Parasitic Circus: On the Feasibility of Golden-free PCB Verification

Maryam Saadat Safa, Patrick Schaumont and Shahin Tajik
Department of Electrical and Computer Engineering,
Worcester Polytechnic Institute, Worcester, MA, USA
Phone : (+1) 508 831-5239, Email : msafa@wpi.edu

2024 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA) | 979-8-3503-6060-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/IPFA61654.2024.10691201

***Abstract*— Printed circuit boards (PCBs) are an integral part of electronic systems. Hence, verifying their physical integrity in the presence of supply chain attacks (e.g., tampering and counterfeiting) is of utmost importance. Recently, tamper detection techniques grounded in impedance characterization of PCB's Power Delivery Network (PDN) have gained prominence due to their global detection coverage, non-invasive, and low-cost nature. Similar to other physical verification methods, these techniques rely on the existence of a physical golden sample for signature comparisons. However, having access to a physical golden sample for golden signature extraction is not feasible in many real-world scenarios. In this work, we assess the feasibility of eliminating a *physical* golden sample and replacing it with a simulated golden signature obtained by the PCB design files. By performing extensive simulation and measurements on an in-house designed PCB, we demonstrate how the parasitic impedance of the PCB components plays a major role in reaching a successful verification. Based on the obtained results and using statistical metrics, we show that we can mitigate the discrepancy between collected signatures from simulation and measurements.**

***Keywords*— Hardware Security, Hardware Trojans, PCB Verification, Power Delivery Network, Scattering Parameters, Tamper Detection.**

I. Introduction

Printed circuit boards (PCBs) serve as the essential foundation for virtually all electronic systems. They house a variety of microelectronic components, starting from basic discrete devices like diodes, transistors, resistors, and capacitors, all the way to sophisticated integrated circuits (ICs) such as microprocessors, field-programmable gate arrays (FPGAs), and memory modules. The globalized supply chain for PCB manufacturing and assembly leaves PCBs vulnerable to attacks, such as tampering [1] and counterfeiting [2]. Therefore, it is critical to verify PCB's physical integrity before their deployment in the field.

Numerous PCB tamper/counterfeit detection methods have been proposed ranging from inspection using imaging techniques (e.g., X-ray [3] and visual inspection [4]) to behavioral analysis using side-channels [5]. However, most of these approaches suffer from lack of scalability, high cost, and limited detection coverage. To mitigate these shortcomings, novel non-invasive techniques based on impedance characterization of PCB's power delivery network have been introduced [6]–[10]. As any tampering attempt on the PCB or IC will lead to changes in the equivalent impedance of the PDN, the physical monitoring of it provides a holistic solution for determining whether the system's integrity has been violated. While these methods are both precise and efficient, similar to other physical verification methods, the dependence on golden samples for comparison poses a significant challenge. Acquiring these golden samples is notably difficult as a trustworthy PCB assembly factory should exist to manufacture them. Naturally, such a condition might not be met in real-world scenarios and only the design files of the system (e.g., PCB netlist, bill of material, and IC package specifications) are accessible to the verifier. Hence, detection methods that do not rely on golden samples are preferred.

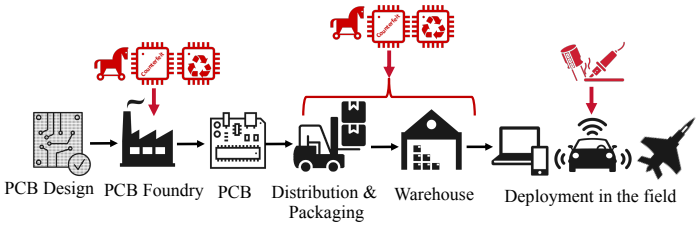


Fig. 1. An illustration of the PCB's supply chain reveals the possible risks, such as hardware Trojans and counterfeit or recycled parts, that may be inserted at each stage of PCB's supply chain.

