Physics-Informed Edge-Based Sparse Recovery for Real-Time PMU Data Integrity Attack Resilience

1st Khwrwmdao Basumatary
Dept. Electrical Engineering
Indian Institute of Technology
Jammu, India
Email: 2021ree2029@iitjammu.ac.in

2nd Anup Shukla
Dept. Electrical Engineering
Indian Institute of Technology
Jammu, India
Email: anup.shukla@iitjammu.ac.in

***Abstract*—The growing possibility of data anomalies originating from PMU measurements can significantly affect wide-area protection and control applications. This paper presents a physics-informed, hardware-native sparse recovery framework for reconstructing PMU data anomalies in real-time. The proposed method formulates anomaly detection as a compressed-sensing problem and employs an ℓ_1-minimization–based reconstruction that runs deterministically on a substation-grade automation controller. A physics-informed dynamic subspace enables the algorithm to reject physically inconsistent measurements while preserving actual system dynamics. The approach is validated on an RTDS–SEL hardware testbed under multiple data integrity attacks and across dynamic operating conditions. Experiments on eight PMUs show 96–99.5% reconstruction accuracy, near-zero error, and low computational overhead, making the approach suitable for practical deployment.**

***Index Terms*—Physics-Informed, Compressive sensing, Dantzig selector, PMU, Sparsity, Automation controller**

I. Introduction

Phasor Measurement Units (PMUs) have become a critical sensing backbone of modern power grids, providing high-resolution, time-synchronised measurements that enable wide-area monitoring, protection, and real-time control. Nevertheless, even within dedicated Operational Technology (OT) infrastructures, PMU data streams remain vulnerable to quality degradations, missing data, and cyber-induced integrity attacks [1]. Notable examples of control layer attacks are: Stuxnet malware [2] and a cyberattack on Ukraine's power grid [3]. In substations, Real-Time Automation Controllers (RTACs) and other Intelligent Electronic Devices (IEDs) are utilised for protection and automation tasks [4], serving as the last line of defence against cyber intrusions and the first layer of resilience to contingencies [5]. Embedding cybersecurity solutions within the IED itself is therefore critical to prevent compromised PMU data from propagating into protection automation and control functions executed.

As reported in [6], approximately 10%-30% of PMU measurements in China's transmission grids exhibit data anomalies or missing samples on a daily basis, which significantly degrades the performance of online data-driven monitoring and control methods [7]. The anomaly detection and reconstruction of compromised signals in the literature can be broadly classified into *system-oriented* and *IED-oriented* approaches. Most of the works on data anomaly detection [8], [9], [10], [11] and reconstruction [12], [13], [14], [15], [16], [17] approaches are *system-centric*, executed on external computational resources without data being pulled live from a Phasor Data Concentrator (PDC). In contrast, this paper presents an *IED-oriented* solution in which the reconstruction algorithm is deployed directly on an IEC 61131-3 Structured Text (ST) logic engine–compliant SEL-RTAC acting as a PDC, enabling embedded, real-time reconstruction of compromised synchrophasor data.

Gao *et al.* [12] proposed a nuclear-norm-based matrix completion to reconstruct missing or corrupted PMU measurement frames. References [13], [14] exploit the low-rank structure of Hankel matrices to detect and reconstruct the random outliers in synchrophasor data. Although the above approaches provide superior oscillatory mode extraction and are effective for recovering missing entries in system matrices, they incur significant computational overhead and are unsuitable for practical deployment. To address the compressed sensing and recovery problem [18], references [15], [16], [17] proposed an interface layer based on Robust Principal Component Analysis (RPCA), implemented in MATLAB, which pre-processes vectors of synchrophasor voltage samples to detect malicious measurements and reconstruct the compromised signals. However, the reliance on the *YALL1* MATLAB solver for the ℓ_p–norm ($0 < p \leq 1$) minimisation step introduces significant computational overhead and software dependency, making their RPCA approaches impractical for real-time execution on resource-constrained substation IEDs for practical applications.

