Security Measures for Grids against Rank-1 Undetectable Time-Synchronization Attacks

Marguerite Delcourt \textit{Student Member, IEEE}, Jean-Yves Le Boudec \textit{Fellow, IEEE}

Abstract—Time-synchronization attacks on phasor measurement units (PMU) pose a real threat to smart grids; it was shown that they are feasible in practice and that they can have a non-negligible negative impact on the state estimation, without triggering the bad-data detection mechanisms. Previous works identified vulnerability conditions when targeted PMUs measure a single phasor. Yet, PMUs are capable of measuring several quantities. We present novel vulnerability conditions in the general case where PMUs measure any number of phasors and can share the same time reference. One is a sufficient condition that does not depend on the measurement values. We propose a security requirement that prevents it and provide an algorithm that enforces it. If this security requirement is satisfied, there is still a possibility that the grid can be attacked, although we conjecture that it is very unlikely. We identify two sufficient and necessary vulnerability conditions which depend on the measurement values. For each, we provide a metric that shows the distance between the observed and vulnerability conditions. We recommend their monitoring for security. Numerical results, on the IEEE-39 bus benchmark with real load profiles, show that the measurements of a grid satisfying our security requirement are far from vulnerable.

I. INTRODUCTION

Accurate system estimation is a crucial element for the control and operation of smart grids. Such an estimation relies on measurements of electrical quantities, taken at various grid locations. We assume the use of phasor-measurement units (PMU) to measure voltage and current phasors. The precision of the estimation from phasors depends on the time synchronization of the PMUs \cite{1}, which can be achieved through either a space-based protocol such as GPS synchronization \cite{2} or a network-based protocol \cite{3} such as White Rabbit \cite{4}. In both cases, it is vulnerable to cyber attacks \cite{5}. The GPS synchronization of PMUs is vulnerable to GPS spoofing attacks \cite{6} and the network-based protocols are vulnerable to the insertion of a delay box between the PMUs and their master clocks \cite{7}. Network-based protocols assume that the transmission time of a packet between a PMU and its master clock is symmetric, or has a known asymmetry. A delay box breaks this symmetry and introduces a time offset in the time reference of the targeted PMU. These are physical attacks that are neither prevented nor detected by the cryptographic tools used by the synchronization protocol. As a result, the phase of phasor measurements is shifted, which can non-negligibly impact the state estimation of the system, as it was shown in \cite{8,9}.

In order to make the state-estimation process robust, it is customary to couple the state-estimation algorithm with a bad-data detection (BDD) algorithm such as the largest normalized residual test or the chi-squared test \cite{10}. However, it was shown in \cite{11} that false-data injection attacks can have a non-negligible impact on the state estimation, without triggering any reaction from the BDD algorithms. Subsequent works focused on undetectable attack strategies \cite{12}, on vulnerability identification \cite{13,14} and on the mitigation of such attacks \cite{15}. Although false-data injections are a threat to the state estimation, the risk is limited by the fact that they require physical access to the targeted monitoring devices.

In contrast, it is possible to remotely alter the time reference of PMUs via GPS spoofing \cite{16} or with delay boxes \cite{7}, thus impacting several smart-grid applications, including the state estimation. The authors of \cite{8} propose a strategy to compute undetectable time-synchronization attacks (UTSAs) against vulnerable pairs of PMUs, each measuring a single phasor. They also discuss how vulnerable pairs of PMUs can be targeted simultaneously in order to maximize an attack. Their techniques require that a specific attack-angle matrix is of rank equal to 1, we refer to such attacks as rank-1 UTSAs.

The authors of \cite{9} give a similar technique to find and undetectably attack a set of at least two vulnerable PMUs, each measuring a single phasor. They also show that when targeting at least three PMUs, the solution set of undetectable-attack offsets forms a continuum. They use this property to overcome constraints posed by clock controllers that prevents too large offsets. Their new attack strategies are to target at least three PMUs with gradually increasing offsets; this, in time, maximizes the attacker’s objective.

In \cite{2} a sufficient and necessary vulnerability condition is identified for sets of PMUs with different time references, each measuring a single phasor. Their theory shows that rank-1 UTSAs are feasible on a set of PMUs if and only if the index of separations (IoS) of the attack-angle matrices computed for each pair of PMUs are equal to 1. The IoS is explained in Section II-C. This condition depends on the measurement values and enables them to find all vulnerable sets of PMUs that measure a single phasor. They also identified a sufficient vulnerability condition that does not depend on the measurements. They showed that if the infimum of the IoS, over all possible measurement values, is equal to 1 for all pairs of PMUs in the targeted set, then rank-1 UTSAs are always feasible.

The attack strategies and vulnerability conditions proposed in \cite{8} and \cite{9} require that each offset alters a single PMU that measures a single phasor. Yet, PMUs are capable of measuring several phasors, and several PMUs can share the same time-reference. In order to understand and mitigate rank-1 UTSAs on real grids, it is important to generalize the theory established in \cite{9} to sets of PMUs that possibly share the same time reference and that measure an arbitrary number of phasors. The techniques employed in \cite{9} do not appear to be trivially generalized, hence we rely on new concepts.

We group PMUs, each measuring one or more phasors, in sites if they share the same time-reference. Hence, an offset on the time-reference of a site impacts all of the corresponding phasor measurements in the same manner. Our first contribution is to identify a sufficient and necessary vulnerability condition for rank-1 UTSAs that target a single site that measures an arbitrary number of phasors: item (b) of Theorem 1. We also provide a metric that reflects how close, at a given time, a site is to being vulnerable: left-hand side ($lhs$) of Eq. (1).

If two sites are not vulnerable by themselves, they could still be vulnerable as a pair. Our second contribution is to identify...
vulnerability conditions to rank-1 UTSAs, for such pairs of sites. One is a sufficient condition that does not depend on the measurements: item (b) of Theorem 2. The other is a sufficient and necessary condition that depends on the measurement values: item (a) of Theorem 2. We provide a second metric that reflects how close a pair of sites is to being vulnerable at a given time: lhs of Eq. (4).

Our third contribution is to show that rank-1 UTSAs, on a set of more than two sites, are feasible if and only if they are feasible for any pair of sites within the set.

