PDNPulse: Sensing PCB Anomaly With the Intrinsic Power Delivery Network

Huifeng Zhu, *Graduate Student Member, IEEE*, Haoqi Shan, Dean Sullivan, Xiaolong Guo, *Member, IEEE*, Yier Jin, and Xuan Zhang, *Senior Member, IEEE*

***Abstract*— The ubiquitous presence of printed circuit boards (PCBs) in modern electronic systems and embedded devices makes their integrity a top security concern. To take advantage of the economies of scale, today's PCB design and manufacturing are often performed by suppliers around the globe, exposing them to many security vulnerabilities along the segmented PCB supply chain. Moreover, the increasing complexity of the PCB designs also leaves ample room for numerous sneaky board-level attacks to be implemented throughout each stage of a PCB's lifetime, threatening many electronic devices. In this paper, we propose *PDNPulse*, a power delivery network (PDN) based PCB anomaly detection framework that can identify a wide spectrum of board-level malicious modifications. PDNPulse leverages the fact that the PDN's characteristics are inevitably affected by modifications to the PCB. By detecting changes to the PDN impedance profile against the golden model and using the Frechet distance-based anomaly detection algorithms, PDNPulse can robustly and successfully discern malicious modifications across the system. Using PDNPulse, we conduct extensive experiments on seven commercial-off-the-shelf PCBs, covering different design scales, different threat models, and seven different anomaly types. The results confirm that PDNPulse creates an effective security asymmetry between attack and defense.**

***Index Terms*— Printed circuits, power distribution networks, impedance, anomaly detection, cyberattack.**

I. Introduction

MODERN consumer electronics brands depend on a continually growing global supply chain. The number of suppliers for a large smartphone manufacturer such as Samsung reaches into the several thousand and stretches across roughly 70 countries at more than 200 different locations [45]. And while it behooves each company to enlist trustworthy vendors, the sheer number of them and scope of global operations precludes thoroughly vetting everyone involved. Trustworthy vendors are paramount for the development of reliable and robust products. Nowhere is this more important than in critical infrastructures such as power grids or water treatment facilities, in privacy compliance relating to healthcare and financial institutions, or in national defense.

Issues in the supply chain are inherently pervasive due to their scope and come with profound consequences. Direct losses and risk from counterfeiting in the global supply chain are estimated to cost billions of dollars annually [41]. The United States alone, which outspends the next 11 richest countries combined on defense, allocates roughly 40% of its military budget on electronics [38]. A fact that has prompted recent legislation requiring both the Pentagon and Department of Defense to take steps to guarantee the security of its supply chain [48]. The issue extends beyond even reliability, with recent news of maliciously implanted microchips in Supermicro server motherboard that allowed the successful infiltration of nearly 30 companies [44].

Despite their ubiquity, detecting both counterfeiting and PCB Trojans remains an open problem. This is, in part, due to the complexity of the global supply chain market itself. Accounting for every potential point-of-failure or susceptibility is impractical. Efforts have been made in academia to classify state-of-the-art threats and defenses [23]. Still, the work is perennially ongoing and largely unsystematic because of different attack vectors that prevent generalization. Although prior research has been presented on detecting counterfeits, and several robust solutions exist that focus on anomaly detection [24] or authentication [40], unfortunately, these solutions are often inherently incapable of detecting PCB Trojans. For example, embedded signature-based authentication that uses the delay of the JTAG scan chain across the PCB [40] can only protect complex logic ICs with the JTAG feature, and is insensitive to PCB Trojans that avoid impacting the JTAG scan chain. Several previous works [8], [50] propose using changes in radio wave propagation within an enclosed system to detect PCB in-field tampering events. However, these methods are not suitable for detecting supply chain attacks, such as Trojans or counterfeits, as they require a metal casing around the system for detection.

To address threats in the PCB supply chain, this paper presents *PDNPulse*, a novel board-level anomaly detection framework that can identify PCB hardware Trojans, on-board counterfeit chips/components, and counterfeit PCBs. PDNPulse leverages the inherent sensitivity of the on-board power delivery network (PDN) to assure that a PCB is free from anomalies by comparing its PDN with the one of a

Manuscript received 24 August 2022; revised 26 January 2023 and 25 April 2023; accepted 4 June 2023. Date of publication 15 June 2023; date of current version 21 June 2023. This work was supported in part by the Defense Advanced Research Projects Agency (DARPA) and NSF Computer and Network Systems (CNS) under Grant 1739643. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Ulrich Rührmair. *(Corresponding author: Huifeng Zhu.)*

Huifeng Zhu and Xuan Zhang are with the Department of Electrical and System Engineering, Washington University in St. Louis, St. Louis, MO 63130 USA (e-mail: zhuhuifeng@wustl.edu).

Haoqi Shan and Yier Jin are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA.

Dean Sullivan is with the Department of Electrical and Computer Engineering, University of New Hampshire, Durham, NH 03824 USA.

Xiaolong Guo is with the Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS 66506 USA.

Digital Object Identifier 10.1109/TIFS.2023.3285490

genuine PCB. The framework relies fundamentally on the uniqueness of PDN characteristics and profiling PDN in the frequency domain. PDNPulse can monitor a range of subtle malicious changes in the PDN impedance profile, making it ideal for accurately identifying board-level anomalies at multiple stages in the supply chain and across different systems. This capability rests on the fact that the PDN is interconnected with all subsystems on the board to provide power throughout its lifetime. In our analysis, we have found that PCB anomalies tend to inevitably affect the PDN and are therefore detectable by PDNPulse.

A PDN in a complex PCB design often consists of subnets from several different voltage domains, with voltage regulator modules (VRMs) in each domain to supply the stable voltages, power traces from the VRMs to connect the chip pins, on-chip power grids to distribute power locally on the die, and decoupling capacitors to mitigate the voltage fluctuations at various PDN stages [10]. All PDN components are connected across multiple levels (e.g., chip, package, board) of the system and form a tree structure to create multiple voltage domains, each with its own VRMs to drive the local supply voltages [63]. In modern electronic systems, the PDN requires low impedance to provide an adequate supply noise margin, a requirement that makes it sensitive to minute modifications. Hence, even minuscule changes to the PCB can affect the PDN characteristics that are detectable by accurate PDN measurements. On the other hand, the PDN is robust to variations in the PCB manufacturing process, which are distinguishable from malicious changes when profiled in the frequency domain.

To the best of our knowledge, PDNPulse is the first *general* board-level anomaly detection method that can be used for monitoring *full-system*, *cross-layer* behavior. Several recent approaches [36], [55] have proposed PDN impedance-based detection, but do not achieve general, full-system, or cross-layer anomaly detection. Nishizawa et al., [36] models the PDN as a resistor and capacitor in parallel, and measure the PDN capacitance by injecting a single-frequency sine wave and measuring the corresponding amplitude of the current. They demonstrate detection of an anomalous capacitor as low as $0.1\mu F$. Wang et al., [55] indirectly measure the PDN impedance at resonant frequency to detect counterfeit PCBs by proposing a ring oscillator (RO) array embedded in integrated circuit (IC). They leverage the fact that when the IC is clocked at the resonant frequency of the PCB's PDN (e.g., red dot in Fig. 1(c)), the observed supply voltage fluctuations are mainly affected by the PCB PDN impedance. This is measurable as changes in the oscillation frequency of the embedded RO and allows anomaly detection by comparison with a trusted database. This solution further allows authentication by clocking the IC at non-resonant frequencies so that the embedded RO acts as a physically unclonable function (PUF).

PDNPulse, on the other hand, analyzes the PDN using a complex model that includes the parasitics of each on-board component (see Fig. 3(c)) using the complete PDN impedance profile in the frequency domain. As a result, we demonstrate significantly improved detection sensitivity of anomalously inserted capacitance as low as $1.8fF$.[1] Both [36] and [55] are currently only capable of detecting anomalies in one voltage domain using one (or two) frequency points. Anomalies in other voltage domains or placed far from the measured ports in those defenses can possibly evade detection due to isolation effects of the VRMs and decoupling capacitors, or motivated attackers that shift the affected frequency band of their malicious insertion to bypass detection. To solve this challenge, we extend the traditional PDN analysis [22] by using multi-domain multi-port detection and measuring both self- and transfer PDN impedance. What is more, based on the designed probe, PDNPulse does not require any embedded, or otherwise, hardware modifications. This feature allows flexibility of detection within varying phases of the supply chain, in the field, and on legacy systems without an existing defense. In addition, detection in [36] and [55] fails to recognize that in frequency-domain PDN analysis, malicious modifications with minimal parasitics are still observable as shifted PDN profiles with discernible magnitudes [30] at high frequencies. This property facilitates PDNPulse's detection sensitivity and allows us to employ a pattern-based method using Frechet distance, decreasing the possibility of evasion and increasing the robustness to PCB process variations.

In general, we demonstrate that PDNPulse provides broad assurance for commercial-off-the-shelf (COTS) electronics across all design layers in the supply chain. The contributions of this work are summarized as follows:

- We coalesce different board-level attack effects using PDN impedance profiling and multi-port, multi-domain PDN measurement methodologies for systematic detection.
- We propose *PDNPulse*, the first general board-level attack detection framework used for monitoring full-system, cross-layer behavior. We present the workflow of PDNPulse, providing comprehensive setup and procedural guidance. We also design a custom probe for PDNPulse that achieves good trade-offs among accuracy, error, and ease-of-use.
- We develop a modified Frechet distance to evaluate the minute differences between the PDNs on two PCBs, which also serves as the security metric. Based on our approach, we develop robust algorithms for both anomaly detection and board classification.
- We present extensive experimental results and analysis of PDNPulse on a wide-range of custom and COTS PCBs. In so doing, we cover different design scales and attack types that demonstrably validate the sensitivity and robustness of PDNPulse for the majority of board-level attacks.

II. Background

A. Power Delivery Network (PDN)

The PDN must provide a stable supply voltage and sufficient power to other on-board modules. In a complex PCB

[1]The value is an order-of-magnitude smaller than the parasitic of the 3pin SOT-23 package, one of the smallest chip package footprints (2.6mm×2.9mm).

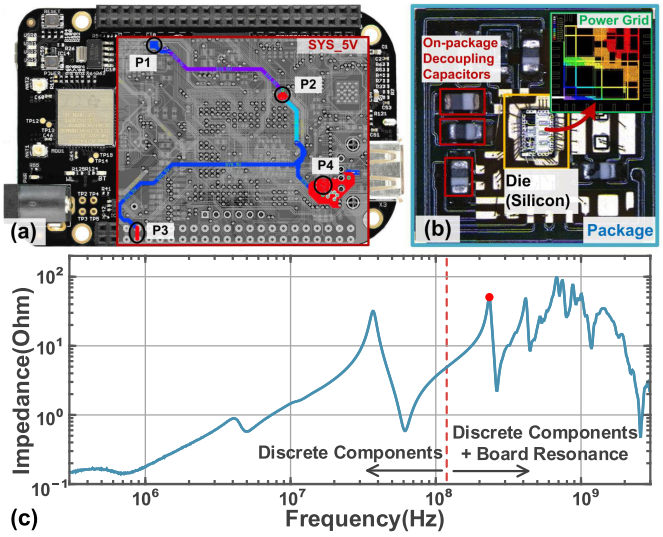

Fig. 1. (a) One voltage domain (SYS_5V) of an example system [3], with the power supply net highlighted. P1-P4 specify accessible probe points for measuring this domain's PDN. (b) A chip-level PDN, with in-package decoupling capacitors and die-level power grid highlighted. (c) An example PDN impedance profile (magnitude of Z_{11}) of a custom experimental board.

design, chips/components have different power distribution requirements for reliable operation, such as supply voltage levels, maximum load currents, and voltage noise margins. Thus, the PDN is composed of VRMs that form a tree structure to create multiple voltage domains. Fig. 1(a) shows one of 17 voltage domains of a BeagleBone single board computer [3], highlighting its power supply net.