There has been a few attempts in the literature to eliminate the need for the physical golden sample requirement [11]–[13]. However, the tamper detection capabilities of such framework are confined to the PCB's circuit or chip's firmware and, hence, cannot detect physical modifications, e.g., adding an extra via to the PCB or modifying the PCB materials. A primary challenge in the physical characterization arises from the slight variances in hardware due to the existing manufacturing process variations. Motivated by the constraints and challenges highlighted previously, we are compelled to confront a pivotal question: *is there a possibility to develop a generic method capable of detecting physical tamper events without relying on a physical golden sample, and if so, under what circumstances?*

Our Contribution: In this work, we demonstrate the feasibility of utilizing PCB design files to generate an estimated golden signature, which is then compared to the measured signature of untrusted boards. To validate this approach, we simulate the trusted PCB layout using a sophisticated tool and extract an RF signature

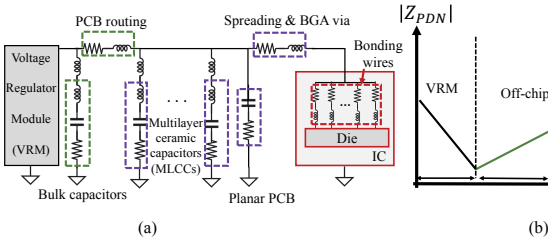


Fig. 2. (a) The equivalent circuit of the PDN of an electronic b
The amplitude of the impedance profile of an electronic board o

characterized by the scattering parameters. We mc
as additions/removals of components to the PCB's l
or replacing them with fake parts. Finally, we compare the trusted simulated data to the measured signature derived from the same physical layout using a similarity measure called dynamic time warping (DTW). Using the DTW metric, we demonstrate that genuine and tampered or counterfeited PCBs can be reliably detected using the simulated golden signatures. Consequently, we provide evidence to support the assertion that *it is feasible to use the simulated signature as the golden signature, provided that the approximate values of the parasitic impedance of the PCB components are known by the verifier.* We also demonstrate that through the application of this tampering attack detection method, *it becomes possible to identify attacks related to the PDNs that are not directly connected to accessible ports*. This detection capability extends beyond conventional means, reaching areas typically considered outside the scope of the testing.

II. Background

A. Power Delivery Network (PDN)

The power delivery network (PDN) serves the crucial role of providing a stable and sufficient power supply to various modules on the PCB, see Fig. 2(a). In complex PCB designs, different chips and components have diverse power distribution requirements, including specific supply voltage levels, maximum load currents, and voltage noise margins. To fulfill these requirements, the PDN employs voltage regulator modules (VRMs) arranged in a tree structure, establishing multiple voltage domains. The off-chip component typically determines the Z_{PDN} (PDN impedance) up to frequencies in the tens of MHz range. However, at higher frequencies, the impedance is primarily influenced by the on-chip PDN, see Fig. 2(b). The primary reason behind such behavior is the existing parasitic impedance of various PCB components, which will be explained in the following subsection.

B. The Impact of Component's Parasitic

The real-world PCB components contain parasitics making them behave differently compared to their ideal models. For instance, in addition to the capacitve behavior, capacitors manifest resistive and inductive characteristics as well, commonly referred to as Equivalent Series Resistance (ESR) and Equivalent Series Inductance (ESL), respectively. The

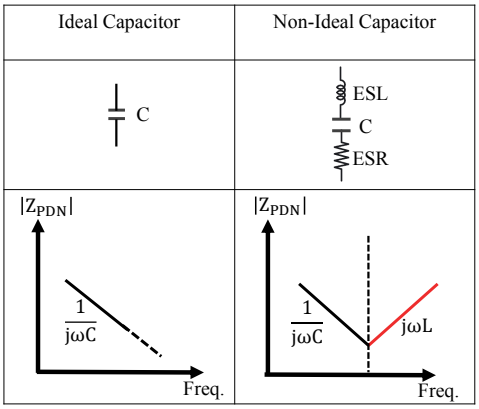


Fig. 3. Impedance profile of an ideal and non-ideal capacitor in log scale.

introduction of components, such as non-ideal capacitors as illustrated in Fig. 3, is modeled by incorporating an RLC branch into the circuit model and introduces a resonance frequency into system. The resonance frequency of such RLC circuit can be obtained as follows.

$$f = \frac{1}{2\pi\sqrt{LC}} \tag{1}$$

Eq. 1 demonstrates that as either capacitance or inductance increases, the resonance frequency decreases. By adding a component to the PDN, the equivalent capacitance and inductance of the system changes, and consequently, the resonance frequency also shifts in the frequency domain. Accurate estimation of parasitic impedance is essential in our study, as we are analyzing the impact of tampering (e.g., addition or removal of components). If the approximate values of parasitic are not known, the simulated signatures could differ significantly from the measured signatures.

