

REFERENCES

[1] G. Liu, J. Quintero, and V. M. Venkatasubramanian, "Oscillation monitoring system based on wide area synchrophasors in power systems," in *iREP Symposium - Bulk Power System Dynamics and Control - VII. Revitalizing Operational Reliability*, 2007, pp. 1–13.

[2] A. Xue, S. Leng, Y. Li, F. Xu, K. E. Martin, and J. Xu, "A novel method for screening the PMU phase angle difference data based on hyperplane clustering," *IEEE Access*, vol. 7, pp. 97 177–97 186, 2019.

[3] R. Zivanovic and C. Cairns, "Implementation of PMU technology in state estimation: an overview," in *in Proc. of IEEE AFRICON*, vol. 2, 1996, pp. 1006–1011 vol.2.

[4] M. Jamei, A. Scaglione, and S. Peisert, "Low-resolution fault localization using phasor measurement units with community detection," in *Proc. of IEEE SmartGridComm*, 2018, pp. 1–6.

[5] *1588-2019 - IEEE Approved Draft Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, 2019 (accessed June 1, 2020). [Online]. Available: https://standards.ieee.org/content/ieee-standards/en/standard/1588-2019.html

[6] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, 2013.

[7] S. Gong, Z. Zhang, M. Trinkle, A. D. Dimitrovski, and H. Li, "GPS spoofing based time stamp attack on real time wide area monitoring in smart grid," in *Proc. of IEEE SmartGridComm*, 2012, pp. 300–305.

[8] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3, pp. 146–153, 2012.

[9] E. Shereen, F. Bitard, G. Dn, T. Sel, and S. Fries, "Next steps in security for time synchronization: Experiences from implementing IEEE 1588 v2.1," in *Proc. of IEEE ISPCS*, 2019.

[10] S. Barreto, A. Suresh, and J. Le Boudec, "Cyber-attack on packet-based time synchronization protocols: The undetectable delay box," in *Proc. of IEEE Intl. Instrumentation and Measurement Technology Conf.*, 2016, pp. 1–6.

[11] M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "Vulnerability of synchrophasor-based WAMPAC applications to time synchronization spoofing," *IEEE Trans. on Smart Grid*, vol. 9, no. 5, pp. 4601–4612, 2018.

[12] T. Bi, J. Guo, K. Xu, L. Zhang, and Q. Yang, "The impact of time synchronization deviation on the performance of synchrophasor measurements and wide area damping control," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1545–1552, 2017.

[13] M. Delcourt and J. L. Boudec, "TDOA source-localization technique robust to time-synchronization attacks," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2020.

[14] R. G. Lins, S. N. Givigi, and P. R. G. Kurka, "Vision-based measurement for localization of objects in 3-d for robotic applications," *IEEE Trans. Instrum. Meas.*, no. 11, 2015.

[15] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Trans. on Smart Grid*, vol. 6, no. 6, 2015.

[16] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Trans. on Smart Grid*, vol. 9, no. 5, pp. 3954–3965, 2018.

[17] E. Shereen and G. Dn, "Model-based and data-driven detectors for time synchronization attacks against PMUs," *IEEE J. Sel. Areas Commun. (JSAC)*, vol. 38, no. 1, pp. 169–179, 2020.

[18] S. Bhamidipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing via a network of receivers for power systems," in *IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2018, pp. 1485–1491.

[19] B. Brinkmann, K. Bicevskis, R. Scott, and M. Negnevitsky, "Evaluation of single-and three-phase state estimation in distribution networks," in *2017 Australasian Universities Power Engineering Conference (AUPEC)*, 2017, pp. 1–5.

[20] J. Blackburn, *Symmetrical Components for Power Systems Engineering*, 12 2017.

[21] C. Muscas, S. Sulis, A. Angioni, F. Ponci, and A. Monti, "Impact of different uncertainty sources on a three-phase state estimator for distribution networks," *IEEE Trans. on Instrumentation and Meas.*, vol. 63, no. 9, pp. 2200–2209, 2014.

[22] A. P. Meliopoulos, G. J. Cokkinides, and G. K. Stefopoulos, "Numerical experiments for three-phase state estimation performance and evaluation," in *Proc. of IEEE Russia Power Tech*, 2005, pp. 1–7.

[23] U. Kuhar, M. Panto, G. Kosec, and A. vigelj, "The impact of model and measurement uncertainties on a state estimation in three-phase distribution networks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3301–3310, 2019.

[24] L. Zhang, A. Bose, A. Jampala, V. Madani, and J. Giri, "Design, testing, and implementation of a linear state estimator in a real power system," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1782–1789, 2017.

[25] Yue Yang and S. Roy, "Pmu placement for optimal three-phase state estimation performance," in *Proc. of IEEE SmartGridComm*, 2013, pp. 342–347.

[26] M. Gl and A. Abur, "A robust PMU based three-phase state estimator using modal decoupling," *IEEE Trans. on Power Syst.*, vol. 29, pp. 2292–2299, 2014.

[27] B. Zargar, A. Angioni, F. Ponci, and A. Monti, "Multiarea parallel data-driven three-phase distribution system state estimation using synchrophasor measurements," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 9, pp. 6186–6202, 2020.

[28] S. Barreto, M. Pignati, G. Dn, J. Le Boudec, and M. Paolone, "Undetectable PMU timing-attack on linear state-estimation by using rank-1 approximation," *IEEE Trans. on Smart Grid*, vol. 9, no. 4, pp. 3530–3542, 2018.

[29] E. Shereen, M. Delcourt, S. Barreto, G. Dn, J. Le Boudec, and M. Paolone, "Feasibility of time-synchronization attacks against PMU-based state estimation," *IEEE Trans. on Instrumentation and Meas.*, vol. 69, no. 6, pp. 3412–3427, 2020.

[30] M. Delcourt and J.-Y. L. Boudec, "Security measures for grids against rank-1 undetectable time-synchronization attacks," *arXiv, eess.SY*, vol. 2002.12607, 2020.

[31] E. Shereen and G. Dán, "Network-aware mitigation of undetectable PMU time synchronization attacks," in *Proc. of IEEE SmartGridComm*, Nov. 2020.

[32] A. Dervikadi, P. Romano, M. Pignati, and M. Paolone, "Architecture and experimental validation of a low-latency phasor data concentrator," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2885–2893, 2018.

[33] L. Zanni, A. Dervikadi, M. Pignati, C. Xu, P. Romano, R. Cherkaoui, A. Abur, and M. Paolone, "Pmu-based linear state estimation of lausanne subtransmission network: Experimental validation," *Electric Power Systems Research*, vol. 189, p. 106649, 2020.

1949-3053 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: KTH Royal Institute of Technology. Downloaded on June 10,2021 at 19:19:02 UTC from IEEE Xplore. Restrictions apply.