Letters

Spectral Decomposition-Based Mitigation of Radiative Side-Channel Noise Intrusion in a Cascaded SST

Debotrinya Sur, *Graduate Student Member, IEEE*, Shantanu Gupta, *Graduate Student Member, IEEE*, Mateo D. Roig Greidanus, *Graduate Student Member, IEEE*, and Sudip K. Mazumder, *Fellow, IEEE*

***Abstract*—Solid-state transformers (SSTs) are an emerging class of converters that have shown potential to replace traditional low-frequency transformers (LFTs). With cascading capabilities similar to modular multilevel converters, SSTs can efficiently handle higher voltage and power levels. A cascaded SST setup usually uses a decentralized hierarchical control architecture, with primary controllers overseeing operations at the module level and secondary controllers keeping an eye on operations at the aggregated phase level. Despite their potential to replace LFTs, reliability concerns hinder their widespread adoption, given their vulnerability to cyberattacks. Nonintrusive attacks, such as side-channel noise intrusion (SNI), threaten the SSTs' stability by corrupting the measurement feedback signals fed to the controllers. This letter proposes a novel technique for rapid intrusion detection and mitigation of radiative SNI threats to provide resilience to the secondary layer of the cascaded SSTs. The technique entails spectral decomposition of the noise-tampered signal, followed by noise-free signal reconstruction of the targeted frequency component. Experimental results validated the solution deployed in a cascaded SST experimental prototype's secondary control layer to deal with radiative noise on global input voltage sensor feedback.**

***Index Terms*—Cyberattack, fast Fourier transform (FFT), intrusion detection, power converters, radiative side-channel intrusion.**

I. Introduction

SOLID-STATE transformers (SSTs) [1], [2], a potential replacement for low-frequency transformers (LFTs) in the power transmission and distribution grid, are capable of handling high voltage and power levels owing to their flexible modularity. Their vulnerability to cyber-attacks impedes their broader adoption, especially considering their crucial role in the electrical power grid. In [3], the catastrophic impact of electromagnetic side-channel noise intrusion (EM-SNI) and its mitigation on modular voltage sensors have been explored. The mitigation is achieved by estimating the noise-free, real signal using the dynamical model of an SST module provided in [4]. Alternatively, in [5], a Kalman filter-based method is employed to detect the effects of false data injection attacks on local controllers of modular multilevel converters. Both solutions employ a model-based approach, enabling rapid detection and accurate mitigation of cyberattacks. The present detection and mitigation techniques are mostly data-driven techniques that require large amounts of high-quality data for effective model training, making them highly dependent on the availability of comprehensive datasets [6], [7]. Moreover, the computational complexity of these data-driven models, especially in real-time applications, demands significant data processing power, limiting their scalability. In addition, the sensitivity of these models to threshold

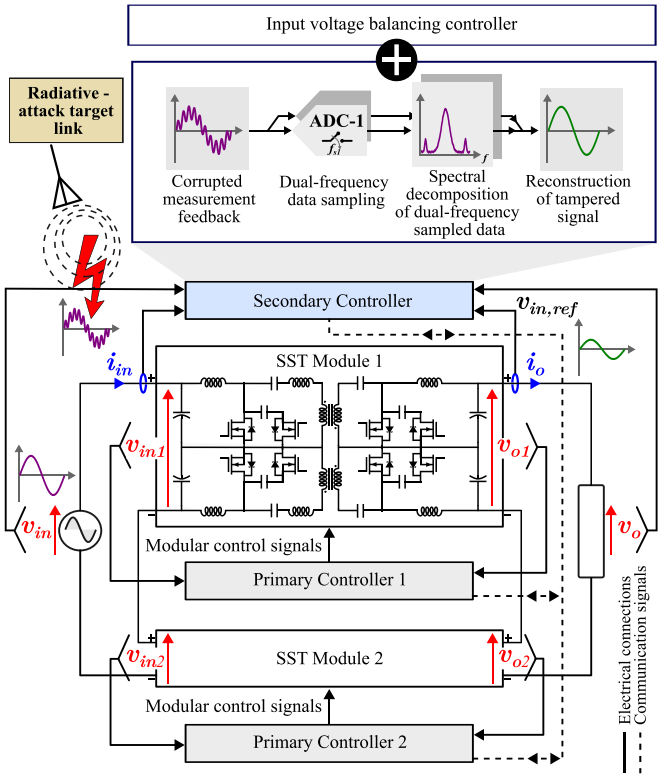

Fig. 1. Cascaded SST architecture, highlighting the radiative side-channel noise target link.