C. Impedance Characterization using Scattering Parameters

To evaluate the PDN's impedance, we utilize S-parameters (Scattering). Given the complex nature of an electronic board, it can be modeled as either a single-port or multi-port network. The transmitted and reflected power of signals entering and leaving the PDN at various frequencies is measured using a Vector Network Analyzer (VNA). Using the VNA, we inject sine waves into the PCB for each frequency sample and capture the signal's reflective response from the PDN. These sine waves in frequency domain analysis are characterized by their frequency, amplitude, and phase. Our study focuses on leveraging the reflected amplitude response ($|S_{11}|$), obtainable directly from the VNA, see Fig. 4. The relationship between the impedance of the device under test (DUT), represented as Z_{DUT}, and the reflection coefficient S_{11}, is expressed in Eq. 2:

$$Z_{DUT} = Z_0 \frac{1 + S_{11}}{1 - S_{11}} \tag{2}$$

where Z_0 is the characteristic impedance of the connecting cables to the VNA. The relationship expressed in Eq. 2 clarifies

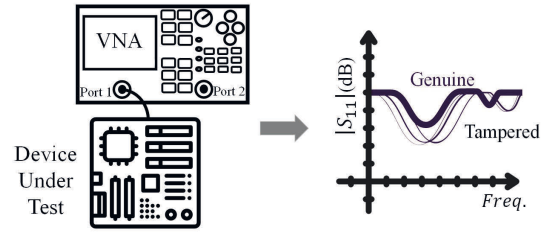
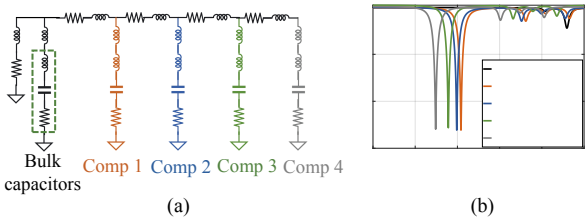


Fig. 4. Hardware signature extraction based on reflection method.



(a) (b)

Fig. 5. (a) PDN circuit model of the PCB. (b) The simulated $|S_{11}|$ displays the impedance contribution of each component. In each step, ranging from 1 to 4, one component is added.

that the reflection coefficient provides valuable insights into the impedance characteristics of the system. Fig. 5 illustrates the impact of tampering with the PCB. In this case, the addition of capacitors to the PDN causes change in the PDN's impedance, and thus, it affects the $|S_{11}|$.

III. Methodology

A. Threat Model

In our threat model, we make the following assumptions. Firstly, we assume that the attacker can make physical alterations to the PCB at any point in its life cycle, encompassing fabrication, integration, distribution, and repair stages. The adversary also possesses the capability to perform various modifications at the PCB level. These PCB modifications could involve changing the substrate material or drilling into it, as well as adding, removing, modifying, or replacing components of the PCB. The goal of such tampering could be creating counterfeit or cloned versions of legitimate products, introducing malicious functionality, or embedding backdoors. Secondly, we assume that the verifier has only access to the design files of the PCB (e.g., PCB netlist, PCB layout, bill of material, and IC package specifications) and the ability to obtain the impedance signature of the PCB's PDN through simulation. Moreover, the verifier is given a population of genuine and tampered boards for verification, and hence, she can cluster the samples by comparing their signatures to the simulated golden signature and setting a threshold. The verification does not require control over specific parts of the supply chain.