Different voltage domains have different power supply specifications and cover different chips/components on the PCB. Each voltage domain has its own VRM to convert the power supply from the upper-node voltage domain and drive the local supply voltage to the chips. The VRM also isolates the two voltage domains since one of its primary functions is to prevent the voltage fluctuations of one domain from propagating to the other domain. When powered off, the VRM is an open circuit, thereby disconnecting the two domains. Between the hierarchical VRMs and chips is the board-level passive distribution network, containing PCB power wire lines, power planes, and on-board discrete decoupling capacitors. Given a voltage domain, probes can be attached to the accessible points (e.g., P1-P4 of Fig. 1(a)) of the power supply net to detect disturbances. Measurements taken at these points can isolate the impedance profile of, for example, SYS_5V, from the 17 possible voltage domains. At the chip level, Fig. 1(b) shows both power grids to distribute power locally on the die and decoupling capacitors at the die or package level. All PDN components are connected across multiple levels (i.e., die, package, and board) of the system and form an infrastructure that can sense disturbance within the system.

B. PDN Impedance Profile

The impedance profile (also known as **Z-parameters**) of a PDN in the frequency domain is widely used to evaluate its performance, which are represented as a symmetric matrix.

$$Z_{PDN}(f) = \begin{bmatrix} Z_{11} & Z_{12} & \cdots & Z_{1n} \\ Z_{21} & Z_{22} & \cdots & Z_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ Z_{n1} & Z_{n2} & \cdots & Z_{nn} \end{bmatrix} \quad (1)$$

where n is the number of measured ports, diagonal elements Z_{xx} are the self-impedance seen from each measurement port, and non-diagonal elements Z_{xy} are the transfer impedance between two ports. For traditional PDN analysis, only self-impedance is of interest since it can represent the quality of power supplied to a chip. While for PDN-based anomaly detection, we should also focus on the transfer impedance since on-board capacitors behave like barriers, separating one voltage domain into multiple subdomains. Self-impedance can precisely characterize the PDN in one subdomain, while transfer impedance can sense across multiple subdomains at the cost of higher noise. By combining self-impedance and transfer impedance, we can increase the overall detection accuracy and sensitivity.

Fig. 1(c) is an example profile of PDN self-impedance (Z_{11}). Both self- and transfer impedance profiles can be roughly divided into two parts: 1) the low-frequency part, which is due to the electrical characteristics of the PDN circuit (specifically, discrete components), and 2) the high-frequency part, which is mainly due to the electromagnetic resonance formed by the PCB cavity between the power planes (i.e., board resonance). Both parts of the profile help reveal the effects introduced by PCB anomalies concerning circuit-level changes and board resonance changes, respectively. Combining both the circuit level and board resonance information, the impedance profile captures minute changes in the PCB design, even if those changes do not directly impact the operability of the PDN circuit itself. Throughout this paper, both low-frequency and high-frequency information are used together to detect PCB modifications.

III. Threat Model

A. Attack Surface

Attackers can perform *physical modifications* during any stage of the PCB's life cycle, such as design, fabrication, integration, distribution, and repair. They have full access to the PCBs and their design details, such as the schematic, layout, and bill-of-material (BoM). The intermediate parties or legitimate end-users can use PDNPulse to detect anomalies on populated (i.e., with all components assembled) PCBs and to verify the trustworthiness along the supply chain.

B. Attackers' Motivation

Attackers are dishonest opportunists driven by financial or security incentives. Their goal is to gain either profit or valuable information. Practical PCB threats need to be stealthy (i.e., no blatant violation of design rules or functional failure) and meaningful (i.e., no frivolous modifications without security or financial gains). Thus, attacks that uncontrollably compromise the basic functionality (e.g., short circuits) or have insignificant security impacts (e.g., moving a single

via) are out of the scope of our work. Attackers that can undo the changes (e.g., remove the malicious plug-in before PDNPulse's detection) are also not in scope. Further, implementing Trojans by exclusively modifying a chips' internal structure (i.e., chip-level Trojans inserted by attackers in chip supply chains) are not considered.

C. Attack Vectors

Attackers can *maliciously yet meaningfully add, remove, alter, and replace arbitrary electrical components of the PCB.* Specifically, attackers can implant anomalies by inserting Trojan circuits or performing counterfeit (including low-quality and recycled) replacements. We show that PDNPulse can effectively detect the majority of practical board-level attacks, as summarized below:

leftmargin=*,topsep=0px,partopsep=0px

- **PCB Trojans (Sec.V-A).** Trojan circuits create a backdoor for attackers and can be utilized to launch attacks compromising security assurance. Known practical PCB Trojans [23], [64] fall into two main categories:

  Triggerable Trojans (Sec.V-A.1 and V-A.2). At the board level, Triggerable Trojans are based on small-package chips. For example, chips that integrate numerous logic gates are implanted to be highly functional yet sneaky. To achieve advanced attacks with complex trigger patterns or payload functions, processor chips (e.g., microcontrollers (MCU)) are commonly adopted [19].

  Always-on Trojans (Sec.V-A.1). One notable attack is to steal sensitive information (e.g., secret keys) on the chips by inserting sampling resistors in the power rails that can perform side-channel analysis attacks [15], [56].

- **Chip/Component Counterfeits (Sec.V-B).** The security of such components are unverified. Thus they can be leveraged by attackers to launch attacks (e.g., inject faults when running code). In this paper, we focus on two main types of on-board counterfeits [20]:

  Counterfeit Chips (Sec.V-B.1). We refer to chips as those with programmable functions, such as MCUs, microprocessors, and field programmable gate arrays (FPGAs).

  Counterfeit Components (Sec.V-B.2). Other chips are of this type. Examples include transistors, logic gates, and amplifiers. Passive components (e.g., resistors) are not considered since there exists no known practical demonstration of their profitability in counterfeiting.

- **PCB Counterfeits (Sec.V-C).** Such counterfeits expose systems to vulnerabilities and increased failure rates. Practical counterfeit PCBs are usually of three types with varying degrees of stealth:

  Imitating (Sec.V-C.1). Attackers have complete access to the PCB design resources. However, for higher profits, they typically replace parts of the original circuit with a low-standard design. The fabricated counterfeit boards are thus different from the original PCBs, which is sometimes observable from the board layout. Still, they can remain undetected since the boards are usually inside the products (e.g., servers), preventing imaging inspection [51].

  Cloning (Sec.V-C.2). Adversaries also have all PCB design information. They can fabricate the board with the same layout while embedding counterfeit or low-quality components [54]. This type of counterfeit can be quite difficult to visually distinguish from a genuine board.

D. Golden Model

Note that PDNPulse fundamentally identifies whether the tested board can be trusted. In this work, genuine boards (i.e., the golden model) can be those supplied directly from the original equipment manufacturer (OEM), including the PCB itself and its on-board electronic components. Genuine boards can also be achieved by selecting one PCB and conducting reverse engineering. When building the golden model, process variations due to both PCB fabrication and component variation need to be considered. Specifically, component variations can arise from either fabrication tolerances or the adoption of multiple BOMs. If the deviation of the PDN impedance profiles exceeds the recorded tolerance for the golden model, we can reasonably regard a board under test as untrusted (i.e., malicious/counterfeit/suspicious). Our method is not designed to pin point the root causes or malicious intent of such deviations.

IV. Proposed Detection Methodology

In this section, we first introduce the overall workflow of the proposed PDNPulse framework. We then elaborate on how PDNPulse can help detect different board-level attacks, and discuss the challenges and considerations when measuring the impedance profile of a PCB with respect to attack vectors.

A. PDNPulse Framework

The components of the PDNPulse framework are shown in Fig. 2(a), in a step-by-step manner. To build the golden model of a new PCB design, Steps 1∼3 should be done once, followed by Step 4 to record several genuine PCB instances. To verify new PCB instances, users should then only conduct Steps 4 and 5.

① **Voltage Domain Selection.** A PCB's PDN is comprised of multiple voltage domains. Each voltage domain corresponds to a set of components connected to this domain and the PCB region of this domain. PDNPulse applies multi-domain detection, obtaining measurements from several voltage domains. Selected voltage domains determine the detection coverage. Complete coverage can be achieved by measuring all voltage domains. Given the multi-domain method, measurements can be either intra-domain or inter-domain. In intra-domain detection, to achieve low noise, each voltage domain is measured separately without including the interaction between

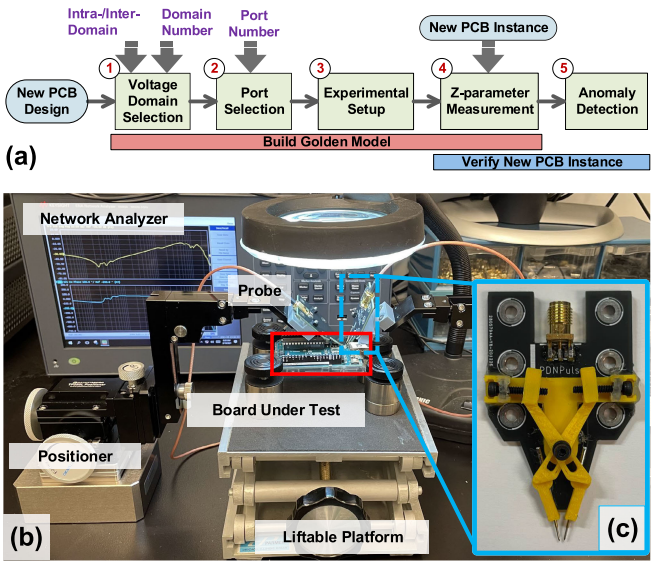

Fig. 2. (a) Proposed PDNPulse framework. (b) The experimental setup for measuring the PDN impedance profile. (c) The customized probe for low-noise PDN impedance measurement.

voltage domains. On the other hand, in inter-domain detection, multiple domains are measured together and the coupling effects between different voltage domains are analyzed. This scheme is especially useful for detecting minute changes in chip/components, because the coupling effects are much more pronounced at the chip level than at the PCB level. Inter-domain detection is also applicable when there are insufficient testing ports in one target voltage domain.

② **Port Selection.** In this step, users choose the number of testing ports, whose locations are based on the detection targets. Note that testing more ports increases the overall anomaly detection performance, but it also increases the testing cost. The selected ports must be the reachable points of the power supply net (see Fig. 1(a)). One rule of thumb for the best performance is to avoid directly placing the probe at low-impedance nodes (e.g., next to decoupling capacitors), because the measured impedance will be dominated by this low impedance, which overshadows the PDN profile we intend to measure, causing large distortion.

③ **Experimental Setup.** Once the port locations are determined, the target PCB is put on the testbed, along with positioners, a vector network analyzer (VNA), and multiple probes for measurement. The VNA is configured with the standard 2-port shunt-through method for small impedance measurements [46], followed by standard 2-port calibration to obtain high-precision measurements.

④ **Z-Parameter Measurement.** The S-parameters of the abstracted PDN are first measured by VNA, which are then converted to Z-parameters (i.e., impedance profiles). One challenge here is that existing method [46] is can only be used in measuring self-impedance. To solve this challenge, we extended the previous method [46]. Take the PDN with two ports as an example, we first measure the self-impedance (i.e., Z_{11} and Z_{22}) of each port using the classic method [46]. Then, two ports of the VNA are connected to the two ports of PDN, respectively, to measure S_{21}. Based on the equivalent circuit, we can calculate the transfer impedance Z_{21} (Z_{12}) [37]:

$$Z_{21} = Z_{12} = S_{21}\frac{Z_0}{2}\frac{1+\frac{Z_{11}}{Z_0}+\frac{Z_{22}}{Z_0}+\frac{Z_{11}}{Z_0}\frac{Z_{22}}{Z_0}}{1+S_{21}\frac{Z_{11}}{2Z_0}} \quad (2)$$

where Z_0 is the reference impedance of VNA. By repeating such a process for every two ports, we can obtain the complete Z-parameters. Note that all measurements are performed off-line without powering the boards.

⑤ **Anomaly Detection.** In this step, users apply anomaly detection algorithms (introduced in Sec.IV-C) to the generated impedance profiles to determine if any anomaly exists.

