Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

Model-Agnostic Semantics in Shipboard Systems Against Data Availability Attacks

Gupta, Kirti; Sahoo, Subham; Panigrahi, Bijaya Ketan

Published in:
IEEE Transactions on Circuits and Systems - II - Express Briefs

DOI (link to publication from Publisher):
10.1109/TCSII.2024.3382645

Creative Commons License
CC BY 4.0

Publication date:
2025

Document Version
Accepted author manuscript, peer reviewed version

Link to publication from Aalborg University

Citation for published version (APA):
Gupta, K., Sahoo, S., & Panigrahi, B. K. (2025). Model-Agnostic Semantics in Shipboard Systems Against Data Availability Attacks. *IEEE Transactions on Circuits and Systems - II - Express Briefs*, 1. Advance online publication. https://doi.org/10.1109/TCSII.2024.3382645

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from vbn.aau.dk on: February 08, 2025

Model-Agnostic Semantics in Shipboard Systems Against Data Availability Attacks

Kirti Gupta, Subham Sahoo, *Senior Member, IEEE*, and Bijaya Ketan Panigrahi, *Fellow, IEEE*

***Abstract*—Data availability attacks, such as latency attacks, data dropouts and time synchronization attacks (TSAs) still remain a prime concern not only at the network level but also impair the control system performance & stability of the physical layer in medium voltage DC (MVDC) shipboard power systems (SPSs). To address its impact on the physical layer, we equip a model-agnostic semantic architecture that can compensate using *process-aware* delay compensation capabilities. Unlike traditional model predictive controllers (MPCs) with a limited prediction horizon, the proposed architecture offers long event-driven prediction even during large random delayed measurements. The *semantic prediction policy* is governed using the inner control loop dynamics of power generation modules (PGMs) to provide reconstructed signals for delay compensation. Its robustness has been extensively tested and validated on nominal 12 kV two-zone MVDC SPS, in an OPAL-RT environment for above-mentioned attacks. Overall, the proposed model-agnostic estimator (MAE) has the potential to significantly improve the resilience of SPSs against cyber-attacks without revealing any model information.**

***Index Terms*—Latency attack, data dropout, distributed control, inner control loop dynamics, model-agnostic estimator (MAE), MVDC shipboard power systems (SPSs), time synchronization attack (TSA).**

I. Introduction

THE development of all-electric ships (AES) has been primarily facilitated by the emerging medium voltage DC (MVDC) technology. For operation of shipboard power system (SPS), this work considers distributed secondary control (DSC) to achieve average voltage regulation and proportional current sharing among the power generation modules (PGMs) in enhancing the system efficiency and preventing overloading [1]. To ensure controlled power generation, SPS is interconnected through global positioning system (GPS), global navigation satellite system (GNSS), etc [2]. This enables efficient and reliable operation of the system by facilitating real-time data sharing, monitoring and control across the vessel. However, the resulting cyber-physical SPS is potentially vulnerable to cyber-attacks. Notably, the maritime sector has recently experienced cyber intrusions in four major companies [3], highlighting the urgency of cyber-threat analysis.

DSC architecture offers reliability against single point-of-failure and supports sparse communication networks, but heavy reliance on communication makes it vulnerable to cyber-attacks. Therefore, out of the various cyber-attacks [4], this work specifically investigates the impact of data availability attacks, such as, latency attacks, data dropouts and time synchronization attacks (TSAs) on MVDC SPS. The latency attacks and TSAs aim to cause information delay whereas, the data dropout causes loss of measurement/control information. These attacks can disrupt the vessel operation by impairing control signals, cause stability issues and/or service downtime.

To address the problem of latency attacks and data dropouts, [5] introduces a distributed predictive control framework, while [6] discusses a finite frequency approach. However, these methods necessitate a priori modeling expertise, and the need for observer design elevates system complexity. To detect TSAs, the authors of [7] propose deployment of passive oscillator circuits (POCs), introducing an additional cost. Latency attacks and TSAs are detected in [8] and [9], respectively through data-driven approaches. These potentially entails high memory and data requirements for training. Although existing literature investigates the issue of above-mentioned attacks separately, there is a requirement of a scheme which actively manages all these vulnerabilities using a single plane, without demanding extensive model information.

To bridge this gap, this paper proposes for the first time a model-agnostic estimator (MAE) to compensate random delays and missing information in MVDC systems using the semantic event-driven signal reconstructed from their voltage controller dynamics. The main contributions of this work are:

- The proposed MAE in each PGM exploits the physical layer semantics extracted from their inner control loop dynamics to provide reconstructed signals to the secondary controller (SC), thereby facilitating delay compensation.
- The proposed scheme is robust against latency attacks, data dropouts and TSAs.
- The proposed MAE employs a distributed approach, streamlining operations and enhancing manageability compared to complex centralized methods.
- The model-agnostic nature simplifies its implementation by eliminating the need for parameter-centric models.
- Unlike data-driven approaches that demand substantial computational resources, extensive datasets, and hyperparameter tuning, the proposed approach operates without training.