B. Dynamic Time Warping (DTW)

Due to existing manufacturing process variation, the parasitic impedance of identical PCB's components varies. As discussed in the Sect. II-B, these variations lead to shifts in resonance frequencies and the amplitude of the entire S-parameter profile. Naturally, such shifts in the signature profiles of identical samples makes the comparison of genuine signatures (generated from simulation and measurement) challenging and could lead to false alarms. While these shifts exist, the overall pattern of the signatures over frequency remains similar. To measure such similarities and reduce the impact of such consistent shifts, we deploy Dynamic Time Warping (DTW), which is a similarity measure between time series [14], [15].

We consider ${\mathcal{S}_{11}}^{Sim}$ and ${\mathcal{S}_{11}}^{Meas}$ as *amplitude* vectors of simulated and measured S_{11} parameters, respectively. We define the DTW distance for ${\mathcal{S}_{11}}^{Sim}$ and ${\mathcal{S}_{11}}^{Meas}$ as follows,

$$DTW_q(\mathcal{S}_{11}^{Sim}, \mathcal{S}_{11}^{Meas}) = \min_{\delta \in A(\mathcal{S}_{11}^{Sim}, \mathcal{S}_{11}^{Meas})} \Big(\sum_{i,j \in \delta} d(\mathcal{S}_{11}^{Sim}, \mathcal{S}_{11}^{Meas})^q\Big)^{\frac{1}{q}} \quad (3)$$

where, an alignment path δ is a sequence of index pairs and $A(\mathcal{S}_{11}^{Gen}, \mathcal{S}_{11}^{Tamp})$ is the set of all admissible paths.

C. Golden-free Tamper Detection Method

This section discusses the overall framework for golden-free PCB verification. The principal basis of the proposed golden-free detection methodology is to rely on the simulated traces of $|S_{11}|$ as a golden signature and compare it with the measured traces collected from PCBs under test. In the first phase, a trusted PCB design file is employed to generate the golden sample signature. The process involves importing and extracting the electrical characteristics of the PCB from its design file, followed by exporting the S-parameter signature of the PCB using simulation software. The PCB's circuit is first segmented into multiple PDNs to reduce its complexity. Next, the verifier defines ports associated with each PDN, simulates the circuit, and extracts the $|S_{11}|$ parameter.

In the second phase, the verifier performs $|S_{11}|$ measurements using a VNA on the PDNs of a population of PCB samples. Afterward, the verifier will apply the DTW metric on the generated simulated golden signature and each of collected measured signatures. If the DTW score is below a predefined threshold, the test will be passed, and the sample is verified as genuine. Otherwise, the test fails and the sample will be considered dissimilar. The verifier should set the threshold during the design phase of the PCB. Depending on the applications in which the PCB will be deployed, the verifier can set various tolerances for components' parasitic. The flowchart in Fig. 6 outlines the major steps that the verifier must undertake during the test phase. Note that the dissimilarity of the samples does not necessarily point to a tamper event, and finding the root-cause of the signature deviation requires further investigations.

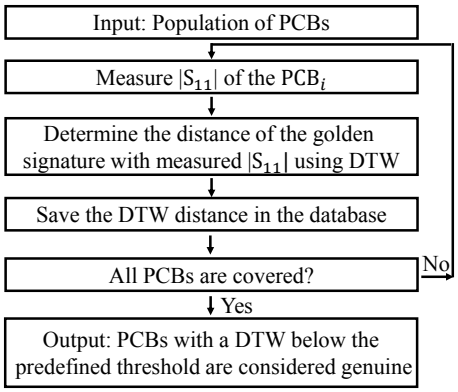


Fig. 6. The main steps of the proposed verification method.

IV. Experimental Setup

A. Device Under Test (DUT)

For our experimental setup, we utilized an in-house designed PCB shown in Fig. 7. This board contains three distinct and isolated PDNs named 1V8, 3V3 and 5V. The board, made of FR4 epoxy substrate, consists of 242 components, including capacitors, resistors, ICs, LEDs, SMA ports, headers, traces, and vias. In this paper, we perform our measurements on the 1V8 PDN and systematically add the components associated with this PDN as shown in Table. 1. The J5 port, which is connected to the VNA via an SMA connector and gives us direct access to the PDN under test.