Huang *et al.* [5] were the first to implement an *IED-oriented multitagging* defense on an SEL-RTAC, but remain to fuse cyber–physical information for contingency detection. In contrast to [15], [16], [17] and other works that focus mainly on anomaly detection without on-device reconstruction, this paper addresses that gap. It introduces the *first end-to-end*, real-time, physics-informed synchrophasor data reconstruction using a LASSO-inspired Edge-Based Sparse–Low-Rank (EDGE-SLR) framework deployed natively on a substation-grade SEL-RTAC. The proposed EDGE-SLR leverages the inherent low-dimensional power system dynamics, passing through a learned low-rank subspace, to guide the reconstruction process,

979-8-3315-8138-1

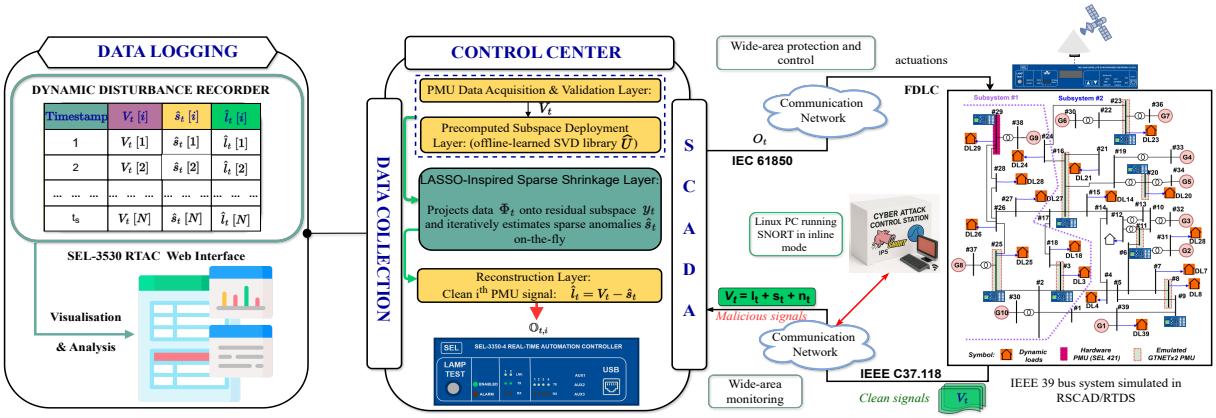

Fig. 1. Proposed real-time edge-embedded sparse recovery framework for anomaly detection and reconstruction of PMU data.

ensuring that only physically inconsistent measurements are treated as anomalous. The sparse-plus-low-rank separation is executed directly within the IEC 61131-3 ST environment, eliminating the need for an external solver and enabling execution on live PMU streams. The feasibility of the proposed approach is demonstrated on a Real-Time Digital Simulator (RTDS)-based testbed with live synchrophasor data streamed to an SEL-RTAC. The method accurately reconstructs the original PMU signal vector from the compromised signal, considering two PMU signals ($\approx 25\%$) are simultaneously compromised.

The remainder of the paper is organised as follows: Section II outlines the proposed architecture; Section III describes the problem formulation and deployment; Section IV presents experimental results; and Section V concludes the paper.

II. Proposed Architecture and System Integration

Figure 1 illustrates the system architecture and integration of the proposed EDGE-SLR framework, enabling practical realisation of attack-resilient synchrophasor data reconstruction at the substation edge. In the proposed framework, a substation-grade automation controller functions as PDC configured to receive high-resolution (20 ms frames/second) streaming synchrophasor (voltage magnitudes) data from remote PMUs deployed at different locations. The proposed EDGE-SLR algorithm operates directly on the streaming voltage magnitudes at the edge controller, eliminating the need for an external preprocessor, as referenced in [15], [16], [17]. Data anomalies in synchrophasor measurements—arising from noise, device failures, communication interruptions, or cyber-induced attacks—are assumed to occur prior to the data being processed by the proposed EDGE-SLR framework.

The following realistic attack types are examined under ambient and dynamic operating conditions:

1) Man-In-The-Middle (MIMT) Attack: An inline SNORT Intrusion Prevention System (IPS) is used to perform protocol-level manipulation of PMU streams.

2) Topology-resembling attack: Archived data segments corresponding to grid events are injected.

3) Data replay attack: Blocks of past PMU data are replayed to the PDC during an $N-1$ generator trip.

4) Data missing entries attack: An inline SNORT IPS injects missing measurements by replacing live PMU frames with Not-a-Number (`NaN`) or zero values before they reach the PDC.

