RF Fingerprinting: Hardware-Trustworthiness Enhancement in the Hardware Trojan Era

Noemí Miguélez-Gómez and Eduardo A. Rojas-Nastrucci

©SHUTTERSTOCK.COM/POPTIKA

Ensuring the security of wireless networks entails ensuring the authenticity, confidentiality, integrity, and availability of the data exchanged through them. In this data-dependent era, global communications systems have been experiencing rapid increases in the amount of data shared daily, thanks to the evolution of technologies that enable low-cost and ubiquitous wireless connectivity. In the last two decades, there has been a continuous increase in wireless traffic due to wireless technology advancements and a wide range of applications, and the increase in wireless network users [1], [2]. Although the total annual

Noemí Miguélez-Gómez (miguelen@my.erau.edu) and Eduardo A. Rojas-Nastrucci (rojase1@erau.edu) are with the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114 USA.

Digital Object Identifier 10.1109/MMM.2023.3303591

Date of current version: 5 October 2023

Among the different HT detection and prevention methods, fingerprint-based mechanisms are one of the most popular in the research community due to their capabilities.

Internet traffic was a few exabytes of data fewer than 15 years ago, more than two hundred exabytes have been reached in the last two years. Moreover, by next year, the average Wi-Fi speed is predicted to be 92 Mb/s, up from 30 Mb/s in 2018 [3], [4]. This evolution has been driven by user demand, which includes higher data rates and broader coverage and bandwidth capabilities in wireless networks. Promising updates for current communication tools are in the making, but the boom in the amount of the data shared by them is making global communication systems a larger and easier target for security attacks [5], [6].

Although a wide range of software-based security attacks have been documented and assessed by sophisticated cybersecurity tools, hardware or physical-layer security attacks have gained ground too and are not as well evaluated. Recent advancements in wireless networks require changes in hardware and software tools. Due to the sophistication of the integrated circuits (ICs) used in wireless network hardware, the number of entities that are a part of their lifecycle is growing, including a large number of companies. Unfortunately, this increase in the number of actors has contributed to the proliferation of malicious hardware-based operation and function vulnerabilities added to ICs, such as hijacking of RF transceiver (Internet Protocols) IPs [64] and hardware Trojans (HTs) [7].

Hardware attacks have been increasingly reported in the last decades. From 1996 to 2005, a few individual hardware attacks were reported, such as timing or power analysis attacks, aimed at extracting information on either power dissipation or computation time for specific operations of the IC under attack [8], [9]. In 2007, the concept of an HT was introduced after several hardware attacks involving the production and supply of ICs with malicious hardware were reported, with the first incident reported in 2005 [10]. Considering the unpredictable characteristics of HTs, there is a need for defense mechanisms that protect wireless communications systems against this type of security attack.

The effectiveness of hardware-based malicious attacks and of the defense mechanisms against them are studied to enable HT detection and to provide countermeasures that enhance the security of wireless systems [11], [12]. With the growth of novel manufacturing techniques such as additive manufacturing (AM), inherent characteristics of the devices can be engineered to provide distinct features among devices [13]. Leveraging unintentional manufacturing defects and engineered electromagnetic (EM) features that traditional manufacturing cannot achieve, AM techniques can impact and benefit future fingerprinting-based countermeasures for HT detection and other security applications [13]. The most common prevention mechanisms for HTs are based on digital modules that allow data encryption and authentication, but there is not a specific prevention or detection model that fits all types of HTs. Due to the effectiveness of HTs and their ability to evade detection, sophisticated countermeasures are being analyzed and adopted. Although some countermeasures can be intrusive, costly, and difficult to perform, RF fingerprint-based mechanisms provide capabilities that take advantage of the variety of IC and system inherent features, novel technologies, and manufacturing techniques.

This article presents an overview of diverse HT attacks and defense mechanisms for wireless networks. In most cases, malicious hardware takes advantage of the hardware functionality of the communication links, such as error-correction blocks or the unused bits of data protocols, to leak sensitive information that is exchanged as a part of the legitimate communications link. Other attacks include exploitation of the margins of the operational specifications of the ICs to remain undetected [14], [15], [16], [17]. The most common countermeasures are based on hardware isolation, side-channel analyses, and reverse engineering, allowing the detection of specific malicious electronic parts by inspection and analysis of the hardware and involved signals of the system [18], [19], [20], [21], [22], [23], [24]. Among the different HT detection and prevention methods, fingerprint-based mechanisms are one of the most popular in the research community due to their capabilities [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59]. By taking advantage of inherent features of the IC and the system, fingerprint-based countermeasures present low-cost, low-complexity, and nondestructive alternatives to other countermeasures that are focused on specific anticipated HT attacks and entail costly procedures that can damage the devices and degrade performance of the system. Figure 1 presents the main concept used in RF fingerprinting-based countermeasures, where a monolithic microwave IC (MMIC) that contains hardware modifications (HTs) modifies the fingerprint of the input RF signal. By analyzing features of the signal's fingerprint, alterations caused by the presence of hardware modifications are detected, thus successfully detecting HTs. Power consumption, temperature, or EM emanations, among other features

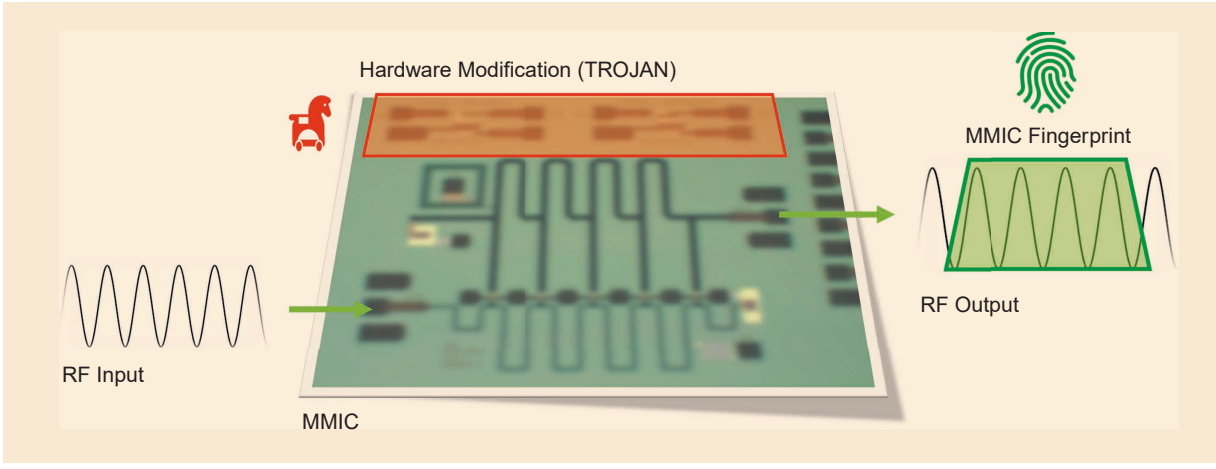

Figure 1. *A visualization of HT insertion into the monolithic microwave IC (MMIC) used in wireless networks.*

and methods, can be used to create fingerprints of the ICs to confirm that they are Trojan free.

This article is presented as follows. The "The Basics of HTs" section introduces the concepts of HTs, and the "Wireless Network Vulnerabilities" section discusses the vulnerabilities they present in wireless networks. The "Threat Models and Attack Analyses for Malicious Hardware" section presents the most common threat models and attacks. The "Analysis of Countermeasures" section discusses the state of the art of detection and prevention of malicious modifications of the electronic hardware in wireless networks. Finally, the "Unanticipated HT Countermeasures: The Future of Communication Trustworthiness," "RF Fingerprinting Beyond HT Detection," and "Conclusions" sections present some conclusions and considerations for HT detection and prevention using fingerprinting-based mechanisms, such as RF fingerprinting, and the use of these techniques for other aspects of hardware security.

The Basics of HTs

HTs are additions to or modifications of a circuit that have malicious purposes. They are one of today's most dangerous and challenging threats as they can be implanted in security-weak parts of a chip and steal the internal security protocols and keys, or they can modify the original functionality of the device, among other wireless system attacks [7], [11]. HTs can be implanted at practically any point of the IC lifecycle, presenting risks for even the most sensitive and protected applications, such as CAD tools or wafer and mask manufacturing.

