Undetectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation

Sergio Barreto, *Member, IEEE,* Marco Pignati, *Member, IEEE,* György Dán, *Member, IEEE,* Jean-Yves Le Boudec, *Fellow, IEEE,* Mario Paolone, *Senior Member, IEEE*

***Abstract*—Smart-grid applications based on synchrophasor measurements have recently been shown to be vulnerable to timing attacks. A fundamental question is whether timing attacks could remain undetected by bad-data detection algorithms used in conjunction with state-of-the-art situational-awareness state estimators. In this paper, we analyze the detectability of timing attacks on linear state-estimation. We show that it is possible to forge delay attacks that are undetectable. We give a closed form for an undetectable attack; it imposes two phase offsets to two or more synchrophasor-based measurement units that can be translated to synchrophasors' time delays. We also propose different methods for combining two-delays attacks to produce a larger impact. We simulate the attacks on a benchmark power-transmission grid, we show that they are successful and can lead to physical grid damage. To prove undetectability, we use classic bad-data detection techniques such as the largest normalized residual and the χ^2-test.**

***Index Terms*—Time Synchronization Attack, False Data Injection, Phasor Measurement Units, Linear State Estimation**

I. Introduction

The coordinated universal time reference (UTC) among phasor-measurement units (PMUs) is essential for the use of synchrophasor measurements in power-transmission networks [1]. This common time-reference is usually obtained through GPS [2], although packet-based time-synchronization protocols (PBTSPs), such as Precise Time Protocol v2 (PTPv2) [3], can be used if the physical location makes the GPS signal inaccessible.

Recent works show that both GPS and PBTSPs can be attacked (e.g., [4], [5]). As civilian GPS satellite signals are not authenticated, they can be spoofed by superimposing a fake signal with a higher signal-to-noise ratio, which would enable an attacker to manipulate a GPS clock [4]. In the case of PBTSPs, an attacker could inject a malicious offset in the time signal by delaying messages, which is feasible because in any PBTSP it is impossible to measure asymmetries in the propagation delay [6]; for this reason, any notion of asymmetry needs to be provided to the protocol (e.g., PTPv2 assumes that propagation delays are symmetric). As the attack involves only delaying messages, such an attack would work even if synchronization messages are encrypted and/or authenticated.

In this paper, we analyze the effect of tampering with the common time reference of PMUs used for linear state estimation of a transmission network, applying the well-known weighted least-square method (WLS) [7]. We show that by manipulating the time reference only, it is possible to perform an attack that does not change the measurement residuals, and thus it bypasses the bad-data detection (BDD) used in state-of-the-art state estimators. We show that a successful attack requires tampering with at least two different angles, and we provide a method to compute attacks that maximize damage while remaining undetectable. We illustrate the findings with respect to a PMU-based linear state-estimator applied to the 39-bus IEEE-benchmark power system. We demonstrate that in given transmission lines, attacks can produce a large mis-estimation of the power flows while passing the χ^2 and largest normalized residual tests (LNR).

The rest of the paper is organized as follows. In Section II, we analyze related work in cyber-attacks on timing references in power systems and on linear state estimators. In Section III, we describe the power system and the attack model. In Section IV, we formulate the time synchronization attack and we provide conditions for undetectability. In Section V, we introduce the rank-1 approximation method, together with a criterion (Index of Separation, IoS) which can be used to find location pairs where the attack is undetectable given the measurement values and a closed-form expression for the attack angles. We also provide an additional criterion IoS* to identify measurements pairs that are attackable regardless of the measurement values. In Section VI, we show how to combine the results of Section V in order to mount attacks with more than two delays. We show that attacks on disjoint pairs, that are each undetectable when performed alone, can be superimposed to produce an undetectable attack. The angles of each attack remain the same as if they were performed alone. Furthermore, attacks on possibly overlapping pairs, that are each undetectable when performed alone, can be combined sequentially. We also show that when performing a sequence of attacks, it is possible to know whether each attack in the sequence will be undetectable before computing the attack, by analyzing the IoS based on the original (non-attacked) measurements. Finally, we show how a sequence of attacks can be computed using a greedy algorithm in order to optimize an attacker's goal such as maximizing the spoof power flow variation (e.g in order to damage a line by an excessive power flow). In Section VII, we use simulations to validate the attacks and to show their effectiveness. In Section VIII, we propose countermeasures for the attacks and discuss the possibility of attacks under the time-correction constraints of PMUs. Section IX concludes the paper.

S. Barreto and J-Y. Le Boudec are with the Laboratory for Communications and Applications 2, École Polytechnique Fédérale de Lausanne EPFL, CH-1015, Lausanne, Switzerland.

M. Pignati and M. Paolone are with the Distributed Electrical Systems Laboratory, École Polytechnique Fédérale de Lausanne EPFL, CH-1015, Lausanne, Switzerland.

G. Dán is with the Laboratory for Communication Networks, School of Electrical Engineering, KTH Royal Institute of Technology, 100 44 Stockholm, Sweden.

II. Related Work

Timing attacks on PMUs have been recently studied. In [8], the authors describe a defense mechanism against GPS spoofing attacks on PMUs, based on cross-check of angle-of-arrival (AOA) detection mechanism and residual-based bad-data detection. Still, AOA detection feature in GPS receivers is not widely available for off-the-shelf PMUs, and residual-based bad-data detection techniques are ineffective against the attack described in this paper. In [9], the cyber-attack mitigation model proposed assumes that at time $t = 0$ the defender may have identified a number of compromised PMUs, which again may not be feasible if the attacker performs an attack such as the one described in this paper. In [4], [10], the authors analyze the implications of timing attacks on synchrophasor-based voltage-stability control in transmission networks but they do not address whether fundamental supervisory control and data acquisition (SCADA) or energy management system (EMS) functionalities, including state estimation (SE), could be affected by these attacks without being detectable.

The first study on undetectable false-data injection (FDI) attacks on linear state-estimators is presented in [11], where the authors formulate an algebraic expression for the existence of undetectable attacks that could not be mitigated by BDD. Other papers that focus in FDI attacks to linear state-estimation can be grouped based on the approach/objective: (i) attack the minimum number of measurements for undetectability [12], [13]; (ii) attack the minimum number of measurements to corrupt a particular target measurement [14], [15]; and (iii) size the attack to compromise information technology (IT) components [14], [16], [17].

In this paper, we combine the objectives of groups (i) and (iii) in the context of timing attacks and propose a criterion for choosing the best attack locations. The prior work assumes that false data injection is performed by tampering with data sent by PMUs or in the SCADA/EMS systems, and requires compromising one or several of these devices. In contrast, our work assumes that the only manipulation concerns the time base used by PMUs. As shown for example in [18], such attacks may be possible without compromising any cryptographic security system. To the best of our knowledge, there is no work that addresses how to perform an undetectable attack on linear state-estimators by maliciously manipulating only the time reference of a set of PMUs.

III. System Model

A. State Model

We consider a one-phase direct-sequence equivalent of a three phase transmission network with N_b buses, and we let $\mathcal{N}$ be the set of all buses (with $N = N_b$ elements). The system state is $x \in \mathbb{C}^N$. It is worth mentioning that state estimators using branch currents as state variables have been proposed, for instance, in [19], and their performance is comparable with voltage-based state estimators as presented in [20]. Therefore, we assume nodal injected-current phasors and/or nodal voltage-phasors measurements coming from PMUs only. We count separately measurements for voltages and for currents. At a bus where both voltage and current are measured, we count two measurement points; at a bus where only voltage (resp. current) is measured, there is a single measurement point. We denote by $\mathcal{M}^V \subseteq \mathcal{N}$ the set of measurement points for voltage, and by $\mathcal{M}^I \subseteq \mathcal{N}$ 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 $M = |\mathcal{M}|$. The measurement vector is $z \in \mathbb{C}^M$.

Let Y be the $(N \times N)$ single-phase complex admittance-matrix, and H be the $M \times N$ complex measurement matrix. We have

$$\begin{aligned} H_{m,m} &= 1,\ m \in \mathcal{M}^V \\ H_{m,n} &= 0,\ m \in \mathcal{M}^V, m \neq n \\ H_{m,n} &= Y_{m,n},\ m \in \mathcal{M}^I, n \in \mathcal{N}. \end{aligned}$$

The measurement model is given by the equation

$$z = Hx + e, \tag{1}$$

where $x \in \mathbb{C}^N$ is the system state, $e \in \mathbb{C}^M$ is the complex measurement-error with a distribution discussed in Section VII-A. Define the verification matrix F as

$$F \triangleq H(H^\dagger H)^{-1}H^\dagger - I \tag{2}$$

We denote with $H^\dagger$ the conjugate transpose of H. Note that $Fz = 0$ if and only if there exists some state x with $z = Hx$. If $Fz = 0$, there is a unique complex vector x that solves $z = Hx$ and it is given by $x = (H^\dagger H)^{-1}H^\dagger z$. In general (i.e., when $Fz \neq 0$), $x = (H^\dagger H)^{-1}H^\dagger z$ is the least-square estimator of the state. Note that in this paper we assume that the state estimation uses a different and more accurate estimation, called *weighted* least-square (WLS), which uses rectangular coordinates instead of complex numbers (SectionVII). The reason for using complex numbers here becomes apparent in the next section, where we find closed form expressions that could not be found otherwise.

