A Continuum of Undetectable Timing-Attacks on PMU-based Linear State-Estimation

Sergio Barreto Andrade
and Jean-Yves Le Boudec
LCA2-EPFL
Lausanne, Switzerland

Ezzeldin Shereen
and György Dán
EES/NSE
KTH
Stockholm, Sweden

Marco Pignati
and Mario Paolone
DESL-EPFL
Lausanne, Switzerland

***Abstract*—Recent innovations in protection and control applications for power systems require the use of Phasor Measurement Unit (PMU) measurements. PMUs rely on precise time synchronization and have been shown to be vulnerable to time synchronization attacks. In this paper, we explore time synchronization attacks against PMU measurements that are undetectable by state-of-the-art Bad-Data Detection (BDD) algorithms, used for Linear State-Estimation (LSE). We show that compromising three or more PMUs enables an attacker to create a continuum of undetectable attacks, and based on geometric arguments we provide a closed form expression for computing the attacks. Furthermore, we provide an algorithm for identifying PMU measurements that are vulnerable to the considered attacks. We use simulations on the IEEE 39-Bus benchmark power system to show that attacks can have a significant impact in terms of power flow mis-estimation that could lead to the violation of ampacity limits in transmission lines.**

***Index Terms*—false-data injection, time synchronization attack, linear state estimation, PMU measurements**

I. Introduction

In the past years there has been an increasing interest in the use of synchrophasor measurements taken by phasor measurement units (PMUs) for applications in power transmission networks (e.g., power-oscillation damping, phase angle monitoring) [1]. PMUs require precise time synchronization, but existing time synchronization solutions are known to be vulnerable [2], even if the time synchronization protocol is authenticated and encrypted [3]. In lack of mitigation, PMU time synchronization attacks could have a significant impact [4], hence it is important to develop an understanding of their feasibility and detectability.

A promising approach for the real-time detection of time synchronization attacks could be bad-data detection (BDD) in conjunction with synchrophasor-based linear state-estimation (LSE). LSE has been known to be prone to undetectable false-data injection attacks since the seminal work in [5], and has been widely studied under different attack models [6]–[9]. Yet, its vulnerability to time synchronization attacks has only been pointed out recently [10], where we proposed a rank-1 approximation method and derived a formula for computing the delays for an undetectable attack against a pair of PMUs. We showed that attacks against pairs of PMUs can be combined, and proposed a greedy algorithm that iterates through a sequence of pairwise undetectable attacks, and picks the one with highest impact. These results on the feasibility of undetectable attacks make it important to understand whether the set of undetectable attacks against three or more PMUs is discrete or continuous, and whether efficient algorithms could exist for maximizing the attack impact. A related question of equal importance is whether the set of PMUs that are vulnerable can be identified by an attacker a priori, based on the system topology only.

In this paper, we answer these fundamental questions by extending the results of [10]. We provide a closed-form expression for attacking $p \geq 3$ non-critical PMU measurement points with p attacking delays, we show that the solution space is a continuum, and we provide an algorithm for performing an attack that maximizes a specific damage function. We show that the attacker can know a priori which PMU sets are vulnerable to the attack. Furthermore, we validate the findings on the 39-bus IEEE benchmark power system by using a synchrophasor-based LSE. We show that even in the case of system dynamics (e.g., sudden reactive power drop) we are able to follow the change in the measurements' phase angles and to keep the attack undetectable by state-of-the-art BDD algorithms. Our results show that the mis-estimation error in the power flows can be up to 1000%, which is almost twice that of the greedy algorithm proposed previously (based on $p = 2$ attacking delays) [10]. This error can lead the network operator into taking wrong protection or control decisions which, as a consequence, could lead to ampacity-limit violations on transmission lines.

The rest of the paper is organized as follows. In Section II, we describe the system and attack model. In Section III we provide algorithms to compute the attacking angles. In Section IV we show how to find the set of PMUs that can be attacked undetectably. In Section V we present numerical results that show the effectiveness of the attack, and in Section VI we conclude the paper.

This research was partially funded by the NanoTera Swiss National Science Foundation project S^3-Grids, and by CTI SCCER-FURIES project

Dán and Shereen were partly funded by the EU H2020 SUCCESS project, grant agreement No. 700416, and by the MSB CERCES project.

II. System and Attack Model

Our system model is akin to that in [10]. We consider a transmission system that consists of N_b buses, with $\mathcal{N}$ being the set of all buses (with $N = N_b$ elements). Let $\mathcal{M}^V \subseteq \mathcal{N}$ be the set of measurement points for voltage, and $\mathcal{M}^I \subseteq \mathcal{N}$ the set of measurement points for nodal currents. Let $\mathcal{M} = \mathcal{M}^V \cup \mathcal{M}^I$ be the set of all measurement points, and $M = |\mathcal{M}|$. Given the measurement matrix H, the measurement model is $z = Hx + e$, where $x \in \mathbb{C}^N$ is the system state, $z \in \mathbb{C}^M$ is the measurement vector and $e \in \mathbb{C}^M$ is the complex measurement-error whose distribution is discussed in detail in [10]. We define the verification matrix

$$F \triangleq H(H^\dagger H)^{-1}H^\dagger - I, \tag{1}$$

where $H^\dagger$ is the conjugate transpose of H. Clearly, $Fz = 0$ occurs if and only if there exists some state x with $z = Hx$.

