Analysis of Cyber Attacks Against Micro-PMUs: The Case of Event Source Location Identification

Mohasinina Kamal, *Student Member, IEEE*, Mohammad Farajollahi, *Student Member, IEEE*,
Hamed Mohsenian-Rad, *Senior Member, IEEE*

***Abstract*— This paper investigates cyber-attacks against *distribution-level phasor measurement units*, a.k.a., micro-PMUs. The focus is on a specific use case of micro-PMUs for locating the source of events in distribution systems. A method is proposed to detect the attack, based on two different detection criteria. Furthermore, a novel optimization-based algorithm is developed to identify which micro-PMU(s) are compromised. Importantly, the proposed attack detection and identification methods do not require prior knowledge on the number and location of affected micro-PMU(s). The proposed methods and algorithms are test through computer simulations on the IEEE 33-bus test system.**

Keywords: Micro-PMUs, event location, cyber attacks, attack detection, attack identification, differential synchrophasors.

I. Introduction

Distribution-level phasor measurement units (PMUs), a.k.a., micro-PMUs, have recently found important applications in power distribution systems [1]. One of such applications is *event source location identification* (ESLI), which can be used for asset monitoring, load modeling, etc., c.f. [2].

In this paper, we seek to answer the following questions: *1) What if the micro-PMUs are compromised via a cyber-attack, such as a false data injection attack* [3], *how would that affect the performance of the ESLI algorithms? 2) How can we detect an attack against micro-PMUs in the context of the ESLI problem? 3) Once an attack is detected, how can we identify the exact micro-PMUs that are compromised?*

A. Literature Review

Since micro-PMUs are an emerging sensor technology, their applications are being explored only recently; and there is very limited studies related to their cyber-security. In fact, the majority of the studies in this field PMU cyber-security focus on traditional PMUs at *transmission level*. A general survey of cyber-security challenges in PMUs is presented in [4]. In [5], a method is proposed to detect anomalies in PMU data by continuously monitoring the equivalent impedances of transmission lines obtained from PMU measurements. In [6], an on-line data-driven attack detection algorithm is proposed by utilizing spatio-temporal correlations among multiple time instants of synchrophasor measurements across a transmission network. In [7], a mixed integer linear program is developed to disable compromised PMUs, such that the remaining PMUs continue to maintain the observability of the power system, while minimizing the probabilistic threat levels of the PMUs.

As for the few studies that have recently addressed cyber-security in micro-PMUs, in [8] a hierarchical anomaly detection method is proposed, which considers a set of rules as signatures, along with an optimal placement algorithm for micro-PMUs, to achieve the maximum sensitivity in detecting an anomaly with limited number of sensors. Also, in [9], distribution-level FACTS devices, i.e., D-FACTS, are used to detect false data injection attacks on power grid state estimation.

Our approach here is fundamentally different from the studies in [8], [10], because our focus is on utilizing certain inherent aspects of the ESLI algorithms that can help evaluate the impact of the attack on the event source location identification results, detect the attack because of such impacts, and ultimately identify the micro-PMU(s) that have been compromised.

B. Summary of Contributions

The contributions in this paper can be summarized as follows:

1) Starting from the basic ESLI algorithm in [2] which utilizes micro-PMU measurements to locate the source of events in distribution systems, we show the extent of how injecting false data into the micro-PMUs can result in the mis-identification of the event locations.
2) We develop a novel attack detection method, based on two different detection criteria, where the decisions for attack detection are carried out based on certain residual calculations or a notion of checking consistency in results.
3) We also develop an optimization-based attack identification algorithm to identify the number and the location(s) of the compromised micro-PMU(s), once the presence of an attack is detected. The technical characteristics of the proposed methods are also discussed.
4) The analysis in this paper sheds lights on the importance of measuring both magnitude and phase angle in distribution synchrophasors, as well as the importance of protecting such measurements. Thus, this paper also contributes to the ongoing efforts in the broader field of understanding micro-PMU data and their applications.