II. Modeling Preliminaries

A. Physical Framework

To demonstrate the modeling and control framework, a notional 12 kV two-zone MVDC SPS with zones Z1 and

This work is supported by the Nordic Energy Research programme via Next-uGrid project n. 117766.

Kirti Gupta and Bijaya Ketan Panigrahi are with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi 110016, India (e-mail: {Kirti.Gupta, Bijaya.Ketan.Panigrahi}@ee.iitd.ac.in).

Subham Sahoo is with the Department of Energy, Aalborg University, 9220 Aalborg, Denmark (e-mail: sssa@energy.aau.dk).

Z2, is presented in Fig. 1(a), powered by two PGMs [10]. Throughout this investigation, each PGM comprises of a DC source (denoting an energy storage system), DC/DC converter, LC filter, and RL output impedance. In addition to PGM, each zone includes power conversion modules (PCMs) and propulsion motor modules (PMMs), modeled as resistive loads. The SPS network is structured with cable sections and switches that connect various sources (PGMs) and loads (PCMs and PMMs) to it, as shown in Fig. 1(a). The control framework comprises inner control loops, such as voltage control (VC) and current control (CC), cascaded with primary droop control (DC) loop, as in Fig. 1(b). The merging units (MUs) transmit the time-synchronized measurements (facilitated by GPS) to these controllers for the control operation. As shown in Fig. 1(b), the GPS clock offers synchronized measurements of time by utilizing various methods, such as, modulated or unmodulated serial time codes (such as IRIG-B), precision time protocol (PTP) through Ethernet, or one pulse per second (1PPS) [11]. More information about its control layer modeling can be referred from [12]. The adopted voltage droop control is:

$$\mathrm{V}_j^*(\mathrm{t}) = \mathrm{V}_{\mathrm{ref}} - \mathrm{R}_j^{\mathrm{vir}}\mathrm{i}_j(\mathrm{t}) \tag{1}$$

where, subscript 'j' represents parameters associated to j^{th} PGM. The terms $\mathrm{V}_{\mathrm{ref}}$ and V_j^* are nominal voltage of DC system and local reference voltage for PGM, respectively. Moreover, droop gain and current are denoted by $\mathrm{R}^{\mathrm{vir}}$ and i, respectively. Since primary control inherently results in non-zero steady-state error, DSC is integrated, as shown in Fig. 1(b), which is described in Section II.B.

B. Cyber Framework

Let us consider a SPS with 'p' PGMs in a sparsely-connected DSC framework. These PGMs are termed as agents/nodes in cyber layer and are represented as $\mathbf{x} = \{\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_p\}$. These agents are linked to their neighbouring agents by edges $\mathbf{E}$ via an associated adjacency matrix, $\mathbf{A}_{\mathrm{G}} = [\mathrm{a}_{jm}] \in \mathbf{R}^{N\times N}$. The neighbours to j^{th} agent is represented as, $\mathrm{N}_j = \{m \mid (\mathrm{x}_m, \mathrm{x}_j) \in \mathbf{E}\}$. Here, the communication weight a_{jm} (from agent m to agent j) is modeled as: $\mathrm{a}_{jm} > 0$, if $(\mathrm{x}_j, \mathrm{x}_m) \in \mathbf{E}$. If there is no cyber link between x_j and x_m, then $\mathrm{a}_{jm} = 0$. Any agent sends/receives the information from the neighbouring agent(s) i.e, $\sigma_m = [\mathrm{R}_m^{\mathrm{vir}}\mathrm{i}_m \ \overline{\mathrm{V}}_m]^{\mathrm{T}}$, where $\overline{\mathrm{V}}_j(\mathrm{t})$is the average voltage of the m^{th} agent. The matrix representing incoming information can be given as, $\mathbf{D}_{\mathrm{in}} = \mathtt{diag}\{\mathrm{d}_j^{\mathrm{in}}\}$, where $\mathrm{d}_j^{\mathrm{in}} = \sum_{m\in \mathrm{N}_j} \mathrm{a}_{jm}$. Combining the sending and receiving end information into a single matrix, we obtain the Laplacian matrix $\mathbf{L} = [\mathrm{l}_{jm}]$, where l_{jm} are its elements defined as, $\mathbf{L} = \mathbf{D}_{\mathrm{in}} - \mathbf{A}_{\mathrm{G}}$. According to [12], the local reference voltage of PGM, as expressed in (1) is redefined as:

$$\mathrm{V}_j^*(\mathrm{t}) = \mathrm{V}_{\mathrm{ref}} - \mathrm{R}_j^{\mathrm{vir}}\mathrm{i}_j(\mathrm{t}) + \underbrace{\Delta\mathrm{V}_{1j}(\mathrm{t}) + \Delta\mathrm{V}_{2j}(\mathrm{t})}_{\Delta\mathrm{V}_j(\mathrm{t})} \tag{2}$$

where, $\Delta\mathrm{V}_1$ and $\Delta\mathrm{V}_2$ are voltage correction terms from voltage observer (VO) and current regulator (CR) respectively:

$$\Delta\mathrm{V}_{1j}(\mathrm{t}) = \mathrm{H}_1(s)\underbrace{(\mathrm{V}_{\mathrm{ref}} - \overline{\mathrm{V}}_j(\mathrm{t}))}_{\mathrm{u}_j^{\mathrm{V}}(\mathrm{t})}, \quad \Delta\mathrm{V}_{2j}(\mathrm{t}) = -\mathrm{H}_2(\mathrm{s})\mathrm{u}_j^{\mathrm{i}}(\mathrm{t}) \tag{3}$$

where, $\mathrm{H}_1(\mathrm{s})$ and $\mathrm{H}_2(\mathrm{s})$ are PI controllers for VO and CR, respectively. Here, $\mathrm{u}_j^{\mathrm{V}}$ and $\mathrm{u}_j^{\mathrm{i}}$ represent the control input to SC from VO and CR, respectively. The local control input of SC can be defined as:

$$\mathbf{u}_j(\mathrm{t}) = \mathrm{g}_j \sum_{m\in \mathrm{N}_j} \underbrace{\mathrm{a}_{jm}\left(\boldsymbol{\sigma}_m(\mathrm{t}) - \boldsymbol{\sigma}_j(\mathrm{t})\right)}_{\mathbf{e}_{jm}(\mathrm{t})} \tag{4}$$

where, $\mathbf{u}_j = [\mathrm{u}_j^{\mathrm{V}} \ \mathrm{u}_j^{\mathrm{i}}]$, $\mathbf{e}_{jm} = [\mathrm{e}_{jm}^{\mathrm{V}} \ \mathrm{e}_{jm}^{\mathrm{i}}]$, depending on the elements in $\boldsymbol{\sigma}$; and g_j is the convergence parameter. The average voltage of the j^{th} agent, $\overline{\mathrm{V}}_j(\mathrm{t})$ is expressed as:

$$\dot{\overline{\mathrm{V}}}_j(\mathrm{t}) = \dot{\mathrm{V}}_j(\mathrm{t}) + \sum_{m\in \mathrm{N}_j} \mathrm{a}_{jm}\left(\overline{\mathrm{V}}_m(\mathrm{t}) - \overline{\mathrm{V}}_j(\mathrm{t})\right) \tag{5}$$

These information exchanges can be limited by data availability cyber-attacks, which then aggravate the system controllability due to missing information, as explained in Section III.

III. Overview of Data Availability Attacks

A. Latency Attacks and Data Dropouts

Real-time periodic communication is vital for the proper functioning of DSC. However, congestion of data packets can result in communication delays that are influenced by cyber

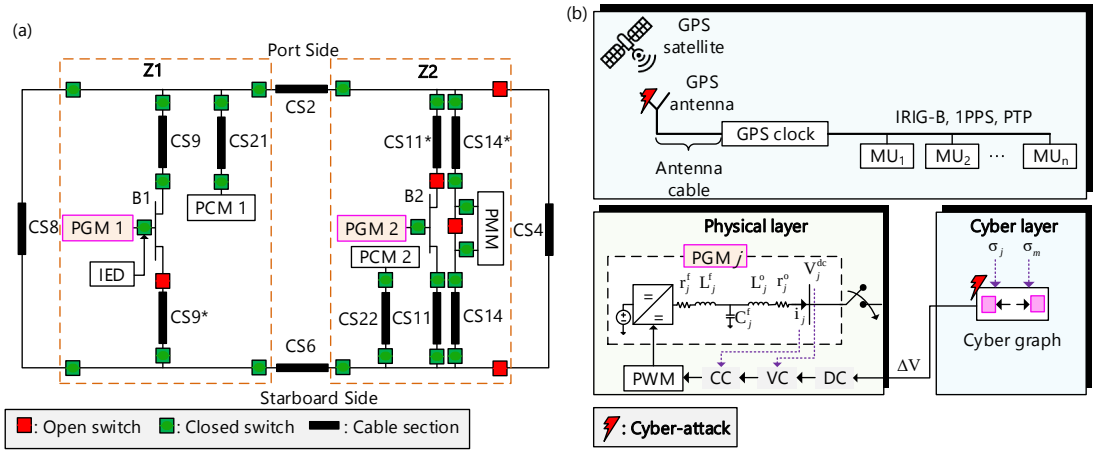

Fig. 1. **(a)** A notional 12 kV two-zone MVDC SPS with two PGMs; and **(b)** block diagram of cyber-physical PGM.