Received 12 August 2024; revised 13 September 2024; accepted 3 October 2024. Date of publication 14 October 2024; date of current version 18 December 2024. The work of Sudip K. Mazumder at the University of Illinois Chicago was supported in part by the U.S. Department of Energy under Grant DE-CR0000019 and in part by the U.S. National Science Foundation under Grant 2219734. *(Corresponding author: Sudip K. Mazumder.)*

The authors are with the Electrical and Computer Engineering Department, University of Illinois Chicago, Chicago, IL 60607 USA (e-mail: dsur2@uic.edu; sgupt57@uic.edu; mgreid2@uic.edu; mazumder@uic.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPEL.2024.3477274.

Digital Object Identifier 10.1109/TPEL.2024.3477274

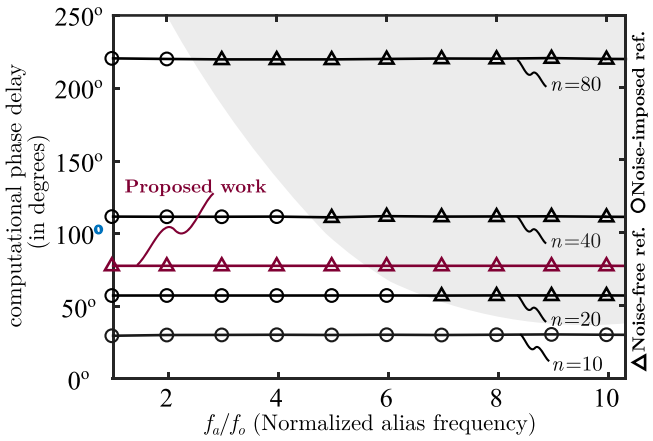

Fig. 2. Comparison of computational phase delay between the proposed work with FIR filters of varied orders.

settings requires careful tuning, which complicates deployment in dynamic environments where conditions frequently change [8].

While the previous work [3] implemented an estimator-based mitigation using a model of a single SST module with a resistive load, this letter presents a model-free approach. Limited research exists on model-free approaches for detecting and mitigating cyber-attacks on sensor feedback. Moreover, modeling the interactions between modular converters and their scalability in a cascaded converter [6], as such in the cascaded single-stage SST setup, as shown in Fig. 1, is a further complex task. To avoid these complexities, this letter introduces a novel spectral decomposition (SD) approach that computes dual fast Fourier transforms (FFTs) of a noise-tampered signal sampled at two different frequencies. The distinct sampling frequencies ensure that the low-frequency aliases of the high-frequency noise signal appear at different frequencies in the FFT window, aiding in the detection of a cyber-attack. Similarly, the positions of these aliases are also utilized to extract the target frequency component from the FFT spectra and reconstruct a noise-free signal, mitigating the effects of cyber-attacks. Comparisons of computational delays between the proposed method and finite impulse response (FIR) filters of different orders are presented in Fig. 2. It is observed that for FIR filters, a higher order filter is required to filter aliases closer to the fundamental frequency, thus significantly increasing the computational delay. In contrast, the proposed method introduces an acceptable and constant computational delay for an entire range of alias frequencies. In addition, if the alias frequency is near the fundamental, it will lead to intermodulation [7], thus making it nearly impossible to extract the fundamental frequency using a simple filter of a practically realizable order.

This work demonstrates the effectiveness of the proposed detection and mitigation strategy to counteract the impact of tampered measurement feedback of the voltage global sensors at the secondary control layer of a cascaded SST network. The secondary controller averages the global sensor feedback according to the number of modules and sends the input voltage reference to the primary controllers. Each primary controller, a proportional resonant controller tuned to the fundamental frequency (60 Hz), manages modular modulation, as discussed in [4]. The rest of this letter is organized as follows. Section II briefly discusses the aliasing effects caused by the undersampling of tampered voltage measurements in discrete time and frequency domains. The methodology based on the SD of a signal sampled at dual frequencies is thereafter explained in detail for detecting and mitigating the effects of tampered signal feedback. Section III presents the experimental validation of the proposed algorithm, along with studies highlighting its effectiveness. Finally, Section IV concludes this letter.