B. Simulation Setup

We used ANSYS SIwave 2023 R2, which is a powerful 2.5D electromagnetic (EM) simulation tool that combines the finite element method (FEM) and the method of moments (MOM) [16]. It utilizes a hybrid solver with a 2-D triangular mesh, enabling it to handle intricate PCB layouts effectively. The tool is capable of solving complex layouts, including traces, planes, and through-hole vias, as well as accounting for the effects of metal thickness and dielectric thickness [17]. To efficiently utilize computing resources and achieve accurate results, we employ dynamic linking of ANSYS SIwave and HFSS for comprehensive system-level electromagnetic interference (EMI) analysis.

C. Measurement Setup

We employed the Mini-circuits eVNA-63+ as our Vector Network Analyzer (VNA), which offers a wide operating bandwidth between 300 kHz to 6 GHz. To establish a direct connection between the VNA and the DUT, we utilized the CBL-2FT-SMNM+ cable, which is a shielded precision test cables. These cables feature male SMA connectors on the side of the DUT, thereby facilitating a seamless connection without the requirement for additional adaptors. For precise calibration, we followed the industry-standard Open-Short-Load (OSL) calibration technique. Calibration was performed until the SMA connection plane on the board, ensuring accurate and reliable measurements for one-port reflection and impedance analysis.

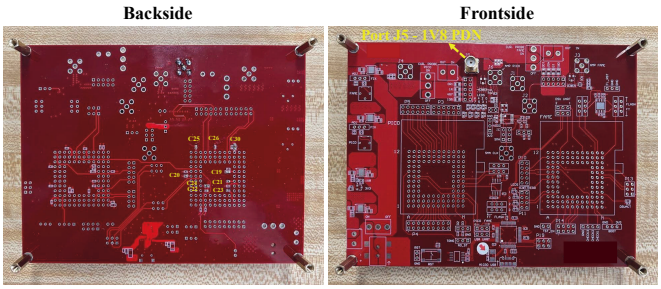


Fig. 7. Front- and backside of the board under test depicting the circuitry and port J5 of the PDN under test (1V8). Capacitors integrated into the PDN are highlighted.

Table 1. Capacitors utilized in the experiments: all capacitors are connected to the 1V8 PDN, with the exception of C_{30} which is connected to 3V3 PDN, C_{19}= C_{20}= C_{30}=10 uF, C_{21}=C_{22}=C_{23}=C_{24}=C_{25}=C_{26}= 0.1 uF.

Exp.	Caps								
2 Caps	c_{19}	c_{20}							
3 Caps	c_{19}	c_{20}	c_{30}						
5 Caps	c_{19}	c_{20}	c_{30}	c_{21}	c_{22}				
7 Caps	c_{19}	c_{20}	c_{30}	c_{21}	c_{22}	c_{23}	c_{24}		
9 Caps	c_{19}	c_{20}	c_{30}	c_{21}	c_{22}	c_{23}	c_{24}	c_{25}	c_{26}

V. Results

A. Emulating Tamper Events

To emulate PCB tampering, various decoupling capacitors with different capacitances are added to the board. Capacitors are chosen primarily due to three reasons. First, they play a major role in delivering power to the integrated circuits (ICs) on the PCB. Second, according to the ERAI [18], the capacitors are the most counterfeiting products in the market. Third, adding, removing or replacing any components on the PCB, e.g., implanting a spy chip, will cause changes in overall capacitance of the PDN, and therefore, such attacks type can be emulated by capacitors.

The process commenced with a bare board configuration, where no components were present. The bare board layout was imported into the simulation software, enabling us to simulate the PCB and obtain the $|S_{11}|$ signature. In Fig. 8, we can observe the simulated and measured $|S_{11}|$ signature of the bare board, which exhibit good agreement. However, there is a 17.2 MHz shift between them. This shift is solely due to the inevitable impurities in the substrate, as there are no components on the board. Subsequently, at each stage, we added one or two capacitors to the PCB's PDN as shown in Table. 1.

