AALBORG UNIVERSITY

DENMARK

A Monolithic Cybersecurity Architecture for Power Electronic Systems

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

[Link to publication from Aalborg University](Link)

A Monolithic Cybersecurity Architecture for Power Electronic Systems

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

Abstract—Power electronic systems (PES) face significant threats from various data availability and integrity attacks, significantly affecting the performance of communication networks and power system operation. As a result, several attack detection and reconstruction techniques are deployed, which makes it a costly & complex cybersecurity operational platform with significant room for incremental extensions for mitigation against future threats. Unlike the said traditional arrangements, our paper introduces a foundational approach by establishing a monolithic cybersecurity architecture (MCA) via incorporating semantic principles into the sampling process for distributed energy resources (DERs). This unified approach concurrently compensates for the intrusion challenges posed by cyber attacks by reconstructing signals using the dynamics of the inner control layer. This reconstruction considers essential semantic attributes, like Priority, Freshness, and Relevance to ensure resilient dynamic performance. Hence, the proposed scheme promises a generalized route to concurrently tackle a global set of cyber attacks in elevating the resilience of PES. Finally, rigorous validation on a modified IEEE 69-bus distribution system and a real-world South California Edison (SCE) 47-bus network, using OPAL-RT under diverse operating conditions, underscores its robustness, model-free design capability, scalability, and adaptability to dynamic cyber graphs and system reconfiguration.

Index Terms—Data dropout, distributed control, false-data injection attacks (FDIAs), inner control loop dynamics, latency attack, power electronic systems (PES), semantic sampling, time synchronization attack (TSA).

I. INTRODUCTION

IN the realm of power electronic systems (PES), the integration of control and communication is pivotal for achieving efficiency, sustainability, and flexibility. However, conventional centralized secondary controllers (SCs) within PES exhibit inherent limitations, including stringent communication bandwidth requirements, susceptibility to single-point failures, and intricate computational demands. Addressing these constraints, the adoption of a distributed secondary control (DSC) architecture has emerged as a compelling alternative, harnessing insights from neighboring agents [1]. Ensuring synchronization among network agents entails the utilization of global navigation satellite signals (GNSSs), acclaimed for their global reach and precision [2]. GNSS facilitates the transfer of time information among intelligent electronic devices (IEDs) and merging units through mechanisms like precision time protocol

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).

(PTP), inter-range instrumentation group time code B (IRIG-B), or one pulse per second (1PPS) over coaxial cable [3].

However, the integration of communication networks into PES introduces several bottlenecks including delays, data losses, and uncertain connections [4]. These factors can potentially result in delayed transmission of control signals among distributed energy resources (DERs), consequently impairing the overall system performance. Furthermore, these integrated cyber-physical systems are also prone to cyber attacks [5], [6]. Given PES's characteristics of low system inertia and swift responsiveness, such attacks can have more profound implications compared to bulk power systems. This research is dedicated to mitigating data availability attacks [7] and data integrity attacks [8], which can be deliberately introduced by malicious entities. Data availability attacks encompass latency attacks, data dropouts, and time-synchronization attacks (TSAs), all of which compromise the timeliness and reliability of signal exchanges. Data integrity attacks, often referred to as false data injection attacks (FDIAs), manipulate transmitted data, significantly disrupting system control.

The development of robust controllers, capable of functioning within real-time constraints to withstand adversarial attacks, is of utmost significance. Diverse methodologies have been presented, each carrying inherent limitations. To make the system resilient against data availability attacks, the strategy outlined in [9] concentrates on enhancing microgrid communication networks, while [10] integrates a controller with a supply-demand optimization algorithm. Despite their advantages, these approaches may impose substantial computational burdens in larger networks. Their susceptibility to initial conditions and hyperparameters may result in sub-optimal outcomes. Cooperative control, leveraging predictive control theory as proposed in [11], presents potential challenges in handling unknown dynamics. This may possibly lead to performance degradation or instability during data availability attacks. TSA detection scheme [12] and FDIA detection [13], focus solely on attack detection and necessitate a training phase to comprehend the system's normal behavior. Relying heavily on extensive training data introduces complexities such as increased memory usage, substantial data prerequisites, and privacy concerns. These constraints, coupled with the inability to explain abnormal data variations, diminish the suitability of data-driven approaches for power electronic converter applications. The existing approaches developed against data availability attacks [14] and data integrity attacks [15] mandate multiple observers/estimators, resulting in increased computational demands and complexity. Earlier studies have separately investigated data availability attacks and data integrity attacks,
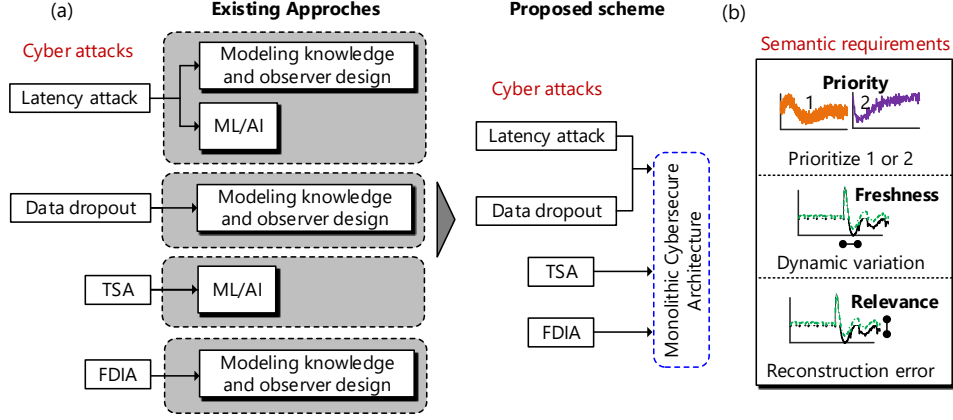
Fig. 1. **(a)** Paradigm shift from a complex architecture of cyber-physical resiliency methods to a monolithic cybersecurity architecture (MCA) – the proposed scheme with semantic sampling offers unified resiliency against data availability and data integrity attacks, **(b)** Semantic requirements governing the proposed MCA scheme.

yielding various detection and control methodologies thereby increasing the computational complexity.

To fill this gap, this paper introduces a foundational approach that leverages semantic principles to establish a monolithic cybersecurity architecture (MCA), specifically designed for PES. Although the infusion of semantic principles into PES may seem like a recent initiative, it is noteworthy that the concept of *semantics* has already found significant applications across various domains. In the broader landscape of communication systems, semantic approaches have proven effective [16]. Likewise, in the domain of networked intelligent systems, semantic techniques have been employed to augment system intelligence and facilitate meaningful interaction [17]. A notable example is in the field of speech recognition, where semantics play a crucial role in transforming spoken language into written text, enabling more precise and efficient speech-to-text transmission [18]. Additionally, as the world transitions into the era of post-5G wireless connectivity, semantic considerations are instrumental in shaping the next generation of wireless networks [19]. For a comprehensive exploration of semantic communication and its applications, readers are encouraged to delve into the detailed insights provided in [20].

The presented methodology employs judicious risk-aware sampling to systematically reconstruct and disseminate critical information within PES, ensuring its precise utilization. This study introduces the innovative concept of semantic communication (SemCom) and employs advanced sampling techniques, prioritizing the filtration of the most significant events through signal processing methods. Upholding privacy as a fundamental aspect of ethical research, our proposed MCA is strategically integrated into each DER. This distributed approach not only empowers individual DERs with localized intelligence regarding cyber attacks, but also adeptly navigates the privacy challenges associated with handling sensitive data. The principal contributions of this work are summarized as:

- **Innovative Architecture:** The proposed MCA leverages vital information derived from the inner control loop dynamics. This enables the generation of reconstructed signals for local SC, addressing both data availability

and data integrity attacks. This strategic approach significantly reduces redundant data transmissions.
- **Robustness Against Cyber Attacks:** The proposed scheme exhibits resilience against various cyber threats, including latency attacks, data dropouts, TSAs, and FDIAs. It also ensures that SC objectives are consistently met even in the presence of such adversarial scenarios.
- **Distributed Approach:** The proposed MCA adopts a distributed approach, offering a streamlined alternative to intricate centralized methods. This approach empowers individual DERs to autonomously manage local cyber attack compensation, enhancing operational efficiency and manageability.
- **Model-Agnostic Design:** Unlike conventional methods relying on device-specific models, our proposed scheme is model-agnostic and can be generalized for the most prominent cyber attacks. This simplifies implementation and saves on computational resources, eliminating the need for a multitude of device-specific models and promoting broader applicability.
- **Training-Free Operation:** In contrast to resource-intensive training-based approaches demanding extensive computational resources, large datasets, and meticulous hyperparameter tuning, our approach operates without the need for training. Additionally, it imposes no extra hardware requirements, offering a more practical and resource-efficient solution.