A. Attack Model

We consider an attacker that is able to manipulate the time synchronization of $p \geq 3$ PMUs, such that the time reference of the attacked PMU is delayed or advanced. This is equivalent to introducing $p \geq 3$ attacking angles $\alpha_i, i = 1 : p$, which correspond to the phase angle shifts of the PMUs due to the attack.

B. Undetectability Condition

In the following we recall the undetectability condition from [10]. Let Ψ be the $M \times p$ attack-measurement indicator matrix, defined by

$$\Psi_{m,i} = 1 \text{ if } m \in \mathcal{A}_i \text{ and } \Psi_{m,i} = 0 \text{ otherwise}, \tag{2}$$

where $\mathcal{A}_i, i = 1 : p$ is the subset of PMU measurements that are affected by attacking angle α_i. Based on Ψ we define the $p \times p$ attack-angle matrix W, which is a Hermitian complex matrix

$$W \triangleq \Psi^T \text{ diag}(z)^\dagger F^\dagger F \text{ diag}(z)\Psi, \tag{3}$$

where z is the complex measurement vector and F is given by (1). Each element of W is given by

$$W_{i,j} = \sum_{l,m,n \in \mathcal{M}} \Psi_{l,i}\Psi_{m,j}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m \tag{4}$$

with $i, j = 1{:}p$, and $\bar{F}_{n,l}$ denotes the conjugate of $F_{n,l}$.

As shown in (Theorem 1, [10]), an attack $\alpha = (\alpha_1, \ldots, \alpha_p)$ is absolutely undetectable if and only if

$$W(\vec{u} - \vec{1}) = 0, \tag{5}$$

where $\vec{u} = (u_1, ..., u_p)^T$, $u_i = e^{j\alpha_i}, i = 1{:}p$ and $\vec{1} = (1, ..., 1)^T$. We call (5) the undetectability condition for an attacking vector $\vec{u}$. In [10], we derived an explicit closed-form expression for α_i for the case where the number of attacking angles is $p = 2$ and when the matrix W in (5) is well approximated by a rank-1 matrix. Furthermore, we showed how to find pairs of PMUs such that this condition holds for any value of the measurement vector z.

III. Computing the attacking angles

In this section we provide algorithms to compute the angles for an undetectable timing attack against vulnerable sets of PMUs, i.e. the W matrix has an effective rank equal to 1. We provide an efficient algorithm in Section IV for finding such sets of PMUs.

A. Computing the Angles for $p = 3$

We start with considering an attack against $p = 3$ PMU measurements. Without loss of generality we denote the attacked measurements by $[z_1, z_2, z_3]$, and the corresponding attack angles by $[\alpha_1, \alpha_2, \alpha_3]$. Since the W has an effective rank equal to 1, we can rewrite (5) as

$$w_1(u_1 - 1) + w_2(u_2 - 1) + w_3(u_3 - 1) = 0, \tag{6}$$

where $[w_1 w_2 w_3]$ is the row of largest norm of the attack angle matrix W, $u_i = e^{i\alpha_i} \in \mathbb{T}$, and $\mathbb{T}$ is the set of complex numbers of modulus 1 (i.e., the circle group).

Equation (6) can be converted to a system of two non-linear equations in three unknowns by equating both the real and imaginary parts of the left-hand side to zero and by using the well-known trigonometric identity $\cos^2\alpha + \sin^2\alpha = 1$. As the number of variables is one more than the number of equations, we expect one variable to be a free variable, e.g., α_3, and this enables a continuum of solutions. Without loss of generality, we assume that the free variable is α_3.

Unfortunately, solving a system of non-linear equations is usually computationally expensive. Therefore, in this section we present a computationally efficient approach to solve (6). Our approach provides a closed-form expression for the solution of (6) based on visualizing it geometrically in the complex plane and consists of the following two steps:

1) Identify the set Θ of feasible values of the free variable α_3.
2) For an $\alpha_3 \in \Theta$, find the corresponding α_1 and α_2 values.

Both steps involve computing the intersection points between two circles. Therefore, it is important to state the following lemma.

Lemma 1. *Consider two circles, C_x and C_y, in the complex plane centered at c_x and c_y and with radii r_x and r_y, respectively. Assume that $r_x > r_y$ and that the two circles intersect. Let $\mathcal{I} = \{I_1, I_2\}$ be the set of intersection points. I_1 and I_2 are given by*

$$I_1 = c_x + a + h, \quad I_2 = c_x + a - h$$

where

$$a = d \cdot \frac{d\bar{d} + r_x^2 - r_y^2}{2d\bar{d}}, \quad h = d \cdot i \cdot \sqrt{\frac{r_x^2 - a\bar{a}}{d\bar{d}}}, \quad d = c_y - c_x.$$

Proof. Figure 1 depicts the problem of finding the intersection of the circles. Let p_f be the point of intersection of the line connecting c_x to c_y and the radical axis of the two circles. Let d be the vector directed from c_x to c_y, that is, $d = c_y -$

