Holistic Multi-timescale Attack Resilient Control Framework for Power Electronics Dominated Grid

Amin Y. Fard, *Student Member, IEEE*, Mohammad B. Shadmand, *Senior Member, IEEE*, and Sudip K. Mazumder, *Fellow, IEEE*
Department of Electrical and Computer Engineering
University of Illinois at Chicago
Chicago, IL, USA

Abstract*— Power system is being upgraded by integrating wide-area communication substructures alongside smart devices. This upgrade might jeopardize the resiliency and security of the grid. Malicious activities could take advantage of potential vulnerabilities of the power-electronics-dominated grid (PEDG) and its heterogeneous components, which might lead to large-scale blackouts. The grid's edge houses numerous distributed resources that could be targeted as manipulation points. Attacks on operating set-points of smart PV inverters (SPVIs) are among the most likely malicious actions. These attacks could cause various issues like voltage fluctuations and frequency instabilities. According to grid integration standards, fluctuations on voltage could push the SPVIs or even the entire grid cluster to go islanded if they are not mitigated in a timely manner. Thus, the grid edge must be equipped with an all-inclusive control approach that alleviates voltage fluctuations within a specified interval. This paper proposes a holistic multi-timescale voltage control framework for dispersed SPVIs at the grid edge. The proposed framework consists of three different tiers with different responsibilities acting on different timescales. By implementing the proposed control framework, the SPVIs will participate in voltage regulation across the grid in occurrence of rapid voltage fluctuations in a sub-second timeframe, while keeping the entire distribution grid at an optimal operating condition in a long term. The proposed control framework is verified via simulation.

Keywords—photovoltaics, smart inverter, resilient control.

I. INTRODUCTION

The electric grid is being integrated with communications and Internet of Things (IoT) to form an infrastructure with bidirectional information and power flows called, "smart grid" [1]. According to the U.S. Department of Energy (DOE), power-electronics-dominated grid (PEDG) must add some new functionalities to the power system including attack resiliency, self-healing, power quality, accommodation of generation /storage parts, enabling market, and optimization of the system. One of the main motivations for moving from the traditional structure of power grid towards the PEDG is enabling high integration of distributed energy resources (DERs) while guaranteeing higher reliability for the entire grid [2-4].

Persistently growing advanced metering infrastructure (AMI) together with several communication technologies and employing progressive demand-side management have improved controllability and monitoring aspects of the entire grid. Noticeably, all these assets are required for realizing the concept of PEDG. Nevertheless, trading-off among reliability, efficiency, optimization and security of an immense complex cyber-physical system such as power grid is still an open question.

Comparing the traditional power grid with the concept of PEDG with high number of power electronics components illustrates much vaster attack surface. Principally, a system with the complexity level of the grid at its edge considering all the integrated smart photovoltaic inverters (SPVIs) and numerous communications is prone to security threats. These threats include thievery and cyber-physical attacks, which would have consequences like failure in unceasing power delivery, cascading failures, tribulations for energy markets, damaging equipment at utility and consumer sides, risking human safety, jeopardizing energizing critical loads, etc.

Although malicious attacks on the electric grid have always been existed, moving towards smarter grid has augmented their incidence with diverse natures. For instance, based on the report published by McAfee [5], at the utility level, 80 percent of the surveyed utilities had experienced at least one major attack on their communication links leading to denial of service (DoS), and almost 85 percent of the surveyed ones underwent intrusions on their networks. The main characteristic of cyber-physical attacks is that they target information networks; however, their potential impacts are on the physical infrastructure. Recent examples are Venezuela power outage occurred at 2019 [6] and cyber attacks on Ukraine's power grid at 2017 [7], which had massive public impacts and caused numerous technical and economic problems.

Since the grid edge houses multiple critical infrastructures like hospitals, airports, water supply set-ups, data centers, telecommunications, etc., this portion of the grid becomes an attractive target for malicious activities. By exploiting operating boundaries for voltage and frequency mapped in grid integration standards [8, 9] by attackers, the energy services at the feeders could be jeopardized.

At the grid edge, an attractive bullseye for attackers is manipulating the operating power set-points of the SPVIs. Fig. 1 illustrates concept of the grid edge with numerous households equipped with SPVIs and possible intrusions. If the power set-points of the SPVIs across the grid are not compatible with the criteria including the physical capabilities of the SPVIs in injecting active power and injecting/absorbing reactive power, configuration of the feeder itself, power quality factors, etc. voltage across the grid edge would start to fluctuate. These fluctuations are not acceptable by the grid codes. If they could not be cleared from the grid in a specified time range, the SPVIs

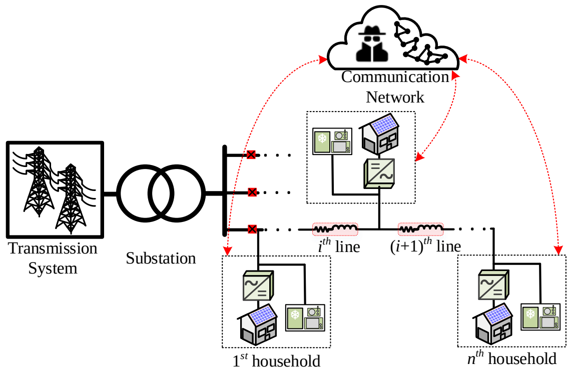

Fig. 1. Importance of resiliency and cybersecurity at the grid edge.

