Delay-Aware Semantic Sampling in Power Electronic Systems

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

Published in:
I E E E Transactions on Smart Grid

DOI (link to publication from Publisher):
10.1109/TSG.2023.3339707

Publication date:
2024

Document Version
Accepted author manuscript, peer reviewed version

Delay-Aware Semantic Sampling in Power Electronic Systems

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

***Abstract*—In power electronic systems (PES), attacks on data availability such as latency attacks, data dropouts, and time-synchronization attacks (TSAs) continue to pose significant threats to both the communication network and the control system performance. As per the conventional norms of communication engineering, PES still rely on time synchronized sampling, which translates every received message with equal importance. In this paper, we go beyond event-triggered sampling/estimation to integrate *semantic* principles into the sampling process for each distributed energy resource (DER), which not only compensates for delayed communicated signals by reconstruction of a new signal from the inner control layer dynamics, but also evaluates the reconstruction stage using key semantic requirements, namely `Freshness`, `Relevance` and `Priority` for good dynamic performance. As a result, the sparsity provided by event-driven sampling of internal control loop dynamics translates as *semantics* in PES. The proposed scheme has been extensively tested and validated on a modified IEEE 37-bus AC distribution system, under many operating conditions and noisy environment in OPAL-RT environment to establish its robustness, model-free design ability and adaptive behavior to dynamic cyber graph topologies.**

***Index Terms*—Data dropout, delay-aware semantic sampling, distributed control, inner control loop dynamics, latency attack, power electronic systems (PES), time synchronization attack (TSA).**

NOMENCLATURE

Indices and sets

N_j	The set of neighbouring DERs to j^{th} DER
j, m	Index of DERs in PES

Parameters

α	Alpha, a tunable parameter
$\Delta\omega\mathrm{c}_j$ and $\Delta\mathrm{Vc}_j$	Frequency and voltage correction term from secondary controller of j^{th} DER
σ_m	Information received from m^{th} DER
τ_m	Time delay from m^{th} DER
a_{jm}	Communication weight
F and R	Freshness and relevance
g_j	Convergence parameter of j^{th} DER
$\mathrm{m}_j^{\mathrm{p}}$ and $\mathrm{n}_j^{\mathrm{q}}$	Active and reactive power droop coefficient of j^{th} DER
$\mathrm{u(t)}$	Timestamp of the latest packet received at destination by time t
D	Downsampling factor

Variables

k_1 and k_2	Tunable gains
t_a	Triggering moment
$\mathbf{e}_j$	Vector of error of j^{th} DER, fed to the prediction policy
$\mathbf{e}_j^{\mathbf{dqD}}$	Vector of downsampled signal of j^{th} DER
$\mathbf{e}_j^{\mathbf{dqVC}}$	Vector of error signals provided to local voltage controller of j^{th} DER
$\mathbf{e}_j^{\mathbf{R}}$	Vector of reconstructed signals of j^{th} DER
$\mathbf{u}_j^{\mathbf{pqf}}$	Vector of final predictive inputs to secondary controller of j^{th} DER
$\mathbf{u}_j^{\mathbf{pq}}$	Vector of local control inputs to secondary controller of j^{th} DER

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).

I. INTRODUCTION

POWER electronic systems (PES) play a crucial role in enhancing efficiency, promoting sustainability and enabling flexibility. Achieving these objectives necessitates resilient control integrated with communication within PES, thus transforming PES into sophisticated cyber-physical system. The control framework of PES in this work, involves primary and secondary controllers. The conventional centralized secondary controllers (SCs) have limitations such as, high communication bandwidth, vulnerability to single-point failures and high computational complexity. To address these drawbacks, a highly reliable and scalable distributed secondary control (DSC) architecture is widely accepted, which only requires information from neighboring agents [1]. This complex network requires time-synchronized measurements. Global navigation satellite signals (GNSSs), such as GPS, GLONASS, BeiDou and Galileo, are the primary sources of time synchronization due to their worldwide coverage and high accuracy [2]. Intelligent electronic devices (IEDs) and merging units depend on GNSS for time transfer, using methods such as precision time protocol (PTP), inter-range instrumentation group time code B (IRIG-B), or one pulse per second (1PPS) [3]. However, integrating communication network exposes them to various constraints, like delays, data loss, and uncertain links [4]. These can cause delayed exchange of measurement/control signals among distributed energy resources (DERs), affecting system performance.

The cyber-physical system further create opportunities for malicious attackers to launch coordinated cyber attacks.

Among several cyber attacks [5], [6], this paper focuses on time delay-based cyber attacks, which can be strategically introduced into the control system by an adversary [7]. The time-synchronization attacks (TSAs) are a new kind of attack, which can manipulate the timing signals by corrupting the GNSS signals. Attackers can use a receiver-spoofer mechanism [8], where the spoofer itself is a GPS receiver. Both space-based time synchronization (SBTS) and network-based time synchronization (NBTS) mechanisms [9] lack integrated security controls and have been accounted as highly vulnerable to TSAs [10]. This leads to false measurements and inaccurate time stamps, severely affecting the stability of the system.

The massive importance of time synchronized real-time measurements in cyber-physical networks makes it a valuable target to adversaries. Moreover, since PES have low system inertia and high response speed, the impact of these attacks are more significant than in bulk power systems. Therefore, making it crucial to design controllers that can withstand such cyber attacks within real-time operational constraints. In prior works, such as [11] and [12], optimization-based methods were proposed for enhancing microgrid dynamic performance under communication delays. Nevertheless, these techniques come with notable computational overhead, especially in complex networks, and can be sensitive to initial conditions, potentially yielding suboptimal results. Another approach, as seen in [13], employs predictive control theory, demanding a substantial amount of modeling knowledge. The requirement of observer/estimator in this scheme, increases the complexity further. Moreover, these schemes often struggle to establish resilience to unknown dynamics, risking performance degradation or instability. Furthermore, [14] introduces an anomaly-based scheme to detect the presence of TSAs and other attacks. However, this scheme necessitates a training phase, potentially entailing high memory and critical data requirements. Data-driven methods like these may require hyperparameter tuning and might encounter overfitting issues. While TSA detection schemes have been investigated in [15] and [16], they lack a mitigation strategy to ensure stable PES operation during delays. Therefore, the existence of numerous distinct strategies to individually address data availability attacks, which often entail complex modeling or training approaches, motivated our proposal of a unified approach, capable of effectively mitigating all forms of such attacks. For this, we exploit the science of semantics to decipher a novel delay-aware semantic sampling scheme in this paper. Semantic principles have gained traction in various domains, including communication systems [17] and networked intelligent systems [18]. In speech recognition, semantics improves accuracy and efficiency in transforming spoken language into text [19]. The post-5G era sees semantics shaping the future of wireless networks [20]. For comprehensive insights into semantic communication and its applications, interested readers are encouraged to refer [21].

Real-time systems, such as smart grids and networked systems, rely on an automated sense-compute-actuate cycle for decision-making. The effectiveness of the connectivity in these systems hinges on the provision of *right information to the right place at the right time*. During data availability attacks, our proposed delay-aware semantic sampling scheme addresses the challenge of real-time control operation and stability due to missing samples by employing *semantic communication & sampling*. The proposed scheme furnishes delay-compensation signals to the controller locally by rectifying the above mentioned missing samples through a semantic reconstruction process. This approach harnesses semantic attributes, namely value, freshness, and relevance, which are governed by factors like prioritization of the most significant signal for estimation, age of information (AoI), and reconstruction error, respectively. These semantics attributes tune the reconstruction process by extraction of *significant* information from the dynamics of inner control loops through semantic sampling. These reconstructed signals are subsequently provided at a local level to SCs, effectively mitigating delays introduced by adversaries through data availability attacks. This distributed learning approach enhances the reliability and timeliness of information flow within real-time systems, enhancing the overall performance and resilience of PES.

In particular, the main contributions and benefits of this work are highlighted as:

- The proposed delay-aware semantic sampling scheme, exploits significant information extracted from the inner control loop dynamics to provide reconstructed signals to local SC, facilitating delay compensation. This strategic approach minimizes redundant data transmissions.
- The proposed scheme in this work, is robust against latency attacks, data dropouts and TSAs. It also guarantees the SC objectives are met under such attack scenarios.
- The proposed delay-aware semantic sampling scheme embraces distributed approach, in contrast to complex centralized methods requiring intricate coordination between numerous components. Here, individual DERs independently handle local delay compensation, streamlining operations and enhancing manageability.
- The proposed scheme in this work, is model-agnostic. This simplifies implementation by eliminating the need for numerous device-specific models.
- Unlike training-based approaches that demand substantial computational resources, extensive datasets, and meticulous hyperparameter tuning, our approach operates without the need for training. It also does not have any additional hardware requirements.

The remainder of this paper is organized as: the science and relevance of semantics is explained in Section II. A brief description on modeling of cyber-physical PES is provided in Section III. The description, challenges and modeling of data availability attacks are illustrated in Section IV. The novel delay-aware semantic sampling approach is presented in Section V. The real-time simulation testbed setup and the performance evaluation of the proposed delay-aware semantic sampling scheme, is presented in Section VI. Finally, Section VII encapsulates the concluding remarks and future work.

II. Science and Relevance of Semantics

The term "*semantics*" originated from the ancient Greek word "*semantikos*", meaning *significant*, and has evolved to refer to "*meaning*" in the context of languages. However,

in this work, the term "*semantics*" is used in its original sense of "significance" with regards to information. This approach recognizes that the relevance of information can vary depending on the application.

