Analysis of Cyber Attacks Against Distribution-Level PMUs: Event Source Location Case Study

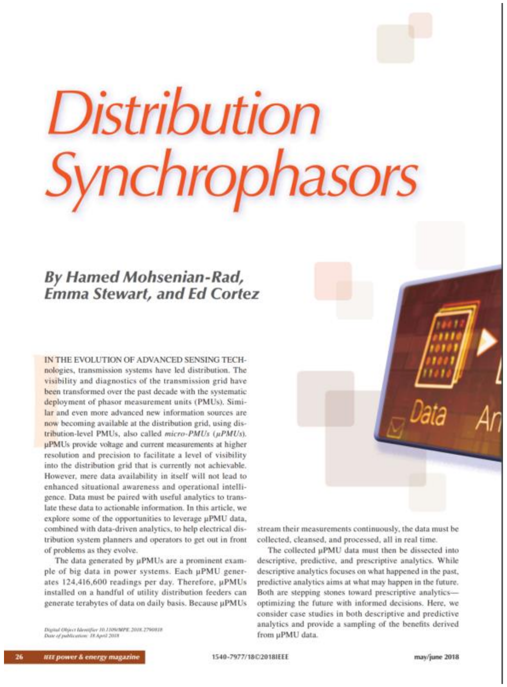
(Tasks 1.2, 1.3, and 2.2)

Mohasinina Kamal
Mohammad Farajollahi
Hamed Mohsenian-Rad

UNIVERSITY OF CALIFORNIA, RIVERSIDE

Application of Micro-PMUs:

- Capacitor Back Switching
- Fault Analysis
- Lightning Analysis
- Inverter Misoperation
- Event Classification
- Event Clustering
- Impedance Calculation
- Topology Identification
- Event Source Location Identification
- …



Distribution Synchrophasors

By Hamed Mohsenian-Rad, Emma Stewart, and Ed Cortez

IN THE EVOLUTION OF ADVANCED SENSING TECHnologies, transmission systems have led distribution. The visibility and diagnostics of the transmission grid have been transformed over the past decade with the systematic deployment of phasor measurement units (PMUs). Similar and even more advanced new information sources are now becoming available at the distribution grid, using distribution-level PMUs, also called *micro-PMUs* (*μPMUs*). μPMUs provide voltage and current measurements at higher resolution and precision to facilitate a level of visibility into the distribution grid that is currently not achievable. However, mere data availability in itself will not lead to enhanced situational awareness and operational intelligence. Data must be paired with useful analytics to translate these data to actionable information. In this article, we explore some of the opportunities to leverage μPMU data, combined with data-driven analytics, to help electrical distribution system planners and operators to get out in front of problems as they evolve.

The data generated by μPMUs are a prominent example of big data in power systems. Each μPMU generates 124,416,600 readings per day. Therefore, μPMUs installed on a handful of utility distribution feeders can generate terabytes of data on daily basis. Because μPMUs stream their measurements continuously, the data must be collected, cleansed, and processed, all in real time.

The collected μPMU data must then be dissected into descriptive, predictive, and prescriptive analytics. While descriptive analytics focuses on what happened in the past, predictive analytics aims at what may happen in the future. Both are stepping stones toward prescriptive analytics—optimizing the future with informed decisions. Here, we consider case studies in both descriptive and predictive analytics and provide a sampling of the benefits derived from μPMU data.

Date of publication: 18 April 2018

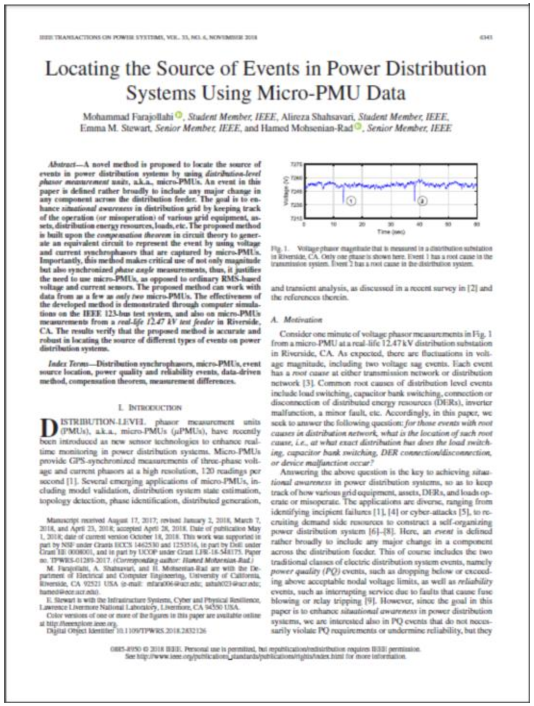
26 IEEE power & energy magazine 1540-7977/18©2018IEEE may/june 2018

IEEE Power and Energy Magazine, May 2018

Application of Micro-PMUs:

- Capacitor Back Switching
- Fault Analysis
- Lightning Analysis
- Inverter Misoperation
- Event Classification
- Event Clustering
- Impedance Calculation
- Topology Identification
- Event Source Location Identification
- …

Our Focus



Locating the Source of Events in Power Distribution Systems Using Micro-PMU Data

Mohammad Farajollahi, *Student Member, IEEE*, Alireza Shahsavari, *Student Member, IEEE*,
Emma M. Stewart, *Senior Member, IEEE*, and Hamed Mohsenian-Rad, *Senior Member, IEEE*

***Abstract*—A novel method is proposed to locate the source of events in power distribution systems by using *distribution-level phasor measurement units*, a.k.a., micro-PMUs. An event in this paper is defined rather broadly to include any major change in any component across the distribution feeder. The goal is to enhance *situational awareness* in distribution grid by keeping track of the operation (or misoperation) of various grid equipment, assets, distribution energy resources, loads, etc. The proposed method is built upon the *compensation theorem* in circuit theory to generate an equivalent circuit to represent the event by using voltage and current synchrophasors that are captured by micro-PMUs. Importantly, this method makes critical use of not only magnitude but also synchronized *phase angle* measurements, thus, it justifies the need to use micro-PMUs, as opposed to ordinary RMS-based voltage and current sensors. The proposed method can work with data from as a few as *only two* micro-PMUs. The effectiveness of the developed method is demonstrated through computer simulations on the IEEE 123-bus test system, and also on micro-PMUs measurements from a *real-life 12.47 kV test feeder* in Riverside, CA. The results verify that the proposed method is accurate and robust in locating the source of different types of events on power distribution systems.**

***Index Terms*—Distribution synchrophasors, micro-PMUs, event source location, power quality and reliability events, data-driven method, compensation theorem, measurement differences.**

I. INTRODUCTION

DISTRIBUTION-LEVEL phasor measurement units (PMUs), a.k.a., micro-PMUs (μPMUs), have recently been introduced as new sensor technologies to enhance real-time monitoring in power distribution systems. Micro-PMUs provide GPS-synchronized measurements of three-phase voltage and current phasors at a high resolution, 120 readings per second [1]. Several emerging applications of micro-PMUs, including model validation, distribution system state estimation, topology detection, phase identification, distributed generation, and transient analysis, as discussed in a recent survey in [2] and the references therein.

Fig. 1. Voltage phasor magnitude that is measured in a distribution substation in Riverside, CA. Only one phase is shown here. Event 1 has a root cause in the transmission system. Event 2 has a root cause in the distribution system.

A. Motivation

Consider one minute of voltage phasor measurements in Fig. 1 from a micro-PMU at a real-life 12.47 kV distribution substation in Riverside, CA. As expected, there are fluctuations in voltage magnitude, including two voltage sag events. Each event has a *root cause* at either transmission network or distribution network [3]. Common root causes of distribution level events include load switching, capacitor bank switching, connection or disconnection of distributed energy resources (DERs), inverter malfunction, a minor fault, etc. Accordingly, in this paper, we seek to answer the following question: *for those events with root causes in distribution network, what is the location of such root cause, i.e., at what exact distribution bus does the load switching, capacitor bank switching, DER connection/disconnection, or device malfunction occur?*

Answering the above question is the key to achieving *situational awareness* in power distribution systems, so as to keep track of how various grid equipment, assets, DERs, and loads operate or misoperate. The applications are diverse, ranging from identifying incipient failures [1], [4] or cyber-attacks [5], to recruiting demand side resources to construct a self-organizing power distribution system [6]–[8]. Here, an *event* is defined rather broadly to include any major change in a component across the distribution feeder. This of course includes the two traditional classes of electric distribution system events, namely *power quality (PQ)* events, such as dropping below or exceeding above acceptable nodal voltage limits, as well as *reliability* events, such as interrupting service due to faults that cause fuse blowing or relay tripping [9]. However, since the goal in this paper is to enhance *situational awareness* in power distribution systems, we are interested also in PQ events that do not necessarily violate PQ requirements or undermine reliability, but they

Manuscript received August 17, 2017; revised January 2, 2018, March 7, 2018, and April 23, 2018; accepted April 28, 2018. Date of publication May 1, 2018; date of current version October 18, 2018. This work was supported in part by NSF under Grants ECCS 1462530 and 1253516, in part by DoE under Grant EE 0008001, and in part by UCOP under Grant LFR-18-548175. Paper no. TPWRS-01289-2017. *(Corresponding author: Hamed Mohsenian-Rad.)*

M. Farajollahi, A. Shahsavari, and H. Mohsenian-Rad are with the Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521 USA (e-mail: mfara006@ucr.edu; ashah023@ucr.edu; hamed@ece.ucr.edu).

