# Cyberattacks Against Event-Based Analysis in Micro-PMUs: Attack Models and Counter Measures

Mohasinina Kamal, *Student Member, IEEE*, Mohammad Farajollahi, *Student Member, IEEE*, Hamidreza Nazaripouya, *Member, IEEE*, and Hamed Mohsenian-Rad, *Fellow, IEEE*

***Abstract*— The recent advent of distribution-level phasor measurement units (D-PMUs), a.k.a., micro-PMUs, has introduced a wide range of new applications in power distribution systems. A sub-class of such emerging applications are called *event-based* methods. These methods focus on the analysis of *events* in the stream of micro-PMU measurements to achieve situational awareness, enhance load modeling, integrate distributed energy resources, etc. In this paper, we explore a scenario, where a cyberattack compromises the micro-PMU measurements during an event. Such a targeted attack could be limited in scope but result in a major impact on the operation of the power grid by highly deviating the outcome of the event-based methods. First, we investigate and model two types of such attacks, *event-unsynchronized* (basic) attacks and *event-synchronized* (advanced) attacks. We then conduct a geometric analysis to understand each attack type, in a setting where the events are represented in the phasor domain in a *differential mode*. Next, we introduce a novel method to *detect* the presence of the attack and then *identify* which micro-PMUs are compromised so as to discard the compromised measurements as a defense mechanism. The proposed approach makes critical use of magnitude as well as phase angle measurements from micro-PMUs. The method is tested on the IEEE 33-bus power distribution test system.**

***Keywords*: Micro-PMUs, Event-based Methods, Cyber Attacks, Differential Mode, Attack Modeling, Detection, and Identification, Geometric Analysis, False Data Injection, Power Distribution.**

## I. Introduction

### A. Background and Motivation

Distribution-level phasor measurement units (D-PMUs), a.k.a., micro-PMUs, provide GPS-synchronized measurements of voltage and current phasors at a high resolution, e.g., up to 120 phasor readings per second [1]. In order to support such a high rate of reporting phasor measurements, micro-PMUs have a sampling rate of 512 samples per cycle [2]. Micro-PMUs have significantly improved our ability to achieve situational awareness in power distribution systems. An important and growing class of such situational awareness methods focuses on the analysis of *events* that are observed in the micro-PMU measurements. In this context, an event is defined rather broadly, such as load switching, capacitor bank switching, DER connection/disconnection, device malfunction, fuse blowing, relay tripping, etc. [3] [4]. The application of *event-based methods* include asset monitoring [5], fault location [6], and contingency analysis [7], etc.

While these new event-based methods have made a great use of available micro-PMU measurements to provide effective situational awareness solutions; they could be *vulnerable* to certain cyberattacks that specifically seek to comprise the micro-PMU measurements during major events in power distribution systems. If such attacks are successful, then they can undermine our ability to analyze events correctly. This in turn can prompt incorrect actions that may compromise system operation. Accordingly, in this paper, we seek to address the open problem of understanding cyberattacks against the analysis of events in micro-PMUs and to develop proper countermeasures.

The authors are with the University of California, Riverside, CA, USA. This work is supported by UCOP grant LFR-18-548175. The corresponding author is Hamed Mohsenian-Rad. E-mail: hamed@ece.ucr.edu.

### B. Summary of Contributions

One can raise a number of questions regarding the cyberattacks against event-based analysis of micro-PMU data: 1) How can such attacks affect the phasor representation of an event? 2) To what extent these attacks are actually harmful, i.e., they affect the final outcome of event-based methods? 3) How can an attack be detected? 4) How can we identify the number and location of the compromised micro-PMUs once an attack is detected? We seek to answer these questions in this paper.

The contributions in this paper can be summarized as follows:

1) This paper opens up a novel study on cyberattacks. It shows how an attack against micro-PMU measurements can jeopardize the functionality of event-based applications and the operation of the power distribution system.
2) Two types of attacks are modeled, *event-unsynchronized* (basic) attacks and *event-synchronized* (advanced) attacks. The later attacks can stay inactive (thus hidden) during normal operating conditions and affect the micro-PMU measurements only during a major event. Geometric analysis is conducted to show how each type of attack can affect magnitude as well as phase angle in the voltage and current phasor measurements. The advanced attacks are more impactful and more difficult to detect.
3) An attack detection method is proposed based on examining consistency in micro-PMU measurements in *differential mode*. By using *differential* measurements instead of direct measurements, the proposed method is able to detect both types of attacks effectively. It outperforms the conventional bad data detection methods, e.g., residue-based distribution system state estimation, when it comes to detecting advanced attack cases.
4) An optimization-based attack identification method is developed to identify the compromised micro-PMU(s), once the presence of an attack is detected. The accuracy of the method is tested on the IEEE 33-bus power distribution test system under different attack scenarios.
5) The proposed attack detection method is robust to inaccuracy in pseudo-measurements and line impedances; as well as errors in micro-PMU measurements.

### C. Related Literature

As the use of information and communication technologies in power systems continues to grow, the sophistication, and the frequency of the cyberattacks against the power grid are increasing rapidly [8]. For example, the report on 2015 Ukraine attack showed how a failure in the communication network security resulted in significant power outages [9]. Attacks against power grid and its components may also lead to cascading failure in the power system, e.g., see [10], [11].

Broadly speaking, attacks on PMUs can be defined as any altering of the measurements or blocking of the flow of data that is reported by PMUs and/or phasor data concentrators (PDCs). These attacks can impede various critical tools, such as state estimation, real-time protection, and control algorithms that rely on continuous streaming data [12] [13].

A detailed sequence of an attack on PMU measurements is portrayed in [14]. In a nutshell, an attack starts by detecting and exploiting vulnerabilities in the target system, including in the operating system (OS) and firmware version, in order to scan devices settings and configurations, e.g., to discover active IP addresses that belong to PMUs. Later, the attack seeks the best way for injecting false data into the PMU traffic without being detected; see [14] for more details.

Different types of attacks against PMUs have been investigated in the literature. Several examples in this area include packet drop attacks [15], Denial of Service (DoS) attacks [16], GPS signal spoofing [17], and data manipulation [18].

Broadly speaking, the nature of cyberattacks that are studied in this paper can be seen as a special case of the general class of *false data injection attacks* (FDIAs) in power systems. Several methods have been introduced to detect FDIAs. For example, in [19] [20], an attack is detected by detecting the mismatch between the values obtained from PMUs and those obtained from SCADA. However, most events in power distribution systems that are of interest in the context of micro-PMU measurements, last only a few milliseconds to a few seconds. Therefore, they do *not* even appear in SCADA measurements. Other methods of detecting FDIAs include applying deep learning techniques to recognize the behavior patterns of FDIAs based on historical measurement data [21], monitoring the line impedances which get affected when data is manipulated [22], and using density-based spatial clustering of applications with noise [23]. Some other approaches focus on creating data redundancy by leveraging optimal PMU placement to ensure system observability despite a cyberattack [24]-[26].

The studies that we mentioned above are related to the cyber-security issues in PMUs in general. They are *not* discussed in the specific context of micro-PMUs. This is because the whole concept of micro-PMUs was introduced only recently. So far, the studies in [27] [28] have proposed methods to model and detect FDIAs against the specific application of distribution system state estimation. Both papers require attackers to have full or at least partial knowledge of the *network topology* and the *system parameters*, such as line impedances, in order to launch a successful attack. Interestingly, for the type of attacks that is explored in this paper, there is *no* need for an attacker to have any such knowledge about the power system. Another study that has addressed cyber-security in micro-PMUs is [29], where the authors proposed an optimal micro-PMU placement method in order to detect anomalies in measurements.

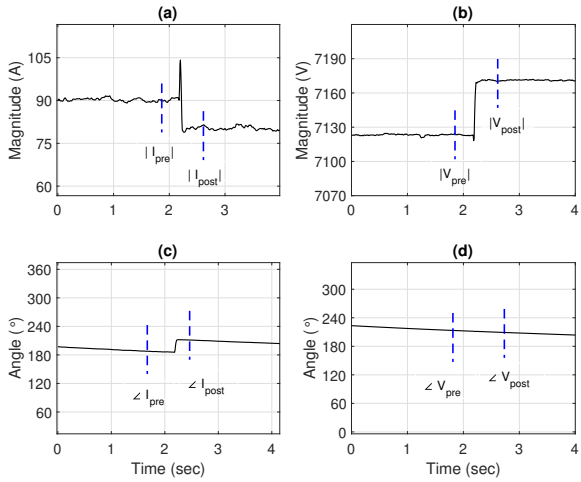



Fig. 1: The voltage and current phasor measurements that are captured by a micro-PMU during a real-life capacitor bank switching event [1].

This manuscript is different from the previous works in [27]-[29], both in terms of the types of attacks that are studied; as well as the methodologies to investigate the attacks, to detect and identify the compromised micro-PMU(s).