Fig. 2(b) shows the experimental setup used throughout this paper. We utilize the Keysight E5063A VNA and take the $300KHz$-$3GHz$ as the band of interest, which is the typical selection for PDN analysis. The VNA is set to $10KHz$ maximum intermediate frequency (IF) bandwidth, and 1024 points are collected for each impedance profile to obtain a proper frequency resolution.

While most components for our testbed were commercially available, the probe was a custom design (see Fig. 2(c)) to meet our unique requirements.[2] We implemented short 50Ω traces to reduce the probe's parasitic effects and match the impedance of VNA. The traces connected two probe tips (signal and ground) with springs to a coaxial adapter, which can be further connected to the VNA. A mechanical probe tuner (the yellow part in Fig. 2(c)) was also designed to precisely adjust the space between the probe tips for measuring ports at various distances. This design overcomes the limitation of commercial probes with fixed tip spacing. The distance between the tips can be adjusted from 0.05mm to 4mm by a screwdriver. Using standard calibration method [12], the probe can be compensated within 3GHz bandwidth, which is the setup throughout this paper. In addition, each probe costs around $20. Overall, our probe is accurate, relatively inexpensive, and easy to use.

B. PDN Sensitivity

Our method leverages the inherent sensitivity of the PDN for board-level anomaly detection. Fig. 3 illustrates the key idea of our method. The PDN of the PCB can be viewed as a three-dimensional impedance network, as shown in Fig. 3(a), where the top side is the power supply and the bottom side is the ground. The entire PDN is then abstracted into multiple ports, e.g., the four ports (P1, P2, P3, and P4) in Fig. 3(a). Between any two ports and between each port and the ground, there exists an impedance component, namely, $Z_a \sim Z_j$. For each impedance component, there can be a subnetwork of a series of resistors (R), inductors (L), and capacitors (C).

To show how each component can affect the impedance profile, we show a simplified example without loss of generality. That is, we ignore P4 and assume P2 has no direct connection to P3 (i.e., $Z_f{=}\infty$). Thus, we can achieve the equivalent circuit shown in Fig. 3(b). According to the Z-parameter's

[2]We release the source files for our probe design: https://github.com/xz-group/PDNPulse/tree/main/probe.

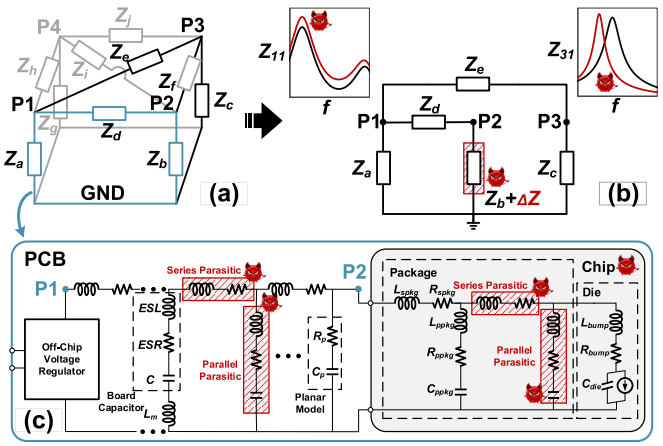

Fig. 3. (a) A conceptual network of a PDN and (b) its equivalent circuit showing the PDN sensitivity, where Z_b is maliciously modified, denoted by $Z_b+\Delta Z$. The effect of the malicious modification on the impedance profile of Z_{11} and Z_{31} is shown in red. (c) Simplified circuit model of the PDN with malicious modifications outlined.

definition, the diagonal and non-diagonal Z-parameters in Eqn. (1) can be calculated as follows [5]:

$$Z_{11} = Z_a \parallel (\boldsymbol{Z_b} + Z_d) \parallel (Z_c + Z_e) \tag{3}$$

$$Z_{13} = Z_{31} = \frac{Z_a \parallel (\boldsymbol{Z_b} + Z_d) + Z_c + Z_e}{Z_c(Z_a \parallel (\boldsymbol{Z_b} + Z_d))} \tag{4}$$

where Z_b is highlighted and works as an example. As shown in Fig. 3(b), if Z_b changes due to the malicious modification, each Z-parameter element of the network will change in a complex way, as modeled by Eqn. (3) and (4). The pattern and amplitude of the impedance profile (Z-parameter) changes depend on the topology of the PDN and the values of each impedance component.

The example in Fig. 3(b) intuitively illustrates the PCB PDN sensitivity. Although the real PDN is much more complex than the above example, Fig. 3(c) shows a simplified PDN schematic, which is part of the entire PCB PDN. In this figure, all electronic components, such as discrete capacitors, power planes, and on-board chips, can be modeled by RLC components. Together, they form a complex network where each of the PDN Z-parameters can be represented as below:

$$Z_{xy} = f(\{R_1, \ldots, R_l\}, \{L_1, \ldots, L_m\}, \{C_1, \ldots, C_n\}) \tag{5}$$

where R_i, L_j, and C_k include the parasitic effects of all PDN components. *Anomalies at different levels will inevitably introduce changes to the original PDN due to the parasitic effects of the modifications*, which can also be modeled as exogenous RLC components, as shown in the red-marked regions in Fig. 3(c). The values of R, L, and C in Eqn. (5) will then deviate from the original values.

C. Frechet Distance-Based Anomaly Detection Algorithms

Note that changes in the impedance profile are mainly due to the parasitic effects of a PCB anomaly, causing a shift of the impedance profile, as shown in red in Fig. 3(b). Besides, different anomalies can affect the impedance profile at different frequency bands. To facilitate unified anomaly detection based on the PDN, we focus on the impedance profile pattern instead of merely comparing the impedance amplitudes at a specific frequency. Therefore, we adopt the Frechet distance [14], which measures the similarity between two curves, as the security metric to evaluate the difference between the impedance profiles and to quantify the uniqueness and stability of PDNPulse. The Frechet distance (FD) is defined as:

$$FD(A, B) = \inf_{\alpha,\beta} \max_{t\in[0,1]} \left\{ d\big(A(\alpha(t)), B(\beta(t))\big) \right\} \tag{6}$$

where A and B are the two curves, $\alpha(t)$ and $\beta(t)$ are arbitrary continuous non-decreasing functions, and d is the Euclidean distance between two points of the two curves. When $t = 0$ and 1, $\alpha(t)$ and $\beta(t)$ are mapped to the endpoints of the curves. Frechet distance takes into account the location and ordering of the points along the curves when measuring similarity. It has been used to distinguish electromechanical impedance curves in the materials science field [29], [49].

For multi-port based PDN measurement, we propose to calculate the FD between two boards (noted as FD') as the norm of the FDs for each port:

$$FD'(B_1, B_2) = \frac{||\{FD(\log_{10}(Z_{xy}^{B_1}), \log_{10}(Z_{xy}^{B_2}))\}_{x\in[1,n], y\in[1,n]}||_m}{(n^2+n)/2} \tag{7}$$

where B_1 and B_2 are two boards, n is the number of ports, and m is the order of the norm. The factor $(n^2+n)/2$ is the number of Z-parameters for an n port network, which is used to normalize the FD'. The FD' is computed with the Z-parameters in log_{10} scale to avoid the high-frequency part dominating FD. Commonly selected norms include the L1 norm, L2 norm, and uniform norm.

The proposed FD' can be viewed as an analog domain alternative of the Hamming Distance (HD) that is widely used for system identification [9]. Here we formulate that stability (i.e., the intra-FD') is the ability of two instances of the same PCB design to generate the same impedance profiles under process variation. It is calculated as $FD'(B_1^{(g)}, B_2^{(g)})$, where both $B_1^{(g)}$ and $B_2^{(g)}$ are genuine boards. The uniqueness (i.e., the inter-FD') is the distinguishability of the impedance profiles of a PCB design with respect to other PCB designs. Inter-FD' is calculated as $FD'(B_1^{(g)}, B_2^{(a)})$, where $B_1^{(g)}$ is the genuine board, and $B_2^{(a)}$ is the board with an anomaly (i.e., malicious modifications or counterfeits). In this paper, the FD's of board pairs are plotted as histograms to show the detection performance. If the intra-FD' and inter-FD' are separable, then malicious boards can be identified without false positives/negatives. Although an ideal FD' histogram should exhibit zero intra-FD' and infinite inter-FD', real measurements often display a more nuanced distribution.

Further, we propose Frechet distance-based classification and anomaly detection methods. For anomaly detection, intra-FD's are calculated for each pair of genuine boards, and the statistical boundary (e.g., $\mu+3\sigma$) of intra-FD' is set as the threshold. Then the FD's between the test board and the training boards are calculated and compared with the threshold to determine if an anomaly exists. For classification, we adopt

Algorithm 1 FD-Based K-Nearest Neighbor Classification

Input: B: test board; K: # of nearest neighbor; $\{B_i, y_i\}_{i\in[1,N]}$: training boards
Output: y: class label of test board

function FD-KNN(B, K, $\{B_i, y_i\}$)
  ▷ e.g., $B = \{Z_{11}, Z_{12}, Z_{22}\}$ when $n = 2$
  Set the value of $D = []$
  for $i = 1$ to N **do**
    Calculate $d_i = FD'(B_i, B)$
    Append $\{y_i, d_i\}$ to D
  end for
  Sort D in the ascending order with respect to d value
  Pick the first K entries $\{y_j, d_j\}$, $j = 1, \ldots, K$ from D
  y = majority-voting($\{y_j, d_j\}$, $j = 1, \ldots, K$)
end function

the modified K-Nearest Neighbor (KNN) algorithm as listed in ALG. 1. The input of the FD-KNN algorithm includes a set of labeled training boards $\{B_i, y_i\}_{i\in[1,N]}$, a test board B, and the number of nearest neighbors K. Instead of calculating the distance of impedance profile features, we use the FD' (i.e., Eqn. (7)) between the test board and the training board as the distance metric. The output label y is decided through majority voting the labels of K nearest neighbors.

D. Anomaly Detection

Herein we analyze the impacts of board-level anomalies on the PDN. These are the source of PDNPulse's high sensitivity and extensive coverage in detecting anomalies.

1) PCB Hardware Trojan: Board-level hardware Trojans are often implemented by adding, removing, or altering discrete components (e.g., components or programmable chips), and they may introduce large deviations in the PDN parameters. Our PDNPulse framework detects such Trojans by directly measuring changes in the PDN impedance profile. *It is common for the pins of the hardware Trojan components to connect to the PDN to be powered on*, which directly creates unexpected parasitic effects on the PDN.

2) Counterfeit or Low-Quality Electronic Components: For counterfeit or low-quality chips/components, *the characteristics of the PDN for both the die and package will be different from the original ones*, enabling detection by PDNPulse. Take a chip with ball grid array (BGA) package as example. The package substrate has a similar structure to the PCB. The substrate consists of multiple layers connected through microvias to rearrange the location of pins. At the die level, the parasitic effects are dominated by three sources: power grid, substrate diffusion, and MOSFET gates. Both the package and die contribute information for anomaly detection.

3) Board Counterfeiting/Recycling: The impedance profile of a counterfeit/recycled PCB is partially altered by changed specifications of the discrete components. In addition, *due to inherent wear or aging, changes in the material characteristics of the PCB (e.g., the dielectric constant of the insulating layer) can also contribute to PDN impedance deviation* and thus be detected with similar methodology.

V. PDNPulse Analysis and Results

In this section, we extensively analyze PDNPulse to illustrate its capability to capture board-level attacks, including PCB Trojans, chip/component counterfeits, and PCB counterfeits. We use a range of custom and COTS boards to demonstrate PDNPulse's broad coverage and high sensitivity. These PCBs cover different scales and complexities of design from 2-layer boards with tens of on-board components to 6-layer boards with hundreds of components. The attacks in our evaluation are deliberately designed to model notable attacks in the real world and are also representative in terms of both stealthiness and impact.