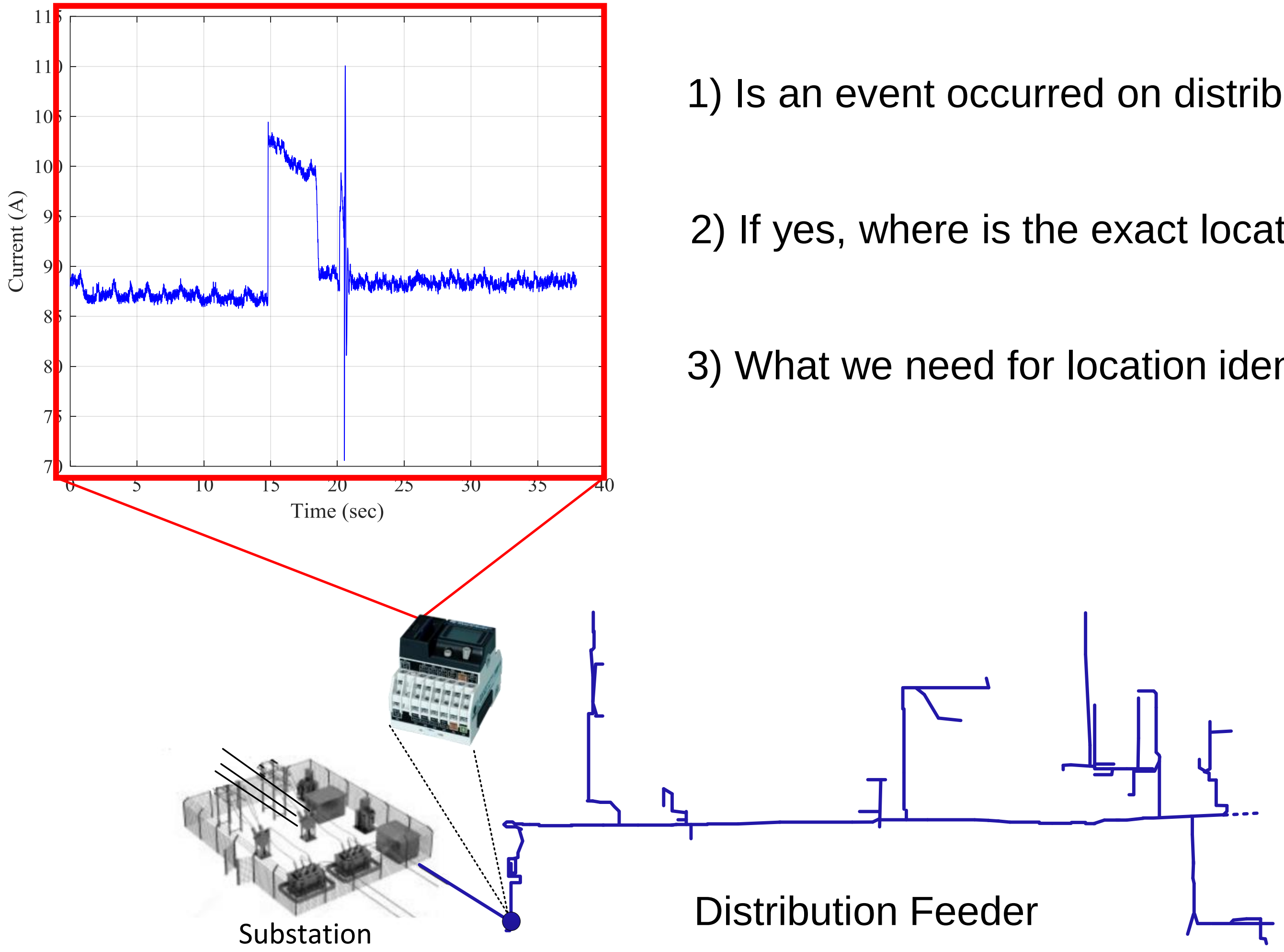
E. Stewart is with the Infrastructure Systems, Cyber and Physical Resilience, Lawrence Livermore National Laboratory, Livermore, CA 94550 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRS.2018.2832126

IEEE Trans. on Power Systems, Nov 2018

Locating Source of Events

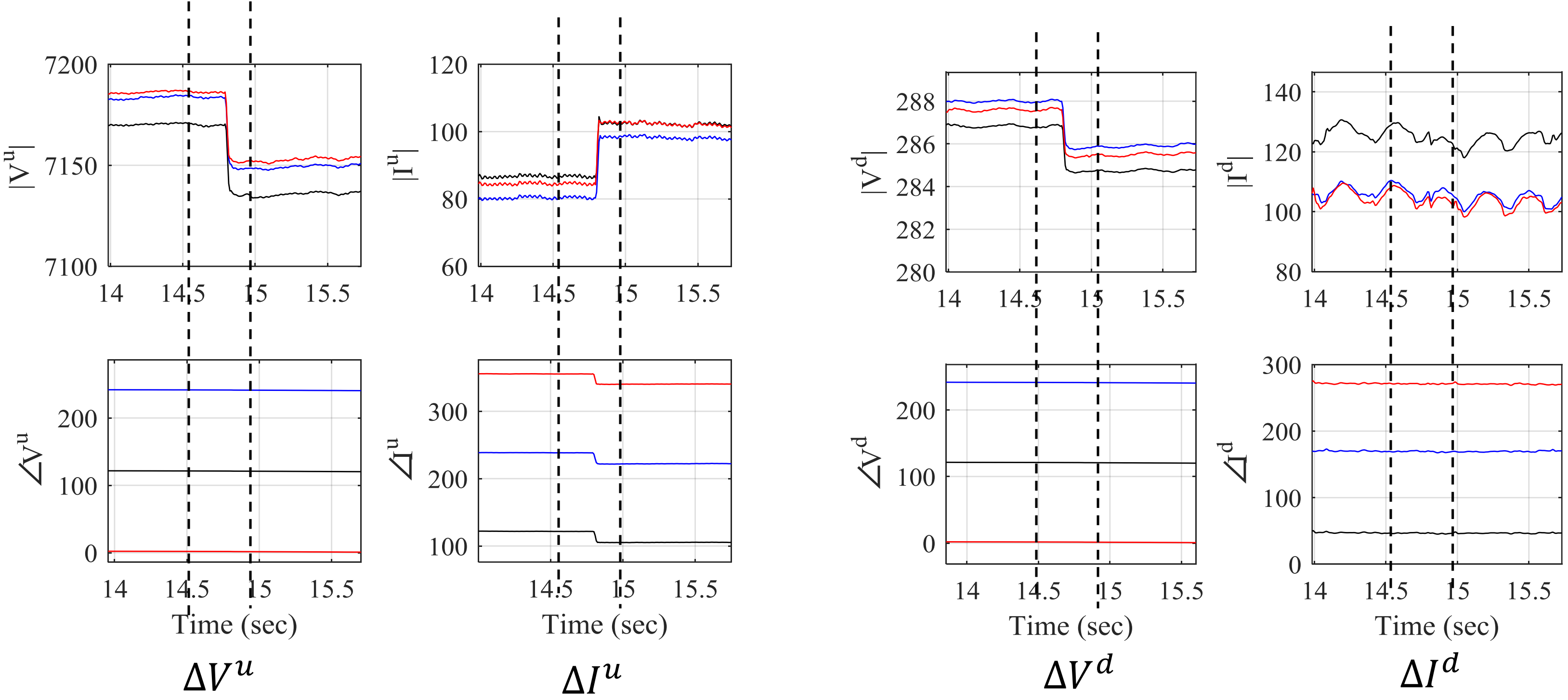


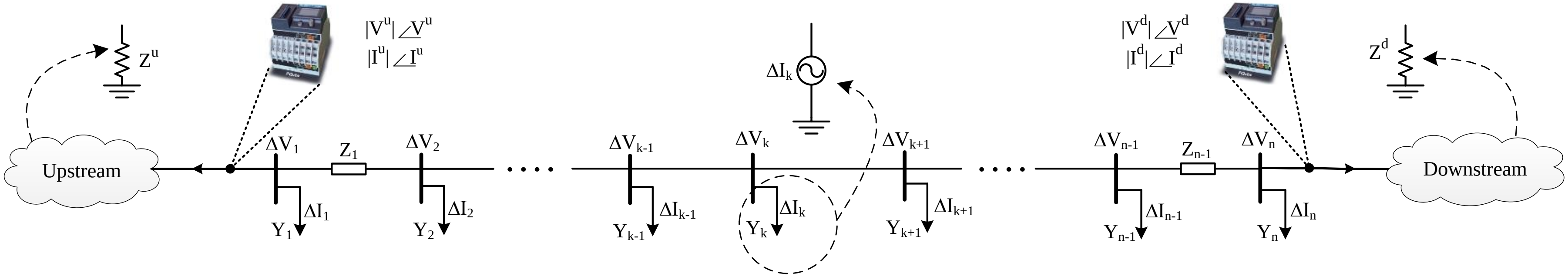
1) Is an event occurred on distribution feeder?

2) If yes, where is the exact location?

3) What we need for location identification?

Equivalent Circuit Analysis





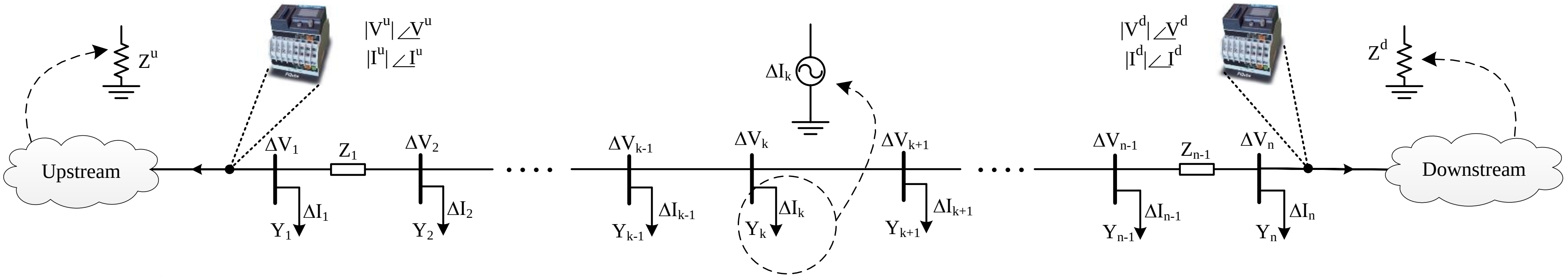
K: Event Bus (Unknown)

Voltage Comparison

Forward: $$\{\underbrace{\Delta V_1^f, \Delta V_2^f, \dots, \Delta V_{k-1}^f, \Delta V_k^f}_{\text{Correct}}, \underbrace{\Delta V_{k+1}^f, \dots, \Delta V_n^f}_{\text{Incorrect}}\}$$