HTs can be classified by their physical representation, activation phase (triggers), and action phase or malicious function (payload). HT triggers can follow different patterns and events, and they present sophisticated characteristics and different attack effectiveness, making them challenging to predict during testing of the hardware of the affected device. Figure 2 presents a diagram of the baseline of an HT design and different types of HTs: the combinational Trojan activated by different conditions that occur at the same instant, and the sequential Trojan activated by different conditions that occur sequentially. Detection and prevention of HTs is challenging as they cannot be virtually removed after fabrication and they are difficult to remedy in their application phase. The detection of HTs through conventional postmanufacturing tests

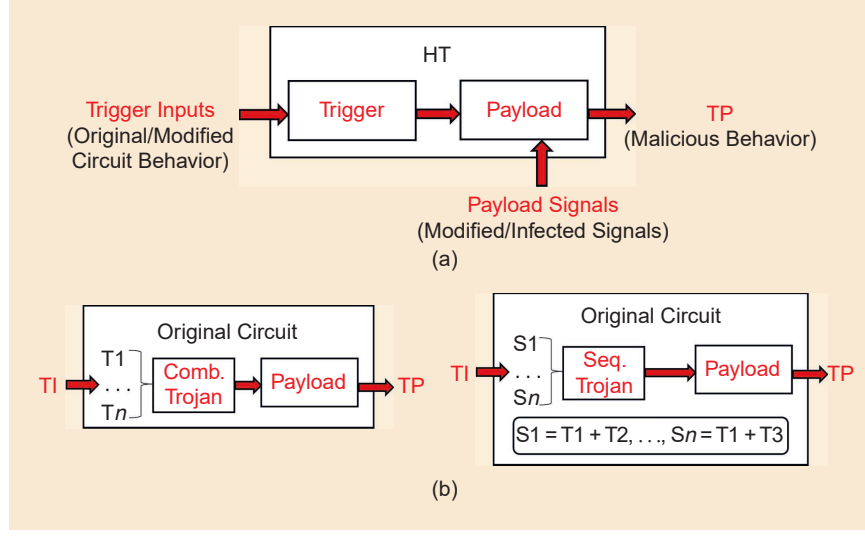

Figure 2. *The general structure of an HT in a design, and models of combinational (Comb.) and sequential (Seq.) HTs [7]. TI: Trojan infested.*

The physical layer is vulnerable to the eavesdropping and jamming attacks that can be achieved using malicious hardware vulnerabilities inserted in the ICs.

is difficult as well; hence, mechanisms must be constantly analyzed and their risk assessed, and countermeasures must be constantly updated by the research community [49].

Wireless systems have become an attractive target for HT attacks due to the growth of wireless communications infrastructures in the last decades and the risks and vulnerabilities they present. In communications systems, an HT can control, modify, disable, or monitor the data link contents. The design of Trojans to leak or monitor data in wireless networks usually considers two principles: the position/source of the leaked or contaminated data and contamination rate. The position of the data affects how undetectable the malicious hardware can be, while the contamination rate is how much the HT activity contaminates the data or legitimate activity of the IC under attack, which also affects the detectability or traceability of the hardware modifications.

Wireless Network Vulnerabilities

Today, wireless networks are used in most electronic systems, sharing sensitive information that relies on the trustworthiness of their ICs. Wireless networks adopt an open systems interconnection-layered protocol architecture, which includes physical, media access control (MAC), network, transport, and application layers. For all these layers, wireless networks must comply with the following set of minimum-security requirements to protect data against adversarial attacks: authenticity, confidentiality, integrity, and availability. However, the security mechanisms adopted in these layers add configuration and setup complexities and may cause overall network performance degradation; and the systems are still vulnerable to security attacks. Figure 3 presents layers of the wireless protocol architecture and examples of attacks [5]. IP and MAC spoofing are the main attack vulnerabilities for the network and MAC layers, respectively. The physical layer is vulnerable to the eavesdropping and jamming attacks that can be achieved using malicious hardware vulnerabilities inserted in the ICs.

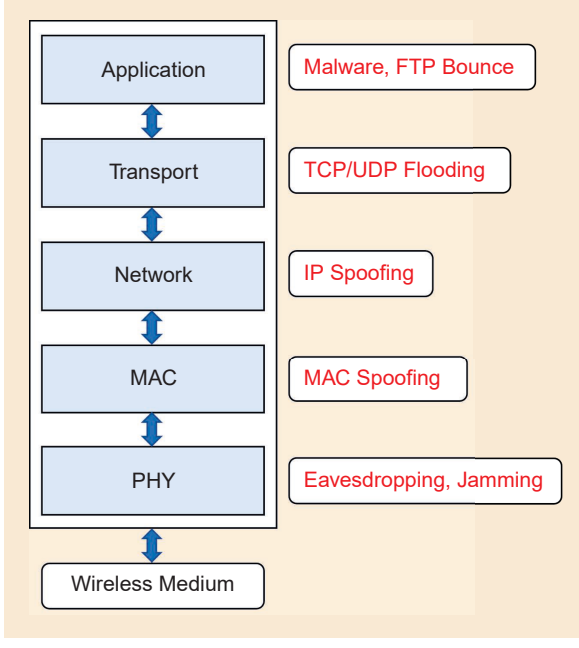

Figure 3. *A standard open systems interconnection protocol architecture for wireless networks [5]. UDP: User Datagram Protocol; PHY: physical layer.*

The ICs used in wireless applications allow a margin of error from the expected operational ranges, such as frequency range or the device's output power and sensitivity, where not even their encryption mechanism can protect the confidentiality of the information they exchange. These performance metric margins are due, among other reasons, to the fact that circuits are designed with enough tolerance to obtain a high yield in the manufacturing process and lower production costs. Moreover, optimal transmission and reception capabilities require intellectual property (IP) considerations and high computational complexity. These operational margins facilitate the addition of malicious hardware that can remain undetected during normal operation of the device [6]. Under nominal operation, the system is expected to be limited by its specifications, and thus, unexpected functions can be performed between the acceptable and the specified margins of operation, without presenting unforeseen performance that could trigger detection [12].

Beyond how ICs' design and fabrication practices can enable HTs, the overall operation concept and wireless communications protocols make the physical layer vulnerable to attack. Two main attacks are considered as a part of this layer: eavesdropping and jamming. Eavesdropping attacks include unauthorized access to shared data, while jamming attacks present denial-of-service characteristics, preventing authorized users from accessing wireless network resources [7]. Among other attack mechanisms, HTs can take advantage of the modification of channel state information to alter it without being detected and exploit unused frame bits to hide additional information and perform unauthorized transmissions that give access to wireless network resources [11].

Threat Models and Attack Analyses for Malicious Hardware

Wireless networks have become targets for a variety of security attacks, especially HTs. To address the possible risks that HTs present to these networks, a series of studies of HT attacks and possible defense mechanisms has been performed by the research community. However, these analyses and studies must constantly be updated due to the unpredictability of malicious hardware insertion and new technology developments. To simplify the analysis of HT attacks, the main threat model discussed in this work is based on data leakage and monitoring and takes into account three actors or wireless nodes: a transmission source that contains an HT and leaks sensitive data (Alice), a legitimate receiver (Bob), and a rogue receiver that is intercepting the legitimate communications link, receiving the leaked information (Eve), as presented in Figure 4. The interruption, or jamming, of the legitimate communication should also be considered.

In data leakage and monitoring attacks, HTs usually trigger a mechanism that leaks sensitive data while the legitimate data are being transmitted, without affecting the communication quality and remaining undetected. Wireless devices rarely operate at the specified nominal performance ranges, which makes it easier to perform these types of attacks without the user experiencing malfunctions. The next sections detail the attacks that are commonly considered in the design of wireless networks and/or have a proven capability to exploit wireless IC vulnerabilities.

Amplitude Modulation

The load impedance used in wireless devices is not ideal due to parasitics and other imperfections of the manufacturing process of ICs. Consequently, an IC includes some margins of error in its specifications to manage the return losses generated by the differences in load impedance. HTs can take advantage of these margins to leak sensitive information while remaining undetectable during testing [15], [19], [63]. In [15], an HT mechanism that includes a switch that alters the input termination impedance of a power amplifier (PA) is described (see Figure 5). These alterations correlate with the bits of the leaked data, allowing access to the legitimately transmitted information by analyzing the amplitude of the leaked data.

Error-Correction Blocks

The baseband circuit of transmitters used in wireless networks, for example, using the IEEE 802.11 standard, includes error-control blocks to improve the quality of the message and to protect the data against noise sources from the communication link. Some of these blocks provide error-correction capabilities, such as forward error correction (FEC), which encodes the transmitted message using a predetermined codebook and adds protection to the channel. These error-correction blocks can be attacked with HTs to leak information. In [17], an FEC block is used to leak information with high data throughput to a rogue receiver, with minimal impact on the legitimate communication link. This is accomplished by replacing some of the user-encoded bits with rogue information, while the legitimate receiver perceives only a slight deterioration of the signal-to-noise ratio.