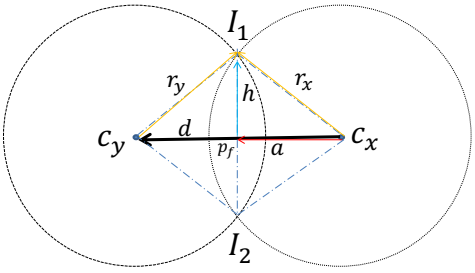

Fig. 1. Example illustrating the intersection between two circles

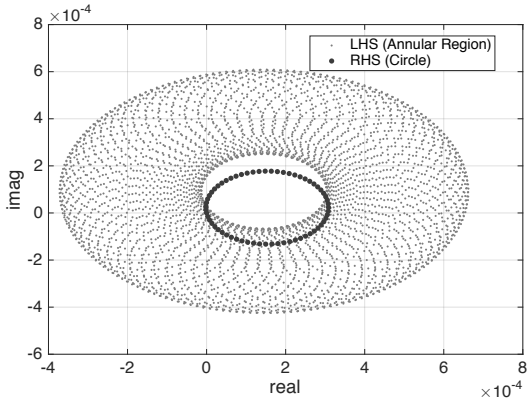

Fig. 2. Illustration of the circle and the annular region of (7) for $[w_1, w_2, w_3] = 10^{-4} * [1.7976, -3.2494 - 9.1894i, 1.5344 + 0.22584i]$

c_x. Furthermore, let vector a be the vector directed from c_x towards p_f, and h be the vector directed from p_f to I_1. Note that a points in the same direction as d and h is perpendicular to both vectors. By inspecting the two triangles (c_x, p_f, I_1) and (c_y, p_f, I_1) we have

$$|a|^2 + |h|^2 = r_x^2, \quad (|d| - |a|)^2 + |h|^2 = r_y^2$$

solving the two equations for $|a|$ and using $|d|^2 = d\bar{d}$, we get

$$|a| = \frac{d\bar{d} + r_x^2 - r_y^2}{2|d|}.$$

Since a is parallel to d, we have $a = d \cdot \frac{|a|}{|d|}$, which yields the expression for a in the lemma. We also know that $|h| = \sqrt{r_x^2 - a\bar{a}}$, and since h is perpendicular to d, we obtain $h = d \cdot i \cdot \frac{|h|}{|d|}$, which in turn yields the expression for h in the lemma. The intersection points can be computed as

$$I_1 = c_x + a + h, \quad I_2 = c_x + a - h.$$

Note that if the two circles intersect only at one point, then $h = 0$, leading to $I_1 = I_2$. □

Now we provide the details of the two steps involved in computing the attack angles.

1) Computing the Feasible Set for the Free Variable: In order to identify the set Θ of feasible values of α_3, let us rearrange (6) to

$$w_1(u_1 - 1) + w_2(u_2 - 1) = -w_3(u_3 - 1) \tag{7}$$

Observe that for $u_3 \in \mathbb{T}$ the set of values of the right-hand side of (7) is a circle C_3 in the complex plane, centered at $c_3 = w_3$ with radius $r_3 = |w_3|$. The set of values of the left-hand side for $u_1, u_2 \in \mathbb{T}$ is an annular region centered at $c_a = -(w_1 + w_2)$, with outer circle C_o of radius $r_o = |w_1| + |w_2|$ and inner circle C_i of radius $r_i = ||w_1| - |w_2||$. Finding a solution to (7) is equivalent to finding a point where C_3 and the annular region intersect, as illustrated in Figure 2.

In general, C_3 could intersect with C_i, C_o, both, or neither; and it is easy to see which of the circles C_3 intersects with. An intersection point will correspond to the beginning or to the end of a feasible interval. We can use Lemma 1 to find those intersection points if they exist. Note that the condition $|d| > r_x + r_y$ or $|d| < r_x - r_y$ is a quick way to check whether an intersection exists or not. To find the corresponding attack angles at the intersection points, we equate the RHS of (7) with each intersection point I. Doing this results in

$$u_3 = \frac{I}{-w_3} + 1, \quad \alpha_3 = arg(u_3) \tag{8}$$

Proposition 1. *For $p = 3$ and $r(W) = 1$, the set U of feasible values of u_3, i.e., $U = \{u_3 : u_3 = e^{i\alpha_3} \ \forall \alpha_3 \in \Theta\}$ is either a non-empty connected compact subset of $\mathbb{T}$ or the union of two non-empty connected compact subsets of $\mathbb{T}$. Furthermore, $u_3 = 1 \in U$.*

Proof. Let $\mathcal{I}_o$ and $\mathcal{I}_i$ be the set of intersection points of the circle C_3 with the outer and the inner circle, respectively. We distinguish between four cases.