Recall that F is a complex matrix, of size $M \times M$. We assume that the system is observable, i.e., dim (range H) = N, so that the rank of F is $M - N$. Such ranks are to be computed while treating F as a $M \times M$ complex matrix.

B. Attack Model

The goal of the attacker is to create a mis-estimation of the state of the grid while maintaining the residuals of the state-estimator unaffected. As illustrated by the attack in Fig. 1, this goal can be achieved using various attack vectors. We consider an attacker that is an insider to the utility, thus he has access to the network topology and to the admittance matrix, but he is not able to physically tamper with any PMU or transducer (sensor). We assume the attacker is able to observe, but cannot forge the measurement vector z, which is consistent with the security standards for synchrophasor data transmission, as those mandate only authentication but not encryption (Section 90-12 in [21]). We thus consider that the attacker can add an offset to the time reference of some PMUs, which will be seen as an offset in the synchrophasor estimation. An attack against the time reference can be done with moderate effort for both PTP and GPS synchronization schemes [10]. For the case of PTP, many overhead lines contain an optical

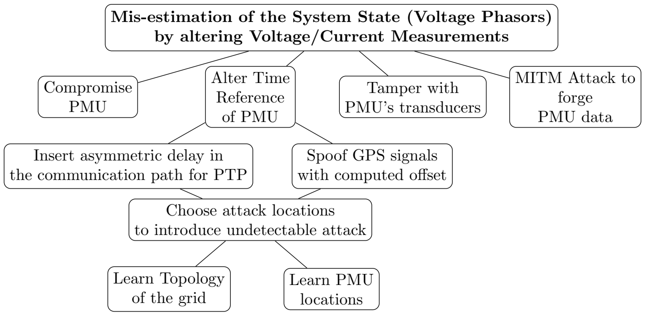

Mis-estimation of the System State (Voltage Phasors)
by altering Voltage/Current Measurements
Compromise PMU
Alter Time Reference of PMU
Tamper with PMU's transducers
MITM Attack to forge PMU data
Insert asymmetric delay in the communication path for PTP
Spoof GPS signals with computed offset
Choose attack locations to introduce undetectable attack
Learn Topology of the grid
Learn PMU locations

Fig. 1. Attack-tree for attacking the time reference of a PMU measurement infrastructure.

fiber with physical layer repeaters placed every few kilometers on the line poles, and it is also common to have unmanned facilities with repeaters. For an attacker it would be sufficient to disconnect a cable and to insert a delay box to attack PTP [18]. In the case of GPS, spoofing GPS transmitters can be built from low-cost components and can be coordinated easily [4], [22].

As a result of the attack, the PMU shifts the time window for which the synchrophasor is computed. Therefore, besides the incorrect estimation of the phase, the attack affects the estimation of the phasor's amplitude, the frequency of its main tone and the ROCOF estimation. As we are considering a transmission network, it follows that the estimation of the phase angle is the one that is most affected by the attack, thus this is the only error we consider in this paper.

IV. Undetectable Time-Synchronization Attacks

In this section, we present a theory of undetectable attacks, which forms the basis for the practical methods presented in the following sections.

A. Absolutely Undetectable Attack

Let p be the number of time references manipulated by the attacker, α_i the i-th phase angle difference between the attacked and the original synchrophasor measurement and $\mathcal{A}_i$ the set of measurement points to which the angle difference α_i is imposed, $i = 1{:}p$.

For all $m \in \mathcal{M}$, define $\Delta z_m = z'_m - z_m$ where z_m is the value of the m^{th} measurement that would be obtained if there would be no attack and z'_m is the value obtained when the timing attack is present. We have:

$$\begin{aligned} \Delta z_m &= z_m(u_i - 1), \text{ if } m \in \mathcal{A}_i \\ \Delta z_m &= 0, \text{ if } m \in \mathcal{M} \setminus \bigcup_i \mathcal{A}_i \\ \text{with } u_i &= \cos\alpha_i + j \sin\alpha_i = e^{j\alpha_i},\ i = 1{:}p. \end{aligned}$$

By the definition of F, an attack that produces a change $\Delta z = (\Delta z_m)_{m=1:M}$ to the true observation vector z is absolutely undetectable if and only if

$$F\Delta z = 0. \tag{3}$$

Let Ψ be the attack-measurement indicator matrix, defined by

$$\Psi_{m,i} = 1 \text{ if } m \in \mathcal{A}_i \text{ and } \Psi_{m,i} = 0 \text{ otherwise,} \tag{4}$$

with $m = 1{:}M$ and $i = 1{:}p$. Then Δz can be re-written as

$$\Delta z = (u_1 - 1) \text{ diag}(z)\Psi_{:,1} + ... + (u_p - 1) \text{ diag}(z)\Psi_{:,p} \tag{5}$$

where $\Psi_{:,i}$ denotes the i-th column of matrix Ψ and diag(z) is the $M \times M$ diagonal matrix with diag$(z)_{m,m} = z_m$. By (3), the attack α is absolutely undetectable if and only if

$$\sum_{i=1}^{p} (u_i - 1)F \text{ diag}(z)\Psi_{:,i} = 0. \tag{6}$$

We can make (6) more tractable by introducing the *attack-angle matrix* W, which is a $p \times p$ hermitian-complex matrix defined as

$$W \triangleq \Psi^T \text{ diag}(z)^\dagger F^\dagger F \text{ diag}(z)\Psi \tag{7}$$

or in other words

$$W_{i,j} = \sum_{l,m,n \in \mathcal{M}} \Psi_{l,i}\Psi_{m,j}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m \tag{8}$$

with $i, j = 1{:}p$. We use $\bar{F}_{n,l}$ to denote the conjugate of $F_{n,l}$. Note that the dimension of the matrix W is $p \times p$, where p is the number of different delays imposed by the attack; it is particularly interesting to use W when p is small.

Theorem 1. *The attack* $\alpha = (\alpha_1, \dots, \alpha_p)$ *is absolutely undetectable if and only if*

$$W(\vec{u} - \vec{1}) = 0 \tag{9}$$

with $\vec{u} = (u_1, ..., u_p)^T, \vec{1} = (1, ..., 1)^T.$

Proof: First recall that the attack is absolutely undetectable if and only if (6) holds. Second, we prove that for any complex vector $y \in \mathbb{C}^p$:

$$Wy = 0 \Leftrightarrow F \text{ diag}(z)\Psi y = 0. \tag{10}$$

The $\Leftarrow$ side of the implication directly follows from the definition of W. Conversely, assume that $Wy = 0$ for some $y \in \mathbb{C}^p$. Then

$$\begin{aligned} &\Psi^T \text{ diag}(z)^\dagger F^\dagger F \text{ diag}(z)\Psi y = 0 \\ &\Rightarrow y^\dagger \Psi^T \text{ diag}(z)^\dagger F^\dagger F \text{ diag}(z)\Psi y = 0 \\ &\Rightarrow \|F \text{ diag}(z)\Psi y\|^2 = 0 \\ &\Rightarrow F \text{ diag}(z)\Psi y = 0. \end{aligned}$$

In the above, $\|\cdot\|$ denotes the ℓ^2 norm, defined for $y \in \mathbb{C}^p$ by $\|y\| = \sqrt{\sum_{i=1}^{p} |y|_i^2}$. □

B. Timing attack with a single delay ($p = 1$)

Consider that the attacker can only induce a single delay, i.e., $p = 1$ and $\alpha = (\alpha_1)$. Then the matrix W is a single complex number $W = (W_{1,1})$, and Theorem 1 becomes

$$W_{1,1}(u_1 - 1) = 0 \tag{11}$$

with $W_{1,1} = \sum_{l,m \in \mathcal{A}_1, n \in \mathcal{M}} \bar{F}_{n,l}F_{n,m}\bar{z}_l z_m$. It is very unlikely that $W_{1,1} = 0$, thus undetectability requires $u_1 = 1$ (i.e. $\alpha_1 = 0$), namely there is is no attack. Thus this case is of no interest.

C. Timing attack with two delays ($p = 2$)

Consider now that the attacker can induce two delays (e.g., with two GPS coverage zones or two different communication paths in a PTP network), i.e., $p = 2$ and $\alpha = (\alpha_1, \alpha_2)$. Observe that for $p = 2$ the matrix W is 2×2, and Theorem 1 becomes

$$\begin{aligned} W_{1,1}(u_1 - 1) + W_{1,2}(u_2 - 1) &= 0 \\ W_{2,1}(u_1 - 1) + W_{2,2}(u_2 - 1) &= 0. \end{aligned}$$

Before we formulate our theorem, we propose the following Lemma.

Lemma 1. *Let $a, b \in \mathbb{C}$. If $a + b \neq 0$ then the solutions of the system of equations*

$$\begin{cases} a(u-1) + b(v-1) = 0 \\ |u| = |v| = 1 \end{cases}$$

with unknowns $u, v \in \mathbb{C}$ are

$$u = v = 1 \textit{ and } u = \frac{\bar{a}(a+b)}{a(\bar{a}+\bar{b})}, \quad v = \frac{\bar{b}(a+b)}{b(\bar{a}+\bar{b})}.$$

If $a + b = 0$, there are infinitely many solutions, given by $u = v, |u| = 1$.