II. Intrusion Detection and Mitigation Using SD

In this section, we introduce the methodology for detecting and mitigating the effects of radiative SNI by reconstructing the tampered signal using SD and positioning low-frequency aliases of inadequately sampled high-frequency signals. High-frequency noise is radiatively injected into the global input voltage sensor, similar to that in [3], leading to signal aliasing as a result of undersampling, as described in [8]. A discrete time representation of the noise-imposed input voltage signal be

$$v_{in}^{'}\ [n] = V_{in}\ \sin\left(2\pi f_o n/f_s\right) + V_n \sin\left(2\pi f_a n/f_s\right) \tag{1}$$

where V_{in} and V_n represents the amplitude of the input and noise signal, respectively, f_o denotes the fundamental frequency (60 Hz), f_a denotes the low-frequency alias of the high-frequency noise signal, and f_s is the analog-to-digital converter (ADC) sampling rate. The discrete Fourier transform (DFT) of (1) is shown

$$V_{in}^{'}[k] = V_{in} \sum_{n=0}^{N-1} \sin\left(2\pi f_o n/f_s\right) e^{-\frac{j2\pi kn}{N}} + V_n \sum_{n=0}^{N-1} \sin\left(2\pi f_a n/f_s\right) e^{-\frac{j2\pi kn}{N}} \tag{2}$$

where N is the number of samples for the DFT and $k = 0, 1, 2, \ldots,\ N-1$. The magnitude spectrum of the DFT or FFT of the signal will exhibit two distinct peaks: one at the fundamental frequency (f_o) and the other at the alias frequency (f_a), as shown in Fig. 3. The extent of spectral leakage amongst the frequency bins is determined by the sampling frequency and the number of sample points of the FFT.

A. Proposed Methodology

In this section, the methodology proposed has been explained in detail, which involves sampling the noise-imposed voltage signal at two distinct but closely spaced frequencies and computing two separate FFTs using the two different set of sampled values. This ensures that the aliases in the magnitude spectra of the two FFTs are spaced apart in frequency, while the fundamental frequency components coincide, as seen in Fig. 3. The two distinct alias frequencies f_{a1} and f_{a2}, majorly appear in the $(\lfloor f_{a1}/f_{bin1} + 1/2 \rfloor + 1)$th and $(\lfloor f_{a2}/f_{bin2} + 1/2 \rfloor + 1)$th bins, respectively, where $\lfloor \cdot \rfloor$ denotes the floor function and the first bin represents the dc value of the signal. Depending on

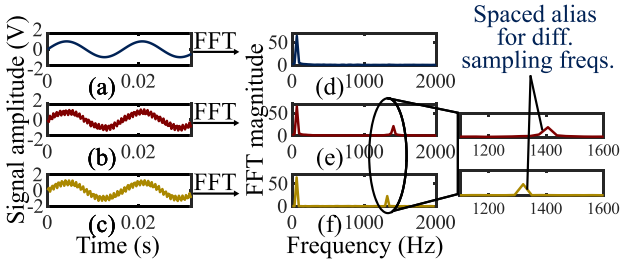

Fig. 3. (a) Untampered 60-Hz voltage signal, with radiatively injected noise at 51.1386 MHz, sampled at (b) 40 kHz and (c) 38.4 kHz. FFT magnitude spectrum of (d) untampered signal, tampered signal sampled at (e) 40 kHz and (f) 38.4 kHz. Zoomed views of (e) and (f) highlighting spaced aliasing for different sampling frequencies.

the alias frequencies, there may be some spectral leakage into the neighboring bins. The fundamental frequency component of the signal (i.e., 60 Hz) appears in the same frequency bin for both FFTs and has a comparable magnitude, ensured by the proximity of the sampling frequencies. Algorithm 1 explains the proposed methodology in detail.

The signals sampled at f_{s1} and f_{s2} are stored in a sliding buffer of length N (lines 5–9). FFTs of the two input datasets are computed (line 10), and the magnitude and phase spectra are separated. For intrusion detection, a bin-by-bin difference of the magnitude spectra is calculated (lines 20–32). Under nominal conditions, i.e., with no noise injection, the spectra should essentially cancel each other out and show no peaks. However, in the case of a monotone noise injection, the presence of spaced-apart peaks ensures that the difference crosses a defined threshold (γ) couple of times, triggering the intrusion detection scheme (*intrusion detection scheme (IDS)_flag*). This results in switching from measurement-based control to estimate-based control. The noise-free signal is reconstructed by extracting the amplitude and phase information from the amplitude and phase spectra. For the amplitude, the minimum of the two magnitude spectra is taken, and the target frequency (i.e., 60 Hz) is extracted with appropriate scaling according to FFT specifications. For the phase, we choose the phase of the target frequency from the FFT phase spectrum of the signal with the alias further away from the target frequency. The spectrum with the alias further away will have minimal spectral leakage at the target frequency. Using these two parameters and compensating for any computational delay, the input voltage signal is estimated (v_{est}) (line 33) and subsequently used for the control of the cascaded SST setup.

Algorithm 1: FFT-based IDS—Mitigation Algorithm.