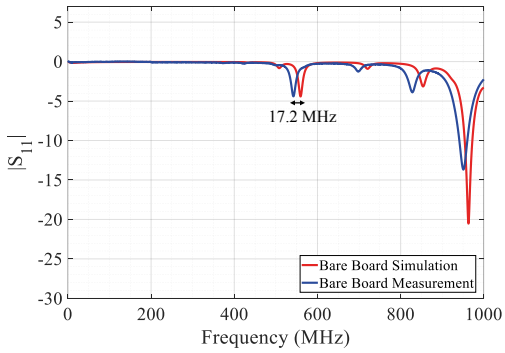


Fig. 8. Simulated signature of $|S_{11}|$ extracted from ANSYS SIwave and measured $|S_{11}|$ of the bare board showing similar patterns with a shift in resonance frequencies.

B. Identifying the Desired Frequency Band

In our investigations, we acknowledge that different Trojans and tamper events exhibit detectable characteristics at different frequency bands, which vary depending on their size and area overhead. Specifically, smaller tampers, such as those at the IC level, tend to be detectable at very high frequencies (GHz bands) [19]. However, our focus lies in the detection of attacks at the board level, indicating our interest in the MHz bandwidth. The frequency bands of interest is the range in which the DTW analysis is applied to the results, allowing us to observe the impact of the components on the board. The resonance frequency of the circuit is highly sensitive to the addition or removal of components. Therefore, we chose the bandwidth such that the resonance frequency is at the center. For high precision, we selected a range that spans 10% around the lowest resonance frequency obtained from simulation, enabling us to specifically observe the effects of component addition or removal. For instance, when two capacitors are added to the circuit, the resonance frequency occurs at 234 MHz. Consequently, the DTW is applied to the frequency range of 222 MHz to 246 MHz. It is important to mention that for the bare board experiment, due to the absence of components on the board, we choose for a wide band comparison. This implies that we compute the DTW distance of the second column from Table. 2, spanning a bandwidth of 1 MHz to 1 GHz. To enhance the SNR and improve detection confidence while mitigating the impact of environmental noise and measurement uncertainties, we performed averaging on multiple measurements.

C. Assessment of the Golden-free Tamper Detection Method

Our methodology is validated through measurements performed on the board mentioned in Sect. IV-A, where we employed a VNA channel probe connected to port J5 to accurately measure the $|S_{11}|$ of the PCB's 1.8V PDN. Notably, no additional physical modifications were made to the system. Incorporating the approximate values of parasitic inductance and resistance in simulation tools enables more accurate predictions of the impedance behavior. In most cases, obtaining the exact values is challenging.

Table 2. Case Study 1: DTW distances using approximate values of ESR and ESL showing the impact of adding or removing components. Diagonal cell values represent lower DTW distances, illustrating golden detection with no components added or removed, (S) indicates simulation, (M) indicates measurement.

Reference ⇒ *Test* ⇓	Bare Board (S)	2 Caps (S)	3 Caps (S)	5 Caps (S)	7 Caps (S)	9 Caps (S)
Bare Board (M)	**189**	1247	1250	1316	1295	1264
2 Caps (M)	1291	**23.8**	33	1316	1270	1239
3 Caps (M)	1283	41.8	**30**	1329	1286	1261
5 Caps (M)	1308	1224	1227	**21.3**	715	1211
7 Caps (M)	1305	1232	1235	60.2	**170**	1210
9 Caps (M)	1205	1247	1251	1331	1263	**212**

Even the component vendors may not possess precise knowledge of these values. To demonstrate the effectiveness of our approach, we performed extensive measurements on several proof-of-concept configurations. The method is comprehensively discussed through two case studies.