Noise Floor Considerations

Spread-spectrum techniques spread modulated signals over a much wider frequency band by multiplying them by a spreading code or sequence, presenting enhanced security against jamming and fading, among other advantages. HTs can take advantage of these techniques to send undetected signals below the noise floor and leak sensitive information, as presented in

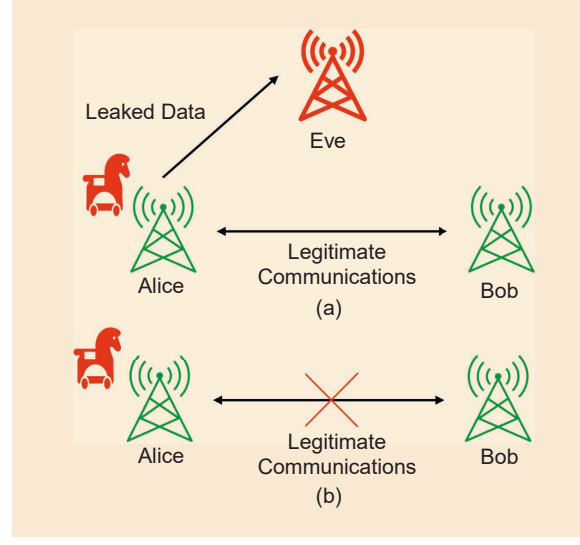

Figure 4. *(a) HT eavesdropping and (b) interruption attack models [15].*

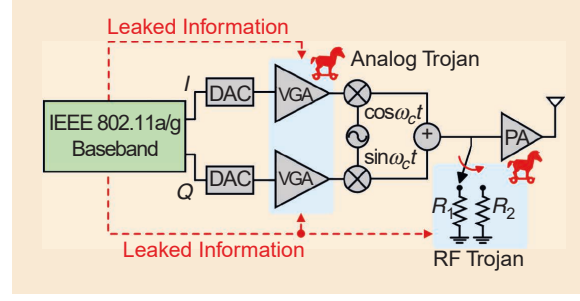

Figure 5. *An amplitude modulation HT attack model that alters the input termination impedance of a PA to leak information [49]. DAC: digital-to-analog converter; VGA: variable gain amplifier.*

Figures 6 and 7. The spectrum of the legitimate signal is practically identical to the spectrum of the signal with the additional leaked data/signal, making the HT activity undetectable. In [16], an HT attack that includes a code-division multiple access channel to hide information below the noise floor is presented. To hide the information, an encryption key is leaked using a different pseudorandom number (PN) sequence for each bit, where the modulated power-side channels are orthogonal to each other. Only the attacker knows the PN sequences and can demodulate the keys by analyzing the power traces.

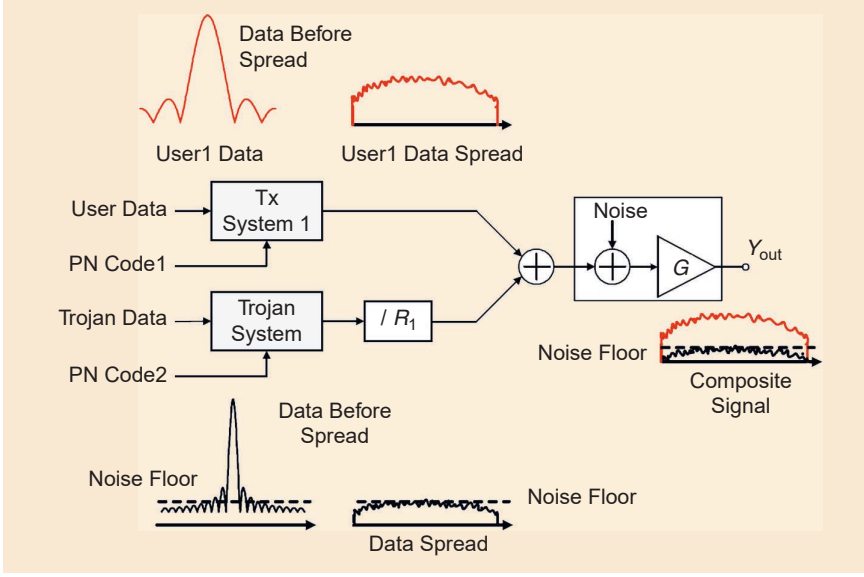

Figure 6. *The model for using spread-spectrum techniques for undetectable HT attacks in wireless networks [14]. Tx: transmitter; PN: pseudorandom number.*

Adaptive Channel Estimation

Wireless networks must consider path loss, fading, and interference conditions as a part of their performance. Based on that, wireless devices include channel estimation algorithms, normally considering the transmission of pilot symbols, to

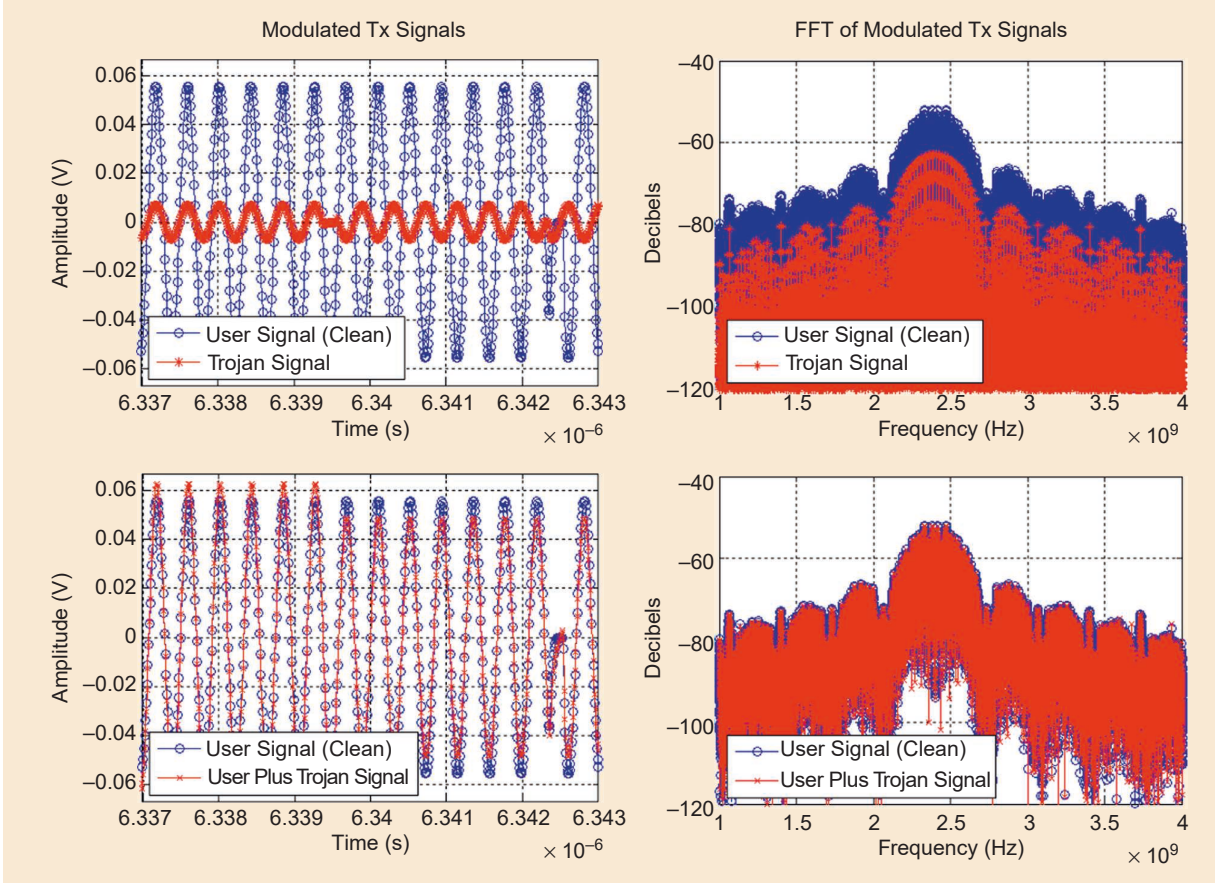

Figure 7. *Time and frequency domain representations of legitimate and leaked data transmissions [14]. Tx: transmitter; FFT: fast Fourier transform.*

estimate the channel conditions and get the transmitted signal. The symbols are known by the receiver and used to get the noise level of the received data and enhance it. However, these algorithms consider any noise source, including possible HTs, which can help the malicious hardware remain undetected [6]. Figure 8 presents the signal strength of the received contaminated signal, which includes both legitimate and leaked data. In this case, the malicious hardware considers the average signal strength for the duration of one rogue bit and increases/decreases the signal power above/below a target threshold to remain undetected. Secondary communication links or covert channels leaking information can be accomplished by taking advantage of the wireless system's ability to operate under different channel and signal conditions [60]. In [61] and [62], covert channels are achieved by applying modifications to the transmitted constellation, which are perceived as a part of the noise variability of the system. These methods can also be used as detection mechanisms for HTs because they impact parameters such as noise and reflection coefficients.