1: **Input:** v_{in}
2: **Output:** IDS_flag, v_{est}
3: **Declare:** $N,\ f_{s1},\ f_{s2}, \gamma$
4: void **main()**
5: $v_{in1} \leftarrow$ **ADC** (v_{in}, f_{s1}); $v_{in2} \leftarrow$ **ADC** (v_{in}, f_{s2})
6: **for** i : 0 to $N-1$ **do**
7: $\text{FFT}_1.\text{inBuff}[i] \leftarrow \text{FFT}_1.\text{inBuff}[i+1]$;
8: $\text{FFT}_2.\text{inBuff}[i] \leftarrow \text{FFT}_2.\text{inBuff}[i+1]$;
9: **end for**
10: $\text{FFT}_1.\text{inBuff}[N] \leftarrow v_{in1}$; $\text{FFT}_2.\text{inBuff}[N] \leftarrow v_{in2}$
11: $[\text{FFT}_x.\text{magBuff},\ \text{FFT}_x.\text{phaseBuff}] \leftarrow$ **FFT**$(\text{FFT}_x.\text{inBuff})$ $\triangleright x = 1,\ 2$ for FFT_1 and FFT_2
12: **IDS_MITIGATION** $(\text{FFT}_x.\text{magBuff},\ \text{FFT}_x.\text{phaseBuff})$ $\triangleright x = 1,\ 2$ for FFT_1 and FFT_2
13: **if** $\text{IDS}_{\text{flag}} = 1$ **then**
14: $v_{ref}^{in} = v_{est}/n$
15: **else**
16: $v_{ref}^{in} = v_{in}/n$
17: **end if**
18: end **main()**
19: **function** IDS_MITIGATION $(\text{FFT}_x.\text{magBuff},\ \text{FFT}_x.\text{phaseBuff})$ $\triangleright x = 1,\ 2$ for FFT_1 and FFT_2
20: **for** j : 0 to N **do**
21: $v_{mag\_diff}[j] \leftarrow \text{FFT}_1.\text{magBuff}[j] - \text{FFT}_2.\text{magBuff}[j]$
22: **if** $v_{mag\_diff}[j] > \gamma$ **then**
23: $\text{IDS\_flag} = 1$
24: $\phi_{fo} \leftarrow \text{FFT}_1.\text{phaseBuff}[k]$
25: **else if** $v_{mag\_diff}[j] > -\gamma$ **then**
26: $\text{IDS\_flag} = 1$
27: $\phi_{fo} \leftarrow \text{FFT}_2.\text{phaseBuff}[k]$
28: **else**
29: $\text{IDS\_flag} = 0$
30: $\phi_{fo} \leftarrow \text{FFT}_1.\text{phaseBuff}[k]$
31: **end if**
32: **end for**
33: $v_{est} = V_{scale}.\min(\text{FFT}_1.\text{magBuff}[k], \text{FFT}_2.\text{magBuff}[k])\ .sin(\phi_{fo} + \phi_{comp\_delay})$
34: **return** IDS_flag, v_{est}
35: **end function**

III. Experimental Validation

The following experimental results validate the proposed methodology for detecting and mitigating the effects of radiative cyber-attacks on cascaded ac/ac direct power conversion SSTs. Fig. 4 shows the experimental setup of the cascaded SST setup and the controller modules. The SST modules (1 and 2) are each controlled by their primary controllers (3 and 4) and are connected in cascaded architecture. The entire setup is overseen by a secondary controller (5) using feedback from the global voltage sensor (6). A detailed description of the converter topology is provided in [4]. Texas Instruments C2000 family microcontroller, TMS320F28379D, is being used to compute the FFTs and control the setup. Parallel computing of the FFTs, utilizing the dual-core functionality of the microcontroller, minimizes computational overhead and prevents interference with the nominal voltage balancing controller in the secondary layer of the cascaded SST setup. The time required for computing each FFT is approximately 18 μs, leading to significantly faster intrusion detection and mitigation compared to current data-driven techniques.

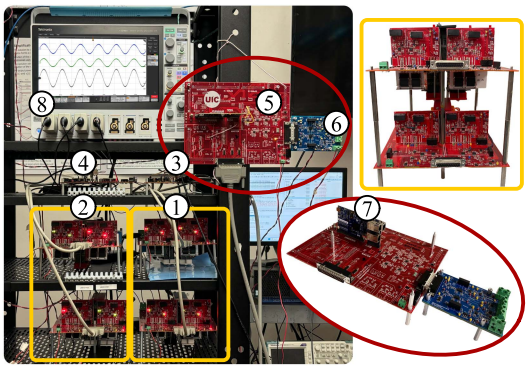

Fig. 4. Experimental hardware setup showcasing the network of cascaded SST modules and the associated controller modules. The denoted blocks are as follows: (1) SST module one, (2) SST module two, (3) primary controller one, (4) primary controller two, (5) secondary controller, (6) global voltage sensor board, (7) TMS320F28379D DSP, and (8) mixed signal oscilloscope.