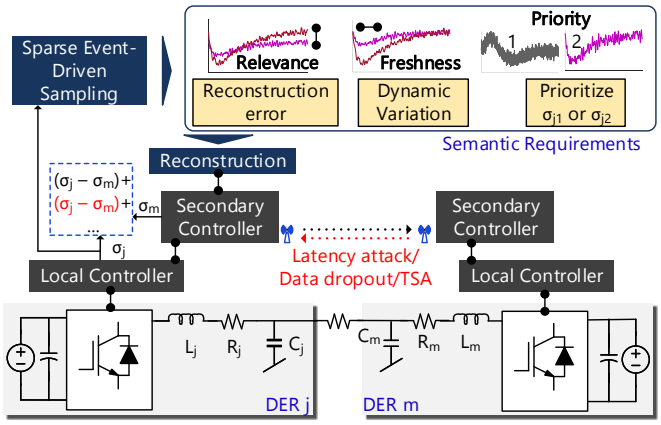

Fig. 1. Semantic information exchange and estimation in PES – sparse event-driven sampling from local error measurements steer the estimation and reconstruction process during latency attack/data dropout/TSAs.

In semantic sampling, the three attributes of evaluating the criticality/significance of information are freshness, value, and relevance. Their definitions are as follows:

- `Freshness` refers to sending new updates at *the right time*. It is defined as the time for the newest sample of information to reach from the source to the destination. Considering $\mathrm{u(t)}$ to be the timestamp of the latest packet received at destination by time t, freshness is expressed as $\mathrm{F(t) = t - u(t)}$.
- `Value` refers to providing timely and *right piece of information* to the *right point of computation*, particularly in cyber-physical and hierarchical control systems. It defines `Priority` of information.
- `Relevance` involves generating the *right piece of information* by sampling. It measures the extent of change in a process since the last recorded sample.

Based on the semantic requirements described above, we exploit it in the sampling and reconstruction process of new signals for each DER locally in PES, as shown in Fig. 1. As a result, the key focus is on steering the accuracy of estimation amid latency attacks, data dropouts and TSAs. Additionally, the semantic attributes i.e, relevance, freshness and priority are governed by reconstruction error, dynamic variation and prioritization of the most significant local signal to be used for estimation, respectively. Therefore, the semantic models pave way towards a standardized mechanism to represent and interpret from the relevant data collected from various devices and sensors across the network.

III. Modeling Preliminaries

A. Physical Framework

To demonstrate the modeling and control framework of a PES, the modified IEEE 37-bus system is presented in Fig. 2(a), with distributed loads powered by seven DERs. In the considered system, each DER can be represented by a DC source (denoting an energy storage system), DC/AC converter, LC filter ($\mathrm{r^f}$, $\mathrm{L^f}$, $\mathrm{C^f}$) and RL output impedance ($\mathrm{r^o}$, $\mathrm{L^o}$). The $d-q$ axis control framework comprises of inner control loops (voltage control (VC) and current control (CC)), cascaded with the primary droop control (DC) loop, as shown in Fig. 2(b). The merging units transmit the time-synchronized measurements (facilitated by GPS) to these controllers for the controller operation. As shown in Fig. 2(b), the GPS clock offers synchronized measurements of time by IRIG-B, PTP or 1PPS. The adopted frequency and voltage droop are:

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

$$\mathrm{V_j^{d*}(t) = V_{nom} - n_j^q Q}_j(\mathrm{t}) \;\;,\;\; \mathrm{V_j^{q*}(t) = 0} \tag{2}$$

where, the subscript 'j' represents the parameters associated to j^{th} DER. The terms ω_{nom} and $\mathrm{V_{nom}}$ are the nominal frequency and voltage of the AC system, respectively. The local reference frequency and voltage of a DER are ω_j^* and $\mathrm{V_j^{dq*}}$. Here, $\mathrm{V_j^{dq*}(t) = [V_j^{d*}(t)\ V_j^{q*}(t)]^T}$. The active and reactive power droop coefficient are $\mathrm{m^p}$ and $\mathrm{n^q}$, respectively. More information about its control layer modeling can be referred from [22]. Since primary control inherently results in non-zero steady-state error, the DSC scheme is integrated, as in Fig. 2(b), described in the next subsection.

B. Cyber Framework

Let us consider PES with M power electronic-interfaced DERs in a sparsely-connected DSC based communication network. These DERs are termed as agents/nodes in cyber layer and are represented as $\mathbf{x} = \{\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_M\}$. These agents are linked to their neighbouring agents by edges $\mathbf{E}$ via an associated adjacency matrix, $\mathbf{A_G} = [\mathrm{a}_{jm}] \in \mathbf{R}^{N\times N}$. 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, $\sigma_m = [\omega_m \;\; \mathrm{m_m^p P} \;\; \mathrm{n_m^q Q}]^{\mathrm{T}}$. The matrix representing incoming information can be given as, $\mathbf{D}_{\mathrm{in}} = \mathtt{diag}\{\mathrm{d_j^{in}}\}$, where $\mathrm{d_j^{in}} = \sum_{m\in \mathrm{N}_j} \mathrm{a}_{jm}$. Combining the sending and receiving end information into a single matrix, we obtain Laplacian matrix $\mathbf{L} = [\mathrm{l}_{jm}]$, where l_{jm} are its elements defined such that, $\mathbf{L} = \mathbf{D}_{\mathrm{in}} - \mathbf{A}_{\mathrm{G}}$. According to [22], local reference frequency and voltage of DER, as expressed in (1) and (2), are re-defined as:

$$\omega_j^*(\mathrm{t}) = \omega_{\mathrm{nom}} - \mathrm{m_j^p P}_j(\mathrm{t}) + \Delta\omega \mathrm{c}_j(\mathrm{t}) \tag{3}$$

$$\mathrm{V_j^{d*}(t) = V_{nom} - n_j^q Q}_j(\mathrm{t}) + \Delta \mathrm{Vc}_j(\mathrm{t}) \tag{4}$$

where, $\Delta\omega\mathrm{c}$ and $\Delta\mathrm{Vc}$ are the frequency and voltage correction terms from the SC, expressed as:

$$\begin{aligned}\Delta\omega \mathrm{c}_j(\mathrm{t}) = &- \mathrm{H}_1(s)[\omega_{\mathrm{nom}} - \omega_j(\mathrm{t}) + \\ &\mathrm{g}_j \sum_{m\in \mathrm{N}_j} \mathrm{a}_{jm}\left(\omega_m(\mathrm{t}) - \omega_j(\mathrm{t})\right) + \\ &\mathrm{g}_j \sum_{m\in \mathrm{N}_j} \mathrm{a}_{jm}\left(\mathrm{m_m^p P}_m(\mathrm{t}) - \mathrm{m_j^p P}_j(\mathrm{t})\right)]\end{aligned} \tag{5}$$

Similarly,

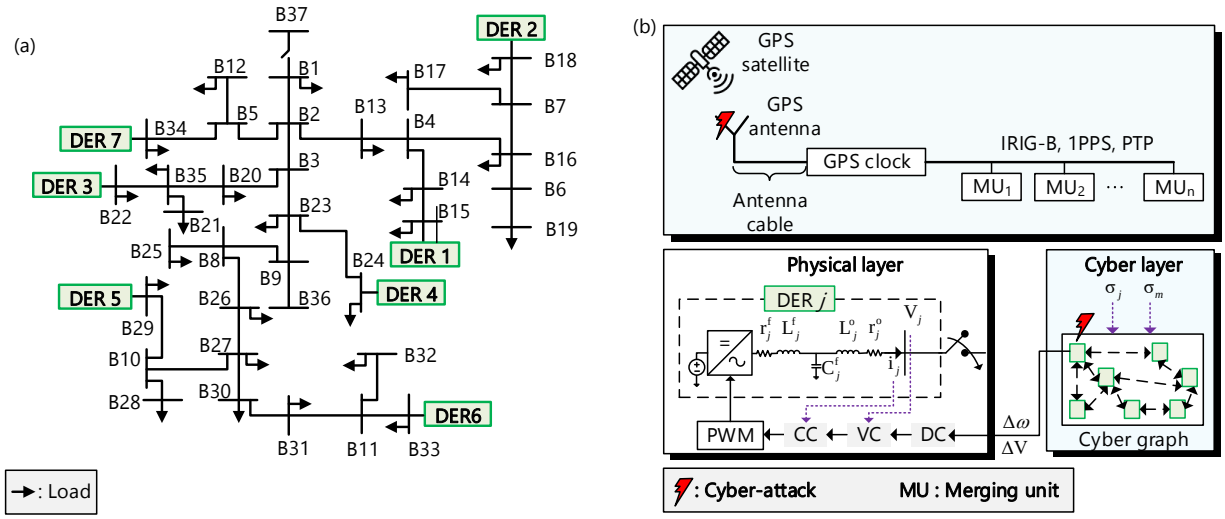

Fig. 2. (a) The modified IEEE 37-bus islanded AC distribution system powered by seven DERs is shown. (b) The block diagram of cyber-physical DER with primary and DSC architecture is presented. The DSC receives local measurements (σ_j) and neighbouring measurements (σ_m) as input to generate frequency and voltage correction terms ($\Delta\omega$ and ΔV). Note that the merging units (MUs) receive the timing information from GPS satellite. These time-stamped measurements are then used by the controllers for generating control signals, which can directly affect the control operation of the system.

$$\Delta \mathrm{Vc}_j(\mathrm{t}) = -\mathrm{H}_2(\mathrm{s})[\mathrm{g}_j \sum_{m\in \mathrm{N}_j} \mathrm{a}_{jm}\left(\mathrm{n}_m^{\mathrm{q}}\mathrm{Q}_m(\mathrm{t}) - \mathrm{n}_j^{\mathrm{q}}\mathrm{Q}_j(\mathrm{t})\right)] \tag{6}$$

where, $\mathrm{H}_1(\mathrm{s})$ and $\mathrm{H}_2(\mathrm{s})$ are PI controllers for frequency restoration along with proportional active power sharing; and proportional reactive power sharing, respectively. The local control input of SC can be given by:

$$\mathbf{u}_j(\mathrm{t}) = \mathrm{g}_j \sum_{m\in \mathrm{N}_j} \underbrace{\mathrm{a}_{jm}\left(\boldsymbol{\sigma}_m(\mathrm{t}) - \boldsymbol{\sigma}_j(\mathrm{t})\right)}_{\mathbf{e}_{jm}(\mathrm{t})} \tag{7}$$

where, $\mathbf{u}_j = [\mathrm{u}_j^{\mathrm{p}} \ \mathrm{u}_j^{\mathrm{q}}]^{\mathrm{T}}$, $\mathbf{e}_{jm} = [\mathrm{e}_{jm}^{\mathrm{p}} \ \mathrm{e}_{jm}^{\mathrm{q}}]^{\mathrm{T}}$, depending on the elements in $\boldsymbol{\sigma}$; and g_j is the convergence parameter.