II. Attack Model

The focus in this paper is on the specific application of micro-PMUs in solving the Event Source Location Identification (ESLI) problem, c.f. [2]. In this section, we first explain how the ESLI method in [2] works. After that, we discuss how a cyber-attack against micro-PMUs can affect the ESLI results, i.e., causing a *misidentification* of the location of the event.

A. Background: Event Source Location Identification

Consider a distribution feeder. Suppose an event occurs somewhere along this feeder. The event could be, a load

This work is supported in part by UCOP grant LFR-18-548175. The corresponding author is Hamed Mohsenian-Rad. E-mail: hamed@ece.ucr.edu.

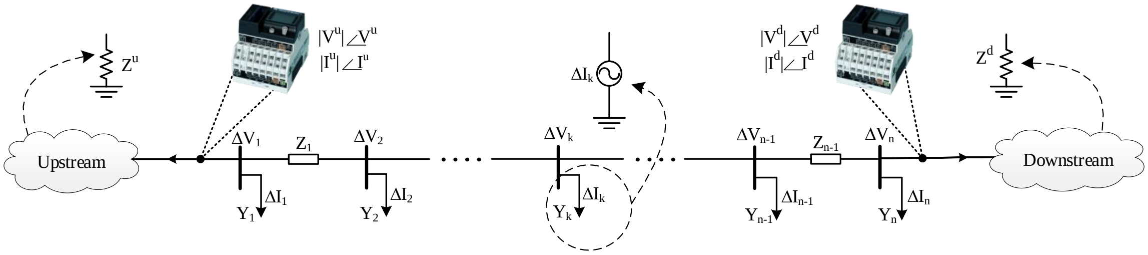

Fig. 1: Representation of a distribution feeder based on compensation theorem equivalent circuit. Measurements are done by two micro-PMUs.

switching, a capacitor bank switching, a connection or disconnection of distributed energy resources (DERs), an inverter malfunction, a minor fault, etc. The question in the ESLI problem is the following: *what is the location of the root cause for a distribution-level event, i.e., at what exact distribution bus does the load switching, capacitor bank switching, DER connection/disconnection, or device malfunction occur?*

As shown in [2], micro-PMUs play a major role in solving the ESLI problem. Specifically, if a micro-PMU is installed at the *beginning* of the feeder and another micro-PMU is installed at the *end* of the feeder, then the synchronized voltage and current phasor measurements from these two micro-PMUs can be used to accurately identify the location of the event. This can be done by taking a few steps, as we summarize next.

The first step is to construct the *differential synchrophasors*:

$$\begin{aligned} \Delta V &= V_{\text{post}} - V_{\text{pre}}, \\ \Delta I &= I_{\text{post}} - I_{\text{pre}}, \end{aligned} \tag{1}$$

where the *pre-* subscript indicates the measurements right before the event and the *post-* subscript indicates the measurements right after the event. By applying the *compensation theorem* from circuit theory [11], we can construct an equivalent circuit for the distribution feeder to analyze the event, as shown in Fig. 1. Here, the feeder has n buses and the event occurs at bus k, which is *not* known. Two micro-PMUs are installed at the beginning and at the end of the feeder, denoted by superscript u and superscript d, respectively. They are used to measure the differential synchrophasors ΔV^u, ΔI^u, ΔV^d, ΔI^d.

The second step is to use the equivalent circuit of the feeder and calculate the differential nodal voltages at each bus, denoted by $\Delta V_1, \cdots, \Delta V_n$; once by doing a *forward* calculation that starts from micro-PMU u; and once by doing a *backward* calculation that starts from micro-PMU d. Given the fact that the location of the event, i.e., bus k, is unknown, we will end up having the following correct and incorrect calculations:

$$\begin{aligned} &\{\underbrace{\Delta V_1^f, \cdots, \Delta V_{k-1}^f, \Delta V_k^f}_{\text{correct}}, \underbrace{\Delta V_{k+1}^f, \cdots, \Delta V_n^f}_{\text{incorrect}}\} \\ &\{\underbrace{\Delta V_1^b, \cdots, \Delta V_{k-1}^b}_{\text{incorrect}}, \underbrace{\Delta V_k^b, \Delta V_{k+1}^b, \cdots, \Delta V_n^b}_{\text{correct}}\}. \end{aligned} \tag{2}$$

From (2), if all measurements are accurate, then we must have $\Delta V_i^f = \Delta V_i^b$ for $i = k$; and $\Delta V_i^f \neq \Delta V_i^b$ for $i \neq k$.