Proof: We can interpret the system of equations as follows. Denote with S^1 the unit circle in the complex plane, i.e., $S^1 = \{u \in \mathbb{C}, |u| = 1\}$. When $u \in S^1$, $z = a(u-1)$ is a point in the circle of center $-a$ and radius $|a|$; similarly, $z = -b(v-1)$ is a generic point in the circle of center b and radius $|b|$. Solutions to the equations are given by the intersection of these two circles, if they intersect. Now they intersect because $u = v = 1$ is a solution. Therefore, there is exactly one other solution, except in the special case where the two circles are tangent or when the two circles are identical.

Further, we can compute the solution in closed form by using standard geometry arguments. □

Theorem 2. *For $p = 2$, if rank$(W) = 1$ there is one non-trivial absolutely undetectable attack vector $\alpha = (\alpha_1, \alpha_2)$, given by*

$$\begin{aligned} &\alpha_1 = 2\arg(W_{1,1} + W_{1,2})(\textit{mod } 2\pi) \\ &\alpha_2 = -2\arg(W_{1,2}) + 2\arg(W_{1,1} + W_{1,2})(\textit{mod } 2\pi) \end{aligned} \tag{12}$$

Proof : With rank$(W) = 1$, the system of equations derived from Theorem 1 is equivalent to

$$W_{1,1}(u_1 - 1) + W_{1,2}(u_2 - 1) = 0 \tag{13}$$

where the unknowns are $u_1, u_2 \in \mathbb{C}$ with the constraints $|u_1| = |u_2| = 1$. This system of equations can be precisely solved by applying Lemma 1 to (13) and obtain a single non-trivial attack, given by

$$\begin{aligned} u_1 &= \frac{W_{1,1} + W_{1,2}}{W_{1,1} + \bar{W}_{1,2}} \\ u_2 &= \frac{\bar{W}_{1,2}(W_{1,1} + W_{1,2})}{W_{1,2}(W_{1,1} + \bar{W}_{1,2})} \end{aligned}$$

from where we derive the attack vector α, using the fact that $W_{1,1}$=$\bar{W}_{1,1}$ because W is hermitian. □

For the case rank$(W) = 2$, there is only one solution $u_1 = u_2 = 1$, i.e., there are no absolutely undetectable attacks.

As we show next, Theorem 2 forms the basis for practical attacks because, even when W is full rank, it can often be well approximated by a rank-1 matrix.

V. Practically undetectable attack with two delays

In this section we describe a strategy for performing a practically undetectable attack when W is full rank and $p = 2$. We assume that each attacking-angle affects a single PMU, i.e., we attack two PMUs in total. In [14] it is shown that attacking at least two PMUs is enough to perform an undetectable attack.

A. Attack based on Rank-1 matrix approximation

Recall that the W matrix is hermitian, thus we can diagonalize W as $W = U\Lambda U^\dagger$, with $UU^\dagger = U^\dagger U = I$ and Λ is a diagonal matrix with real, nonnegative and descending-ordered eigenvalues. Let us construct $\tilde{\Lambda} = \text{diag}\,(\Lambda_{1,1}, 0)$, with $\Lambda_{2,2} = 0$ and we define $\tilde{W} = U\tilde{\Lambda}U^\dagger$, i.e., we replace the smallest eigenvalue by 0. The approximate attack is one that satisfies

$$\tilde{W}(\vec{u} - \vec{1}) = 0, \tag{14}$$

and the attack vector α is then given by (12) with $\tilde{W}$ in lieu of W.

B. The IoS criterion

The effectiveness of using $\tilde{W}$ instead of W depends on the value of $\Lambda_{2,2}$ and whether or not zeroing this value is a good approximation. To investigate this, we use the index of separation (IoS) of the matrix W, which is classically defined as

$$\text{IoS} = \frac{\lambda_{\text{max}}}{\sum_i \lambda_i} = \frac{\Lambda_{1,1}}{\Lambda_{1,1} + \Lambda_{2,2}}. \tag{15}$$

We obtain the two eigenvalues of W as roots of the characteristic polynomial:

$$\begin{aligned} \Lambda_{1,1} &= \frac{1}{2}\left(\text{trace}\,(W) + \sqrt{\text{trace}\,(W)^2 - 4\det(W)}\right) \\ \Lambda_{2,2} &= \text{trace}\,(W) - \Lambda_{1,1} \end{aligned}$$

and using $\Lambda_{1,1}$ and $\Lambda_{2,2}$ in (15) we get

$$\text{IoS} = \frac{1}{2} + \frac{1}{2}\sqrt{1 - 4\frac{\det(W)}{\text{trace}\,(W)^2}}. \tag{16}$$

Note that for an attack with two delays ($p = 2$), IoS$(W) \in [0.5, 1]$ and IoS$(W) = 1 \implies$ rank$(W) = 1$.

An attacker should therefore look for attack locations such that IoS$(W) \approx 1$. In general, for a given choice of locations, IoS(W) depends on the measurement vector z; however, it is possible to avoid this dependency by computing the *minimum index of separation* (IoS*), defined as the minimum value of IoS(W) taken over all values of $z \in \mathbb{C}^M$. If IoS$^* \approx 1$ for a given choice of locations, then the delay attack given by (12) and $\tilde{W}$ in lieu of W is undetectable, regardless of the value of the measurements. The following theorem provides a closed-form expression for IoS*.

Theorem 3. *For an attack with two delays ($p = 2$), and one attacked measurement point per delay ($\mathcal{A}_1 = \{z_1\}$ and $\mathcal{A}_2 = \{z_2\}$), the minimum index of separation (IoS*) is equal to*

$$IoS^* = \frac{1}{2} + \frac{|f_{12}|}{2\,(f_{11}f_{22})^{\frac{1}{2}}} \tag{17}$$

with

$$f_{i,j} = \sum_{l,m}\sum_{n} \Psi_{l,i}\Psi_{m,j}\bar{F}_{n,l}F_{n,m} \tag{18}$$

where Ψ is defined as in (4). Note that IoS* depends only on the measurement matrix H and the location of the attacked PMUs.

Proof: We want to find the minimum of (16). First we need to compute the elements $W_{i,j}$ of W to find $\det(W)$ and $\operatorname{trace}(W)$ as a function of attacked measurements z_1 and z_2. We use (8) with $p = 2$ and one attacked measurement per delay

$$\begin{aligned} W_{1,1} &= \sum_{l,m,n} \Psi_{l,1}\Psi_{m,1}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m = |z_1|^2 f_{11} \\ W_{1,2} &= \sum_{l,m,n} \Psi_{l,1}\Psi_{m,2}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m = \bar{z}_1 z_2 f_{12} \\ W_{2,1} &= \sum_{l,m,n} \Psi_{l,2}\Psi_{m,1}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m = \bar{z}_2 z_1 f_{21} \\ W_{2,2} &= \sum_{l,m,n} \Psi_{l,2}\Psi_{m,2}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m = |z_2|^2 f_{22}. \end{aligned} \tag{19}$$

The trace and determinant of W are given by

$$\begin{aligned} \operatorname{trace}(W) &= |z_1|^2 f_{11} + |z_2|^2 f_{22} \\ \det(W) &= |z_1|^2 f_{11}|z_2|^2 f_{22} - |z_1|^2|z_2|^2 f_{21}f_{12} \\ &= |z_1|^2|z_2|^2\left(f_{11}f_{22} - |f_{12}|^2\right). \end{aligned} \tag{20}$$

Note that $f_{21}f_{12} = |f_{21}|^2 = |f_{12}|^2$. Using (16) and (20) we can express the problem as

$$\min_{z_1,z_2} \quad \frac{1}{2}\sqrt{1 - 4\frac{|z_1|^2|z_2|^2\left(f_{11}f_{22} - |f_{12}|^2\right)}{(|z_1|^2 f_{11} + |z_2|^2 f_{22})^2}}. \tag{21}$$

Note that the objective function can be simplified if we substitute $s = \frac{|z_2|^2}{|z_1|^2}$ in (21), which brings

$$\min_{s} \quad \frac{1}{2}\sqrt{1 - 4\frac{s\left(f_{11}f_{22} - |f_{12}|^2\right)}{(f_{11} + s f_{22})^2}}.$$

By analyzing the sign of the derivative with respect to s we find a minimum when $s = \frac{f_{11}}{f_{22}}$, and substituting this in (16) we obtain the value of IoS* given in the theorem. □

Theorem 3 can be used to find pairs of PMUs that can be attacked undetectably by finding that the corresponding IoS$^* \approx 1$. This is computationally simpler than the algorithms in [14] or [16].

For locations where Theorem 3 does not provide IoS$^* \approx 1$, depending on the operating conditions of the grid, the following result shows than an attacker could still find alternative attack locations to produce an undetectable attack.