sampling rate, data volume, and cyber graph topology. If these delays exceed the timescale operation of SC (typically in seconds), it can cause oscillatory instability due to continuous missed updates. Moreover, an intentional time delay can be added to the time-critical messages by the adversaries as shown in Fig. 2(a). Here, the information transmitted from the SC of m^{th} agent i.e, $\boldsymbol{\sigma}_m(\mathrm{t}_1)$ to the SC of j^{th} agent at time t_1 experiences a delay. This causes it to be received at a later time, t_2. These are commonly termed as latency attacks. Furthermore, network congestion can also lead to frequent data dropouts [13]. This is also presented in Fig. 2(a), where the information sent by the SC of m^{th} agent ($\boldsymbol{\sigma}_m(\mathrm{t}_3)$) to the SC of j^{th} agent encounters excessive delay, beyond the acceptable limits. Consequently, this prolonged delay results in the data being dropped from the communication stream. The control law under the influence of latency attacks is:

$$\mathbf{u}_j^{\mathrm{L}}(t) = \mathrm{g}_j \sum_{m \in \mathrm{N}_j} \mathrm{a}_{jm} \left(\boldsymbol{\sigma}_m(\mathrm{t} - \tau_m) - \boldsymbol{\sigma}_j(\mathrm{t} - \tau_j) \right) \quad (6)$$

where, τ_j and τ_m are local and neighbouring delays.

B. Time Synchronization Attacks (TSAs)

Recently, TSAs have become a huge concern due to ever-increasing frequency across all sectors. The integrity of GPS signals can be compromised by unintentional sources such as radio frequency (RF) interference and solar flares. This interference can cause timing errors or even result in a complete loss of signal reception [14]. Moreover, the GPS receiver in a substation clock or a MU can be tricked by fraudulent GPS signals being broadcasted or by re-broadcasting of GPS signals captured at a different time-step [15]. The GPS receiver depending on GNSS for time transfer, using 1PPS [11] is shown in Fig. 2(b). It can be observed that the 1PPS signal of the neighbouring agent (m^{th} PGM) is fabricated to a different time stamp under TSA. Assuming TSA fabricates the time-stamped information of $\boldsymbol{\sigma}_m(\mathrm{t})$ by $\mathrm{nT_s}$ samples:

$$\sigma_m^{\mathrm{T}}(\mathrm{t}) = \sigma_m(\mathrm{t} \pm \mathrm{nT_s}) \quad (7)$$

Whether the adversary chooses to add or subtract these $\mathrm{nT_s}$ samples, time synchronization is lost.

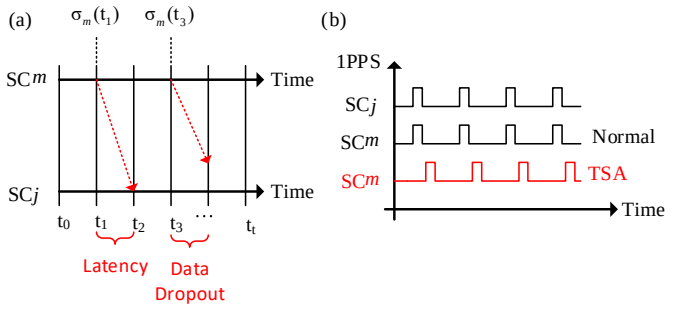

Fig. 2. **(a)** Latency attack and data dropout; and **(b)** TSA.

The above-mentioned cyber-attacks can either lead to sub-optimal operating conditions, or even cause stability issues in SPS. This may also lead to unintentional disconnection of source/loads causing local/full shut down of the SPS, disrupting the security of electrical supply. Hence, in this paper, the efforts are accumulated to combat these issues.