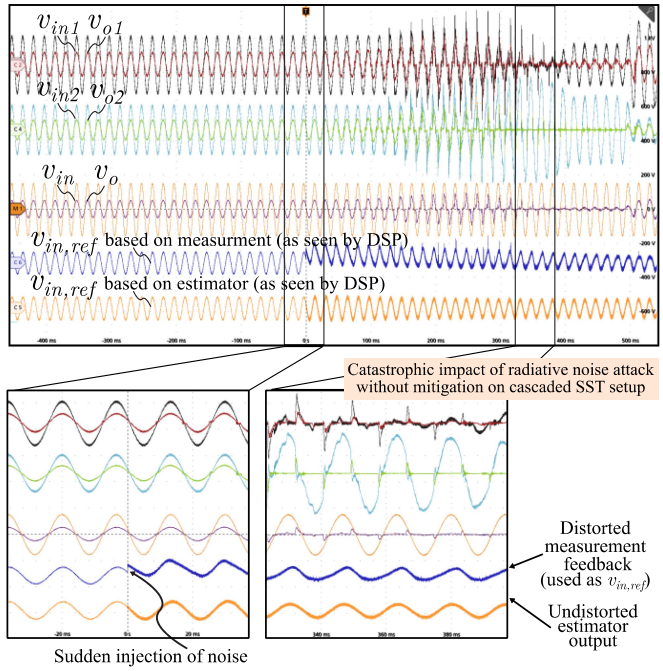

Fig. 5. Time-domain results showcasing the impact of radiative SNI on a cascaded SST setup without mitigation with zoomed view of instances highlighting the sudden injection of radiative noise on the cascaded SST setup and highlighting the catastrophic effect of radiative noise on a cascaded SST setup without any mitigation.

The experimental results presented here were obtained by operating the setup at an input voltage of 220 V and a power level of 400 W. The setup operates at a switching frequency (f_{sw}) of 40 kHz and maintains a unity gain. During validation, the ADC sampling frequencies (f_{s1} and f_{s2}) were set to 40 and 38.4 kHz, respectively. These samples were then downsampled by a factor of 10 to enhance the resolution of a 128 ($= N$) point FFT. The chosen frequencies serve specific purposes: the 40-kHz sampling frequency allows the use of the same pulsewidth modulation signals for switching the power semiconductor devices and triggering the ADC, while the 38.4-kHz sampling frequency minimizes the effects of spectral leakage around the fundamental frequency (60 Hz) in a 128-point FFT. Sinusoidal noise with a frequency (f_n) of 51.1386 MHz was purposefully introduced onto the printed circuit board (PCB) traces to disrupt the signals and impact the system. This frequency significantly affected the signals, as seen in Fig. 6(a), when emitted and tweaked within a range from 40 to 60 MHz.

In the worst-case scenario, as depicted in Fig. 5, the effect of radiative-SNI on a cascaded SST system is illustrated without any active mitigation algorithm in place. At time $\boldsymbol{t} = 0$, a sudden noise injection distorts the feedback-based reference signal by superimposing the fundamental 60 Hz signal with a low-frequency alias of the radiative-SNI. This distorted reference is then used by the secondary controller to generate the input voltage references for the individual primary modules. The catastrophic impact of this distorted voltage reference is evident, as it destabilizes the entire cascaded setup and disrupts its operation. In contrast, the estimator output (orange trace) generates a voltage reference consisting solely of the 60-Hz component, which, when applied, mitigates the effects of radiative-SNI attacks and preserves system stability.

Figs. 6 and 7 depict the real-time experimental validation of the proposed algorithm under the previously mentioned conditions. An intentional four-line cycle delay was introduced between the detection of an intrusion and its mitigation by changing over to estimate-based control, as shown in Fig. 6(a). This delay demonstrates the impact of radiative-SNI on the cascaded setup. The superposition of low-frequency aliases of the high-frequency noise with the actual signal distorts the input voltage feedback, which is subsequently used to generate the input voltage reference for maintaining voltage balance across the individual SST modules. In a type-1 ac/ac converter [4], as here, disturbances at the input propagate to the output with minimal delay due to the absence of a dc link. The effect of the disturbance is evident in the output voltages and is supported by the rise in total harmonic distortion (THD), as seen in Fig. 6(b), when the attack is carried out without any mitigation. Upon initiation of the mitigation strategy, the THD levels return to below nominal values. This occurs because the 60-Hz component is extracted from the FFT spectra, ensuring it does not contain any other frequency components. The actual efficacy of the algorithm is demonstrated in Fig. 7, where the intrusion is mitigated within a switching line cycle (25 μs) of detection, resulting in minimal impact on the converter setup.