The structure of this paper is as follows: Section II delves into the principle of semantics and its impact on cybersecurity. Section III provides an overview of the modeling aspects pertaining to cyber-physical PES. The challenges related to data availability and data integrity attacks are detailed in Section IV. The novel MCA framework is expounded in Section V. Section VI outlines the real-time simulation testbed setup and rigorously evaluates the performance of the proposed scheme. Finally, Section VII concludes the paper by summarizing the findings and outlining potential future directions.

II. Semantics – Principles & Impact on Cybersecurity

As highlighted in the existing literature, prevailing methodologies have primarily directed their efforts towards addressing data availability attacks and data integrity attacks as distinct challenges, as illustrated in Fig. 1(a). However, these approaches exhibit inherent constraints, notably necessitating multiple detection metrics (e.g., D_1 and D_2 in Fig. 1) and observers/estimators for each attack scenario, thereby escalating the computational resources. Consequently, this study introduces a holistic strategy confronting both types of attacks while concurrently mitigating communication delays.

Drawing inspiration from the field of linguistics, there has been a notable surge of interest within the communications theoretical community towards the concept of SemCom [21]. SemCom transcends Shannon's conventional viewpoint of reliable transmission, which treats all bits uniformly. Instead, SemCom focuses on the rationale behind data transmission, emphasizing the interpretation of content, context, and timing aspects at the receiver's end [22]. This perspective provides methodologies that aim to reduce unnecessary transmissions and prioritize data, thereby enhancing overall performance.
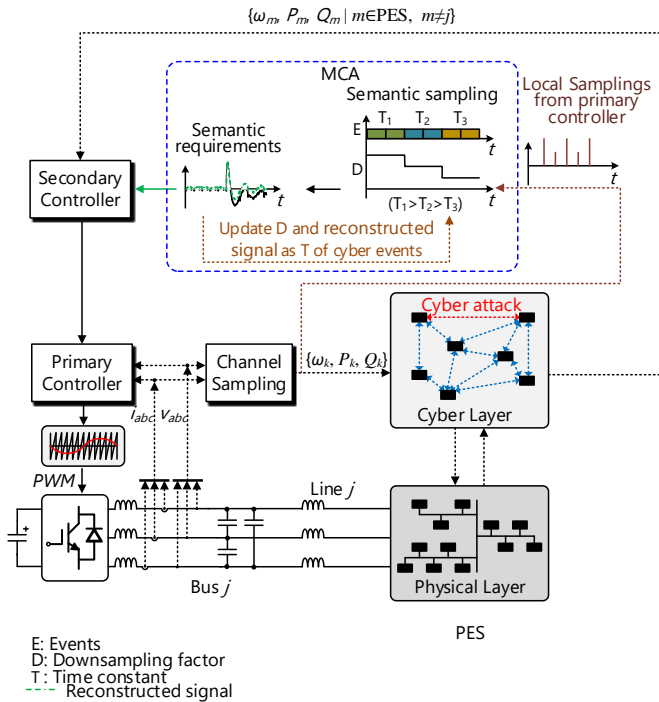

Fig. 2. Schematic diagram of the deployment of the proposed scheme (enclosed in dotted blue box) in the existing PES. The semantic information exchange from local error measurements drives the estimation and reconstruction process (to SC) during cyber attacks.

In the context of semantic sampling, the evaluation of information criticality or significance revolves around the following three key attributes (in Fig. 1(b)):

1) **Value** of information (VoI), establishes the priority of information. This ensures that the significant data reaches the right destination for efficient processing and decision-making.

2) **Freshness** is the concept of delivering new updates at the right time. It is quantified as $F(t) = t - S(t)$, denoting the time discrepancy between the present time and the arrival of the most recent packet. This quantification determines the age of information (AoI).

3) **Relevance** quantifies the magnitude of change in a process since the last recorded sample, to capture relevant updates and meaningful insights. Furthermore, the requisite alteration is precisely conveyed to the right place.

Leveraging the aforementioned semantic requirements, the error signals from the inner voltage control (VC) loop are downsampled (D is the downsampling factor) and the reconstructed signals are sent to each SC for attack compensation to each DER within PES, as depicted in Fig. 2. The signals continuously undergo downsampling according to event time constants (T), which determine events' significance. This minimizes redundant bulk data transmissions, thus improving overall efficiency of the system. Therefore, we only utilize the most significant data at the right time at the right place. This approach prioritizes the preservation of estimation accuracy under attack scenarios, such as latency attacks, data dropouts, TSAs and FDIAs. Furthermore, the semantic attributes, namely priority, freshness, and relevance, are determined by factors such as prioritization of the most significant local signal used for estimation, dynamic variation, and the reconstruction error, respectively. Consequently, the integration of semantic models establishes a standardized mechanism for interpreting relevant data collected from diverse devices and sensors across the network, fostering improved decision-making processes and enhancing overall system performance.

III. Modeling Preliminaries

A. Physical Framework

This study examines two test PES: a modified IEEE 69-bus system with nine DERs [23] in Fig. 3 and a real-world South California Edison (SCE) 47-bus network with five DERs [24] in Fig. 4. To depict the modeling and control structure of a PES, each DER comprises of a DC source (indicating an energy storage system), a DC/AC converter (inverter), LC filter, and RL output impedance, as shown in Fig. 2. The dq axis control framework encompasses internal voltage control (VC) and current control (CC) loops, coupled with the primary droop control (DC) loop, inside the primary controller. Synchronized measurements, enabled by global positioning system (GPS), are transmitted to these controllers to enable their operation.

The frequency and voltage droop schemes for PES are:

$$\omega_j^*(t) = \omega_{\text{nom}} - \text{m}_j^{\text{p}} \text{P}_j(t) \tag{1}$$

$$\text{V}_j^{\text{d}*}(t) = \text{V}_{\text{nom}} - \text{n}_j^{\text{q}} \text{Q}_j(t) \quad , \quad \text{V}_j^{\text{q}*}(t) = 0 \tag{2}$$

Here, the subscript 'j' indicates parameters related to the jth DER. The terms ω_{nom} and V_{nom} represent the nominal frequency and voltage of the AC system, respectively. The local reference frequency and voltage of a DER are designated as ω_j^* and $\text{V}_j^{\text{dq}*}$, where $\text{V}_j^{\text{dq}*}(t) = [\text{V}_j^{\text{d}*}(t) \ \text{V}_j^{\text{q}*}(t)]^{\text{T}}$. Moreover, the active power droop coefficient is represented by m^{p}, and
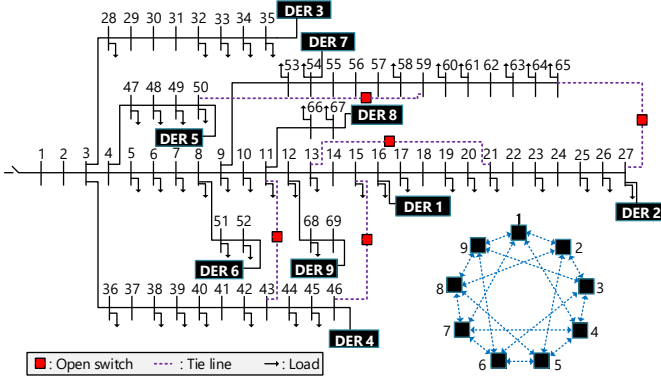
Fig. 3. Modified 69-bus distribution system with nine DERs in partially-connected topology [23].

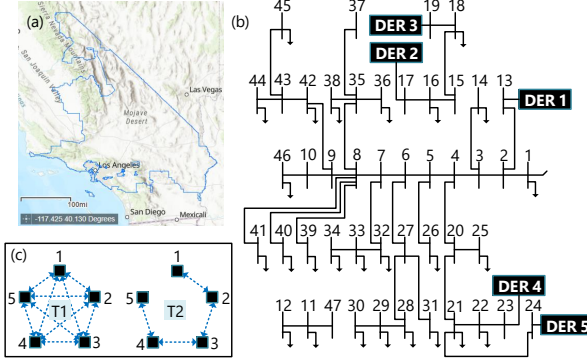Fig. 4. **(a)** South California Edison's (SCE's) Distributed Energy Resource Interconnection Map (DERiM) [25]; **(b)** real-world SCE 47-bus network with five DERs [24] and; **(c)** cyber topologies T1 and T2.

the reactive power droop coefficient is denoted as n^q. For a comprehensive understanding of the control layer modeling, refer to [26]. As the primary control inherently leads to non-zero steady-state error, the integration of the DSC scheme, depicted in Fig. 2, is introduced and discussed in forthcoming subsection. Such framework aids to counteract these errors, thereby enhancing overall system performance.