IV. Proposed Model-Agnostic Estimator

Within the SC, the integrator continually accumulates errors based on the latest accessible data. Continuously missed updates due to data availability attacks lead to a gradual accumulation of error over time, representing the physical layer's semantics. The proposed MAE scheme (local to each SC), harnesses these semantics to generate delay compensation signals. Therefore, in order to comprehend the proposed MAE approach, it is crucial to apply the PI consensusability law [16]. It anticipates the physical layer semantics through the dynamics of local controller. These physical semantics are used to generate the reconstruction signals. This reconstruction process compensates for missing samples of information. Finally, the reconstructed signals are input to local SC for delay compensation. Therefore, at first, the error signal provided to the VC ($\mathrm{e}_j^{\mathrm{VC}}$) is downsampled as ($\mathrm{e}_j^{\mathrm{D}}$) by:

$$\mathrm{e}_j^{\mathrm{D}} = \sum_{w=0}^{\mathrm{W}-1} \mathrm{e}_j^{\mathrm{VC}}[\mathrm{nD} - w].\delta[w] \quad (8)$$

where, $\delta[w]$ is an impulse response, W is the length of window, D is the downsampling factor. Downsampling is a resampling technique that decreases the resolution of the incoming signal, typically used to minimize memory usage. However, in this study, it is performed to align the dynamic performance of the error being fed to the VC (i.e, $\mathrm{e}_j^{\mathrm{VC}}$) and the error being fed to the SC (i.e, u_j). This crucial step aids in the synchronization of the multi-time scale error signals. Furthermore, the generated downsampled signal ($\mathrm{e}_j^{\mathrm{D}}(\mathrm{t})$) is compared with the local control inputs from the SC (i.e, $\mathrm{u}_j^{\mathrm{V}}(\mathrm{t})$ and $\mathrm{u}_j^{\mathrm{i}}(\mathrm{t})$), as in Fig. 3. The semantic prediction policy

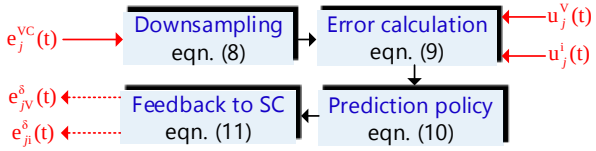

Fig. 3. Proposed MAE scheme.

subsequently rebuilds the signals used for delay compensation (i.e, $\mathbf{e}_j(\mathrm{t}_a) = [\mathrm{e}_j^{\mathrm{V}}(\mathrm{t}_a) \;\; \mathrm{e}_j^{\mathrm{i}}(\mathrm{t}_a)]$) based on following expression:

$$\mathbf{e}_j(\mathrm{t}_a) = \mathrm{e}_j^{\mathrm{D}}.[1 \;\; 1] - \mathbf{u}_j \quad (9)$$

Additionally, the error is fed into the prediction policy stage to generate a signal that compensates for significant delays. The prediction policy condition is expressed as:

$$||\mathbf{e}_j(\mathrm{t}_a)|| > \alpha ||e^{-\mathrm{t}/\mathrm{T}} \mathrm{e}_j^{\mathrm{VC}}.[1 \;\; 1]|| \quad (10)$$

where, α is a tunable parameter, $\mathrm{T} = \mathrm{K_p}/\mathrm{K_i}$ is the controller time constant of $\mathrm{H}_1(\mathrm{s})$ and $\mathrm{H}_2(\mathrm{s})$ PI control loops. If the condition expressed in (10) is met, triggers are produced. These triggers are utilized to reconstruct $\mathbf{e}_j(\mathrm{t}_a)$ using a sample-and-hold circuitry, with t_a as the triggering moment. The resulting reconstructed signals are subsequently fed back to VO and CR in SC, with their tunable gains, k_1 and k_2, represented as:

$$\mathrm{e}_{j\mathrm{V}}^{\delta}(\mathrm{t}_a) = \mathrm{k}_1 \mathrm{e}_j(\mathrm{t}_a) \;\; , \;\; \mathrm{e}_{j\mathrm{i}}^{\delta}(\mathrm{t}_a) = \mathrm{k}_2 \mathrm{e}_j(\mathrm{t}_a) \quad (11)$$

Finally these inputs are added to the control inputs of SC as:

$$\mathrm{u}_j^{\mathrm{Vf}}(\mathrm{t}) = \mathrm{u}_j^{\mathrm{V}}(\mathrm{t}) + \mathrm{e}_{j\mathrm{V}}^{\delta}(\mathrm{t}_a) \;\;,\;\; \mathrm{u}_j^{\mathrm{if}}(\mathrm{t}) = \mathrm{u}_j^{\mathrm{i}}(\mathrm{t}) + \mathrm{e}_{j\mathrm{i}}^{\delta}(\mathrm{t}_a) \quad (12)$$

where, $\mathrm{u}_j^{\mathrm{Vf}}$ and $\mathrm{u}_j^{\mathrm{if}}$ are the final predictive inputs to the SC to compensate the delays. The proposed scheme is for distributed learning, where the final predictive inputs to SC can be expressed as:

$$\mathbf{u}_j^{\mathbf{Vif}}(\mathrm{t}) = \mathbf{e}_j^{\delta}(\mathrm{t}) + \underbrace{\mathrm{g}_j \sum_{m \in \mathrm{N}_j} \mathrm{a}_{jm} \left(\boldsymbol{\sigma}_m(\mathrm{t}) - \boldsymbol{\sigma}_j(\mathrm{t})\right)}_{\mathbf{u}_j(\mathrm{t})} \quad (13)$$