Moreover, this paper and the work in [30] are in two opposite directions. The work in [30] provides a new method for an event-based analysis based on micro-PMU measurements. In this paper, we make the case that an event-based analysis, such as the one in [30], is *vulnerable* to cyder-attacks against micro-PMUs. Both the analysis in this paper and the one in [30] use *differential synchrophasors*; however, this is simply because differential synchrophasors are very well-suited to mathematically represent the events in distribution synchrophasor measurements. Importantly, the method in [30] uses differential synchrophasors to identify the location of an event. In contrast, we use differential synchrophasors to detect whether any micro-PMU is compromised; and subsequently to identify which exact micro-PMUs are compromised; regardless of the application of the event-based analysis. Of course, the outcome of this paper can help make any event-based analysis of micro-PMU measurements, including the method in [30], to be more resilient to cyberattacks against micro-PMUs.

Finally, compared to the preliminary conference version of this work in [31], the current journal submission has several new and important contributions. The analytical geometric studies of attack models, the performance comparison of the detection method, and the sensitivity analysis to errors in measurements and pseudo-measurements are all new in this journal version. Furthermore, the proposed attack detection and identification method is independent of any specific event-based application; as opposed to the application-specific analysis in [31]. Last but not least, we have analyzed a series of different events in our case studies in this journal version to emphasize that the proposed method using *pre-event* and *post-event* measurements can work for various distribution-level events.

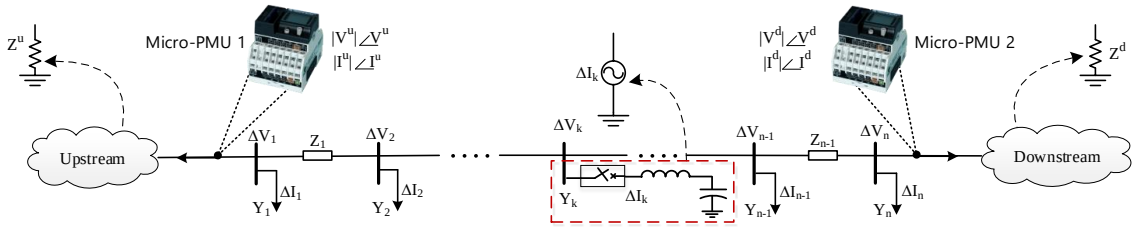



Fig. 2: An example event-based method that can be vulnerable to the type of cyberattacks that we study in this paper. Here, the measurements from two micro-PMUs are collected in differential mode in order to identify the location of the capacitor bank switching event.

## II. Events in Distribution Systems

Recall from Section I that the definition of events in the context of this paper is rather broad. For example, Fig. 1 shows the micro-PMU measurements (on one phase) during a real-world capacitor bank switching event in a 12 kV power distribution system. Hundreds of such events occur in each power distribution feeder every day. The focus of the event-based methods in the literature are to capture and analyze the micro-PMU measurements during this type of events and infer the states of the system, or the health of the grid equipment, events detection and classification, etc. [32] [33].

### A. Phasor Representation of Events

In many cases micro-PMUs are geared to steady-state analysis of the distribution system. When it comes to an event, two sets of synchronized phasors from micro-PMUs are often used in order to analyze the event: the synchronized phasor measurements *before* the event and the synchronized phasor measurement *after* the event. For example, consider the capacitor bank switching event in Fig. 1. The *pre-event* and *post-event* phasors are marked on the figure. Together, these two sets of synchrophasor measurements represent the event in the phasor domain in the *differential* mode, as follows [30]:

$$\Delta V = V_{\text{post}} - V_{\text{pre}}, \tag{1}$$

$$\Delta I = I_{\text{post}} - I_{\text{pre}}. \tag{2}$$

Note that, both $\Delta V$ and $\Delta I$ are themselves phasors. They are sometimes referred to as *differential phasors* [34].

The analysis in this paper is applicable to any event that creates a steady-state change in the phasor measurements, such that the phasors "before" the event are different from the phasors "after" the event. Accordingly, such events can be represented based on their *differential synchrophasors*. Several events in practice meet the above requirement, including load switching, capacitor bank switching, transformer tap changing, fuse blowing, etc. All these events are important for the utility and of focus for event-based analysis, e.g., see the studies in [3]-[7]. Therefore, they are all good targets for attacks against events-based analysis; which is the focus of this paper.

The above phasor representation of an event is a key step in some of the emerging event-based methods to analyze micro-PMU measurements as we will see in Section II-B.

### B. An Example Event-Based Analysis

While this paper is not concerned with a particular event-based method or a particular application of such methods, it is worth to briefly discuss one such application to see how the outcome of an event-based analysis can be manipulated by corrupting the micro-PMU measurements in differential mode.

Again, consider the capacitor bank switching event in Fig. 1. Suppose we want to know the location of the capacitor bank. This is an important piece of information for the utility operator. As shown in Fig. 2, the location of the capacitor bank can be obtained by representing the event in the phasor domain in the differential mode. By applying the *compensation theorem* from circuit theory [35], we can construct an equivalent circuit for the distribution feeder in differential mode. Here, the feeder has $n$ buses and the event occurs at bus $k$; which is assumed to be unknown. Using the measurements from two micro-PMUs, the location of the event is identified as [30]:

$$k = \arg\min_{i} \quad |\Delta V_i^u - \Delta V_i^d|. \tag{3}$$

where at each bus $i$, differential nodal voltage phasors $\Delta V_i^u$ and $\Delta V_i^d$ are calculated based on the measurements of the upstream micro-PMU and the downstream micro-PMU, respectively, and by applying the circuit laws; see [30].

From (3), it is clear that if a cyberattack can compromise the micro-PMU measurements, whether at micro-PMU 1 or micro-PMU 2, then the attacker can seek to change $\Delta V_i^u$ or $\Delta V_i^d$, respectively. In either case, the attack can *completely change the outcome* of the event location identification algorithm; thus, voiding the whole advantage of the method in [30]. We will further investigate the impact of a cyberattack against the above event location identification algorithm in Section III-C.

## III. Two Types of Attacks and Their Geometric Analysis

In practice, each micro-PMU has two separate channels to report the magnitude and phase angle for a phasor measurement [36]. Let us denote the readings at these two channels as

$$|X| \quad \text{and} \quad \angle X, \tag{4}$$

respectively. Phasor $X$ could be either a voltage phasor or a current phasor. If the micro-PMU is compromised, then the attacker can corrupt and change the above two readings to

$$|X^{\text{corrupt}}| \quad \text{and} \quad \angle X^{\text{corrupt}}, \tag{5}$$

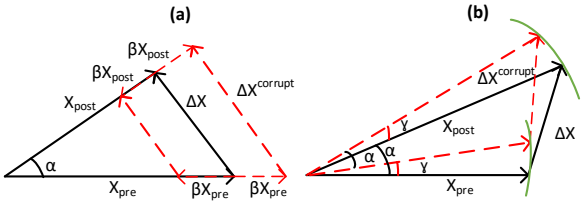



Fig. 3: Geometric illustration of the basic attack and its impact on $\Delta X$: (a) an attack that only affects the magnitude channel of the micro-PMU; (b) an attack that only affects the phase angle channel of the micro-PMU.

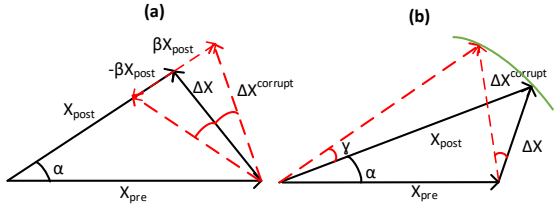



Fig. 4: Geometric illustration of the advanced attack and its impact on $\Delta X$: (a) an attack that only affects the magnitude channel of the micro-PMU; (b) an attack that only affects the phase angle channel of the micro-PMU.

where

$$|X^{\text{corrupt}}| \neq |X| \quad \text{and} \quad \angle X \neq \angle X^{\text{corrupt}}. \tag{6}$$

Since our focus in this paper is on attacks against event-based methods, we are interested in understanding how a cyberattack may compromise the phasor representation of the event. That is, we are interested in evaluating how the following vector

$$\Delta X^{\text{corrupt}} = |X^{\text{corrupt}}_{\text{post}}|\angle X^{\text{corrupt}}_{\text{post}} - |X^{\text{corrupt}}_{\text{pre}}|\angle X^{\text{corrupt}}_{\text{pre}} \tag{7}$$

would be different from the original vector $\Delta X$. We are also interested in understanding how such difference can affect the decisions that are made based on the phasor representation of an event, e.g., for the event-based application in Section II-B.

In this section, we introduce two types of attacks and study their impact on differential phasors using geometric analysis.