Finally, our fourth contribution is to mitigate the feasibility of rank-1 UTSAs on a grid by combining our first three results. We establish a security requirement to prevent vulnerabilities identified by item (b) of Theorem 2. Hence, to prevent vulnerabilities that do not depend on the measurements. We provide an algorithm that outputs a set of measurement points that satisfies our requirement. A grid satisfying our requirement can still be vulnerable if it satisfies item (b) of Theorem 2 or item (a) of Theorem 2. Although we conjecture that this is unlikely to occur, we still recommend the monitoring of the two provided metrics: lhs of Eq. (4) and lhs of Eq. (4).

The paper is structured as follows. Section II defines the system model, the attack model and explains the undetectability conditions. Sections III, IV and V prove our first three contributions. Section VI provides security measures to mitigate the feasibility of rank-1 UTSAs. An algorithm to secure grids against structural vulnerabilities is also provided in Section VI. Numerical results, on the IEEE-39 bus benchmark with real load profiles from the Lausanne grid, are given in Section VII. They show that the measurements of a grid satisfying our requirement can still be vulnerable if it satisfies item (b) of Theorem 2. Hence, to prevent vulnerabilities that do not depend on the measurements. If it is equal to or close to zero, we can construct the estimated measurement

\[ H = H x + e, \]

where \( e \in \mathbb{C}^m \) is the measurement error and the topology matrix \( H \in \mathbb{C}^{m \times n} \) is composed of admittance-matrix and binary values. We say that the system is observable when \( H \) is full rank and we say that a set of measurements is critical when removing it renders the system non-observable, i.e., the sub matrix of \( H \) obtained by removing the corresponding rows is not full rank.

The least-squares estimate of the state vector has a closed-form solution \( \hat{x} = (H^H H)^{-1} H^T \hat{z}, \) where \( H^T \) denotes the complex conjugate transpose of \( H \). It is widespread to use the weighted least-squares estimate by using the noise covariance matrix. From the estimated state vector \( \hat{x} \), we can construct the estimated measurement vector \( \hat{z} = H \hat{x} \) and compute its difference with the observed measurement vector \( z \). The result of this difference is the residual vector that is analysed by the BDD algorithms. Define the verification matrix \( F = (H^T H)^{-1} H^T \) and that he knows the topology of the system (i.e. he knows \( H \)) and that he is able to manipulate the time reference of \( q \) sites via a GPS spoofing attack or a delay box insertion. The attack on \( q \) sites affects a total of \( p \geq q \) measurements. An injected time offset \( \delta \) in the time reference of a site directly shifts the phase of all measured phasors in this site by an angle of \( \alpha = 2\pi \delta f \), where \( f \approx 50 \) or 60 Hz is the instantaneous voltage frequency and the offset \( \delta \) is in seconds. Therefore, a measurement \( z_i \) affected by an attack angle \( \alpha \) is of the form \( z_i^o = z_i e^{j\alpha} \); its phase is shifted by the attack angle and its magnitude is unchanged. Note that the injection of an offset in the time reference of a site shifts the phase of all phasors measured in this site by the same attack angle.

The system model and the attack model are the same as in [8], [9]. We now introduce the system model that is the same as in [8], [9], and we define rank-1 UTSAs.

A. System Model

We consider a grid consisting of \( n \) buses. The state estimation is based on \( n \) PMU measurements. Therefore, they correspond to electrical phasors such as currents or voltages. We suppose that the PMUs are placed at various sites of the grid. Each site is equipped with an arbitrary number of PMUs, each simultaneously measuring an arbitrary number of phasors. We suppose that the PMUs within a single site share the same time reference and that the PMUs in different sites have a different time reference.

Because PMUs measure directly voltage and current phasors, the measurement vector \( z \in \mathbb{C}^m \) and the voltage state vector \( x \in \mathbb{C}^m \) are linearly linked by the following equation

\[ z = H x + e, \]

where \( e \in \mathbb{C}^m \) is the measurement error and the topology matrix \( H \in \mathbb{C}^{m \times n} \) is composed of admittance-matrix and binary values. We say that the system is observable when \( H \) is full rank and we say that a set of measurements is critical when removing it renders the system non-observable, i.e., the sub matrix of \( H \) obtained by removing the corresponding rows is not full rank.

B. Attack Model

We suppose that an attacker can observe the measurement vector \( z \), that he knows the topology of the system (i.e. he knows \( H \)) and that he is able to manipulate the time reference of \( q \) sites via a GPS spoofing attack or a delay box insertion. The attack on \( q \) sites affects a total of \( p \geq q \) measurements. An injected time offset \( \delta \) in the time reference of a site directly shifts the phase of all measured phasors in this site by an angle of \( \alpha = 2\pi \delta f \), where \( f \approx 50 \) or 60 Hz is the instantaneous voltage frequency and the offset \( \delta \) is in seconds. Therefore, a measurement \( z_i \) affected by an attack angle \( \alpha \) is of the form \( z_i^o = z_i e^{j\alpha} \); its phase is shifted by the attack angle and its magnitude is unchanged. Note that the injection of an offset in the time reference of a site shifts the phase of all phasors measured in this site by the same attack angle.

C. Undetectability Condition

To the best of our knowledge, all BDD techniques are based on the analysis of residuals computed as the difference between the observed and estimated measurements [17]–[19]. Hence, an attack carefully crafted to ensure that the residuals are unchanged will not be detected. Thus, an attack is undetectable if and only if \( F \Delta z = 0 \), where \( \Delta z \) is the difference between the attacked and unattacked measurement vectors. Suppose that the attacker introduces a time offset \( \delta \) to sites \( q \), define the attack vector \( u = (u_{11}, \ldots, u_{q})^T = (e^{j\alpha_{1}}, \ldots, e^{j\alpha_{q}})^T \in \mathbb{C}^q \), and the \( m \times q \) indicator matrix \( \varphi \) such that

\[ \varphi_{ji} = \begin{cases} 1 & \text{if measurement of index } j \text{ is affected by angle } \alpha_{i}, \\ 0 & \text{otherwise.} \end{cases} \]

It was proven in [8] that the attacks are absolutely undetectable if and only if \( \sum_{i=1}^q (u_{i} - 1) F \text{diag}(z) \varphi_{i} = 0 \), where \( \varphi_{i} \) is the \( i \)-th column of \( \varphi \) and \( \text{diag}(z) \) is the diagonal matrix with measurement values along the diagonal. For scalability, the authors of [8] introduced the \( q \times q \) attack-angle complex hermitian matrix \( W = \varphi^T \text{diag}(z) F^\dagger \text{diag}(z) \varphi \). They showed that an attack vector \( u \) is undetectable if and only if \( W(u - 1) = 0 \). To the best of our knowledge, all known techniques to compute undetectable attack offsets require that the rank of \( W \) is equal to 1. We refer to such attacks as rank-1 UTSAs.