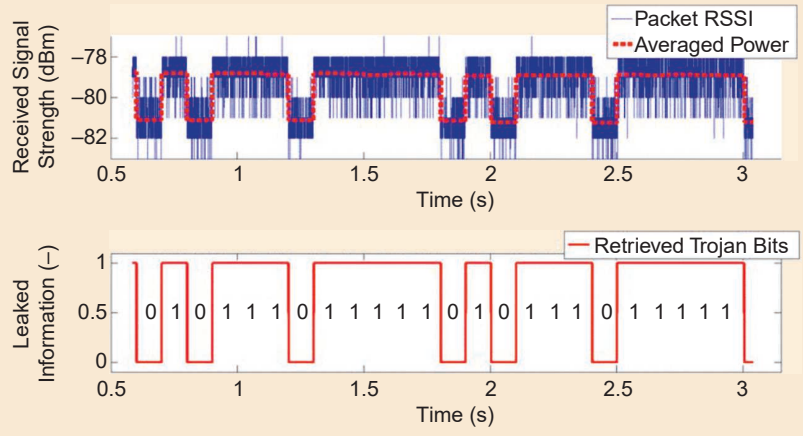

Figure 8. *Received signal strength with legitimate and leaked information adapting signal power: leaked data capability to be decoded [18]. RSSI: Received Signal Strength Indicator.*

Analysis of Countermeasures

There are different methods used for HT detection, but most of them require IC tests that are slow, difficult, and sometimes destructive for the components. As HTs can have different effects on the chip in which they are integrated, detection and prevention methods have been analyzed for specific HT attacks. These include a series of tests and checks based on assumptions about where the HT can be inserted or about its trigger and payload logic. Some of these methods involve additional hardware design or chip transitions, which adds difficulty to the testing and verification of the system. Countermeasures based on complete analyses of the chips to detect possible HTs without previous knowledge are important to consider. The next sections discuss the countermeasures commonly proposed by the research community to detect, monitor, or prevent HT attacks and have been proven effective for their respective specific HT attacks.

Adaptive Channel Estimation

Adaptive channel estimation methods can be used to detect specific HT attacks. In [17], a detection method is studied for an FEC block-based HT. In this case, noise characteristics are used to detect the malicious modifications of electronic hardware over different channel conditions, as shown in Figure 9. In [18], a method that uses an adaptive approach to isolate HT activity from the actual channel and device noise is presented. This is achieved by exploiting the slow-fading characteristics of indoor communication to distinguish between channel- and Trojan-induced impacts on the computed channel coefficient.

Formal Methods

The information flow of ICs can be tracked to detect HTs. In [20], a noninvasive method converts the netlist of the analog/RF circuitry to a Verilog representation to create a framework that automatically generates a series of tools to detect sensitive information leakage from the digital and analog domains. The basis of this information-flow tracking is the proof-carrying hardware intellectual property framework, which includes formal proofs of security properties in the hardware description language code of the components. This method presents some limitations as it can only be applied in the

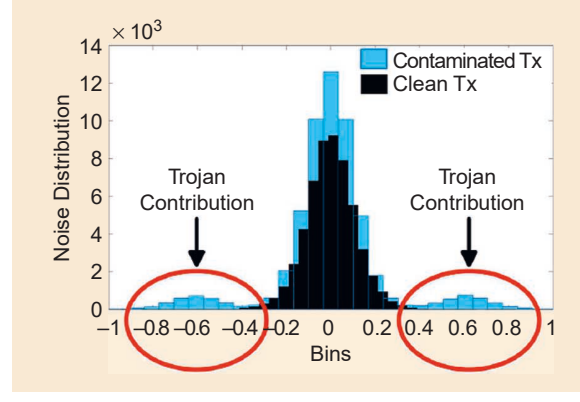

Figure 9. *Channel noise profiling against a constellation-changing Trojan: noise distribution at a signal-to-noise ratio of 15 dB [17]. Tx: transmitter.*

As HTs can have different effects on the chip in which they are integrated, detection and prevention methods have been analyzed for specific HT attacks.

digital domain and cannot detect HTs that the user does not anticipate, although in the analog domain, it can achieve flow tracking at the transistor level of the IC [21].

Hardware Isolation

Hardware-isolation mechanisms isolate the application runtime into different execution modes (normal and secure) to prevent unauthorized users from accessing data in the normal operation mode of the device. Different platforms facilitate different hardware-isolation techniques, such as ARM TrustZone, an isolation technology for ARM processors that is adopted on mobile systems. A hardware-isolation-based security primitive is presented in [22] to protect sensitive data on the target hardware system. In this case, an ARM platform is used to implement and evaluate an information-leakage HT in a malicious normal application, and security settings are applied and deployed in the TrustZone, which serves to separate the HT from the environment where the application is running so it cannot leak information, as presented in Figure 10. This approach successfully protects the information with only a small performance cost for the additional security, although it requires the aforementioned capabilities.

Reverse Engineering

Reverse engineering methods analyze the internal structure of ICs to get information about how they operate. As invasive methods, they include several time-consuming steps that can damage the devices:

- *Decapsulation*: removing the die from its package
- *Delayering*: stripping the layers of the die using chemical methods and polishing
- *Imaging*: getting a complete view of the layers using a scanning electron microscope (SEM)
- *Annotation*: annotating the complete structure of the device
- *Schematic creation, organization, and analysis*: generating a flat netlist from all the images and information gathered in the previous steps.

In [23], the authors propose a robust reverse engineering approach that uses machine learning methods to detect HT structures in the netlists of ICs, which can be missed by only comparing them with a golden model. Figure 11 presents an example of three types of Trojans identified by analyzing the SEM images of ICs.

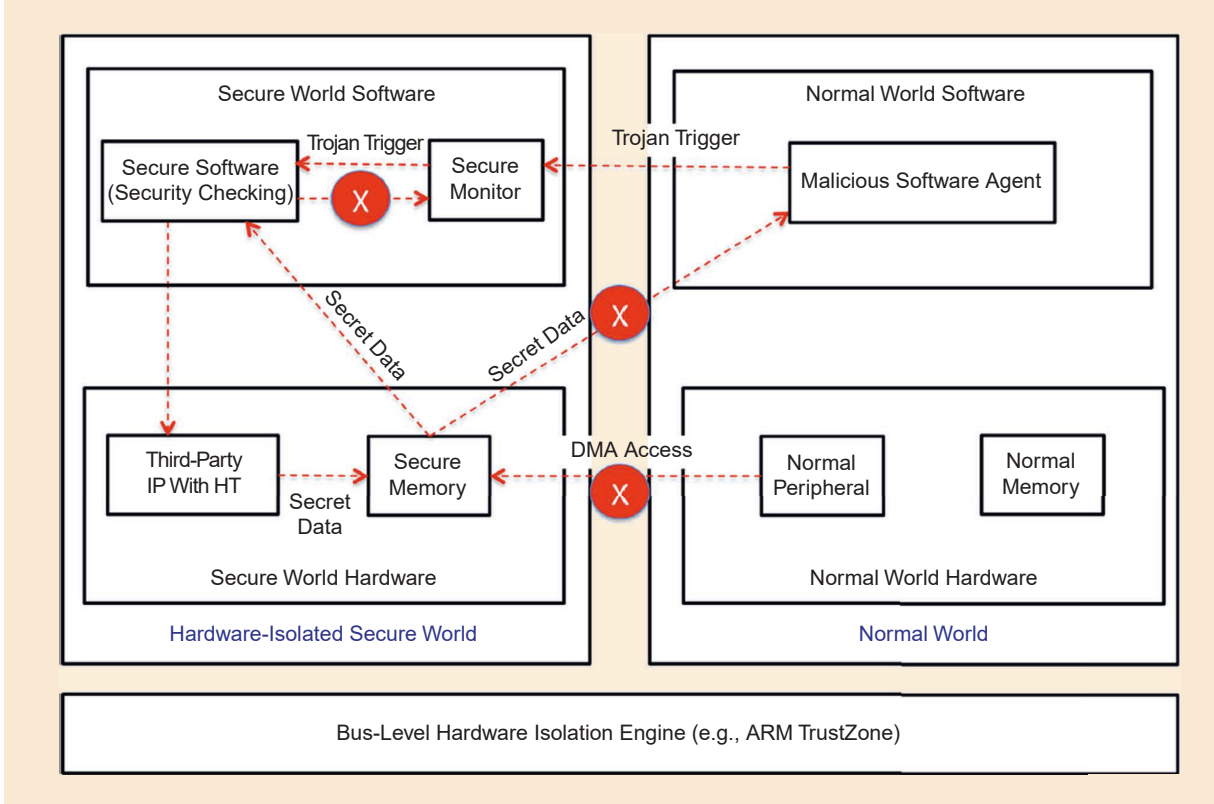

Figure 10. *A hardware-isolation framework that prevents information leakage from HT attacks [22]. DMA: direct memory access.*

Unanticipated HT Countermeasures: The Future of Communication Trustworthiness

As can be seen from the previously presented attacks, HTs are designed to be undetected and they are often unpredictable. Hence, a wide range of countermeasures are being studied by the research community to detect and prevent these malicious actions. Some of these mechanisms require the anticipation or estimation of aspects of HTs to analyze the target devices and confirm that they can be trusted, as presented in Table 1. Hence, there is a need for blind countermeasures that, without any previous knowledge of the specifics of the threat, can protect the sensitive information that wireless networks exchange by detecting Trojan-infected ICs.