### A. Basic Attack: Event-Unsynchronized

In this "basic" attack scenario, the attack cannot distinguish the pre-event phasor measurements and the post-event phasor measurements. Therefore, the attack cannot affect $X_{\text{pre}}$ and $X_{\text{post}}$ differently. We refer to this type of attacks as *event-unsynchronized*; because the attacker is unable to synchronize the false data injection actions with the occurrence of the event. Nevertheless, the attack can still affect the phasor representation of the event, i.e., $\Delta X$, as it is shown in Fig. 3.

In Fig. 3(a), the attacker only corrupts the measurements at the magnitude channel of the micro-PMU; but not at the phase angle channel. In particular, the attack is designed to increase or decrease the magnitude measurements with a factor of $\beta$. Since the attack is event-unsynchronized, we have;

$$|X^{\text{corrupt}}_{\text{pre}}| = |X_{\text{pre}}| + \beta\,|X_{\text{pre}}|, \tag{8a}$$
$$|X^{\text{corrupt}}_{\text{post}}| = |X_{\text{post}}| + \beta\,|X_{\text{post}}|. \tag{8b}$$

By replacing (8) in (7), the magnitude of the phasor representation of the event under attack is

$$|\Delta X^{\text{corrupt}}| = (1+\beta)|\Delta X|. \tag{9}$$

Note that, if $\beta < 0$, then the magnitude decreases.

In Fig. 3(b), the attacker only corrupts the measurements at the phase angle channel of the micro-PMU; but not at the magnitude channel. In particular, the attack is designed to increase or decrease the phase angle by an amount of $\gamma$. Since the attack is event-unsynchronized, we have

$$\angle X^{\text{corrupt}}_{\text{pre}} = \angle X_{\text{pre}} + \gamma \tag{10a}$$
$$\angle X^{\text{corrupt}}_{\text{post}} = \angle X_{\text{post}} + \gamma. \tag{10b}$$

By replacing (10) in (7), the phase angle of the phasor representation of the event under attack is impacted as follows:

$$\angle \Delta X^{\text{corrupt}} = \angle \Delta X + \gamma. \tag{11}$$

The above two cases exemplify how a basic attack can affect the phasor representation of an event. As we will see in Section V, basic attacks are easier to detect when it comes to attack detection methods that we will develop in differential mode.

### B. Advanced Attack: Event-Synchronized

In this "advanced" attack scenario, the attacker has the ability to detect when an event occurs. Thus, the attack can be specific and target to only compromise the phasor representation of the event. Importantly, event-synchronized attacks can stay inactive (and thus hidden) during normal operating conditions and affect the micro-PMU measurements only during the events. As a result, they can have a drastic impact on event-based methods while they do not trigger attack detection mechanisms that monitor power system sensor measurements during normal operating conditions. Note that, event-synchronized attacks may have no footprint other than specifically during the events.

An event-synchronized attack can compromise the pre-event measurements and the post-event measurements, separately. Alternatively, the attack may only change the post-event measurements; the impact can be similar in terms of affecting the phasor representation of the event. Thus, to simplicity the discussions, for the rest of this paper, we assume that the attacker corrupts only the post-event phasor measurements.

As in Section III-A, we can characterize event-synchronized attacks using geometric analysis. This is illustrated in Fig. 4.

In Fig. 4(a), the attacker only corrupts the measurements at the magnitude channel of the micro-PMU. Thus, we have:

$$|X^{\text{corrup}}_{\text{pre}}| = |X_{\text{pre}}|, \tag{12a}$$
$$|X^{\text{corrupt}}_{\text{post}}| = |X_{\text{post}}| + \beta\,|X_{\text{post}}|, \tag{12b}$$

From (12) and (7), we have:

$$|\Delta X^{\text{corrupt}}| = [\,|X_{\text{pre}}|^2 + |X_{\text{post}}|^2(1+\beta)^2 - 2(1+\beta)X_{\text{pre}} \cdot X_{\text{post}}\,]^{\frac{1}{2}}, \tag{13}$$

and

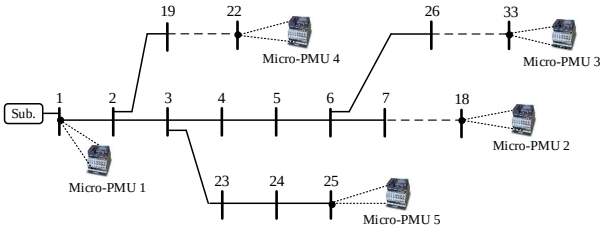



Fig. 5: The IEEE 33-bus test system that is used in our case studies. The micro-PMUs are deployed at the end of main feeder and laterals.

$$\angle\Delta X^{\text{corrupt}} = \angle\Delta X + \arcsin\left\{\frac{|X_{\text{post}}|(1+\beta)}{|\Delta X^{\text{corrupt}}|}\sin\alpha\right\} - \arcsin\left\{\frac{|X_{\text{post}}|}{\sqrt{|X_{\text{pre}}|^2+|X_{\text{post}}|^2-2X_{\text{pre}}\cdot X_{\text{post}}}}\sin\alpha\right\}, \tag{14}$$

where $(\cdot)$ denotes the operator for inner product of phasors.

In Fig. 4(b), the attacker only corrupts the measurements at the phase angle channel of the micro-PMU. Thus, we have:

$$\angle X_{\text{pre}}^{\text{corrupt}} = \angle X_{\text{pre}}, \tag{15a}$$

$$\angle X_{\text{post}}^{\text{corrupt}} = \angle X_{\text{post}} + \gamma. \tag{15b}$$

Then from (12) and (7), we have:

$$|\Delta X^{\text{corrupt}}| = [\ |X_{\text{pre}}|^2 + |X_{\text{post}}|^2 - 2|X_{\text{pre}}||X_{\text{post}}|cos(\alpha+\gamma)\ ]^{\frac{1}{2}}, \tag{16}$$

and

$$\angle\Delta X^{\text{corrupt}} = \angle\Delta X - \arcsin\left\{\frac{|X_{\text{post}}|}{|\Delta X^{\text{corrupt}}|}\sin(\alpha+\gamma)\right\} + \arcsin\left\{\frac{|X_{\text{post}}|}{\sqrt{|X_{\text{pre}}|^2+|X_{\text{post}}|^2-2X_{\text{pre}}\cdot X_{\text{post}}}}\sin\alpha\right\}. \tag{17}$$

From the above analysis, we can conclude that an advanced attack against either the magnitude channel or the phase angle channel can compromise *both* the magnitude and phase angle of $\Delta X$. Whereas in the case of a basic attack, an attack against the magnitude (phase angle) channel can compromise only the magnitude (phase angle) of $\Delta X$. Therefore, advanced attacks can be more impactful on event-based methods.

### C. Impact of Attacks on Event-Based Analysis

In this section, we provide a numerical example to illustrate the impact of the basic and advanced attacks on an event-based analysis. This example is meant to motivate our discussion on attack detection and identification in the next section.

Again consider the event-based method in Section II-B and the capacitor bank switching event performed in IEEE-33 bus test system in Fig. 5. Recall that the method in [30] uses the measurements from micro-PMUs to identify the location of the capacitor bank; which is placed on bus 10 in Fig. 5. The outcome of the method in [30] is shown in Fig. 6, for different choices of attack parameters $\beta$ and $\gamma$, when micro-PMU-2 located at bus 18 is compromised by the attacks that we introduced in Sections III-A and III-B, respectively. The

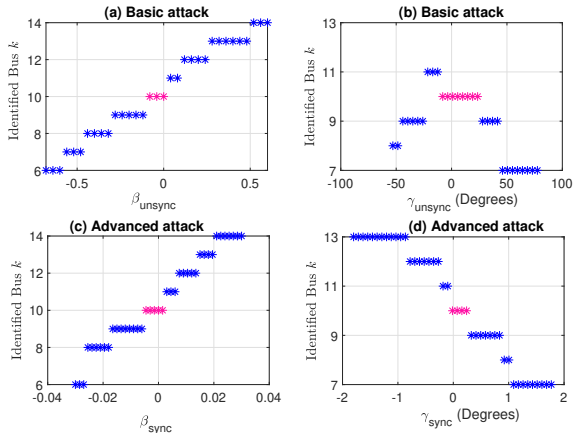



Fig. 6: Impact of the attack on the ability of the event-based method in [30] to correctly identify the location of the capacitor bank at bus 10: (a)-(b) event-unsynchronized attack, and (c)-(d) event-synchronized attack. The correct bus location is shown in pink; an incorrect bus location is shown in blue.

pink markers in Fig. 6 refer to the *correct* bus number as the source location of the event, i.e., bus 10; which are identified when $\beta$ and $\gamma$ are close to zero on the x-axis. However as $\beta$ and $\gamma$ increase on the positive side or decrease on the negative side, we get highly *incorrect* bus number on the y-axis as the source location of the event. They are shown with blue markers in Fig. 6. Overall, we can see that the method in [30] results in falsely identified event source location for the capacitor bank switching event, under both types of attacks.