III. Problem Formulation and Sparse Recovery Algorithm Deployment

Let $\mathbf{V}_t = [v_{t,1}, v_{t,2}, \ldots, v_{t,N}]^\top$ denote the high-resolution PMU voltage magnitude vector received at time t. During operations, a set of $\mathbf{V}_t$ streams may contain noise (n_t) and cyber-induced anomalies (s_t). Thus, $\mathbf{V}_t$ signal can be better represented using (1).

$$\mathbf{V}_t := l_t + \mathbf{s}_t + \mathbf{n}_t \tag{1}$$

where $l_t \in \mathbb{R}^{N\times 1}$ is the low-rank dense component, $s_t \in \mathbb{R}^{N\times 1}$ is the sparse anomaly component, and $\mathbf{n}_t \in \mathbb{R}^{N\times 1}$ is small additive noise component.

Therefore, the target here is to detect the corrupted entries and estimate their amplitudes (i.e., the sparse vector (s_t)), at each time instant using an LASSO-based optimisation scheme. We assume that no more than 25% of the PMU channels are compromised at a given time instant, although an individual compromised PMU may exhibit a high percentage of anomalous samples. During normal operation, when there are no anomaly entries and noise, then $\mathbf{V}_t := l_t$.

In the literature, the problem of recovering sparse anomalous samples in s_t is presented as an online RPCA problem using the Recursive Projected Compressed Sensing (ReProCS) approach [15], [16], [17], [19]. Since their work relies on the *YALLI*-ℓ_1 minimisation toolbox [20] and involves iterative convex optimisation with non-deterministic execution time, making them unsuitable for real-time deployment on substation-grade controllers. To make real-time feasible, inspired by the projection step of ReProCS, we replace its computationally expensive Least Squares (LS) support refinement with a *solver-free, fixed-iteration gradient-descent*-based sparse–low-rank reconstruction scheme suitable for deployment on a substation-grade controller.

As detailed in reference [15], [19], for a given training voltage measurements from dynamic event (generation loss), $\mathrm{V}_{\text{train}} = [\mathbf{V}_t\,; 0 < t_s \leq t_{\text{train}}]$ with $\mathbf{V}_t := l_t$, estimate the initial subspace U where l_t lies. Thus, from a training set $\mathrm{V}_{\text{train}} \in \mathbb{R}^{N\times t_s}$ containing N PMU signals (voltage magnitude) of sample length (t_s), we decomposed the $\mathrm{V}_{\text{train}}$ set using Singular Value Decomposition (SVD) as in [15] below.

$$\mathrm{V}_{\text{train}} = \sum_{i=1}^{k_{\text{true}}} \sigma_i\, u_i v_i^T \tag{2}$$

Here, k_{true} denotes the full rank of the data matrix. A reduced subspace $\widehat{U}$ is obtained by retaining the first $k_{\text{approx}} < k_{\text{true}}$ dominant singular vectors that capture at least 95–99% of the total spectral energy, thereby preserving the true system dynamics while suppressing noise present.

Perpendicular Projection onto Subspace: The learned physics-informed subspace $\widehat{U}$ is deployed within the IEC 61131-3 ST controller, and each incoming voltage vector $\mathbf{V}_t$ is projected onto the orthogonal complement of the learned subspace via projection matrix $\Phi_t = \mathbf{I}_N - \widehat{U}\widehat{U}^T$, to get the measurement vector $\mathbf{y}_t$.

$$\mathbf{y}_t := \Phi_t \mathbf{V}_t = \Phi_t(\mathbf{l}_t + \mathbf{s}_t + \mathbf{n}_t) = \Phi_t \mathbf{s}_t + \underbrace{\Phi_t(\mathbf{l}_t + \mathbf{n}_t)}_{\Gamma_t} \tag{3}$$

This equation helps retain the sparse anomaly component s_t and nullifies the contribution from the residual term Γ_t.

Sparse Recovery (s_t): To recover s_t from y_t, unlike [15], [16], [17], [19] which rely on *YALL1*-based ℓ_1-minimisation, we employ LASSO-inspired, a fixed-iteration, iterative thresholding–based gradient shrinkage scheme. This eliminates solver dependency and ensures deterministic execution on IEDs. We solve ℓ_1-minimisation using Dantzig selector [21]:

$$\hat{\mathbf{s}}_t = \min_{\mathbf{x}_t} \|\mathbf{x}_t\|_1 \quad \text{s.t.} \quad \|\mathbf{\Phi}_t^T(\Phi_t \mathbf{x}_t - \mathbf{y}_t)\|_\infty \leq \delta \tag{4}$$

where $\|\cdot\|_1$ promotes sparsity and $\|\cdot\|_\infty$ norm enforces a bound on the maximum projected residual. The noise bound δ is estimated offline from PMU data, following the Dantzig selector formulation [21], which ensures the feasibility of the true signal and stable deployment. Since Φ_t is symmetric ($\Phi_t^\top = \Phi_t$) and idempotent ($\Phi_t^2 = \Phi_t$), the Dantzig–selector residual satisfies: $\Phi_t^\top(\,\Phi_t \mathrm{x}_t - \mathrm{y}_t\,) = \Phi_t\big(\Phi_t \mathrm{x}_t - \mathrm{y}_t\big)$.