Backward: $$\{\underbrace{\Delta V_1^b, \Delta V_2^b, \dots, \Delta V_{k-1}^b}_{\text{Incorrect}}, \underbrace{\Delta V_k^b, \Delta V_{k+1}^b, \dots, \Delta V_n^b}_{\text{Correct}}\}$$

$$\Rightarrow \quad k = \arg\min_i \overbrace{|\Delta V_i^f - \Delta V_i^b|^2}^{\Phi_i}$$

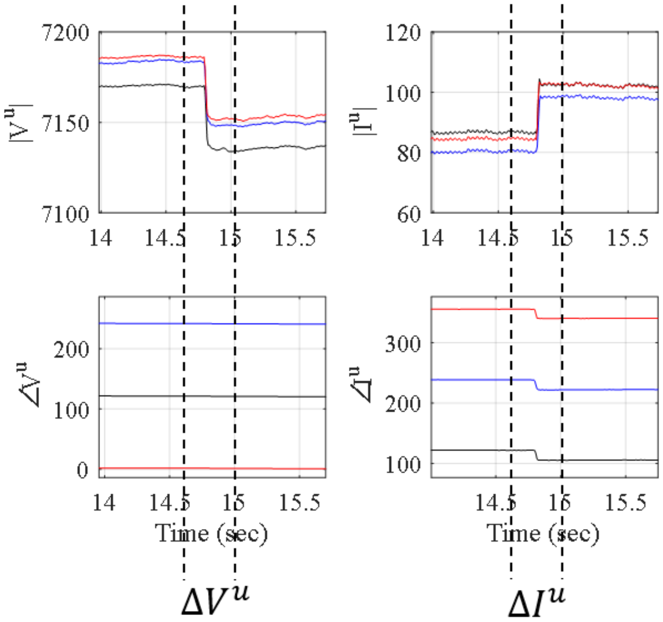


Forward

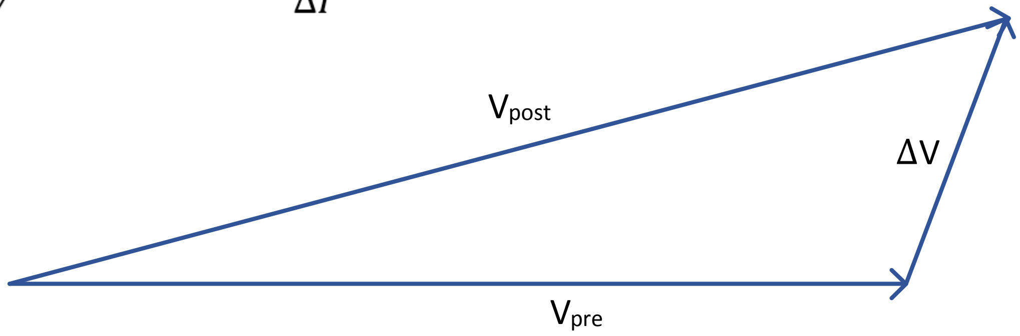
K: Event Bus (Unknown)

Backward

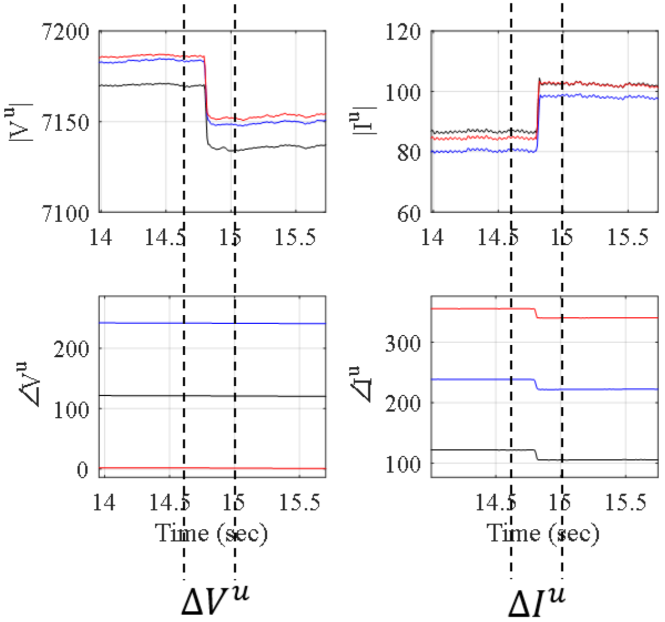
Micro-PMU Measurements



$$\Delta V = V_{post} - V_{pre}$$

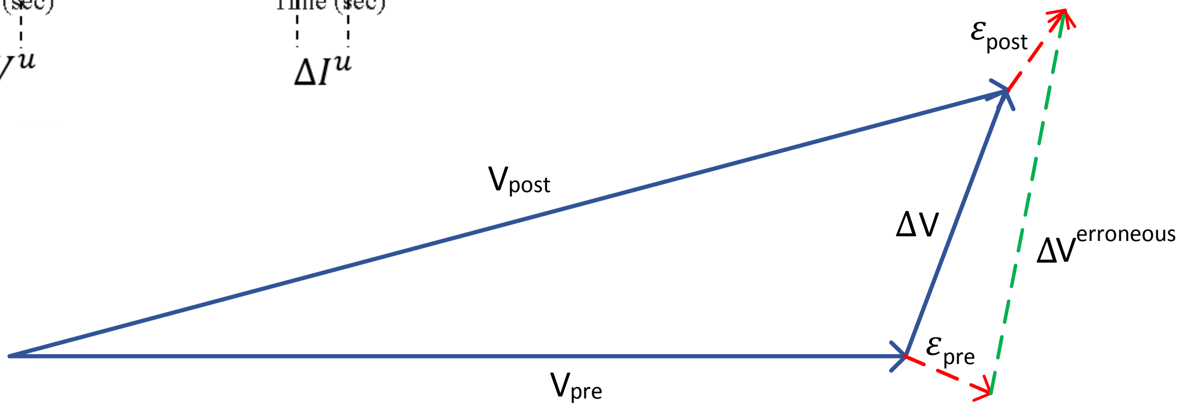


Micro-PMU Measurements

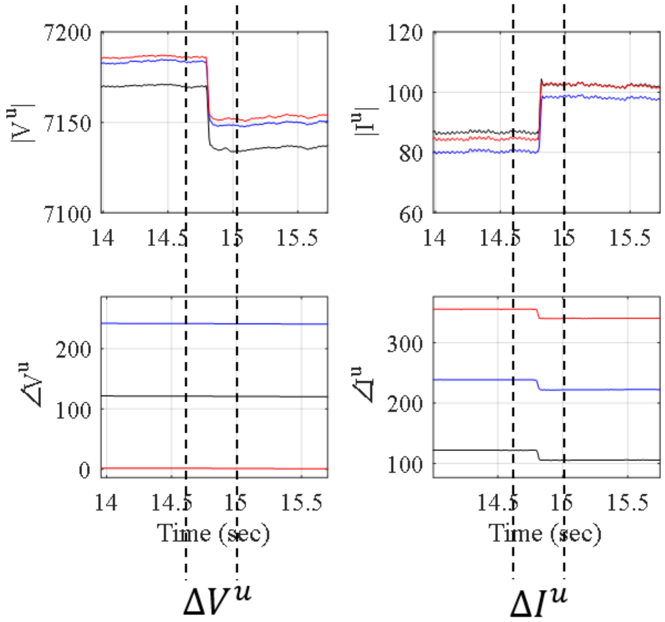


$$\Delta V = V_{post} - V_{pre}$$

$$\Delta V^{erroneous} = V_{post} + \varepsilon_{post} - (V_{pre} + \varepsilon_{pre})$$
$$= \Delta V + (\varepsilon_{post} - \varepsilon_{pre})$$

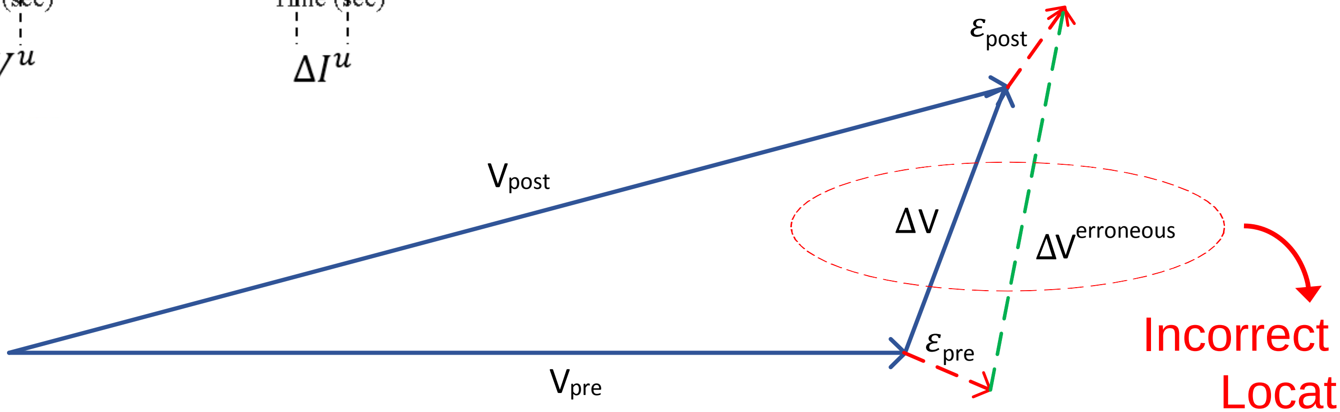


Micro-PMU Measurements



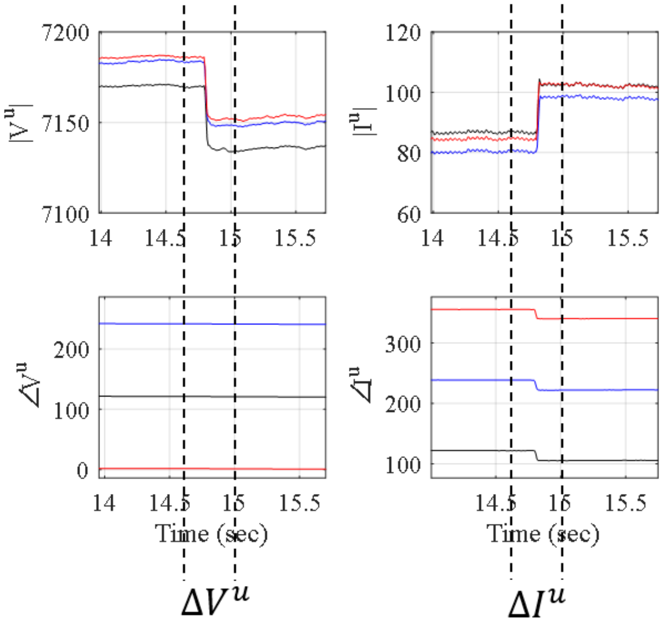
$$\Delta V = V_{post} - V_{pre}$$

$$\Delta V^{erroneous} = V_{post} + \varepsilon_{post} - (V_{pre} + \varepsilon_{pre})$$
$$= \Delta V + (\varepsilon_{post} - \varepsilon_{pre})$$