Theorem 4. *For an attack with two delays ($p = 2$) , one attacked measurement per delay ($\mathcal{A}_1 = \{z_1\}$ and $\mathcal{A}_2 = \{z_2\}$), and $\operatorname{rank}(W) = 2$, there is still a possibility of performing a practically undetectable attack if the ratio between the magnitude of the attacked measurements is either very small or very large.*

Proof: By analyzing (16), it follows that IoS$(W) \approx 1$ if and only if IoS$(W) \approx 1 \Leftrightarrow \operatorname{trace}(W)^2 >> \det(W)$. By using (20) we can express the inequality as

$$\begin{aligned} &\left(|z_1|^2 f_{11} + |z_2|^2 f_{22}\right)^2 >> |z_1|^2|z_2|^2\left(f_{11}f_{22} - |f_{21}|^2\right) \\ &\left(\frac{|z_1|}{|z_2|}f_{11} + \frac{|z_2|}{|z_1|}f_{22}\right)^2 >> \left(f_{11}f_{22} - |f_{21}|^2\right). \end{aligned} \tag{22}$$

Define $d = \frac{|z_2|}{|z_1|}, d \geq 0, d \in \mathbb{R}$; substituting d in (22)

$$\left(\frac{1}{d}f_{11} + d f_{22}\right)^2 >> \left(f_{11}f_{22} - |f_{21}|^2\right) \tag{23}$$

If we take the left-handside of (23) and plot it as a function of d, we can observe that it has a quadratic behavior with minimum in $d^* = (f_{11}/f_{22})^{\frac{1}{2}}$ and expands to $+\infty$, both when $d \to 0$ and when $d \to +\infty$, i.e., if the ratio between the magnitude of the attacked measurements is either very small or very large. □

In summary, an attacker can compute IoS* for arbitrary pairs of locations; this requires only the knowledge of H. If he finds location pairs with IoS$^* \approx 1$, he has obtained candidate locations where an undetectable attack is possible; he can then test the effect of such attacks. If, in contrast, there is no location with IoS$^* \approx 1$, the attacker can rely on Theorem 4 to assess the candidate measurements to be attacked, and pick two measurements with smallest or largest magnitude ratio.

VI. Practically undetectable attack with more than two delays ($p > 2$)

In this section we consider the problem of computing attacks with more than two delays, i.e., finding a solution to the problem in Theorem 1 for $p > 2$. In what follows, we show how to combine attacks against two delays ($p = 2$) to obtain an attack against $p > 2$ delays.

A. Combining Attacks on Disjoint Pairs of PMUs

As a first step, we consider that there is a set of disjoint PMU pairs ($p = 2$) that can be attacked using the algorithm proposed in Theorem 2, i.e., pairs of PMUs for which the IoS is close to 1. In what follows we show that even though an attack modifies the apparent measurements (and the apparent system state), when the attacked pairs of PMUs are disjoint, the attacks can be computed independently in parallel.

Theorem 5. *Consider a collection of K attacks, and let $\mathcal{A}_i^{(k)}$ be the set of measurements affected by the i^{th} angle of the k^{th} attack. Let z_m be the m^{th} measurement value when no attack is performed and let $W^{(k)}$ be the matrix given by (7) when it is only attack k that is performed. Then*

(i) the matrix $W^{(k)}$ depends only on the values z_m for $m \in \cup_i \mathcal{A}_i^{(k)}$.

Assume furthermore that the sets $\mathcal{A}_i^{(k)}$ are disjoint, i.e. any measurement point appears in some $\mathcal{A}_i^{(k)}$ for at most one k and at most one i. Then

(ii) if each attack k is absolutely undetectable if performed on its own, then so is any combination of the attacks, performed sequentially or simultaneously.

Proof: By (8),

$$\begin{aligned} W_{i,j}^{(k)} &= \sum_{\ell,m\in\mathcal{M}} \bar{z}_\ell z_m \mathbb{1}_{\{\ell\in\mathcal{A}_i^{(k)}\}} \mathbb{1}_{\{m\in\mathcal{A}_j^{(k)}\}} g_{\ell,m} \\ &= \sum_{\ell\in\mathcal{A}_i^{(k)}} \sum_{m\in\mathcal{A}_j^{(k)}} \bar{z}_\ell z_m g_{\ell,m} \end{aligned}$$

with $g_{\ell,m} = \sum_n \bar{F}_{n,\ell} F_{n,m}$. Note that $g_{\ell,m}$ depends only on the verification matrix F and is thus independent of the measurements and of the attack. Statement (i) follows.

Now assume that the attacked sets of measurements $\mathcal{A}^{(k)} = \cup_i \mathcal{A}_i^{(k)}$ are disjoint. The matrix $W^{(k)}$ for attack k depends only on the values of z_m for $m \in \mathcal{A}^{(k)}$. An attack $k' \neq k$ affects only the measurement sites in $\mathcal{A}^{(k')}$ and $\mathcal{A}^{(k')} \cap \mathcal{A}^{(k)} = \emptyset$ therefore for $m \in \mathcal{A}^{(k)}$, the values of z_m remain the same before or after after attack k'. Therefore $W^{(k)}$ also remains the same before and after attack k' is performed. □

The above result implies that for a set of disjoint PMU pairs with IoS ≈ 1 a practically undetectable attack can be performed by attacking each pair of PMUs simultaneously with the angles given by (12).

B. Combining Attacks on Overlapping Pairs

Let us now consider attacks on overlapping pairs of PMUs. Unfortunately, we cannot apply the previous result because the W matrix of an attack now may depend on the apparent measurement values due to another, overlapping attack. However, as we show next, it is possible to combine attacks *sequentially*, provided that the effect of the previous attack in the sequence is accounted for.

Theorem 6. *Consider a sequence of $k = 1{:}K$ attacks, computed one after the other. The pairs of PMUs attacked may be overlapping. Let $z_m^{(0)} = z_m$ be the true value of measurement m, and $z_m^{(k)}$ the apparent value after the kth attack. Let attack k be constructed so as to be absolutely undetectable assuming that the measurements are $z_m^{(k-1)}$. Then the combination of the K attacks is absolutely undetectable.*

Proof: Note that by assumption the kth attack, resulting in $z^{(k)}$, is undetectable, i.e., by (3) it satisfies

$$F\left(z^{(k)} - z^{(k-1)}\right) = 0$$

where F is the verification matrix, which is independent of the measurements. Summing all these equations for $k = 1{:}K$ gives:

$$F\left(z^{(K)} - z^{(0)}\right) = 0$$

which shows that the combination is undetectable. □

The theorem implies that if a sequence of attacks on pairs of PMUs is practically undetectable, then so is their combination. One may think that it is difficult to predict, in the general case, whether a sequence of attacks is practically undetectable, since the undetectability condition (IoS$^{(k)} \approx 1$) depends on the matrix $W^{(k)}$ which itself depends on the result of the previous attack. As we show next, this is not the case, as the IoS of a pair of PMUs does not change due to an attack against a subset of those PMUs.

Theorem 7. *Consider a pair of PMUs, with matrix W given by (8) derived using the original measurements z. Assume that an attack is performed that affects a subset of this pair of PMUs, producing an apparent measurement z'. Let W' be the matrix given by (8) computed using the apparent measurements z'. Then IoS(W) = IoS(W').*

Proof: Observe that by (15) and (20), IoS(W) depends only on the modulus of the complex measurements z_m. Since an attack modifies only the angle of the measurements, the modulus are unchanged, and so is IoS(W). □

The practical implication of the above results is that an attacker can identify an arbitrary set of pairs of PMUS with IoS ≈ 1 based on the true measurement values, or a set of pairs of PMUs with IoS$^* \approx 1$. The attacker can then take an arbitrary sequence of these PMU pairs, computes the angles of the kth attack using (12) and with matrix $W^{(k)}$ updated to account for the effect of the preceding $k-1$ attacks in the sequence, and this way the attacker obtains an undetectable attack. In the example studied in Section VII we consider a case where 10 pairs of PMUs have IoS$^* \approx 1$, and we found that, in general, every sequence of attacks gives a different set of attack angles.

A special case of interest is if we repeatedly attack a particular pair of PMUs (that has IoS ≈ 1). The effect of doing so is that the second attack restores the original measurement, i.e., it undoes the first attack. To see why, let z be the original measurement value, $z^{(1)}$ the apparent measurement after the first attack and $z^{(2)}$ the apparent measurement after the second attack (computed using the updated matrix $W^{(1)}$). We have $z^{(2)} \neq z^{(1)}$ by construction of the second attack. By Theorems 6 and 7, the sequential combination is an undetectable attack on z, which has produced an apparent measurement $z^{(2)}$. Nonetheless, by Theorem 1 there is only one non trivial undetectable attack, therefore $z^{(2)} = z$.

C. A Greedy Heuristic

In the previous subsections we have shown how to find a potentially very large number of undetectable attacks. In this section we propose a greedy heuristic for computing an attack that aims at optimizing a certain attacker objective [23].

We assume that the attacker has an objective that it wants to maximize; for example she might want to to underestimate the apparent-power flow of a transmission line (with the potential consequence of burning it). The attacker has access to the admittance matrix Y, the PMU measurement type and locations and the measurement vector z. The attacker's goal is to mount an undetectable delay attack that induces a forged measurement vector z' that maximizes the attacker's objective, say $J(z')$.