If for a pair of sites, that each measures a single phasor, the rank of \( W \) is not equal to 1, the authors of [8] and [9] show that it is sometimes possible to use a rank-1 approximation of \( W \) for rank-1 UTSAs. This is possible when the index of separation (IoS), defined in [8] as the largest eigenvalue of \( W \) over the sum of both its eigenvalues, is close to 1. This occurs if the largest eigenvalue is significantly larger than the remaining one. In [8], the infimum of the IoS over all measurement values is introduced as IoS*. This quantity does not depend on the measurements. If it is equal to or close to 1, then the IoS is always equal to or close to 1. This condition is used, in [8] and [9], to find vulnerable sets of PMUs, that each measures a single phasor, from the verification matrix only. For sites measuring an arbitrary number of phasors we are required, in Section IV, to study the effective rank of rectangular matrices with possibly more than
two singular values. For this purpose, we introduce the effective rank ratio (ERR) of a matrix as its largest singular value over the sum of all its singular values. The ERR is close to 1 if the largest singular value is significantly larger than the others, in which case the effective rank of the matrix is close to 1. We use this condition to find vulnerable sets of sites that each measure an arbitrary number of phasors.

III. VULNERABILITY CONDITIONS FOR A SINGLE SITE

We now provide a novel sufficient and necessary condition for rank-1 UTSA on a single site measuring $p$ phasors with indices in $S_1$, such that no measurement alone is critical and no measurement is equal to 0.

A. Vulnerability Conditions

We assume that an attacker injects an offset in the time reference of a site; this affects the measurement values. The remaining measurements are not affected by the attack. The following theorem gives necessary conditions in order to mount a rank-1 UTSA.

**Theorem 1.** Consider a rank-1 UTSA on a site measuring $p$ phasors with indices in $S_1$, such that no measurement alone is critical and no measurement is equal to 0.

(a) If $p = 1$: such an attack is never feasible.
(b) If $p \geq 2$: such an attack is feasible if and only if $z_{S_1}$ is in the null space of $F_{S_1}$, which is equivalent to

$$
\|F_{S_1}z_{S_1}\| = 0,
$$

where $\|\|_2$ is the $l_2$-norm and $(F_{S_1})^+$ is the Moore-Penrose inverse of $F_{S_1}$.

**Proof.** When $q = 1$, notice that by definition $W$ corresponds to a single complex value: $W = \left(\sum_{i \in S_1} F_{i}z_{i}\right) \left(\sum_{j \in S_2} F_{j}z_{j}\right)$. In this case, a rank-1 UTSA corresponds to a single complex value $u$ such that $W(u - 1) = 0$. As mentioned in [8], non-trivial attacks exist in this case if and only if $W = 0$. Thus, if and only if

$$
\sum_{i \in S_1} F_{i}z_{i} = 0.
$$

(a) If $p = 1$, then Eq. (2) is equivalent to $F_{1}z_{1} = 0$. In other words, because $z_{1}$ is non-zero, a rank-1 UTSA on a single site that measures a single phasor is feasible if and only if its corresponding column of $F$ is equal to the null vector. Hence, such an attack is feasible if and only if the phasor is critical. As we assume that no single measurement is critical, we conclude that if $p = 1$, then no rank-1 UTSA is feasible.

(b) If $p \geq 2$, observe that the $\textit{lhs}$ of Eq. (2) is equal to $F_{S_1}z_{S_1}$. Therefore, Eq. (2) is satisfied if and only if the targeted measurement vector is in the null space of $F_{S_1}$. Hence, a rank-1 UTSA is feasible if and only if vector $z_{S_1}$ is equal to its orthogonal projection onto the kernel of $F_{S_1}$, in which case the sinus of the angle between them is equal to 0. This sinus is given by the ratio between the length of the orthogonal projection of $z_{S_1}$ onto the orthogonal complement of the kernel of $F_{S_1}$ and the length of $z_{S_1}$. The orthogonal projection onto the orthogonal complement of the kernel of $F_{S_1}$ is $(F_{S_1})^+F_{S_1}$, where $(F_{S_1})^+$ corresponds to the Moore-Penrose inverse of $F_{S_1}$. Therefore a rank-1 UTSA is feasible if and only if

$$
\text{Eq. (1)}
$$

is satisfied.

If a site is not vulnerable to rank-1 UTSA, it might still be close to satisfying the vulnerability condition identified by item (b) of Theorem 1. In other words, if $z_{S_1}$ is not in the null space of $F_{S_1}$, it might still be close to it. The sinus of the angle between $z_{S_1}$ and $\ker(F_{S_1})$ gives insights on the distance between the observed conditions and the ones necessary to mount a rank-1 UTSA. Therefore, the metric given by the $\textit{lhs}$ of Eq. (1) is a measure of the distance between the observed conditions and the vulnerability condition. The closer this metric is to 0, the closer the site is to being vulnerable.

B. Feasibility of the Vulnerability Condition

If a rank-1 UTSA is feasible, then there exists a relation among the measurement values with coefficients computed from values of vectors spanning $\ker(F_{S_1})$. For example, in the case where $p = 2$, an attack is feasible if and only if the two involved measurements $(z_{1},z_{2})$ are such that they satisfy the relation

$$
\frac{z_{1}}{z_{2}} = \frac{n_{1}}{n_{2}},
$$

where $(n_{1},n_{2})^T$ is a fixed vector that spans $\ker(F_{S_1})$. This is because $F_{S_1}$ is an $m$ by 2 matrix, hence its rank is at most equal to 2. As none of the measurements are critical by themselves, its rank cannot be equal to 0 and as $z_{S_1}$ is in the null space of $F_{S_1}$, its rank cannot be equal to 2. Hence, its rank is equal to 1. By the rank theorem, $\ker(F_{S_1})$ is of dimension equal to 1. Hence, $z_{S_1}$ must be a non-zero complex multiple of any vector that spans $\ker(F_{S_1})$, which leads to Eq. (3).