To best illustrate the practical utility of our method, we adopt the reference designs of COTS boards. Many such designs do not provide specific PDN measuring ports. Thus, we employ the in-house-developed probe (see Sec.IV-A) to perform precise measurements. Without loss of generality, here we focus on one voltage domain covering the majority of the PCB, but measuring multiple domains is recommended to avoid blind points. For the results, besides the FD' histogram, we also report the standard detection performance metrics, true positive rate (TPR), and false positive rate (FPR). An 100% TPR and 0% FPR would be ideal, indicating that the distributions of genuine and malicious/counterfeit boards are completely separable.

A. PCB Trojan Detection

In this subsection, we show that PDNPulse can effectively detect the three types of PCB Trojans discussed in Sec.III. We fabricated genuine (i.e., Trojan-free) and malicious (i.e., Trojan-inserted) boards of two designs: a customized proof-of-concept (PoC) board and an Arduino Due board. The experimental Trojans are representative of known threats and are designed to ensure the original functionality of the board.

1) Coverage Evaluation with Custom PoC Boards: We first conduct PoC experiments on a customized microprocessor development board with a relatively simple PDN to validate the coverage of PDNPulse on Trojans.

Platform Description: Fig. 4 illustrates the PCB design. This is a 2-layer board containing a SoC chip and its peripheral circuit. Its PDN follows the guideline of the SoC datasheet and has one voltage domain. Fig. 4(a) shows the experimental setup. As a custom design, we implement SMA coaxial adapters attached to the PDN, thus the VNA can directly connect to the PDN for accurate measurements. In this experiment, we fabricated and tested 4 boards.

Anomaly Description: Fig. 4(b) shows the three inserted Trojans. Each of them is using jumpers to turn on/off. The triggerable Trojan is an ATtiny85 MCU that performs malicious operations using a preloaded program. A real-world attack based on this MCU is to attack a firewall device [19]. The always-on Trojan is a malicious sampling resistor enabling power side-channel analysis attacks and the value of the resistor is set to be the typical 1Ω [56]. The simplified PDN schematic with Trojans is shown in Fig. 4(c).

Detection Results Analysis: We show that we can effectively detect all three Trojans, and achieves 100% TPR and 0% FPR.

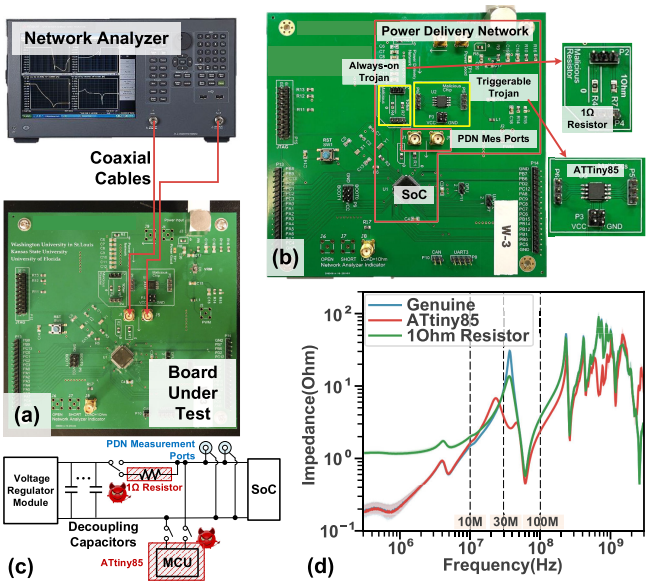

Fig. 4. (a) The setup for measuring the PDN impedance of customized board. (b) Layout of the customized board with Trojans inserted. (c) Simplified PDN schematic of the board. Its PDN profiles show PDNPulse's coverage on (d) triggerable Trojan (ATtiny85) and always-on Trojan (1Ω sampling resistor).

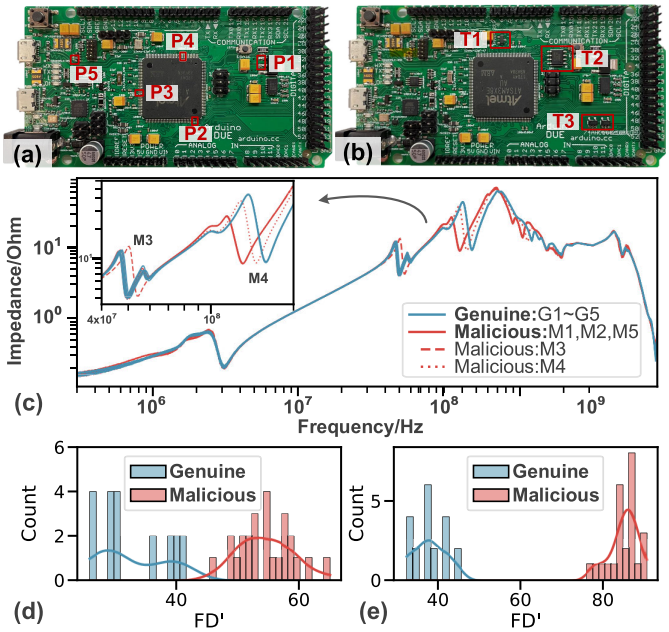

Fig. 5. Layouts of the (a) genuine Arduino Due board with measurement ports highlighted, and (b) the malicious board with three triggerable Trojans highlighted. (c) Impedance profiles (i.e., Z_{55}) of the 5 genuine boards (G1∼G5) and 5 malicious boards (M1∼M5), where each of the 10 curves represents one board. (d)(e) Histogram of FD' of all board pairs calculated using the Z-parameters of (d) 3 ports (P1-P3) and (e) all 5 ports. Malicious boards can be clearly distinguished from genuine boards.

In this PoC experiment, the measurement is based on one port, thus we have one Z-parameter. Fig. 4(d) illustrate the mean Z_{11} impedance (with 95% PI shadowed[3]) when enabling different Trojans. The blue line show the genuine impedance when none of the Trojans are connected to the circuit.

Triggerable Trojan: In Fig. 4(d), the red line depicts the PDN impedance profile when the ATtiny85 MCU is inserted to the circuit. This MCU's power pins are connected to the PDN and its functional pins are connected to the target signal traces. Due to the parasitic effects of ATtiny85, an equivalent RLC network is introduced to the PDN, affecting the R_i, L_j, and C_k values in Eqn. (5). Thus, a dent at $30MHz$ is observed. Meanwhile, ATtiny85 also affects the board resonance, causing impedance profile differences above $100MHz$.

Always-on Trojan: The green line in Fig. 4(d) depicts the PDN impedance profile when the 1Ω sampling resistor is connected in series to the PDN. Due to the insertion of the resistor, the impedance below $10MHz$ raises from 0.2Ω to 1.2Ω, and the impedance around $30MHz$ also deviates from the genuine impedance. Since the genuine impedance at low frequency is 0.2Ω, with ±10% PCB fabrication tolerance, we can detect malicious resistors larger than 0.02Ω.

2) Triggerable Trojan on Arduino Due Boards: Herein, we validate PDNPulse can detect the foremost type of Trojans, triggerable Trojans, on complex COTS Arduino Due boards [2] using designed probes. Three different triggerable Trojans are inserted to the PCBs during the design stage.

Platform Description: Fig. 5(a) shows the genuine Arduino Due board. It is a 2-layer MCU development board based on ATsam3 × 8e. There are four voltage domains (5V, 3.3V, USBVCC, and XVCC), supporting more than 50 on-board components. In this experiment, we focus on the 3.3V voltage domain since it supplies power to most on-board components. The PDN is abstracted into a 5-port network and the locations of PDN measurement ports are highlighted in Fig. 5(a). The ports are ensured to diversely distribute on the PCB and not on or close to the capacitors. We fabricate 5 genuine Arduino Due boards and 5 malicious ones for testing.

Anomaly Description: Fig. 5(b) highlights the three Trojans, which are carefully designed to be impactful while sneaky. T1 is a small-package MOSFET chip for leaking information through a LED. The LED was used for indicating the output pulse-width modulation signal. At T2, a maliciously programmed MCU ATtiny102F is implemented. Attackers can send messages through UART to the board and trigger ATtiny102F to erase the on-board Flash memory. T3 is based on two 74xx XOR logic chips with small packages, which can be triggered by the software and then crash the system. The readers are referred to [64] for more details of the Trojans.

Detection Results Analysis: Fig. 5(c)-(e) show the robustness and effectiveness of our framework. We also find that PDNPulse is sensitive to changes in PCB design while resistant to process variation. We obtain 15 Z-parameters for each of the 10 boards, then calculate FD' for 5×4=20 genuine-genuine pairs and 5×5=25 genuine-malicious pairs.

Fig. 5(c) shows that due to the Trojans, the malicious boards can be distinguished from genuine boards with process variation, where we exhibit one of the measured impedance profiles, Z_{55}, and plot the profiles of all 10 boards.

In Fig. 5(d)(e), histograms of FD' demonstrate the effectiveness of FD-based detection algorithm and the benefits of

[3]The Percentile Interval (PI) error bar is adopted here as a data spread measure, representing the spreading interval ranging from 2.5 to 97.5 percentiles [4].

multi-port detection. For the FD' histograms in this paper, the FD' is with respect to the genuine boards, where we calculate the intra-FD' for all genuine-genuine board pairs and mark them as Genuine (blue bars in Fig. 5(d)), and we mark the inter-FD' of all genuine-malicious board pairs as Malicious (red bars in Fig. 5(d)). Fig. 5(d) is based on 3-port detection, where only ports P1-P3 (with 6 Z-parameters) are utilized. The gap between the intra-FD' and inter-FD' implies that a threshold can be set to identify potential boards. Then Fig. 5(e) shows the results leveraging all 5 ports (with 15 Z-parameters). The gap increases, making the detection more resistant to PCB tolerance and sensitive to Trojans. In both 3-port and 5-port detection, we achieve 100% TPR and 0% FPR.

We further show that PDNPulse maintains its sensitivity on complex COTS boards. We remove one chip at T3 on the M4 board (the Malicious board with index 4) during the testing for ease of debugging. The profile of M4 board is different from other Malicious boards, as illustrated in the inset of Fig. 5(c). The package of the removed chip is smaller than any other digital chip on this board. Since the parasitic effects are correlated with the chip's physical size [30], this result indicates the sensitivity of PDNPulse.

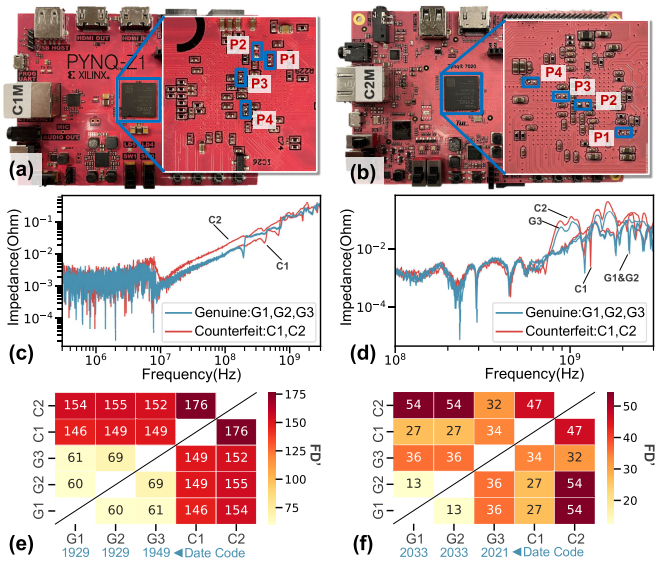

Fig. 6. The layouts (a)(c)(e) PYNQ-Z1 and (b)(d)(f) PYNQ-Z2 boards, with results showing PDNPulse's effectiveness in detecting counterfeit chips. (c)(d) The Z_{12} profiles of 5 boards, with each curve representing one board. (e)(f) Heat maps show FD' based on all Z-parameters, with FPGA chip date codes highlighted.