A greedy algorithm for achieving this objective is as follows.

1) Establish a list $\mathcal{L}$ of pairs of PMUs that have IoS ≈ 1 given the measurement vector z. Alternatively, the list $\mathcal{L}$ can be computed using IoS* ≈ 1, in which case it is independent of the measurement z.
2) Let $z^{(0)} = z$ and $k = 0$
3) $k = k+1$. Find the pair $j_k \in \mathcal{L}$ that maximizes $J(z^{(k)})$ where $z^{(k)}$ is the forged measurement obtained after applying the attack to the pair j_k and to the measurement $z^{(k-1)}$
4) If $k < KMAX$ and $J(z^{(k)}) - J(z^{(k-1)}) > \varepsilon$ goto 3) else exit and output $j_1, j_2, ...$

In other words, the algorithm finds at every step, among all the computed attacks, the one that gives the largest damage. It then updates the measurement vector z based on the attack, and continues until no new attack can increase the damage line. The attack to be mounted is then given by the sequence of pairs of PMUs $j_1, j_2, ...$. By the theorems in the previous section, this combined attack is practically undetectable. In Section VII-C we provide numerical results for testing undetectability of the resulting attack, and in Section VII-D we compare the apparent-power flow mis-estimation obtained by this method versus an undetectable attack on a single pair of PMUs.

VII. Performance evaluation

In this section we illustrate how the previously presented attack method can be applied to the IEEE 39-bus system, a benchmark for power transmission grids [24]. We show in particular how the computation of IoS* can be used to easily find attack locations. We also demonstrate that the attacks are non detectable by bad-data detection methods based on residuals.

The performance evaluation was entirely done in MATLAB 2015b-64 bit, on a PC with Intel$^{®}$ core i7-5500U, 2.40GHz and 8 Gb of RAM. The procedure consisted in:

1) Every 20 ms, a load flow is computed in order to determine the true state of the network;
2) The synthetic measurements forwarded to the state estimator are obtained by perturbing the true quantities inferred from the previous step with randomly-generated Gaussian noise characterized by the cumulated standard deviation of the PMUs and their sensors. We assumed to use class-P PMUs;
3) Computation of the attack vector according to the method described in the paper;
4) WLS estimation;
5) WLS estimation with attacked measurements;
6) Comparison of the detectability for step 5 with respect to step 4;
7) Comparison of estimated power flows for steps 4 and 5.

The computational cost of the attack is compatible with the delays involved in a typical PMU-measurement flow. For instance, with the adopted software and hardware, an attacker needs an average of 0.4 ms with a max of 1.3 ms over a 300 s attack window to compute the attack vector when $p = 2$.

A. Analysis of Residuals

In this section we describe how residuals are analyzed with standard methods. Residuals are relative to the estimation method used, which in practice is often WLS [7], [25].

WLS cannot be expressed easily using complex matrix operations as we use in Section III, because the measurement errors cannot be assumed to have circular symmetry, as we discuss later. This is why in this section we have to introduce a slightly different formalism than in Section III.

The error covariance matrix R is defined as

$$R = \mathbb{E}\left(ee^{\dagger}\right) \tag{24}$$

where e is the measurement error vector from (1), assumed to be Gaussian. Note that if PMU errors in polar coordinates are relatively small, their projection in rectangular coordinates result into a Gaussian distribution [26], [27]. R is a complex hermitian matrix, namely $R^{\dagger} = R$. In order to work with rectangular coordinates, we need to move from $R \in \mathbb{C}^{M \times M}$ to a matrix $R' \in \mathbb{R}^{2M \times 2M}$. Let $e = a + jb \in \mathbb{C}^{M}$ and define $e' = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^{2M}$. Then, using the same expression as in (24) it follows that

$$R' = \mathbb{E}\left(e'e'^{T}\right) = \begin{pmatrix} R_{aa} & R_{ab} \\ R_{ba} & R_{bb} \end{pmatrix}$$

Note that $R_{aa}, R_{bb} \in \mathbb{R}^{M \times M}$ are diagonal matrices. Assume now that the measurement error e' can be modeled as independent Gaussian noise, then $R_{ab} = R_{ba} = 0$. The hypothesis of independent measurement errors is properly justified, based on the following considerations:

- measurement values obtained by different devices can be reasonably considered independent (e.g., [28]);
- we only use PMUs, i.e., no typical measurements are used (e.g., power flows, power injections) or historical data;
- voltage and current amplitude measurements taken by the same PMU can usually be considered uncorrelated [28];
- in [28] it is confirmed that neglecting PMU correlations (both in amplitude and phase) in the estimator model, does not lead to a significant decrease of the SE quality;
- based on the nomenclature and definitions given in [29], we use only *independent Gaussian-distributed measured data* and not *processed dependent measurements*;
- A unique sensor per measured quantity (i.e., voltage / current) is used and the cross-talk interference is negligible.

In view of the above, R' is diagonal and can be expressed as

$$R' = \begin{pmatrix} R_{aa} & 0 \\ 0 & R_{bb} \end{pmatrix} = \text{diag}(\sigma^2_{e'_1}, \ldots, \sigma^2_{e'_{2M}}) \tag{25}$$

where $\sigma_{e'_m}$ $(m = 1, \ldots, 2M)$ is the standard deviation of the mth measured quantity. (Note that if we would have $R_{bb} = R_{aa}$, then e would have circular symmetry and we could do least square estimation in complex numbers, but such an assumption cannot usually be made.)

Let us rewrite the system state as $x' \in \mathbb{R}^{2N}$

$$x' = [V_{1,re}, \ldots, V_{N,re}, V_{1,im}, \ldots, V_{N,im}]^{T} \tag{26}$$

where $V_{n,re}$ and $V_{n,im}$ are the 1-ph real and imaginary parts of the voltage phasor at bus n (n = $1, \ldots, N$), respectively. The corresponding measurement set becomes $z' \in \mathbb{R}^{2M}$.

The estimated state becomes:

$$\hat{x}' = (H'^T DH')^{-1} H'^T Dz' = G^{-1} H'^T Dz' \tag{27}$$

where $H' \in \mathbb{R}^{2M \times 2N}$ and $D = \mathrm{diag}(1/R')$.

We can compute the estimated measurements based on the estimated state as $\hat{z}' = H'\hat{x}'$, which can be used for computing the measurement residual $r = \hat{z}' - z'$. Measurement residuals are distributed as $r \sim N(0, \Omega)$ [25], where Ω is defined as

$$\begin{aligned} \Omega = SR' = (I - K)R' = (I - H'G^{-1}H'^T R'^{-1})R' \\ = R' - H'G^{-1}H'^T. \end{aligned} \tag{28}$$

This can be used to define the *normalized* residual for measurement m as

$$r_m^N = \frac{r_m}{\sqrt{\Omega_{m,m}}} \sim N(0,1) \tag{29}$$

Well-known BDD methods (e.g., χ^2-test, largest normalized residual test (LNR) [25], [30], [31]) take advantage of the standard distribution of the normalized residuals to detect the presence of BD. The χ^2-test exploits the property that the sum of normally-distributed random variables is a variable with a χ^2 distribution and a certain number of degrees of freedom. If the sum of the residuals does not respect this distribution with a certain confidence level, one or more measurements in the data set are not normal, therefore the existence of one of more corrupted measurements is suspected.
The LNR test is another method that exploits the distribution of the normalized residuals. The largest residual among those that are above a certain threshold (set usually equal to 3 standard deviations) is marked as potential BD and removed from the data set.

Recall that the undetectable attack is structured such that the distribution of the residuals, and their values after the attack, remain unchanged when compared with the values obtained without the attack. Hence, all the detection methods based on the normality of the residuals are expected to fail in identifying the attack. This is shown numerically in section VII-C.

B. Electrical model

The IEEE 39-bus system is shown in Fig.2. We assume Bus #31 as the connection point to the external grid with a short-circuit power of S_{sc} = 50 GVA. The ratio between the real and imaginary parts of the short-circuit impedance is R_{sc}/X_{sc} = 0, as usually assumed for transmission networks. We assume the network has 13 PMUs that measure voltage and injected-current phasors and 8 PMUs that measure injected-current phasors only, for a total of 21 PMUs installed. Network observability (i.e., matrix H of full rank [32]) is the only criterion followed when selecting measurement type (i.e., nodal voltage and injected-current phasors v.s. injected-current phasors only) and PMU locations. These PMU locations, their measurement type, together with the presence of 12 zero-injection buses[1], are sufficient conditions to guarantee the observability of the system state. Note that other combination of PMU locations and measurement type would affect the verification matrix F and all the quantities computed from it such as the attack-angle matrix W and the minimum index of separation IoS* defined in equations (7) and (17), respectively. In summary, this would mean different attack-location as the ones showed in this analysis.