1) $|\mathcal{I}_o| + |\mathcal{I}_i| = 1$, i.e., C_3 is tangent to one of the circles. This intersection point must be the one corresponding to $\alpha_3 = 0$, because we know that $\alpha_1 = \alpha_2 = \alpha_3 = 0$ (no attack) is a solution to (6). Thus $\Theta = \{0\}$.
2) $2 \leq |\mathcal{I}_o| + |\mathcal{I}_i| < 4$, i.e., C_3 intersects with one of the circles at two points and could be tangent to the other circle. Let the two intersection points (not the tangent) correspond to angles α_3^1 and α_3^2. If we assume $\{\alpha_3^1, \alpha_3^2\} \in [0, 2\pi]$ and $\alpha_3^1 < \alpha_3^2$ then we have two intervals, $[\alpha_3^1, \alpha_3^2]$ and $[\alpha_3^2, \alpha_3^1 + 2\pi]$, and the set of feasible values is the one including 0, since we know $\alpha_3 = 0$ is a feasible solution. Hence, $\Theta = [\alpha_3^2, \alpha_3^1 + 2\pi]$.
3) $(|\mathcal{I}_o| = |\mathcal{I}_i| = 2)$, i.e., four intersection points. Let the corresponding angles in increasing order be $\{\alpha_3^1, \alpha_3^2, \alpha_3^3, \alpha_3^4\}$. Observe that due to the ordering, angles 1 and 2 correspond to intersection points with the same circle. The feasible set consists of the intervals between angles that correspond to intersection points with different circles. Thus, $\Theta = [\alpha_3^2, \alpha_3^3] \cup [\alpha_3^4, \alpha_3^1 + 2\pi]$. Notice that the second interval includes $\alpha_3 = 0$.
4) $|\mathcal{I}_o| + |\mathcal{I}_i| = 0$ or $|\mathcal{I}_o| + |\mathcal{I}_i| = \infty$. Since $\alpha_3 = 0$ is a feasible solution, we know that $|\mathcal{I}_o| + |\mathcal{I}_i| = 0$ implies that C_3 is inside the annular region, while $|\mathcal{I}_o| + |\mathcal{I}_i| = \infty$ implies C_3 coincides with one of the circles. Thus, in both cases $\Theta = [0, 2\pi[$

Note that Θ always includes the intersection angles because they correspond to feasible solutions, hence the set of feasible

Algorithm 1 Compute-Feasible-Angles(C_3, C_i, C_o)

Input: Centers and radii of $\{C_3, C_i, C_o\}$
Compute $\mathcal{I}_i = \{I_1, I_2\}$ by applying Lemma 1 on (C_3, C_i).
Compute $\mathcal{I}_o = \{I_1, I_2\}$ by applying Lemma 1 on (C_3, C_o).
Compute Θ using Proposition 1
Output: Θ

Algorithm 2 Compute-Angle-Pairs(C_1, C_2)

Input: centers and radii of $\{C_1, C_2\}$
$S \leftarrow \phi$
Compute $\mathcal{I}_{12} = \{I_1, I_2\}$ by applying Lemma 1 on (C_1, C_2).
for all $I \in \mathcal{I}_{12}$ **do**
Compute (α_1, α_2) by using I in equations (10) , (11)
$S \leftarrow S \cup (\alpha_1, \alpha_2)$
end for
Output: S

solutions is closed. Furthermore, due to the structure of the circle group $\mathbb{T}$, an interval of feasible angles maps into a connected set. Moreover, in all four cases, $0 \in \Theta$. In other words, $1 \in U$. □

Algorithm 1 summarizes the procedure of computing the set Θ of feasible values for the free variable.

2) Computing α_1 and α_2: We now turn to the computation of α_1 and α_2 for a chosen $\alpha_3 \in \Theta$. By substituting $s = -w_3(u_3 - 1)$ into (7) we obtain

$$w_1(u_1 - 1) = s - w_2(u_2 - 1). \tag{9}$$

Proposition 2. *For each $\alpha_3 \in \Theta$ there exist either one or two pairs of (α_1, α_2).*

Proof. Both the left- and right-hand sides in (9) represent circles in the complex plane. We will refer to them as C_1 and C_2, respectively. C_1 is centered at $c_1 = -w_1$ with radius $r_1 = |w_1|$, and C_2 is centered at $c_2 = w_2 + s$ with radius $r_2 = |w_2|$. An intersection point of these circles corresponds to a solution to (9). We know that the two circles intersect as $\alpha_3 \in \Theta$. Again, we can use Lemma 1 to find the set of intersection point(s) I_{12}, and each intersection point corresponds to a pair (α_1, α_2).

For each intersection point I we can compute the corresponding (u_1, u_2) and (α_1, α_2) by equating the left and right hand sides of (9) to I. We then get

$$u_1 = \frac{I}{w_1} + 1, \quad u_2 = \frac{-w_3(u_3 - 1) - I}{w_2} + 1 \tag{10}$$

$$\alpha_1 = arg(u_1), \quad \alpha_2 = arg(u_2). \tag{11}$$

□

Algorithm 2 summarises the procedure of computing α_1 and α_2 corresponding to $\alpha_3 \in \Theta$.