These information exchanges can be limited by data availability cyber-attacks, which then aggravates the system monitoring and controllability due to missing information, as explained in the next section.

IV. Overview of Data Availability Attacks

A. Latency Attacks and Data Dropouts

Description and challenges: Communication time-delays are an inherent part of any communication system encompassing four primary components: propagation delay, transmission delay, processing delay, and queuing delay [24]. In the DSC architecture, real-time periodic communication is essential for efficient operation. However, data congestion can introduce unpredictable delays, influenced by factors like cyber sampling rate, data volume, and cyber graph connection. These delays, ranging from milliseconds to seconds, can disrupt system operation if they exceed SC operational time limits [25]. Preventive measures are crucial to avoid missed updates that could lead to oscillatory instability or system failure.

Furthermore, cyber attackers can exacerbate issues by intentionally adding time delays to critical messages, known as latency attacks (as shown in Fig. 3(a)). This can severely impact time-critical information transfer between SCs. Network congestion can also cause frequent data dropouts (as shown in Fig. 3(a)), further compromising dynamic performance.

Attack model: The DSC fundamentally relies on the accurate transmission of data from neighboring agents. Latency attacks, which introduce falsifications in timing signals, pose a substantial threat to the operational stability of the system. These attacks can exert a profound influence on the control laws that govern the behavior of cyber-physical PES, potentially leading to significant deviations from desired performance.

In this context, considering the neighbors of the j^{th} agent be denoted as $\mathrm{N}_j = m \mid (\mathrm{x}_m, \mathrm{x}_j) \in \mathbf{E}$. The local control input of the SC, when subjected to latency attack is:

$$\mathbf{u}_j^{\mathrm{L}}(t) = \mathrm{g}_j \sum_{m\in \mathrm{N}_j} \mathrm{a}_{jm}\left(\boldsymbol{\sigma}_m(\mathrm{t}-\tau_m) - \boldsymbol{\sigma}_j(\mathrm{t}-\tau_j)\right) \tag{8}$$

where, τ_j and τ_m are the delays from the local and neighbouring agents. By Leibnitz formula, the delayed parameter can be expressed as, $\sigma(\mathrm{t}-\tau) = \sigma(\mathrm{t}) - \int_{\mathrm{t}-\tau}^{\mathrm{t}} \dot{\sigma}(\mathrm{s})\mathrm{ds}$. For a delay of τ_m, substituting this in (8), we obtain, $\dot{\sigma}(\mathrm{t}) = -\mathbf{L}\sigma(\mathrm{t}) - \mathbf{A}\int_{\mathrm{t}-\tau_{\mathrm{m}}}^{\mathrm{t}} \dot{\sigma}(\mathrm{s})\mathrm{ds}$. Similarly, the expression for local delay can also be obtained. For a fixed, undirected and connected cyber graph, the equilibrium is reached, if and only if, $0 < \tau < \frac{\pi}{2\lambda_{\max}\mathbf{L}}$, with λ_{max} being the largest eigenvalue of $\mathbf{L}$. Thus, the communication delay (τ) must be bounded inside these limits to obtain $\dot{\sigma}(\mathrm{t}) = 0$.

B. Time Synchronization Attacks (TSAs)

Recently, there has been a significant upsurge in TSAs, which is becoming a growing concern across various sectors. This concern arises from the susceptibility of GPS signals to compromise by unintentional sources like radio frequency (RF) interference and space weather events such as solar flares. Such interference can result in timing errors or even complete signal loss, posing critical risks to time-sensitive applications.

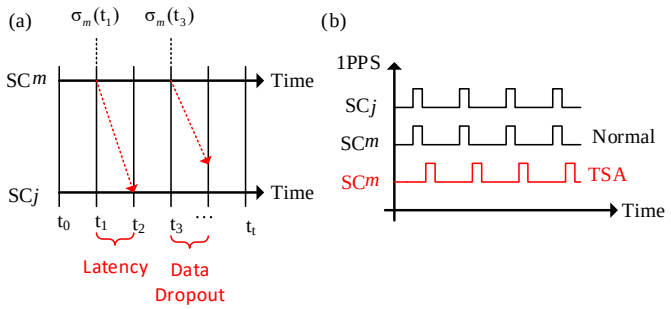

Fig. 3. **(a)** Latency attack and data dropout; and **(b)** TSA.

Beyond unintentional disruptions, GPS receivers in devices like substation clocks or merging units face vulnerability to deliberate attacks by malicious actors. For instance, GNSS signals, transmitted by satellite constellations in medium earth orbit (MEO), exhibit low power levels, with a power density of fW/m^2 (10^{-15} W/m^2) upon reaching the Earth's surface [26]. To illustrate, this is akin to observing a 25 W light bulb from a distance of 10,000 miles. Consequently, these signals become susceptible to blocking or jamming over extensive areas through low-power terrestrial transmitters, effectively saturating the GNSS signal spectrum with noise or an unmodulated carrier.

While the *blocking/jamming attack* is relatively straightforward to detect due to a complete time loss, *spoofing* of GNSS signals presents a more challenging threat. Spoofing entails the broadcast of fraudulent GPS signals or the rebroadcasting of GPS signals captured at a different time-step at the target receiver (as shown in Fig. 3(b)). This deceptive manipulation can lead to time synchronization loss, diminishing network synchronization performance and, consequently, reducing the stability and reliability of the PES.

Attack model: GNSS timing relies on phase of pseudo-random noise (PRN) codes within received signals [15]. To manipulate timing results, TSA signals must alter these values, as shown in Fig. 4. Initially, the attacker aligns TSA signal code phases with authentic ones, maintaining a relatively low signal power, as shown in Fig. 4(a). Once alignment is achieved, the attack can be initiated at any time by increasing TSA signal power while slowly shifting code phases away, as shown in Fig. 4(b). Tracking loops will then lock onto TSA correlation peaks due to their higher power, enabling TSA signals to dominate all tracking loops without causing them to lose lock on signals. Simultaneously, the victim's code undergo gradual alteration, introducing errors into the timing results, as shown in Fig. 4(c). More details regarding TSA modelling can be referred from [10].

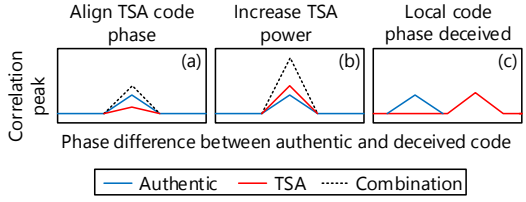

Fig. 4. Spoofing procedure for TSA. **(a)** Aligning TSA code phase with authentic one; **(b)** initiating attack by increasing TSA signal power; and **(c)** gradual alteration of the victim's code to introduce timing error.

In such events the time-stamped data of the victim node, $\boldsymbol{\sigma}_m(\mathrm{t})$ is manipulated by an offset of $\mathrm{nT_s}$ samples, the resultant attacked information can be expressed as:

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

Whether the adversary chooses to add or subtract these $\mathrm{nT_s}$ samples, the timing information is compromised, which can lead to time synchronization loss. Consequently, inaccurate time stamps which reverberate through the entire system, exerts a detrimental influence on the precise coordinated operation of DERs within the PES. Within the SC, the integrator accumulates error based on the latest available data. The gradual accumulation of error over time can be substantial which can steer the control system away from its intended setpoint. The control system may exhibit undesirable behaviors such as oscillations, overshooting, etc. As the error accumulates and amplifies, it has the potential to induce instability.

In PES, the above-mentioned cyber attacks can result in a host of problems ranging from sub-optimal operating conditions to outright instability of the system. This instability may even cause inadvertent disconnection of sources/ loads, leading to partial/full shutdown of the system, thereby jeopardizing the security of electrical supply. To address these challenges, it is crucial to implement a robust control system to handle unpredictable delays. Therefore, efforts are accumulated to work in this direction, presented in the next section.

V. Proposed Delay-Aware Semantic Sampling

As previously mentioned, the term *semantics* refers to the significance of information. By incorporating the concept of information semantics, this paper aims to provide a more nuanced and comprehensive understanding of the role of information in decision-making during delays in networked PES. The contextual representation of semantics in PES refers to capturing the attributes of inner control loop signals, such as timeliness and value, to reconstruct significant information necessary for delay compensation in scenarios involving random delay attacks. In distributed control of AC distribution systems, timely consensus negotiation among agents is crucial for global frequency regulation and proportional active/reactive power sharing. Semantic-aware transmission, which respects the time-dependent value of signals, is essential to ensure achieving the SC objectives.