would trip. For instance, the German EN50160 standard requires that the voltage across the grid stays within ±10% of the ten minute average value of the RMS voltage [10]. In the United States, according to the IEEE 1547, the DERs including SPVIs could regulate their active and reactive powers [8]. According to the definition provided in Range A of the ANSI C84.1 released at 2016 [11], the voltage at low voltage side cannot go beyond 0.95 to 1.05 p.u. Based on this standard, the voltage at medium voltage side should not exceed more than 5 percent of the nominal voltage; moreover, it cannot decrease less than 2.5 percent of nominal value. Thus, pushing voltage across the grid beyond these established boundaries could cause grid disconnection of SPVIs. This would yield to losing control over critical infrastructures, and the upper hand-side grid would start facing low-frequency oscillations (LFOs) that might cause large-scale blackouts in various areas. Therefore, the grid edge with high penetration of SPVIs needs a voltage control framework to keep the voltage across the grid in a pre-defined boundary no matter what the source of the fluctuations is.

In the literature, the existing voltage control approaches are divided into two main categories, distributed voltage control schemes [12, 13] and centralized ones [14-16]. The central approaches are not suitable for addressing fast voltage fluctuations due to communication delays imposed by AMI and burdensome calculations for fleet of SPVIs. The attacker could take advantage of slow decision-making procedure of the central supervisory unit. Thus, to confront fast voltage fluctuations on the grid, distributed approaches suit the grid demands better. On the other hand, distributed schemes might not be able to fulfill the optimal operation of the entire grid because of their restricted knowledge from the rest of the grid. Losing optimal operation of the grid means higher power loss due to extra reactive power circulation in the feeders. Imposing extra power loss to the utilities and customers could be considered another form of attack on the grid that does not have an immediate effect of the grid, however, in a long term it could cause financial difficulties for the system. The majority of the research performed to mitigate these resiliency/security-related issues is on the attack detection approaches [17-21]. In [22], the mitigation of cyber attacks on AC microgirds has been proposed. In this reference, the focus of the authors is on frequency restoration and mitigation of cyber attacks that cause voltage fluctuations have not been addressed. In [23], a cyber attack mitigation approach is proposed for AC microgirds to ensure reliable operation of voltage control protocols.

This article proposes a resilient mitigation framework for intrusions on the voltage at the grid edge. The proposed intrusion mitigation scheme is a holistic multi-timescale three-tiered voltage control approach (conceptualized in Fig. 2). The topmost tier of this framework called long-term supervisory tier (LTST) watches the entire cluster to ensure optimal operation of the entire cluster while power delivery loss is minimized in one-minute timeframe. In short term, the middle tier of the proposed framework called short-term distributed tier (STDT) ensures cooperative operation of the SPVIs for regulating voltage across the cluster in a sub-second timeframe to mitigate potential cyber attacks on power set-points of the SPVIs. The undermost tier, called the model-predictive-based local tier (MPLT), fulfills the operational commands dictated by the upper layers with fast dynamics and adequate power quality. By implementing the proposed control framework, the SPVIs will participate in voltage regulation across the grid in occurrence of rapid voltage fluctuations while keeping the entire distribution grid at the optimal operating condition for a long term.

Beyond the introduction, Section II presents the methodology for MPLT of the proposed framework. Section III presents the short-term fast acting tier of the framework called STDT. Then, the long-term tier, LTST is detailed in section IV. The framework has been verified and the results are illustrated in section V. Finally, the paper is concluded via section VI.

II. Model-Predictive-based Local Tier

The upper tiers (the STDT for mitigating fast voltage fluctuations i.e. due to intrusion and the LTST for ensuring optimal operation of the entire grid) determine the share of each SPVI in providing reactive power according to the physical structure of the feeder, inverter ratings and minimum power delivery loss. The commanded references by upper tiers of the framework will be fulfilled via the local controller, which implements model predictive control (MPC) to overcome design challenges of using conventional control techniques like tuning PI controllers for different operating modes besides MPC's potential adaptive feature for filter size degradation over time. In addition, implementing computationally-efficient optimal control is achievable by a hierarchical MPC for PECs [24]. Other attractive feature of MPC over classical control methods is simplicity of operational constraints and multi-objectives inclusion in the related cost function [25]. The fast dynamic response feature of MPC is leveraged at MPLT to ensure fast re-establishment of the feeder voltage in a grid cluster after any intrusion. Using the second-order generalized integrator (SOGI) based phase-locked loops (PLL) [26] to extract the angle of the grid voltage for synchronization purpose makes the controller robust to distorted grid condition due to its inherent harmonic filtering capability.