where, $\mathbf{u}_j^{\mathbf{Vif}}(\mathrm{t}) = [\mathrm{u}_j^{\mathrm{Vf}}(\mathrm{t}) \;\; \mathrm{u}_j^{\mathrm{if}}(\mathrm{t})]^{\mathrm{T}}$ and $\mathbf{e}_j^{\delta}(\mathrm{t}) = [\mathrm{e}_{jV}^{\delta}(\mathrm{t}) \;\; \mathrm{e}_{ji}^{\delta}(\mathrm{t})]^{\mathrm{T}}$. Hence, neighbouring agents' dynamics are taken into consideration during the reconstruction process.

V. Performance Evaluation

A real-time simulation testbed setup [17], used to test the feasibility of the proposed scheme is shown in Fig. 4. It comprises of OP-5700 (real-time simulator), which is integrated with HYPERSIM software (on the host PC) to model a notional 12 kV two-zone MVDC SPS. The host PC and OP-5700 simulator are interconnected through Ethernet interface. This interface facilitates establishment of the cyber layer of the considered system, over IEC 61850 sampled values (SV) protocol. The attack models expressed by (6) and (7) are developed in the HYPERSIM software, installed in the host PC. The design and control parameters of the considered system is tabulated in Table I. The evaluation of the proposed scheme for various test conditions is presented further.

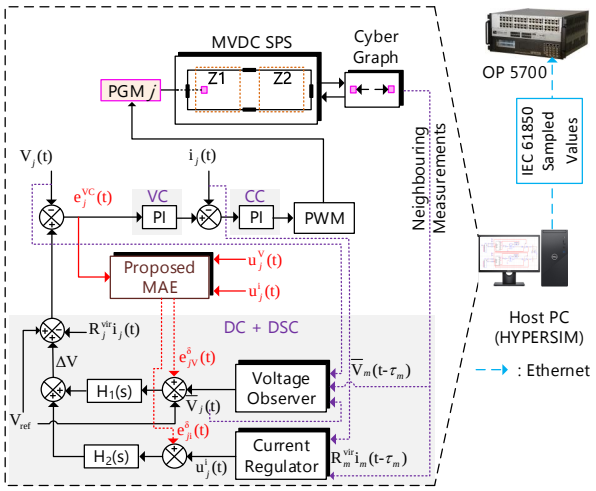

Fig. 4. Deployment of the proposed scheme in real-time simulation testbed with notional 12 kV two-zone MVDC SPS powered by two PGMs. The testbed is interfaced with Ethernet to facilitate establishment of IEC 61850 sampled values protocol.

TABLE I
Test System Parameters

Parameters for PGMs		
Parameter	Symbol	Rating
Power rating, Nominal voltage	P, $\mathrm{V_{ref}}$	72 MW, 12 kV
Filter parameters	$\mathrm{L^f}$, $\mathrm{r^f}$, $\mathrm{C^f}$	3 mH, 1 mΩ, 12.1 mF
Output impedance	$\mathrm{L^o}$, $\mathrm{r^o}$	0.97 mH, 0.121 Ω
Proportional gain (CC, VC)	$\mathrm{K_p^i}$, $\mathrm{K_p^V}$	0.2, 2
Integral gain (CC, VC)	$\mathrm{K_i^i}$, $\mathrm{K_i^V}$	0.01, 7.1
Secondary control (SC) parameters		
Proportional gain (CR, VO)	$\mathrm{K_p^{Si}}$, $\mathrm{K_p^{SV}}$	0.15, 0.1
Integral gain (CR, VO)	$\mathrm{K_i^{Si}}$, $\mathrm{K_i^{SV}}$	15, 10
Network and load parameters of notional 12 kV MVDC SPS ([10])		

A. System under latency attacks

A latency attack on the measurements from PGM 2 was injected with τ_m=0.05 s. Further, it was accompanied by load changes at following time instants i.e, 10 s, 15 s and 20 s. It can be observed from Fig. 5(a) and 5(b) that the system takes time to converge to the steady state values corresponding to the average voltage and the current. Moreover, after the load change at 20 s, the system becomes unstable. On deploying the proposed scheme to the MVDC SPS network, it can be observed from Fig. 5(c) and 5(d) that the system reaches convergence (in less time) and remains stable.