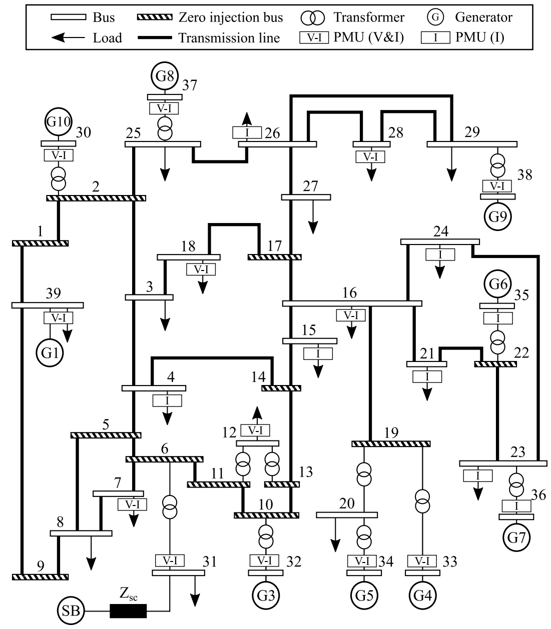


Fig. 2. Benchmark IEEE 39-bus transmission system and PMU locations.

PMU measurements are generated by adding a white Gaussian noise to the amplitude and phase of the ideal phasors obtained by running a load flow. The standard deviation of the measurements is compatible with class 0.1 voltage and current sensors as described in [33]–[35].

The load profiles are obtained from real measurements taken at 50 frames-per-second by real PMUs installed in the 125-kV sub-transmission network of Lausanne, Switzerland. For this reason, the load profiles present time-domain behavior typical of transmission networks. This sub-transmission network is constituted by five 3-ph loads. In order to obtain values for the 19 1-ph equivalent loads available in the IEEE 39-bus system, some of the load profiles have been replicated. It is worth mentioning that the load profiles are then adapted to match the values provided in [24]. Moreover, as we do not use the transformer tap changers, the power at three selected buses (#7, #8 and #12) is adapted so that, in all the buses, the voltage stays within the ± 5% range of the rated voltage. In order to verify the effectiveness of the attack during non-steady-state conditions of the grid, we use a time window in which a sudden reactive power drop takes place at Bus #4 (see Fig. 3).

C. Results for undetectability and attacking methods

We applied Theorem 3 to all possible combinations of attack locations, with $p = 2$, one measurement per delay, and taking PMUs that measure only injected currents. Table I shows the results for the IoS* at each location pair, where any pair that has an IoS* = 1, will allow an undetectable attack.

To demonstrate the undetectability of an attack at a pair of PMUs where IoS* $= 1$, we perform the χ^2-test for BD

[1] A zero-injection bus is defined as a bus where no load or generation is connected therefore this information can be exploited as a so-called virtual measurement.

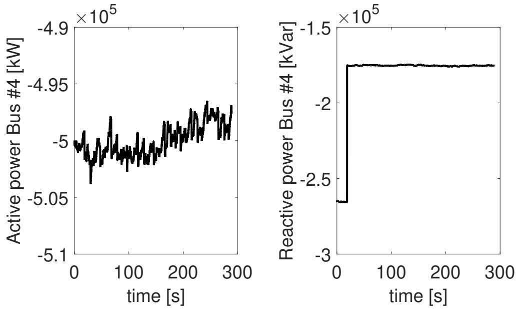


Fig. 3. Reactive power drop in Bus #4.

TABLE I. IoS* for all the two-delays attack combinations for buses with current measurements only in Fig. 2.

Bus1	Bus2	IoS*	Bus1	Bus2	IoS*
4	15	0.8437	21	24	1.0000
4	21	0.6613	21	26	0.8395
4	23	0.6613	21	35	1.0000
4	24	0.6613	21	36	1.0000
4	26	0.5282	23	24	1.0000
4	35	0.6613	23	26	0.8395
4	36	0.6613	23	35	1.0000
15	21	0.9516	23	36	1.0000
15	23	0.9516	24	26	0.8395
15	24	0.9516	24	35	1.0000
15	26	0.7669	24	36	1.0000
15	35	0.9516	26	35	0.8395
15	36	0.9516	26	36	0.8395
21	23	1.0000	35	36	1.0000

in the non-attacked and attacked scenarios with a detection confidence of 99%, and we confirm the results by performing the LNR test in the same scenarios. Both tests were executed using the approach described in [25]. We attack the pair of Buses [#21, #36] as a representative of an attack where $\text{IoS}^* = 1$; we use the pair [#4, #26], as it has the lowest IoS^*, as a basis for comparison.

Fig. 4 shows the p-values of the χ^2-test. At the top of Fig. 4 we observe that the p-values of the χ^2-test for the pair of Buses [#21, #36] are not modified by the attack, making the attack undetectable. In the bottom of Fig. 4, we show result for the pair [#4, #26], and the p-values for non-attacked and attacked scenarios are largely different, meaning that the χ^2-test detects the attack.

In Fig. 5 we show the LNR-test results for the attacks shown in Fig. 4. For each pair of PMUs, we plot $\text{LNR} = \max_m |r_m^N|$, with r_m^N given by (29) and $m = 1 : M$. The dotted line shows the threshold corresponding to a confidence of 99.73%, which maps to a 3σ deviation for a single measurement. It can be seen that when attacking the undetectable location pair (top), the normalized residuals are invariant. Conversely, if we attack the second location pair (bottom), the majority of the LNRs are above the identification threshold making the attack easily detectable. Note that the reactive power drop in Fig. 3 has no effect on the LNR after the attack, when the attack location has an $\text{IoS}^* = 1$. This behavior holds under any transient.

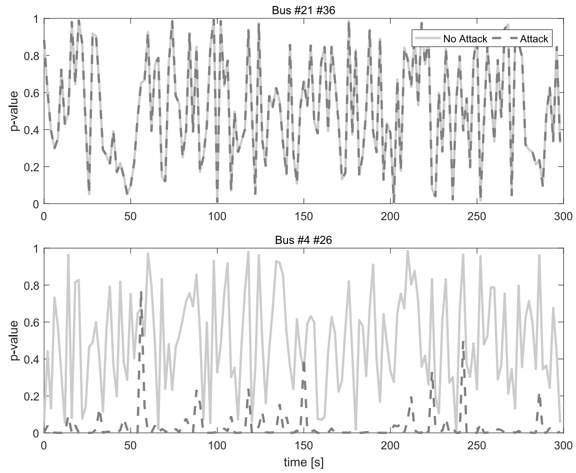


Fig. 4. Comparison of p-values for the χ^2-test applied to two attack locations.

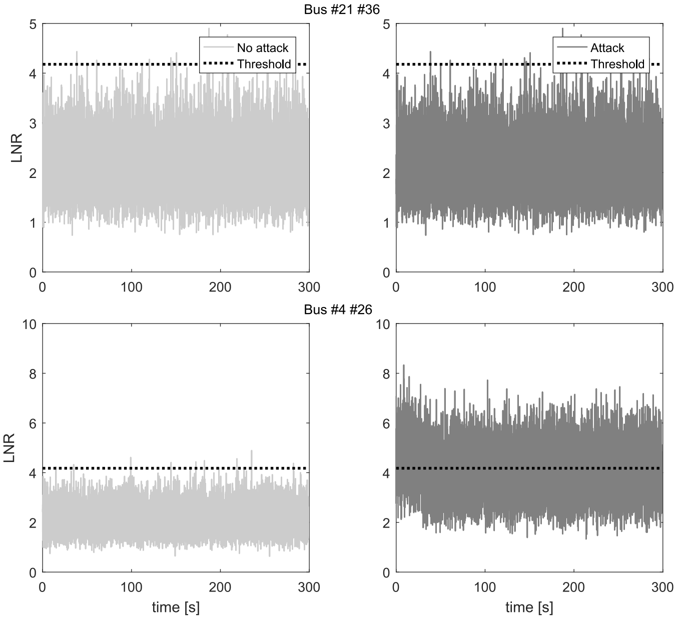


Fig. 5. LNR test applied to two different attack locations for the no-attack and attack scenarios.

To numerically illustrate Theorem 4, in Fig. 6 we show the LNR-test results for buses [#26, #35], which have an $\text{IoS}^* = 0.8395$, for a case when the magnitude of the measurement in Bus #35 is 9 times larger than that in Bus #26. The figure shows the LNR-test results before and after the attack, and shows that the attack remains undetectable despite the fact that $\text{IoS}^* < 1$.

To illustrate Theorem 5, we show results for $p = 6$, for the disjoint PMU pairs [#21, #36], [#26, #35] and [#23, #24] for which either $\text{IoS}^* = 1$ (first and third pairs), or Theorem 4 can be applied (second pair). The attack is performed in parallel, and Fig. 7 shows the results of the LNR-test, comparing attacked and non-attacked measurements. We can observe again that the results are statistically indistinsguishable from the non-attacked case.

Finally, we used the greedy algorithm described in Section VI-C with the objective of under-estimating the apparent power flow for the line between Buses #16 and #24. The algorithm found the maximum underestimation with $p = 10$, attacking pairs [#21, #36], [#23, #24], [#24, #35], [#23, #36], [#21, #23]. We can see the LNR-test applied to the

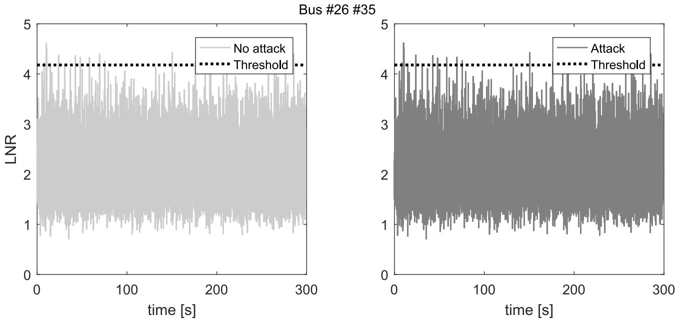


Fig. 6. Undetectability of a pair of PMUs that have large measurement-magnitude ratio, with IoS < 1.