By applying Kirchhoff's voltage law across the filter depicted at Fig. 2,

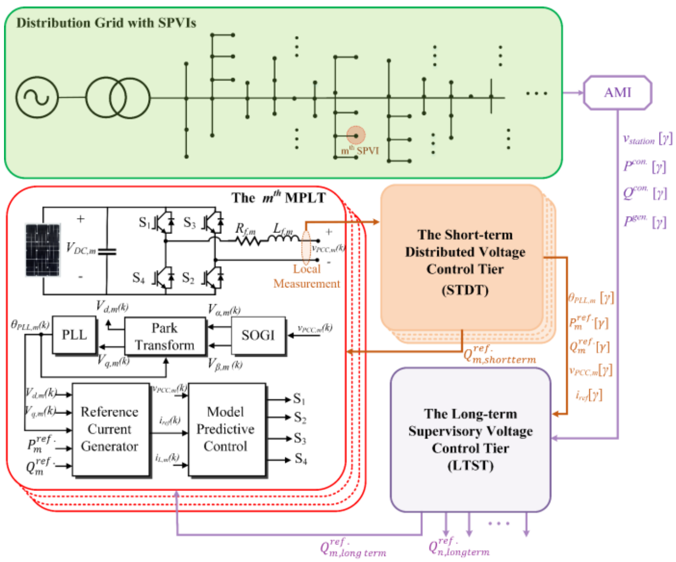

Fig. 2. General concept of the proposed multi-timescale three-tiered voltage

$$v_{inv}(t) = L_f \frac{di_L(t)}{dt} + R_f i_L(t) + v_g(t) \tag{1}$$

By employing the Euler forward method, this equation can be discretized. By rearranging it, the current at k+1 can be predicted as,

$$i_L(k+1) = \frac{T_s}{L_f}\left[v_{inv}(k) - v_g(k) - R_f i_L(k)\right] + i_L(k) \tag{2}$$

where $v_{inv}(k)$ is a function of switching sequence and voltage of the dc bus as,

$$v_{inv}(k) = v_{dc}(S_1 - S_3)$$
$$S_n(n = 1 \text{ or } 3) = \begin{cases} 1 & S_n \ \ is \ \ on \\ 0 & S_n \ \ is \ \ \text{off} \end{cases} \tag{3}$$

By employing instantaneous power theory, the relationship between the reference active and reactive powers in the rotating reference frame can be calculated,

$$\begin{bmatrix} P_{ref} \\ Q_{ref} \end{bmatrix} = 0.5 \begin{bmatrix} v_d(k) & v_q(k) \\ v_q(k) & -v_d(k) \end{bmatrix} \begin{bmatrix} i_{ref,d}(k) \\ i_{ref,q}(k) \end{bmatrix} \tag{4}$$

where P_{ref} and Q_{ref} are the reference set-points for active and reactive powers. These set-points are determined by STDT or LTST. Correspondingly, $v_d(k)$ and $v_q(k)$ are d-q components of the grid voltage, while $i_{ref,d}(k)$ and $i_{ref,q}(k)$ are rotating reference frame components of the reference current to be injected to the grid to ensure that the SPVI is obeying the active and reactive power set-points. The reference current in d-q frame can be calculated as,

$$\begin{bmatrix} i_{ref,d}(k) \\ i_{ref,q}(k) \end{bmatrix} = \frac{2}{v_d^2(k) + v_q^2(k)} \begin{bmatrix} v_d(k) & v_q(k) \\ v_q(k) & -v_d(k) \end{bmatrix} \begin{bmatrix} P_{ref} \\ Q_{ref} \end{bmatrix} \tag{5}$$

Now, by using inverse Park transform, and considering $\psi = 2 / (v_d^2 + v_q^2)$, the cost function which should be subject to minimization could be calculated as,

$$\min \ J = \left| \psi \begin{bmatrix} (v_d(k)\sin(\theta(k)) + v_q(k)\cos(\theta(k)))P_{ref} + \\ (v_q(k)\sin(\theta(k)) + v_d(k)\cos(\theta(k)))Q_{ref} \end{bmatrix} - i_L(k+1) \right| \tag{6}$$

where $\theta(k)$ comes from the SOGI-PLL. The reference for reactive power is determined depending on what actually is happening on the grid according to measurements received by the STDT or LTST from the SPVIs, PMUs, smart meters, etc.