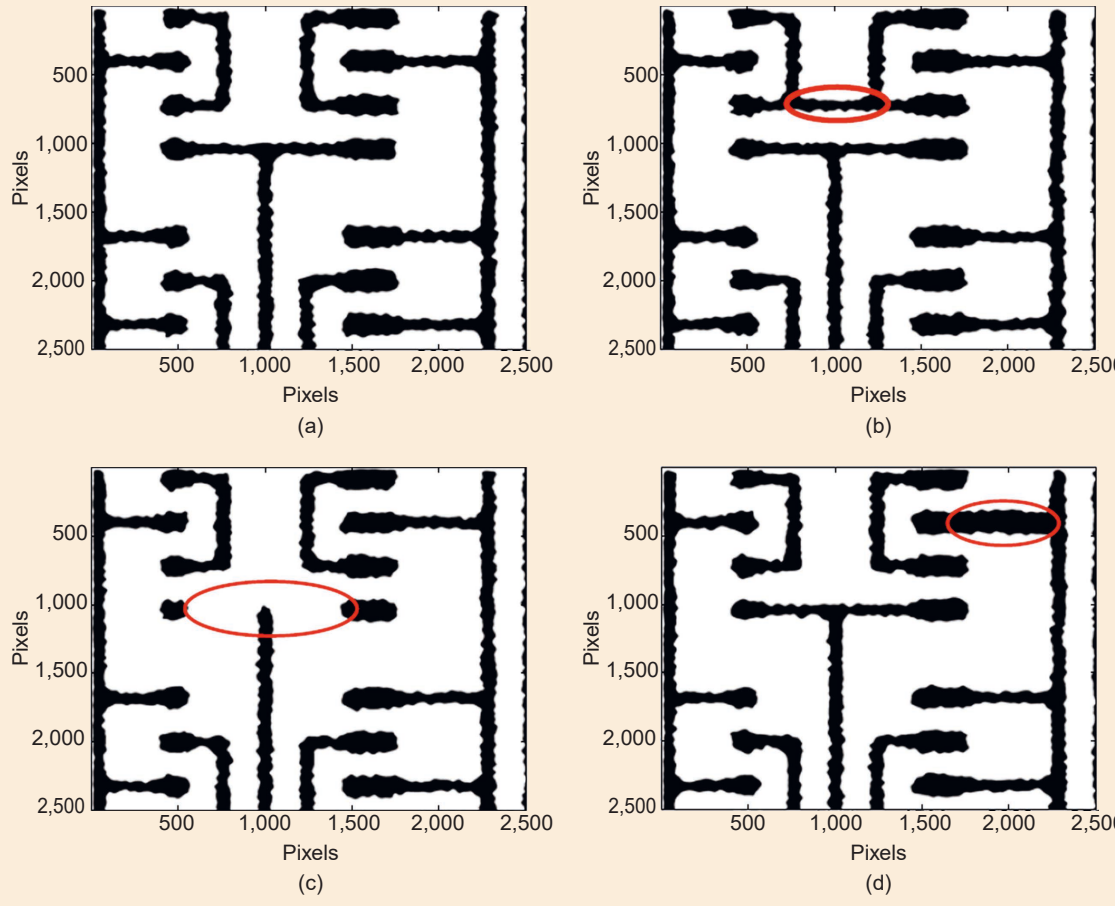

Figure 11. *The three Trojans identified in the SEM images of metal 1 layer. (a) Trojan free, (b) Trojan addition, (c) Trojan deletion, and (d) Trojan parametric [23].*

TABLE 1. A comparison of HT attack countermeasures.

Type	Attack Detection	Anticipated Information	Intrusive	Costly	Time Consuming	Additional Tools	References
Adaptive channel estimation	AM, SS/CDMA	Yes	No	No	Usually	Yes	[17], [18]
Formal methods	Nonspecific	Yes	No	Yes	Yes	Yes	[20], [21]
Hardware isolation	Nonspecific	No	Yes/No	Yes	Usually	Yes	[22]
Reverse engineering	Nonspecific	Yes	Yes	Yes	Yes	Yes	[23]

CDMA: code-division multiple access; SS: signal spectrum.

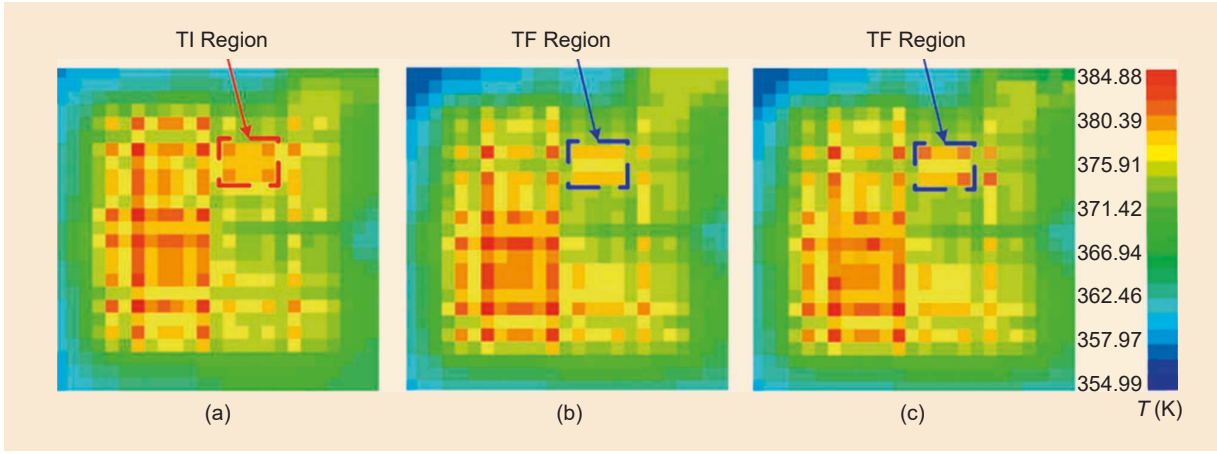

Figure 12. *Thermal maps of ICs at different timings. (a) A TI IC at t1. (b) A Trojan-free (TF) IC t2. (c) A TF IC at t3 [31].*

What Is RF Fingerprinting?

The inherent characteristics of the devices used in wireless networks can be used to create a fingerprint based on either signals generated by them or on their response to external signals (side channels) [25], [26]. HTs require a specific structure to perform their attacks, which can alter certain features of legitimate ICs, modifying their previously analyzed fingerprints. These fingerprints can be sufficient to statistically identify whether the IC can be trusted and to expose the HT. Fingerprint-based countermeasures are designed to take advantage of any kind of feature unique to a device or a series of devices within a certain margin. They can detect anomalies from different parts of the device without the need for anticipation of the type of malicious hardware or its position. These anomalies can be either due to the presence of an HT or the trigger or payload of malicious hardware.

The devices used in wireless networks present inherent margins in their operating ranges that can be exploited by HTs. By performing a specific selection of signatures, a fingerprinting-based method can exploit anomalies that the described attacks cannot avoid, focusing on performance characteristics of the ICs. These signatures can be measured during certain operations of the ICs, exploiting side-channel parameters such as power consumption, temperature, or EM emissions or radiation. The next sections detail methods that are examples of successful fingerprinting-based countermeasures for detection of unanticipated HTs.

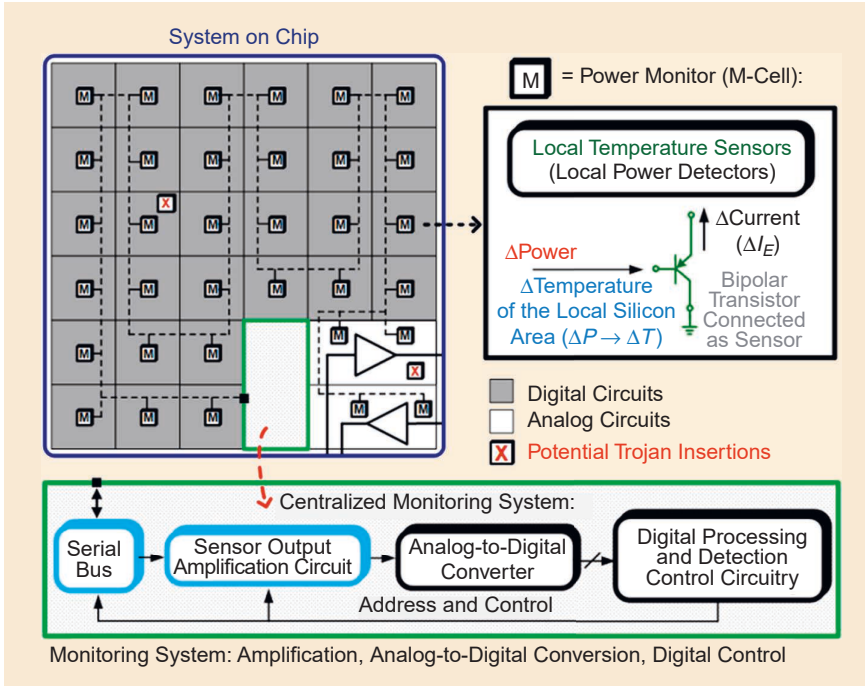

Figure 13. *A runtime thermal HT detection system. A module with a power/temperature sensing transistor and monitoring system that amplifies, converts, and processes the measurements to detect fluctuations [33].*

Power Consumption and Temperature

Methods based on power consumption measurements aim to analyze the internal activities of ICs as well as detect the power fluctuations that differ between Trojan-free and Trojan-infected ICs. Because power features are susceptible to the noise generated by the IC and temperature variations, in some cases, partition of the chip is necessary to properly analyze it [27].