B. Counterfeit Chip/Component Detection

In this subsection, we demonstrate the desirable performance and sensitivity of PDNPulse in detecting both counterfeit chips and components. While, existing works may fail to detect both types since they typically utilize specific design features that are not compatible with both chips and components (e.g., JTAG, which is only available in chips [40]). Besides, the labels (i.e, markings) of chips/components can be removed or occluded (e.g., by EM shields), invalidating imaging/visual inspection. We overcome these limitations by utilizing unified PDN electrical properties. Here we perform detection on three platforms: PYNQ-Z1 and PYNQ-Z2 FGPA development board, and MSI H310M computer motherboard. The target chips/components are in various packages to show PDNPulse's coverage.

1) Counterfeit Chip on PYNQ Boards: We detect counterfeit chips on two platforms, PYNQ-Z1 and PYNQ-Z2 boards.

Platform Description: Fig. 6(a) and (b) highlight the measured ports on both PYQN boards. These two boards are FPGA development boards based on the Xilinx XC7Z020 FPGA. The boards have 6 layers and more than 100 on-board components. In this experiment, we purchase 5 PYNQ-Z1 boards and 5 PYNQ-Z2 boards. The PDNs are elaborately designed, including more than 15 voltage domains. The FPGA chip is supplied by 4 voltage domains (3.3V, 1.0V, 1.8V, and 1.5V). We select the ports from these 4 voltage domains (at the bottom side of the FPGA), and abstract the PDN into a 4-port network with each port for one domain.

Anomaly Description: To mimic chip counterfeiting, we replace the original FPGA chips of 2 PYNQ-Z1 boards and 2 PYNQ-Z2 boards with recycled ones considering that chip recycling is the main source for chip counterfeiting. Note that these recycled chips may not be authentic before recycling.

Detection Results Analysis: Fig. 6(c)-(f) illustrate that the counterfeit FGPA chips are distinguishable from genuine ones. Since there are 4 ports in 4 voltage domains, 10 Z-parameters are available. We collect 6 non-diagonal Z-parameters (e.g., Z_{12}, Z_{24}) for each board to emphasize the coupling effects between voltage domains. In Fig. 6(c)(d), one of the Z-parameters, Z_{12} of all boards are plotted to show the differences between genuine boards and counterfeit ones.

Then, in Fig. 6(e)(f), we use FD' matrix to quantitatively validate the results in Fig. 6(c)(d) by considering all measured Z-parameters and analyzing the relationship between FPGA chip date codes [60]. In Fig. 6(e), the genuine boards have low FD' with each other while having high FD' with the counterfeit boards. Thus, a threshold can be set to identify counterfeit boards with 100% TPR and 0% FPR. Compared with PYNQ-Z1, the differences between PYNQ-Z2 boards with different FPGA date codes are more obvious. Interestingly, as shown in Fig. 6(f), the FD' between G1 and G3 or between G2 and G3 are even higher than the FD' between G1 and C1. We find that both G1 and G2 are manufactured at 2033 (the 33th week of 2020), while G3 is manufactured at 2021 (the 21st week of 2020). We also see this relationship in Fig. 6(e), where G1 (date code: 1929) is closer to G2 (1929) compared to G3 (1949). For PYNQ-Z2, single threshold-based detection yields false positives/negatives. As will be discussed in Sec.VI, these faults can be avoided by modeling multiple batches and applying the FD-KNN algorithm.

To further analyze the impact of de-/re-soldering the chips on anomaly detection, we de-solder the FPGAs chips on all PYNQ-Z1 boards (i.e., including the genuine ones and counterfeit ones) and then re-solder the chips. For each PYNQ-Z1 board, the impedance profiles are measured again, and the FD' between the newly and previously measured impedance profiles are calculated. The FD' ranges from 2.7 to 11.4,

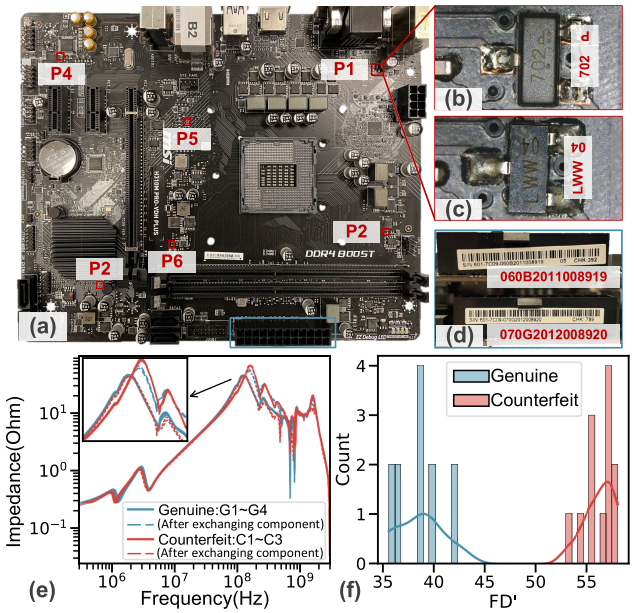

Fig. 7. (a) The layout of MSI H310M computer motherboard with measurement ports highlighted. (b)(c) The labels of the transistor at P1 on boards fabricated by two production lines are different. (d) The two production lines have different S/N codes. (e) Seven Z_{11} profiles including 4 genuine and 3 counterfeit boards, where the boards from one production line are deliberately regarded as counterfeits. The 4 dashed lines (2 genuine boards with counterfeit transistor, and 2 counterfeit boards with genuine transistor) confirm the difference between the two types of boards. (f) The FD' histogram based on all Z-parameters shows detection effectiveness.

indicating that if we set the anomaly detection threshold at 100 (see Fig. 6(e)), no false positive nor false negative will be induced due to the de-/re-soldering operations.

2) Counterfeit Component on Motherboards: We further show both PDNPulse's effectiveness in detecting counterfeit components and its scalability for assuring the security of large-scale PCB designs. The high sensitivity of PDNPulse for detecting counterfeit chips/components is also validated.

Platform Description: Fig. 7(a) shows the selected large-scale design, MSI H310M computer motherboard, and PDN measurement ports. The board contains 6 layers and hundreds of components. On the motherboard, there exist more than 30 voltage domains and the supply voltage ranges from 1V to 12V with different specifications. For most voltage domains, the supplied components usually concentrate in a small area of the board. In this experiment, we focus on the 3.3V voltage domain and abstract the PDN to a 6-port network. The components supplied by 3.3V voltage domain spread across the board, thus we can evaluate the board with one domain. We purchase 4 and 3 brand-new motherboards fabricated by two production lines (confirmed by checking the S/N code shown in Fig. 7(d)) for PDN measurements. We further show both PDNPulse's effectiveness in detecting counterfeit components and its scalability for assuring the security of large-scale PCB designs.

Anomaly Descriptio: While both boards are legitimate versions, the BOMs of the two production lines are different. Thus, to mimic component counterfeit, the boards from one production line are regarded as genuine and the other production line is treated as counterfeit. Based on the PDN measurements, after carefully examining the two motherboards, we notice that only the transistor at P1 (see Fig. 7(a)) for power management is different in both boards (see Fig. 7(b) and (c)). This transistor is thus utilized as an instance of mimicking component counterfeiting attacks.

Detection Results Analysis: Fig. 7(e) illustrates the impacts on PDN impedance profile due to the transistor at P1. With 6 ports, we measure 21 Z-parameters for each board. Here, the Z_{11} of all 7 motherboards are plotted, where the differences between the 4 genuine and 3 counterfeit boards are distinguishable. By examining other Z-parameters, the differences are observable mainly in the Z-parameters related to P1. Since the two boards have different transistor models at P1, even though the two transistors have the same package, the impedance profiles are different from each other. To confirm this finding, we exchange this transistor among four boards (2 from genuine boards, 2 from counterfeit boards). As shown in Fig. 7(e), the 2 blue dashed lines are the genuine boards with transistors from counterfeit boards, and the 2 red dashed lines are counterfeit boards with genuine transistors. We observe that the impedance profiles of the modified boards match with the other type of boards, meaning that the transistor at P1 causes the differences between profiles.

We further use the FD' based on all 21 Z-parameters to quantitatively show PDNPulse effectively detects the counterfeit component. There are total 12 genuine-genuine pairs and 12 genuine-counterfeit pairs. Fig. 7(f) shows the histogram of board pairs. The TPR and FPR are 100% and 0%, respectively. Since we detect a counterfeit component in a small package on a relatively large-scale PCB, the results not only show PDNPulse's scalability for complex designs such as motherboards, but also indicate its acceptable sensitivity in counterfeit chip/component detection.

C. Counterfeit PCB Detection

In this subsection, we show that PDNPulse can also detect PCB counterfeit with varying degrees of sneakiness. Two PCB designs are selected, an Intel I350-T4 Ethernet adapter and an Arduino Uno board, covering the two types of PCB counterfeit.

1) Imitation Network Adapter Boards: We demonstrate the capability of PDNPulse in detecting an imitation Intel I350-T4 Ethernet adapter. This imitation is a real-world attack and is well documented [51]. We also illustrate PDNPulse can perform cross-board detection, where imaging inspection may not be available.

Platform Description: Intel I350-T4 is a network adapter board based on the Intel I350 processor. There are three voltage domains on PCI-E connector as well as the adapter board, 12V, 3.3V, and 3.3Vaux. Correspondingly, we abstract the PDN to a 3-port network for direct detection and the locations of these ports are shown in Fig. 8(a). For cross-board detection, we plug the network adapter into the MSI H310M PRO-VDH PLUS computer motherboard. The probe is attached to the PCI-E 12V power pin on the motherboard. Note that here the computer motherboard is not powered.

Anomaly Description: We purchase 3 genuine boards and 3 counterfeit ones, as shown in Fig. 8(a) and (b). We confirm

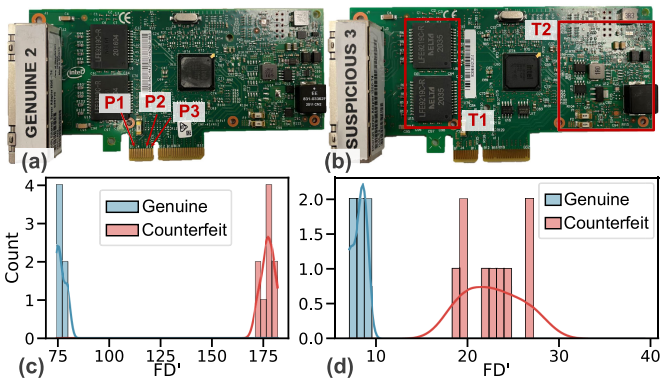

Fig. 8. (a) Genuine Intel I350-T4 board with measurement ports highlighted. (b) Counterfeit board with suspicious areas marked. The FD' histograms of (c) direct detection and (d) cross-board detection, showing PDNPulse can detect board imitations.

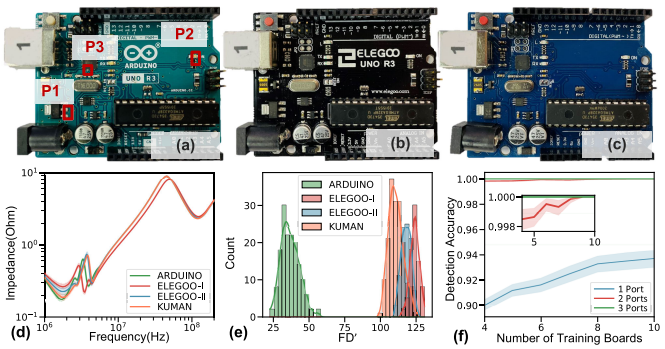

Fig. 9. Arduino Uno boards from three vendors: (a) official Arduino, (b) Elegoo, and (c) Kuman. We treat the official Arduino as genuine, and the other two as counterfeit to mimic cloned PCBs. (d) The mean Z_{33} profiles (with 95% PI) of Arduino boards. (e) Histogram of FD' based on all Z-parameters, where the boards can be clearly identified as genuine or counterfeit. (f) Results of FD-3NN classification for different numbers of measurement ports.

that the counterfeit boards are imitated boards for two reasons. First, the word "Delta" on the Delta Ethernet transformers (T1 in Fig. 8(b)) should be embossed on the chip. Second, the peripheral circuit (T2 in Fig. 8(b)) is replaced with a low-standard design. As reported in [51], the counterfeit boards are equipped with low-quality chips and components such that these boards will probably fail within one year.