B. Cyber Framework

Consider DERs in a sparsely-connected DSC architecture denoted as a PES with 'M' agents (or nodes in the cyber layer), represented as $\mathbf{x} = \{x_1, x_2, \ldots, x_M\}$. These agents are interconnected by edges $\mathbf{E}$ through an adjacency matrix, $\mathbf{A}_G = [e_{jm}] \in \mathbf{R}^{N \times N}$. The neighbors of the jth agent are denoted as, $N_j = \{m \mid (x_m, x_j) \in \mathbf{E}\}$. The communication weight e_{jm} (from agent m to agent j) is modeled as: $e_{jm} > 0$, if $(x_j, x_m) \in \mathbf{E}$. If there is no cyber link between x_j and x_m, then $e_{jm} = 0$. Each agent exchanges information with neighboring agent(s), $\mathbf{\Psi}_m = [\omega_m \ m_m^p P \ n_m^q Q]^T$. The incoming information matrix is, $\mathbf{D}_{in} = \texttt{diag}\{d_j^{in}\}$, where $d_j^{in} = \sum_{m \in N_j} e_{jm}$. The Laplacian matrix $\mathbf{L} = [l_{jm}]$, where l_{jm} are its elements defined such that, $\mathbf{L} = \mathbf{D}_{in} - \mathbf{A}_G$. Referring to [26], the local reference frequency and voltage of a DER, initially expressed in (1) and (2), are re-defined as:

$$\omega_j^*(t) = \omega_{nom} - m_j^p P_j(t) + \delta\omega_j(t) \tag{3}$$

$$V_j^{d*}(t) = V_{nom} - n_j^q Q_j(t) + \delta V_j(t) \tag{4}$$

Here, $\delta\omega$ and δV are the frequency and voltage correction terms from the SC, that can be given by:

$$\begin{aligned}
\delta\omega_j(t) = & - H_1(s)[\omega_{nom} - \omega_j(t) + \\
& c_j \sum_{m \in N_j} e_{jm} \left(\omega_m(t) - \omega_j(t)\right) + \\
& c_j \sum_{m \in N_j} e_{jm} \left(m_m^p P_m(t) - m_j^p P_j(t)\right)]
\end{aligned} \tag{5}$$

Similarly,

$$\delta V_j(t) = -H_2(s)[c_j \sum_{m \in N_j} e_{jm} \left(n_m^q Q_m(t) - n_j^q Q_j(t)\right)] \tag{6}$$

where, $H_1(s)$ and $H_2(s)$ denote the PI controllers for frequency restoration and proportional active power sharing, as well as proportional reactive power sharing, respectively. The local control input of the SC can be defined as:

$$\zeta_j(t) = c_j \sum_{m \in N_j} \underbrace{e_{jm} \left(\mathbf{\Psi}_m(t) - \mathbf{\Psi}_j(t)\right)}_{\boldsymbol{\varrho}_{jm}(t)} \tag{7}$$

where, $\boldsymbol{\zeta}_j = [\zeta_j^p \ \zeta_j^q]$, $\boldsymbol{\varrho}_{jm} = [\varrho_{jm}^p \ \varrho_{jm}^q]$, depending on the elements in $\mathbf{\Psi}$; and c_j is the convergence parameter.

These information exchanges may encounter limitations caused by data availability and data integrity cyber attacks. These challenges can disrupt the system's monitoring and controllability, leading to the absence and corruption of critical information, as elaborated in the following section.

IV. MODELING OF CYBER ATTACKS

A. Latency Attacks and Data Dropouts

The effectiveness and reliability of the DSC architecture heavily rely on real-time periodic communication. Nonetheless, the occurrence of congestion and delays in data packets can usher in unanticipated disruptions. These delays, influenced by factors like cyber sampling rate and data volume, can span from milliseconds to seconds. If these delays surpass the operational time limits of the SC, missed updates can incite oscillatory instability and instigate system failure [27].

Moreover, malicious cyber attackers can exploit these vulnerabilities by intentionally introducing time delays to critical messages, known as latency attacks. Such attacks can severely compromise system functionality, particularly when time-sensitive information exchange occurs between SCs. Additionally, network congestion can cause frequent data dropouts, further undermining communication and dynamic performance.

Attack model: When confronted with latency attacks, the control laws that govern the behavior of cyber-physical PES can undergo substantial modifications. These alterations in the SC can be mathematically represented as follows:

$$\zeta_j(t) = c_j \sum_{m \in N_j} e_{jm} \left(\mathbf{\Psi}_m(t - \tau_m) - \mathbf{\Psi}_j(t - \tau_j)\right) \tag{8}$$

where, τ_j represents the delay from the local unit, while τ_m represents the delay from neighboring units. By utilizing the Leibnitz formula, the delayed parameter can be expressed as $\Psi(t - \tau) = \Psi(t) - \int_{t-\tau}^t \dot{\Psi}(s)ds$. Substituting this expression into equation (8) for a delay of τ_m, we obtain

$\dot{\Psi}(t) = -\mathbf{L}\Psi(t) - \mathbf{A}\int_{t-\tau_m}^{t}\dot{\Psi}(s)ds$. A similar expression can be derived for the local delay. For a fixed, undirected, and connected cyber graph, equilibrium is achieved if and only if $0 < \tau < \frac{\pi}{2\lambda_{\max}\mathbf{L}}$, where λ_{max} represents the largest eigenvalue of the matrix $\mathbf{L}$. Thus, the communication delay (τ) must be constrained within these limits in order to obtain $\dot{\Psi}(t) = 0$.
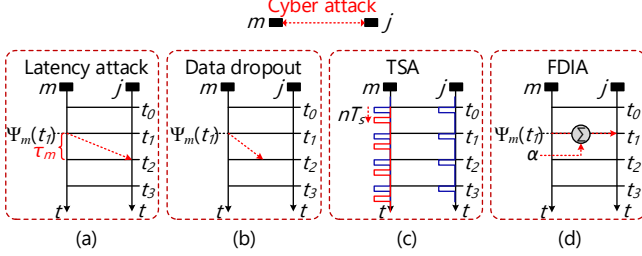

Fig. 5. The depicted models illustrate cyber attacks on two communicating SCs in terms of **(a)** latency attack; **(b)** data dropout; **(c)** TSA; and **(d)** FDIA.

B. Time Synchronization Attacks (TSAs)

Time-synchronized real-time measurements in cyber-physical networks hold paramount importance, rendering them susceptible to malicious attacks. In recent times, there has been a notable upswing in TSAs, which has raised significant concerns across diverse sectors. This issue becomes particularly critical due to potential vulnerabilities in the integrity of GPS signals. Unintentional sources like radio frequency (RF) interference and space weather events, such as solar flares, hold the potential to introduce timing inaccuracies or even outright signal loss. These discrepancies bear substantial risks for applications hinging on precise temporal synchronization.

Furthermore, GPS receivers in substation clocks or merging units are vulnerable to deliberate attacks orchestrated by malicious entities. A notable example is the receiver-spoofer mechanism [28], wherein the spoofer masquerades as a GPS receiver, manipulates authentic GPS signals, and transmits spoofed signals to the target. Both space-based time synchronization (SBTS) and network-based time synchronization (NBTS) mechanisms [29] lack integrated security controls, rendering them highly susceptible to TSAs.

Attack model: In the case of a TSA, where the time-stamped information of $\mathbf{\Psi}_m(t)$ is falsified by nT_s samples, the resulting information can be expressed as:

$$\Psi_m^{\mathrm{T}}(t) = \Psi_m(t \pm nT_s) \tag{9}$$

C. False Data Injection Attacks (FDIAs)

Adversaries possess the capability to manipulate the data interchanged between agents, strategically aiming to deceive the control system into pursuing actions that serve the attacker's agenda. Such actions may include destabilizing the PES, inducing power imbalances, or causing harm to the system's components. It can be categorized as balanced attack and unbalanced attack [30], each having distinct modeling implications. Balanced attacks ensure a stable and feasible solution, aligning with the SC objectives. In contrast, unbalanced attacks deviate from SC objectives.