Iterative Gradient Descent Steps: During sparse recovery, the descent variable $\mathbf{x}_t^{(h)}$ is iteratively updated, initialised with $\mathbf{x}_t^{(0)} = \mathbf{y}_t$. At each iteration h, the update direction is computed as a *smooth-approximation* of the ℓ_1-subgradient as (5). A tentative update is then formed as $\mathbf{z}_t^{(h)} := \mathbf{x}_t^{(h)} + \gamma_h \odot \mathbf{d}_t^{(h)}$; where γ_h denotes the step size.

$$\mathbf{d}_t^{(h)} := -\frac{\mathbf{x}_t^{(h)}}{|\mathbf{x}_t^h| + \epsilon} \approx -\operatorname{sign}(\mathbf{x}_t^{(h)}) \tag{5}$$

To enforce the Dantzig feasibility constraint, the algorithm computes the first residual: $\mathbf{r}_{1,t}^{(h)} := (\Phi_t \mathbf{z}_t^{(h)} - \mathbf{y}_t)$, and, exploiting the fact that: $\Phi_t := \Phi_t^\top := \Phi_t^2$, if the projected residual: $\mathbf{r}_{2,t}^{(h)} = \Phi_t \mathbf{r}_{1,t}^{(h)}$ is $\geq \delta$, then a diagonal correction is applied in (6), otherwise $x_t^{(h+1)} = z_t^{(h)}$.

$$\mathrm{x}_t^{(h+1)} = z_t^{(h)} - \big(\mathbf{r}_{2,t}^{(h)} - \operatorname{sign}(\mathbf{r}_{2,t}^{(h)})\,\delta\big) \odot \Phi_t \tag{6}$$

This update ensures that each iterate satisfies the Dantzig constraint $\|\Phi_t^\top(\Phi_t \mathrm{x}_t - \mathrm{y}_t)\|_\infty \leq \delta$ while preserving the sparsity-promoting behaviour of the ℓ_1-minimisation.

Recover ($\hat{l}_t$): Once h_{max} descent iterations completes, the anomalous presence is estimated as $\hat{\mathbf{s}}_t \approx \mathbf{x}_t^{(h+1)}$. Using the $\hat{s}_t$ estimate, $\hat{l}_t$ is estimated as $\hat{l}_t := \mathbf{V}_t - \hat{s}_t$. Once the $\hat{s}_t$ is accurately estimated, so $\hat{l}_t$ will. This recovery procedure is executed at every time step in a substation-grade controller.

Proposed Algorithm: In contrast to [15], [16], [17] (*YALL1-based*), and following [19], we propose a physics-informed, LASSO-inspired EDGE-SLR algorithm for detecting anomalous synchrophasor streaming data *on-the-fly*. The procedure for recovering a clean signal vector from the compromised signal is detailed in Algorithm 1.

Algorithm 1: Proposed LASSO-Inspired EDGE-SLR

Input: Streaming PMU voltage vector $\mathbf{V}_t \in \mathbb{R}^N$; **Output:** $\hat{s}_t$, $\hat{l}_t$
Data: Apply SVD on $\mathbf{V}_{train}$ to obtain U and $\sum$; Choose subspace approximate: $\widehat{U} \in \mathbb{R}^{N\times k_{\text{approx}}}$