To validate the extensibility of the proposed algorithm, it was tested across a range of noise frequencies. Parametric results, as shown in Fig. 8, highlight the impact of noise on the output voltage THD, both with and without the proposed mitigation algorithm, compared to nominal noise-free operation. A noise frequency range of 50.98151–50.98159 MHz was selected because the low-frequency alias appears in the 30–110 Hz range. This range has the most significant effect on the system due to its proximity to the 60-Hz component, around which the primary proportional resonant controller is tuned. Without mitigation, the maximum THD rises to around 7%, exceeding permissible operational limits. However, with active mitigation, the THD drops to an average of approximately 2.5%. The selected frequency range has the greatest impact on the converter, given the

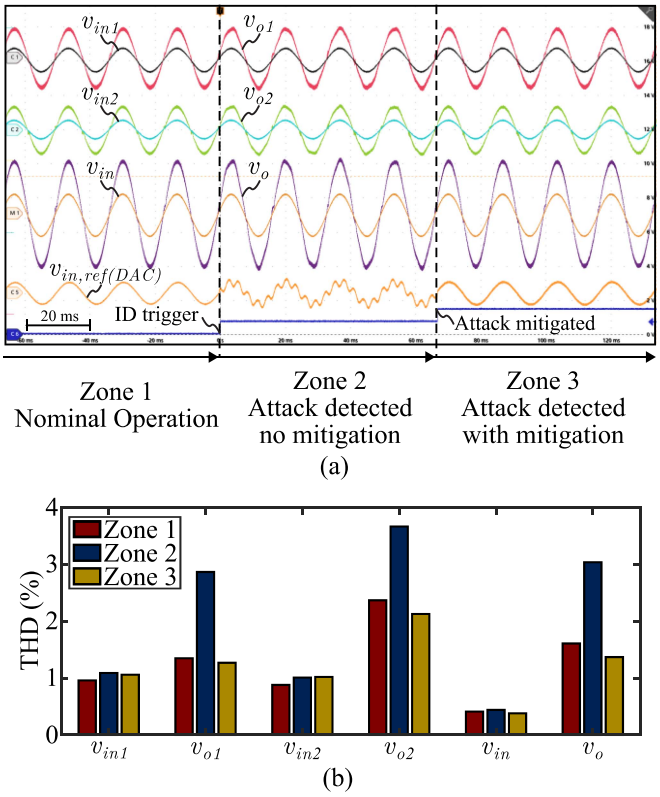

Fig. 6. Real-time experimental validation of the proposed ID and mitigation method for a cascaded SST system operating at $V_{in} = 220\,V_{RMS}$. (a) Impact of EM-SNI at 51.1386 MHz with an intentional four-line cycle delay between ID and mitigation. (b) THD comparison of different system voltages during nominal operation (Zone 1), with attack detected but no mitigation (Zone 2), and with attack detected and mitigated (Zone 3) for the case presented in (a). Scales for input voltages: 500 V/div, output voltages: 200 V/div, ref. (DAC): 1 V/div.

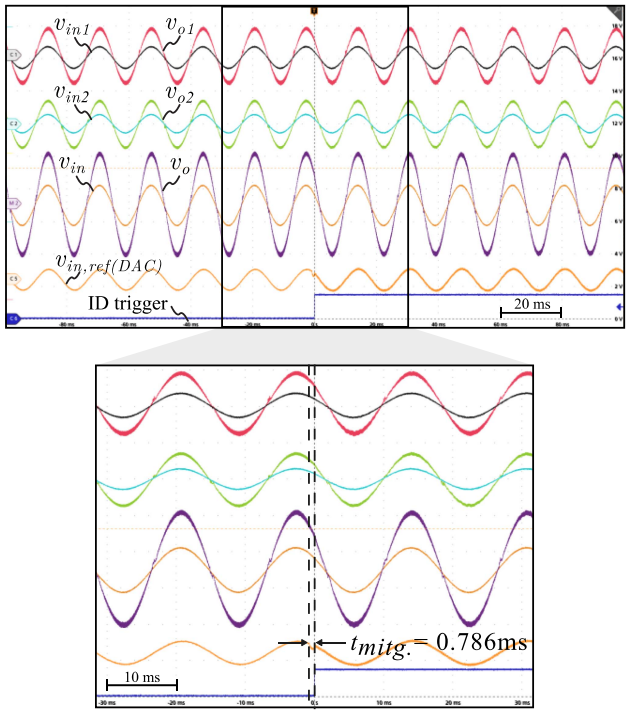

Fig. 7. Instantaneous changeover from measurement-based control to estimate-based control to mitigate the effects of EM-SNI at 51.1386 MHz. Scales for input voltages: 500 V/div, output voltages: 200 V/div, ref. (DAC): 1 V/div.