Finally, the third step is to identify the location of the event by identifying the bus which has the minimum *discrepancy* in its calculated nodal voltages. In a general case, suppose $m \geq 2$ micro-PMUs are available, one at the beginning of the feeder, one at the end of the feeder, and one at the end of each lateral. The location of the event is identified as

$$k = \arg\min_{i} \quad \phi_i, \tag{3}$$

where at each bus i, the discrepancy is defined as

$$\phi_i = \sum_{j=1}^{m-1} \sum_{s=j+1}^{m} ||\Delta V_i^j - \Delta V_i^s||^2. \tag{4}$$

For the rest of this paper, we refer to the above three steps as the ESLI algorithm, see [2] for more details.

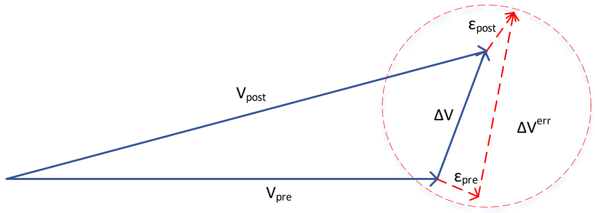

Fig. 2: An illustration of how an attack against micro-PMU measurements can affect calculating the differential nodal voltage synchrophasors.

B. Attack Against Micro-PMUs

Suppose one or more micro-PMUs are compromised. The question is: *how will it affect the performance of the ESLI algorithm?* To answer this question, consider the fact that the ESLI algorithm is built on analyzing differential synchrophasors. Thus, what matters here is the impact of the attack *not* on measuring phasors *but* rather on calculating differential phasors. This issue is illustrated in Fig. 2. Suppose the pre-event and the post-event voltage phasors are measured as

$$V_{\text{pre}} + \epsilon_{\text{pre}} \tag{5}$$

and

$$V_{\text{post}} + \epsilon_{\text{post}}, \tag{6}$$

where ϵ_{pre} and ϵ_{post} are phasors indicating the *injected error* into the pre-event and post-event readings of the micro-PMU.

The error in differential voltage phasor is obtained as

$$\begin{aligned} \Delta V^{\text{err}} &= V_{\text{post}} + \epsilon_{\text{post}} - (V_{\text{pre}} + \epsilon_{\text{pre}}) \\ &= \Delta V + \epsilon_{\text{post}} - \epsilon_{\text{pre}}. \end{aligned} \tag{7}$$

Thus, the key in affecting the ESLI algorithm is the value of phasor $\epsilon_{\text{post}} - \epsilon_{\text{pre}}$. If ϵ_{pre} and ϵ_{post} are the same then the attack has no impact on the ESLI algorithm. However, in general, ϵ_{post} and ϵ_{pre} are not the same; thus, ΔV^{err} deviates from ΔV. Such deviation is benign as long as it does not change the solution of the argument minimization problem in (3).

III. Attack Detection and Identification

In this section, we propose methods to be integrated into the ESLI algorithm in order to detect and subsequently identify attacks against micro-PMUs. Our proposed methods are built directly upon the way that the ESLI algorithm works. Therefore, it can be easily integrated into the ESLI algorithm.

Recall from Section II that, if all measurements are accurate, then the minimum discrepancy, i.e., ϕ_k, which is the optimal objective value of the argument minimization problem in (3), must be close to zero. A larger value of ϕ_k could be an indication of bad data, which includes the case where one or multiple micro-PMUs are compromised. Therefore, we may detect an attack in the ESLI algorithm if the following holds:

$$\mathbb{I}(\phi_k > \delta) = 1, \tag{8}$$

where $\mathbb{I}(.)$ is the indicator function, which is 1 if $\phi_k > \delta$; and 0 otherwise. The value of the threshold δ can be set as:

$$\text{Prob}(\phi_i > \delta : \phi_i \text{ is chi-squared}) = \alpha, \tag{9}$$

where α is a predetermined parameter which represents the probability of the presence of an attack vector.