Importantly, in case of an advanced attack, the attacker needs to inject a *much smaller false data* into the compromised micro-PMU in order to corrupt the outcome of the method, compared to the case of basic attacks. From Figs. 6(a) and (c), the attacker needs to inject 20 times larger $\beta$ in the basic attack to get similar impact as in the advanced attack. Here, $\beta$ reflects the fractional changes in per unit voltage magnitude according to (8) and (12); therefore, it has no unit. Also, from Figs. 6(b) and (d), it is quite impossible for the basic attacker to create a considerable impact without raising alarms, injecting only into the phase angle channel of micro-PMUs. Whereas, $\gamma$ is almost 50 times smaller and have a larger impact in advanced case scenarios. These make advanced attacks harder to detect. In all the cases, subscript *unsync* and *sync* with $\beta$ and $\gamma$ is used to indicate basic and advanced attacks, respectively.

## IV. Attack Detection and Identification

As we saw in Section III-C, even a small deviation that is caused by an attack in readings from a micro-PMU can have a significant impact on event-based applications in power distribution systems. This is particularly true under event-synchronized attacks. This makes attack detection a challenging task. Furthermore, once an attack is detected, we need to also identify *which* micro-PMU(s) are compromised. This is also a challenging task because we do not know how differently an event may affect the measurements at different micro-PMUs; and we often do not know how the true (not corrupted) measurements corresponding to an event may look like.

In this section, we show that the key to addressing the above challenges are to develop event detection and event identifica-

tion methods in differential mode, i.e., based on differential synchrophasors, as opposed to ordinary synchrophasors.

### A. Attack Detection

Consider a pair of micro-PMUs and suppose an event occurs on the distribution feeder. Suppose the feeder is modeled as an equivalent circuit in differential mode, as in Fig. 2 in Section II. First, let us start from the differential phasor that is obtained by micro-PMU 1 at bus 1 and successively apply the Kirchhoff Voltage Law (KVL) in the *forward* direction and calculate the following differential phasors from bus 1 all the way to bus $n$:

$$\Delta V_1^1, \Delta V_2^1, ..., \Delta V_n^1. \tag{18}$$

Next, let us start from the differential phasor that is obtained by micro-PMU 2 at bus $n$ and successively apply the KVL in the *backward* direction and calculate the following differential phasors from bus $n$ all the way back to bus 1:

$$\Delta V_1^2, \Delta V_2^2, ..., \Delta V_n^2. \tag{19}$$

Note that, the superscripts in (18) and (19) denote the micro-PMU from which we started the successive calculation of the differential voltages across the power distribution feeder. Another note is that, both the forward sweep that results in (18) and the backward sweep that results in (19) need some knowledge about the loading at each bus. Such knowledge can be obtained by using the measurements from smart meters; in case smart meters are available. Otherwise, we can simply use *pseudo-measurements*, such as the ratings of load transformers or the historical load data that is available to the utility. As we will discuss in Section V-D, our analysis is robust to limited accuracy in our knowledge about the loading at each bus.

In general, the fundamental observation in (18) and (19) is that the difference between the calculated differential voltages should be minimum at the event location; because the event for which the differential phasors are obtained is the same [30]. However, if one of the two micro-PMUs is compromised, whether an event-unsynchronized or event-synchronized attack, the calculated differential phasors at the event location in (18) and (19) would not match, which increases the inconsistency in the measurements. This could indicate that something is not right with respect to the measurements; thus giving us the main clue that the micro-PMUs might have been compromised.

The above analysis can be done similarly for any number of available micro-PMUs. That is, suppose a total of $m$ micro-PMUs are installed on the power distribution system. For each micro-PMU $l$, where $l = 1, \ldots, m$, suppose we calculate the differential voltage phasors at all buses in the network, and place the results in one vector, denoted by $\Delta V^l$. This will result in obtaining a total of $m$ calculations for the differential voltage phasor for every single bus $i$, where $i = 1, \ldots n$; all being associated with the *same event* that is being captured. Accordingly, for each bus $i$ we can obtain [37]:

$$\begin{aligned}\text{Var}\{\Delta V_i\}_M &= \text{Var}\{\text{Re}\{\Delta V_i\}_M\} + \text{Var}\{\text{Im}\{\Delta V_i\}_M\} \\ &= \frac{1}{m}\sum_{l=1}^{m}\left\{\text{Re}\{\Delta V_i^l\} - \frac{1}{m}\sum_{l=1}^{m}\text{Re}\{\Delta V_i^l\}\right\}^2 \\ &+\frac{1}{m}\sum_{l=1}^{m}\left\{\text{Im}\{\Delta V_i^l\} - \frac{1}{m}\sum_{l=1}^{m}\text{Im}\{\Delta V_i^l\}\right\}^2.\end{aligned} \tag{20}$$

where $M$ denotes the set of all buses with micro-PMUs. The cardinality of set $M$ is $m$; and $\text{Re}\{\cdot\}$ and $\text{Im}\{\cdot\}$ denote the real part and the imaginary part of the complex number, respectively.

The calculation of the *variance* in (20) is done across the $m$ different calculations of the differential voltage phasor at each bus $i$. Ideally, and in the absence of any attack, the minimum variance, which accounts for the event bus, must be zero. However, in practice, the variance is always a small number due to the measurement errors.

Based on the above analysis, we detect an attack against the micro-PMUs during an event if the following condition holds:

$$\Phi_M > \sigma, \tag{21}$$

where for a given set $M$ we define:

$$\Phi_M = \min_i \quad \text{Var}\{\Delta V_i\}_M. \tag{22}$$

Here $\sigma$ is a threshold parameter, which is calculated by analyzing the historical attack and non-attack scenarios. We will discuss the choice of $\sigma$ in details later in Section V.

The proposed attack detection method is applicable only when more than one micro-PMU is installed in the distribution feeder; such that we can check for the inconsistency in measurements. Also, in general, micro-PMUs are installed at least as a pair [38]. This is because the synchronization aspect among phasor measurements is meaningful only when there are multiple micro-PMUs present in the system.

### B. Attack Identification

The notion of variance in (20) can be used also to *identify* the attack, i.e., to identify which micro-PMU(s) are causing the inconsistency. This can be done as we explain next.

Suppose, for some reason, we decide *not* to use the measurements from certain *subset* of micro-PMUs, denoted by $P \subset M$, where the cardinality of set $P$ is $p$. In this regard, we can introduce $\text{Var}\{\Delta V_i\}_{M\setminus P}$ similar to the formulation for $\text{Var}\{\Delta V_i\}_M$ in (20), but based on only the measurements from the rest of the micro-PMUs, i.e., those in set $M\setminus P$. We can also define $\Phi_{M\setminus P}$ similar to (22), but based on $\text{Var}\{\Delta V_i\}_{M\setminus P}$ instead of $\text{Var}\{\Delta V_i\}_M$. Accordingly, we have:

$$\begin{aligned}&\Phi_{M\setminus P} = \min_i \\ &\frac{1}{m-p}\sum_{l\in M\setminus P}\left\{\text{Re}\{\Delta V_i^l\} - \frac{1}{m-p}\sum_{l\in M\setminus P}\text{Re}\{\Delta V_i^l\}\right\}^2 + \\ &\frac{1}{m-p}\sum_{l\in M\setminus P}\left\{\text{Im}\{\Delta V_i^l\} - \frac{1}{m-p}\sum_{l\in M\setminus P}\text{Im}\{\Delta V_i^l\}\right\}^2.\end{aligned} \tag{23}$$

The basic idea in our proposed attack identification method is to compare $\Phi_{M\setminus P}$ with $\Phi_M$ to see if the inconsistency is suddenly resolved, *if we remove the measurements* that come from the micro-PMUs in set $P$. Accordingly, we propose the following two steps to identify the compromised micro-PMUs.

*1) Step I:* For now, suppose we know how many micro-PMUs are compromised, but we do *not* know which ones. That is, we know $p$, but we do not know $P$; which is the set of micro-PMUs that must be removed due to being compromised. We can obtain $P$ by solving the following optimization problem:

$$\underset{P\subset M}{\textbf{minimize}} \quad \Phi_{M\setminus P} \tag{24a}$$

$$\textbf{subject to} \quad |P| = p, \tag{24b}$$

where $|\cdot|$ denotes the cardinality of the set. By solving (24), we find the set of micro-PMUs of cardinality $p$ such that the inconsistency in the analysis of the circuit in differential mode across the remaining micro-PMUs is minimized.