Detection Results Analysis: Fig. 8(c)(d) show PDNPulse's effectiveness of both direct and cross-board detection. We obtain FD' for 6 genuine-genuine pairs, and 9 genuine-counterfeit pairs. In Fig. 8(c), the FD' are calculated based on all 6 Z-parameters (3 ports). Even though the two boards have the same PCB layout, due to the usage of different on-board components, the intra- and inter-FD' are significantly different. Fig. 8(d) shows the results of cross-board detection, where FD' is based on one Z-parameter. In cross-board detection, the impedance profiles of network adapters are distorted by the PDN of the motherboard and the parasitics of PCI-E connector, which reduces the inter-FD'. However, we still can identify the counterfeit boards. We have 100% TPR and 0% FPR in both types of detection.

2) Cloned Arduino Uno Boards: We then demonstrate PDNPulse on cloning detection by experimenting with Arduino Uno boards [6], which are popular in the market for their low cost.

Platform Description: Arduino Uno is an open-source MCU development board based on the ATmega328P. It has been fabricated and sold by many manufacturers, which serves as an excellent example of cloning attacks. Fig. 9(a) shows the locations of the three measurement ports. We measure the 5V voltage domain which is the main supply voltage of the PCB and abstract the PDN to a 3-port network.

Anomaly Description: We purchase a total of 39 boards from three different vendors (13 from each vendor): Arduino.cc, Elegoo, and Kuman, as shown in Fig. 9(a)-(c), respectively. All three designs share the same schematic and layout. We mimic PCB cloning by referring to Elegoo and Kuman boards as counterfeit boards, while the official Arduino boards from Arduino.cc are treated as genuine ones.

Detection Results Analysis: Fig. 9(d) illustrates PDNPulse can successfully detect the cloned boards, where we show Z_{33} out of 6 collected Z-parameters. During the measurements, we notice that there are two batches of Elegoo boards (marked as Elegoo-I and Elegoo-II), which cannot be visually distinguished from each other. However, we can confirm the two batches from their impedance profiles. The impedance profiles of Elegoo-I and Elegoo-II are different from each other for all Z-parameters. For each batch, the impedance profiles of the boards are consistent with other boards of the same batch. Since the differences are mostly at the low frequency, we infer that the two batches have the same PCB layout, but the on-board components may be from different vendors or have different specifications.

In Fig. 9(e), we plot the FD' histogram of the three vendors with respect to official Arduino boards, to show that the genuine Arduino boards can be distinguished from the counterfeit (i.e., non-Arduino) boards with 100% TPR and 0% FPR. We also demonstrate that the developed FD'-KNN algorithm can classify the boards into multiple classes to prevent false positives on different batches of boards. Moreover, multi-port measurement can increase the classification accuracy. Fig. 9(f) illustrates the relationship between the average classification accuracy, the number of boards for training, and the number of ports. We use FD'-3NN to classify the board into 4 classes (i.e., Arduino, Kuman, Elegoo-I, and Elegoo-II). For each configuration (i.e., # of training boards and # of ports), we run 500 trials and compute the average accuracy. Both the training boards and the measured ports are randomly selected for each trial. Compared with 1-port detection, 2-port detection improves the classification accuracy to higher than 99.8%. In addition, using the 3-port detection, a 100% detection accuracy can be reliably achieved with 4 training boards from each class.

VI. Defending Against Adaptive Attackers

In this section, we discuss PDNPulse's capabilities against adaptive attackers who attempt to bypass PDNPulse intentionally. The detection sensitivity is first explored to show the performance of detecting well-designed Trojans. Then other stealthier mechanisms that attackers can utilize are discussed.

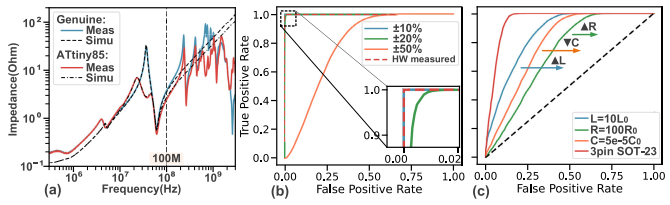

Fig. 10. (a) Measured and simulated PDN profiles of customized PCB. Simulated ROC curves (b) with different PCB tolerances and (c) when taking ATtiny85 (C_0,L_0,R_0) as a reference and scaling the malicious modifications. The results show PDNPulse's sensitivity.

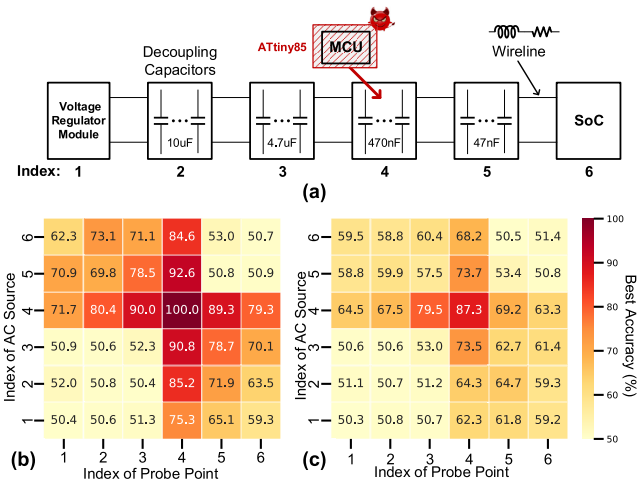

Fig. 11. (a) The simplified structure of updated PDN structure in simulation. The best anomaly detection accuracy with varying locations of AC source and probe point when PDN has a total of (b) 6 capacitors and (c) 12 capacitors.

Overall, PDNPulse aims to create *an effective security asymmetry between attack and defense*. Although PDNPulse is not an ultimate solution for PCB attacks, implementing PDNPulse can significantly mitigate potential threats. The most motivated attackers can intentionally bypass PDNPulse but likely at the cost of making their malicious implants more easily detected by orthogonal approaches (e.g., inspection, functional test, and integrity check), or requiring significantly advanced techniques.

A. Detection Sensitivity

To achieve both visual and electrical stealth, attackers may deliberately miniaturize malicious circuits (e.g., by using small-package chips). This strategy aims to bypass PDNPulse anomaly detection because chips/components with small footprints also tend to have lower parasitics, making them closer to the ideal open circuit (C=0, L=∞, R=∞) when connected in parallel with the PDN. However, in frequency-domain PDN analysis, malicious modifications with minimal parasitics are still observable as shifted PDN profiles with discernible magnitudes [30] at high frequencies. This property facilitates PDNPulse's detection sensitivity.

To investigate the limits of detection sensitivity of PDNPulse in response to attackers' efforts, we build a simulation model to capture the PDN of the custom PoC boards in Sec.V-A.1 and study the impact of various malicious modifications. We use the well-accepted modeling methodology described in the industry documentation [27] and abstract the chips as RLC networks in parallel with the PDN. The circuit model is validated by toggling the connection/disconnection of ATtiny85 to the PDN, then comparing the simulated impedance profiles with the experimentally measured one. The simulation results are consistent with the hardware measurements (see the black dashed lines in Fig. 10(a)). Note that we focus on modeling the parasitics of custom PCB and anomalies. The analysis of board resonance (e.g., $>100MHz$ for custom PCB) is out of the scope of this work.

The sensitivity of PDNPulse is affected by both PCB process variation (i.e., tolerance) and intrinsic parasitics of the anomalies. In Fig. 10(b), we present the simulated PDNPulse performance for detecting ATtiny85 with varying levels of PCB tolerances using Monte-Carlo simulation, where process variation follows Gaussian distribution and the tolerance is 3σ. Results in Fig. 10(b) show that PDNPulse has desirable performance under ±20% tolerance, beyond the worst case variations for COTS boards. Acceptable performance can be achieved even with ±50% tolerance. We thus conclude that PDNPulse detection sensitivity is sufficient to handle process variation of typical COTS boards. This conclusion is further validated by comparing the simulated ROC curves with hardware measurements (the red dashed line in Fig. 10(b)).

In Fig. 10(c), we present PDNPulse's sensitivity as a function of the RLC parameters. We first simulate the chip with 3pin SOT-23 package (C=$0.12pF$, L=$1.4nH$, R=3Ω) [26], one of the smallest package footprints available (2.6mm×2.9mm). Results show PDNPulse can successfully spot these stealthy changes. We then use the parasitics of an ATtiny85 chip (C_0=$0.9nF$,L_0=$21nH$,R_0=3Ω) as a reference and scale its RLC values to explore the limits of PDNPulse. We can achieve acceptable performance with even $10L_0$, $100R_0$, or $5\times10^{-5}C_0(1.8fF)$, where the parasitics of anomaly are an order-of-magnitude smaller than the SOT-23 package. Even though the simulation is based on the Trojan PoC board, we are confident that the conclusion and trends here can be extended to other types of anomalies including counterfeits. Note that the RLC network model is not specific to ATtiny85 and can represent any type of anomaly described in this paper. By including the board resonance, adopting multi-port detection, and increasing the measurement bandwidth, the performance can be further improved.

Besides miniaturizing malicious circuits, attackers may exploit capacitors' isolation effect to bypass PDNPulse. Precisely, attackers can place the anomalies in close proximity to the decoupling capacitors, making the anomalies connected in parallel with low-impedance capacitors. We conduct a simulation by updating the previous PDN model to study the potential for attackers to conceal anomalies. The updated PDN structure is shown in Fig. 11 (a) and includes four groups of decoupling capacitors with values of 10uF, 4.7uF, 470nF, and 47nF, whose models are adopted from [27]. The four groups contain 1, 1, 2, and 2 capacitors, respectively. We also include a wireline model [63] to connect the VRM, the capacitor groups, and the SoC. For clarity, we index the locations of VRM, each

TABLE I
COMPARISON OF DETECTION ACCURACY ON ARDUINO DUE BOARDS USING SINGLE PORT VS. FOUR PORTS UNDER VARIOUS PORT SELECTION SCENARIOS

Single Port	84.4%	73.3%	62.2%	91.1%	91.1%
Four Ports	100%	100%	100%	100%	100%

group of capacitors, and SoC from 1 to 6. An ATtiny85 chip, mimicking anomaly, is inserted in the 470nF capacitor group (i.e., index 4) to attempt to bypass PDNPulse. Similar to the previous simulation, we use the Monte-Carlo simulation and set the process variation as ±10% tolerance.

Fig. 11 (b) illustrate the best anomaly detection accuracy (i.e., $(TP+TN)/(TP+TN+FP+FN)$). By setting the AC source x and probe point y to different indexes, we measure various transfer impedance (e.g., Z_{21} if AC source index x=1 and probe point index y=2). Note that when x=y, the measured impedance is self-impedance. The results indicate that if the detection is only based on the self-impedance (i.e., x=y) unless the measurement point is at the same index as the ATtiny85 chip, we fail effectively detect the chip (with maximum 52.3% accuracy). However, leveraging the transfer impedance, the ATtiny85 chip can be acceptably detected as long as the measured transfer impedance covers the location of the ATtiny85 chip (e.g., x>4 and y<4). We also find that the detection accuracy decrease as the increase of the distance between AC source and probe point ($|x$-$y|$). For example, with $x = 1$ and $y = 6$, the accuracy decreases to only 59.3%.

We further investigate the impact of implementing more capacitors in the PDN. The number of capacitors in each group is doubled, and the results are presented in Fig. 11 (c). Compared to the previous configuration, the accuracy decreases for both self-impedance and transfer impedance. The decline in accuracy results from more capacitors causing a lower impedance, making anomaly impacts less obvious. Please note that here we consider only using at most two ports to detect anomalies. The accuracy can be increased by measuring from more ports and applying KNN algorithms.

B. Multi-Port Detection Trade-Offs

This subsection examines the advantages of multi-port detection in comparison to single-port detection using experiments on Arduino Due boards. It contrasts the detection accuracy when using a single port versus employing four ports under various port selections. The results are listed in Table I. For the Arduino Due board, where the PDN is abstracted into a five-port network, we iteratively select single port/four-port combinations to conduct detection. By using multi-port detection, PDNPulse can achieve a stable full coverage of all anomalies, which cannot be achieved by single-port detection.