B. Computing the Angles for $p \geq 3$

In the following, we provide an algorithm for computing undetectable attacks for the general case of $p \geq 3$. In this case, (7) would become

$$\sum_{i=1}^{p-1} w_i(u_i - 1) = -w_p(u_p - 1) \tag{12}$$

where w_i is the entry in the row of largest norm of the attack angle matrix and the i^{th} column of W. In (12), the right hand side represents a circle in the complex plane with center $c_p = w_p$ and radius $r_p = |w_p|$, while the left hand side represents an annular region with center $c_a = -\sum_{i=1}^{p-1} w_i$, outer radius $r_{ao} = \sum_{i=1}^{p-1} |w_i|$, and inner radius $r_{ai} = \max\{0, 2|w_{i^*}| - \sum_{i=1}^{p-1} |w_i|\}$, where $i^* = \arg\max_{i \in \{1..p-1\}} |w_i|$. Similar to the procedure of the case when $p = 3$, the feasible set Θ_p of α_p can be computed by Algorithm 1. For any choice of $\alpha_p^* \in \Theta_p$ (and corresponding u_p^*) we can rewrite (12) as

$$\sum_{i=1}^{p-2} w_i(u_i - 1) = -w_{p-1}(u_{p-1} - 1) + s_p$$

where $s_p = -w_p(u_p^* - 1)$. Again, Algorithm 1 can be used to compute the feasible range Θ_{p-1} of α_{p-1}. After $p - 2$ iterations of computing the feasible regions, we end up with

$$w_1(u_1 - 1) = \sum_{i=3}^{p} s_i - w_2(u_2 - 1) \tag{13}$$

We notice that (13) has the same form as (9). Therefore, α_1^* and α_2^* can be computed using Algorithm 2. The recursive procedure of computing attacks for $p \geq 3$ is illustrated in Algorithm 3. It is easy to see that Algorithm 3 works for $p = 2$ as well. Note that in Algorithm 3 we do not specify either the order in which the sets Θ_p of feasible values of the angles are computed nor the selection criteria for $\alpha_p^* \in \Theta_p$. For these two factors, the best choice depends on the attack objective and the optimization method used for maximizing this objective.

Algorithm 3 Compute-Attack-Vector$(w, p, \vec{u}^*, s)$

Input: w (first row of W), p, $\vec{u}^*$ (initially $\vec{u}^* \leftarrow 0^{p \times 1}$), s (initially $s \leftarrow 0$)
if p = 2 **then**
$C_1 \leftarrow$ circle defined by $w_1(u_1 - 1)$
$C_2 \leftarrow$ circle defined by $s - w_2(u_2 - 1)$
$S \leftarrow$ Compute-Angle-Pairs(C_1, C_2)
choose $(\alpha_1^*, \alpha_2^*) \in S$
$\vec{u}_1^* \leftarrow e^{j\alpha_1^*}, \quad \vec{u}_2^* \leftarrow e^{j\alpha_2^*}$
return $\vec{u}^*$
else
$C_x \leftarrow$ circle defined by $s - w_p(u_p - 1)$
$(C_i, C_o) \leftarrow$ annular region defined by $\sum_{i=1}^{p-1} w_i(u_i - 1)$
$\Theta_p \leftarrow$ Compute-Feasible-Angles(C_3, C_i, C_o)
choose $\alpha_p^* \in \Theta_p$ and compute $\vec{u}_p^* \leftarrow e^{j\alpha_p^*}$
$s \leftarrow s - w_p(\vec{u}_p^* - 1)$
return Compute-Rank-1-Attack$(w, p - 1, \vec{u}^*, s)$
end if
Output: $\vec{u}^*$

IV. Finding sets of vulnerable PMUs

In what follows we provide sufficient conditions for a set of three or more PMU measurements to be vulnerable, i.e., a sufficient condition for the effective rank of the matrix W in (5) to be equal to 1.

For some $p \geq 2$ and $m \geq 2$ let us denote by $W^{(i_1,..,i_m)}$ the submatrix of W with only rows and columns $(i_1,..,i_m)$. In other words, $W^{(i_1,..,i_m)}$ is the attack angle matrix for attacking only a subset of m measurements from the p measurements attacked in W. For a subset of $m = 2$ measurements let us recall the following definition from [10].

Definition 1. *For a pair (z_i, z_j) of PMU measurements the minimum index of separation*

$$IoS^*_{(i,j)} = \frac{1}{2} + \frac{|f_{ij}|}{2\sqrt{f_{ii}f_{jj}}},$$

where

$$f_{ij} = \sum_{l,m} \sum_{n} \Psi_{l,i}\Psi_{m,j}\bar{F}_{n,l}F_{n,m}.$$

Note that $IoS^*_{(i,j)}$ depends only on the measurement matrix H (i.e. on the admittance matrix of the grid) and does not depend on the actual values of the measurement vector z. Furthermore, from [10] we know that if $IoS^*_{(i,j)} = 1$ then the rank of $(W^{(i,j)})$ is 1 for *any* value of the measurement vector z.

Our main contribution in the following is that we show that the set $\mathcal{M}$ of measurements can be divided into equivalence classes of attackable measurements based on their pairwise IoS^*. Two measurements $\{i, j\}$ belong to the same equivalence class if their pairwise $IoS^*_{(i,j)} = 1$. If three measurements are in the same class, they constitute a vulnerable set, regardless of the actual value of the measurement z; a continuum of undetectable attacks can thus be mounted against them, using the algorithm presented in the previous section. The following theorem summarizes this result.

Theorem 1. *If $IoS^*_{(i,j)} = 1$ and $IoS^*_{(i,k)} = 1$, then $IoS^*_{(j,k)} = 1$. Furthermore, the rank of $W^{(i,j,k)}$ is 1 for* any *value of the measurement vector z.*

In order to prove the theorem, we will first formulate the following lemmas.