Time-critical applications like smart grids and networked control require a restructured message transfer system due to the huge amount of data involved. Hence, this paper proposes a semantic sampling architecture as shown in Fig. 5, that generates and transmits the right amount of data to the right place at the right time. This includes following steps:

i) *Delay-aware semantics:* To comprehend the proposed approach, it is crucial to apply the PI consensusability law [27] to anticipate the physical layer semantics using the response of each control loop under disturbances.

This proposed scheme is local to each SC and firstly extracts significant information from the error signal corresponding to the VC ($\mathbf{e}_j^{\mathbf{dqVC}}(\mathrm{t})$). Here, $\mathbf{e}_j^{\mathbf{dqVC}}(\mathrm{t}) = [\mathrm{e}_j^{\mathrm{dVC}}(\mathrm{t}) \;\; \mathrm{e}_j^{\mathrm{qVC}}(\mathrm{t})]^{\mathrm{T}}$.

ii) *Process-aware sparse sampling [28], [29]:* The signal $\mathbf{e}_j^{\mathbf{dqVC}}(\mathrm{t})$, is then downsampled (shown in Fig. 5(a)), as:

$$\mathrm{e}_j^{\mathrm{dD}} = \sum_{w=0}^{\mathrm{W}-1} \mathrm{e}_j^{\mathrm{dVC}}[\mathrm{nD} - w].\delta[w] \tag{10}$$

$$\mathrm{e}_j^{\mathrm{qD}} = \sum_{w=0}^{\mathrm{W}-1} \mathrm{e}_j^{\mathrm{qVC}}[\mathrm{nD} - w].\delta[w] \tag{11}$$

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 error quantities fed to VC (i.e, $\mathrm{e}_j^{\mathrm{dVC}}(\mathrm{t})$ and $\mathrm{e}_j^{\mathrm{qVC}}(\mathrm{t})$) and error fed to SC (i.e, $\mathbf{u}_j(\mathrm{t})$). This crucial step aids in the synchronization of the multi-time scale error signals. This approach significantly lowers device energy consumption. This effect is rooted in the definition of energy consumption, which is the product of power consumption and processing time for each sample [30]. Downsampling, by reducing the number of samples based on the D, decreases energy consumption as D increases. This is crucial particularly for low-power/energy-harvesting sensors, while also enabling efficient bandwidth utilization.

iii) *Effective decision making:* The generated downsampled signals ($\mathrm{e}_j^{\mathrm{dD}}(\mathrm{t})$ and $\mathrm{e}_j^{\mathrm{qD}}(\mathrm{t})$) are compared with the local control inputs from the SC (i.e, $\mathrm{u}_j^{\mathrm{p}}(\mathrm{t})$ and $\mathrm{u}_j^{\mathrm{q}}(\mathrm{t})$), as shown in Fig. 5(a). The semantic prediction policy subsequently rebuilds the signals used for delay compensation (i.e, $\mathbf{e}_j(t_a) = [\mathrm{e}_j^{\mathrm{p}}(t_a) \;\; \mathrm{e}_j^{\mathrm{q}}(t_a)]^{\mathrm{T}}$) as:

$$\mathbf{e}_j(t_a) = [\mathrm{e}_j^{\mathrm{dD}}(t_a) \;\; \mathrm{e}_j^{\mathrm{qD}}(t_a)] - \mathbf{u}_j \tag{12}$$

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:

$$||\mathbf{e}_j(t_a)|| > \alpha||e^{-\mathrm{t}/\mathrm{T}}.[\mathrm{e}_j^{\mathrm{dVC}} \;\; \mathrm{e}_j^{\mathrm{qVC}}]|| \tag{13}$$

where, α is a tunable parameter, $\mathrm{T} = \mathrm{K_p}/\mathrm{K_i}$ is the controller time constant of $\mathrm{H_1(s)}$ and $\mathrm{H_2(s)}$ PI control loops. If the condition expressed in (13) is met, triggers are produced. These triggers are utilized to reconstruct $\mathbf{e}_j^{\mathbf{R}}(\mathrm{t}_a)$ using a sample-and-hold circuitry, with t_a being the triggering instant. This is followed by evaluation of semantic attributes i.e, freshness ($\mathrm{F(t)}$), value and relevance ($\mathrm{R(t)}$) defined as:

$$\mathrm{F(t)} = \mathrm{t} - \mathrm{u(t)} \;\;,\;\; \mathrm{R(t)} = \mathbf{e}_j(t) - \mathbf{e}_j^{\mathbf{R}}(t) \tag{14}$$

where, $\mathrm{u(t)}$ is the timestamp of the latest packet received at destination by time t.

iv) *Feedback generation:* The resulting reconstructed signals are subsequently fed back to SC, with their tunable gains, $\mathrm{k_1}$ and $\mathrm{k_2}$, represented as:

$$\mathrm{e}_j^{\mathrm{p}\varphi}(t_a) = \mathrm{k_1}\mathrm{e}_j^{\mathrm{Rp}}(t_a) \;\;,\;\; \mathrm{e}_j^{\mathrm{q}\varphi}(t_a) = \mathrm{k_2}\mathrm{e}_j^{\mathrm{Rq}}(t_a) \tag{15}$$

where, $\mathbf{e}_j^{\mathbf{R}}(t_a) = [\mathrm{e}_j^{\mathrm{Rp}}(t_a) \;\; \mathrm{e}_j^{\mathrm{Rq}}(t_a)]^{\mathrm{T}}$. Finally these inputs are added to the control inputs of SC as:

$$\mathrm{u}_j^{\mathrm{pf}}(\mathrm{t}) = \mathrm{u}_j^{\mathrm{p}}(\mathrm{t}) + \mathrm{e}_j^{\mathrm{p}\varphi}(t_a) \;\;,\;\; \mathrm{u}_j^{\mathrm{qf}}(\mathrm{t}) = \mathrm{u}_j^{\mathrm{q}}(\mathrm{t}) + \mathrm{e}_j^{\mathrm{q}\varphi}(t_a) \tag{16}$$

where, $\mathrm{u}_j^{\mathrm{pf}}$ and $\mathrm{u}_j^{\mathrm{qf}}$ are the final predictive inputs to the SC to compensate the delays.

The control objectives of the proposed delay-aware semantic sampling scheme, may be summarized as:

(i) To address delayed communication signals resulting from latency attacks, data dropouts, or TSAs by incorporating

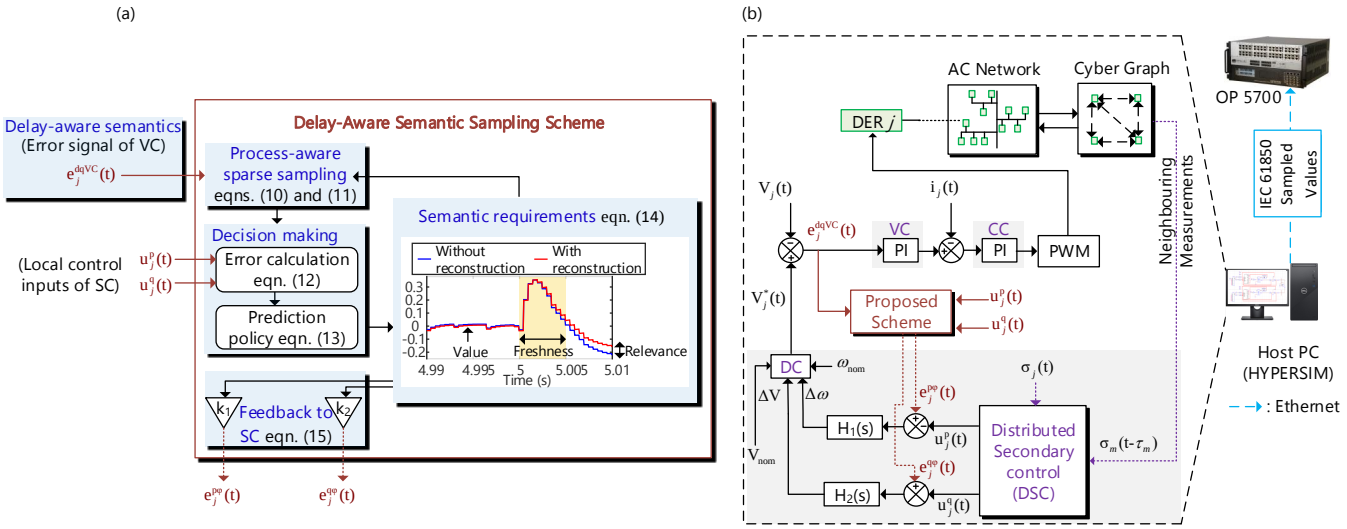

Fig. 5. **(a)** Proposed delay-aware semantic sampling scheme. **(b)** Deployment of the proposed scheme in real-time simulation testbed. The testbed is interfaced with Ethernet to facilitate establishment of IEC 61850 sampled values protocol.