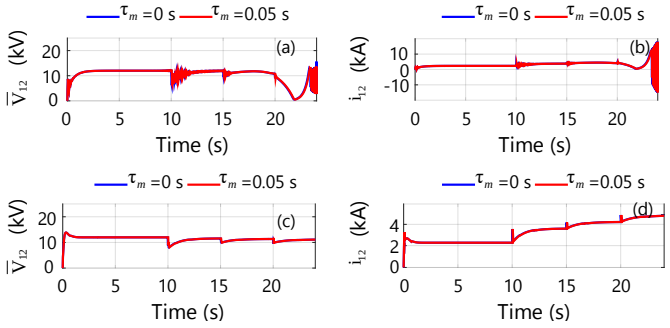

Fig. 5. Time-domain signals during latency attack, without the proposed scheme for **(a)** average voltage; **(b)** current; and with the proposed scheme for **(c)** average voltage and **(d)** current, received at PGM 1.

B. System under latency attacks and data dropouts

A latency attack (τ_m=0.05 s) along with 10% data dropout was carried out on the measurements from PGM 2. This case study was also accompanied by the same load changes, similar to case A. It can be observed from Fig. 6(a) that with the inclusion of data dropout, the system tends to become unstable at about 7.5 s. However, this was not the case in Fig. 5(a). Therefore, the data dropout further intensifies the impact of latency attack on the system. With the proposed scheme, it can be observed from Fig. 6(c) and 6(d) that the system not only converges to steady state but also remains stable.

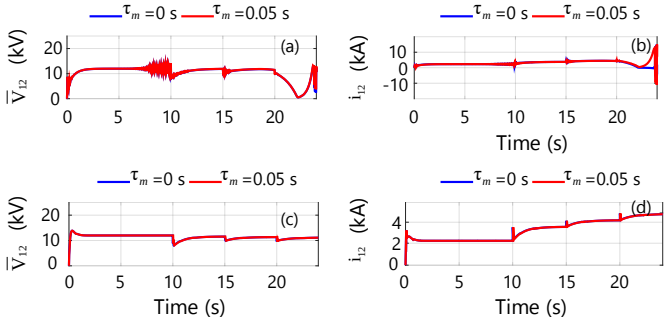

Fig. 6. Time-domain signals during latency attack and data dropouts, without the proposed scheme for **(a)** average voltage; **(b)** current; and with the proposed scheme for **(c)** average voltage and **(d)** current, received at PGM 1.

C. System under TSAs

On applying TSA, it can be observed in Fig. 7(a) and 7(b) that the system is tending towards instability from 10 s onwards. With the adoption of the proposed scheme, it can be observed in Fig. 7(c) and 7(d), that the system becomes stable with the average voltage and current reaching the steady state.

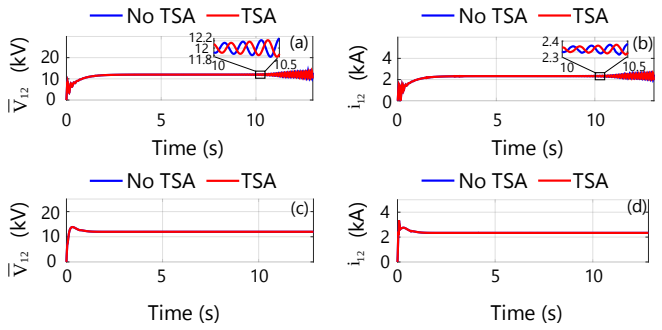

Fig. 7. Time-domain signals during TSA, without the proposed scheme for **(a)** average voltage; **(b)** current; and with the proposed scheme for **(c)** average voltage and **(d)** current, received at PGM 1.

The key competitive advantages of the proposed scheme is summarized in Table II. In contrast to existing methodologies

TABLE II
FEATURES OF THE PROPOSED MAE SCHEME.

Parameters	Proposed work
Delay compensation (during latency attacks and TSAs)	✓
Data dropout resiliency	✓
Distributed approach	✓
Computational complexity	Low
Additional resources	✗

tailored for specific attack types, such as latency attack [8] and TSA [9], our proposed scheme offers a comprehensive solution addressing latency attacks, TSAs, and data dropouts in a unified manner. Furthermore, while conventional approaches like the distributed predictive control framework [5] and finite frequency approach [6] necessitate intricate modeling expertise, our proposed model-agnostic estimator (MAE) eliminates the need for parameter-centric models. Leveraging a distributed architecture, our scheme enhances computational efficiency through nodal semantic intelligence. Unlike the solutions necessitating supplementary resources [7], our scheme emerges as a cost-effective solution without any additional resources. These distinguishing features position the proposed MAE as a promising solution for widespread commercial application.