1) Case Study 1: Addition or Removal of Components

In this case study, we assess the feasibility of detecting addition or removal of a component from the PCB. To emulate the tampering, we added multiple capacitors in various trials to the board. To generate the simulated golden signature for each trial, the verifier sets the expected values for parasitic impedance of the PCB's component. As shown in Table. 2, if we consider the first row as the reference signature obtained from the simulation data and the first column as the measured signatures corresponding to each of the experiments, the values in the diagonal cells represent the DTW distances between the simulation and measurement data of each experiment. As it can be observed the simulated and measured $|S_{11}|$ signatures of identical configurations exhibit lower DTW distances compared to cases, where the simulated configuration differs from the physical sample configuration.

Table 3. Case Study 2: DTW distances using deviating values of ESL and ESR to emulate the replacement genuine parts with counterfeit ones showing significantly larger DTW distances than the diagonal cell values in the Table. 2.

Sim vs Meas	2 Caps	3 Caps	5 Caps	7 Caps	9 Caps
DTW Distances	1100	1095	1205	1127	856

2) Case Study 2: Replacing Parts with Counterfeit Ones

In this case study, we assess the feasibility of detecting a component that has been replaced with a counterfeit part. The assumption here is that the counterfeit part has a significant parasitic impedance deviation. Since we did not have access to counterfeit components, we edited instead the ESL and ESR values in our simulations. We chose deviations in order of 10 and 1.3 for our ESL and ESR values. Such factors were obtained by averaging the existing ESL and ESR values of similar components from various vendors mentioned in their datasheets. As it can be observed in Table. 3, the measured and simulated signatures exhibit substantial disparities to the

point where the DTW distance between them becomes very large compared to the distances of the previous case study, where no components were added or removed. This confirms that replacing components with fake parts could be detected if the fake parts have a different parasitic behavior.

3) Accuracy of the Proposed Method

The case studies offers valuable insights into the method's sensitivity to the parasitic values. To gain a deeper insight into the method, the verifier can introduce a margin factor, denoted as η. This factor illustrates the difference in the DTW distance value between an untampered board and the smallest DTW distance observed in all experiments. Ideally, this margin should be zero. However, manufacturing process variations lead to a non-zero value, and poorly selected ESL and ESR values further increase η. The smaller the margin factor, the better our method becomes at detecting minor tamper events, enhancing its effectiveness. Consequently, the sufficiency of the ESL and ESR choice determines the types of tamper events we aim to detect. Detecting more sophisticated tampering requires greater accuracy in the ESL and ESR values.

D. Validation of the Tamper Detection Across Different PDNs

In this section, we discuss the robustness of the proposed method in detecting tampering events connected to other adjacent PDNs. When electric currents are directed through one PDN, magnetic fields are generated, which have the potential to induce voltages within neighboring PDNs due to the principle of mutual inductance. The mutual coupling between PDNs allows us to detect alterations in the impedance within one PDN by leveraging another PDN. This becomes especially valuable in situations where access is typically limited to a single PDN, yet we maintain the ability to identify tampers associated with other PDNs. In our experimental investigation, the PDN under test is the 1V8 PDN. In the third experiment in Sect.V-A, we added the C_{30} connected to the 3V3 PDN to the board. The introduction of C_{30} to the circuit brought about changes in the $|S_{11}|$ parameter, consequently affecting the DTW distances as well. The obtained results are presented in Table. 2, where it can be observed that the DTW distances between the second and third experiments differ. Although the observed difference is not as pronounced as the values associated with components directly connected to the PDN under test, the changes in the DTW distances remain detectable.

VI. Conclusion

In this paper, we explored the feasibility of using simulated golden signatures as a substitute for the physical ones. Our results validate the efficacy of the proposed detection method, which relies on configuring the expected parasitic values during simulation. Given approximated values for the parasitic impedance of components on the PCB, replacing the physical golden sample with its simulated signature is feasible. Moreover, the proposed approach not only detects potential attacks on specific PDNs of the PCB but also extends its capabilities to identify attacks on other PDNs, proving particularly valuable when access to all PDNs is unavailable. We believe this work lays the foundation for improving the proposed method for other real-world scenarios, such as the golden-free verification of much larger systems with hundreds of components, detection of combined tampering and counterfeiting attacks using more advanced machine learning algorithms, and defining reliable thresholds based on the parasitic values.