Note that, the above method simply indicates that the results in calculating the differential synchrophasors are *inconsistent* with each other. Therefore, further inspection is needed in order identify the root cause of the observed inconsistency.

The inconsistency in calculating differential synchrophasors can be quantitatively measured also by using a notion of *variance*, which at each bus i can be defined as:

$$\text{Var}\{\Delta V_i\}_M = \frac{1}{m}\sum_{l=1}^{m}(\Delta V_i^l)^2 - \left(\frac{1}{m}\sum_{l=1}^{m}\Delta V_i^l\right)^2, \tag{10}$$

where ΔV_i^l denotes the differential phasor at bus i that is calculated by solving the equivalent circuit starting from micro-PMU l, where $l = 1, \ldots, m$. Here, M denotes the set of all buses with micro-PMUs. The cardinality of set M is m.

As an alternative to (8), we can detect an attack also by checking the above variance, i.e., when the following holds:

$$\mathbb{I}\left(\text{Var}\{\Delta V_i\} > \sigma\right), \; \exists\, i, \tag{11}$$

where σ is a known parameter, which is calculated by analyzing the attack and non-attack cases. Note that, both (8) and (11) seek to detect inconsistency in the measurements from different micro-PMUs with respect to the ESLI algorithm. However, this is done *directly* in (11), but *indirectly* in (8), where it checks for inconsistency in calculating the minimum discrepancy solution.

Importantly, the notion of variance in (10) 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 we use the measurements from only a subset of micro-PMUs, denoted by $D \subset M$, where the cardinality of set D is d. Note that, $d < m$. The variance with respect to the identification of the event bus location based on the measurements that come from set D is obtained as:

$$\text{Var}\{\Delta V_i\}_D = \frac{1}{d}\sum_{l=1}^{d}(\Delta V_i^l)^2 - \left(\frac{1}{d}\sum_{l=1}^{d}\Delta V_i^l\right)^2. \tag{12}$$

Please notice the subscript M in (10) versus the subscript D in (12). Accordingly, the basic idea in our proposed attack identification method is to compare (12) with (10) to see if the inconsistency is suddenly resolved, i.e., variance suddenly drops, *if we remove the measurements* that come from the micro-PMUs in set $M \backslash D$. In that case, we can argue that the compromised micro-PMUs are either in set D or in set $M \backslash D$.

Next, suppose we *make a guess* on the *number* of compromised micro-PMUs. That is, suppose we *assume* that the number of compromised micro-PMUs is p. We would naturally want to *remove* the measurements from these p micro-PMUs. However, even if this is a correct guess, we still need to figure out *which* micro-PMUs are compromised. We can resolve this issue by solving the following optimization problem:

$$\begin{aligned} \underset{X}{\arg\min} \quad & \max_{\mathrm{i}}\Bigg\{\frac{1}{\mathrm{m-p}}\sum_{\mathrm{l=1}}^{\mathrm{m}}\mathrm{X_l}(\Delta \mathrm{V_i^l})^2 \\ & \qquad - \left(\frac{1}{m-p}\sum_{l=1}^{m}X_l\Delta V_i^l\right)^2\Bigg\} && \text{(13a)} \\ \text{subject to} \quad & \sum_{l=1}^{m}X_l = m-p && \text{(13b)} \\ & X_l \in \{0,1\}, \quad l = 1, \ldots, m. && \text{(13c)} \end{aligned}$$

Here, vector X is binary and it has m rows. For each $l = 1, \ldots, m$, if $X_l = 0$ then we remove the measurements from micro-PMU l. In this regard, the constraint in (13b) is to make sure that we always use the measurements from exactly $m - p$ micro-PMUs, i.e., we remove the measurements from exactly p micro-PMUs. As for the objective function, it indicates the *maximum* variance, across all buses, in calculating the differential nodal voltage synchrophasors. Our goal here is to remove the measurements from exactly p micro-PMUs to achieve the minimum variance, i.e., the *minimum inconsistency* in calculating the differential nodal voltage synchrophasors.