Algorithm: Proposed delay-aware semantic sampling scheme at j^{th} DER

Inputs: Error signals provided to VC ($\mathbf{e}_j^{\mathbf{dqVC}}(\mathrm{t})$), length of window (W), downsampling factor (D), local control inputs to SC ($\mathbf{u}_j^{\mathbf{pq}}(\mathrm{t})$), tunable parameter ($\alpha$), controller time constant of $\mathrm{H_1(s)}$ and $\mathrm{H_2(s)}$ PI control loops ($\mathrm{T = K_p/K_i}$), triggering moment (t_a), tunable gains ($\mathrm{k_1}$ and $\mathrm{k_2}$)

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

Note: $\mathbf{e}_j^{\mathbf{dqVC}}(\mathrm{t}) = [\mathrm{e}_j^{\mathrm{dVC}}(\mathrm{t})\ \ \mathrm{e}_j^{\mathrm{qVC}}(\mathrm{t})]^{\mathrm{T}}$,
$\mathbf{e}_j^{\mathbf{dqD}}(\mathrm{t}) = [\mathrm{e}_j^{\mathrm{dD}}(t)\ \ \mathrm{e}_j^{\mathrm{qD}}(t)]^{\mathrm{T}}$, $\mathbf{u}_j(\mathrm{t}) = [\mathrm{u}_j^{\mathrm{p}}(\mathrm{t})\ \ \mathrm{u}_j^{\mathrm{q}}(\mathrm{t})]^{\mathrm{T}}$,
$\mathbf{e}_j(\mathrm{t}_a) = [\mathrm{e}_j^{\mathrm{p}}(\mathrm{t}_a)\ \ \mathrm{e}_j^{\mathrm{q}}(\mathrm{t}_a)]^{\mathrm{T}}$,
$\mathbf{e}_j^{\mathbf{R}}(\mathrm{t}_a) = [\mathrm{e}_j^{\mathrm{Rp}}(\mathrm{t}_a)\ \ \mathrm{e}_j^{\mathrm{Rq}}(\mathrm{t}_a)]^{\mathrm{T}}$,
$\mathbf{u}_j^{\mathbf{pqf}}(\mathrm{t}) = [\mathrm{u}_j^{\mathrm{pf}}(\mathrm{t})\ \ \mathrm{u}_j^{\mathrm{qf}}(\mathrm{t})]^{\mathrm{T}}$

Data: $i \geq 0$

$I \leftarrow i$;

// Initialize: $\mathrm{F(t)} = 0$, $\mathrm{R(t)} \neq 0$

while $I \neq 0$ **do**

  if *(*$\mathrm{F(t)} = 0$ && $\mathrm{R(t)} \neq 0$*)* **then**

    // Compute freshness (14): $\mathrm{F(t)} = \mathrm{t} - \mathrm{u(t)}$

    // Process-aware sparse sampling (10), (11)

    $\mathrm{e}_j^{\mathrm{dD}} = \sum_{w=0}^{\mathrm{W}-1} \mathrm{e}_j^{\mathrm{dVC}}[\mathrm{nD} - w].\delta[w]$

    $\mathrm{e}_j^{\mathrm{qD}} = \sum_{w=0}^{\mathrm{W}-1} \mathrm{e}_j^{\mathrm{qVC}}[\mathrm{nD} - w].\delta[w]$

    // Error generated for prediction policy (12)

    $\mathbf{e}_j(\mathrm{t}_a) = [\mathrm{e}_j^{\mathrm{dD}}(\mathrm{t}_a)\ \mathrm{e}_j^{\mathrm{qD}}(\mathrm{t}_a)] - \mathbf{u}_j$

    // Triggers generation with the prediction policy condition (13)

    if *(*$||\boldsymbol{e}_j(\mathrm{t}_a)|| > \alpha||e^{-\mathrm{t}/\mathrm{T}}.[\mathrm{e}_j^{\mathrm{dVC}}\ \mathrm{e}_j^{\mathrm{qVC}}]||$*)* **then**

      // Reconstruction of signals

      $\mathbf{e}_j^{\mathbf{R}}(r\mathrm{t}_a + \Gamma)$=$\mathbf{e}_j(r\mathrm{t}_a)$; $0 \leq \Gamma < \mathrm{t}_a$ and r=0,1,2,...

      // Reconstructed signals fed back to SC with tunable gains (15)

      $\mathrm{e}_j^{\mathrm{p}\varphi}(\mathrm{t}_a) = \mathrm{k_1}\mathrm{e}_j^{\mathrm{Rp}}(\mathrm{t}_a)$

      $\mathrm{e}_j^{\mathrm{q}\varphi}(\mathrm{t}_a) = \mathrm{k_2}\mathrm{e}_j^{\mathrm{Rq}}(\mathrm{t}_a)$

      // Final predictive inputs fed to the SC for delay compensation (16)

      $\mathrm{u}_j^{\mathrm{pf}}(\mathrm{t}) = \mathrm{u}_j^{\mathrm{p}}(\mathrm{t}) + \mathrm{e}_j^{\mathrm{p}\varphi}(\mathrm{t}_a)$

      $\mathrm{u}_j^{\mathrm{qf}}(\mathrm{t}) = \mathrm{u}_j^{\mathrm{q}}(\mathrm{t}) + \mathrm{e}_j^{\mathrm{q}\varphi}(\mathrm{t}_a)$

      // Compute relevance (14): $\mathrm{R(t)} = \mathbf{e}_j - \mathbf{e}_j^{\mathbf{R}}$

    else

      // No reconstruction: $\mathrm{R(t)} = 0$

    end

  else

    // Compute freshness (14): $\mathrm{F(t)} = \mathrm{t} - \mathrm{u(t)}$

  end

end

semantic principles into the sampling process for each DER. This integration enables the generation of reconstruction signals (fed back to local SC), based on the inner control layer dynamics.

(ii) To evaluate the reconstruction phase by filtering significant events caused during data availability attacks. Considering dynamic variation, prioritization of signals and computation of reconstruction error, reconstruction signals are tuned to generate delay compensation signals.

Thus, the scheme targets optimal information gathering, dissemination, and decision-making policies in cooperative networks, achieving jointly optimal performance. The convergence analysis of the proposed scheme is discussed further.

A. Convergence Analysis of the Proposed Scheme

Let $\circ(\mathrm{t}_a)$ denotes the triggered samples of the respective signals when triggering condition is met during data availability attacks. The proposed delay-aware semantic sampling scheme's convergence analysis is theoretically discussed and validated. Let the reconstructed signals ($\mathbf{e}_j^{\mathbf{R}}(\mathrm{t}_a)$) produce the triggered voltage correction term ($\Delta\mathrm{Vc}(\mathrm{t}_a)$) and frequency correction term ($\Delta\omega\mathrm{c}(\mathrm{t}_a)$) from the SC. Taking into account the triggered sampled measurements as:

$$\hat{\Upsilon}_j(k) = \Upsilon_j(\mathrm{t}_a) \tag{17}$$

where, $k \in [\mathrm{t}_a, \mathrm{t}_{a+1}]$ and $\Upsilon_j = \{\Delta Vc_j, \Delta\omega\mathrm{c}_j\}$. Let us define

$$y_j(\mathrm{t}_a) = \hat{\Upsilon}_j(\mathrm{t}_a) - \frac{1}{N_j}\sum_{m\in N_j} \Upsilon_j^T(t) \forall j \in M \tag{18}$$

Let $\mathrm{t}_a^j, \forall a = 1, 2, ...$ represent the triggering instants in the j^{th} agent. M is the total number of DERs in a network and N_j is the neighbouring agents to j^{th} agent. Consequently, the sampled control input becomes a piece-wise constant function, where $\hat{u}_j(k) = u_j(\mathrm{t}_a^{N_j})$ for $k \in [\mathrm{t}_a^{N_j}, \mathrm{t}_{a+1}^{N_j})$. Considering the initial condition $\Upsilon(0)$, the iteration within the proposed delay-aware semantic sampling scheme for the j^{th} agent is:

$$\Upsilon_j(k+1) = \Upsilon_j(k) + \beta_j u_j(k) \tag{19}$$

Here, β_j represents the step length. Employing a Lyapunov candidate function, denoted as $V(\Upsilon(k)) = f(\Upsilon(k)) - f(\hat{\Upsilon}(k))$ for the system in (19), it is trivial to deduce from (18) to (19) that $\Delta V(\Upsilon) = \Delta f(\Upsilon)$. For all $k \geq 0$,

$$\Delta V \leq \sum_{j=1}^{M}\left\{\beta_j u_j\left[\sum_{m\in N_i}(\Upsilon_m - \hat{\Upsilon}_j) - u_j\right] + \frac{M}{2}\beta_j^2 u_j^2\right\} \tag{20}$$

Utilizing Young's inequality, given as $xy < \frac{x^2}{2\xi} + \frac{\xi y^2}{2}$, where ξ represents an infinitesimal value, we obtain

$$\Delta V \leq \sum_{j=1}^{M}\left\{-\beta_j(1 - \frac{\xi_j}{2} - \frac{M}{2}\beta_j)u_j^2 + \frac{\beta_j}{2\xi_j}\left[\sum_{m\in N_i}(\Upsilon_m - \hat{\Upsilon}_j)\right]^2\right\} \tag{21}$$

With N_j terms in $\sum_{m\in N_j}(\Upsilon_m - \hat{\Upsilon}_j)$ and using the sum of squares inequality, we get

$$\left[\sum_{m\in N_i}(\Upsilon_m - \hat{\Upsilon}_j)\right]^2 \leq |M_j| \sum_{m\in N_j}(\Upsilon_m - \hat{\Upsilon}_j)^2 \tag{22}$$

Substituting (22) in (21), we obtain

$$\Delta V \leq \sum_{j=1}^{M} \left\{ -\beta_j(1-\frac{\xi_j}{2}-\frac{M}{2}\beta_j)u_j^2 + \frac{\beta_j|N_j|}{2\xi_j}\sum_{m\in N_j}(\Upsilon_m-\hat{\Upsilon}_j)^2 \right\} \tag{23}$$