Acknowledgment

This effort was sponsored in part by NSF under the grant number 2338069 and in part by Electric Power Research Institute (EPRI). We also gratefully thank William L. Appleyard at Worcester Polytechnic Institute for components soldering and PCB preparation.

References

[1] J. Robertson and M. Riley, "The Big Hack: How China used a Tiny Chip to Infiltrate US Companies," *Bloomberg Businessweek*, vol. 4, 2018.

[2] D. Janushkevich, "The Fake Cisco: Hunting for Backdoors in Counterfeit Cisco Devices," *F-Secure Consulting, Hardware Security Team*, 2020.

[3] U. J. Botero, R. Wilson, H. Lu, M. T. Rahman, M. A. Mallaiyan, F. Ganji, N. Asadizanjani, M. M. Tehranipoor, D. L. Woodard, and D. Forte, "Hardware trust and assurance through reverse engineering: A tutorial and outlook from image analysis and machine learning perspectives," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 17, no. 4, pp. 1–53, 2021.

[4] V. Chaudhary, I. R. Dave, and K. P. Upla, "Automatic visual inspection of printed circuit board for defect detection and classification," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 732–737, IEEE, 2017.

[5] G. Piliposyan and S. Khursheed, "PCB hardware Trojan run-time detection through machine learning," *IEEE Transactions on Computers*, 2022.

[6] T. Mosavirik, F. Ganji, P. Schaumont, and S. Tajik, "Scatterverif: Verification of electronic boards using reflection response of power distribution network," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 18, no. 4, pp. 1–24, 2022.

[7] F. T. Werner, M. Prvulovic, and A. Zajić, "Detection of recycled ICs using backscattering side-channel analysis," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 9, pp. 1244–1255, 2022.

[8] H. Zhu, H. Shan, D. Sullivan, X. Guo, Y. Jin, and X. Zhang, "PDNPulse: sensing PCB anomaly with the intrinsic power delivery network," *IEEE Transactions on Information Forensics and Security*, 2023.

[9] M. S. Safa, T. Mosavirik, and S. Tajik, "Counterfeit chip detection using scattering parameter analysis," in *2023 26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, IEEE, 2023.

[10] T. Mosavirik, P. Schaumont, and S. Tajik, "Impedanceverif: On-chip impedance sensing for system-level tampering detection," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 301–325, 2023.

[11] A. Bhattacharyay, P. Chakraborty, J. Cruz, and S. Bhunia, "VIPR-PCB: a machine learning based golden-free PCB assurance framework," in *Proceedings of the 59th ACM/IEEE Design Automation Conference*, pp. 793–798, 2022.

[12] A. B. Chowdhury, A. Mahapatra, Y. Liu, P. Krishnamurthy, F. Khorrami, and R. Karri, "A golden-free approach to detect Trojans in COTS multi-PCB systems," *IEEE Micro*, 2023.

[13] P. Krishnamurthy, V. R. Surabhi, H. Pearce, R. Karri, and F. Khorrami, "Multi-modal side channel data driven golden-free detection of software and firmware Trojans," *IEEE Transactions on Dependable and Secure Computing*, 2022.
[14] T. K. Vintsyuk, "Speech discrimination by dynamic programming," *Cybernetics*, vol. 4, no. 1, pp. 52–57, 1968.
[15] H. Sakoe and S. Chiba, "Dynamic programming algorithm optimization for spoken word recognition," *IEEE transactions on acoustics, speech, and signal processing*, vol. 26, no. 1, pp. 43–49, 1978.
[16] ANSYS, Inc., "ANSYS SIwave 2023 R2." http://www.ansys.com, 2023.
[17] B. Wei and S. G. P. Jr, "New integrated workflow for EMI simulation," *APEMC 2015*.
[18] Akhoundov, Damir, "2019 ERAI Reported Parts Statistics," *ERAI Blog*, 2020.
[19] T. Mosavirik, S. K. Monfared, M. S. Safa, and S. Tajik, "Silicon echoes: Non-invasive Trojan and tamper detection using frequency-selective impedance analysis," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 238–261, 2023.