Lemma 2. *The entries on the main diagonal of W are non-zero, $W_{i,i} \neq 0$.*

Proof. The diagonal elements of the W matrix are given by

$$W_{i,i} = \sum_{l,m,n \in \mathcal{M}} \Psi_{l,i}\Psi_{m,i}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m \tag{14}$$

Since we assume only one attacked measurement per delay, $l = m$. Thus (14) can be written as

$$W_{i,i} = \sum_{n \in \mathcal{M}} \bar{F}_{n,m}F_{n,m}\bar{z}_m z_m \tag{15}$$

In (15), each term in the summation is indeed a real non-negative value. $W_{i,i}$ could be equal to zero if either $z_m = 0$ or $F_{n,m} = 0, \quad \forall n \in \mathcal{M}$. The first condition is not of interest as it is highly unlikely that a measured value is zero.

The second condition means that the m^{th} column of the F matrix is all zeros. Recall that $F\Delta z = 0$ is the condition for undetectable attacks. If F contains a column m that contains only zeros, the manipulation of z_m would not be detected by the state estimator independent of z, and z_m is not part of state estimation, as there are no redundant measurements for it. Therefore, this case is not of interest either. This concludes the proof. □

Lemma 3. *The rank of the hermitian matrix W is r if and only if there is a principal $r \times r$ submatrix A that is of rank r and all principal submatrices of W obtained by adding to A the same row and the same column, or the same 2 rows and columns are singular.*

Proof. See Theorem 15 in [11]. □

Lemma 4. *If W is hermitian positive semi-definite and the principal submatrix $W^{(i_1,..,i_m)}$ is singular then W is singular.*

Proof. We will call a vector $\vec{x}$ isotropic with respect to a matrix W if $\vec{x}^H W\vec{x} = 0$. Null vectors (i.e. vectors such that $W\vec{x} = 0$) are obviously isotropic; the converse is not true in general, but is true when W is hermitian semi-definite (this can easily be seen by diagonalization).

As $W^{(i_1,..,i_m)}$ is singular, there is a non-zero vector $\vec{x}^{(i_1,..,i_m)} \in \mathbb{C}^m$ such that $W^{(i_1,..,i_m)}\vec{x}^{(i_1,..,i_m)} = 0$. Subsequently, $\vec{x}^{(i_1,..,i_m)}$ is isotropic with respect to $W^{(i_1,..,i_m)}$. We obtain the vector $\hat{\vec{x}}^{(i_1,..,i_m)} \in \mathbb{C}^p$ by expanding $\vec{x}^{(i_1,..,i_m)}$ to dimension p and by filling missing values with zeros (we assume W is a matrix of dimensions $p \times p$). $\hat{\vec{x}}^{(i_1,..,i_m)}$ is isotropic with respect to W, hence is in the null-space of W. Since $\hat{\vec{x}}^{(i_1,..,i_m)}$ is non-zero, W is singular. □

Lemma 5. *If W is hermitian positive semi-definite, the rank of W is r if and only if there is a principal $r \times r$ submatrix A that is of rank r and all principal submatrices of W obtained by adding to A the same row and the same column are singular.*

Proof. Follows directly from Lemma 3 and Lemma 4 □

We are now ready to prove Theorem 1.

Proof of Theorem 1. Consider $W^{(i,j,k)}$. It is hermitian positive semi-definite because of (3). By Lemma 2 the diagonal terms $W_{i,i}$ are non-zero. The principal submatrix obtained by adding row and column j is singular because $IoS^*_{i,j} = 1$ by hypothesis. The same holds if we add row and column k instead of j. By Lemma 5, it follows that the rank of $W^{(i,j,k)}$ is 1. By Lemma 4, it follows that $W^{(j,k)}$ is singular, therefore $IoS^*_{(j,k)} = 1$. □

In practice, Theorem 1 can be used as follows: Compute $IoS^*_{(i,j)}$ for all pairs of measurements i, j and partition the set of measurements by putting i and j into the same class whenever $IoS^*_{(i,j)} = 1$. Any class that has more than one measurement is vulnerable, and can be attacked by using the method of Section III.

V. Numerical Results

In this section we illustrate the proposed methodology on the IEEE 39-bus IEEE benchmark power transmission grid [12]. For ease of comparison, we use the same PMU locations as in [10, Figure 2].

A. Vulnerable Measurements

For the considered PMU locations [10, Table I] provides the pairs of PMUs for which $IoS^*_{(i,j)} = 1$, and we can observe that $IoS^*_{(i,j)} = 1$ when $i, j \in \{21, 23, 24, 35, 36\}$, and $IoS^*_{(i,j)} < 1$ otherwise. This is in accordance with Theorem 1, which establishes that the condition $IoS^*_{(i,j)} = 1$ is transitive. Thus the set of PMUs $\{21, 23, 24, 35, 36\}$ forms an equivalence class, and we can mount an undetectable delay attack against any three or more PMUs in this set using the algorithm proposed in Section III. In what follows we show results for PMUs #21, #23, #24, #35 and #36, and we used the tests described in [13] to ensure that we pick non-critical measurements.