Attack model: In the event of a FDIA, where the exchanged information between neighbors ($\Psi_m(t)$) is fabricated with $\alpha = [\alpha^\omega \ \alpha^{\mathrm{P}} \ \alpha^{\mathrm{Q}}]^{\mathrm{T}}$, the resultant attacked information can be mathematically represented as:

$$\Psi_m^{\mathrm{F}}(t) = \Psi_m(t) + \Lambda.\alpha \tag{10}$$

where, Λ is a binary number signifying '1' for presence of attack and '0' for no attack. Furthermore, these attacks can also be executed in a coordinated manner to deceive the system operator as follows:

$$\dot{\Psi}(t) = -(\mathbf{L}\Psi(t) + \alpha) \tag{11}$$

where, Ψ and α denote column matrices of the measured information and the attack signal respectively. Therefore, (11) can be used to model the balanced and unbalanced attacks as:

$$\dot{\Psi}(t)\begin{cases} = 0 \ ; \text{balanced attack} \\ \neq 0 \ ; \text{unbalanced attack} \end{cases} \tag{12}$$

Further details on FDIA modeling can be found in [30]. In the domain of PES, the aforementioned cyber attacks carry significant implications for the system's optimal functioning. These attacks, illustrated in Fig. 5, can trigger a spectrum of issues, ranging from sub-optimal operational conditions to system instability. Such scenarios might lead to unintended disconnections of sources and/or loads, ultimately resulting in partial or complete shutdown of the system, thereby undermining the reliability of power supply. To effectively tackle these challenges, the establishment of a one-stop simple monolithic solution becomes imperative. This architecture must be capable of addressing unforeseen delays, data dropouts, and cyber attacks. With this objective in mind, this paper embarks on the development of a novel MCA framework, which is comprehensively explained in the next section.

V. PROPOSED MCA FRAMEWORK

In the pursuit of comprehending the role of information in decision-making during instances of data availability (and/or) data integrity attacks in networked PES, this study introduces the concept of information semantics. Through this integration, it aims to provide a more nuanced and comprehensive insight into the functioning of information under such circumstances.

In the context of PES, semantic contextuality entails capturing the attributes inherent to signals within the inner control loops of each DER, such as their timeliness and intrinsic value. This enables the reconstruction of vital information that remains critical for compensation strategies in scenarios involving random delay attacks and FDIAs, as visually depicted in Fig. 2. Particularly, concerning the distributed control of AC distribution systems, prompt consensus negotiations among agents stand as a crucial factor for achieving global frequency regulation and proportional active/reactive power sharing. Consequently, a semantic-aware transmission approach that respects the time-varying value of signals becomes indispensable for realizing the objectives of the SCs. The architecture entails a series of distinct steps, presented as:

i) *Risk-aware semantics:* To grasp the intricacies of the proposed methodology, it becomes imperative to apply

the PI consensusability law [31] to anticipate the inherent semantics at the physical layer. This is accomplished by investigating the response of each control loop when subjected to disturbances. It is of significance to acknowledge that the introduced schemes at the local level target individual SC units. Implementing the proposed framework entails a systematic approach, commencing with the extraction of crucial information from the error signal associated with the VC loop. This particular error signal is denoted as $\varrho_j^{\mathbf{dqVC}}(t)$, where $\varrho_j^{\mathbf{dqVC}}(t) = [\varrho_j^{\mathrm{dVC}}(t) \quad \varrho_j^{\mathrm{qVC}}(t)]^{\mathrm{T}}$.

ii) *Semantic sampling:* Next, the signal $\varrho_j^{\mathbf{dqVC}}(t)$ undergoes downsampling, resulting in a reduced rate of data acquisition. This downsampling process is implemented as:

$$\varrho_j^{\mathrm{dD}} = \sum_{w=0}^{\mathrm{W}-1} \varrho_j^{\mathrm{dVC}}[n\mathrm{D} - w].\delta[w] \tag{13}$$

$$\varrho_j^{\mathrm{qD}} = \sum_{w=0}^{\mathrm{W}-1} \varrho_j^{\mathrm{qVC}}[n\mathrm{D} - w].\delta[w] \tag{14}$$

In this context, the downsampling procedure entails the utilization of an impulse response, indicated as $\delta[w]$, characterized by a window length of W and a downsampling factor of D. Downsampling, conventionally used as a resampling mechanism to mitigate memory consumption and curtail the resolution of the incoming signal, is repurposed in this study. Here, the downsampling operation aims to align the dynamic behavior of the error signals supplied to the VC loop with the error being fed to the SC, as shown in the Fig. 2. This alignment is crucial for achieving synchronization of the multi-time scale error signals, which is achieved by sampling based on the time constant of events. Moreover, it facilitates efficient utilization of bandwidth resources, contributing to overall system optimization.

iii) *Semantic prediction policy:* The downsampling process generates two downsampled signals, namely $\varrho_j^{\mathrm{dD}}(t)$ and $\varrho_j^{\mathrm{qD}}(t)$. These downsampled signals are then compared with the local control inputs obtained from the SC, denoted as $\zeta_j^{\mathrm{p}}(t)$ and $\zeta_j^{\mathrm{q}}(t)$. Following the comparison, the semantic prediction policy comes into play. It reconstructs the signals necessary for attack compensation, denoted as $\varrho_j(t_a) = [\varrho_j^{\mathrm{p}}(t_a) \quad \varrho_j^{\mathrm{q}}(t_a)]^{\mathrm{T}}$, based on:

$$\varrho_j(t_a) = [\varrho_j^{\mathrm{dD}}(t_a) \quad \varrho_j^{\mathrm{qD}}(t_a)] - \zeta_j \tag{15}$$

In SC, integrator accumulates error from the latest data. Persistent error accumulation due to cyber attacks may deviate the control system, causing undesired behaviors and potential instability. The generated reconstructed signals (guided by (15)) act as feedback to local SCs, aiding in compensating for cyber attack impacts. In this regard, error signal is introduced into the prediction policy stage which is mathematically expressed as:

$$||\varrho_j(t_a)|| > \beta ||e^{-t/\mathrm{T_c}}.[\varrho_j^{\mathrm{dVC}} \quad \varrho_j^{\mathrm{qVC}}]|| \tag{16}$$

Algorithm: Proposed MCA at j^{th} DER

Inputs: Error signals to inner VC loop ($\varrho_j^{\mathbf{dqVC}}(t)$), window length (W), downsampling factor (D), local control inputs to SC ($\zeta_j^{\mathbf{pq}}(t)$), tunable parameter (β), controller time constant of $H_1(s)$ and $H_2(s)$ PI control loops ($T_c = K_p/K_i$), triggering moment (t_a), tunable gains (g_1 and g_2)

Signals: impulse response ($\delta[w]$), downsampled signal ($\varrho_j^{\mathbf{dqD}}(t)$), error fed to semantic prediction policy ($\varrho_j(t_a)$), reconstructed signals ($\varrho_j^{\mathbf{R}}(t_a)$), final predictive inputs to SC ($\zeta_j^{\mathbf{pqf}}(t)$), freshness (F(t)), relevance (R(t)), S(t) is the timestamp of the latest packet received at destination by time t.

Note: $\varrho_j^{\mathbf{dqVC}}(t) = [\varrho_j^{\mathrm{dVC}}(t) \quad \varrho_j^{\mathrm{qVC}}(t)]^{\mathrm{T}}$, $\varrho_j^{\mathbf{dqD}}(t) = [\varrho_j^{\mathrm{dD}}(t) \quad \varrho_j^{\mathrm{qD}}(t)]^{\mathrm{T}}$, $\zeta_j(t) = [\zeta_j^{\mathrm{p}}(t) \quad \zeta_j^{\mathrm{q}}(t)]^{\mathrm{T}}$, $\varrho_j(t_a) = [\varrho_j^{\mathrm{p}}(t_a) \quad \varrho_j^{\mathrm{q}}(t_a)]^{\mathrm{T}}$, $\varrho_j^{\mathbf{R}}(t_a) = [\varrho_j^{\mathrm{Rp}}(t_a) \quad \varrho_j^{\mathrm{Rq}}(t_a)]^{\mathrm{T}}$, $\zeta_j^{\mathbf{pqf}}(t) = [\zeta_j^{\mathrm{pf}}(t) \quad \zeta_j^{\mathrm{qf}}(t)]^{\mathrm{T}}$

Data: $k \geq 0$
$K \leftarrow k$;
// Initialize: F(t) = 0, R(t) $\neq$ 0
while $K \neq 0$ **do**
    if *(F(t) = 0 && R(t) $\neq$ 0)* **then**
        // Compute freshness (17): F(t) = t $-$ S(t)
        // Semantic sampling: (13) and (14)
        // Triggers generation with the semantic prediction policy condition
        if *((16) holds)* **then**
            // Reconstruction of signals
            $\varrho_j^{\mathbf{R}}(rt_a + \Gamma) = \varrho_j(rt_a)$; $0 \leq \Gamma < t_a$ and r=0,1,2,...
            // Reconstructed signals fed back to SC with tunable gains by (18)
            // Final predictive inputs fed to the SC for delay compensation by (19)
            // Compute relevance (17): R(t) = $\varrho_j - \varrho_j^{\mathbf{R}}$
        else
            // No reconstruction: R(t) = 0
        end
    else
        // Compute freshness (17): F(t) = t $-$ S(t)
    end
end