Parameter: $\epsilon, h_{\max}, \gamma_h, k_{approx}(k)$; **Variables:** h, **med**$(\cdot)$, RealArr[], L, i, j, `Clock_tick`

for $i = 1$ **to** N **do**
  Validate: isValid[i] := fun_IsValidReal($\mathbf{V}_t[i]$);
  Set the initial support $\hat{l}_{t-1}[i], \Phi[i,j], y_t[i], \mathbf{r}_{1,t}^{(h)}[i], \mathbf{r}_{2,t}^{(h)}[i], \mathbf{r}_{2,t}^{(\pm)} := [\cdot]$.
For each isValid[i] := **TRUE** Count L := L + 1; Store RealArr[L] := $\mathbf{V}_t[i]$; Sort fun_SortReal(`ADR(RealArr), L`)
Compute median of valid entries as **med**$(\cdot)$:= `RealArr`$(\cdot)$; For each isValid[i] := **FALSE** perform $\mathbf{V}_t[i]$:= **med**$(\cdot)$
for $i = 1$ **to** N **do**
  for $j = 1$ **to** N **do**
    for $i = 1$ **to** k **do** $\Phi_t[i,j] := \Phi_t[i,j] - (\hat{U}[i,k]) \cdot \hat{U}[j,k]$;
    if $i = j$ **then** $\Phi_t[i,j] := \Phi_t[i,j] + 1$;
if `Clock_tick` **then**
  for $i = 1$ **to** N **do**
    for $j = 1$ **to** N **do** $\mathbf{y}_t[i] := \mathbf{y}_t[i] + \Phi_t[i,j] \cdot \mathbf{V}_t[j]$;
    Initialised $\mathbf{x}_t^{(h)}[i] := \mathbf{y}_t[i]$;
  while $h < h_{\max}$ **do**
    for $i = 1$ **to** N **do**
      $\mathbf{x}_t^{(h)}[i] := \mathbf{z}_t^{(h)}[i]$; $\mathbf{r}_{1,t}^{(h)}[i] := \mathbf{r}_{1,t}^{(h)}[i] - \mathbf{y}_t[i]$;
      $\mathbf{d}_t^{(h)} := \frac{-\mathbf{x}_t^{(h)}}{|\mathbf{x}_t^{(h)}[i]|+\epsilon}$;$\mathbf{r}_{2,t}^{(\pm)} :=$ $\operatorname{sign}(\mathbf{r}_{2,t}^{(h)}[i])$;$\mathbf{z}_t^{(h)}[i] := \mathbf{x}_t^{(h)}[i] + \gamma_h \cdot \mathbf{d}_t^{(h)}[i]$;
      for $j = 1$ **to** N **do** $\mathbf{r}_{1,t}^{(h)}[i] := \mathbf{r}_{1,t}^{(h)}[i] + \Phi_t[i,j] \cdot$ $\mathbf{z}_t^{(h)}[j]$; $\mathbf{r}_{2,t}^{(h)}[i] := \mathbf{r}_{2,t}^{(h)}[i] + \Phi_t[i,j] \cdot \mathbf{r}_{1,t}^{(h)}[j]$;
      if $|\mathbf{r}_{2,t}^{(h)}[i]| \geq \delta$ **then**
        $\mathbf{x}_t^{(h)}[i] := \mathbf{x}_t^{(h)}[i] - (\mathbf{r}_{2,t}^{(h)}[i] - \mathbf{r}_{2,t}^{(\pm)} \cdot \delta) \cdot \Phi[i,i]$;
    Next iteration $h := h + 1$;
Estimate $\hat{s}_t[i] := \mathbf{x}_t^{(h)}[i]$; Recover $\hat{l}_t[i] := \mathbf{V}_t[i] - \hat{s}_t[i]$, Save for next iteration $\hat{l}_{t-1}[i] := \hat{l}_t[i]$

IV. Evaluation: Test System and Use Cases

To realise the proposed EDGE-SLR and its effectiveness, the IEEE-39 bus network is considered, and a total of eight

PMUs ($N = 8$), including a SEL-421-4 relay, have been deployed across the network as reported in reference [22], as shown in Figure 1. In the experimental setup, eight synchronised voltage magnitude measurements, sampled at a reporting rate of 50 frames per second, are streamed to the SEL-3530 RTAC. The incoming signals are *de-trended* prior to entering the sparse-recovery algorithm to remove steady-state biases. An N–1 generation trip event (825 MW) is simulated to generate raw training data comprising approximately 4792 samples. A Singular Value Decomposition (SVD) is then applied to extract a physics-informed dynamic training subspace $\hat{U}$, which provides a low-rank approximation of the raw data. The tuned parameter values used in the implementation are: $\epsilon = 10^{-4}$, $h_{\max} = 10$, $\gamma_h = 0.005$, and $k_{\text{approx}} = 3$. To evaluate robustness, two PMU signals are deliberately compromised, and their reconstructions under ambient and dynamic operating conditions are obtained following Algorithm 1. Reconstruction accuracy is computed from the reduction in Root Mean Squared Error (RMSE) between the original–compromised and original–reconstructed signals. Accuracy is first computed per PMU using RMSE reduction, and the global accuracy is obtained by averaging across all $N = 8$ PMUs.