Intuitively, such a relation seems unlikely to occur as measurement values depend on independent loads. For example, if $z_{1}$ is a voltage value $V$ and $z_{2}$ a current value $I$, then at all time instant $i$, a rank-1 UTSA is feasible if and only if

$$
\frac{z_{1}}{z_{2}} = \frac{V_{i}}{I_{i}} = \frac{V_{i}^2}{I_{i}^2} = S_{inj} = \frac{n_{1}}{n_{2}}.
$$

Hence, at all time instants the phase of the complex injected power $S_{inj}$ must remain constant and equal to $\arg\frac{n_{1}}{n_{2}}$. Also, observe that the relation implies that $\frac{V_{i}^2}{I_{i}^2} = \frac{n_{1}}{n_{2}}$. As the magnitude of voltage values is always close to 1, the magnitude of the current values is approximately invariant and close to $\frac{n_{1}}{n_{2}}$. In practice, the injected current and power depends on the loads that vary in time due to external factors. Hence, it seems unlikely that they could be of constant magnitude or phase and even less likely that such constant values could be equal to specific values computed from the verification matrix only. Therefore, we conclude that the necessary conditions for a rank-1 UTSA on a single site that measures two phasors are unlikely to occur on a realistic grid.

We present numerical values of the metric given by the $\textit{lhs}$ of Eq. (1) obtained through realistic simulations in Section VIII. In our simulations, we always encountered large values far from being equal to 0, which corroborates our intuition that necessary conditions to mount a rank-1 UTSA on a single site seem unrealistic; but we still recommend to monitor it on a real grid.

IV. VULNERABILITY CONDITIONS FOR A PAIR OF SITES

If two sites are not vulnerable by themselves to rank-1 UTSA, they could still be attackable together. We identify two novel conditions to simultaneously mount rank-1 UTSA on such two sites. One of them is a sufficient vulnerability condition that is structural as it depends on the verification matrix only. The other is a general necessary and sufficient condition that depends on the measurement values. We then discuss the feasibility of this general vulnerability condition. Finally, we establish the relation between our novel conditions and the vulnerability conditions presented in [8, 9] for the special case where both sites measure only a single phasor (i.e. $p = 2$).

A. Vulnerability Conditions

We suppose that an attacker injects different offsets in the time reference of $q = 2$ sites, hence affecting a total of $p$ phasor measurements with indices listed in $S_1$ and $S_2$ for the first and
second sites, respectively. The following theorem gives necessary conditions in order to mount a rank-1 UTSA.

**Theorem 2.** Consider a rank-1 UTSA on \( q = 2 \) sites measuring phasors with indices in \( S_1 \) and \( S_2 \), respectively, such that \(|S_1| + |S_2| = p\), no measurement is critical by itself, no measurement is equal to 0 and neither site is vulnerable to rank-1 UTSA by itself.

(a) Such an attack is feasible if and only if
\[
(F_{S_1} \cdot z_{S_1} + F_{S_2} \cdot z_{S_2}) = 0.
\]
(b) If \( \text{rank}(F_{S_1} \cdot z_{S_1}) = 1 \), i.e. if all pairs of measurements in \( S_1 \cup S_2 \) are critical: such an attack is always feasible.
(c) If \( \text{rank}(F_{S_1} \cdot z_{S_1}) = p \), i.e. if the combined set of measurements \( S_1 \cup S_2 \) is not critical: such an attack is never feasible.

**Proof.** By definition, rank-1 UTAs are feasible if and only if \( \text{rank}(W) = 1 \). By the rank properties of complex matrices, we have that \( \text{rank}(W) = \text{rank}(T^*T) = \text{rank}(T), \) with \( T = F \text{diag}(z) \cdot \phi \). Hence, rank-1 UTAs are feasible if and only if
\[
\text{rank}(\left[ \sum_{i \in S_1} F_{i,1}z_i \right. \sum_{i \in S_2} F_{i,2}z_i ] = 1.
\]

(a) Eq. (3) is satisfied if and only if either

- one of the columns of the matrix is equal to the null vector.
- or the two columns of the matrix are colinear. Specifically \( F_{S_1} \cdot z_{S_1} \) and \( F_{S_2} \cdot z_{S_2} \) are colinear, which is equivalent to saying that the cosine of the angle between them is equal to 1, this is equal to Eq. (4).

Since \( F_{S_1} \cdot z_{S_1} \) and \( F_{S_2} \cdot z_{S_2} \) are non-zero, they are colinear if and only if there exists an \( l \in \mathbb{C}^* \) such that \( F_{S_1} \cdot z_{S_1} = l F_{S_2} \cdot z_{S_2} \) if and only if
\[
\dim(E_Z \cap E_N) \geq 1, \text{ with } E_Z = \text{span}\{\{z_{S_1},0\}^T,\{0,z_{S_2}\}^T\}
\]
and \( E_N = \ker(F_{S_1} \cdot z_{S_1}) \). According to Grassmann’s formula, this is equivalent to
\[
\dim(E_Z) + \dim(E_N) - \text{rank}([Z|N]) \geq 1,
\]
where \([Z|N] = \begin{bmatrix} z_{S_1} & 0 \\ 0 & z_{S_2} \end{bmatrix} \) and where \( N \) is a matrix with independent columns that span \( \ker(F_{S_1} \cdot z_{S_1}) \). Therefore, rank-1 UTAs are feasible if and only if
\[
2 + p - \text{rank}(F_{S_1} \cdot z_{S_1}) \geq 1 + p - \text{rank}([Z|N]) \geq \text{rank}([Z|N]).
\]
(b) If \( \text{rank}(F_{S_1} \cdot z_{S_1}) = 1 \), then Eq. (6) \( \iff p \geq \text{rank}([Z|N]) \). Observe that in this case, \([Z|N] \) is a p by \( p+1 \) matrix. Hence, it is always the case that the rank of \([Z|N] \) is at most equal to \( p \). In other words, a rank-1 UTSA is always feasible.
(c) If \( \text{rank}(F_{S_1} \cdot z_{S_1}) = p \), then Eq. (6) \( \iff 1 \geq \text{rank}(Z) \), which is never satisfied as \( Z \) is a matrix of rank equal to 2. In other words, a rank-1 UTSA is never feasible.

As mentioned previously, Theorem 2 establishes two novel vulnerability conditions:

- a **structural vulnerability** condition defined by item (b) of Theorem 2; this sufficient vulnerability condition depends on the verification matrix only. In other words, if two sites satisfy this condition, then they are vulnerable but it is also possible that two sites that do not satisfy this condition are vulnerable.
- a **general vulnerability** condition defined by item (a) of Theorem 2; this condition is necessary and sufficient for vulnerability to rank-1 UTAs. It depends on both the verification matrix and the measurement values.