Since the binary-relaxation of problem (13) is convex, it can be solved using software such as CVX (http://cvxr.com/cvx/).

If our initial assumption regarding the choice of parameter p is correct, then by solving problem (13) we identify which micro-PMUs are compromised, as long as we have:

$$p \leq \lfloor (m-1)/2 \rfloor. \tag{14}$$

Next, we need a mechanism to identify the number of compromised micro-PMUs. This can be done by applying a *sensitivity analysis*, similar to the one in [12]. In this regard, suppose $F(p)$ denotes the optimal objective value in problem (13) for a given parameter p, where p is upper-bounded as in (14). Note that, by construction, $F(p)$ is a *non-increasing* function of p. Accordingly, let us define a normalized version of function $F(p)$, denoted by $N(p)$, as follows:

$$N(p) = \begin{cases} 1, & \text{if} \quad p = 0 \\ F(p)/F(0), & \text{if} \quad p \neq 0 \end{cases} \tag{15}$$

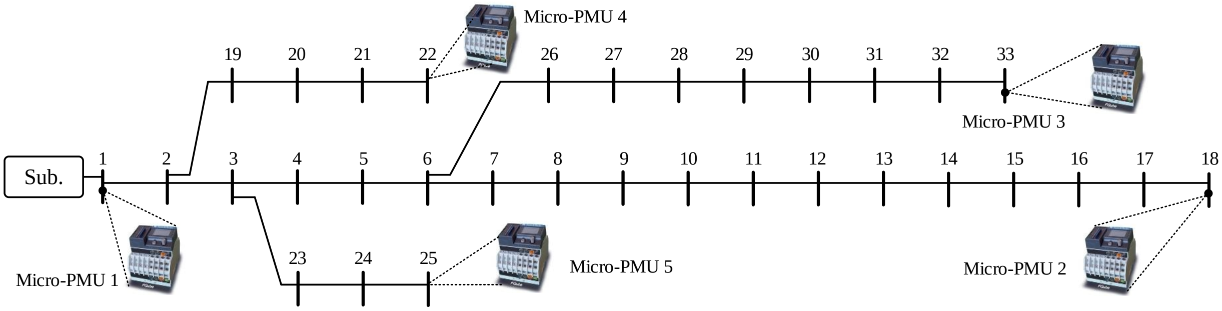

Fig. 3: The IEEE 33-bus test system that is used in our case studies. The micro-PMUs are deployed at the end of main feeder and laterals [2].

Algorithm 1 Attack Detection and Identification

```
Run ESLI Algorithm.
$P = \{\,\}$;    $p = 0$;
if conditions (8) or (11) hold then
    for $p = 1$ to $\lfloor (m-1)/2 \rfloor$ do
        Solve the optimization problem (13).
        if condition (17) holds then
            Set $P$ to include all $l$ for which $X_l = 0$.
            Set $p$ as the cardinality of $P$.
            break;
        end if
    end for
end if
return $P$, $p$
```

Note that, $F(0)$ is essentially the same as the maximum of the variance in (10) across all buses. That is, we have:

$$F(0) = \max_i \ \text{Var}\{\Delta V_i\}_M. \tag{16}$$

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:

$$\begin{cases} N(p) - 1 & > \mu \\ N(p) & \leq \mu. \end{cases} \tag{17}$$

In this regard, parameter μ can be selected by using historical data of different fault and attack scenarios, so as to maintain a desirable sensitivity of the identification system.

The proposed attack detection and 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. If no attack is detected then $P = \{\,\}$ and $p = 0$.

IV. Case Studies

The performance of our proposed method is examined on the IEEE 33-bus test system, as shown in Fig. 3.

A. Impact of Attack

Suppose micro-PMU 2 is compromised. Fig. 4 shows the results when the attack injects errors into the measured voltage magnitude at this micro-PMU. When the injected error is zero, the ESLI algorithm identifies the correct event location, which is at bus 10. However, once we inject error into the voltage magnitude, the ESLI algorithm results in incorrect location identification, either to the left to buses 9, 8, 7, or to the right to buses 11, 12, 13. The direction and extent of deviation from the correct bus depends on the sign and size of the error.