Here, β is a tunable value, and $T_c = K_p/K_i$ is controller time constant of PI control loops $H_1(s)$ and $H_2(s)$. When the condition stated in (16) is satisfied, triggers are generated. These triggers play a crucial role in the reconstruction of $\varrho_j^{\mathrm{R}}(t_a)$ using a sample-and-hold circuitry. Here, t_a denotes the instant of triggering. After the triggering moment, the assessment of semantic attributes ensues, encompassing parameters such as, freshness (F(t)), priority

and relevance $(R(t))$, delineated as:

$$F(t) = t - S(t) \quad , \quad R(t) = \varrho_j - \varrho_j^{\mathbf{R}} \qquad (17)$$

Here, $S(t)$ denotes the timestamp of the most recent packet successfully received at the destination by the time t. Relevance computes the reconstruction error. Additionally, the inner control loop dynamics are prioritized to generate the reconstruction signals.

iv) *Feedback generation:* The reconstructed signals obtained from the previous step are then fed back to the SC module, incorporating tunable gains denoted as g_1 and g_2. These gains represent the adjustable parameters (here, $g_1 = 0.3$ and $g_2 = 0.5$) controlling the feedback mechanism, expressed as:

$$\varrho_j^{\mathrm{p}\varphi}(t_a) = g_1 \varrho_j^{\mathrm{Rp}}(t_a) \quad , \quad \varrho_j^{\mathrm{q}\varphi}(t_a) = g_2 \varrho_j^{\mathrm{Rq}}(t_a) \qquad (18)$$

In this equation, $\varrho_j^{\mathbf{R}}(t_a) = [\varrho_j^{\mathrm{Rp}}(t_a) \; \varrho_j^{\mathrm{Rq}}(t_a)]^{\mathrm{T}}$ represents the reconstructed signals obtained at the triggering instant t_a. These reconstructed signals are then added to the control inputs of the SC module as follows:

$$\zeta_j^{\mathrm{pf}}(t) = \zeta_j^{\mathrm{p}}(t) + \varrho_j^{\mathrm{p}\varphi}(t_a) \quad , \quad \zeta_j^{\mathrm{qf}}(t) = \zeta_j^{\mathrm{q}}(t) + \varrho_j^{\mathrm{q}\varphi}(t_a)$$
$$(19)$$

Here, ζ_j^{pf} and ζ_j^{qf} are the final predictive inputs to the SC module. These inputs compensate for the cyber attacks experienced in the system.

A comprehensive visual representation of the equations equations (13)–(19), involved in the proposed MCA is illustrated in the detailed control block diagram depicted in Fig. 6.
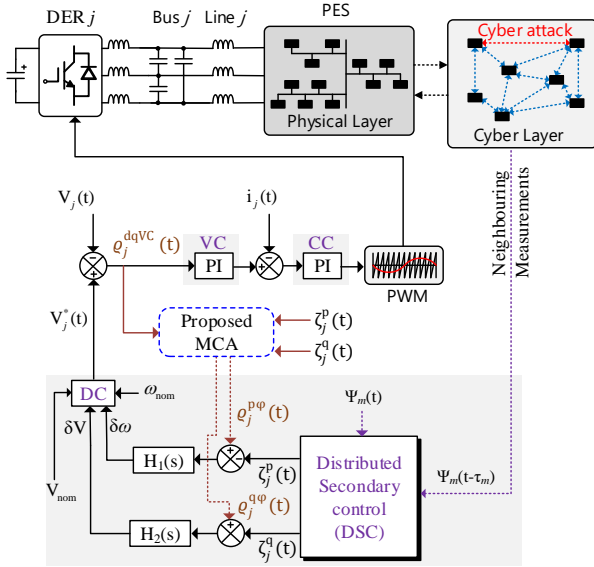

Fig. 6. Detailed control block diagram of the proposed MCA scheme.

Further, a comprehensive exploration of the convergence analysis through a detailed mathematical analysis can be referred in [32]. Hence, the MCA aims to optimize information gathering, dissemination, and decision-making policies within cooperative networks, leading to a collectively optimal performance.

VI. Performance Evaluation

The real-time simulation testbed [26] is presented in Fig. 7, to validate the effectiveness and feasibility of the proposed MCA scheme. The setup involves an OP-5700 real-time simulator integrated with HYPERSIM software on the host PC, enabling modeling of the required test system. Efficient communication is achieved through seamless interconnection of the PC and OP-5700 via the IEC 61850 sampled values protocol. The details regarding network parameters and loads for the two test systems (i.e, the modified IEEE 69-bus system with nine DERs and real-world SCE 47-bus network with five DERs) can be obtained from [23] and [24], respectively. The design and control parameters of the deployed DERs in these test systems are mentioned in Table I and II, respectively.
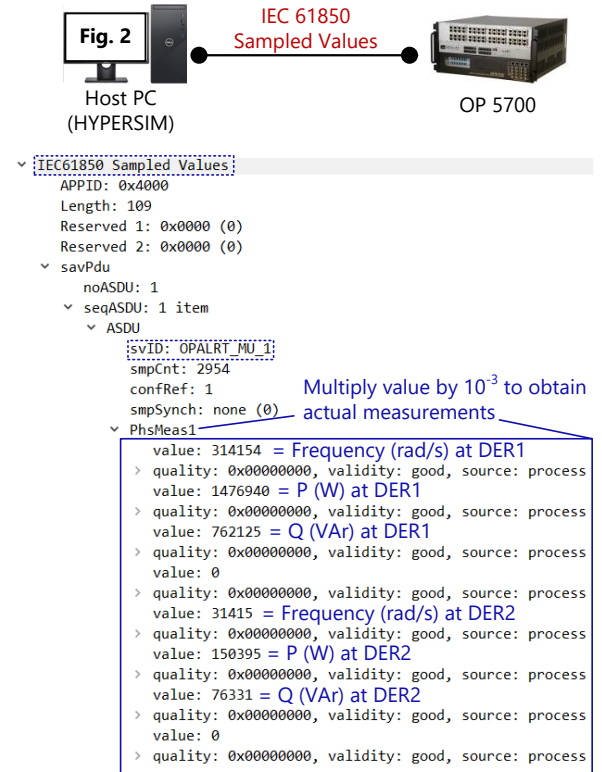

Fig. 7. Real-time simulation testbed with snapshot captured from wireshark, showing packet communicated through IEC 61850 sampled valued protocol.

TABLE I
TEST SYSTEM PARAMETERS FOR IEEE 69-BUS DISTRIBUTION SYSTEM

Parameters for DER		
Parameter	Symbol	Rating
Active power droop coefficient	m^{P}	9.4×10^{-5} rad/(W.s)
Reactive power droop coefficient	n^{q}	1.3×10^{-3} V/VAr
Proportional gain (CC, VC)	$K_{\mathrm{p}}^{\mathrm{i}}, K_{\mathrm{p}}^{\mathrm{V}}$	0.2, 50
Integral gain (CC, VC)	$K_{\mathrm{i}}^{\mathrm{i}}, K_{\mathrm{i}}^{\mathrm{V}}$	1, 100
Secondary control (SC) parameters		
Proportional gain	$K_{\mathrm{p}}^{\mathrm{S}\omega}, K_{\mathrm{p}}^{\mathrm{SV}}$	0.1, 0.1
Integral gain	$K_{\mathrm{i}}^{\mathrm{S}\omega}, K_{\mathrm{i}}^{\mathrm{SV}}$	100, 10

The performance of proposed MCA scheme is rigorously evaluated in contrast to a conventional DSC scheme, referred

TABLE II
TEST SYSTEM PARAMETERS FOR REAL WORLD SCE 47-BUS NETWORK

Parameters for DER		
Parameter	Symbol	Rating
Active power droop coefficient	m^P	9.4×10^{-5} rad/(W.s)
Reactive power droop coefficient	n^q	1.3×10^{-3} V/VAr
Proportional gain (CC, VC)	K_p^i, K_p^V	0.1, 40
Integral gain (CC, VC)	K_i^i, K_i^V	0.5, 80
Secondary control (SC) parameters		
Proportional gain	$K_p^{S\omega}, K_p^{SV}$	0.1, 0.1
Integral gain	$K_i^{S\omega}, K_i^{SV}$	10, 1.5

Fig. 9. **(a)** The time-domain plots of active and reactive power sharing are shown by solid and dashed lines respectively, before cyber attack; and **(b)** phase portrait of a DER in n^qQ-m^PP domain before cyber attack is shown.

to as 'without MCA' in subsequent sections. The assessment includes various scenarios, such as latency attacks, data dropouts, TSAs, and FDIAs. The subsequent sections detail the results of these evaluations.