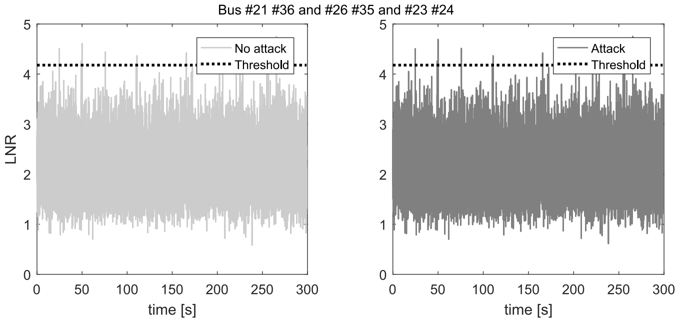


Fig. 7. LNR-test applied to an attack on three disjoint pairs ($p = 6$), following the method described in Theorem 5.

measurements before and after the attack in Fig. 8, which shows that the sequential attack on pairs of PMUs that give an undetectable attack, is also undetectable.

D. Results on power-flows mis-estimation

To illustrate the potential impact of time synchronization attacks, we show results for an attack against a pair of PMUs (i.e., [#21, #36]), which leads to over- and under-estimation of power flows in the power system. The attack angles computed are $\alpha_1 = 1.14$ rad for Bus #21 and $\alpha_2 = 0.57$ rad for Bus #36, and they increased of 0.02 rad after the reactive power drop.

We applied the same random numbers for generating the measurement noise to the scenarios with and without attack, ensuring that any difference in the state-estimation results is only due to the attack.

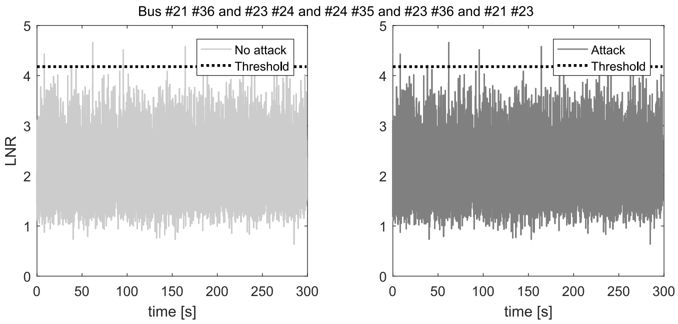


Fig. 8. LNR-test on a sequential attack with $p = 10$, using the greedy algorithm strategy.

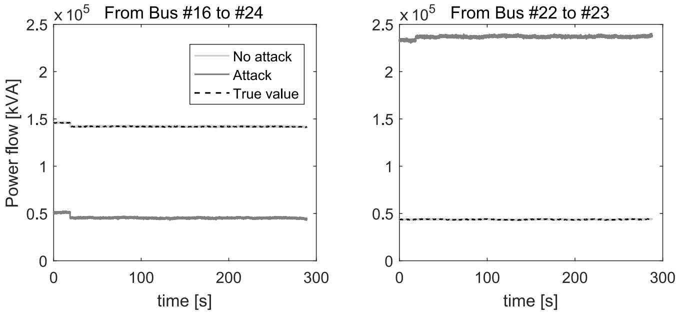


Fig. 9. Comparison of the true apparent-power flow in two lines and the estimated apparent-power flow for the no-attack and attack scenarios.

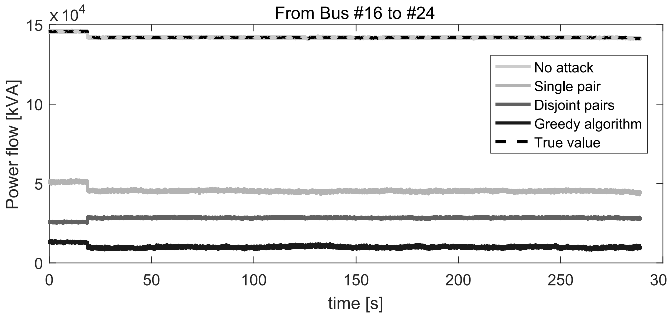


Fig. 10. Comparison of the under-estimated power flow in a transmission line, for different attack scenarios.

The attack worsens the estimated voltages, hence all the inferred quantities from there are affected (e.g., injected currents, current flows, active and reactive powers, etc.), with errors going above 500 %, as shown in the right side of Fig. 9. In this case, the system operator believes that the power flowing in the line between Buses #22 and #23 is much higher than it really is, therefore the system operator could decide to shed some loads or to reconfigure the network when this is not necessary. On the contrary, in the left side of Fig. 9, the system operator under-estimates the power flowing in the line between Buses #16 and #24 thus exposing the line to power flows larger than those it is designed for (in all the cases where the true power flow is close to the line's ampacity limit).

Fig. 10 compares the under-estimation of the apparent-power flow on the line between Buses #16 and #24 obtained by different attacks. We compare (i) the attack on a single pair of PMUs (i.e., [#21, #36]); (ii) the attack on disjoint pairs of PMUs described in Theorem 5 and (iii) the heuristic greedy algorithm described in Section VI-C. Although we see that adding extra pairs appears to increase the impact of the attack, the assertion does not always hold (e.g., attacking twice the same pair of PMUs cancels the attack, as mentioned before). In general, it is the attacker that, by knowing the IoS* criterion, can build a strategy to best achieve its objective.

VIII. Discussion

A. Countermeasures to avoid the attacks

The methodology of the attack presented here does not have any influence on the value of the residuals, hence the BD cannot be identified and removed from the measurement set by applying the classic BDD algorithms. A possible defense approach is discussed in [36], where the authors propose strategies to maintain integrity of measurements, and describe a bad-data detection technique based on a comparison between measurements from PMUs and measurements from SCADA (from other remote terminal units (RTUs)). Notwithstanding, the differences between both types of measurements could make ineffective the use of SCADA measurements to validate the integrity of PMU measurements. Typical SCADA measurements are available every 4 seconds and are not time synchronized, while PMUs can provide 50 or 60 synchrophasors per second.

Successful countermeasures capable to identify the GPS spoofing need to be implemented at the device (PMU) level. The recent literature has discussed potential countermeasures using this approach. Additional features need to be added in the GPS controller embedded in the PMU to detect, and eventually mitigate, the GPS spoofing. As listed in [37], reference [38] has discussed these techniques that can be clustered as follows:

- detect changes of power-related parameters of the GPS hardware (e.g., carrier-to-noise density ratio, absolute received signal power, power variations, etc);
- observe time-related parameters of the GPS receiver like the length of interval between phase transitions, the delay between signals transmitted on different frequencies;
- analyse multiple signals with the same direction of arrival using multi-antenna receivers;
- add secondary sources of time synchronization like, for instance, precision time protocol (PTP).

Note that the attacks presented in the paper require knowledge of the measurement vector, thus integrity or authentication mechanisms are not sufficient for mitigation. Given the impact of the attacks, and how simple and useful the IoS* criterion is, we strongly suggest that confidentiality of PMU measurements be mandated by the standards.

B. Timing attacks under clock-drift conditions

The clock of any PMU has an internal oscillator that is controlled by a clock-servo. A clock-servo is a filter that prevents the clock from making abrupt changes in time and has a stiffness that depends on the manufacturer. The described attacks in the paper could cause a change in time which could produce an alarm in the clock-servo, making the attack detectable. Taking the clock-servo described in [39] as an example, the total attack's time-adjustment would require to be divided in "chunks" of $5\mu s/s$ to avoid an overfeeding to the clock-servo that could trigger an alarm. Further research in this direction could consider proposing an optimal attack with a constraint in the derivative of the attack-angle calculation of the form $|\alpha_i(t+\Delta t) - \alpha_i(t)| \leq \eta_{att}$ with Δt being the refresh rate of PMU measurements and η_{att} the maximum incremental step in time to avoid a clock-servo alarm.

IX. Conclusions

We show that, by manipulating the time reference of one pair of PMUs, it is possible to perform undetectable attacks in PMU-based linear state estimators. We introduce a criterion to find location pairs where the attack is undetectable and provide a closed-form expression to compute the attack angles. We also provide an additional criterion to identify attackable locations regardless of the measurement values. We mount attacks with more than two delays and show that attacks on disjoint pairs can be superimposed such that the attack is executed in parallel. Furthermore, we show how combined sequentially attacks are possible and can be used with a greedy algorithm in order to damage transmission lines. We also show that when performing a sequence of attacks, it is possible to know whether each attack in the sequence will be undetectable before computing the attack. Finally, we use simulations to verify the attacks and to demonstrate their efficacy.