Incorrect Event Location

Micro-PMU Measurements

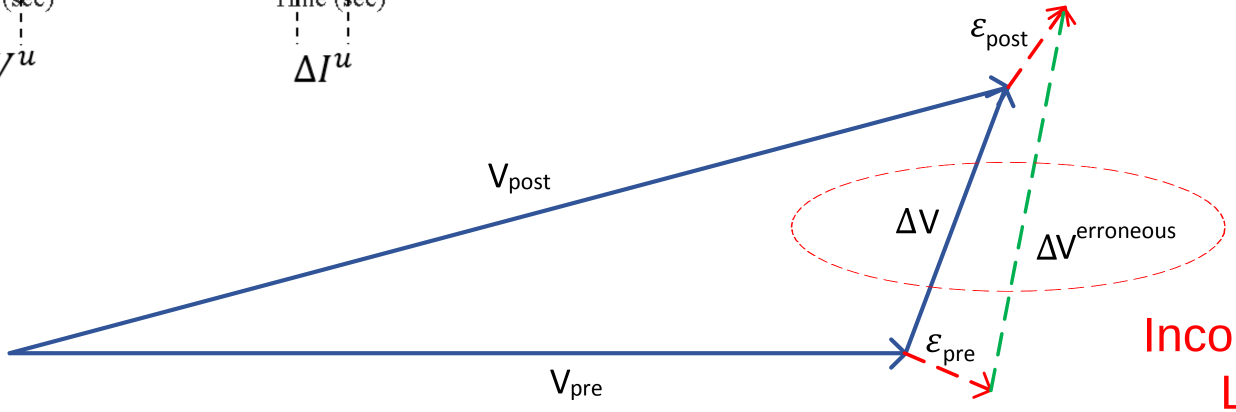


Intentional?

$$\Delta V = V_{post} - V_{pre}$$

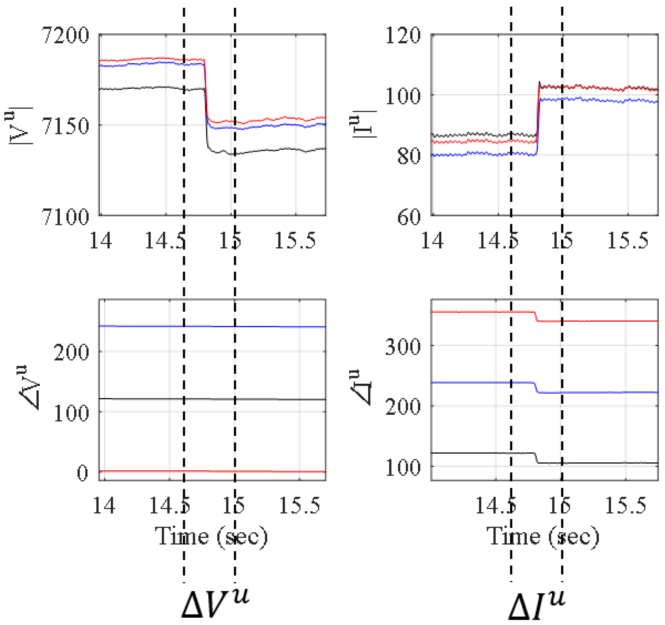
$$\Delta V^{erroneous} = V_{post} + \overbrace{\varepsilon_{post}} - (V_{pre} + \overbrace{\varepsilon_{pre}})$$

$$= \Delta V + (\varepsilon_{post} - \varepsilon_{pre})$$



Incorrect Event Location

Micro-PMU Measurements

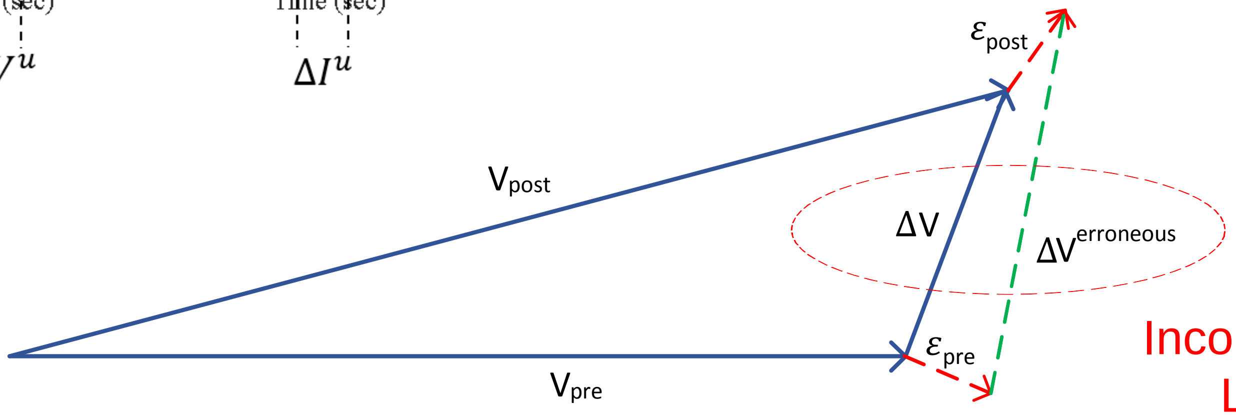


False Data Injection Attack

$$\Delta V = V_{post} - V_{pre}$$

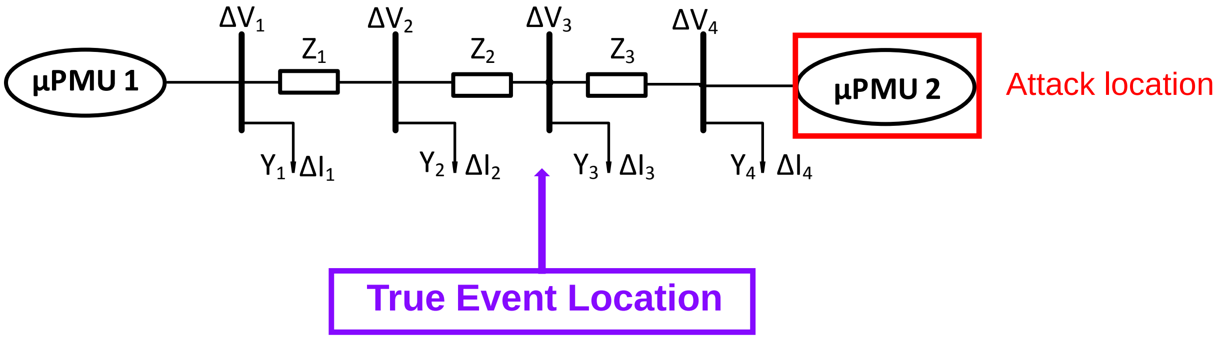
$$\Delta V^{erroneous} = V_{post} + \overbrace{\varepsilon_{post}} - (V_{pre} + \overbrace{\varepsilon_{pre}})$$