III. Short-term Distributed Voltage Control Tier

This section presents the short-term distributed voltage control scheme so called STDT for fleets of SPVIs at the grid edge. This tier of the framework is established in a distributed manner and handles rapid fluctuations on the voltage due to intrusions. Due to communication delays and burdensome calculations of centralized controllers, they are not suitable for rapid voltage fluctuations, since according to the IEEE 1547-2018 (Section 6.4), these fluctuations must be cleared in a sub-second timeframe. To establish the voltage across the grid cluster after any intrusions, each SPVI must inject reactive power according to its own actual apparent power boundaries in addition to the configuration of the grid. The apparent power transfer between the m^{th} SPVI and grid can be calculated as,

$$S_m = V_{PCC,m} \frac{V^*_{PCC,m} - V^*_{grid}}{R_m - jX_m} \tag{7}$$

The real power delivered to the grid through the impedance is,

$$P_{SPVI,m} - P_{load,m} = \frac{R_m}{Z_m^2}\left|V_{PCC,m}\right|^2 + \frac{\left|V_{grid}\right|\left|V_{PCC,m}\right|}{Z_m^2}\left(-R_m\cos(\delta_{V,m}) + X_m\sin(\delta_{V,m})\right) \tag{8}$$

where $P_{SPVI,m}$ and $P_{load,m}$ are the active power generated by the m^{th} SPVI and active power demand by the local load, respectively, and Z_m is the impedance between m^{th} SPVI and the slack bus that equals to $\sqrt{R_m^2 + X_m^2}$. In addition, $\delta_{V,m}$ is the voltage angle of the m^{th} SPVI at its PCC. The reactive power injected to the grid could be calculated as,

$$Q_{SPVI,m} - Q_{load,m} = \frac{X_m}{Z_m^2}\left|V_{PCC,m}\right|^2 - \frac{\left|V_{grid}\right|\left|V_{PCC,m}\right|}{Z_m^2}\left(R_m\sin(\delta_{V,m}) + X_m\cos(\delta_{V,m})\right) \tag{9}$$

where $Q_{SPVI,m}$ and $Q_{load,m}$ are the reactive power generated by the m^{th} SPVI and reactive power demand by the local load, respectively. By solving the quadratic equation presented in eq. (8), the $V_{PCC,m}$ can be obtained as,

$$\left|V_{PCC,m}\right| = 0.5\left|V_{grid}\right|\left(\cos(\delta_{V,m}) - \frac{X_m}{R_m}\sin(\delta_{V,m})\right) + \sqrt{0.25\left|V_{grid}\right|^2\left(-\frac{1}{R_m}\cos(\delta_{V,m}) + \frac{X_m}{R_m^2}\sin(\delta_{V,m})\right)^2 + \frac{Z_m^2}{R_m}(P_{SPVI,m} - P_{load,m})} \tag{10}$$

By replacing (10) in eq. (9), the required reactive power to be injected by m^{th} SPVI can be calculated as,

$$Q_{SPVI,m} = Q_{load,m} + \frac{X_m}{Z_m^2}\left(\begin{array}{l} 0.5\left|V_{grid}\right|(\cos(\delta_{V,m}) - \frac{X_m}{R_m}\sin(\delta_{V,m})) + \\ \sqrt{0.25\left|V_{grid}\right|^2(-\frac{1}{R_m}\cos(\delta_{V,m}) + \frac{X_m}{R_m^2}\sin(\delta_{V,m}))^2 + \frac{Z_m^2}{R_m}(P_{SPVI,m} - P_{load,m})} \end{array}\right)^2$$
$$-\frac{\left|V_{grid}\right|}{Z_m^2}\left(R_m \sin(\delta_{V,m}) + X_m \cos(\delta_{V,m})\right)$$
$$\left(\begin{array}{l} 0.5\left|V_{grid}\right|(\cos(\delta_{V,m}) - \frac{X_m}{R_m}\sin(\delta_{V,m})) + \\ \sqrt{0.25\left|V_{grid}\right|^2(-\frac{1}{R_m}\cos(\delta_{V,m}) + \frac{X_m}{R_m^2}\sin(\delta_{V,m}))^2 + \frac{Z_m^2}{R_m}(P_{SPVI,m} - P_{load,m})} \end{array}\right) \quad (11)$$

The m^{th} SPVI can establish the voltage at its PCC by injecting reactive power calculated by eq. (11). Obviously, the calculated $Q_{SPVI,m}$ must not jeopardize the physical reliability of the SPVI itself considering the maximum apparent power of the SPVI. The STDT of the proposed framework handles fast voltage boundary violations. Due to limited information used by the STDT, the optimal operation of the distribution might be faded in long term i.e. due to higher power delivery losses. The STDT clears the voltage violations and prevents tripping of the SPVIs at the grid edge due to intrusions, which if happens the entire system could go unstable because of unbalance generation and consumption.

IV. Long-term Supervisory Voltage Control Tier

In the previous section, the methodology for the short-term distributed voltage control scheme presented. Although this tier is essential for the rapid set-point adjustments of SPVIs that are facing any intrusion to make sure their continuous grid connectivity, the STDT is not aware of the system-wide operating circumstances. For instance, in long term, the balance between generation and consumption might slip away or power loss across the distribution grid might increase significantly due to excessive reactive power flow. Thus, in a longer timeframe another tier is required to make sure that the entire grid is working optimally. This tier of the holistic multi-timescale three-tiered control framework is proposed in this section so called LTST. This tier of the framework performs slower than the STDT and makes sure that (a) the voltage across the distribution grid is within the pre-defined boundaries in the grid integration standards, (b) power loss is minimized across the grid, and (c) physical limitations of the SPVIs are met. The time-wise collaboration of the STDT and LTST of the proposed framework is abstracted in Fig. 3.