Since the triggering instants in j^{th} agent during data availability attacks are evaluated by

$$u_j^2(k) = \gamma_i \hat{u_j^2}(k) \tag{24}$$

$$(\Upsilon_m(k) - \hat{\Upsilon_j}(k))^2 \leq \frac{\sum_{j=1}^{M}\frac{\gamma_j\beta_j}{N_j}(1-\frac{\xi_j}{2}-\frac{M}{2}\beta_j)\hat{u}_j^2}{\sum_{j=1}^{M}\frac{\beta_j N_j}{2\xi_j}} \tag{25}$$

Adding and subtracting $\gamma_j\beta_j(1-\frac{\xi_j}{2}-\frac{M}{2}\beta_j)\hat{u}_j^2$ in (23),

$$\Delta V \leq -\sum_{j=1}^{M}\beta_j(1-\frac{\xi_j}{2}-\frac{M}{2}\beta_j)(u_j^2-\gamma_j\hat{u_j}^2)+ \sum_{j=1}^{M}\left[\frac{\beta_j|N_j|}{2\xi_j}\left(1-\frac{\xi_j}{2}-\frac{M\beta_j}{2}\right)\hat{u}_j^2\sum_{m\in N_j}(\Upsilon_m-\hat{\Upsilon}_j)^2\right] \tag{26}$$

Theorem 1: $\Delta V(\Upsilon) \leq 0$ is guaranteed for all k using equations (24)–(26) for any $j \in M$ and $m \in N_j$. The only scenario where $\Delta V = 0$ can happen when

$$\begin{cases} u_j = \hat{u}_j = 0 & \forall j \in M \\ \Upsilon_j = \hat{\Upsilon}_j = 0 & \forall m \in N_j \end{cases} \tag{27}$$

Theorem 2: Using (27), it is proved that $\hat{\Upsilon}(k)$ is asymptotically stable and converges to the semantic sampling signals.

VI. Performance Evaluation

A real-time simulation testbed setup [22], used to test the feasibility of the proposed delay-aware semantic sampling scheme is shown in Fig. 5(b). It comprises of OP-5700 (real-time simulator), which is integrated with HYPERSIM software (on the host PC) to model the required test system. The PC and OP-5700 simulator are seamlessly linked via an Ethernet interface, facilitating the establishment of IEC 61850 sampled values protocol for efficient communication and data exchange. The standard IEEE 37-bus system is modified by adding seven inverters at buses B 15, B 18, B 22, B 24, B 29, B 33, and B 34 as shown in Fig. 2(a). This modified test system is considered to validate the proposed delay-aware semantic sampling approach. The design and control parameters of DERs is provided in Table I. The evaluation of this proposed scheme for various test conditions of latency attacks, data dropouts, TSAs is presented further.

TABLE I
Test System Parameters

Parameter	Symbol	Rating
Parameters for DERs		
Power rating	P	32 kW
Nominal V and ω	V_{nom}, ω_{nom}	$220\sqrt{2}$ V, 314.15 rad/s
Filter parameters	L^f, r^f, C^f	3 mH, 1 mΩ, 12.1 mF
Output impedance	L^o, r^o	1 mH, 0.121 Ω
P droop coefficient	m^p	9.4×10^{-5} rad/(W.s)
Q droop coefficient	n^q	1.3×10^{-3}V/VAr
Proportional gain (CC, VC)	K_p^i, K_p^V	0.2, 50
Integral gain (CC, VC)	K_i^i, K_i^V	1, 100
Secondary control (SC) parameters		
Communication weight	a_{jm}	1
Convergence parameter	g_j	1
Proportional gain	$K_p^{S\omega}$, K_p^{SV}	0.1, 0.1
Integral gain	$K_i^{S\omega}$, K_i^{SV}	42, 1.5
Network and load parameters of modified IEEE 37-bus AC distribution system ([31])		
Alpha	α	0.3

A. System under latency attacks

A latency attack was carried out on the considered system with the time delay, τ_m = 0.05 s. It was then followed by load variation at 5 s. Although the voltage remains within acceptable bounds, as shown in Fig. 6(a), but the SC objectives are not accomplished. It can be observed from the time-domain plots of frequency, active and reactive power sharing (as in Fig. 6(b), 6(c), and 6(d), respectively) that the consensus convergence time is increased due to delay.

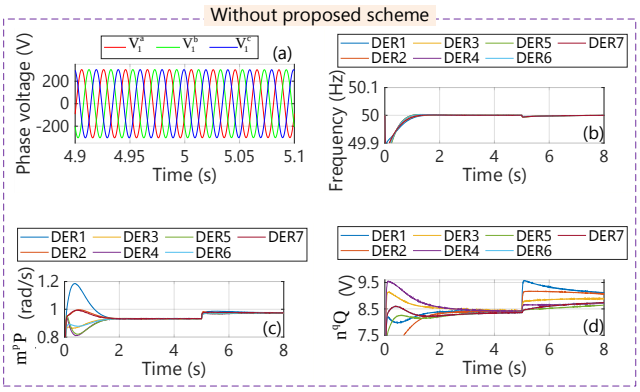

Fig. 6. Time-domain signals during latency attack (τ_m=0.05 s), without the proposed scheme for **(a)** phase voltage of DER 1; **(b)** frequency; **(c)** active power sharing; and **(d)** reactive power sharing for all DERs.

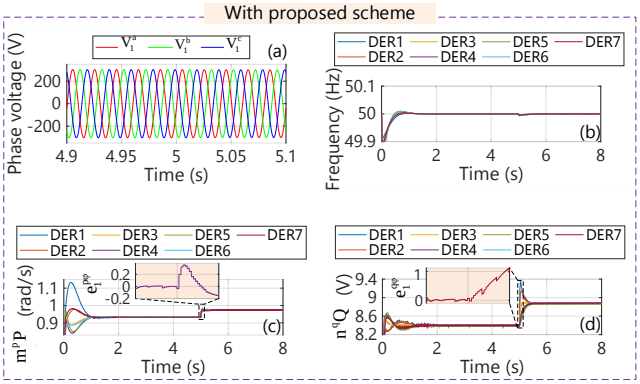

Fig. 7. Time-domain signals during latency attack (τ_m=0.05 s), with the proposed scheme for **(a)** phase voltage of DER 1; **(b)** frequency; **(c)** active power sharing; and **(d)** reactive power sharing for all DERs.

However, with the inclusion of the proposed scheme, resulting reconstructed signals ($e_j^{p\varphi}$ and $e_j^{q\varphi}$) as shown in Fig. 7(c) and 7(d) compensates for delay. It can be seen from time-domain plots of frequency, active and reactive power sharing (as in Fig. 7(b), 7(c), and 7(d), respectively), that convergence is much faster, with steady-state settling time within 0.45 s.

B. System under latency attacks and data dropouts

Considering a latency attack (τ_m = 0.05 s) with 10% data dropout and load variation at 5 s, it can seen in Fig. 8(a), 8(b), and 8(c), that time required to attain SC objectives is further increased as compared to initiation of only latency attack as in case A. Further, with proposed scheme SC objectives are attained at much faster rate as seen in Fig. 8(d), 8(e), and 8(f) for frequency, active and reactive power sharing, respectively. This can be attributed to reconstructed signal from the local controller that drives the control process during such attacks.

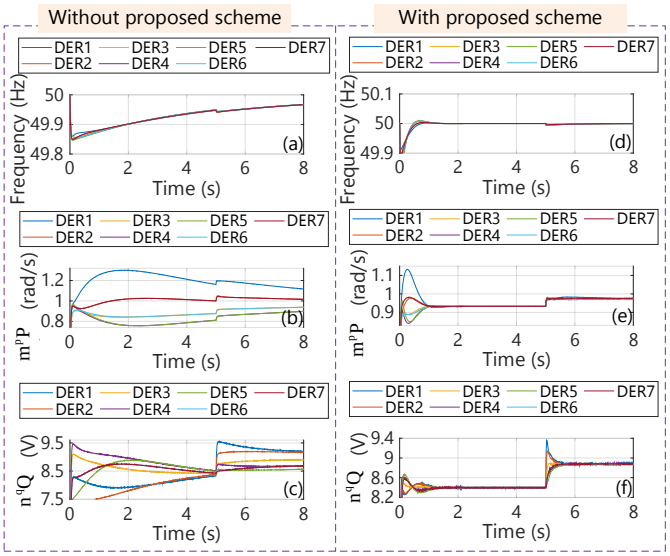

Fig. 8. The time-domain signals during latency attack (τ_m=0.05 s) and 10% data dropout for **(a)** frequency; **(b)** active power sharing; **(c)** reactive power sharing, without the proposed scheme are shown. Further, the time-domain signals for **(d)** frequency; **(e)** active power sharing; **(f)** reactive power sharing, with the proposed scheme are shown.

C. System under TSAs

Similarly, the time-domain simulation for the system under TSA attack (considering load variation at 5 s) without the proposed scheme is shown in Fig. 9(a), 9(b), and 9(c). It can be observed that with the deployment of the proposed scheme, the dynamic performance is increased because of the reconstructed signals ($e_j^{p\varphi}$ and $e_j^{q\varphi}$), as shown in Fig. 9(e) and 9(f). It can be seen in Fig. 9(d), 9(e), and 9(f), that the convergence time to attain SC of frequency restoration, proportional active and reactive power sharing decreases.