$$= \Delta V + (\varepsilon_{post} - \varepsilon_{pre})$$



Incorrect Event Location

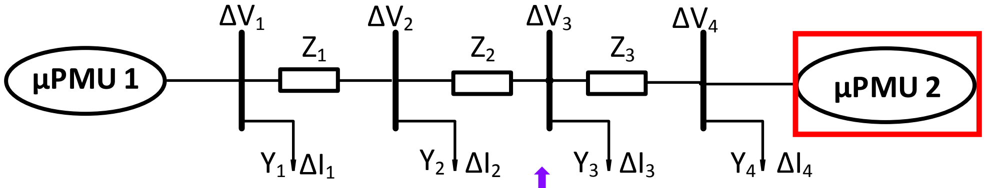
FDIA Against Micro-PMU data



Attack location

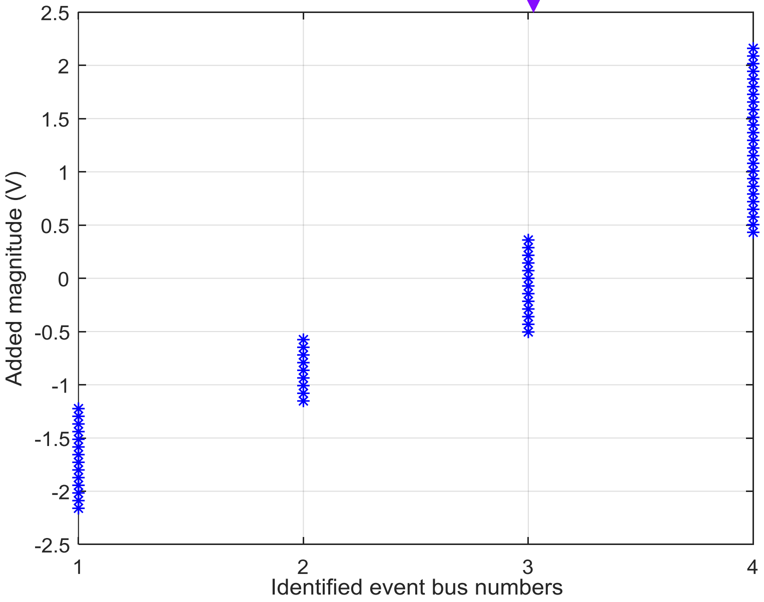
True Event Location

FDIA Against Micro-PMU data

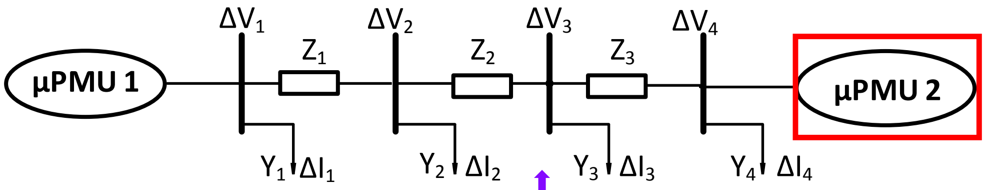


Attack location

True Event Location

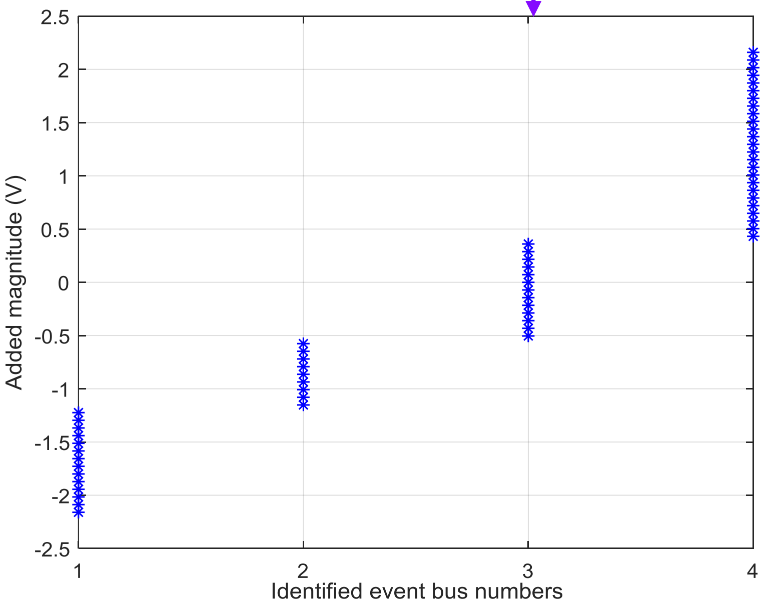


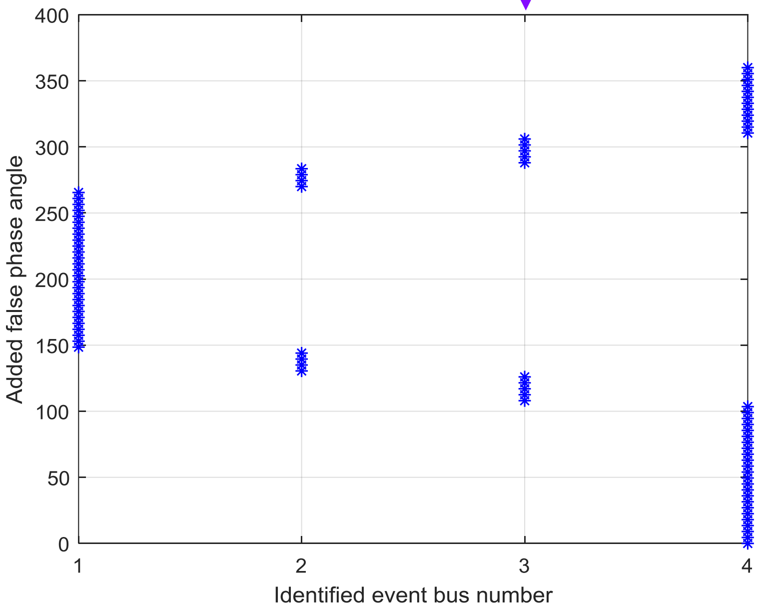
FDIA Against Micro-PMU data



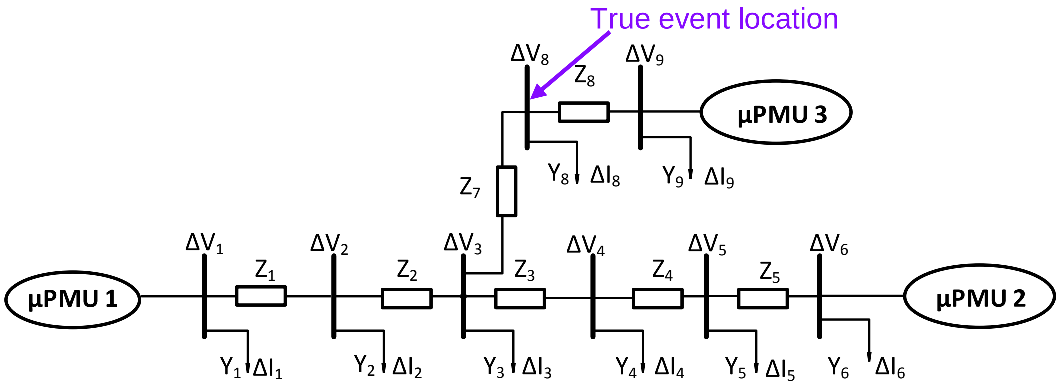
Attack location

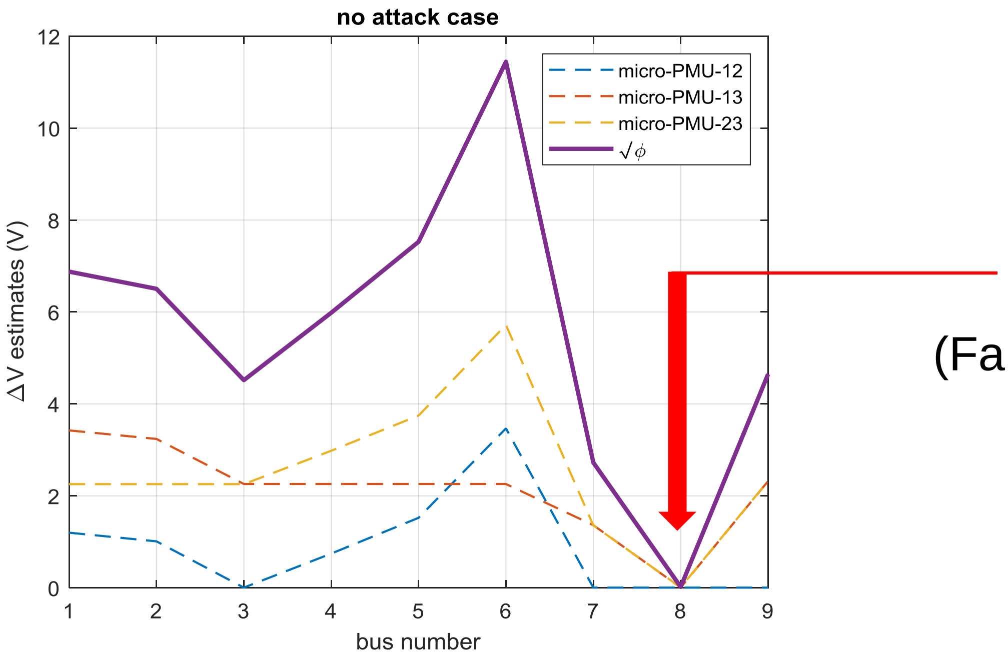
True Event Location





Effects of bad measurements in Micro-PMU data

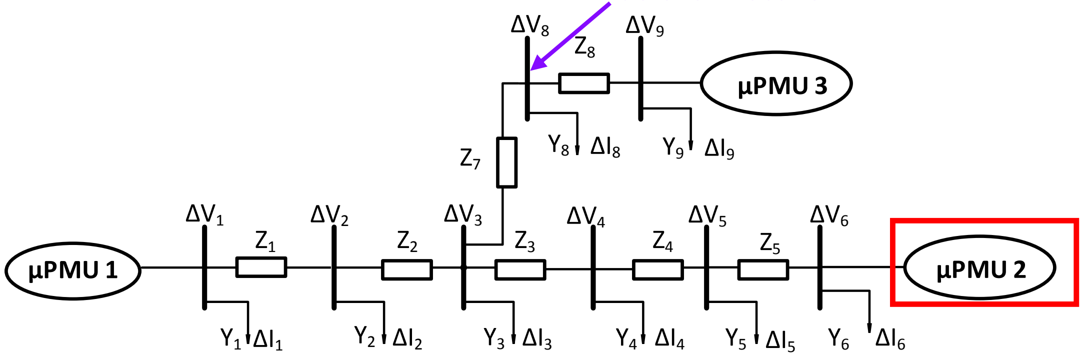




Correct Location

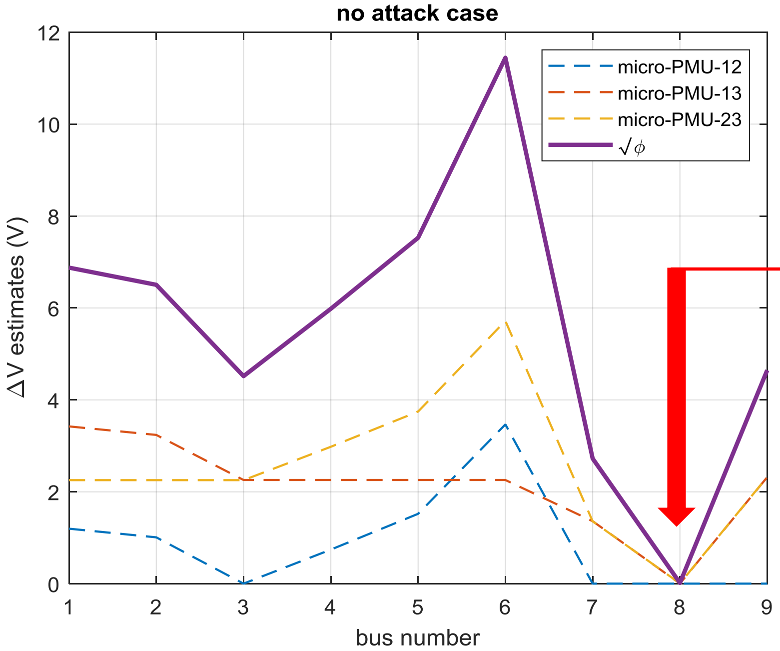
(Farajollahi, et. al. 2018)