Optimization problem (24) can be solved in its current form using exhaustive search. Alternatively, one can introduce the following *equivalent binary reformulation* for problem (24) to be solved using standard solvers:

$$\begin{aligned}\underset{I,B,\vartheta,\nu}{\textbf{minimize}} \quad & \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m}\Big\{\mathrm{Re}\{\Delta V_i^l\}^2(I_i^l-1)\\ & +\Big(\mathrm{Re}\{\Delta V_i^l\}-\mathrm{Re}\{\nu_i^l\}\Big)^2\Big\}\\ & +\frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m}\Big\{\mathrm{Im}\{\Delta V_i^l\}^2(I_i^l-1)\\ & +\Big(\mathrm{Im}\{\Delta V_i^l\}-\mathrm{Im}\{\nu_i^l\}\Big)^2\Big\} \end{aligned} \tag{25a}$$

$$\textbf{subject to} \quad \sum_{i=1}^{n}\sum_{l=1}^{m} I_i^l = m-p, \tag{25b}$$

$$\sum_{i=1}^{n} B_i = 1, \tag{25c}$$

$$I_i^l \le B_i, \quad \forall\, l=1,\dots,m \tag{25d}$$

$$\vartheta = \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m}\Delta V_i^l I_i^l, \tag{25e}$$

$$\begin{aligned}&\mathrm{Re}\{\vartheta\}-L(1-I_i^l) && \forall\, l=1,\dots,m,\\ &\quad\le \mathrm{Re}\{\nu_i^l\}, && \forall\, i=1,\dots,n\end{aligned} \tag{25f}$$

$$\begin{aligned}&\mathrm{Im}\{\vartheta\}-L(1-I_i^l) && \forall\, l=1,\dots,m,\\ &\quad\le \mathrm{Im}\{\nu_i^l\}, && \forall\, i=1,\dots,n\end{aligned} \tag{25g}$$

$$\mathrm{Re}\{\nu_i^l\} \le L\, I_i^l, \qquad \begin{matrix}\forall\, l=1,\dots,m,\\ \forall\, i=1,\dots,n\end{matrix} \tag{25h}$$

$$\mathrm{Im}\{\nu_i^l\} \le L\, I_i^l, \qquad \begin{matrix}\forall\, l=1,\dots,m,\\ \forall\, i=1,\dots,n\end{matrix} \tag{25i}$$

$$0 \le \mathrm{Re}\{\nu_i^l\} \le \mathrm{Re}\{\vartheta\}, \qquad \begin{matrix}\forall\, l=1,\dots,m,\\ \forall\, i=1,\dots,n\end{matrix} \tag{25j}$$

$$0 \le \mathrm{Im}\{\nu_i^l\} \le \mathrm{Im}\{\vartheta\}, \qquad \begin{matrix}\forall\, l=1,\dots,m,\\ \forall\, i=1,\dots,n\end{matrix} \tag{25k}$$

$$I_i^l, B_i \in \{0,1\}, \tag{25l}$$

**Algorithm 1** Attack Identification

```
P = { };   p = 0;
if condition (21) holds then
    for p = 1 to ⌊(m − 1)/2⌋ do
        Solve the optimization problem (24).
        if condition (31) holds then
            Set P identifies the compromised micro-PMUs.
            break;
        end if
    end for
end if
return P, p
```

where $I$ is a binary $n\times m$ indicator matrix that gives the exact location of the $p$ compromised micro-PMUs. Variables $\vartheta$ and $\nu$ are complex; and $L$ is a constant large number. The details on the equivalence of problems (25) and (24) are provided in the Appendix. It is evident that the *binary-relaxation* of problem (25) is convex. Therefore, it can be solved by using a standard solver, such as CVX [39]. Nevertheless, given that in practice, only a handful of micro-PMUs are installed on a distribution feeder in practice, one can choose to either solve problem (25) in CVX; or simply solve problem (24) using exhaustive search.

*2) Step II:* As a fundamental requirement in attack identification, the number of compromised micro-PMUs should *not* be more than the number of micro-PMUs that are not compromised [40]. Thus here the parameter $p$ is upper bounded by:

$$p \le \lfloor (m-1)/2 \rfloor. \tag{26}$$

The solution of the optimization problem in (24) identifies exactly which micro-PMUs are compromised for a given $p$, i.e., it maps any $p$ to set $P$. However, we still need a mechanism to find $p$ itself. This can be done by applying a *sensitivity analysis* on the objective function similar to the one in [41].

**Proposition 1:** Suppose $F(p)$ denotes the optimal objective value in problem (24) for a given $p$ that is upper-bounded as in (26). Suppose we define a *sensitivity* function for $F(p)$ as

$$S(p) = F(p) - F(p+1). \tag{27}$$

We can show that $S(p)$ has the following two properties:
(a) It is *non-negative*, i.e., we have:

$$S(p) = F(p) - F(p+1) \ge 0. \tag{28}$$

(b) It is a *non-increasing* function of parameter $p$, i.e., we have:

$$S(p+1) \le S(p). \tag{29}$$

The proof of Proposition 1 is similar to that of Theorem 1 in [41]. In short it works based on the basic principle that if we increase $p$, i.e., discard more micro-PMUs, then the optimal objective value in (24) either decreases or does not change.

Based on Proposition 1, let us define a normalized version of the sensitivity function $S(p)$, denoted by $N(p)$, as follows:

$$N(p) = \begin{cases} 1, & \text{if} \quad p = 0 \\ S(p)/S(1), & \text{if} \quad p \neq 0 \end{cases} \tag{30}$$

Since the non-increasing function $N(p)$ starts from 1 and gradually approaches 0, one can determine parameter $p$ by applying a horizontal cut to function $N(p)$ at a proper threshold $(0 < \mu < 1)$, for which the following condition holds:

$$\begin{cases} N(p-1) & > \mu \\ N(p) & \leq \mu. \end{cases} \tag{31}$$

Parameter $\mu$, the *identification threshold* can be selected by using historical data of different attack scenarios, so as to maintain a desirable sensitivity of the identification system.

The proposed attack identification method is summarized as in Algorithm 1. This algorithm returns set $P$ as the set of identified compromised micro-PMUs; and its cardinality $p$.

## V. Additional Case Studies

All case studies in this section are performed on the IEEE-33 bus test system. A total of 136 events are simulated. Each event occurs at a randomly selected bus; in form of sudden interconnection of a load or a power generation source with 1) peak active and reactive power capacity at the bus; 2) half of the peak active and reactive power capacity at the bus; 3) peak active power at that bus with a fixed reactive power; or 4) peak reactive power at that bus with a fixed active power.

Recall that each event is represented in form of differential synchrophasors based on the pre-event and post-event phasors. For the events that we generated, fractional changes in p.u. voltage magnitude, $1 - |V_{\text{post}}|/|V_{\text{pre}}|$, has a normal distribution with zero mean and standard deviation 0.015; and changes in angle, $\angle V_{\text{post}} - \angle V_{\text{pre}}$, has a normal distribution with zero mean and standard deviation $0.39°$. These values due to the events range within $[-0.08, \quad 0.08]$ and $[-2°, \quad 2°]$, respectively.

Each event was simulated under normal operation as well as under event-unsynchronized attacks and event-synchronized attacks. Attack parameters $\beta$ and $\gamma$ are chosen at their smallest value that is needed to incorrectly identify the location of the event at least 3 buses away from the correct location.

### A. Impact of Attacks on Differential Synchrophasors

Fig. 7 shows $\text{Var}\{\Delta V_i\}$ across buses as well as its minimum, $\Phi_M$, under two scenarios: no attack and event-synchronized attack. The event occurs at bus 10, and the attack compromises the micro-PMU at bus 18. In the absence of the attack, i.e., in Fig. 7(a), the variance is relatively small at all buses and $\Phi_M$ is practically zero, i.e., $\Phi_M = 3.75 \times 10^{-10}$. In the presence of the event-synchronized attack, i.e., in Fig. 7(b), the variance increases at all buses; and $\Phi_M$ jumps to $1.19 \times 10^{-4}$. A similar figure can be plotted for the event-unsynchronized attack.

To further analyze the impact of the attack, we measure $\Phi_M$ for all the four types of considered events, at bus 10. Figs. 8 (a) and (b) portray the change in $\Phi_M$ versus the advanced attack parameters $\beta$ and $\gamma$, respectively. From these results, it can be realized that the extent of events almost does not change $\Phi_M$, rather the extent of attacks has more impact on it.

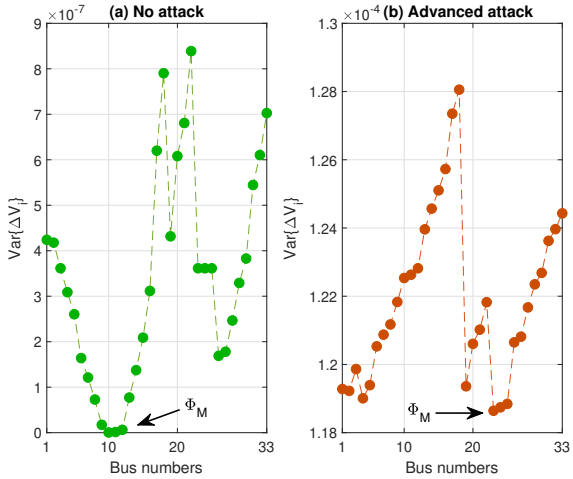



Fig. 7: Changes of variance across each bus for an example event at bus 10.