For brevity, only representative reconstruction results are illustrated; however, the proposed framework is applicable across a wide range of operational and attack scenarios.

1) Ambient Condition: To mimic real-world ambient variability, Gaussian noise with SNR = 1 and zero mean is added to the three-phase voltage inputs of PMU 1 and PMU 5. Under ambient conditions, two use cases are presented to evaluate the performance of the proposed algorithm.

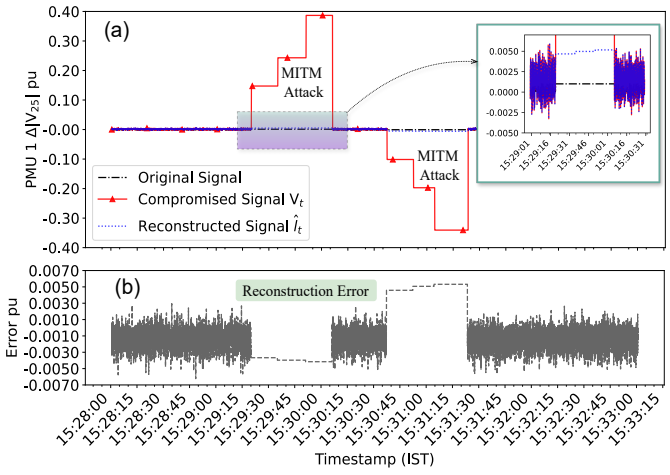

Fig. 2. Case-I: Correlated MITM attack via SNORT IPS on PMU 1 and PMU 5: (a) reconstruction profile, and (b) reconstruction error.

MITM Attack (Case I): Figure 2 shows the parameter-manipulation (MITM) attack injected via SNORT IPS *inline mode* in PMU 1 voltage magnitude $|V_{25}|$ signal. The attack consists of an upward distortion from 15:29:20 to 15:30:06 (2300 samples at 50 fps) followed by a downward distortion from 15:30:37 to 15:31:24 (2350 samples). Only the deviations in the voltage magnitudes from the nominal condition have been shown. Figure 2 (b) shows the degree of reconstruction error, i.e., measured by subtracting the compromised signal from the original signal. The error remains close to zero, except for bounded shifts during attack periods, which demonstrates very good reconstruction in real-time at the SEL-3530 RTAC. Overall, it is observed that the EDGE-SLR method achieves a reconstruction accuracy of 99.52%. PMU-1 and PMU 5 – the only affected devices – achieved 98% and 98.29% accuracy, respectively.

Topology Resembling Attack (Case II): Figure 3 shows the grid-topology–resembling (generator-trip) attack—mimicking the 825-MW G9 trip—applied to the PMU-5 voltage magnitude $|V_{11}|$, occurring from 16:13:49 to 16:14:28 (1950 samples). Despite the large attack magnitude, the proposed algorithm effectively learns the underlying system dynamics and rejects the injected artificial disturbance, as evidenced by the near-zero reconstruction error shown in Figure 3(b). Under

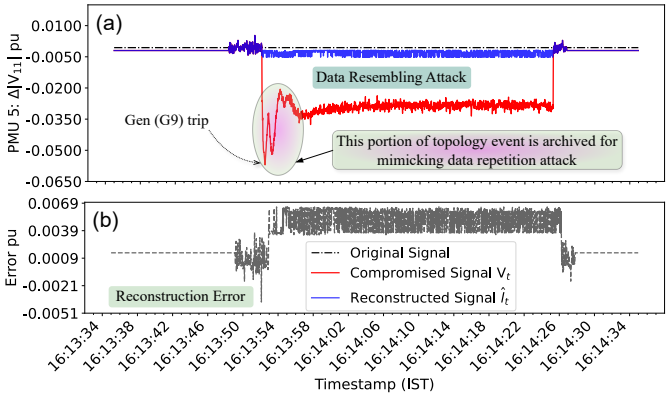

Fig. 3. Case-II: Correlated data resembling attack on PMU 1 and PMU 5: (a) reconstruction profile, and (b) reconstruction error.

ambient conditions with a data-resembling attack, the overall reconstruction accuracy remained high at 96.32%. The two targeted devices—PMU 1 and PMU 5 achieved reconstruction accuracies of 81.19% and 89.42%, respectively.