Effects of bad measurements in Micro-PMU data



True event location

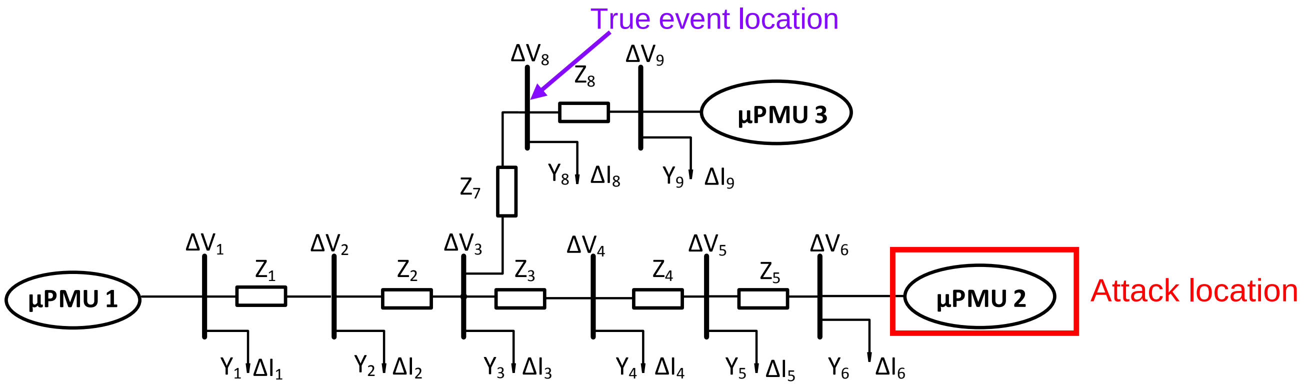
Attack location

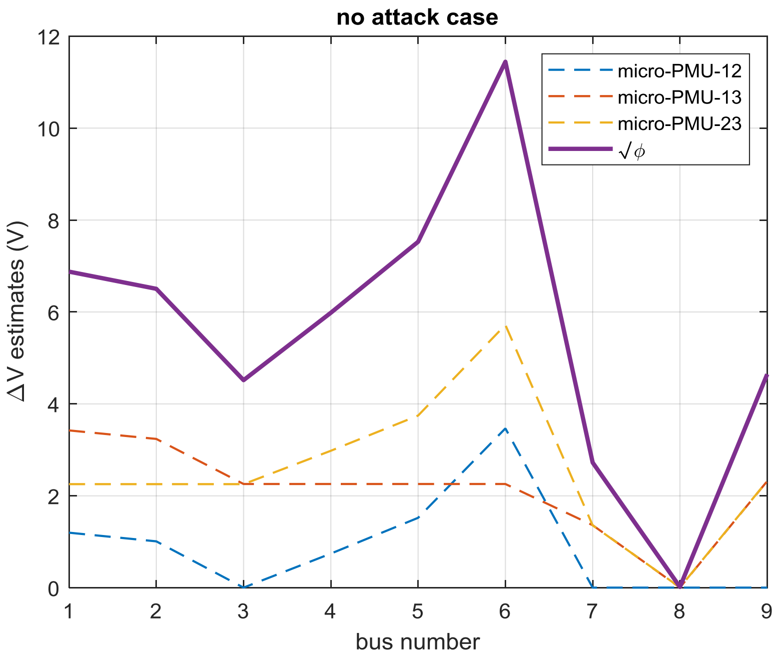


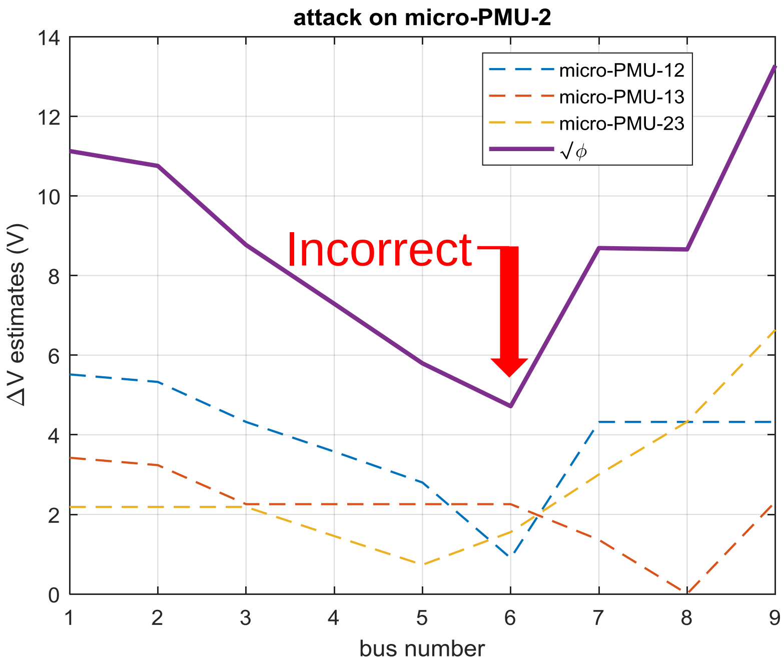
Correct Location

(Farajollahi, et. al. 2018)

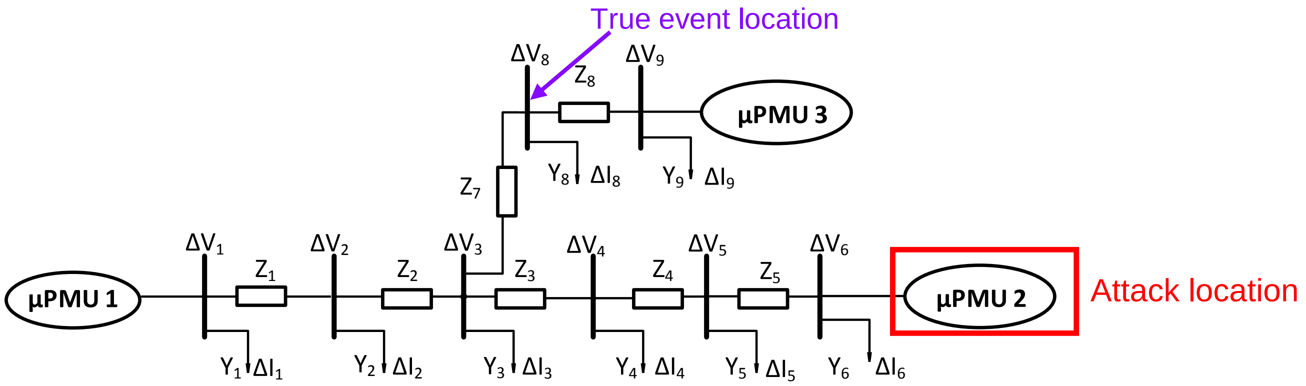
Effects of bad measurements in Micro-PMU data