In [28], a runtime detection model that analyzes power consumption data by applying chaos theory approaches (e.g., not making any assumptions about the statistical distribution of the data) and uses spatial vectors to discriminate different cases is presented. Thermal sensors compensate for the noise from additional hardware and detect HT activity. In some cases, the HT can remain undetected if no power is used unless it is activated in a very rare condition and the transient power fluctuations are within predetermined margins. Therefore, multiple-parameter analyses are considered, such as adding the maximum operating frequency of the circuit to improve detection accuracy [29]. The test conditions used in these methods also considerably impact the HT's detection accuracy, as, for example, the supply voltage can affect how fast the gates switch in the IC.

HT activity can cause temperature fluctuations and alterations in an IC. When an HT is triggered, the additional power consumption can be exploited to detect Trojan-infected components, as seen in the thermal maps presented in Figure 12 [31]. In some cases, these changes may not be able to be detected, but electrothermal coupling mechanisms have been proposed to improve these methods. In [33], the HT activity is detected using on-chip temperature sensors, as presented in the circuit of Figure 13, detecting deviations lower than 2% in power/thermal profiles with a low-cost approach. System-level concepts and designs for on-chip thermal profiling are also presented in [32].

Path Delay

An IC consists of many paths that include diverse characteristics that can be exploited to create fingerprints. These paths can present delays in their responses if an HT is inserted. By analyzing the expected delays of a Trojan-free device, a fingerprint can be created with different path delay features for different device configurations or conditions [46].

The aging and natural degradation of an IC can also alter its path delay distribution or fingerprint; however, statistical data analyses can differentiate these effects on path delay from other sources, such as HT insertion. Figure 14 presents a method to detect and locate Trojans through path delay analysis, using satisfiability-based test patterns and multiplexer-based debugging techniques.

Fingerprint-based countermeasures are designed to take advantage of any kind of feature unique to a device or a series of devices within a certain margin.

Transient-Based Methods

The turn-on transients of a device can provide identification capabilities. In [47], the signal transient features from different transmission modules are analyzed to extract their fingerprints. The energy spectrum of turn-on transient signals presents good classification accuracy [48]. This method is robust against multipath, distance, and supply changes, however, antenna polarization affects

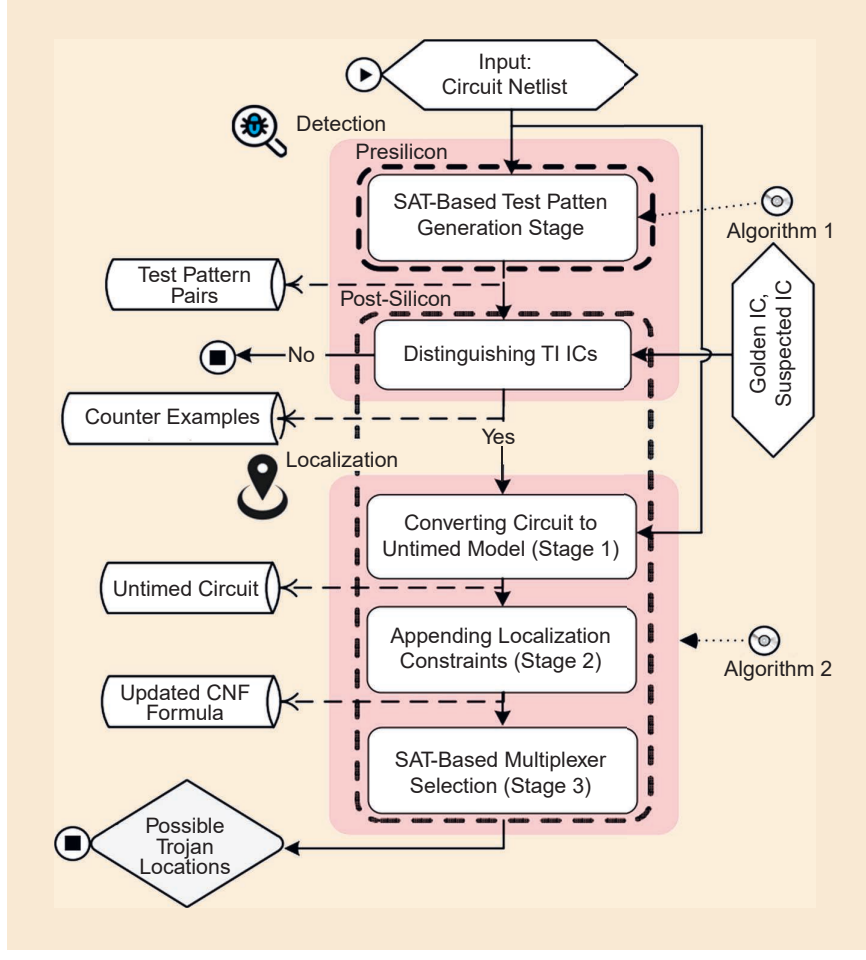

Figure 14. *An HT Detection and Localization through Path-Delay Analysis (DELPA) methodology flow diagram using a multiplexer-based debugging technique and exposing timing variations [46]. CNF: conjunctive normal form; SAT: satisfiability.*

EM emanations from ICs while operating at different conditions can be used to detect HTs, taking into account their sensitivity to hardware changes.

the transient shape and needs to be considered as a part of the analysis and as a feature to characterize. Figure 15 presents radio signal transient shapes for three different Wi-Fi (IEEE 802.11) transmitters, which can be successfully used to differentiate them based on their distinctiveness. The exploitation of features from transmitted signals can benefit from the use of capabilities provided by recurrent neural networks or long short-term memory algorithms, processing the correlation of legitimate and unknown devices effectively and in a timely manner [45].

EM-Based Methods

EM emanations from ICs while operating at different conditions can be used to detect HTs, taking into account their sensitivity to hardware changes [35], [36], [37]. This hardware sensitivity is based on the correlation that EM radiation has with the currents traveling through the different layers of the ICs, and the configuration of their logic gates based on their operational configuration. The emanations from Trojan-free, or golden, ICs can be compared with the ones with hardware modifications, revealing these modifications and, therefore, HT presence [35], [38]. The use of EM radiation is not limited to radio and microwaves, it also includes the use of infrared or visible light, among others. Moreover, the techniques that use EM radiation are nonintrusive and can be applied to devices that present limited resources or space. One of the main drawbacks, like in previously presented countermeasures, is the setup requirements: specialized measuring tools and measurements [40], [41], [42].

EM backscattering is also used for HT detection, injecting a carrier signal into the IC and analyzing the emanations as modulated scattering [39], [43]. In this case, to be able to study the backscattered fields of a region of the IC, near-field probes are commonly used, even though the spatial resolution of the probes limits the detection accuracy. Figure 16 presents a series of bitmaps for different HT-infected circuits. These bitmaps are created from the time domain vectors measured with EM probes at different locations of the device under test, which are then compared with the ones obtained from measuring golden modules.

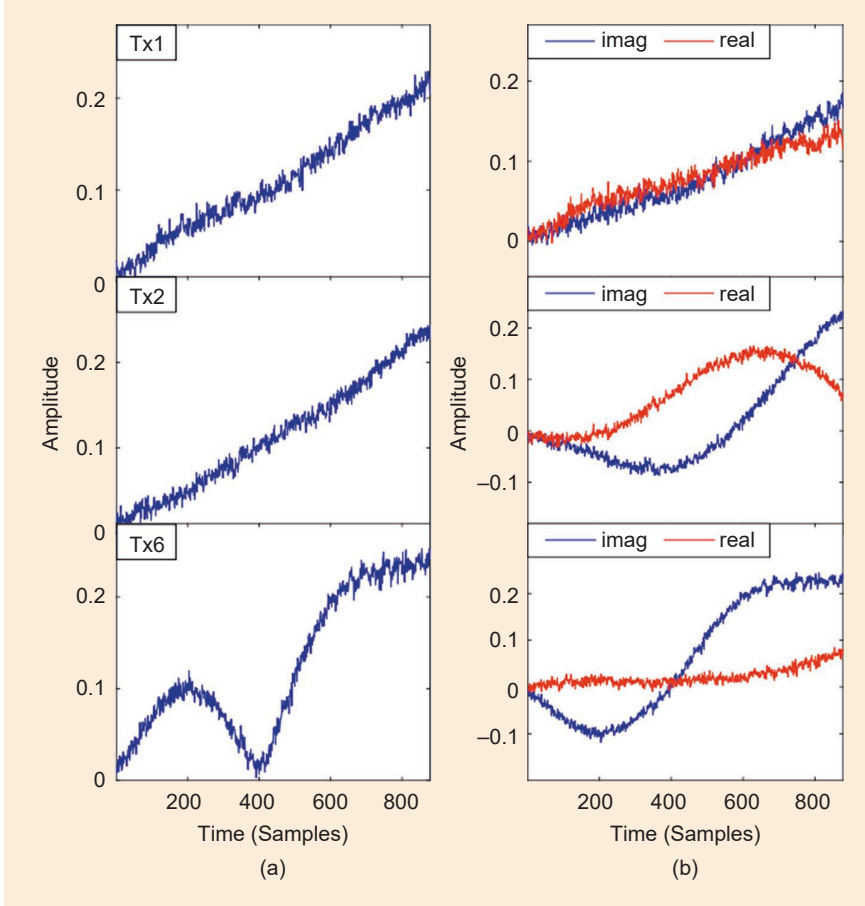

Figure 15. *(a) Instantaneous amplitude profiles and (b) real and imaginary (imag) parts of complex transient signals for three different transmitters, presenting distinctive characteristics for identifying them [48]. Tx: transmitter.*