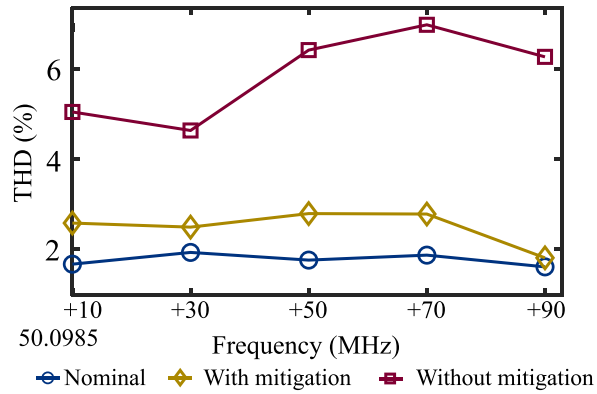

Fig. 8. Comparison of impact of EM-SNI at different attack frequencies ranging from 50.098510–50.098590 MHz on output voltage THD with and without the proposed mitigation with respect to nominal operation.

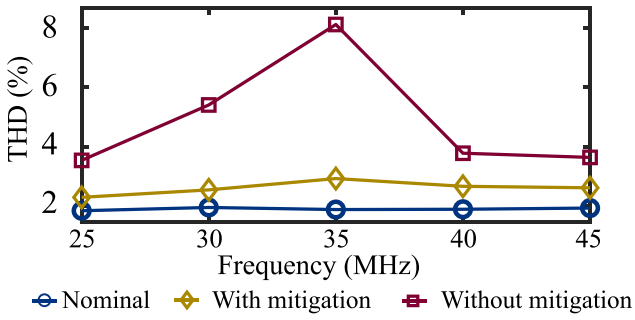

Fig. 9. Comparison of impact of EM-SNI at different attack frequencies ranging from 25 to 45 MHz on output voltage THD with and without the proposed mitigation with respect to nominal operation.

high degree of coupling between the antenna traces and the PCB traces of the converter, as previously discussed in [3]. In addition, THD comparisons are made over a broad frequency range, from 25 to 45 MHz, as shown in Fig. 9. The impact is lower in this range due to the reduced transfer or coupling of energy between the antenna and the traces. However, a significant reduction in THD is observed once the mitigation is activated, compared to when no mitigation is applied.

The robustness and reproducibility of the detection algorithm were tested over 30 iterations. The results, illustrated as a Gamma distribution in Fig. 10, use parameters a and b to define the distribution. The detection density indicates the percentage of attacks detected within a specified timeframe, while the probability of detection represents the likelihood of an attack being detected after a certain duration. The data reveal that approximately 30% of attacks are detected within 0.4 ms, with an average detection time of around 0.5 ms. In addition, the probability of detecting an attack exceeds 95% after 1 ms. The algorithm is impervious to triggering a false positive in the IDS when a 37.5% step change in input voltage is applied, as shown in Fig. 11, highlighting its operability during transient conditions. A step change introduces various harmonic components with

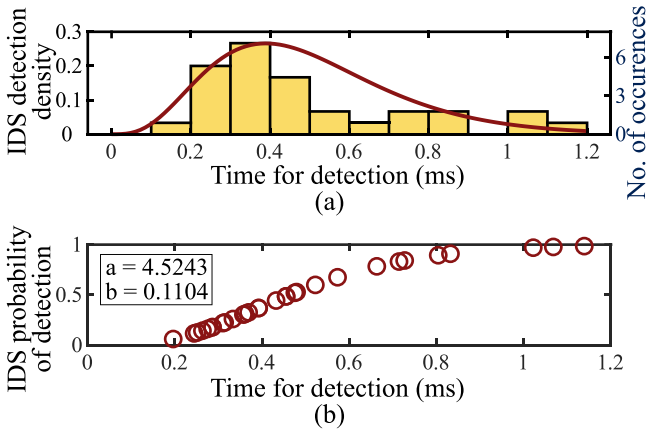

Fig. 10. Analysis of IDS performance. (a) Distribution of IDS detection times and (b) probability of IDS detection over time, with radiative noise injection at 51.1386 MHz.