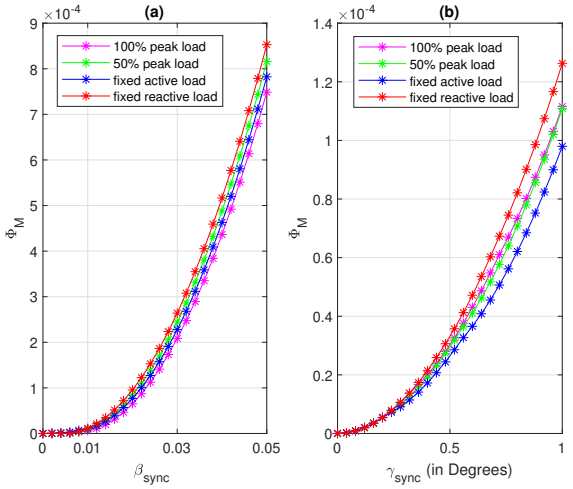



Fig. 8: Minimum variance of $\Delta V_i$, i.e., $\Phi_M$, for a range of $\beta$ and $\gamma$ values in the case of event-synchronized attacks where an event occurs at bus 10.

### B. Performance Evaluation of Attack Detection

Next, we compare our proposed attack detection method with a recent bad data detection method that is applied on micro-PMU measurements in distribution system state-estimation (DSSE) [42]. The results for comparison are shown in Fig. 9 over a total of 4000 simulations of events and attacks scenarios. Specifically, we compare the distribution of $\Phi_M$ as the key measure for attack detection in our method, versus the distribution of the *residue* in DSSE, as the key measure for bad data (and attack) detection based on DSSE. All the residues are calculated based on post-event measurements. Per [43], the errors in micro-PMU are set to be 0.05% in magnitude and 0.002 degrees in angle. From the three plots on the left hand side, it is clear that although the DSSE-based residue method can detect the basic attacks, it cannot detect the advanced attacks; because the advanced attacks do not change the distribution of the residue. In contrast, from the three plots on the right-hand side, our proposed method can detect *both* basic and advanced attacks; because both types of attacks change the distribution of $\Phi_M$ significantly.

As a side note, based on the results in Fig. 9, we can decide the value of the detection threshold $\sigma$ in (21) to be in the range of $5 \times 10^{-7}$. From the insets, it is shown that there is no value

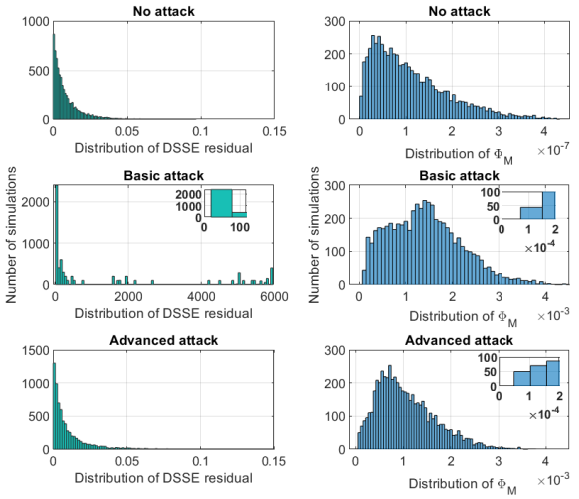



Fig. 9: Comparison between the distribution of residue in a DSSE-based detection (left) and that of $\Phi_M$ in the proposed detection method (right).

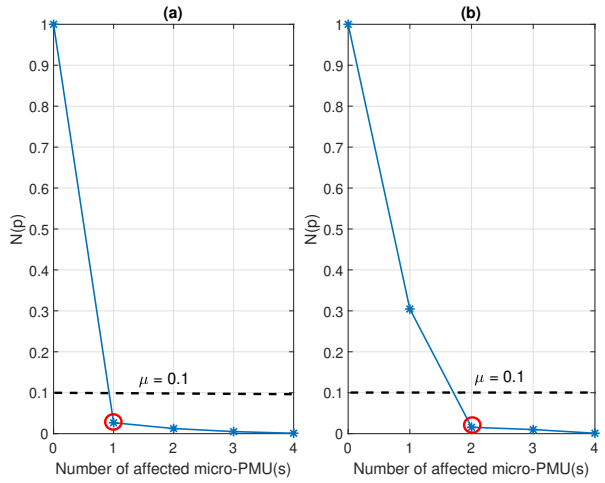



Fig. 10: Function $N(p)$ for attack identification: (a) Case I and (b) Case II.

of $\Phi_M$ for the attacked cases that falls below this threshold.

### C. Performance Evaluation of Attack Identification

Consider two cases: Case I) only micro-PMU 3 is compromised; and Case II) micro-PMUs 3 and 5 are compromised. By running the sensitivity analysis in section IV-B, appropriate identification threshold $\mu$ is found to be 0.1. As shown in Fig. 10, the number of the compromised micro-PMU(s), $p$, is correctly identified to be 1 and 2 in Cases I and II, respectively.

Next, given the value of $p$, we can solve (24) and identify the exact micro-PMU(s) that are compromised. This is illustrated in Figs. 11(a) and (b) for Case I and Case II, respectively. Pay attention to the minimum of the curve in each case. Algorithm 1 returns $P = \{3\}$ and $p = 1$ in Case I, and $P = \{3, 5\}$ and $p = 2$ in Case II. Both results are indeed correct.

To identify the attacks successfully, the total number of compromised micro-PMUs should be *less than half* of the total number of all the micro-PMUs in the system, see (26). However, this limitation is inherently inevitable because if the majority of the micro-PMUs are compromised, then we can no longer rely on consistency among the micro-PMU measurements as the key indicator to detect and identify the

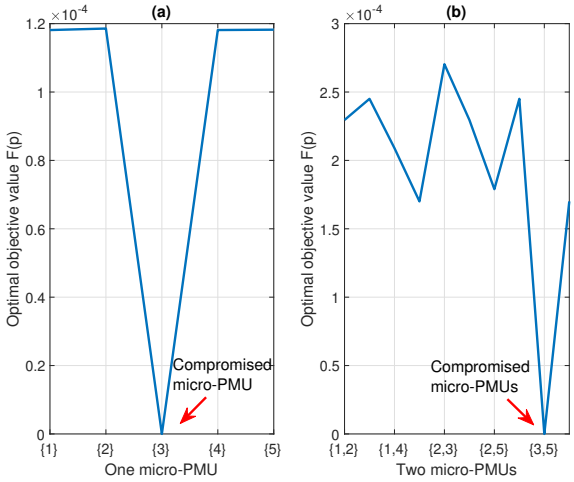



Fig. 11: Attacked micro-PMU(s) identification: (a) Case I and (b) Case II.

attack. Another limitation is for the case when the event is very small. In such cases, the information that is available about the event is very limited compared to the background noise in the system. Therefore, with or without the attack, there is not much information to check. Of course, a very small event is of less importance to the utility anyways; and accordingly, a degraded ability to evaluate it may not be a concern in practice.

### D. Analyses of Sensitivity and Robustness

In practice, the utility's knowledge about the system parameters is not perfect and measurements are not precise. Uncertainty varies for different parameters and measurements. In this section, we examine the robustness of the proposed event detection algorithm against different levels of parameters and measurements inaccuracy. We use the Monte Carlo method to generate different scenarios for each level of parameter error.

*1) Errors in Pseudo-Measurements:* Pseudo-measurements can be obtained by aggregating smart meter data, as long as such data is available; or they can be estimated solely based on the historical load data that is available to the utility, when smart meters are not available. Depending on how the pseudo-measurements are obtained, they may carry a wide range of errors, as low as 10% [44], when smart meter data is available, or as high as 50%, when pseudo-measurements are obtained from historical load data. In our simulations, the errors are being drawn from a normal distribution with zero mean and standard deviation followed by the specified measurement inaccuracies. Besides the mentioned typical range of error, we consider errors in pseudo-measurements up to 500%, which indicates the possibility of bad data injection in load information.