B. Evaluation Methodology

We used the following evaluation procedure

1) On every time step, we compute a load flow to determine the true state of the grid;
2) We perturb the result from the previous step with randomly-generated Gaussian noise characterized by the cumulated standard deviation of the PMUs and their sensors (assuming class 0.1 voltage and current sensors);
3) We compute the attack vector according to the method described in V-D
4) We perform the WLS estimation;
5) We perform the WLS estimation with the attacked measurements;
6) We perform the largest normalized residual (LNR) test ([10], [13]) for the residuals from Step 4 and from Step 5;
7) We compute the estimated power flow for the line between buses #16 and #24, for Steps 4 and 5.

C. Continuum of Solutions in $\alpha_1, \alpha_2, \alpha_3$ $(p = 3)$ Space

Figure 3 shows the set of solutions for the $p = 3$ case in the $\alpha_1, \alpha_2, \alpha_3$ space, i.e., the set of all combinations of attacking angles $(\alpha_1, \alpha_2, \alpha_3)$ that are undetectable for PMUs #21,#23 and #36, at time $t = 0$. The figure shows that the solution set is indeed closed, and a numerical evaluation showed that the solution set in fact forms a quasi-ellipse, i.e., all points lie on a two dimensional plane in three dimensional space. Note that the quasi-ellipse is a function of the measurement vector, it thus changes over time, and during inrushes the curve at time t might be far away from the curve at time $t + 1$. Note that even if the quasi-ellipse changes, it will swivel around the point $(0, 0, 0)$ (no attack), as that is always a solution to (5).

D. Maximization of the Attack Impact

Next, we show how to construct an undetectable attack that maximizes the attack impact. We used the proposed algorithm to build an attack on 5 different PMUs ($p = 5$). To simplify

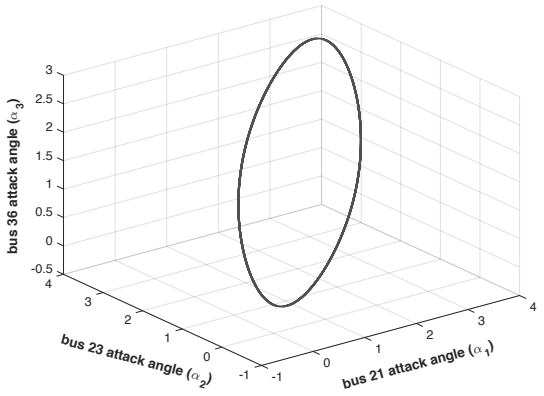

Fig. 3. Set of all combinations of attacking angles $(\alpha_1, \alpha_2, \alpha_3)$ that are undetectable for an attack on PMUs #21,#23 and #36 at time $t = 0$. All units are in radians.

the notation, we set $i = 1, 2, 3, 4, 5$ for PMUs #21, #23, #24, #35 and #36. The goal of the attacker is to find a vector of undetectable attacking angles $\alpha = [\alpha_1, \alpha_2, \alpha_3, \alpha_5, \alpha_5]$, representing the time offsets of the attacked PMUs, which produces a mis-estimation of the power-flow on a specific transmission line. We define the attack impact $\mathcal{V}(\alpha, z)$ to be the perceived reduction of the apparent power-flow on the line between buses #16 and #24. $\mathcal{V}(\alpha, z)$ can be calculated from the power-flow equations; the result depends on the attacking angles α and the measurement z.

Let $z_i(t)$ be the true value of the i-th measurement at time t. In practice, to compute the attacking angles, the attacker cannot have the measurements at time t and needs to use a prediction $\hat{z}(t)$. The attacker's problem at time t can then be formulated as the following non-linear optimization problem:

$$\begin{aligned} &\underset{\alpha(t)}{\text{maximize}}\ \mathcal{V}\left(\alpha(t), \hat{z}(t)\right) \\ &\text{subject to constraints} \\ &W(\hat{z}(t)) \cdot (\vec{u}(t) - \vec{1}) = 0 \\ &\qquad \vec{u}_i(t) = e^{j\alpha_i(t)}, i = 1:5 \end{aligned} \tag{16}$$

In the following numerical illustration we used the persistent predictor $\hat{z}(t) = z(t-1)$. We solve (16) using an exhaustive search on the solution curve, which is possible since we can sample all points of the solution curve using Section III. The attack algorithm is as follows.

1) Use Algorithm 3 to find the feasible region Θ_5 for α_5
2) Choose a subset $\Omega_{\text{test-5}} = \{\alpha_5^1, \alpha_5^2, \ldots, \alpha_5^n\}$, of n equally spaced values in Θ.
3) For each $\alpha_5^i \in \Omega_{\text{test-5}}$: apply Step 1 for α_4 and $\alpha 3$.
4) compute the two combinations of α_1, α_2 given by Algorithm 2 and evaluate $\mathcal{V}((\alpha_1, \alpha_2, \alpha_3^k, \alpha_4^j, \alpha_5^i), \hat{z}(t))$.
5) Choose the combination of α_1, α_2, α_3^k, α_4^j, α_5^i that maximizes $\mathcal{V}((\alpha_1, \alpha_2, \alpha_3^k, \alpha_4^j, \alpha_5^i), \hat{z}(t))$.

In our implementation we used $n = 20$ points for searching in the feasible region of α_5, α_4 and α_3.

Figure 4 shows the LNR test applied to the residuals of the LSE for the unattacked and attacked measurements scenarios.