D. Cyber graph variations

The system is tested for two cyber graphs (G) under latency attack (τ_m = 0.05 s). These graphs are G1 and G2 representing fully-connected graph and ring-connected graph, respectively. Initially, the system is connected in G1 configuration and later switched to G2 configuration at 5 s. It can be observed from 10(a), 10(b) and Fig. 10(c), that the system tends towards instability under latency attack followed with dynamic cyber graph variations. This instability can be attributed to both the resulting sparse network and the additional delay to the signals,

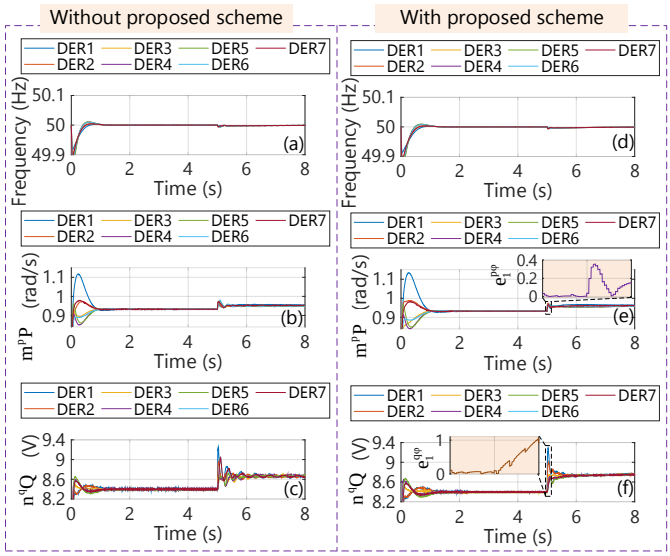

Fig. 9. The time-domain signals during TSA for **(a)** frequency; **(b)** active power sharing; **(c)** reactive power sharing, without the proposed scheme are shown. Further, the time-domain signals for **(d)** frequency; **(e)** active power sharing; **(f)** reactive power sharing, with the proposed scheme are shown.

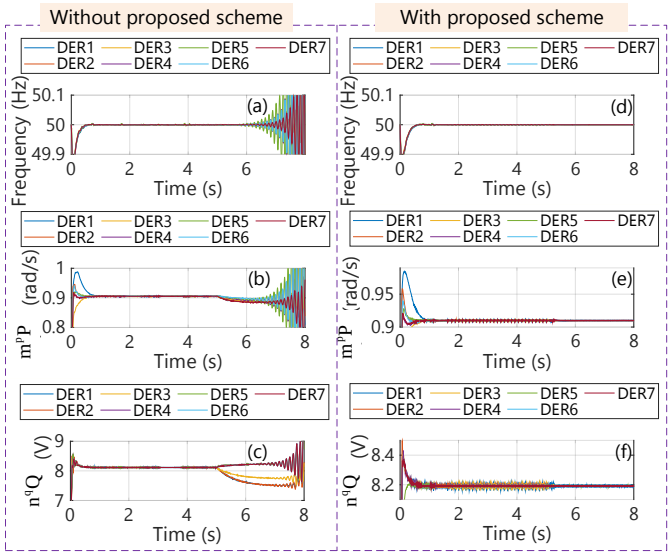

Fig. 10. The time-domain signals during latency attack (τ_m=0.05 s) with cyber graph variations for **(a)** frequency; **(b)** active power sharing; **(c)** reactive power sharing, without the proposed scheme are shown. Further, the time-domain signals for **(d)** frequency; **(e)** active power sharing; **(f)** reactive power sharing, with the proposed scheme are shown.

due to which the agents were not able to update their states continuously thereby slowing down the convergence. However, delay-aware semantic sampling actively synchronizes the error signals at primary and secondary controllers to generate reconstructed signals, thereby making this proposed scheme robust to dynamic cyber graph variations along with the latency attack as shown in Fig. 10(d), 10(e) and Fig. 10(f).

Let us consider that different attacks are represented as: a) I: latency attack; b) II: latency attack and data dropout; and c) III: TSA. The convergence time (T_c) plots for the system under these attacks are depicted in Fig. 11. Let O1 and O2

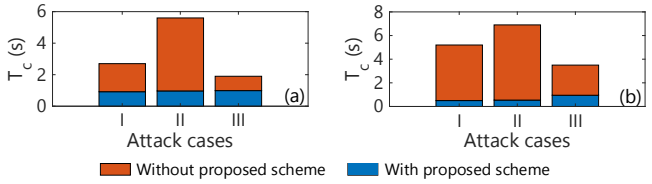

Fig. 11. Plots of time of convergence (T_c) for **(a)** O1; and **(b)** O2, without and with the deployment of the proposed scheme.

are defined as the objectives of SC. Here, O1 is attaining frequency restoration and proportional active power sharing; and O2 is attaining proportional reactive power sharing. It is evident from Fig. 11(a) and 11(b), that cases without the proposed delay-aware semantic sampling scheme, particularly those subjected to latency attacks with τ_m=0.05 s and 10% data dropout, exhibit longer convergence times compared to instances featuring only latency attacks with τ_m=0.05 s. In contrast, the deployment of our proposed delay-aware semantic sampling scheme substantially reduces convergence times across all attack scenarios (as shown in Fig. 11(a) and 11(b)), thereby enhancing overall system performance. Additionally, the steady-state error is assessed for the aforementioned attack scenarios to achieve SC objectives O1 and O2. Specifically, we define the absolute value of the steady-state error as

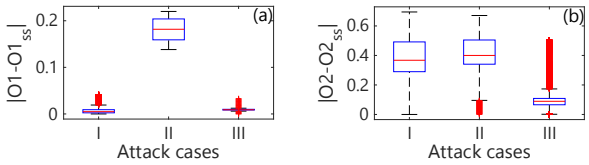

Fig. 12. Plots of steady-state error with different attack cases for **(a)** O1; and **(b)** O2, without the proposed scheme.

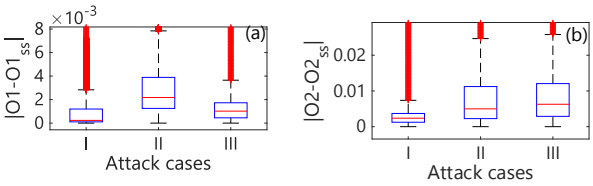

Fig. 13. Plots of steady-state error with different attack cases for **(a)** O1; and **(b)** O2, with the proposed scheme.

$|\mathrm{O1} - \mathrm{O1_{ss}}|$ and $|\mathrm{O2} - \mathrm{O2_{ss}}|$ for O1 and O2, respectively. Here O1 and O2 represent the instantaneous values, and $\mathrm{O1_{ss}}$ and $\mathrm{O2_{ss}}$ denote the steady-state values, according to SC objectives. Fig. 12(a) and 12(b) illustrate the steady-state error for achieving O1 and O2, respectively, in the system without the proposed scheme. Conversely, Fig. 13(a) and 13(b) reveal significantly reduced steady-state errors to attain O1 and O2 with the deployment of our proposed scheme, thereby improving system performance.

Further, the various error signals for latency attack (τ_m=0.05 s) with cyber graph variations, at DER 1 are investigated. The error signals provided by VC (e_1^{dVC}, e_1^{qVC}) are shown in Fig. 14(a) and Fig. 14(d), respectively. The process-aware sparse

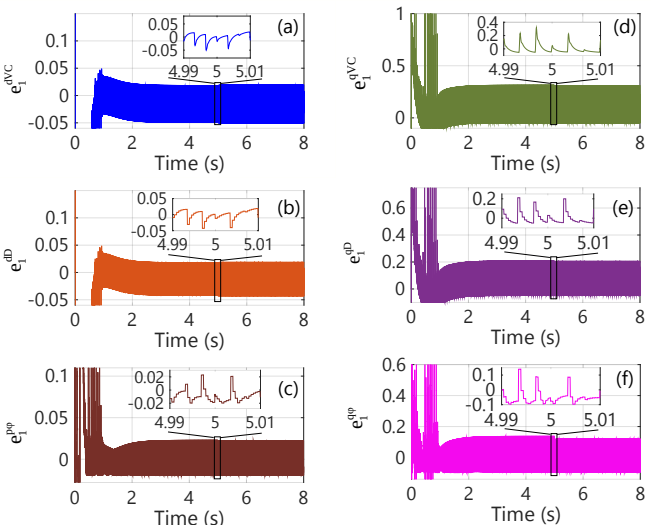

Fig. 14. The time-domain signals during latency attack (τ_m=0.05 s) with cyber graph variations for **(a)** d-axis error signals input to VC, e_1^{dVC}; **(b)** process-aware sparsely sampled d-axis error signals input to VC, e_1^{dD}; **(c)** reconstructed signal input to SC, $e_1^{p\varphi}$; **(d)** q-axis error signals input to VC, e_1^{qVC}; **(e)** process-aware sparsely sampled q-axis error signals input to VC, e_1^{qD}; and **(f)** reconstructed signal input to SC, $e_1^{q\varphi}$.

sampling of these signals are carried out as shown in Fig. 14(b) and Fig. 14(e), respectively. The resulting reconstructed signals which are fed to the SC for delay compensation are shown in Fig. 14(c) and Fig. 14(f), respectively.

The system's performance was evaluated by varying the downsampling factor (D), as shown in Fig. 15(a). The results

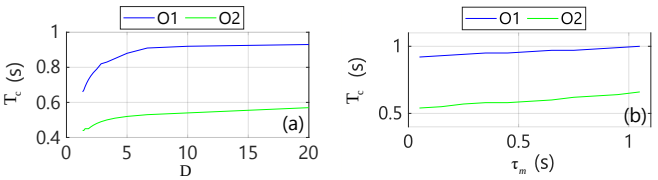

Fig. 15. Plots for variation in T_c for attaining O1 and O2 with variations in **(a)** downsampling factor (D); and **(b)** amount of delay (τ_m).

indicate a non-linear relationship between D and T_c to achieve the SC objectives. As expected, T_c increases with increasing D. Therefore, selecting the appropriate value of D involves a trade-off between low-cost operation versus fast efficient performance. In this study, a value of 10 was chosen for D, which offers a good balance of low-cost and fast efficient operation. The proposed delay-aware semantic sampling scheme was also tested for system performance under different levels of delay (τ_m), as shown in 15(b), demonstrating its robustness to large random delayed-measurements.