If a pair of sites is not vulnerable to rank-1 UTAs, it could still be close to satisfying the general vulnerability condition. Specifically, if \( F_{S_1} \cdot z_{S_1} \) and \( F_{S_2} \cdot z_{S_2} \) are not colinear, they can still be close to it. The cosine of the angle between them gives insights on this distance, hence on how close the measurements of a pair of sites are to satisfying rank-1 UTSA conditions. As a result, the closer the \( \text{lhs} \) of Eq. (4) is to 0, the closer the pair of sites is to being vulnerable.

Interestingly, Theorem 2 implies that if three different sites \( S_1, S_2, S_3 \) are not vulnerable by themselves, then such a pair is vulnerable. In other words, Eq. (4) defines an equivalence relation over the set of sites that are not vulnerable by themselves.

If a pair of sites is not exactly *structurally* vulnerable to rank-1 UTAs, it can be practically so. Specifically, if the rank of \( F_{[S_1,S_2]} \) is not equal to 1, its effective rank can be close to 1. As mentioned in Section III-B, this distance is captured by the \( \text{ERR} \) of \( F_{[S_1,S_2]} \), which is equal to 1 if and only if the rank is equal to 1. Numerically, it can occur that a column of \( F_{[S_1,S_2]} \) has significantly larger values than the remaining columns, in which case the effective rank is smaller than the computed rank. As a result, \( \text{ERR}(F_{[S_1,S_2]}) \) can be very close to 1. In this case it is likely that a rank-1 UTSA computed from a rank-1 approximation of \( F_{[S_1,S_2]} \), is feasible in practice irrespective of the measurement values.

We present numerical results through realistic simulations in Section VII. Our simulations show that when the rank of \( F_{[S_1,S_2]} \) is not equal to 1, its \( \text{ERR} \) is sometimes very close to 1, in which case the corresponding pair of sites is practically vulnerable.

**B. Feasibility of the General Vulnerability Condition: Eq. (4)**

If a pair of structurally non-vulnerable sites satisfies the general vulnerability condition, there exists a relation between the measurements with coefficients computed from the verification matrix. Specifically, if \( \text{rank}(F_{[S_1,S_2]}) \neq 1 \) but \( z_{S_1} \) and \( z_{S_2} \) are such that \( F_{S_1} \cdot z_{S_1} \) and \( F_{S_2} \cdot z_{S_2} \) are colinear, then at least one of the measurements is directly determined by a combination of the other measurements and values of the vectors spanning \( \ker(F_{[S_1,S_2]}) \).

For example if phasors \( (z_{1,2}) \) and \( (z_{3,2}) \) are measured at the first and second sites, respectively, then a rank-1 UTSA on the two sites is feasible if and only if either
\[
\frac{z_1}{z_2} = \lambda_1 \quad \text{and} \quad \frac{z_3}{z_4} = \lambda_2
\]
where \( (n_1,n_2,n_3,n_4)^T \) is a fixed vector that spans the null space of \( F_{[S_1,S_2]} \); or
\[
\frac{z_3}{z_4} = \frac{1}{2} (u_1n_3 - u_3n_1 + 2u_1n_3 - u_3n_1)
\]
where \( (n_1,n_2,n_3,n_4)^T \) are independent vectors that span the null space of \( F_{[S_1,S_2]} \). The proof of this is not given here but is similar to the one given in Section III-B. As for the single-site vulnerability condition discussed in Section III-B, we conjecture that such relations are unlikely to occur on real grids, as measurement values depend on independent loads.

In our simulations presented in Section VII, the observed values of the \( \text{lhs} \) of Eq. (4) for pairs of sites that do not satisfy the structural vulnerability condition are far from being equal to 0. This corroborates our intuition that the general vulnerability condition seem unlikely to occur for pairs of sites that are not already structurally vulnerable to rank-1 UTAs.
C. Relation with the Vulnerability Conditions of [8], [9]

We now show that if each site measures a single phasor (i.e., \( p = 2 \)), then our vulnerability conditions are equivalent to the vulnerability conditions identified in [8], [9]. The following theorem gives the equivalence for the general vulnerability condition.

**Theorem 3.** Consider a rank-1 UTSA on \( q = 2 \) sites, each measuring a single phasor \( z_1 \) and \( z_2 \), respectively, such that no measurement is critical by itself and no measurement is equal to 0. Then \( \text{IoS}_{1,2}(z_1,z_2) = 1 \) if and only if \( F^1 z_1 \) and \( F^2 z_2 \) are colinear.

**Proof.** As there are only 2 involved measurements, \( W \) is a 2 by 2 matrix. As no measurement is critical by itself, the rank of \( W \) is equal to either 1 or 2. By definition, the IoS of \( W \) is equal to 1 if and only if its smallest eigenvalue is equal to 0, which is equivalent to the rank of \( W \) being equal to 1. Recall from the proof of Theorem 2 that the rank of \( W \) is equal to 1 if and only if Eq. (5) is satisfied. As no measurement is equal to zero or critical by itself, this is equivalent to \( F^1 z_1 \) and \( F^2 z_2 \) being colinear.

Similarly, the following theorem gives the equivalence for the structural vulnerability condition.

**Theorem 4.** Consider a rank-1 UTSA on \( q = 2 \) sites, each measuring a single phasor \( z_1 \) and \( z_2 \), respectively, such that no measurement is critical by itself and no measurement is equal to 0. Then \( \text{IoS}_{1,2}^s = 1 \) if and only if \( \text{rank}(F^{[1,2]}) = 1 \).

**Proof.** We show both directions:

- \( \text{IoS}_{1,2}^s = 1 \rightarrow \text{rank}(F^{[1,2]}) = 1 \): By definition of \( \text{IoS}^s \), if it is equal to 1, then the IoS is equal to 1, whatever the values of \( z_1 \) and \( z_2 \). Therefore, Eq. (5) is satisfied even if \( z_1 = z_2 = 1 \), which is equivalent to \( \text{rank}(F^{[1,2]}) = 1 \).