In the LTST, an optimal power flow analysis is utilized to calculate the voltage at each bus, optimally. This tier of the framework is designed to assure that the entire distribution grid is back to optimal operating condition after possible set-point changes decided by the STDT after each intrusion. To perform the optimal power flow analysis at the LTST, the distribution system must be equipped with AMI. The AMI will provide required information for the LTST including voltage of the bus connected to the substation, active power generation/consumption, and reactive power generation/consumption across the grid. Time steps for the

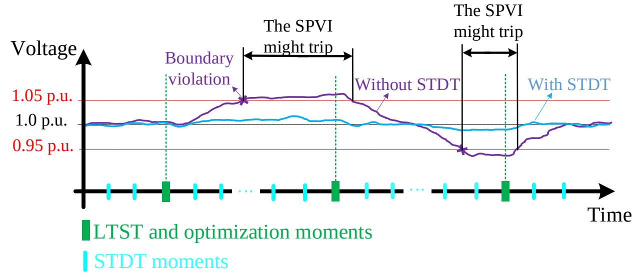

Fig. 3. Collaboration of STDT and LTST of the framework.

LTST and STDT are not same i.e. the LTST is executed in one-minute intervals while the STDT handles the voltage boundary violations in sub-second intervals. The LTST ensures minimum power losses across the distribution grid by minimizing the following function,

$$minimum \sum_{m,n \in branches} r_{m,n} \frac{P_{m,n}^2[\gamma] + Q_{m,n}^2[\gamma]}{v_m^2[\gamma]} \quad (12)$$

where $P_{m,n}[\gamma]$ and $Q_{m,n}[\gamma]$ are active and reactive power flow between buses m and n, while $v_m[\gamma]$ is the voltage on the bus m. Here, γ is time steps at which system-wide data is delivered to the LTST using AMI through communication substructure. Also, $r_{m,n}$ is the resistive part of the impedance of the branch between buses m and n. According to [27], $P_{m,n}[\gamma]$, $Q_{m,n}[\gamma]$ and $v_m[\gamma]$ could be calculated as,

$$P_{m,n}[\gamma] = \sum_{n,r \in branches} P_{n,r}[\gamma] + r_{m,n} \frac{P_{m,n}^2[\gamma] + Q_{m,n}^2[\gamma]}{v_m[\gamma]} + P_n^{con.}[\gamma] - P_n^{gen.}[\gamma] \quad (13)$$

$$Q_{m,n}[\gamma] = \sum_{n,r \in branches} Q_{n,r}[\gamma] + x_{m,n} \frac{P_{m,n}^2[\gamma] + Q_{m,n}^2[\gamma]}{v_m[\gamma]} + Q_n^{con.}[\gamma] - Q_n^{gen.}[\gamma] \quad (14)$$

$$v_m[\gamma] = 2(r_{m,n}P_{m,n}[\gamma] + x_{m,n}Q_{m,n}[\gamma]) - (r_{m,n}^2 + x_{m,n}^2)\frac{P_{m,n}^2[\gamma] + Q_{m,n}^2[\gamma]}{v_m[\gamma]} + v_n[\gamma] \quad (15)$$

where $P_n^{con.}[\gamma]$, $Q_n^{con.}[\gamma]$, $P_n^{gen.}[\gamma]$, and $Q_n^{gen.}[\gamma]$ are active/reactive power consumption/generation on n^{th} bus, while $x_{m,n}$ is the reactance of branch between buses m and n. The final goal is to maintain the voltages on each bus within the boundary. Thus, eq. (12) is subject to the following constraint,

$$v_m^{\min} \le v_m[\gamma] \le v_m^{\max} \quad (16)$$

where $v_m^{\min}$ and $v_m^{\max}$ are lower and upper boundaries for voltage of m^{th} bus, respectively, according to grid interconnection standards. In this paper, $P_m^{con.}[\gamma]$ and $Q_m^{con.}[\gamma]$, together with $P_m^{gen.}[\gamma]$ are not subject to optimization nor control by the LTST. Therefore, the values reported from the field for these variables are assumed as the optimal value at time step γ. Furthermore, the upper layer of the framework must consider the physical capability of each SPVI in injecting or absorbing reactive power. This constraint is implemented in the upper layer of the controller as,

$$Q^{min}_{m^{th}\ inv.} \leq Q^{optimal}_{m^{th}\ inv.}[\gamma] \leq Q^{max}_{m^{th}\ inv.} \tag{17}$$

where $Q^{min}_{m^{th}\ inv.}$ and $Q^{max}_{m^{th}\ inv.}$ are lower and upper reactive power injection/absorption limits for m^{th} SPVI. The actual apparent power of the SPVI is different from the values on nameplate of the SPVI. To consider this criterion, eq. (17) is modified as follows,

$$0.95\ Q^{min}_{m^{th}\ inv.} \leq Q^{optimal}_{m^{th}\ inv.}[\gamma] \leq 0.95\ Q^{max}_{m^{th}\ inv.} \tag{18}$$