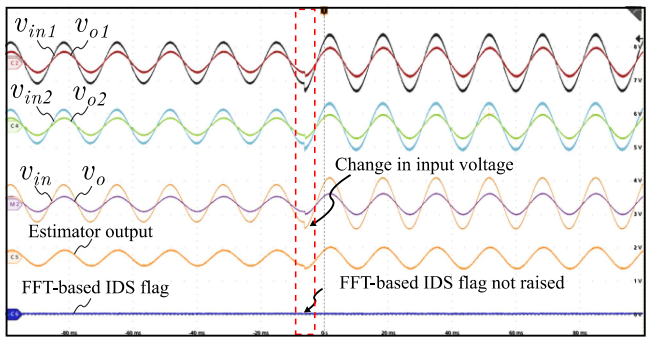

Fig. 11. Transient operation with a step change in input voltage, without falsely raising the FFT-based IDS flag.

progressively decreasing magnitudes, as shown by its Fourier series. These harmonics fall within the Nyquist frequency of the sampling rates and thus cancel each other out when comparing the magnitude spectra differences used by the IDS.

IV. Conclusion

Radiative noise intrusions on global sensors of cascaded SST setups pose a significant threat to the stable operation of converters. This letter proposes an IDS and mitigation scheme based on SD of a tampered voltage signal at two distinct but close sampling frequencies. When the noise-injected signal is sampled at different frequencies, the aliased noise components are spaced apart in the frequency domain. This technique extracts the amplitude and phase of the target component through the real-time FFT spectra, enabling fast intrusion detection (less than 1 ms) and reconstruction of the noise-free voltage signal. The effectiveness and efficacy of the proposed technique are demonstrated through multiple trials and its implementation on a hardware platform. The frequency of injected noise was bounded by the Nyquist frequency of the ADCs. The technique could be readily extended to other attack vectors that impact the control measurement feedback, such as the conductive interference attacks discussed in [11], which demonstrate a similar impact due to aliases arising from undersampling a high-frequency signal injected conductively. Continued research into robust and resilient control of power electronic converters to counteract cyber-attacks will further enhance the efficacy and applicability of this approach.

References

[1] S. K. Mazumder, "Solid-state power-conversion system," U.S. Patent 11594978, 2023.
[2] R. Raju, M. Dame, and R. Steigerwald, "Solid-state transformers using silicon carbide-based modular building blocks," in *Proc. IEEE 12th Int. Conf. Power Electron. Drive Syst.*, Honolulu, HI, USA, 2017, pp. 1–7.
[3] M. D. R. Greidanus, S. D'Silva, S. Gupta, D. Sur, S. K. Mazumder, and M. B. Shadmand, "Electromagnetic side-channel noise intrusion on solid-state transformer," *IEEE Trans. Power Electron.*, vol. 39, no. 8, pp. 9244–9256, Aug. 2024.
[4] S. Gupta and S. K. Mazumder, "A differential-mode isolated AC/AC converter," *IEEE Trans. Power Electron.*, vol. 38, no. 10, pp. 12846–12858, Oct. 2023.
[5] C. Burgos-Mellado et al., "Cyber-attacks in modular multilevel converters," *IEEE Trans. Power Electron.*, vol. 37, no. 7, pp. 8488–8501, Jul. 2022.
[6] M. Baker, A. Y. Fard, H. Althuwaini, and M. B. Shadmand, "Real-time AI-based anomaly detection and classification in power electronics dominated grids," *IEEE J. Emerg. Sel. Topics Ind. Electron.*, vol. 4, no. 2, pp. 549–559, Apr. 2023.
[7] J. Zhang, L. Guo, and J. Ye, "Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3929–3942, Sep. 2022.
[8] N. Souri and A. Mehrizi-Sani, "Hybrid machine learning approach for cyberattack mitigation of parallel converters in a DC microgrid," 2024. [Online]. Available: https://arxiv.org/abs/2406.07503
[9] C. Cheng, F. Xie, B. Zhang, D. Qiu, W. Xiao, and H. Ji, "Modeling and nonlinear dynamic analysis of cascaded DC–DC converter systems based on simplified discrete mapping," *IEEE Trans. Ind. Electron.*, vol. 70, no. 6, pp. 5830–5839, Jun. 2023.
[10] L. Guo, T. Ge, and J. Chang, "Intermodulation distortions of bang–bang control class D amplifiers," *IEEE Trans. Power Electron.*, vol. 29, no. 12, pp. 6604–6614, Dec. 2014.
[11] N. Gajanur, M. D. R. Greidanus, S. K. Mazumder, and M. A. Abbaszada, "Impact and mitigation of high-frequency side-channel noise intrusion on the low-frequency performance of an inverter," *IEEE Trans. Power Electron.*, vol. 37, no. 10, pp. 11481–11485, Oct. 2022.