In [39] and [44], high-resolution E- and H-field probes are analyzed to enable the detection of small HTs employing EM-based methods. In this case, a carrier frequency is excited inside an IC with a specific clock frequency. The IC unintentionally modulates the carrier by the harmonics of the clock's frequency. By interpreting the characteristics of these harmonics, the state of the IC can be analyzed and HT activity can be exposed, as presented in Figure 17.

In [50] and [51], an oscillator-based EM emission technique is used to study the difference in the delay of circuit elements

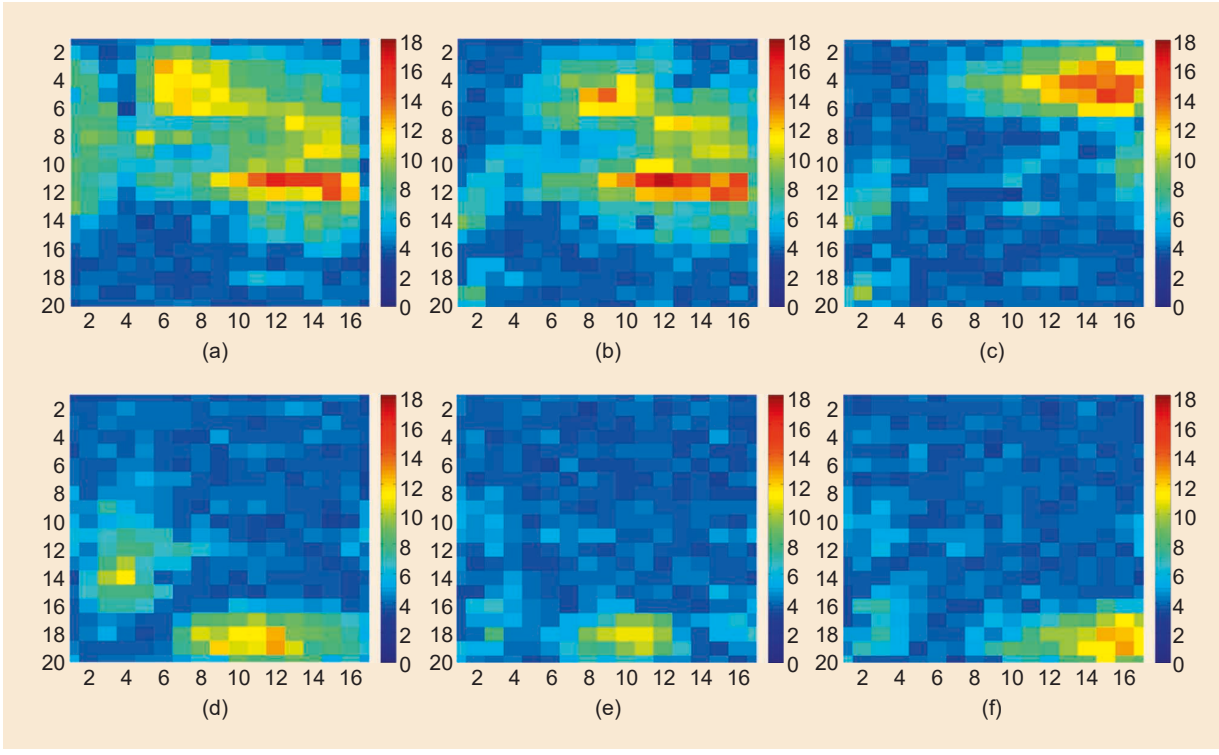

Figure 16. *(a)–(f) HT-infected module EM bitmaps correlations, where each point is a different EM probe location measurement. Colors other than blue represent the detection of hardware modifications or fluctuations (HT presence) [44].*

by analyzing the EM radiation due to the switching activity of the transistors. In this way, fingerprints that are able to characterize different semiconductor devices can be extracted from oscillator-based ICs. The measurements in this case can take advantage of the frequency spectrum or any other domain response that is accurate and easy to replicate. In [52], a ring oscillator circuit is used to detect the variability of oscillations caused by the process variations (e.g., a lithographic mask and spatial variability due to the geometric variation of transistors [53]) of the ICs under test. The ring oscillator circuit is based on inverters or delay elements in cycles, connecting the first and last stages to produce an oscillation that is affected by the process variations of the ICs. This circuit is widely used in variability detection applications because the oscillations are sensitive to hardware variations. As shown in Figures 18 and 19, these variations in oscillations can be analyzed as a part of the fundamental

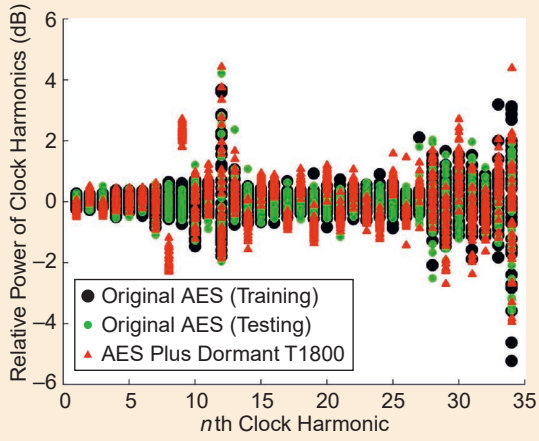

Figure 17. *Amplitude ratios of backscattered clock harmonics for HT-free and HT-infected modules. The data points are normalized to the mean of their HT-free measurement [43]. AES: Advanced Encryption Standard.*

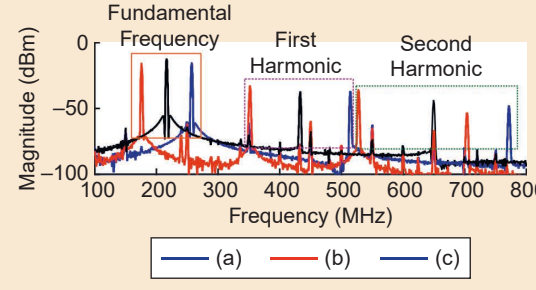

Figure 18. *The frequency of a ring oscillator circuit for varying interconnect lengths and number of stages of an inverter (fundamental frequency and higher harmonics). (a) A three-stage inverter ring oscillator. (b) A five-stage inverter ring oscillator. (c) A three-stage inverter ring oscillator with a longer interconnect length between logic elements [52].*

frequency and its higher harmonics to differentiate among different devices under test.

Antenna Parameters

The inherent features of some RF components can be used to detect alterations or insertion of malicious components. The study reported in [54] presents a method that uses antenna S_{11} parameters far beyond its operational frequency as the main features for HT detection in a commercial off-the-shelf wireless module. In this case, a module that includes the main ICs and the antenna in the same printed circuit board (PCB) is considered, where any additional components can alter the parameters of the antenna due to their proximity and the sensitivity to hardware changes of the antenna's parameters. The effects when the HT is activated can also be considered, which can directly or indirectly affect the antenna's parameters. Figure 20 presents the differences caused by the insertion of an HT into the PCB design used in that work. As shown, the measurements are slightly different in all the considered frequency ranges, but especially between 4 and 6 GHz, outside the operational frequency (2.4 GHz) of the module. Similarity and distance metrics can be used to compute a classification threshold to identify alterations in the modules and classify them as suspicious, such as correlation coefficients or Manhattan distances.