Using a convex relaxation [27], the non-linear AC optimal power flow could be solved. To establish this approach, the square values of the voltage magnitudes are used instead of voltage magnitudes in eqs. (13)-(15) ($v_m[\gamma] \to v_m^2[\gamma]$, $v_n[\gamma] \to v_n^2[\gamma]$). Then, an additional variable like $I_{m,n}$ is introduced, which is the square of the magnitude of the current between buses m and n. Eventually, eqs. (12)-(15) will be represented by linear functions that yields to solving the AC optimal power flow using a second-order cone- program, with considering the following inequality constraint on $I_{m,n}$,

$$I_{m,n} \geq \frac{P^2_{m,n}[\gamma] + Q^2_{m,n}[\gamma]}{v_m^2[\gamma]} \tag{19}$$

The outcome of this tier of the framework is modifying the reactive power set-points of the SPVIs if needed to make sure that voltage across the distribution grid is within the pre-defined boundaries, power loss is minimized while the physical limitations of the SPVIs are all considered. The LTST needs data from the field through AMI and cloud-based communications, and since it is overseeing the entire grid, it needs more time to be executed.

V. Simulations and Results

In this paper, a residential grid cluster with high penetration of SPVIs is considered for detailed simulation studies. The performance of the proposed holistic multi-timescale three-tiered voltage control framework is investigated thoroughly and effectiveness of the framework in mitigating short-term voltage boundary violations via STDT under malicious intrusions alongside long-term optimal operation of the entire grid cluster using LTST is evaluated. The aggregated power demand in a

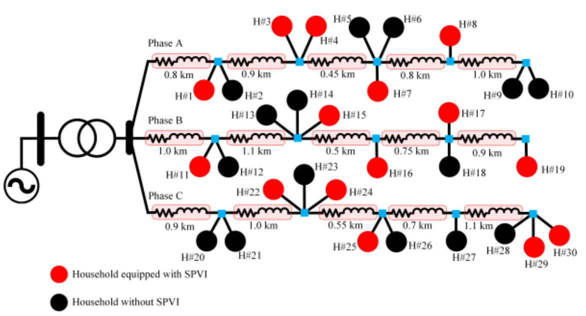

Fig. 4. The considered grid cluster for case studies.

household is modelled as a constant PQ load with $cos\varphi$ = 0.9. The system under study is depicted in Fig. 4. This figure illustrates a grid cluster situated at the grid edge consisting of thirty households. Half of the households are equipped with SPVIs. The rest are modelled as loads. Each household equipped with PV panels, is considered to have an SPVI of 7500 W. This capacity is considered for an effective rooftop area of 520 ft^2 for each household with PV panels via 15% efficiency [28]. The specifications of the considered grid cluster are collected in Table I. In addition, the specifications of are summarized in Table II.

It is considered that at H#18 connected to phase B, an intrusion happens at t = 0.1 *sec* and voltage starts to fluctuate. This intrusion causes voltage fluctuations across the phase B due to sudden increase in reactive power demand. The STDT of the framework by considering the physical configuration of the grid cluster, capacity of SPVIs and available power manages reactive power set-points of SPVIs on phase B. This procedure must happen in a short timeframe such that the consumers and the equipment do not experience voltage fluctuations. Otherwise, the SPVI connected to the cluster at H#17 would trip due to predefined voltage boundary violation longer than a specific clearing time [8]. If the SPVI connected to the H#17 trips, the balance between power generation and consumption would be lost. This unbalance situation might cause tripping of the entire grid cluster (see Fig. 4). In this case, not only the critical loads (like hospitals, governmental facilities, water-pumping amenities, etc.) would be disconnected from the grid, but also ultra-low frequency oscillations (ULFOs) might occur on the upper power grid. As depicted in Fig. 5, at t = 0.1 *sec*, the PCC voltage of the SPVI located at H#17 starts to fluctuate. As illustrated in Fig. 5-a, the assigned reactive power set-point for each SPVI is decided based on the location and configuration of the grid cluster. However, the STDT immediately adjusts the set-points of the SPVIs such a way that the voltage does not exit the pre-defined boundary, thus the malicious intrusion can not push any SPVI to be tripped because the STDT establishes the voltage after any incident (Fig. 5-b).

Table. I Grid Cluster Specifications

Parameter	Value
No. of Households	30
No. of Households with SPVI	15
Grid Voltage	120 V_{RMS}
Grid Frequency	60 Hz
Resistance of Overhead Line	0.32 Ω/km
Reactance of Overhead Line	0.1 mH/km
Effective Rooftop Area	520 ft^2
Rated Power of SPVI	7.5 kW

Table. II MPLT Specifications

Parameter	Value
Filter Resistance	0.1 mΩ
Filter Inductance	1.0 mH
Sampling Time	10 μs

In addition, some of the malicious activities might target the entire feeder to be disconnected from the upper hand-side grid due to unbalance condition. Some of buses have critical loads connected like hospitals. Due to malicious attacks, the voltage balance between the phases might be lost. In this case, the entire grid cluster will be tripped from the grid, which obviously is not desired. The proposed STDT has the capability of handling these attacks with quick set-point adjustment of