VI. CONCLUSION AND FUTURE SCOPE

The proposed MAE approach addresses the challenges of random communication delays due to data availability attacks in MVDC SPS. The proposed model-agnostic approach leverages inner control loop dynamics to construct local delay compensation signals. It eliminates model-intensive requirements and their associated prediction accuracy, inherent in existing controllers. The real-time simulation results have demonstrated the efficiency of the proposed controller. As a future scope of work, a theoretical investigation of the system stability and the maximum communication delay that it can withstand will be carried out. Hence, the findings of this study contributes to new model-agnostic technologies for MVDC SPS cybersecurity, opening promising avenues for future research.

REFERENCES

[1] L. Xing et al., "Distributed Secondary Control for Current Sharing and Voltage Restoration in DC Microgrid," *IEEE Trans. on Smart Grid*, vol. 11, no. 3, pp. 2487-2497, May 2020, doi: 10.1109/TSG.2019.2956515.

[2] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, M. Michaloliakos, "Cybersecurity Challenges in the Maritime Sector", *Network*, vol. 2, no. 1, pp.123-138, 2022, https://doi.org/10.3390/network2010009.

[3] C. Cimpanu, "All four of the world's largest shipping companies have now been hit by cyber-attacks," https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/, 2020 (accessed March 16, 2023).

[4] S. Sahoo, F. Blaabjerg, and T. Dragicevic, *Cyber Security for Microgrids*. IET, 2022, doi:https://doi.org/10.1049/PBPO196E.

[5] Y. Yu, G. -P. Liu and W. Hu, "Coordinated Distributed Predictive Control for Voltage Regulation of DC Microgrids with Communication Delays and Data Loss," *IEEE Trans. Smart Grid*, 2022, doi: 10.1109/TSG.2022.3208946.

[6] Y. Wu and J. Dong, "Cyber-Physical Attacks Against State Estimators Based on a Finite Frequency Approach," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 2, pp. 864-874, Feb. 2021, doi: 10.1109/TSMC.2018.2882852.

[7] A. Ameli, K. A. Saleh, A. Kirakosyan, E. F. El-Saadany and M. M. A. Salama, "An Intrusion Detection Method for Line Current Differential Relays in Medium-Voltage DC Microgrids," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3580-3594, 2020, doi: 10.1109/TIFS.2020.2991892.

[8] P. Ganesh et al., "Learning-Based Simultaneous Detection and Characterization of Time Delay Attack in Cyber-Physical Systems," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3581-3593, July 2021, doi: 10.1109/TSG.2021.3058682.

[9] A. Mohammad Saber, A. Youssef, D. Svetinovic, H. H. Zeineldin and E. F. El-Saadany, "Anomaly-Based Detection of Cyberattacks on Line Current Differential Relays," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4787-4800, Nov. 2022, doi: 10.1109/TSG.2022.3185764.

[10] N. Doerry, "Next Generation Integrated Power Systems for the Future Fleet," *Corbin A. McNeill Symposium*, United States Naval Academy, Annapolis, 2009.

[11] Z. Idrees et al., "IEEE 1588 for Clock Synchronization in Industrial IoT and Related Applications: A Review on Contributing Technologies, Protocols and Enhancement Methodologies," *IEEE Access*, vol. 8, pp. 155660-155678, 2020, doi: 10.1109/ACCESS.2020.3013669.

[12] V. Nasirian, S. Moayedi, A. Davoudi and F. L. Lewis, "Distributed Cooperative Control of DC Microgrids," *IEEE Trans. Power Electronics*, vol. 30, no. 4, pp. 2288-2303, April 2015, doi: 10.1109/TPEL.2014.2324579.

[13] D. Maity, M. H. Mamduhi, S. Hirche and K. H. Johansson, "Optimal LQG Control of Networked Systems Under Traffic-Correlated Delay and Dropout," *IEEE Control Systems Letters*, vol. 6, pp. 1280-1285, 2022, doi: 10.1109/LCSYS.2021.3091492.

[14] K. Gupta, S. Sahoo and B. K. Panigrahi, "Delay-Aware Semantic Sampling in Power Electronic Systems," *IEEE Trans. Smart Grid*, 2024. doi: 10.1109/TSG.2023.3339707 *(Early access)*.

[15] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. Conf. Crit. Infrastruct. Protect.*, vol. 5, nos. 3–4, pp. 146–153, 2012.

[16] M. Leng, S. Sahoo and F. Blaabjerg, "Stabilization of DC Microgrids Under Cyber Attacks – Optimal Design and Sensitivity Analysis," *IEEE Trans. Smart Grid*, doi: 10.1109/TSG.2023.3278094.

[17] K. Gupta, S. Sahoo, B. K. Panigrahi, F. Blaabjerg and P. Popovski, "On the assessment of cyber risks and attack surfaces in a real-time co-simulation cybersecurity testbed for inverter-based microgrids", *Energies*, vol. 14, no. 16, pp. 4941, Aug. 2021