References

[1] "IEEE standard for synchrophasor measurements for power systems," *IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*, pp. 1–61, Dec 2011.

[2] A. Phadke, "Synchronized phasor measurements in power systems," *IEEE Computer Applications in Power*, vol. 6, no. 2, pp. 10–15, April 1993.

[3] "IEEE standard for a precision clock synchronization protocol for networked measurement and control systems," *IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002)*, pp. 1–269, July 2008.

[4] 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.

[5] Q. Yang, D. An, and W. Yu, "On time desynchronization attack against IEEE 1588 protocol in power grid systems," in *IEEE Energytech 2013*, May 2013.

[6] N. Freris, S. Graham, and P. Kumar, "Fundamental limits on synchronizing clocks over networks," *IEEE Transactions on Automatic Control*, vol. 56, no. 6, pp. 1352–1364, June 2011.

[7] 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. PP, no. 99, pp. 1–8, 2016.

[8] 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 Transactions on Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov 2015.

[9] S. Mousavian, J. Valenzuela, and J. Wang, "A probabilistic risk mitigation model for cyber-attacks to pmu networks," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 156–165, Jan 2015.

[10] 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.

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

[12] 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.

[13] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures;," in *IEEE International Conference on Smart Grid Communications (SmartGridComm), 2011*, Oct 2011, pp. 232–237.

[14] 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.

[15] 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.

[16] 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.

[17] I. Shames, A. M. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica*, vol. 47, no. 12, pp. 2757 – 2764, 2011.

[18] 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.

[19] M. Baran and A. Kelley, “A branch-current-based state estimation method for distribution systems,” *IEEE Transactions on Power Systems*, vol. 10, no. 1, Feb 1995.

[20] M. Pau, P. Pegoraro, and S. Sulis, “WLS distribution system state estimator based on voltages or branch-currents: Accuracy and performance comparison,” in *2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, May 2013, pp. 493–498.

[21] I. TC57, “IEC 61850: Communication networks and systems for power utility automation,” *International Electrotechnical Commission Std*, 2015.

[22] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. OHanlon, and P. M. Kintner Jr, “Assessing the spoofing threat: Development of a portable GPS civilian spoofer,” in *Proceedings of the ION GNSS international technical meeting of the satellite division*, vol. 55, 2008, p. 56.

[23] T. H. Cormen, C. Stein, R. L. Rivest, and C. E. Leiserson, *Introduction to Algorithms*, 2nd ed. McGraw-Hill Higher Education, 2001.

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

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

[26] S. Sarri, “Methods and Performance Assessment of PMU-based Real-Time State Estimation of Active Distribution Networks,” Ph.D. dissertation, STI, Lausanne, 2016.

[27] D. Lerro and Y. Bar-Shalom, “Tracking with debiased consistent converted measurements versus ekf,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 29, no. 3, pp. 1015–1022, Jul 1993.

[28] C. Muscas, M. Pau, P. Pegoraro, and S. Sulis, “Effects of measurements and pseudomeasurements correlation in distribution system state estimation,” *IEEE Transactions on Instrumentation and Measurement*, vol. 63, no. 12, pp. 2813–2823, 2014.

[29] E. Caro, A. J. Conejo, and R. Minguez, “Power system state estimation considering measurement dependencies,” *IEEE Transactions on Power Systems*, vol. 4, no. 24, pp. 1875–1885, 2009.

[30] A. Monticelli, “Electric power system state estimation,” *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, Feb 2000.

[31] J. Grainger and W. Stevenson, *Power system analysis*. McGraw-Hill New York, 1994, vol. 152.

[32] N. M. Manousakis, G. N. Korres, and P. S. Georgilakis, “Taxonomy of PMU placement methodologies,” *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 1070–1077, 2012.

[33] “Instrument transformers - Part 1: General Requirements,” *IEC Standard 61869-1*, 2007.

[34] “Instrument transformers - Part 2: Additional Requirements for current transformers,” *IEC Standard 61869-2*, 2012.

[35] “Instrument transformers - Part 3: Additional Requirements for inductive voltage transformers,” *IEC Standard 61869-3*, 2011.

[36] J. Zhang and A. D. Domnguez-Garca, “On the failure of power system automatic generation control due to measurement noise,” in *2014 IEEE PES General Meeting & Conference Exposition*, July 2014, pp. 1–5.

[37] J. Magiera and R. Katulski, “Accuracy of differential phase delay estimation for gps spoofing detection,” in *2013 36th International Conference on Telecommunications and Signal Processing (TSP)*, July 2013, pp. 695–699.

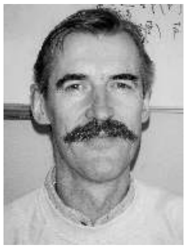
[38] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle., “GPS vulnerability to spoofing threats and a review of antispoofing techniques,” *International Journal of Navigation and Observation*, vol. 2012, no. 127072, 2012.

[39] D. L. Mills and P.-H. Kamp, “The nanokernel,” in *Proceedings of the Precision Time and Time Interval (PTTI) Applications and Planning Meeting*, 2000.

Sergio Barreto is a doctoral researcher in the Laboratory of Communications and Applications 2 at EPFL. In 2002, he graduated from the Monterrey Institute of Technology at Mexico City, where he received his B.Sc (Hons.) in electronics and communications engineering. Among his industry certifications, he holds the Certified Information Systems Security Professional by the ISC^2 and Cisco Certified Security Professional by Cisco. In 2004 he co-founded a service-integration Cisco-partner company in Mexico, where he worked for 10 years in designing, implementing and troubleshooting voice, security and wireless solutions for different markets, such as financial, energy, education and health. He was also head of the R&D team, where he developped and customized Cisco solutions for the mexican market. His research interests include secure time synchronization, machine learning applied to deep-packet inspection and cyber-security for the Internet of Things with particular focus in smart grids.

Marco Pignati (M’13) received the B.Sc. and M.Sc. degrees (Hons.) in electrical engineering from the University of Bologna, Italy, in 2009 and 2012, respectively. He is currently pursuing the Ph.D. degree with the Distributed Electrical System Laboratory, Swiss Federal Institute of Technology of Lausanne, Switzerland. His current research interests include real-time monitoring and control of active distribution networks with particular focus on synchrophasor-based applications.

György Dán is an Associate professor at KTH Royal Institute of Technology, Stockholm, Sweden. He received the M.Sc. in computer engineering from the Budapest University of Technology and Economics, Hungary in 1999, the M.Sc. in business administration from the Corvinus University of Budapest, Hungary in 2003, and the Ph.D. in Telecommunications from KTH in 2006. He worked as a consultant in the field of access networks, streaming media and videoconferencing 1999-2001. He was a visiting researcher at the Swedish Institute of Computer Science in 2008, a Fulbright research scholar at University of Illinois at Urbana-Champaign in 2012-2013, and an invited professor at EPFL in 2014-2015. He was co-chair of the Cyber Security and Privacy Symposium at IEEE SmartGridComm 2014, and is an area editor of Elsevier Computer Communications. His research interests include the design and analysis of content management and computing systems, game theoretical models of networked systems, and cyber-physical system security in power systems.



Jean-Yves Le Boudec is professor at EPFL and fellow of the IEEE. He graduated from Ecole Normale Supérieure de Saint-Cloud, Paris, where he obtained the Agrégation in Mathematics in 1980 and received his doctorate in 1984 from the University of Rennes, France. From 1984 to 1987 he was with INSA/IRISA, Rennes. In 1987 he joined Bell Northern Research, Ottawa, Canada, as a member of scientific staff in the Network and Product Traffic Design Department. In 1988, he joined the IBM Zurich Research Laboratory where he was manager of the Customer Premises Network Department. In 1994 he became associate professor at EPFL. His interests are in the performance and architecture of communication systems and smart grids. He co-authored a book on network calculus, which forms a foundation to many traffic control concepts in the internet, an introductory textbook on Information Sciences, and is also the author of the book “Performance Evaluation”.

Mario Paolone (M'07 - SM'10) received the M.Sc. (Hons.) and Ph.D. degrees in electrical engineering from the University of Bologna, Bologna, Italy, in 1998 and 2002, respectively. In 2005, he was an Assistant Professor in power systems at the University of Bologna, where he was with the Power Systems Laboratory until 2011. In 2010, he received the Associate Professor eligibility from the Politecnico di Milano, Italy. He is currently an Associate Professor at the Swiss Federal Institute of Technology, Lausanne, Switzerland, where he accepted the EOS Holding Chair of the Distributed Electrical Systems Laboratory. He is the Secretary and Member of several IEEE and Cigré Working Groups. He was the Co-Chairperson of the Technical Committee of the 9th edition of the International Conference of Power Systems Transients (2009) and of the 19th Power Systems Computation Conference (2016). He is author or coauthor of more than 220 scientific papers published in reviewed journals and international conferences. He is the Editor-in-Chief of the Elsevier journal *Sustainable Energy, Grids and Networks* and the Head of the Swiss Competence Center for Energy Research "FURIES." His research interests include power systems with particular reference to real-time monitoring and operation of active distribution networks, integration of distributed energy storage systems, power system protections and power system transients. In 2013, he received the IEEE EMC Society Technical Achievement Award.