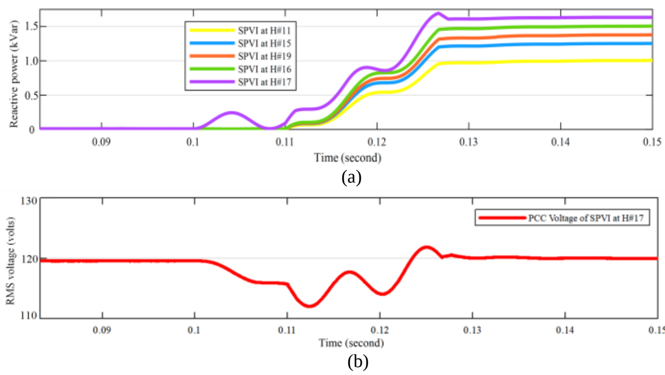

Fig. 5. Cooperative MPLT and STDT performance under malicious intrusion: a) reactive power injection by SPVIs to mitigate the intrusion, and b) RMS voltage at the PCC of H#17.

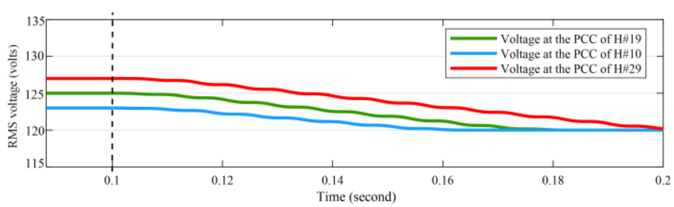

Fig. 6. Collaborative operation of SPVIs via STDT to mitigate malicious intrusion on all three feeders.

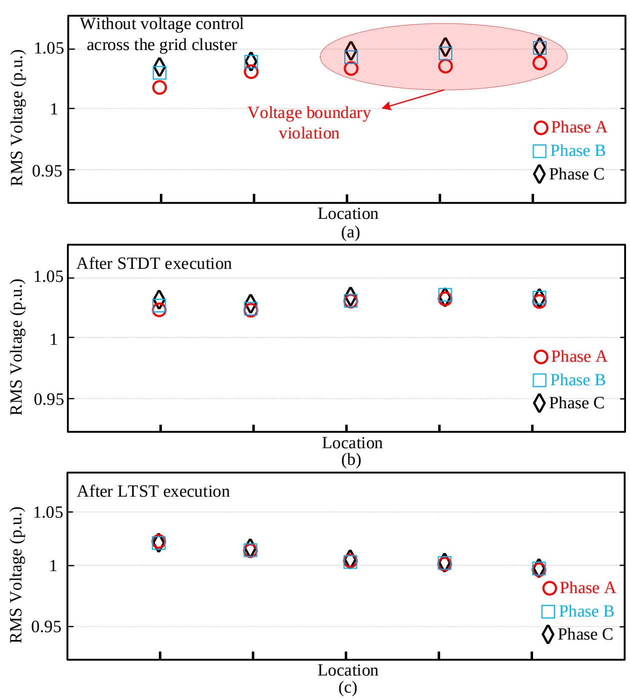

Fig. 7. RMS voltage across the grid cluster: a) before employing the proposed framework, b) after executing STDT, and c) after executing LTST.

TABLE. III Summary of The Proposed Framework Performance

Stage	P_{loss} (p.u.)	ΔP_{loss} (%)	v_{min} (p.u.)	v_{max} (p.u.)
Before executing the proposed framework	0.18	-	1.02	1.06
After STDT	0.187	+ 3.89	1.03	1.04
After LTST	0.149	- 17.22	1.005	1.02

nearby SPVIs. By considering critical loads on H#10, H#19, and H#29, the STDT must try to keep the three phases of the grid cluster balanced. To do this, the SPVIs absorb reactive power to keep the voltage among the three phases of the grid cluster balanced. In Fig. 6, at t = 0.1 *sec*, the STDT is activated to return back the voltage at H#10, H#19, and H#29 to nominal value. As depicted in Fig.6, the voltage rise is worsen at H#29 (phase c). However, the framework still performs voltage control in a timely manner according to standard, and keeps the entire feeder balanced.

After mitigating the rapid fluctuations across the grid and avoiding tripping of the SPVIs to keep the generation and consumption balanced to keep the entire system stable and avoid ULFOs, there is a high possibility that the optimal operation of the grid cluster is deteriorated due to excessive reactive power flow on the grid and probable increased power delivery loss. Thus, the proposed framework executes the LTST in one-minute intervals. One-minute interval is sufficient for data gathering and giving time for the STDT to stabilize the network, after that the LTST optimizes operation of the entire grid. In Fig. 7-a, voltage at different buses before executing the proposed framework is depicted. Before employing the STDT, the predefined voltage boundaries are violated towards the end of the cluster on all of the three phases. To avoid tripping the SPVIs, the STDT performs in a subsection interval and as presented in Fig. 7-b, the STDT brings back the voltage across the cluster into the allowable vicinity. This action happens in a sub-second timeframe. After this stage, although the SPVIs are not going to be tripped, the operation of the cluster is not optimal. The LTST is executed every one minute, and ensures that the cluster is at its optimal point. The voltage across the cluster after the LTST is illustrated at Fig. 7-c. Clearly, the LTST pushes the system to a safe margin of the voltage violation boundaries. Moreover, the voltage among three phases is pushed to be balanced after this stage. As summarized in Table III, after executing the STDT, although the voltage boundary violation has been solved, the power delivery loss has been increase. The framework, by executing the LTST brings back the entire grid cluster to the optimal operating point by reducing the power delivery loss 17.22 percent.