The distribution of $\Phi_M$ for different ranges of error in pseudo-measurements is shown in Fig. 12. By comparing the distributions of $\Phi_M$ in Figs. 12 (a)-(c) versus the distribution of $\Phi_M$ for the no attack case in Fig. 9, we can realize that for the typical ranges of pseudo-measurements errors, i.e. less than 50%, the distribution does not change. Only very large errors in the pseudo-measurements can change the distribution of $\Phi_M$. For example, if the errors in pseudo-measurements are as high as 500%, then they increase $\Phi_M$ by two orders

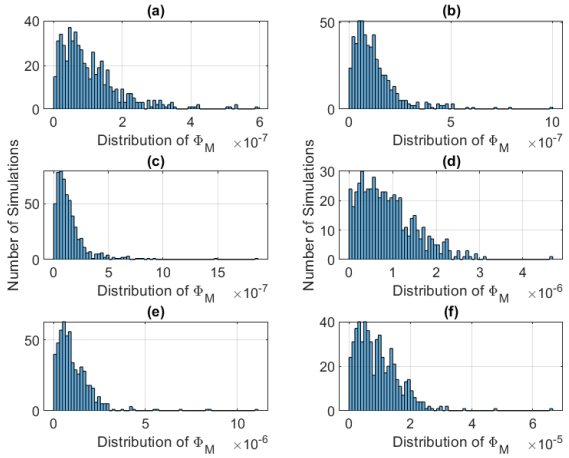



Fig. 12: The distribution of $\Phi_M$ for different levels of error in pseudo-measurements: (a) 10%, (b) 25%, (c) 50%, (d) 100%, (e) 250%, (f) 500%.

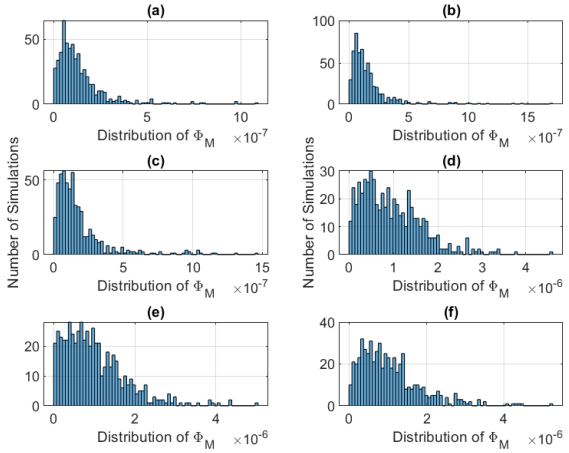



Fig. 13: The distribution of $\Phi_M$ for different levels of error in lines impedance: (a) 5%, (b) 10%, (c) 15%, (d) 20%, (e) 25%, (f) 30%.

of magnitude. Even for a large value of pseudo-measurements error, the distribution of $\Phi_M$ when there is no attack, as in Fig. 12, is very different from the distribution of $\Phi_M$ when there is an attack, as in Fig. 9. Therefore, attacks in pseudo-measurements do not considerably affect our ability to detect an attack in micro-PMUs.

*2) Errors in Distribution Line Impedances:* We further examine the performance of the proposed attack detection method against imperfect knowledge about the line impedances in the distribution system model. The results are shown in Fig.13. We can see that, the error in line impedances does *not* increase the distribution of $\Phi_M$ more than one order of magnitude. Of course, this does not mean that the imperfect line impedances do not affect the analysis of the equivalent circuit in differential mode. For example, these errors can result in an incorrect event source location identification, e.g., see [30]. However, these errors do not cause any major issue for our proposed attack detection and attack identification algorithms.

## VI. Conclusions

A new class of cyberattacks against micro-PMUs was investigated that aims to compromise event-based applications in power distribution systems. Based upon the phasor representation of events in differential mode, two types of attacks are modeled: event-unsynchronized (basic) and event-synchronized (advanced) attacks. Through a geometric analysis, it was shown that advanced attacks are more impactful and difficult to detect. A recent event-based application of micro-PMUs is scrutinized to show how the true location of the event source can be miscalculated due to the attack. A novel method is proposed to *detect* the presence of attacks and to *identify* which micro-PMUs are compromised. Case studies are presented to evaluate the proposed methods and their characteristics. It is shown that they are effective in detecting and identifying the attacks against micro-PMUs. The results in this paper can be helpful to utilities and data-driven application developers as interests in micro-PMUs and their applications continue to grow.

## Appendix

In this appendix, we explain why problem (25) and problem (24) are equivalent. The objective function in (25) can be derived by multiplying the binary indicator matrix $I$ with variance of $\Delta V$. In this regard, we can rewrite (23) as

$$\begin{aligned}\Phi_{M\setminus P} = \min_i \quad & \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m} I_i^l \Bigg\{ \mathrm{Re}\{\Delta V_i^l\} \\ & - \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m} \mathrm{Re}\{\Delta V_i^l\} I_i^l \Bigg\}^2 \\ & + \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m} I_i^l \Bigg\{ \mathrm{Im}\{\Delta V_i^l\} \\ & - \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m} \mathrm{Im}\{\Delta V_i^l\} I_i^l \Bigg\}^2 . \end{aligned} \tag{32}$$

As in (25e), let us define the following auxiliary variable, which is a complex number:

$$\vartheta = \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m} \Delta V_i^l I_i^l,$$

Accordingly, we can write the first term in (32) as

$$\frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m} I_i^l \Big\{ \mathrm{Re}\{\Delta V_i^l\} - \mathrm{Re}\{\vartheta\} \Big\}^2 \tag{33a}$$

$$\begin{aligned} = & \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m} \mathrm{Re}\{\Delta V_i^l\}^2 I_i^l + I_i^l \mathrm{Re}\{\vartheta\}^2 \\ & - 2 I_i^l \mathrm{Re}\{\vartheta\}\mathrm{Re}\{\Delta V_i^l\} \end{aligned} \tag{33b}$$

$$\begin{aligned} = & \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m} \mathrm{Re}\{\Delta V_i^l\}^2 (I_i^l - 1) \\ & + \Big\{ \mathrm{Re}\{\Delta V_i^l\} - I_i^l \mathrm{Re}\{\vartheta\} \Big\}^2 \end{aligned} \tag{33c}$$

$$\begin{aligned} = & \frac{1}{m-p}\sum_{i=1}^{n}\sum_{l=1}^{m} \mathrm{Re}\{\Delta V_i^l\}^2 (I_i^l - 1) \\ & + \Big\{ \mathrm{Re}\{\Delta V_i^l\} - \mathrm{Re}\{\nu_i^l\} \Big\}^2 . \end{aligned} \tag{33d}$$

Similar formulation can be derived for the imaginary part. Here, the product of variables $I_i^l$ and $\vartheta$ in (33c) is replaced by a new

non-negative auxiliary variable $\nu_i^l$ in (33d). Instead, for each $i$ and each $l$, we use the constraints in (25f)-(25k), to enforce the relationship between $\nu_i^l$, $\vartheta$, and $I_i^l$; see [45] and Appendix B in [46]. Thus, problems (25) and (24) are equivalent. ■

## REFERENCES


[1] H. Mohsenian-Rad, E. Stewart, and E. Cortez, "Distribution synchrophasors: Pairing big data with analytics to create actionable information," *IEEE Power and Energy Magazine*, vol. 16, no. 3, pp. 26–34, May 2018.

[2] Micro-synchrophasors for distribution grids: instrumentation lessons learned. [Online]. Available: https://www.naspi.org/

[3] M. Saini and R. Kapoor, "Classification of power quality events–a review," *Int. J. of Electrical Power & Energy Systems*, vol. 43, pp. 11–19, Dec. 2012.

[4] O. Samuelsson, M. Hemmingsson, A. H. Nielsen, K. O. H. Pedersen, and J. Rasmussen, "Monitoring of power system events at transmission and distribution level," *IEEE Trans. on Power Systems*, vol. 21, no. 2, pp. 1007–1008, May 2006.

[5] E. Stewart, M. Stadler, C. Roberts, J. Reilly, D. Arnold, and J.-Y. Joo, "Data-driven approach for monitoring, protection, and control of distribution system assets using micro-pmu technology," *CIRED-Open Access Proceedings Journal*, pp. 1011–1014, Oct. 2017.

[6] M. Farajollahi, A. Shahsavari, and H. Mohsenian-Rad, "Location identification of high impedance faults using synchronized harmonic phasors," in *Proc. of the IEEE PES ISGT*, Washington, DC, Apr. 2017.

[7] A. Shahsavari, M. Farajollahi, E. Stewart, C. Roberts, and H. Mohsenian-Rad, "A data-driven analysis of lightning-initiated contingencies at a distribution grid with a PV farm using micro-PMU data," in *Proc. of the IEEE PES North American Power Symposium*, WV, Sept. 2017.

[8] U. D. of Energy, "Enabling modernization of the electric power system."

[9] T. Rueters, "Cyberattack that crippled ukrainian power grid was highly coordinated," *CBC News*, vol. 11, 2016.

[10] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. on Smart Grid*, vol. 7, no. 1, pp. 530–538, Oct. 2015.

[11] H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.

[12] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Trans. on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, Sept. 2016.

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

[14] R. Khan, K. McLaughlin, J. H. D. Laverty, H. David, and S. Sezer, "Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid," in *16th Annual Conference on Privacy, Security and Trust (PST)*, Belfast, UK, Aug. 2018.

[15] S. Pal, B. Sikdar, and J. Chow, "Real-time detection of packet drop attacks on synchrophasor data," in *Proc. of IEEE SmartGridComm*, Venice, Italy, Nov. 2014.