- \( \text{IoS}_{1,2}^s = 1 \leftarrow \text{rank}(F^{[1,2]}) = 1 \): It was shown in [8] that if \( p = 2 \), then

\[
\text{IoS}^s = \frac{1}{2} + \frac{|f_{12}|}{2(|f_{11}|f_{22})^{1/2}},
\]

with \( f_{ij} = \sum_{i,m} F_{ni}^1 F_{mi}^2 F_{ni} F_{mi} \). Notice that \( |f_{12}|^2 = (\sum_{i,m} F_{ni}^1 F_{mi}^2)^2 = \sum_{i,m} F_{ni}^1 F_{mi}^2 \). If rank \( F^{[1,2]} = 1 \), then there exists \( l \in \mathbb{C}^* \) such that \( F_{ni}^1 = l F_{ni} \) because no measurement is neither equal to 0 nor critical. Hence, \( f_{11} = |l|^2 f_{22} \) and \( |f_{12}|^2 = |l|^2 |f_{22}|^2 \). By plugging them into Eq. (7), we get that \( \text{IoS}^s = 1 \).

Note that \( \text{IoS}_{1,2}^s(z_1,z_2) \) is the IoS of the attack-angle matrix \( W \) computed from measurements (\( z_1,z_2 \)). Also, \( \text{IoS}^{s}_{1,2} \) is the infimum of \( \text{IoS}_{1,2}(z_1,z_2) \) over all possible values of (\( z_1,z_2 \)). Both \( E\text{RR}(F^{[1,2]}) \) and \( \text{IoS}^s_{1,2} \) are independent of measurement values. Theorem 4 implies that one of them is equal to 1 if and only if the other is also equal to 1. Therefore, they are both equal to 1 for an exactly structurally vulnerable pair of sites measuring a single phasor. However, it can easily be seen that \( E\text{RR}(F^{[1,2]}) \) may be close to 1 when \( \text{IoS}^{s}_{1,2} \) is not. In other words, our structural vulnerability condition is better than the one in [8] and [9] as it identifies more sets that are practically vulnerable.

**V. VULNERABILITY CONDITIONS FOR AN ARBITRARY NUMBER OF SITES**

We now show that a rank-1 UTSA targeting an arbitrary number of sites \( q \geq 2 \) that are not vulnerable by themselves, is feasible if and only if for every pair of sites among the targeted set of sites, a rank-1 UTSA is feasible. As a result, the vulnerability analysis of a grid reduces to the vulnerability analysis of each site and each pair of sites. We then establish the relation between our result and those identified in [9] for the special case where all targeted sites measure only a single phasor.

### A. Vulnerability Conditions

The following theorem establishes the general vulnerability condition for an arbitrary number of sites that are not vulnerable by themselves to rank-1 UTSA.

**Theorem 5.** A set of \( m \geq q \geq 2 \) sites, each measuring an arbitrary number of phasors, such that none of the sites are vulnerable to rank-1 UTSA by themselves, are vulnerable together if and only if each pair of sites within the set is vulnerable to rank-1 UTSA.

**Proof.** Define \( S_1, S_2, ..., S_q \) to be the set of measurement indices corresponding to phasors measured in the first, second, up to \( q^{th} \) targeted sites, respectively. Then, the rank of the attack-angle matrix \( W \) corresponds to the rank of the following matrix

\[
T = \begin{bmatrix}
\sum_{i \in S_1} F_{1,i} z_i & \ldots & \sum_{i \in S_q} F_{1,i} z_i \\
\vdots & \ddots & \vdots \\
\sum_{i \in S_1} F_{q,i} z_i & \ldots & \sum_{i \in S_q} F_{q,i} z_i 
\end{bmatrix}.
\]

The rank of this \( m \) by \( q \) matrix is equal to 1 if and only if all columns of \( T \) are dependent. As none of the sites are vulnerable to rank-1 UTSA by themselves, no column of \( T \) is equal to the null vector. Therefore, all sub matrices consisting of two columns of \( T \) must be of rank equal to 1. This means that the attack-angle matrix \( W \) that corresponds to the attack targeting the corresponding two sites is of rank equal to 1. In other words, if a set of \( q \) sites is vulnerable to rank-1 UTSA, then any two sites within the set of targeted sites are also vulnerable to rank-1 UTSA.

Similarly, if there is a set of \( q \) sites such that all pairs of sites within the set are attackable undetectably, then all columns of \( T \) are dependent, which means that its rank is equal to 1. Therefore the large set of \( q \) sites is vulnerable to rank-1 UTSA.

**Theorem 5 implies that a site is vulnerable to rank-1 UTSA either if it is vulnerable by itself or if its combination with at least one other site forms a vulnerable set where all pairs of sites are vulnerable together. Hence, mitigating the feasibility of rank-1 UTSA for each site and each pair of sites is sufficient to mitigate the attack feasibility of the grid.**

### B. Relation with the Results of [9]

The authors of [9] show that measurements can be grouped in equivalence classes, when the IoS values of the attack-angle matrices of all pairs of measurements are equal to 1. Then, they show that a set of measurements is vulnerable to rank-1 UTSA if and only if the set of measurements belong to the same equivalence class. In other words, they show that a set of sites, each measuring a single phasor, is vulnerable to rank-1 UTSA if and only if all pairs of sites within the targeted set is vulnerable. Recall that Eq. (4) defines an equivalence relation over the set of sites that are not

| structural vuln. | general vuln. | distance metric |
|------------------|---------------|----------------|
| single site      | none          | Eq. (6)        |
| pair of sites    | \( E\text{RR}(F^{[1,2]}) \geq 1 \) | Eq. (1) |
vulnerable by themselves. Hence, Theorem 5 shows that a set of non-vulnerable sites is vulnerable if and only if the sites belong to the same equivalence class. Therefore, Theorem 5 applied to sites measuring a single phasor coincides with the result of [9].

VI. MITIGATING RANK-1 UTSAS

To minimize the feasibility of rank-1 UTSAs, we now combine results from Sections III–V and V. We propose an algorithm for ensuring that no pair of sites is structurally vulnerable. Even if a grid is not structurally vulnerable, there is still an unlikely possibility that measurement values are such that some sites or pairs of sites are vulnerable. In order to check the non-vulnerability of the system, we recommend the monitoring of the vulnerability metrics.