A. Performance on the Modified IEEE 69-Bus Distribution System

1) System under latency attack: A latency attack was initiated on the system with a time delay of τ_m = 0.05 s, followed by a load variation at 5 s. While the system remained stable, the convergence time for achieving SC objectives was longer without the proposed scheme (Fig. 8(a), (b), and (c)) compared to the proposed scheme (Fig. 8(d), (e), and (f)) due
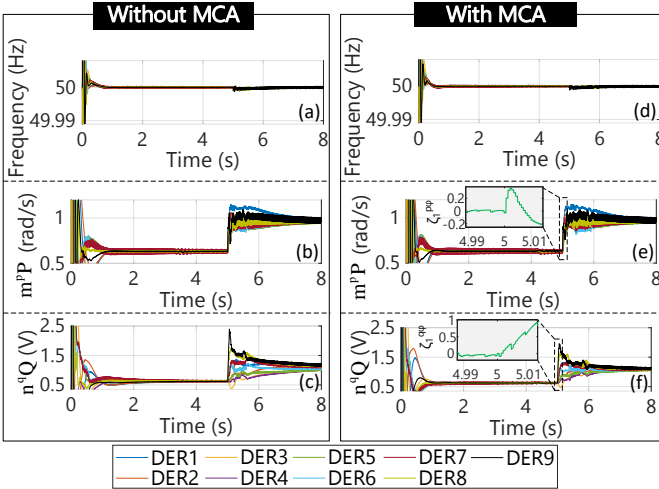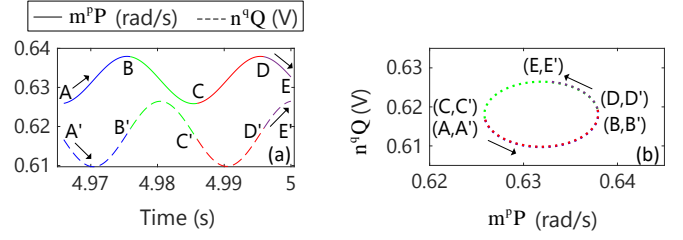

Fig. 8. Performance during latency attack (τ_m=0.05 s) for **(a)** frequency; **(b)** active power sharing; **(c)** reactive power sharing, without MCA are shown. Further, the time-domain signals for **(d)** frequency; **(e)** active power sharing; **(f)** reactive power sharing, with MCA are shown.

to the resulting reconstructed signals ($\zeta_j^{p\varphi}$ and $\zeta_j^{q\varphi}$). These reconstructed signals generated through semantic sampling, actively synchronizes the error signals at primary and secondary controllers to compensate for the latency attack.

The variations of active and reactive power sharing are depicted in Fig. 9(a), with time on the X-axis and power on the Y-axis. The corresponding Y-axis coordinates (A, B, C, D, E) and (A', B', C', D', E') for active and reactive power sharing curves are plotted against each other (n^qQ-m^PP as Y-X) to generate a phase portrait, as illustrated in Fig. 9(b). These phase portraits serve as a basis for result evaluation.

In Fig. 8, the MCA scheme notably accelerates the convergence time for SC objectives. Similar trends are observed in the phase portrait, as depicted in Fig. 10(a), which is further magnified in Fig. 10(b). The shift of operating point O_1 (prior to the cyber attack) to O_2 and O_{2P} signifies the operating points achieved without and with MCA, respectively.
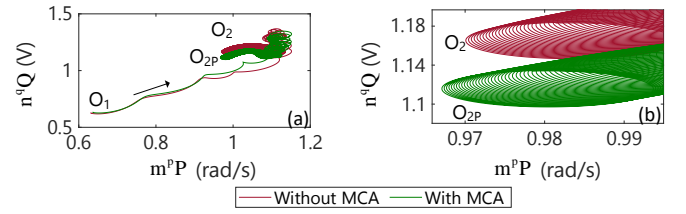

Fig. 10. **(a)** Phase portrait of a DER 1 in n^qQ-m^PP domain during latency attack (τ_m=0.05 s) is shown. The operating point O_1 (before cyber attack) traverses to O_2 and O_{2P}, representing operating points obtained without and with MCA respectively. **(b)** Zoomed plot for (a) is shown.

2) System under latency attack and data dropout: For a latency attack (τ_m = 0.05 s) combined with 10% data dropout and load variation at t = 5 s, Fig. 11(a) indicates that the
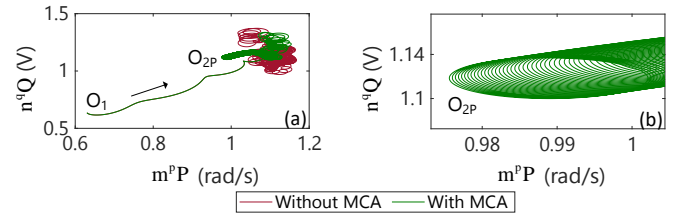

Fig. 11. **(a)** Phase portrait of a DER 1 in n^qQ-m^PP domain during latency attack (τ_m=0.05 s) and 10% data dropout is shown. The operating point O_1 (before cyber attack) traverses to O_2 and O_{2P}, representing operating points obtained without and with MCA respectively. **(b)** Zoomed plot for (a) is shown.

system without the MCA scheme fails to reach a steady-state operating point (even within 3 s of attack initiation), unlike the system with MCA. This is attributed to the signal reconstruction from the local controller steering the control process during the attack. The Fig. 11(b) is zoomed plot for Fig. 11(a). Additionally, it is noted that the convergence time is extended in this scenario for the system without MCA, compared to the case of the sole latency attack.

3) System under TSA: Likewise, the phase portrait for the system subjected to a TSA attack (with load variation at 5 s) is depicted in Fig. 12(a). Evidently, the proposed scheme leads to
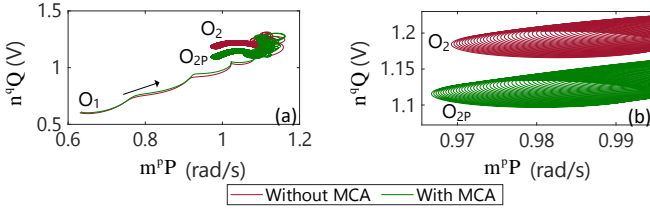
Fig. 12. **(a)** Phase portrait of a DER 1 in $n^q Q$-$m^p P$ domain during TSA is shown. The operating point O_1 (before cyber attack) traverses to O_2 and O_{2P}, representing operating points obtained without and with MCA respectively. **(b)** Zoomed plot for (a) is shown.

enhanced dynamic performance due to signal reconstruction. The zoomed-in plot in Fig. 12(b) further demonstrates that the MCA scheme reduces the convergence time for achieving SC objectives.

4) System under balanced FDIA: The phase portrait for the system under a balanced FDIA at 5 s is presented in Fig. 13(a). Additionally, Fig. 13(b) displays the phase portrait for the system exposed to above case along with a time delay of $\tau_m = 0.05$ s. Clearly, the proposed scheme demonstrates improved dynamic performance through signal reconstruction aided through risk-aware semantic sampling in both scenarios. The semantic sampling expedites convergence through the transmission of significant information.
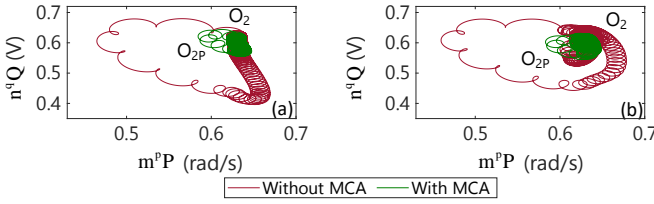

Fig. 13. Phase portrait of a DER 1 in $n^q Q$-$m^p P$ domain during **(a)** balanced FDIA; and **(b)** balanced FDIA with latency attack (τ_m=0.05 s) is shown. O_2 and O_{2P} represents operating points obtained without and with MCA respectively.

5) System under system configuration variation and latency attack: Consider a modified 69-bus distribution system with nine DERs, as shown in Fig. 3. Let this system is initially in network topology N1, with all tie-line switches being open. Suppose the system rearranges at 5 s to a new network topology. This is denoted as N2, with all tie-line switches
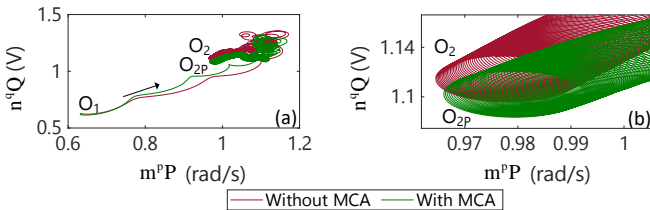

Fig. 14. **(a)** Phase portrait of a DER 1 in $n^q Q$-$m^p P$ domain during latency attack (τ_m=0.05 s) with system reconfiguration is shown. The operating point O_1 (before cyber attack) traverses to O_2 and O_{2P}, representing operating points obtained without and with MCA respectively. **(b)** Zoomed plot for (a) is shown.

being closed. This is further accompanied by a latency attack with time delay of $\tau_m = 0.05$ s. As evident from Fig. 14(a), the

steady state operating point is attained quickly as compared to the absence of the MCA scheme. Fig. 14(b) presents a magnified view of Fig. 14(a). This improved convergence can be attributed to the local reconstruction error provided by the SC, enabled by semantic sampling approach in the proposed scheme.