[16] A. Chawla, P. Agrawal, A. Singh, B. K. Panigrahi, K. Paul, and B. Bhalja, "Denial-of-service resilient frameworks for synchrophasor-based wide area monitoring systems," *Computer*, vol. 53, no. 5, pp. 14–24, May 2020.

[17] X. Fan, L. Du, and D. Duan, "Synchrophasor data correction under gps spoofing attack: A state estimation-based approach," *IEEE Trans. on Smart Grid*, vol. 9, no. 5, pp. 4538–4546, Sept. 2018.

[18] S. Paudel, P. Smith, and T. Zseby, "Data integrity attacks in smart grid wide area monitoring," in *4th International Symposium for ICS & SCADA Cyber Security Research*, Belfast, UK, Aug. 2016.

[19] S. Pal, B. Sikdar, and J. Chow, "Detecting data integrity attacks on SCADA systems using limited PMUs," in *Proc. of the IEEE International Conference on Smart Grid Communications*, SY, Australia, Nov. 2016.

[20] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. on Smart Grid*, vol. 9, no. 3, pp. 1636–1646, July 2016.

[21] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, May 2017.

[22] S. Pal, B. Sikdar, and J. H. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Trans. on Smart Grid*, vol. 9, no. 5, pp. 5057–5066, Sep 2017.

[23] X. Wang, D. Shi, J. Wang, Z. Yu, and Z. Wang, "Online identification and data recovery for PMU data manipulation attack," *IEEE Trans. on Smart Grid*, vol. 10, no. 6, pp. 5889–5898, Jan. 2019.

[24] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On optimal PMU placement-based defense against data integrity attacks in smart grid," *IEEE Trans. on Information Forensics and Security*, vol. 12, no. 7, pp. 1735–1750, Mar. 2017.

[25] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," *IEEE Trans. on Power Systems*, vol. 21, no. 4, pp. 1608–1615, Oct. 2006.

[26] Q. Yang, L. Jiang, W. Hao, B. Zhou, P. Yang, and Z. Lv, "PMU placement in electric transmission networks for reliable state estimation against false data injection attacks," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1978–1986, Nov. 2017.

[27] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. on Smart Grid*, vol. 10, no. 3, pp. 2871–2881, Mar 2018.

[28] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices," *IEEE Trans. on Ind. Informatics*, June 2019.

[29] M. Jamei, A. Scaglione, C. Roberts, E. Stewart, S. Peisert, C. McParland, and A. McEachern, "Anomaly detection using optimally placed micro-PMU sensors in distribution grids," *IEEE Trans. on Power Systems*, vol. 33, no. 4, pp. 3611–3623, July 2018.

[30] M. Farajollahi, A. Shahsavari, E. M. Stewart, and H. Mohsenian-Rad, "Locating the source of events in power distribution systems using micro-pmu data," *IEEE Trans. on Power Systems*, vol. 33, no. 6, Nov 2018.

[31] M. Kamal, M. Farajollahi, and H. Mohsenian-Rad, "Analysis of cyber attacks against micro-PMUs: The case of event source location identification," in *Proc. of the IEEE PES ISGT*, Washington, DC, May 2020.

[32] Y. Zhou, R. Arghandeh, I. Konstantakopoulos, S. Abdullah, A. von Meier, and C. J. Spanos, "Abnormal event detection with high resolution micro-PMU data," in *Proc. of the IEEE Power Systems Computation Conference (PSCC)*, Genoa, Italy, June 2016.

[33] A. Shahsavari, M. Farajollahi, E. M. Stewart, E. Cortez, and H. Mohsenian-Rad, "Situational awareness in distribution grid using micro-PMU data: A machine learning approach," *IEEE Trans. on Smart Grid*, vol. 10, no. 6, pp. 6167–6177, Feb 2019.

[34] A. Akrami, S. Asif, and H. Mohsenian-Rad, "Sparse distribution system state estimation: An approximate solution against low observability," in *Proc. of the IEEE PES ISGT*, Washington, DC, May 2020.

[35] K. S. Kumar, *Electric circuits and networks*. Pearson, India, 2009.

[36] "IEEE standard for synchrophasor measurements for power systems," *IEEE Std C*, vol. 37, pp. 1–61, 2011.

[37] K. I. Park and Park, *Fundamentals of Probability and Stochastic Processes with Applications to Communications*. Springer, 2018.

[38] A. Von Meier, E. Stewart, A. McEachern, M. Andersen, and L. Mehrmanesh, "Precision micro-synchrophasors for distribution systems: A summary of applications," *IEEE Trans. on Smart Grid*, vol. 8, no. 6, pp. 2926–2936, Nov. 2017.

[39] http://cvxr.com/cvx/.

[40] M. Zhang, C. Shen, N. He, S. Han, Q. Li, Q. Wang, and X. Guan, "False data injection attacks against smart gird state estimation: Construction, detection and defense," *Science China Tech Sciences*, Sept. 2019.

[41] S. Amini, F. Pasqualetti, M. Abbaszadeh, and H. Mohsenian-Rad, "Hierarchical location identification of destabilizing faults and attacks in power systems: A frequency-domain approach," *IEEE Trans. on Smart Grid*, vol. 10, no. 2, pp. 2036–2045, March 2017.

[42] M. Farajollahi, A. Shahsavari, and H. Mohsenian-Rad, "Linear distribution system state estimation using synchrophasor data and pseudo-measurement," in *Proc. of the IEEE PES SGSMA*, HO, TX, Aug. 2019.

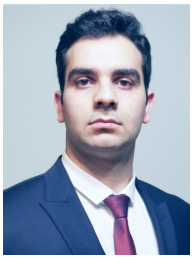
[43] https://www.powerstandards.com/product/micropmu/.

[44] F. Ni, P. Nguyen, J. Cobben, H. van den Brom, and D. Zhao, "Uncertainty analysis of aggregated smart meter data for state estimation," in *Proc. of Applied Measurements for Power Systems*, Aachen, Germany, Sept. 2016.

[45] F. Glover, "Improved linear integer programming formulations of nonlinear integer problems," *Management Science*, vol. 22, no. 4, pp. 455–460, Dec. 1975.

[46] H. Mohsenian-Rad and V. W. S. Wong, "Joint channel allocation, interface assignment and mac design for multi-channel wireless mesh networks," in *Proc. of the IEEE INFOCOM*, Anchorage, AK, May 2007.

**Mohasinina Kamal** (S'14) received the B.Sc. degree in electrical and electronic engineering from Bangladesh University of Engineering and Technology, Dhaka, Bangladesh, in 2014, the M.Sc. degree in electrical engineering from the University of Akron, Akron, OH, U.S., in 2018, and is currently pursuing her Ph.D. degree at the University of California, Riverside, CA, U.S. Her research interests include cybersecurity in power distribution grid, specifically applications of data-driven techniques and mathematical modeling and optimization to secure electricity grid monitoring and situational awareness applications.



**Mohammad Farajollahi** (S'15) received the B.Sc. degree in electrical engineering from the University of Tehran, Tehran, Iran, in 2014, and the M.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, in 2016. He is currently pursuing the Ph.D. degree with the University of California at Riverside, Riverside, CA, USA. He is specifically researching on applications of micro-PMUs and data analysis in distribution system monitoring. His research interests include power system planning, operation, reliability, as well as optimization.

**Hamidreza Nazaripouya** (S'12–M'17) received the B.S. degree in electrical engineering from the University of Tehran, Iran, the M.Sc. degree in power electronics from the Sharif University of Technology, Tehran, Iran, and the M.Sc. degree in power systems from Louisiana State University, LA, USA. He obtained his Ph.D. degree from the University of California, Los Angeles (UCLA). He is currently an Assistant Professor at Oklahoma State University, OK, USA and an Assistant Adjunct Professor at the University of California, Riverside (UCR), CA, USA. His research interests include control and optimization in power systems, distributed energy resources modeling, control and integration, power system dynamics, and power system resilience. He holds U.S. patents in control of energy storage systems. His patented technology won the NSF Grant Award with him as the Entrepreneurial Lead. He also received IEEE SFV Section Rookie of the Year Award, IEEE IAS and PES Presentation awards, and the UC Dissertation-Year Fellowship Award.

**Hamed Mohsenian-Rad** (F'20) received the Ph.D. degree in electrical and computer engineering from the University of British Columbia, Vancouver, BC, Canada, in 2008. He is currently a Professor of electrical engineering and Bourns Family Faculty Fellow at the University of California, Riverside, CA, USA. His research interests include monitoring, data analysis, and optimization of power systems and smart grids. He is the author of the book *Smart Grid Sensors: Principles and Applications*. He was the recipient of the National Science Foundation CAREER Award, the Best Paper Award from the IEEE Power and Energy Society General Meeting, and the Best Paper Award from the IEEE Conference on Smart Grid Communications. He is an Editor of the IEEE TRANSACTIONS ON SMART GRID and the IEEE POWER ENGINEERING LETTERS.