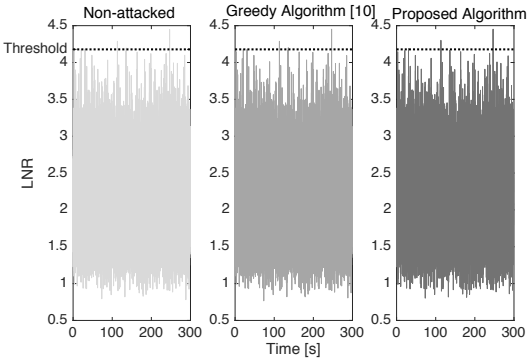

Fig. 4. LNR-test for non-attack and attack scenarios with $p = 5$

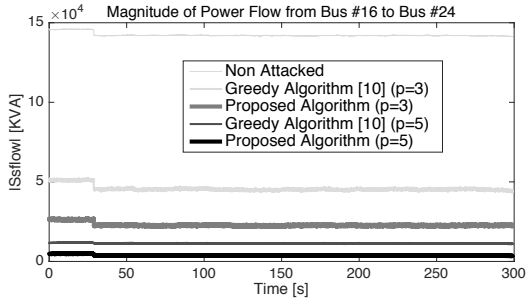

Fig. 5. Comparison of the estimated power flow in the target transmission line between the non-attacked, greedy algorithm used in [10] and the proposed algorithm, both for $p = 3$ and $p = 5$.

The dotted line shows the detection threshold with a confidence of 99.73%, which corresponds to a 3σ deviation for a single measurement. For the sake of comparison, we also show the result of the attack based on the greedy algorithm described in [10] using the same set of three PMU locations. We observe a few extra or increased LNR values in both attacked measurements (e.g., at $t \approx 24s$). They occur whenever the persistent predictor is not a very good predictor, for example when there are changes in the power flows. Notwithstanding, these points are rare and the deviations are very small, so chances are high that the overall perception from the network operator would be that the residuals are not anomalous.

Figure 5 shows the effect of the attack on the magnitude of the apparent power flow in the target line, i.e. the line between buses #16 and #24. In thin light-grey we show the non-attacked scenario, and in black (resp. thick medium-grey) the perceived apparent power when we use the algorithm described in this subsection for $p = 5$ (resp. $p = 3$). We also show, as comparison, in thin medium-grey (resp. thick light-grey) the result of the attack based on the greedy algorithm described in [10] for $p = 5$ (resp. $p = 3$). For the case $p = 3$, we used PMUs #21, #23, and #36. We can verify that the attack computed using the approach proposed in this paper has almost twice as big an impact as the one described in [10] (for both cases $p = 3$ and $p = 5$). This illustrates that being able to discover the entire solution space (a continuum of attacking angles) makes the attack significantly more powerful. Moreover, the mis-estimation error of the power flow, as compared to the non-attacked scenario, is in the order of 1000%. This confirms that, for the network operator, there is a significant impact in terms of the estimated power flow for the target line.

VI. Conclusion

We have shown that it is possible to find a closed-form expression for attacking $p \geq 3$ non-critical measurements with p different angles. The attacker is able to produce a continuum of undetectable attacks from which he can derive an attacking strategy to maximize his goal (e.g., burn a line). We have shown that it is possible to have an a-priori knowledge of the attack locations with an easy-to-implement method that requires only the notion of the H matrix. We have validated our findings with simulations on a benchmark transmission network, and we have shown that there is an important impact on the mis-estimation of the power flows. Future work includes a comparison of the proposed attack against bad-data detection techniques based in measurement prediction [14], rather than residual-based test (e.g., LNR).

References

[1] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, "Wide-area monitoring, protection, and control of future electric power networks," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80–93, Jan 2011.

[2] X. Jiang, J. Zhang, B. Harding, J. Makela, and A. 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.

[3] S. Barreto, A. Suresh, and J.-Y. Le Boudec, "Cyber-attack on Packet-Based time synchronization protocols: the undetectable delay box," in *2016 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, Taipei, Taiwan, May 2016.

[4] Z. Zhang, S. Gong, A. 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, March 2013.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," 2009, pp. 21–32.

[6] O. Kosut, L. Jia, R. 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.

[7] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010*, Oct 2010, pp. 214–219.

[8] Y. Yamaguchi, A. Ogawa, A. Takeda, and S. Iwata, "Cyber security analysis of power networks by hypergraph cut algorithms," in *IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014*, Nov 2014, pp. 824–829.

[9] O. Vukovic, K. C. Sou, G. Dan, 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.

[10] S. Barreto, M. Pignati, G. Dan, J. LeBoudec, and M. Paolone, "Undetectable pmu timing-attack on linear state-estimation by using rank-1 approximation," *IEEE Transactions on Smart Grid*, 2016.

[11] L. E. Dickson, "Modern algebraic theories," *Chicago*, 1930.

[12] A. Pai, *Energy function analysis for power system stability*. Springer Science & Business Media, 2012.

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

[14] K. D. Jones, A. Pal, and J. S. Thorp, "Methodology for performing synchrophasor data conditioning and validation," *IEEE Trans. on Power Systems*, vol. 30, no. 3, May 2015.