B. Performance on the real-world SCE 47-bus network

1) System under balanced FDIA: A balanced FDIA was initiated on the system at t = 5 s. Despite system stability being maintained, the convergence time for achieving SC objectives was extended in the absence of the proposed scheme (Fig. 15(a), (b), and (c)) when contrasted with its presence (Fig. 15(d), (e), and (f)). The reconstructed signals ($\zeta_j^{p\varphi}$ and $\zeta_j^{q\varphi}$), generated through the MCA scheme improves the dynamic performance of the system under FDIA. Consequently, the convergence time is reduced.
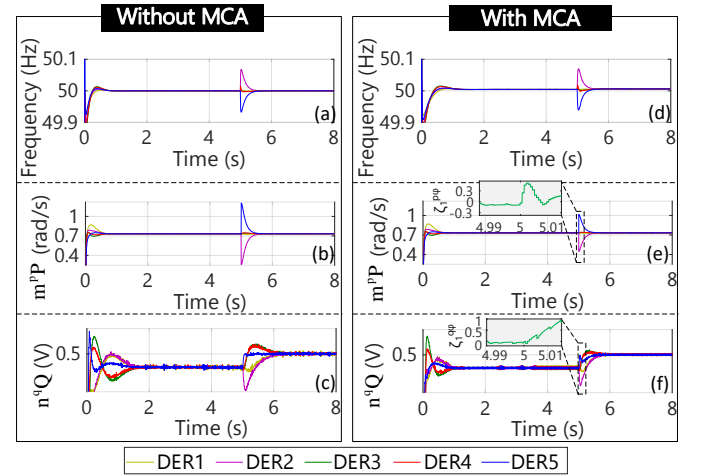

Fig. 15. The time-domain signals during balanced FDIA for **(a)** frequency; **(b)** active power sharing; **(c)** reactive power sharing, without MCA are shown. Further, the time-domain signals for **(d)** frequency; **(e)** active power sharing; **(f)** reactive power sharing, with MCA are shown.

2) System under unbalanced FDIA: The phase portrait of the system subjected to an unbalanced FDIA at t = 5 s is depicted in Fig. 16(a). System instability is evident without the MCA scheme, while the MCA scheme achieves a steady-state operating point. This achievement is attributed to signal reconstruction facilitated by risk-aware semantic sampling.
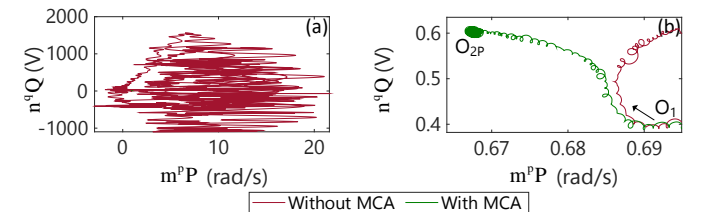

Fig. 16. **(a)** Phase portrait of a DER 1 in $n^q Q$-$m^p P$ domain during unbalanced FDIA is shown. **(b)** Zoomed plot for (a) is shown, where the operating point O_1 (before cyber attack) traverses to O_2 and O_{2P}, representing operating points obtained without and with MCA respectively.

3) System under balanced FDIA and latency attack: A FDIA was initiated on the system with a time delay of $\tau_m = 0.05$ s at 5 s. While system stability was maintained, achieving SC objectives took longer without the proposed scheme (Fig. 17(a), (b), and (c)) compared to with the proposed scheme (Fig. 17(d), (e), and (f)). Additionally, the convergence time is extended in this scenario (without MCA) compared to the case of balanced FDIA attack alone. The proposed scheme actively captures the semantic attributes to enhance its dynamic behavior and reconstruct the required signal to compensate for both FDIA and latency attack at the same time.
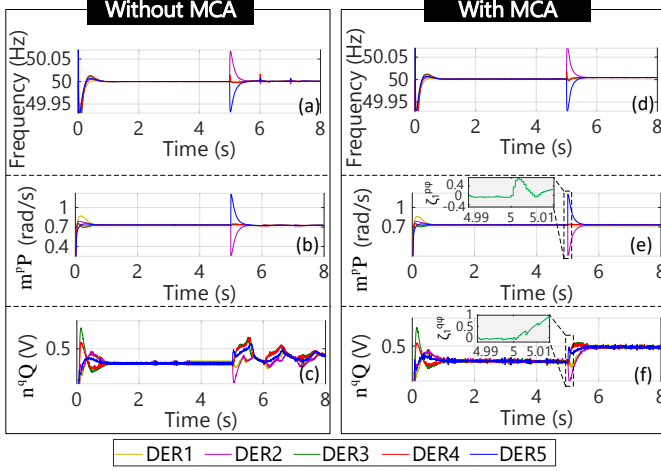

Fig. 17. The time-domain signals during balanced FDIA with latency attack (τ_m=0.05 s) for **(a)** frequency; **(b)** active power sharing; **(c)** reactive power sharing, without MCA are shown. The time-domain signals for **(d)** frequency; **(e)** active power sharing; **(f)** reactive power sharing, with MCA are shown.

4) System under cyber graph variations and latency attack: The system was assessed for cyber graphs variation from fully-connected (T1) to spanning tree (T2), as shown in Fig. 4(c). This is accompanied with a time delay of $\tau_m = 0.05$ s. Fig. 18(a) illustrates that the system trends towards instability due to the sparse network and additional signal delay. The agents couldn't update their states continually, thereby slowing convergence. However, the risk-aware semantic sampling synchronizes error signals at primary and secondary controllers to generate reconstructed signals, rendering the proposed scheme

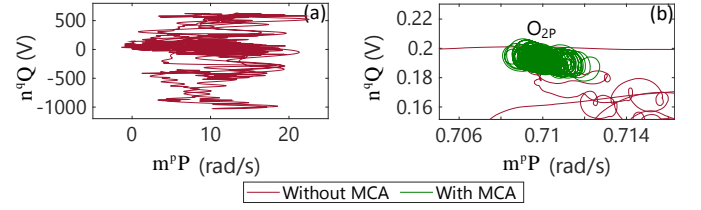robust to dynamic cyber graph variations and latency attacks (Fig. 18(b)).

Fig. 18. **(a)** Phase portrait of a DER 1 in n^qQ-m^pP domain during latency attack (τ_m=0.05 s) with cyber topology variation from T1 to T2 is shown. **(b)** Zoomed plot for (a) is shown, where O_{2P} is the operating point with MCA.

A comparative evaluation of our proposed MCA in contrast to established methodologies is presented in Table III. The proposed methodology in this study distinguishes itself as a computationally efficient solution by incorporating distributed concepts that enhance resilience against data availability and data integrity attacks into a monolithic plane. Its model-agnostic nature further facilitates an easy and streamlined implementation. Additionally, its support for dynamic cyber graphs emphasizes its practicality and flexibility. Furthermore, the scalability of the proposed scheme has been rigorously tested and validated. Consequently from an implementation perspective, the semantic edge intelligence presented by our approach emerges as a highly promising and commercially viable solution to address the intricate challenges within the realm of PES.

VII. CONCLUSIONS AND FUTURE SCOPE OF WORK

This paper introduces methodology to tackle challenges posed by random communication delays, data dropouts, and data integrity attacks single-handedly using a monolithic cybersecurity architecture in PES, incorporating semantic intelligence. The proposed MCA framework leverages the inner control loop dynamics of inverter-integrated DERs and incorporates key semantic attributes, including Priority, Freshness, and Relevance to generate localized compensation signals. This approach has the potential to revolutionize the cybersecurity landscape of PES by simultaneously addressing multiple types of attacks, offering a one-stop solution. Notably, it eliminates the requirement for various intricate models and their complex deployment, a common practice in existing methodologies.

TABLE III
COMPARATIVE ANALYSIS OF THE PROPOSED MONOLITHIC CYBERSECURITY ARCHITECTURE (MCA) FOR PES.

S.No.	Features	[33]	[34]	[35]	**Proposed scheme**
1.	Computational burden	Medium	Medium	High	Low
2.	Distributed concept	✗	✗	✗	✓
3.	Resilient to latency attacks	✓	✓	Not tested	✓
4.	Resilient to TSAs	Not tested	Not tested	Only detection	✓
5.	Resilient to data dropouts	Not tested	Not tested	Not tested	✓
6.	Resilient to FDIAs	Not tested	Not tested	Not tested	✓
7.	Robust to loading variations	✓	✓	✓	✓
8.	Model-agnostic	✗	✗	✓	✓
9.	Supports dynamic cyber graphs	✓	Not tested	Not tested	✓
10.	Scalable	✓	Not tested	Not tested	✓

Real-time simulations conducted in an OPAL-RT environment validate the effectiveness of this approach.