Multi-port detection entails certain costs, which can be assessed from two perspectives: the number of measurements (represented by $(n^2+n)/2$ for n port detection) and the supplementary computational expenditures linked to calculating the S- to Z-parameter conversion (as shown in Equation (2)) and the multi-port FD' (as illustrated in Equation (7)). Nonetheless, PDNPulse is tailored for static detection, allowing these overheads to be effectively amortized through parallelization with other standard PCB tests. Hence, the advantages provided by multi-port detection significantly outweigh the incremental costs for security-critical applications.

C. Attacker Response

We explore available attack vectors that either undermine PDNPulse by avoiding connection to the PDN, or attempt to bypass PDNPulse by hiding its impact on the PDN impedance profile and discuss their feasibility in what follows.

1) Avoid PDN Connection: PDNPulse assumes that counterfeits and persistent PCB Trojans require a power supply to operate and that their power pins are typically attached to the PDN. Thus, adversaries can avoid connecting the PDN to bypass PDNPulse.

Using an Alternative Power Source: An adversary may use self-powered circuits or harvest power from data signals to avoid connecting directly to the PDN. If a self-powered Trojan employs a battery that is intended to be both persistent and long-term, then both its capacity and size need to meet those specifications (e.g., to spy on the target system [44]). COTS batteries are not an option in this case since the diameters of most are greater than 6mm [58]. Thus, attackers would need to adopt significantly advanced battery fabrication and integration techniques to be successful. Circuits that harvest ambient energy are typically based on coils or photodiodes with relatively large footprints to maximize energy extraction. In this case, the main challenge of the adversary would be evading visual inspection. However, we expect multiple anomaly detection techniques to be employed, such as ones that detect hidden modifications [7], [28], because PDNPulse is not intended to be an ultimate solution. Trojans that harvest power from data signals are also plausible. Note that a practical implementation should consider the loading effect on the signal pins and avoid impacting the signal quality to pass the standard functionality tests. Another consideration for such an attack is that to provide a stable power supply the adversary would also need to control the status (e.g., keep logic high) of that signal pin when the Trojan is working, which requires additional handling circuitry. It is worth mentioning that attacks using the above three methods have not been reported.

Passive Attacks: Attackers may also use purely passive circuits which do not require a power supply. However, we believe the potential attacks using only passive circuits are limited (typically to signal traces) and often lead to uncontrollably compromise of essential functions. For example, an attack is presented in [17] that alters trace spacing and dimensions to cause cross-talk, but also impacts the original signal quality due to increased interference. Detecting such modifications to signal traces is out of the scope of our work but it can be achieved by functionality tests. Please note that PDNPulse can detect passive attacks related to the PDN (see Sec.V-A.1). Designing configurable and stealthy Trojans using passive circuits is still an open question, and we are unaware of any documented attacks.

2) Hidden Impact on PDN Impedance Profile: Although Trojans have to attach to the PDN, attackers may try to reduce their impact on PDN profiles to evade PDNPulse. We discuss several possible methods for doing so below.

Conceal in the Decoupling Capacitors: Adversaries may hide anomalies near decoupling capacitors to evade PDNPulse detection. But this strategy creates a challenge in maintaining short wiring distance from the anomalies to the desired point on the PDN while also keeping the wiring distance from the anomalies to the payload short. If this challenge is not addressed, the anomalies may not be stealthy enough. Our earlier discussion (Sec. VI-A) has shown that the proposed transfer impedance-based detection methods can effectively detect anomalies hiding in capacitors. However, we also found that for large-scale and high-performance PCBs that require ultra-low impedance PDN, detection becomes more challenging as more capacitors are implemented. One way to improve detection performance is to increase the number of measurement ports and include board resonance in the analysis.

Exploit Insufficient Measurements: Adversaries may learn the measurement parameters of PDNPulse, such as the measured voltage domains and ports, and then intentionally implant their Trojan outside of those parameters to avoid being detected. The challenge for this approach is that malicious modification will unpredictably affect multiple impedance profiles (i.e., multiple Z-parameters) simultaneously (see Sec. IV-B). To find reliable measurement blind spots for implantation under multi-domain multi-port detection, attackers would need to obtain the RF models of both the victim PCB and Trojan circuits, then simulate the PDN profiles when placing Trojans in each potential location to verify the blind spot will remain hidden. Note that such RF models are usually not available and attackers typically need to measure the whole PDN using our method to obtain the models.

Compensate for PDN Impedance Effect: As described in the previous section, a motivated attacker may obtain the RF model of the PDN. They may then adjust the circuit design to compensate for the parasitics of the Trojan and avoid detection. Unfortunately, passive R, L, and C components have different (instead of mutually offset) effects in the frequency domain, which prevents them from canceling one another out. However, they can shift the affected spectrum band (i.e., compensate the impedance at one or several frequency points). To fully compensate for the PDN profiles, attackers would have to adjust the original PDN design (e.g., remove decoupling capacitors). However, since the adjustment for one Z-parameter will inevitably affect other Z-parameters attackers must exhaustively search for a solution to fully compensate the PDN profile (all Z-parameters), and there may even be no such solution.

Transient Physical Modifications: PDNPulse is not designed as a tamper-evident technology and attacks that can be undone, or are not persistent physical modifications, are outside its scope. One possible attack can be de-soldering, maliciously programming, then re-soldering the memory chip [1]. However, such attack can be caught by software integrity verification [52].

VII. Discussion and Future Work

Please note that PDNPulse could suffer detection failures when insufficient or inappropriate ports/voltage domains are measured. We have analyzed its robustness to port selection (e.g., Fig. 5 and 9) in multi-port detection. However, the strategy for determining the minimum number of ports and the most appropriate port/voltage domain is device-specific and anomaly-specific. We plan to investigate it with a complex distributed simulation model in future work.

In practical conditions, the tolerance of the golden model can be affected by various factors such as production process and manufacturing defects, making it challenging to determine the optimal deviation value. One limitation of our proposed method, PDNPulse, is that it can be difficult to distinguish between manufacturing flaws and malicious modifications in a PCB, as both can result in anomalies. For example, as shown in Fig. 5(c), the impedance profile of the M3 board is surprisingly different from the others, but we could not see any difference between the M3 and the other four malicious boards. That is, confusion about manufacturing flaws and malicious modifications may lead to a false security alarm. Interpreting the PDN impedance profile can solve this issue and will be a focus of our future work.

We have shown that PDNPulse is robust to non-anomaly changes such as de-soldering and replacing with the same IC (e.g., Fig. 7(e)) as well as typical process variation (e.g., Fig. 10 (b)). However, to prevent false positives, the process variation due to different batches/vendors should be included in building the golden model. For instance, in Fig. 6(f), due to the large process variation between chip batches, directly applying the FD' algorithm will yield false positives. Our FD'-KNN method can effectively deal with such situations by classifying the board under test into multiple vendors/batches, as shown in Sec.V-C.2.

One of the salient features of PDNPulse is it has no hardware overhead and can be applied to legacy PCBs without any modifications. Potential PCB changes such as adding test points connected to the PDN can be made to increase PDNPulse's stability and performance. A PDNPulse-aware PCB design framework will be our future direction, which can efficiently insert PDN test points during the design stage.

VIII. Related Work

Facing numerous board-level attacks, detection methods have been developed, but they are often piecemeal solutions, capable of identifying only a particular attack under specific restrictions.

A. Reverse Engineering and Image Inspections

Reverse engineering [11], [18] provide most comprehensive detection, but it suffers from long detection time and high cost, and it is destructive. Image inspection methods can be divided into surface imaging and volumetric imaging. Surface imaging uses such as visible light [59] and interferometry [33] to detect anomalies. Cameras or microscopes are needed to detect the change of PCB surface pattern [28] or to visually examine

PCBs [13]. However, surface imaging cannot detect sophisticated counterfeits. For volumetric imaging using radiation, X-ray [7], [28] is commonly applied to comprehensively capture the internal structure of PCBs, which also suffers high cost and needs to de-solder components. In contrast, our method does not require expensive optical/X-ray equipment and can be conducted with a standard VNA.

B. Side-Channel Analysis

System-level delay side-channel information (such as based on JTAG [25], I2C [47]), power side-channel information [42], or combined multiparameter side-channel analysis [17] can be utilized to perform anomaly detection and run-time monitoring. Although, power and delay side-channel leakage are fundamentally caused by the PDN of target devices, their analysis is usually limited to specific anomaly types and offers only partial PCB area coverage. Rather than relying on leaked information, we directly measure the PDN and thus can retrieve more in-depth information.

C. Impedance Measurement

The changes to impedance patterns, resonant frequency, signal response of the trace, bus, or transmission line can be measured to detect anomalies [16], [21], [32], [39], [57], [61], [62]. However, due to using parts of the PCB design (e.g., bus), these approaches can only detect the anomalies attached to this trace, limiting both detectable anomaly types and locations. Since PDNPulse is based on the PDN, which is connected to each part of the system, the coverage of detection is significantly increased.

D. PDN Impedance-based Measurement

PDN impedance-based detection has been explored in various ways [36], [55]. As discussed in Sec.I, although successful, existing PDN impedance solutions only focus on specific types of anomalies and parts features (e.g., impedance at fixed frequencies) of the local PDN. Our work comprehensively explores the characteristics of PDN of the whole PCB. We specify the systematic analysis of PDN effects and the experimental setup for accurate multi-port, multi-domain PDN measurements and demonstrate experimentally PDNPulse's robustness to probe location, PCB scale, and port numbers. Our extensive experimental results show PDNPulse's effectiveness in detecting board-level attacks and counterfeiting.

In recent work [34], [35], the authors proposed a PCB tampering and counterfeit detection framework based on monitoring changes in the scatter parameters (i.e., S-parameters) of the PDN. Our work, PDNPulse, is distinct from this approach as we utilize multi-port and multi-domain detection, measuring transfer impedance between ports to detect system-level anomalies. Additionally, we use Z-parameters, which are commonly used in modeling PDN [22], [31], [43], [53], allowing for direct comparison with simulation results to better interpret and model the impacts of anomalies. Our measurement setup also utilizes a customized probe that can be applied to legacy systems and attached to any point on the PCB, eliminating the need for hardware modifications and allowing for multi-port detection. Our experiments cover a wide range of PCBs, demonstrating the robustness and effectiveness of our proposed method in various design scenarios. Overall, our work achieves a unique contribution to the field.

IX. Conclusion

We propose a novel board-level attack detection framework named PDNPulse. It leverages the inherent sensitivity of the on-board PDN to reliably authenticate that a PCB is free from tampering and/or anomalies. It is light-weight and compatible with legacy systems, and requires no hardware overheads or design modifications for deployment. We conduct extensive experiments on custom and COTS PCBs covering different design scales, anomaly types, and threat models. We demonstrate that PDNPulse can capture a wide range of threats at a low cost.

References

[1] DEF CON. (2017). *All Your Things are Belong to us*. [Online]. Available: https://www.exploitee.rs/

[2] (2020). *Arduino Due*. [Online]. Available: https://store.arduino.cc/usa/due

[3] (2020). *Beaglebone-Wireless*. [Online]. Available: https://github.com/beagleboard/beaglebone-black-wireless

[4] (2023). *Statistical Estimation and Error Bars—Seaborn*. [Online]. Available: https://seaborn.pydata.org/tutorial/error_bars.html#percentile-interval-error-bars

[5] (2023). *Wikipedia: Series and Parallel Circuits*. [Online]. Available: https://en.wikipedia.org/wiki/Serie and parallel circuits

[6] Arduino.CC. (2021). *Arduino Uno Rev3*. Accessed: Apr. 2021. [Online]. Available: https://store.arduino.cc/usa/arduino-uno-rev3

[7] N. Asadizanjani, S. Shahbazmohamadi, M. Tehranipoor, and D. Forte, "Non-destructive PCB reverse engineering using X-ray micro computed tomography," in *Proc. Int. Symp. Test. Failure Anal.*, Nov. 2015, pp. 1–5.