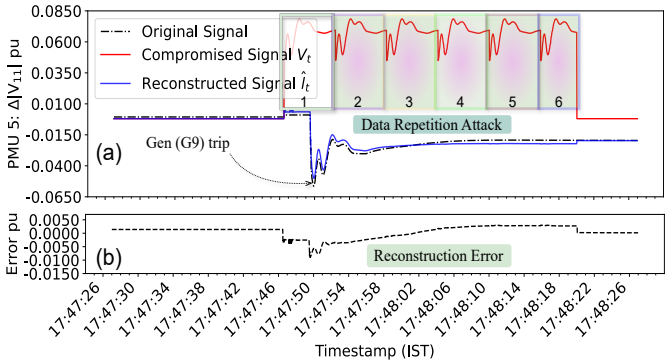

Fig. 4. Case-III: Correlated data repetition attack on PMU 1 and PMU 5: (a) reconstruction profile, and (b) reconstruction error.

2) Dynamic Condition: A dynamic disturbance is emulated by initiating an N–1 contingency in which the 825 MW generator (G9) at Bus 29 is tripped. Two representative attack

use cases are presented under this condition to evaluate the performance of the proposed algorithm.

Data Repetition Attack (Case III): In this case, an archived segment of data—shown in Figure 3—was repeated six times and injected into the PMU-5 voltage-magnitude signal $|V_{11}|$ to mimic the data repetition attack as illustrated in Figure 4. Even though the repeated sequence was inverted relative to the original data to induce a large deviation, the proposed algorithm still tracks the underlying physical system dynamics, resulting in near-zero reconstruction error, as shown in Figure 4(b). Under dynamic operating conditions and in the presence of this data-repetition attack, the proposed method achieved an overall reconstruction accuracy of 97.21%, with the two affected PMUs—PMU 1 and PMU 5—achieving accuracies of 81.11% and 96.64%, respectively.

Data-Missing Attack (Case IV): During the dynamic event, $|V_{11}|$ was compromised via SNORT IPS by injecting NaN and zero samples, producing the *green dashed* missing-data gaps shown in Figure 5. The algorithm's resiliency under missing data—with near-zero reconstruction error—is illustrated in Figure 5(b).

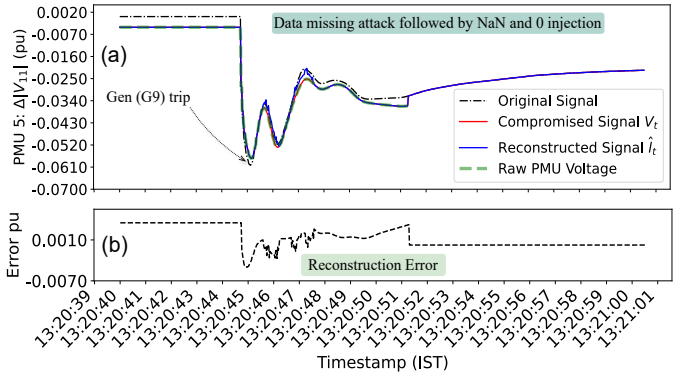

Fig. 5. Case-IV: Correlated data missing attack on PMU 1 and PMU 5: (a) reconstruction profile, and (b) reconstruction error.

Remarks on Memory Footprint: On the SEL-3530 RTAC, the algorithm ran at a 20 ms cycle using only 27% CPU and 215 MB RAM (29%). This demonstrates that the anomaly-detection and sparse-recovery pipeline operates effectively within device limits, leaving ample headroom for real-time deployment.

V. Conclusion

This work presented a physics-informed, LASSO-inspired sparse-recovery algorithm deployed natively on an SEL-3530 RTAC for real-time PMU data anomaly reconstruction. Hardware-in-the-loop evaluations under multiple data integrity attack scenarios showed near-zero reconstruction error and 96–99.5% accuracy across the PMU signals, including under dynamic grid events. The algorithm's fixed-iteration and solver-free designs ensure deterministic execution on SEL-RTAC, with a memory footprint of 27% CPU and 215 MB RAM, making it suitable for practical deployment in control centres, which can significantly enhance cyber-physical resilience in wide-area monitoring and control applications.