A. Securing against the Structural Vulnerability Condition

Apart from vulnerability conditions, Theorem 2 also identifies a structural non-vulnerability condition. Item (c) of Theorem 2 states that if the combined set of measurements from the two sites does not form a critical set, then they are not vulnerable to rank-1 UTSAs, irrespective of their measurement values. Hence, a natural idea to secure all pairs of sites is to ensure that none of them forms a critical set of measurements. However, from an engineering perspective, it is not realistic to impose this security measure, as it would either be impossible to enforce or require much redundancy in the measurements. This would require substantially more PMUs than what is required for observability of the system, which would be costly. For example, by placing PMUs on every bus of the grid used for simulations in Section VII, we obtain that 34% of pairs are critical.

In contrast, it is possible to carefully modify a grid’s PMU allocation such that no pair of sites is structurally vulnerable. Specifically, a security requirement is that the ERR of the measured phasor coincides with the result of [9].

Recall that ERR(F[S1,S2]) = 1 if and only if all pairs of measurements in S1 and S2 are critical. In an observable system, if a pair of sites is such that no measurement is critical and all pairs are critical, by adding one phasor measurement in one of the two sites, at least one pair of measurements will be non-critical. As a result, the ERR of F[S1,S2] will no longer be equal to 1. However, the practical security requirement is stronger and requires that the ERR is not close to 1. Therefore, to secure an observable but vulnerable grid, we propose to identify critical pairs of sites such that the ERR of F[S1,S2] is close to 1 and to iteratively increase the number of phasors that should measure until no critical pair of sites has a high ERR value. A strategy is to increase the number of measured phasors at sites that appear most frequently in the list of vulnerable pairs of sites. Algorithm 1 implements this strategy by recursively building the secured set of measurement points.

The authors of [9] present a rank-1 UTSA targeting g = 5 structurally vulnerable sites. In Section VII, we secure the grid using Algorithm 1 which increases the number of phasor measurements by 15%, and we show that the attack is no longer feasible.

B. Monitoring the General Vulnerability Metrics

Once the grid is secured against structural vulnerabilities, the measurements of sites or of pairs of sites can still satisfy the general vulnerability conditions identified by item (b) of Theorem 2 and by item (a) of Theorem 2. As discussed in Sections III–B and IV–B, we conjecture that such conditions are unlikely to be satisfied in reality. By precaution, we propose to compute, at every estimation of the system’s state, the lhs of Eq. (1) for every site and the lhs of Eq. (4) for every pair of sites. If over time it can be observed that one of the metrics is frequently close to 0, then the measurements satisfy either exactly or approximately a relation with coefficients computed from the verification matrix. In this case, we recommend breaking this relation by modifying the PMU allocation around the corresponding site or pair of sites.

VII. SIMULATIONS

We validate our results with simulations on the IEEE 39 bus benchmark with real load profiles taken from the Lausanne grid at 50 Hz. We apply the security requirements, established in the previous section, and show that they achieve the desired security.

A. Electrical Model

The PMU allocation we consider is depicted in Figure 1. Specifically, there are 12 zero-injection buses, PMUs measuring both voltages and currents, and are placed at buses {30, 37, 28, 38, 18, 39, 12, 16, 7, 31, 32, 34, 33, 20, 25, 26, 29} and PMUs measuring only currents are placed at buses {24, 35, 15, 21, 4, 23, 36}. We define sites to be groups of buses separated by transformers only: {2, 30}, {6, 31}, {10, 32}, {11, 12, 13}, {19, 20, 33, 34}, {22, 35}, {23, 36}, {25, 37}, {29, 38}, the other buses correspond to one-bus sites. With this allocation, no measurement is critical by itself, no PMU is critical by itself but some sites are critical.

Our simulations are done every 20ms over 700s, thus at 35’000 different time instants. At each time instant, we create a measurement vector by computing the load flow. This results in the true state of the system. We then add randomly generated Gaussian noise to the true state, which results in the simulated measurement vector z.

---

**Algorithm 1 Secure-Grid(M)**

**Input:** M (set of measurement points for an observable grid)

**Output:** M new (updated set of measurement points for an observable and structurally non-vulnerable grid)

H ← Create topology matrix from admittance and M
Vulnerable ← ∅
F ← H(HH†)−1H† − Id

for site i in grid do
    Si ← M(i)
end for

for j ≠ i in grid do
    Sj ← M(j)
    Λ ← Singular-Values(F[Si,Sj])
    if max(Λ) ≥ η then
        Vulnerable ← Vulnerable ∪ (i,j)
    end if
end for

if Vulnerable ≠ ∅ then
    while Vulnerable ≠ ∅ do
        freq ← Get the most frequent index in Vulnerable
        M ← M ∪ freq
        for tuple ∈ Vulnerable do
            if freq ∈ tuple then
                Vulnerable ← Remove tuple from Vulnerable
            end if
        end for
    end while
    M ← Secure-Grid(M)
end if

M new ← M
return M new
This attack is performed on a grid with a slightly different PMU allocation. Specifically, only one phasor is measured at bus 26 and no phasors are measured at bus 29. In this setting, they presented an attack on buses 26, 28 and 38. Notice that buses 28 and 38 both measure two phasors simultaneously. This successful attack was found by trials and errors but was not explained by the theory of \cite{9}. We now understand that this set of buses was in fact structurally vulnerable because the rank of the corresponding sub matrix of $F$ is equal to 1. We are now also able to secure the grid against this attack by adding phasors to measure at buses 26 and 29. All attacks presented in \cite{8} and \cite{9} targeted sets of PMUs which were in fact structurally vulnerable to rank-1 UTSAs. Our new security requirement therefore prevents all of them.

Even though the resulting grid is not structurally vulnerable, it is still possible that measurement values satisfy the general vulnerability conditions for a site or a pair of sites. We show that such specific conditions are far from appearing on our realistic grid.

### C. General Vulnerability Condition for Single Sites

At each of the 35,000 time instants of the simulation, we compute the metric given by the lhs of Eq. (4). Recall that this metric is equal to 0 if and only if the targeted measurement vector is in the null space of $F^{S_1}$. The obtained values for the sites measuring more than a single phasor are shown in Figure 3. We observe that for 10 sites, the metric is always approximately equal to 1, which means that the vector is approximately always orthogonal to the null space of $F^{S_1}$, hence extremely far from satisfying the attackability conditions. For four sites, the metric is between 0.32 and 0.5, which is still far from 0. To illustrate that 0.32 reflects that the site is far from being vulnerable, we perform an attack on the corresponding site \{19,20,33,34\} with a constant offset of 20\mu s, which is the maximum offset allowed by the PMU clock controllers in \cite{9}. The obtained largest normalized residuals are approximately 6 times larger than those obtained without an attack. Such a difference is easily identified. In other words, the site that is the closest to satisfying the single-site vulnerability condition is far from being vulnerable in practice. As a result, we observe that the measurement values of all sites of the grid are always far from satisfying the conditions necessary to mount a rank-1 UTSAs.