In forthcoming research, demand response scenarios will be investigated through a semantic framework, with a focus on flexibility estimation and synchronizing market requests and bid parameters. The findings will contribute to the development of an innovative demand response model suitable for systems with diverse resources and varied communication protocols.Additionally, semantic-based quantum communication architecture will be explored to expedite fault detection and localization within PES. This enhancement will lead to reduced response times and minimized downtime during substantial disturbances, thereby strengthening system resiliency.

REFERENCES

[1] A. Singhal, T. L. Vu and W. Du, "Consensus Control for Coordinating Grid-Forming and Grid-Following Inverters in Microgrids," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 4123-4133, Sept. 2022, doi: 10.1109/TSG.2022.3158254.

[2] S. Patel, S. Chakraborty, B. Lundstrom, S. M. Salapaka and M. V. Salapaka, "Isochronous Architecture-Based Voltage-Active Power Droop for Multi-Inverter Systems," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1088-1103, March 2021, doi: 10.1109/TSG.2020.3037159.

[3] D. C. Mazur, R. D. Quint and V. A. Centeno, "Time Synchronization of Automation Controllers for Power Applications," *IEEE Trans. Ind. Appl.*, vol. 50, no. 1, pp. 25-32, Jan.-Feb. 2014, doi: 10.1109/TIA.2013.2267710.

[4] Y. Han, K. Zhang, H. Li, E. A. A. Coelho and J. M. Guerrero, "MAS-Based Distributed Coordinated Control and Optimization in Microgrid and Microgrid Clusters: A Comprehensive Overview," *IEEE Trans. Power Electron.*, vol. 33, no. 8, pp. 6488-6508, Aug. 2018, doi: 10.1109/TPEL.2017.2761438.

[5] K. Gupta, S. Sahoo, R. Mohanty, B. Ketan Panigrahi and F. Blaabjerg, "Distinguing Between Cyber Attacks and Faults in Power Electronic Systems—A Noninvasive Approach," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 11, no. 2, pp. 1578-1588, April 2023, doi: 10.1109/JESTPE.2022.3221867.

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

[7] R. Kateb, P. Akaber, M. H. K. Tushar, A. Albarakati, M. Debbabi and C. Assi, "Enhancing WAMS Communication Network Against Delay Attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2738-2751, May 2019, doi: 10.1109/TSG.2018.2809958.

[8] K. Gupta, S. Sahoo, B. K. Panigrahi and C. Konstantinou, "Impact Assessment of Data Integrity Attacks in MVDC Shipboard Power Systems," *IEEE Electric Ship Technologies Symposium (ESTS)*, Alexandria, VA, USA, 2023, pp. 512-519, doi: 10.1109/ESTS56571.2023.10220547.

[9] L. Sheng, G. Lou, W. Gu, S. Lu, S. Ding and Z. Ye, "Optimal Communication Network Design of Microgrids Considering Cyber-Attacks and Time-Delays," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3774-3785, Sept. 2022, doi: 10.1109/TSG.2022.3169343.

[10] M. Kumar, "Resilient PIDA Control Design Based Frequency Regulation of Interconnected Time-Delayed Microgrid Under Cyber-Attacks," *IEEE Trans. Ind. Appl.*, vol. 59, no. 1, pp. 492-502, Jan.-Feb. 2023, doi: 10.1109/TIA.2022.3205280.

[11] T. Yang, Y. He and G. -P. Liu, "Distributed Voltage Restoration of AC Microgrids Under Communication Delays: A Predictive Control Perspective," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 6, pp. 2614-2624, June 2022, doi: 10.1109/TCSI.2022.3163204.

[12] 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.

[13] J. Zhang et al., "Machine Learning-Based Cyber-Attack Detection in Photovoltaic Farms," *IEEE Open J. Power Electron.*, vol. 4, pp. 658-673, 2023, doi: 10.1109/OJPEL.2023.3309897.

[14] M. Alizadeh, H. A. Abyaneh and K. Rouzbehi, "An Enhanced Distributed Event-Triggered Mechanism of Cyber-Switched Communications for Control of Islanded AC Microgrids," *IEEE Sys. J.*, vol. 17, no. 1, pp. 1501-1511, March 2023, doi: 10.1109/JSYST.2022.3206026.

[15] H. Yang, C. Deng, X. Xie and L. Ding, "Distributed Resilient Secondary Control for AC Microgrid Under FDI Attacks," *IEEE Trans. Circuits Syst. II-Express Briefs*, vol. 70, no. 7, pp. 2570-2574, July 2023, doi: 10.1109/TCSII.2023.3245282.

[16] H. Xie, Z. Qin, G. Y. Li and B. -H. Juang, "Deep Learning Enabled Semantic Communication Systems," *IEEE Trans. Signal Process.*, vol. 69, pp. 2663-2675, 2021, doi: 10.1109/TSP.2021.3071210.

[17] M. Kountouris and N. Pappas, "Semantics-Empowered Communication for Networked Intelligent Systems," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 96-102, June 2021, doi: 10.1109/MCOM.001.2000604.

[18] T. Han, Q. Yang, Z. Shi, S. He and Z. Zhang, "Semantic-Preserved Communication System for Highly Efficient Speech Transmission," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 1, pp. 245-259, Jan. 2023, doi: 10.1109/JSAC.2022.3221952.

[19] P. Popovski, O. Simeone, F. Boccardi, D. Gunduz, and O. Sahin, "Semantic-effectiveness filtering and control for post-5G wireless connectivity," *J. Indian Inst. Sci.*, vol. 100, no. 2, pp. 435–443, Apr. 2020.

[20] X. Luo, H. -H. Chen and Q. Guo, "Semantic Communications: Overview, Open Issues, and Future Research Directions," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 210-219, February 2022, doi: 10.1109/MWC.101.2100269.

[21] M. Kountouris and N. Pappas, "Semantics-Empowered Communication for Networked Intelligent Systems," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 96-102, June 2021, doi: 10.1109/MCOM.001.2000604.

[22] D. Gündüz et al., "Beyond Transmitting Bits: Context, Semantics, and Task-Oriented Communications," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 1, pp. 5-41, Jan. 2023, doi: 10.1109/JSAC.2022.3223408.

[23] A. Ali, K. Mahmoud and M. Lehtonen, "Multiobjective Photovoltaic Sizing With Diverse Inverter Control Schemes in Distribution Systems Hosting EVs," *IEEE Trans. Ind. Inform.*, vol. 17, no. 9, pp. 5982-5992, Sept. 2021, doi: 10.1109/TII.2020.3039246.

[24] V. Kekatos, G. Wang, A. J. Conejo and G. B. Giannakis, "Stochastic Reactive Power Management in Microgrids With Renewables," *IEEE Trans. Power Sys.*, vol. 30, no. 6, pp. 3386-3395, Nov. 2015, doi: 10.1109/TPWRS.2014.2369452.

[25] The South California Edison's Distributed Energy Resource Interconnection Map (DERiM). [Online]: https://drpep.sce.com/drpep/.

[26] 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.

[27] M. Elsayed, M. Erol-Kantarci, B. Kantarci, L. Wu and J. Li, "Low-Latency Communications for Community Resilience Microgrids: A Reinforcement Learning Approach," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1091-1099, March 2020, doi: 10.1109/TSG.2019.2931753.

[28] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela and A. D. Domı́nguez-Garcı́a, "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units," *IEEE Trans. Power Sys.*, vol. 28, no. 3, pp. 3253-3262, Aug. 2013, doi: 10.1109/TPWRS.2013.2240706.

[29] E. Shereen, R. Ramakrishna and G. Dán, "Detection and Localization of PMU Time Synchronization Attacks via Graph Signal Processing," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3241-3254, July 2022, doi: 10.1109/TSG.2022.3150954.

[30] S. Sahoo, Y. Yang and F. Blaabjerg, "Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks," *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73-77, Jan. 2021, doi: 10.1109/TPEL.2020.3005208.

[31] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative Control of Multi-Agent Systems: Optimal and Adaptive Design Approaches*. New York, NY, USA: Springer-Verlag, 2014.

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

[33] L. Sheng, G. Lou, W. Gu, S. Lu, S. Ding and Z. Ye, "Optimal Communication Network Design of Microgrids Considering Cyber-Attacks and Time-Delays," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3774-3785, Sept. 2022, doi: 10.1109/TSG.2022.3169343.

[34] T. Yang, Y. He and G. -P. Liu, "Distributed Voltage Restoration of AC Microgrids Under Communication Delays: A Predictive Control Perspective," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 6, pp. 2614-2624, June 2022, doi: 10.1109/TCSI.2022.3163204.

[35] 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.