Additionally, the cyber layer of a PES (comprising of two DERs) was developed over IEC 61850 sampled values protocol through Ethernet interface. This communication model is based on a publish-subscribe architecture [22]. The data loss attack (of 10 packets) at 1 s (followed by load change at 1 s), was further tested on this system with the deployment of the proposed scheme. It can be observed from Fig. 16(a), 16(b) and 16(c) that all objectives of SC are achieved. Moreover,

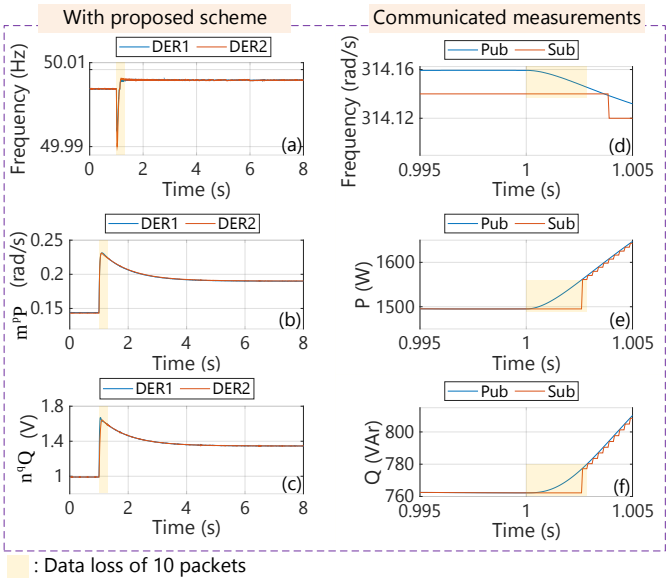

Fig. 16. The time-domain signals during data loss of 10 packets for **(a)** frequency; **(b)** active power sharing; and **(c)** reactive power sharing, with the proposed scheme are shown. Further, the time-domain signals showing data loss of 10 packets in the communicated signals i.e, **(d)** frequency; **(e)** active power; and **(f)** reactive power, over IEC 61850 sampled values protocol are presented.

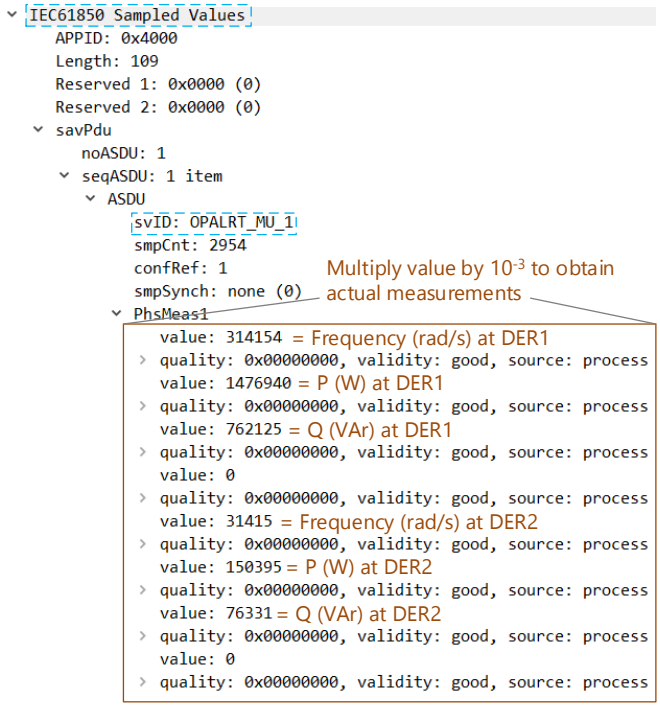

Fig. 17. Details of IEC 61850 sampled values packet comprising of svID, values of communicated signals etc., obtained from *wireshark* application.

the signals being published over the established protocol are indicated as "*Pub*" and the signals being subscribed are indicated as "*Sub*", as shown in Fig. 16(d), 16(e) and 16(f). Whenever data loss occurs, the subscribers hold on to the last received sample until the next packet arrives as shown in Fig. 16(d), 16(e) and 16(f). The details of the packet over IEC 61850 sampled values protocol are mentioned in Fig. 17.

A comparative evaluation of our delay-aware semantic sampling scheme against existing methodologies is presented in Table II. The proposed scheme in this work, distinguishes itself as a computationally efficient solution, incorporating distributed concept that enhance its resilience against data availability attacks. Moreover, it demonstrates notable robustness when confronted with load variations, highlighting its practical adaptability. The model-agnostic nature of this approach further streamlines its implementation. Additionally, it supports dynamic cyber graphs, underscoring its practicality and flexibility. As a result, the delay-aware nodal semantic intelligence presented by our approach emerges as a highly promising and commercially viable solution, well-poised to address the intricate challenges within the realm of PES.

VII. Conclusions and Future Scope of Work

In the landscape of PES, data availability challenges underscore the critical need for an innovative approach to mitigate the impact of random communication delays. Motivated by this imperative, our proposed delay-aware semantic methodology harnesses the inherent dynamics of the inner control loops within DERs to generate localized delay compensation signals. This approach not only yields robust performance and precise predictions by transmitting only the significant information but also obviates the need for intricate models and training that often accompany in prevailing methods. Real-time simulations on the OPAL-RT platform convincingly affirm the efficacy of our approach. While this study addresses the immediate challenges, several others loom ahead, such as understanding the limits of maximum communication delay tolerance and scalability in larger, complex systems. In future investigations,

TABLE II
Comparative Analysis of the Proposed Delay-Aware Semantics Scheme for PES.

Sl. no.	Features	[11]	[13]	[14]	**Proposed scheme**
1.	Computational complexity	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.	Robust to loading variations	✓	✓	✓	✓
7.	Model-agnostic	✗	✗	✓	✓
8.	Supports dynamic cyber graphs	✓	Not tested	Not tested	✓

system stability under semantic sampling concerning the maximum communication delay it can handle will be explored and scalability in more extensive systems will be assessed.

In the evolving domain of demand response, diverse resources, such as electric vehicles, adaptable residential loads, and energy storage systems, are ready for integration. However, real-time data exchange among them necessitates varied communication protocols, posing a challenge for semantic interoperability. Our upcoming research aims to overcome this hurdle by developing a semantic framework to predict, activate, and manage heterogeneous resources efficiently. This research direction, not only promises to advance the field but also address the complexities of the PES energy market. Furthermore, semantic-based quantum communication will be explored to enhance fault detection and localization, reducing response times and downtime during disturbances, fortifying 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] S. Rath, L. D. Nguyen, S. Sahoo and P. Popovski, "Self-Healing Secure Blockchain Framework in Microgrids," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4729-4740, Nov. 2023.

[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] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela and A. D. Domı´nguez-Garcı´a, "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.

[9] 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.

[10] Z. Zhang, S. Gong, A. D. Dimitrovski and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," in *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87-98, March 2013, doi: 10.1109/TSG.2012.2227342.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] W. Gao, H. Li, M. Zhong and M. Lu, "An Underestimated Cybersecurity Problem: Quick-Impact Time Synchronization Attacks and A Fast-Triggered Detection Method," *IEEE Trans. Smart Grid*, doi: 10.1109/TSG.2023.3258963.

[16] W. Gao, H. Li, M. Zhong and M. Lu, "The Separate Clock Drift Matched Filter to Detect Time Synchronization Attacks Toward Global Navigation Satellite Systems," *IEEE Transactions Ind. Electron.*, vol. 70, no. 6, pp. 6305-6315, June 2023, doi: 10.1109/TIE.2022.3194578.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

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

[23] K. Gupta, S. Sahoo, R. Mohanty, B. K. Panigrahi and F. Blaabjerg, "Decentralized Anomaly Characterization Certificates in Cyber-Physical Power Electronics Based Power Systems," *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*, Cartagena, Colombia, pp. 1-6, 2021.

[24] J. S. Choi, S. Lee and S. J. Chun, "A Queuing Network Analysis of a Hierarchical Communication Architecture for Advanced Metering Infrastructure," *IEEE Trans. Smart Grid,* vol. 12, no. 5, pp. 4318-4326, Sept. 2021, doi: 10.1109/TSG.2021.3088879.

[25] 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.

[26] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Los Alamos Nat. Lab.*, Los Alamos, NM, USA, Rep. LAUR-03-6163, 2003. [Online]. Available: http://lewisperdue.com/DieByWire/GPS-Vulnerability-LosAlamos.pdf (accessed April 28, 2023).

[27] 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.

[28] S. Sahoo and F. Blaabjerg, "A Model-Free Predictive Controller for Networked Microgrids with Random Communication Delays," *2021 IEEE Appl. Power Electron. Conf. and Expo. (APEC)*, Phoenix, AZ, USA, pp. 2667-2672, 2021.

[29] M. D. Roig Greidanus, S. Sahoo, S. Mazumder and F. Blaabjerg, "Novel control solutions for DoS attack delay mitigation in grid-connected and standalone inverters," *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Chicago, IL, pp. 1-7, 2021.

[30] M. H. Najafi and D. J. Lilja, "High Quality Down-Sampling for Deterministic Approaches to Stochastic Computing," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 1, pp. 7-14, 1 Jan.-March 2021, doi: 10.1109/TETC.2017.2789243.

[31] L. Luo and S. V. Dhople, "Spatiotemporal model reduction of inverter-based islanded microgrids," *IEEE Trans. Energy Convers.*, vol. 29, no. 4, pp. 823–832, Dec. 2014.