### D. General Vulnerability Condition for Pairs of Sites

At each of the 35,000 time instants of the simulation we compute the metric given by the lhs of Eq. (1). As in the single-site case, this metric is equal to 0 if and only if $F^{S_1} - z\mathbf{1}_{S_1}$ and $F^{S_2} - z\mathbf{1}_{S_2}$ are colinear. The obtained values for every pair of sites at all time instants are given in Figure 4. We observe that for almost all pairs of sites, the values are always above 0.9 and above 0.8 otherwise. This means that the vectors are approximately always orthogonal to each other, thus extremely far from satisfying the attackability conditions. As
Lhs of Eq. (1)

Fig. 4. Values of the metric given by the left-hand-side of Eq. (1) for each site with more than one measurement. It is never equal to 0: the condition for a rank-1 UTSA on a single site is never satisfied.

Lhs of Eq. (4)

Fig. 5. Value of the metric given by the left-hand-side of Eq. (4) for each pair of sites. It is never equal to 0: the condition for a rank-1 UTSA on a pair of sites is never satisfied.

a result, we observe that at each time instant of the simulation, the measurement values of all pairs of sites are far from satisfying the conditions necessary to mount rank-1 UTSAs.

VIII. CONCLUSION

We showed that the analysis of the vulnerability of a grid to rank-1 UTSAs reduces to the vulnerability analysis for every site and every pair of sites. We identified a sufficient vulnerability condition for pairs of sites that measure an arbitrary number of phasors. This condition does not depend on the measurement values. We established a security requirement to prevent this vulnerability. We also provided an algorithm that enforces our security requirement. If our security requirement is satisfied, it is still possible that measurement values are such that attacks are feasible, although we conjecture that it is unlikely. We identified sufficient and necessary vulnerability conditions for single sites and for pairs of sites, each measuring an arbitrary number of phasors. We recommend the monitoring of two metrics associated to these conditions in order to check the non-vulnerability of the grid. Numerical results, on the IEEE-39 bus benchmark with real load profiles from the Lausanne grid, show that the measurements of a grid satisfying our security requirement are far from being vulnerable to rank-1 UTSAs. Finally, our results, applied to sites measuring a single phasor, coincide with the results of \[1\]. Our new theory also enables us to better understand and thus prevent attacks presented in \[9\].

REFERENCES

[1] G. Barchi, D. Fontanelli, D. Macii, and D. Petri, “On the accuracy of phasor angle measurements in power networks,” IEEE Trans. on Instrumentation and Measurement, 2015.

[2] A. Carta, N. Locci, C. Muscas, and S. Sulis, “A flexible gis-based system for synchronized phasor measurement in electric distribution networks,” IEEE Trans. on Instrumentation and Measurement, 2008.

[3] M. Livia, A. Besigni, A. Flammini, C. Muscas, F. Ponci, and A. Monti, “A software-only ptp synchronization for power system state estimation with pmus,” IEEE Trans. on Instrumentation and Measurement, 2012.

[4] A. Derviškadić, R. Razzaghi, Q. Walger, and M. Paolone, “The white rabbit time synchronization protocol for synchrophasor networks,” IEEE Transactions on Smart Grid, vol. 11, no. 1, pp. 726–738, Jan 2020.

[5] E. Shereen, B. Bitard, G. Dán, T. Sel, and S. Fries, “Next steps in security for time synchronization: Experiences from implementing ieee 1588 v2.1,” in 2019 IEEE International Conference on Control and Communication (ISPCS), Sep 2019, pp. 1–6.

[6] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, “Spoofing gps receiver clock offset of phasor measurement units,” IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 3253–3262, Aug 2013.

[7] S. Barreto, A. Suresh, and J. Y. L. Boudec, “Cyber-attack on packet-based time synchronization protocols: The undetectable delay box,” in 2016 IEEE Int. Instrumentation and Measurement Technology Conf. Proceedings, May 2016, pp. 1–6.

[8] S. Barreto, M. Pignati, G. Dán, J.-Y. L. Boudec, and M. Paolone, “Undetectable pmu timing-attack on linear state-estimation by using rank-1 approximation,” IEEE Trans. on Smart Grid, 2016.

[9] E. Shereen, M. Delcourt, S. Barreto, G. Dán, J.-Y. Le Boudec, and M. Paolone, “Feasibility of time synchronization attacks against pmu-based state-estimation,” IEEE Transactions on Instrumentation and Measurement, pp. 1–1, 2019.

[10] A. Abur and A. Exposito, Power system state estimation: theory and implementation. CRC, 2004, vol. 24.

[11] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” in Proceedings of the 16th ACM Conference on Computer and Communications Security, ser. CCS ’09. New York, NY, USA: ACM, 2009, pp. 21–32. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653666

[12] O. Kosut, L. Jin, K. J. Thomas, and L. Tong, “Malicious data attacks on the smart grid,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 645–658, Dec 2011.

[13] G. Dán and H. Sandberg, “Stealth attacks and protection schemes for state estimators in power systems,” in 2010 First IEEE International Conference on Smart Grid Communications, Oct 2010, pp. 214–219.

[14] A. Ansar, A. N. Mahmood, and Z. Tari, “Identification of vulnerable node clusters against false data injection attack in an ami based smart grid,” Inf. Syst., vol. 53, no. C, pp. 201–212, Oct. 2015. [Online]. Available: http://dx.doi.org/10.1016/j.ins.2014.12.001

[15] O. Vuković, K. C. Son, 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, July 2012.

[16] Z. Zhang, S. Gong, A. Dimitrović, and H. Li, “Time synchronization attack in smart grid: Impact and analysis,” IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 87–98, March 2013.

[17] Y. Lin and A. Abur, “A highly efficient bad data identification approach for very large scale power systems,” IEEE Transactions on Power Systems, 2018.

[18] M. Glad and A. Abur, “A modified chi-squares test for improved bad data detection,” IEEE Eindhoven PowerTech, 2015.

[19] Y. Al-Eryani and U. Baroudi, “An investigation on detecting bad data injection attack in smart grid,” International Conference on Computer and Information Sciences (ICCIS), 2019.