Future work will explore advanced sparse-recovery formulations to improve performance and extend the framework to jointly reconstruct multi-domain PMU measurements.

References

[1] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, "Cyber security impacts on all-pmu state estimator-a case study on co-simulation platform geco," in *2012 IEEE third international conference on smart grid communications (SmartGridComm)*. IEEE, 2012, pp. 587–592.

[2] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE security & privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[3] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity information sharing and analysis center (E-ISAC)*, vol. 388, no. 1-29, p. 3, 2016.

[4] Basumatary et al, "Real-time controller hardware-in-the-loop cyber physical testbed using iec 61850 goose protocol," in *2024 IEEE PowerCon*, 2024, pp. 1–5.

[5] H. Huang, P. Wlazlo, Z. Mao, A. Sahu, K. Davis, A. Goulart, S. Zonouz, and C. M. Davis, "Cyberattack defense with cyber-physical alert and control logic in industrial controllers," *IEEE Transactions on Industry Applications*, vol. 58, no. 5, pp. 5921–5934, 2022.

[6] L. Zhu and D. J. Hill, "Cost-effective bad synchrophasor data detection based on unsupervised time-series data analytic," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2027–2039, 2020.

[7] B. Tan, J. Yang, T. Zhou, X. Zhan, Y. Liu, S. Jiang, and C. Luo, "Spatial-temporal adaptive transient stability assessment for power system under missing data," *International Journal of Electrical Power & Energy Systems*, vol. 123, p. 106237, 2020.

[8] Cai et al., "Ics anomaly detection based on sensor patterns and actuator rules in spatiotemporal dependency," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 8, pp. 10 647–10 656, 2024.

[9] M. Zhou, Y. Wang, A. K. Srivastava, Y. Wu, and P. Banerjee, "Ensemble-based algorithm for synchrophasor data anomaly detection," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2979–2988, 2018.

[10] Ganjkhani et al., "Integrated cyber and physical anomaly location and classification in power distribution systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7040–7049, 2021.

[11] Zhang et al., "Spatio-temporal correlation-based false data injection attack detection using deep convolutional neural network," *IEEE transactions on smart grid*, vol. 13, no. 1, pp. 750–761, 2021.

[12] P. Gao, R. Wang, M. Wang, and J. H. Chow, "Low-rank matrix recovery from noisy, quantized, and erroneous measurements," *IEEE Transactions on Signal Processing*, vol. 66, no. 11, pp. 2918–2932, 2018.

[13] Y. Hao, M. Wang, and J. H. Chow, "Modeless streaming synchrophasor data recovery in nonlinear systems," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1166–1177, 2019.

[14] S. Zhang, Y. Hao, M. Wang, and J. H. Chow, "Multi-channel missing data recovery by exploiting the low-rank hankel structures," in *2017 IEEE 7th International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)*, 2017, pp. 1–5.

[15] K. Mahapatra and N. R. Chaudhuri, "Malicious corruption-resilient wide-area oscillation monitoring using online robust pca," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*, 2018, pp. 1–5.

[16] K. Mahapatra, M. Ashour, N. R. Chaudhuri, and C. M. Lagoa, "Malicious corruption resilience in pmu data and wide-area damping control," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 958–967, 2019.

[17] K. Mahapatra and N. R. Chaudhuri, "Online robust pca for malicious attack-resilience in wide-area mode metering application," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 2598–2610, 2019.

[18] R. Tibshirani, "Regression shrinkage and selection via the lasso: a retrospective," *Journal of the Royal Statistical Society Series B: Statistical Methodology*, vol. 73, no. 3, pp. 273–282, 2011.

[19] H. Guo, C. Qiu, and N. Vaswani, "An online algorithm for separating sparse and low-dimensional signal sequences from their sum," *IEEE Transactions on Signal Processing*, vol. 62, no. 16, pp. 4284–4297, 2014.

[20] J. Yang and Y. Zhang, "Alternating direction algorithms for \ell_1-problems in compressive sensing," *SIAM journal on scientific computing*, vol. 33, no. 1, pp. 250–278, 2011.

[21] E. J. Candes, M. B. Wakin, and S. P. Boyd, "Enhancing sparsity by reweighted ℓ_1 minimization," *Journal of Fourier analysis and applications*, vol. 14, no. 5, pp. 877–905, 2008.

[22] Aminifar et al., "Contingency-Constrained PMU Placement in Power Networks," *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 516–523, 2010.