VI. Conclusion

Increasing number of SPVIs at the distribution level introduces new challenges for controlling and optimal utilization of the entire grid. Moreover, this part of the grid is prone to more cyber attacks. These attacks might push the SPVIs or even the entire grid cluster to be disconnected from the reset of the grid due to voltage boundary violation specified in grid integration standards. To avoid this. In this paper a holistic multi-timescale voltage control framework proposed and tested. By employing the proposed framework, the rapid incidents on the voltage of the grid will be mitigated to avoid tripping of SPVIs while optimal operation of the entire grid is ensured as well to prevent imposing extra expenses to the utility and consumer sides.

References

[1] C. W. Gellings, M. Samotyj, and B. Howe, "The future's smart delivery system [electric power supply]," *IEEE Power Energy Mag.*, vol. 2, no. 5, pp. 40-48, 2004.

[2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — The new and improved power grid: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944-980, 2012.

[3] V. C. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28-42, 2013.

[4] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998-1010, 2012.

[5] S. A. Baker, N. Filipiak, and K. Timlin, *In the dark: Crucial industries confront cyber attacks*. McAfee, Incorporated, 2011.

[6] *Venezuela crisis: Fresh power cuts black out Caracas* [Online]. Available: https://www.bbc.com/news/world-latin-america-47703864.

[7] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317-3318, 2017.

[8] "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces - Redline," *IEEE Std 1547-2018*, pp. 1-227, 2018.

[9] "*IEEE Application Guide for IEEE Std 1547™, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*," 2009.

[10] E. Troester, "New German grid codes for connecting PV systems to the medium voltage power grid," in *2nd International workshop on concentrating photovoltaic power plants: optical design, production, grid connection*, 2009, pp. 1-4.

[11] *American National Standard for Electric Power Systems and Equipment—Voltage Ratings (60 Hz)*, 100277, 2016.

[12] Z. Zhang, L. F. Ochoa, and G. Valverde, "A novel voltage sensitivity approach for the decentralized control of DG plants," *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 1566-1576, 2018.

[13] S. Weckx and J. Driesen, "Optimal local reactive power control by PV inverters," *IEEE Trans. Sustain. Energy*, vol. 7, no. 4, pp. 1624-1633, 2016.

[14] A. Safayet, P. Fajri, and I. Husain, "Reactive power management for overvoltage prevention at high PV penetration in a low-voltage distribution system," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5786-5794, 2017.

[15] A. Cagnano and E. De Tuglie, "Centralized voltage control for distribution networks with embedded PV systems," *Renewable Energy*, vol. 76, pp. 173-185, 2015.

[16] K. E. Antoniadou-Plytaria, I. N. Kouveliotis-Lysikatos, P. S. Georgilakis, and N. D. Hatziargyriou, "Distributed and decentralized voltage control of smart distribution networks: models, methods, and future research," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2999-3008, 2017.

[17] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715-2729, 2013.

[18] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: an adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532-543, 2016.

[19] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370-379, 2014.

[20] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216-1227, 2014.

[21] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396-1407, 2014.

[22] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731-6741, 2018.

[23] A. Bidram, L. Damodaran, and R. Fierro, "Cybersecure Distributed Voltage Control of AC Microgrids," in *2019 IEEE/IAS 55th Industrial and Commercial Power Systems Technical Conference (I&CPS)*, 2019, pp. 1-6.

[24] D. Chatterjee and S. K. Mazumder, "Switching-sequence control of a higher order power-electronic system driving a pulsating load," *IEEE Trans. Power Electron.*, vol. 35, no. 1, pp. 1096-1110, 2020.

[25] C. Bordons and C. Montero, "Basic principles of MPC for power converters: Bridging the gap between theory and practice," *IEEE Ind. Electron. Mag.*, vol. 9, no. 3, pp. 31-43, 2015.

[26] M. Ciobotaru, R. Teodorescu, and F. Blaabjerg, "A new single-phase PLL structure based on second order generalized integrator," *37th IEEE Power Electronics Specialists Conference*, 2006.

[27] M. Farivar, C. R. Clarke, S. H. Low, and K. M. Chandy, "Inverter VAR control for distribution systems with renewables," *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011.

[28] A. P. Dobos, "PVWatts version 5 manual," National Renewable Energy Lab.(NREL), Golden, CO (United States), 2014.