[8] M. S. Awal, A. Madanayake, and M. T. Rahman, "Nearfield RF sensing for feature-detection and algorithmic classification of tamper attacks," *IEEE J. Radio Freq. Identificat.*, vol. 6, pp. 490–499, 2022.

[9] S. Bhunia and M. Tehranipoor, *Hardware Security: A Hands-On Learning Approach*. San Mateo, CA, USA: Morgan Kaufmann, 2018.

[10] E. Bogatin, *Signal and Power Integrity–Simplified*. London, U.K.: Pearson, 2010.

[11] U. J. Botero et al., "Hardware trust and assurance through reverse engineering: A survey and outlook from image analysis and machine learning perspectives," 2020, *arXiv:2002.04210*.

[12] National Instruments Corp. (2023). *Short-Open-Load-Through (Solt) Calibration*. [Online]. Available: https://www.ni.com/docs/en-US/bundle/ni-vna/page/vnahelp/calibration solt.html

[13] T. J. Mazon De Oliveira, M. A. Wehrmeister, and B. T. Nassu, "Detecting modifications in printed circuit boards from fuel pump controllers," in *Proc. 30th SIBGRAPI Conf. Graph., Patterns Images (SIBGRAPI)*, Oct. 2017, pp. 87–94.

[14] T. Eiter and H. Mannila, "Computing discrete fréchet distance," Christian Doppler Lab. Expert Syst., Tech. Univ. Vienna, Vienna, Austria, Tech. Rep. CD-TR 94/64, 1994.

[15] C. Flynn, "I, for one, welcome our new power analysis overlords," presented at the Black Hat USA, vol. 2018, 2018. [Online]. Available: https://i.blackhat.com/us-18/Wed-August-8/us-18-OFlynn-I-For-One-Welcome-Our-New-Power-Analysis-Overloards.pdf

[16] D. Fujimoto, S. Nin, Y. Hayashi, N. Miura, M. Nagata, and T. Matsumoto, "A demonstration of a HT-detection method based on impedance measurements of the wiring around ICs," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 10, pp. 1320–1324, Oct. 2018.

[17] S. Ghosh, A. Basak, and S. Bhunia, "How secure are printed circuit boards against trojan attacks?" *IEEE Des. Test*, vol. 32, no. 2, pp. 7–16, Aug. 2014.

[18] J. Grand, "Printed circuit board deconstruction techniques," in *Proc. 8th USENIX Workshop Offensive Technol. (WOOT)*, 2014, p. 1.

[19] A. Greenberg. (2019). *A New Proof-of-Concept Hardware Implant Shows how Easy it May be to Hide Malicious Chips Inside it Equipment*. [Online]. Available: https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/

[20] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.

[21] Z. Guo, X. Xu, M. M. Tehranipoor, and D. Forte, "MPA: Model-assisted PCB attestation via board-level RO and temperature compensation," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, Oct. 2017, pp. 25–30.

[22] M. S. Gupta, J. L. Oatley, R. Joseph, G.-Y. Wei, and D. M. Brooks, "Understanding voltage variations in chip multiprocessors using a distributed power-delivery network," in *Proc. Design, Autom. Test Eur. Conf. Exhib.*, Apr. 2007, pp. 624–629.

[23] J. Harrison, N. Asadizanjani, and M. Tehranipoor, "On malicious implants in PCBs throughout the supply chain," *Integration*, vol. 79, pp. 12–22, Jul. 2021.

[24] J. He, Y. Zhao, X. Guo, and Y. Jin, "Hardware trojan detection through chip-free electromagnetic side-channel statistical analysis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 10, pp. 2939–2948, Oct. 2017.

[25] A. Hennessy, Y. Zheng, and S. Bhunia, "JTAG-based robust PCB authentication for protection against counterfeiting attacks," in *Proc. 21st Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2016, pp. 56–61.

[26] MACOMTechnology Solutions Inc. (2021). *Ma4e1340 Series Datasheet*. Accessed: Jul. 30, 2021. [Online]. Available: https://cdn.macom.com/datasheets/MA4E1340%20Series.pdf

[27] Intel. (2015). *Using the Altera PDN Tool to Optimize Your Power Delivery Network Design*. Accessed: Apr. 30, 2020. [Online]. Available: https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/an/an750.pdf

[28] T. Iqbal and K.-D. Wolf, "PCB surface fingerprints based counterfeit detection of electronic devices," *Electron. Imag.*, vol. 29, no. 7, pp. 144–149, Jan. 2017.

[29] C. F. Jekel, G. Venter, M. P. Venter, N. Stander, and R. T. Haftka, "Similarity measures for identifying material parameters from hysteresis loops using inverse analysis," *Int. J. Mater. Forming*, vol. 12, no. 3, pp. 355–378, May 2019.

[30] J. Kim et al., "Chip-package hierarchical power distribution network modeling and analysis based on a segmentation method," *IEEE Trans. Adv. Packag.*, vol. 33, no. 3, pp. 647–659, Aug. 2010.

[31] W. Kim, M. S. Gupta, G.-Y. Wei, and D. Brooks, "System level analysis of fast, per-core DVFS using on-chip switching regulators," in *Proc. IEEE 14th Int. Symp. High Perform. Comput. Archit.*, Feb. 2008, pp. 123–134.

[32] M. McGuire, U. Ogras, and S. Ozev, "PCB hardware trojans: Attack modes and detection strategies," in *Proc. IEEE 37th VLSI Test Symp. (VTS)*, Apr. 2019, pp. 1–6.

[33] D. Mehta et al., "The big hack explained: Detection and prevention of PCB supply chain implants," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 16, no. 4, pp. 1–25, Oct. 2020.

[34] T. Mosavirik, F. Ganji, P. Schaumont, and S. Tajik, "ScatterVerif: Verification of electronic boards using reflection response of power distribution network," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 18, no. 4, pp. 1–24, Oct. 2022.

[35] T. Mosavirik, P. Schaumont, and S. Tajik, "Impedanceverif: On-chip impedance sensing for system-level tampering detection," Cryptol. ePrint Arch., Tech. Rep., 2022.

[36] M. Nishizawa, K. Hasegawa, and N. Togawa, "Capacitance measurement of running hardware devices and its application to malicious modification detection," in *Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS)*, Oct. 2018, pp. 362–365.

[37] D. I. Novak and J. R. Miller, *Frequency-Domain Characterization of Power Distribution Networks*, vol. 1. Norwood, MA, USA: Artech House, 2007.

[38] *Dod Budget Request*, Office Under Secretary Defense (Comptroller)/ CFO, Washington, DC, USA, 2020.

[39] S. Paley, T. Hoque, and S. Bhunia, "Active protection against PCB physical tampering," in *Proc. 17th Int. Symp. Quality Electron. Design (ISQED)*, Mar. 2016, pp. 356–361.

[40] S. D. Paul and S. Bhunia, "SILVerIn: Systematic integrity verification of printed circuit board using JTAG infrastructure," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 17, no. 3, pp. 1–28, Jul. 2021.

[41] M. Pecht and S. Tiku, "Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectr.*, vol. 43, no. 5, pp. 37–46, May 2006.

[42] G. Piliposyan, S. Khursheed, and D. Rossi, "Hardware trojan detection on a PCB through differential power monitoring," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 2, pp. 740–751, Apr./Jun. 2020.

[43] L. Ren et al., "Frequency-dependent via inductances for accurate power distribution network modeling," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 2009, pp. 63–68.

[44] J. Robertson and M. Riley, "The big hack: How China used a tiny chip to infiltrate U.S. companies," Bloomberg Businessweek, vol. 4, 2018.

[45] *A Journey Towards a Sustainable Future: Sustainability in the Samsung Supply Chain*, Samsung, Seoul, South Korea, 2019.

[46] S. M. Sandler, "Extending the usable range of the 2-port shunt through impedance measurement," in *Proc. IEEE MTT-S Latin Amer. Microw. Conf. (LAMC)*, Dec. 2016, pp. 1–3.

[47] O. Shwartz, A. Cohen, A. Shabtai, and Y. Oren, "Inner conflict: How smart device components can cause harm," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101665.

[48] W. M. M. Thornberry, "National defense authorization act for fiscal year 2021," *Public Law*, vol. 116, p. 283, 2021.

[49] R. Soman, S. K. Singh, T. Wandowski, and P. Malinowski, "Development of robust metric based on cumulative electrical power for electromechanical impedance based structural health monitoring," *Smart Mater. Struct.*, vol. 29, no. 11, Nov. 2020, Art. no. 115047.

[50] P. Staat, J. Tobisch, C. Zenger, and C. Paar, "Anti-tamper radio: System-level tamper detection for computing systems," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2022, pp. 1722–1736.

[51] STH. (2015). *Comparison: Intel i350-t4 Genuine vs Fake*. Accessed: Apr. 2021. [Online]. Available: https://forums.servethehome.com/index.php?threads/comparison-intel-i350-t4-genuine-vs-fake.6917/

[52] G. E. Suh, D. Clarke, B. Gasend, M. V. Dijk, and S. Devadas, "Efficient memory integrity verification and encryption for secure processors," in *Proc. 36th Annu. IEEE/ACM Int. Symp. Microarchitecture (MICRO)*, Dec. 2003, pp. 339–350.

[53] M. Swaminathan, J. Kim, I. Novak, and J. P. Libous, "Power distribution networks for system-on-package: Status and challenges," *IEEE Trans. Adv. Packag.*, vol. 27, no. 2, pp. 286–300, May 2004.

[54] M. Tehranipoor et al. (2017). *Invasion of the Hardware Snatchers Cloned Electronics Pollute the Market*. [Online]. Available: https://spectrum.ieee.org/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

[55] X. Wang, Y. Han, and M. Tehranipoor, "System-level counterfeit detection using on-chip ring oscillator array," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2884–2896, Dec. 2019.

[56] L. Wei, B. Luo, Y. Li, Y. Liu, and Q. Xu, "I know what you see: Power side-channel attack on convolutional neural network accelerators," in *Proc. 34th Annu. Comput. Secur. Appl. Conf.*, Dec. 2018, pp. 393–406.

[57] T. Wei and J. Huang, "Transmission line identification via impedance inhomogeneity pattern," *IEEE J. Radio Freq. Identificat.*, vol. 3, no. 4, pp. 245–251, Dec. 2019.

[58] Wikipedia. (2021). *List of Battery Sizes*. Accessed: 2021. [Online]. Available: https://en.wikipedia.org/wiki/List_of_battery_sizes

[59] F. Xie, A. Uitdenbogerd, and A. Song, "Detecting PCB component placement defects by genetic programming," in *Proc. IEEE Congr. Evol. Comput.*, Jun. 2013, pp. 1138–1145.

[60] Xilinx. (2012). *Device Package User Guide UG112*. Accessed: Apr. 2021. [Online]. Available: https://www.xilinx.com/support/documentation/user_guides/ug112.pdf

[61] Z. Xu, T. Mauldin, Z. Yao, S. Pei, T. Wei, and Q. Yang, "A bus authentication and anti-probing architecture extending hardware trusted computing base off CPU chips and beyond," in *Proc. ACM/IEEE 47th Annu. Int. Symp. Comput. Archit. (ISCA)*, May 2020, pp. 749–761.

[62] F. Zhang, A. Hennessy, and S. Bhunia, "Robust counterfeit PCB detection exploiting intrinsic trace impedance variations," in *Proc. IEEE 33rd VLSI Test Symp. (VTS)*, Apr. 2015, pp. 1–6.

[63] H. Zhu, X. Guo, Y. Jin, and X. Zhang, "PowerScout: A security-oriented power delivery network modeling framework for cross-domain side-channel analysis," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, Dec. 2020, pp. 1–6.

[64] H. Zhu, X. Guo, Y. Jin, and X. Zhang, "PCBench: Benchmarking of board-level hardware attacks and trojans," in *Proc. 26th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2021, pp. 396–401.