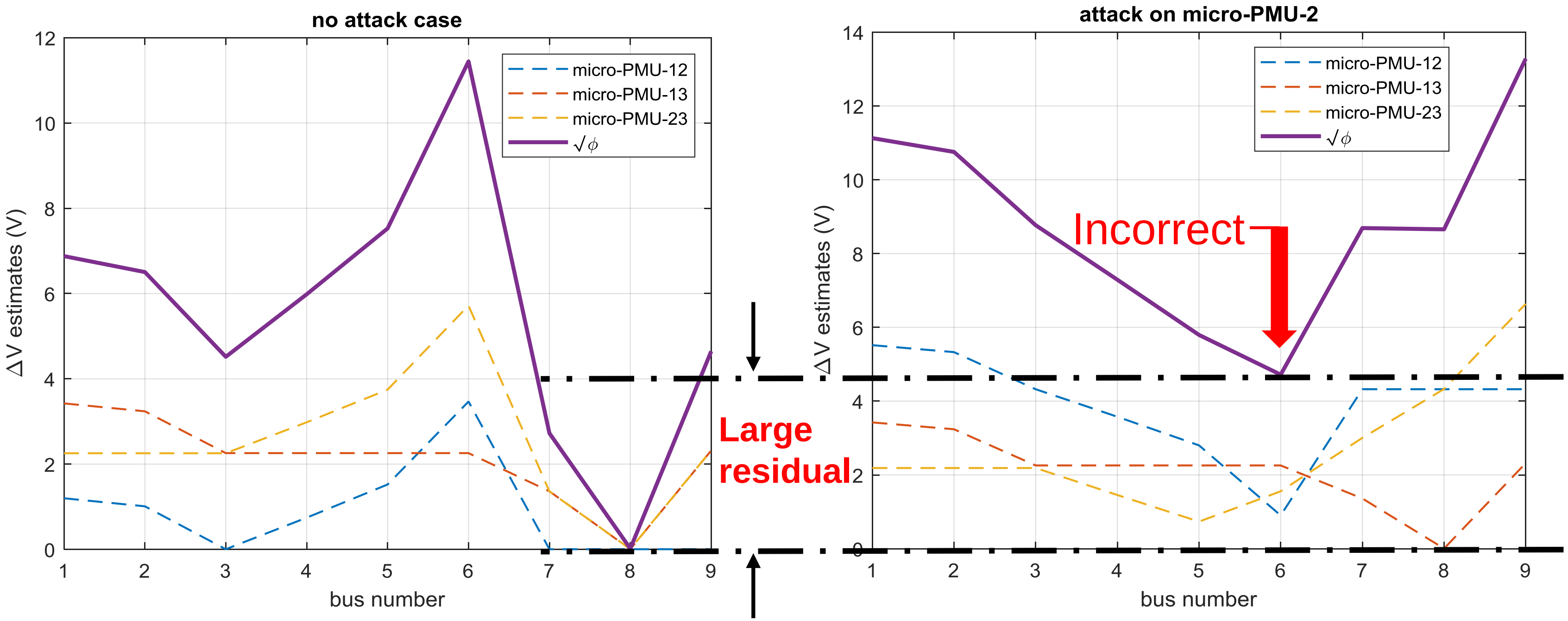




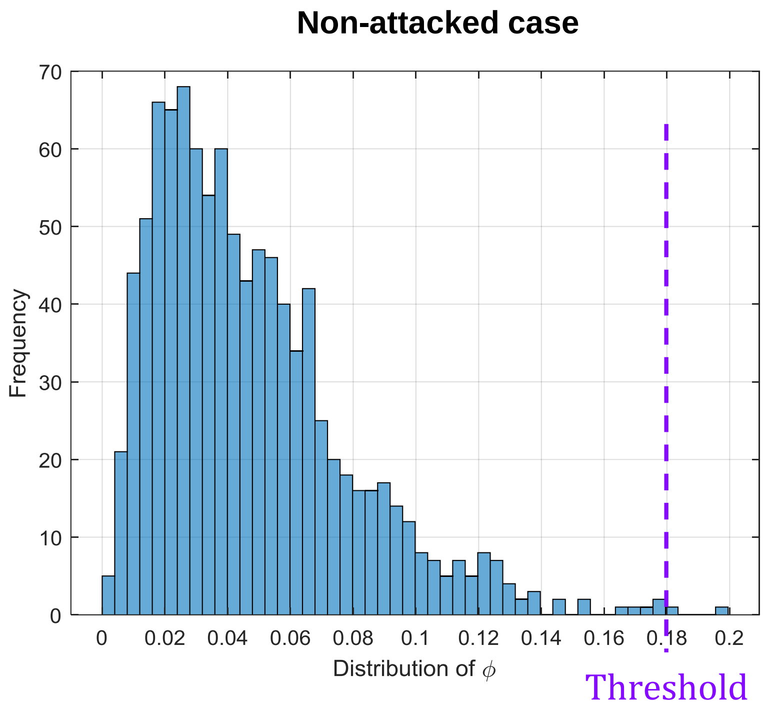


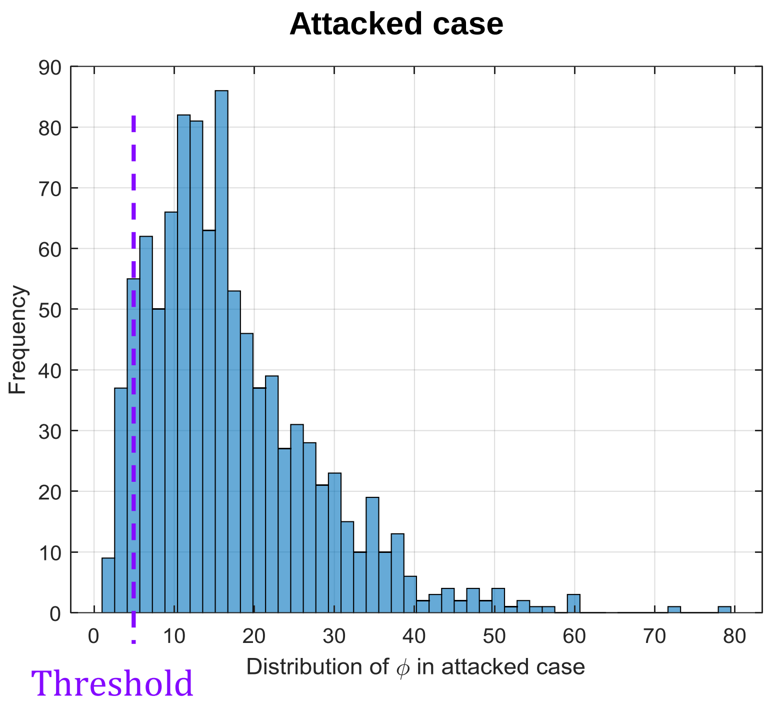
Effects of bad measurements in Micro-PMU data





Proposed Attack Detection Method


Non-attacked case


Attacked case

$$\mathbb{I}(\varphi > \tau) = 1$$

$$prob(\varphi_i > \tau \mid \varphi_i \; is \; chi - squared) = \alpha$$

$$\varphi_i = \; |\Delta V_i^f - \Delta V_i^b|^2$$

Proposed Attack Identification Method

$$arg \min_{j} \quad \frac{1}{N-1}\sum_{j=1}^{N}(\Delta V I_j)^2 - (\frac{1}{N-1}\sum_{j=1}^{N}\Delta V I_j)^2$$

$$subject\ to \ \sum_{j=1}^{N} I_j = N-1$$

$$I_j \in \{1,0\}$$

Where

$$I_j = \begin{cases} 1, & if\ \mu PMU\ j\ is\ kept \\ 0, if\ \mu PMU\ j\ is\ dropped \end{cases}$$

Proposed Attack Identification Method

Variance across measurements in absence of dropped micro-PMU

$$arg\min_{j} \quad \frac{1}{N-1}\sum_{j=1}^{N}(\Delta VI_j)^2 - (\frac{1}{N-1}\sum_{j=1}^{N}\Delta VI_j)^2$$

$$subject\ to\ \sum_{j=1}^{N} I_j = N-1$$

$$I_j \in \{1,0\}$$

Where

$$I_j = \begin{cases} 1, & if\, \mu PMU\, j\ is\ kept \\ 0, if\ \mu PMU\, j\ is\ dropped \end{cases}$$

Proposed Attack Identification Method

$$arg\min_{j} \quad \frac{1}{N-1}\sum_{j=1}^{N}(\Delta VI_j)^2-(\frac{1}{N-1}\sum_{j=1}^{N}\Delta VI_j)^2$$

Variance across measurements in absence of dropped micro-PMU

$$subject\ to \ \sum_{j=1}^{N} I_j = N-1$$

The number of micro-PMUs kept

$$I_j \in \{1,0\}$$

Where

$$I_j = \begin{cases} 1, & if\ \mu PMU\ j\ is\ kept \\ 0, if & \mu PMU\ j\ is\ dropped \end{cases}$$

Proposed Attack Identification Method

$$arg\min_{j} \quad \frac{1}{N-1}\sum_{j=1}^{N}(\Delta V I_j)^2 - (\frac{1}{N-1}\sum_{j=1}^{N}\Delta V I_j)^2$$

Variance across measurements in absence of dropped micro-PMU

$$subject\ to \sum_{j=1}^{N} I_j = N-1$$

The number of micro-PMUs kept

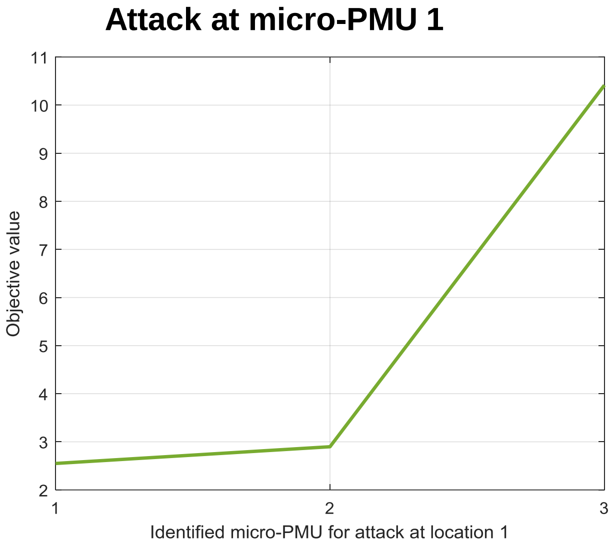
$$I_j \in \{1,0\}$$

Where

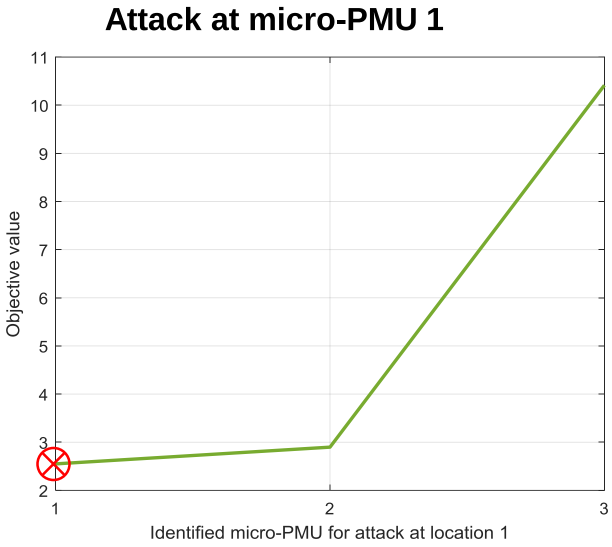
$$I_j = \begin{cases} 1, & if\ \mu PMU\ j\ is\ kept \\ 0, if\ \mu PMU\ j\ is\ dropped \end{cases}$$