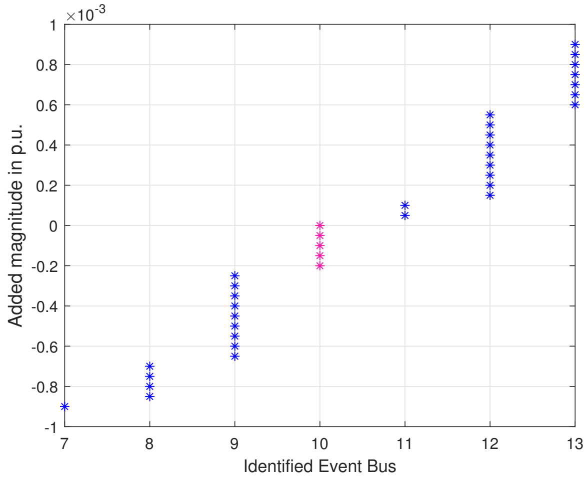

Fig. 4: The identified event location by the ESLI algorithm under various levels of injected error into the voltage *magnitude* at micro-PMU 2. The true event location is bus 10. The injected errors cause incorrect location identification.

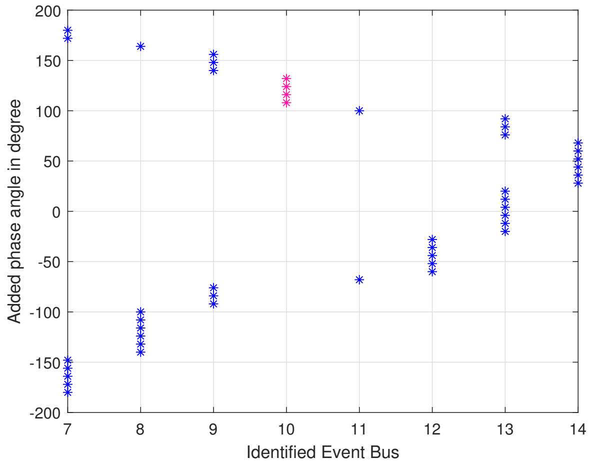

Fig. 5: The identified event location by the ESLI algorithm under various levels of injected error into the voltage *phase angles* at micro-PMU 2. The injected error into the voltage magnitude is fixed at 8×10^{-4} per unit.

Next, consider the results in Fig. 5, where the attack injects errors into the measured voltage phase angle. There is also a small but fixed injected error into the voltage magnitude at 8×10^{-4} per unit. We again see that the attack can result in major mis-identification of the event bus. The results in this figure however are not as monotone as those in Fig. 4.

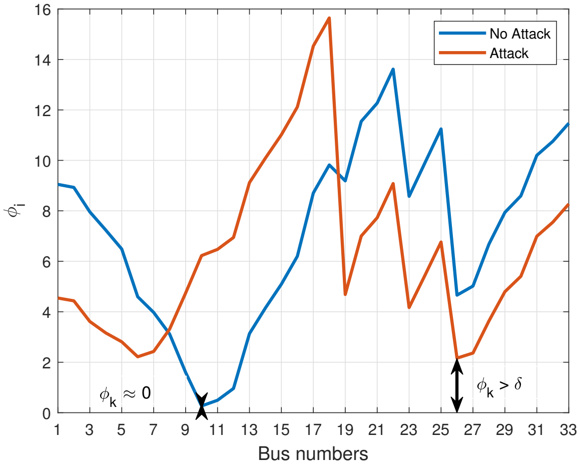

Fig. 6: The discrepancy index ϕ_i across all buses.