Decision Variable

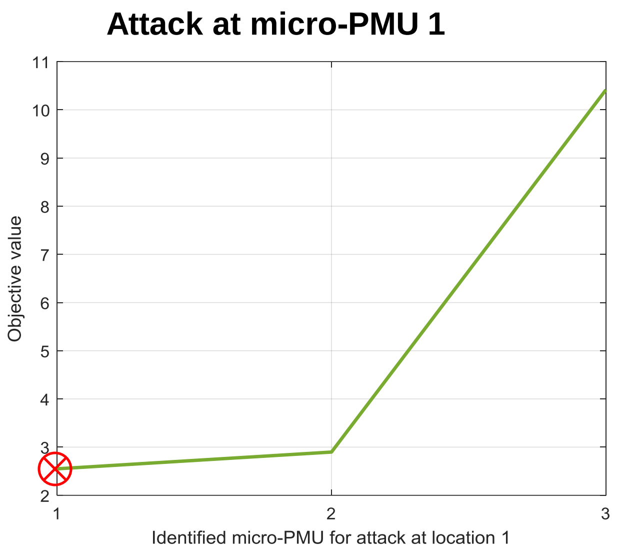
Identified affected μPMU



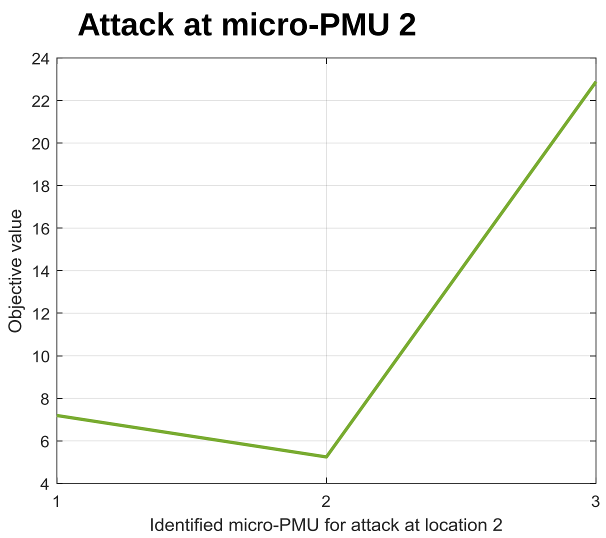
Identified affected μPMU



Identified affected μPMU

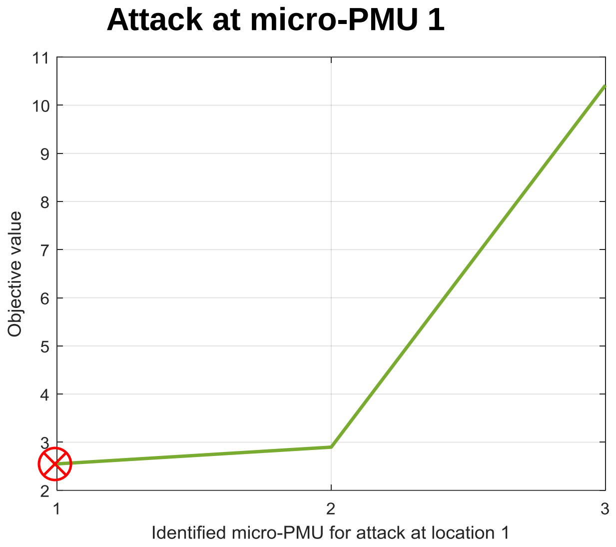


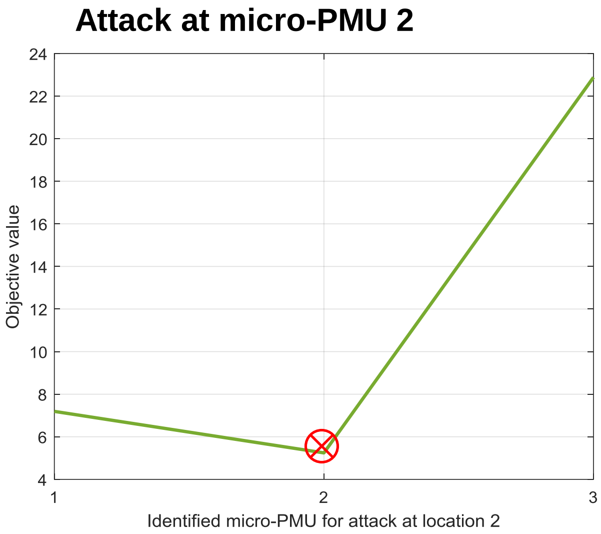
Attack at micro-PMU 1



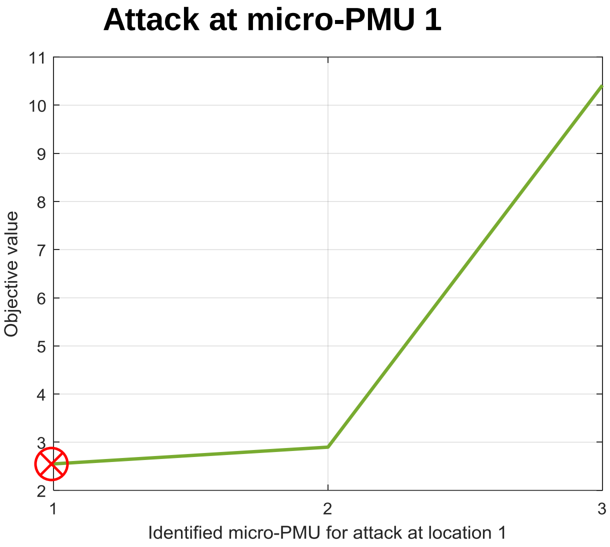
Attack at micro-PMU 2

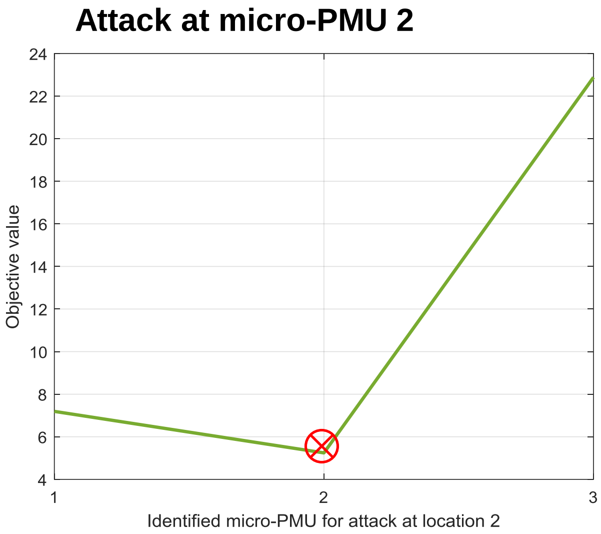
Identified affected µPMU

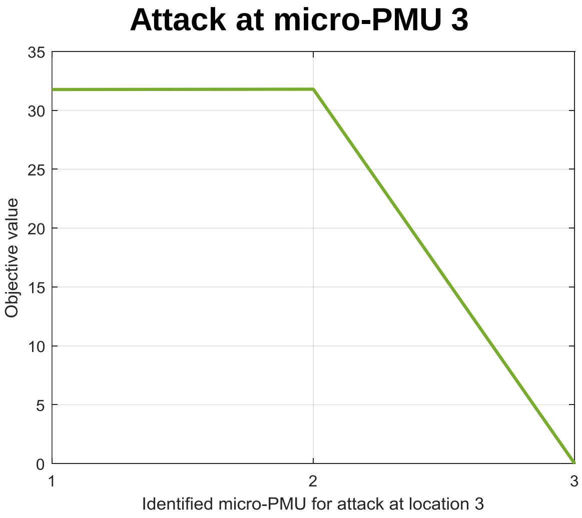




Identified affected μPMU


Attack at micro-PMU 1

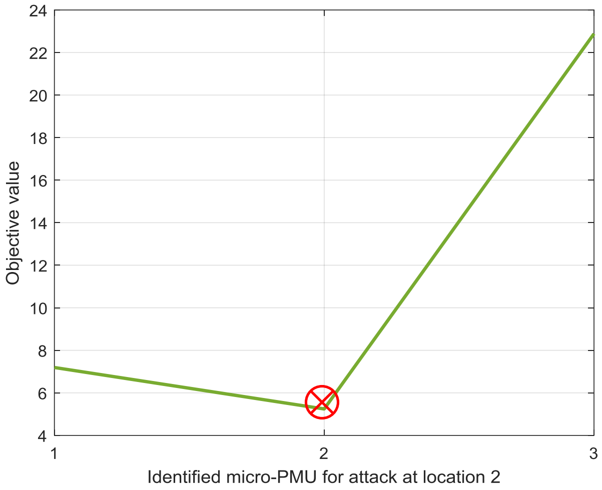

Attack at micro-PMU 2


Attack at micro-PMU 3

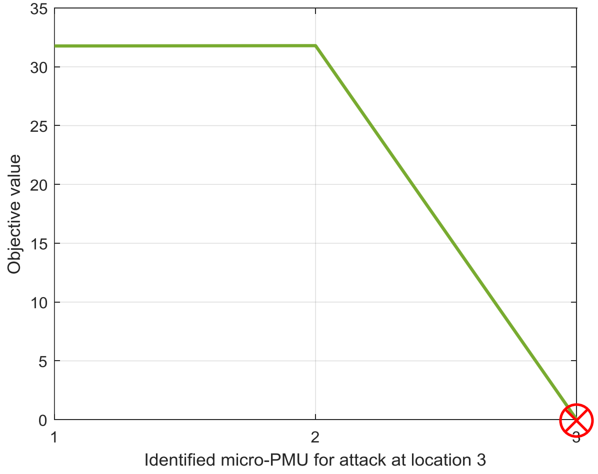
Identified affected μPMU

Attack at micro-PMU 1

Attack at micro-PMU 2



Attack at micro-PMU 3



References

[1] Mohsenian-Rad, Hamed, Emma Stewart, and Ed Cortez. "Distribution synchrophasors: Pairing big data with analytics to create actionable information." IEEE Power and Energy Magazine 16.3 (2018): 26-34.

[2] Farajollahi, Mohammad, et al. "Locating the source of events in power distribution systems using micro-pmu data." IEEE Transactions on Power Systems 33.6 (2018): 6343-6354.

[3] He, Youbiao, Gihan J. Mendis, and Jin Wei. "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism." IEEE Transactions on Smart Grid 8.5 (2017): 2505-2516.

[4] Amini, Sajjad, et al. "Hierarchical Location Identification of Destabilizing Faults and Attacks in Power Systems: A Frequency-Domain Approach." IEEE Transactions on Smart Grid (2017).

[5] R. Deng, P. Zhuang and H. Liang, "False Data Injection Attacks Against State Estimation in Power Distribution Systems," in IEEE Transactions on Smart Grid.

[6] M. Kamal, M. Farajollahi, H. Mohsenian-Rad, “Analysis of Cyber Attacks Against Distribution Synchrophasors: The Case of Event Location Identification,” to be submitted May 2019.

[7] M. Farajollahi, A. Shahsavari, H. Mohsenian-Rad, "Tracking State Estimation in Distribution Networks Using Distribution-level Synchrophasor Data," accepted for publication in IEEE Power & Energy Society General Meeting, Portland, OR, August 2018.

[8] M. Farajollahi, A. Shahsavari and H. Mohsenian-Rad, "Location Identification of Distribution Network Events Using SynchrophasorData" , in Proc. of North American Power Symposium, Morgantown, WV, September 2017.

[9] M. Farajollahi, A. Shahsavari, and H. Mohsenian-Rad, "Location Identification of High Impedance Faults Using Synchronized Harmonic Phasors" in Proc. of the IEEE Power & Energy Society Conference on Innovative Smart Grid Technologies (ISGT), Washington, DC, April 2017.