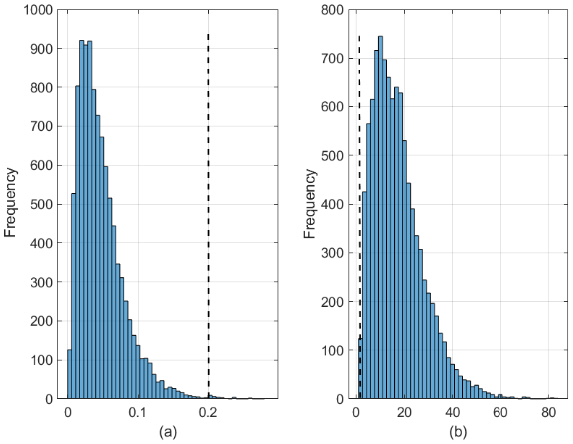

Fig. 7: Distribution of ϕ_k under (a) no attack; and (b) attack.

B. Analysis of Attack Detection

Again, suppose only micro-PMU 2 is compromised. Fig. 6 shows the profile for the discrepancy index ϕ_i across all buses, once *without* an attack and once *with* an attack. From (3), the minimum of each curve is where the ESLI algorithm identifies as the location of the attack. Under the attack, the event location is identified incorrectly at bus 26. However, the more important observation is that, the minimum discrepancy, i.e., ϕ_k, is almost zero when there is no attack, but it is a large number when there *is* an attack. And that's exactly the idea behind using (8) to detect the attack. Of course, parameter δ should be selected such that it can distinguish the difference between the value of ϕ_k in the two curves. This can be done using (9). From the distribution of ϕ_k in Fig. 7, we use $\delta = 0.2$.

C. Analysis of Attack Identification

Here, we study two cases, and the results are shown in Figs. 8(a) and (b), respectively. In case I, only micro-PMU 3 is compromised. In Case II, micro-PMUs 3 and 5, are compromised. By choosing $\mu = 0.1$, the number and location(s) of the compromised micro-PMU(s) are identified correctly in both cases. Algorithm 1 returns $P = \{3\}$ and $p = 1$ in Case I and $P = \{3, 5\}$ and $p = 2$ in Case II; which are all correct.

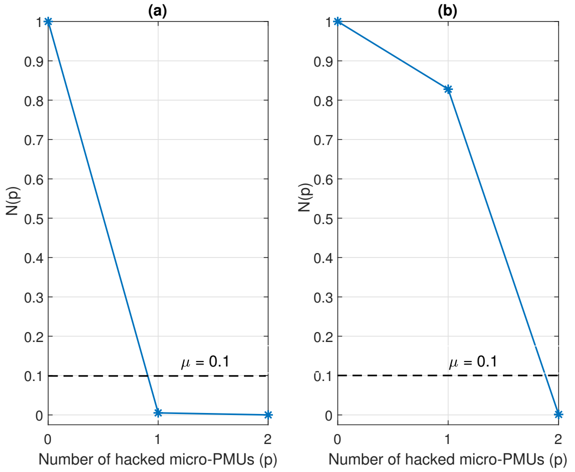

Fig. 8: Function $N(p)$ for attack identification: (a) Case I and (b) Case II.

V. Conclusions

In this paper, a novel methodology and algorithm is proposed to *detect* the presence of an attack against micro-PMUs and also to *identify* which micro-PMUs are compromised; both for the application of micro-PMUs in solving the ESLI problem. The proposed methods are built upon the way that the basic ESLI algorithms work. Therefore, they can be easily integrated into the existing ESLI algorithms. Case studies are presented to evaluate the performance of the proposed methods and their characteristics. It is shown that they are effective in both detecting and identifying the attacks against micro-PMUs.

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] 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.

[3] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems (SCS)*, Stockholm, Sweden, Apr. 2010.

[4] A. Sundararajan, K. Tanwir, A. Moghadasi, and A. I. Sarwat, "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 3, pp. 449–467, May 2019.

[5] 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.

[6] M. Wu and L. Xie, "Online detection of false data injection attacks to synchrophasor measurements: A data-driven approach," in *Proc. of the 50th Hawaii international conference on system sciences*, HI, Jan. 2017.

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

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

[9] 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.

[10] T. Sreeram and S. Krishna, "Managing false data injection attacks during contingency of secured meters," *IEEE Trans. on Smart Grid*, May 2019.

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

[12] 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.