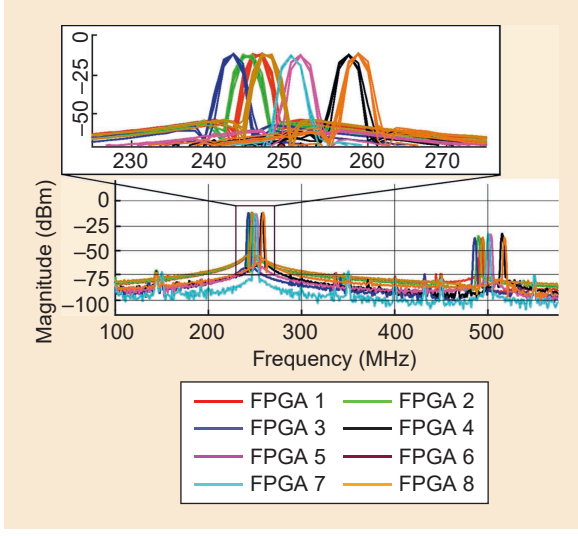

Figure 19. *RF signals emitted by eight different FPGAs with the same ring oscillator circuit in bandwidths up to 530 MHz, and (inset) a zoomed-in view around the fundamental frequency peak (with repetitive measurements) for all devices under test [52]. FPGA: field-programmable gate array.*

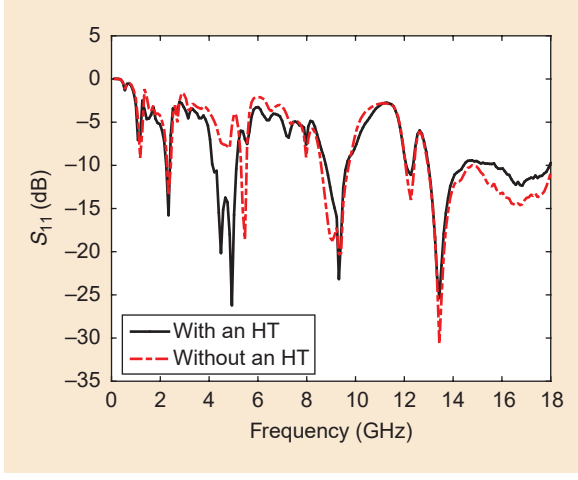

Figure 20. *Wireless module S_{11} parameters with and without an HT, presenting differences outside the operating frequency range of the module, thus allowing for detection of HT presence/modification [54].*

RF Fingerprinting Beyond HT Detection

Beyond HT detection applications, RF fingerprinting-based mechanisms have been used for a wide range of applications, including source identification and classification. In these cases, the effects of all the components and the channel conditions play an important role in feature extraction. In large-scale applications, the differences among fingerprints can present a margin that is too low to differentiate among different sources, requiring additional feature engineering techniques to improve these characteristics. The antennas used in these wireless systems are examples of components that can be exploited to apply feature engineering techniques and provide a wider range of fingerprints for source identification and classification. Parameters such as polarization and radiation pattern produce effects to the fingerprints that, taking advantage of novel manufacturing techniques, can be engineered to improve their uniqueness when compared to other antennas. Miguélez-Gómez and Rojas-Nastrucci [13] present a technique that intentionally modifies features, and therefore the fingerprint of wireless modules.

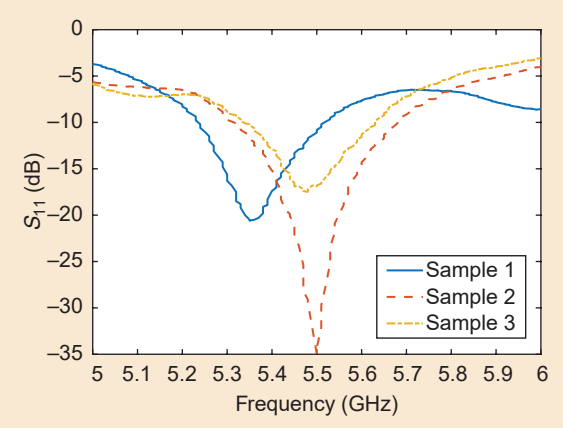

Figure 21. *S_{11} parameters of additively manufactured antennas with distinctive features to be used as fingerprints [13].*

The fingerprint's uniqueness is achieved by using AM techniques, which allows rapid prototyping and conformal designs that traditional manufacturing techniques cannot achieve. Figure 21 presents an example of S_{11} feature differences for additively manufactured antennas that are part of the same design.

Features from other RF components, such as PAs, can also be used to create physically unclonable functions

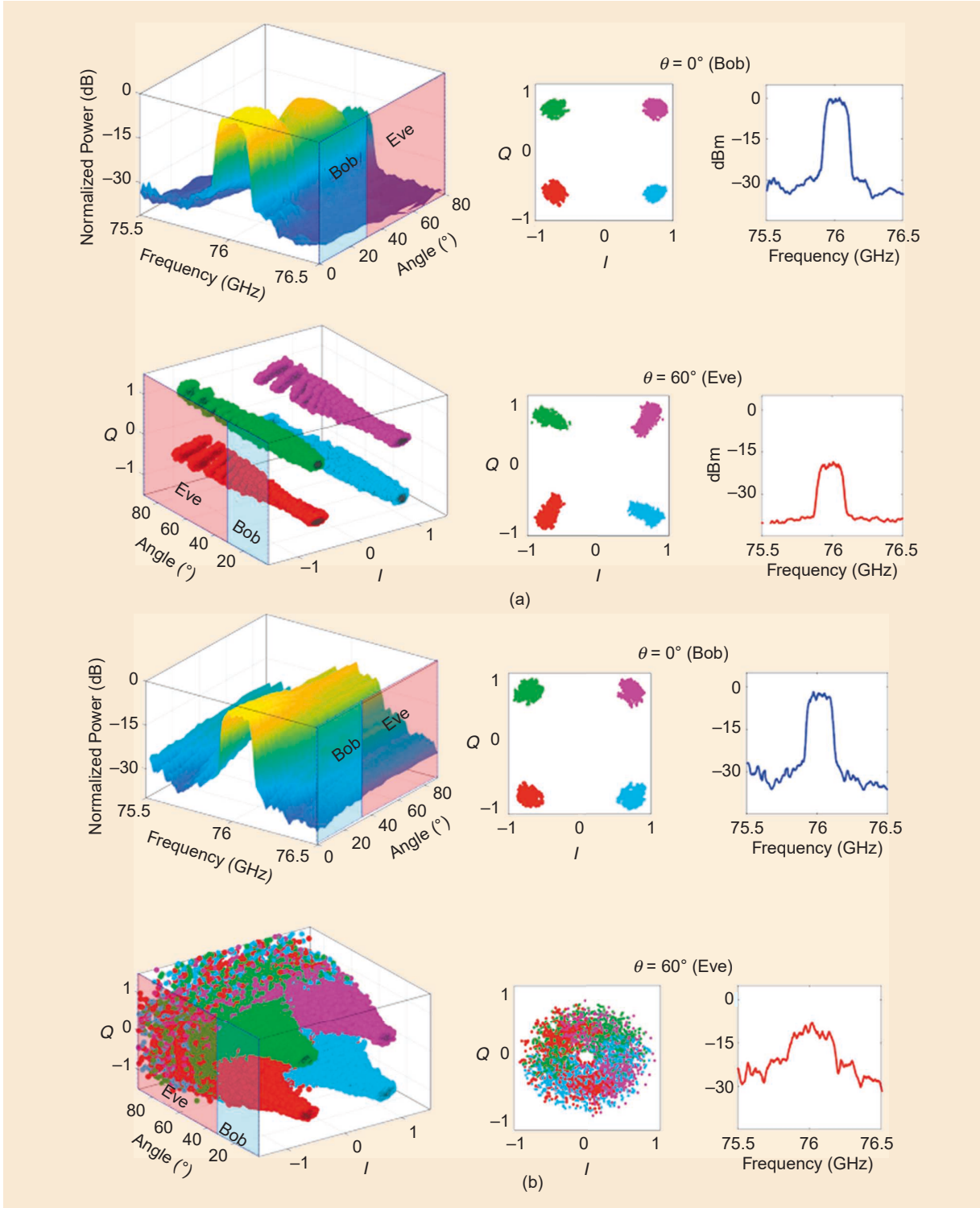

Figure 22. *(a) Conventional and (b) space-time modulated phased arrays. The received SS and data constellation are based on the alignment of the receiver and transmitter sides [57]. Q: quadrature.*

Features from other RF components, such as PAs, can also be used to create physically unclonable functions for security enhancement.

(PUFs) for security enhancement. In [56], the PA's spectral regrowth (i.e., its out-of-band nonlinearity) is used to implement a PUF to amplify intrinsic device variation and manipulate the probability distribution of spectral regrowth across all the devices.

Spatiotemporal features can also add additional physical-layer security levels. By taking advantage of space-time modulated-array characteristics, methods that generate directional modulation are presented in [57], [58], and [59]. Using these arrays, the correct symbols are transmitted only in the direction of interest, while the other directions present some misalignment, thus producing an erroneous constellation and, therefore, data at the receiver side. A potential eavesdropper not aligned with the transmitter would not be able to get the data from the legitimate communications link. Figure 22 presents a comparison of quadrature phase-shift keying data constellations and received spectra as a function of spatial elevation angles for both a conventional phased array and a spatiotemporal modulated array. As shown in Figure 23, for the nonconventional array, both the

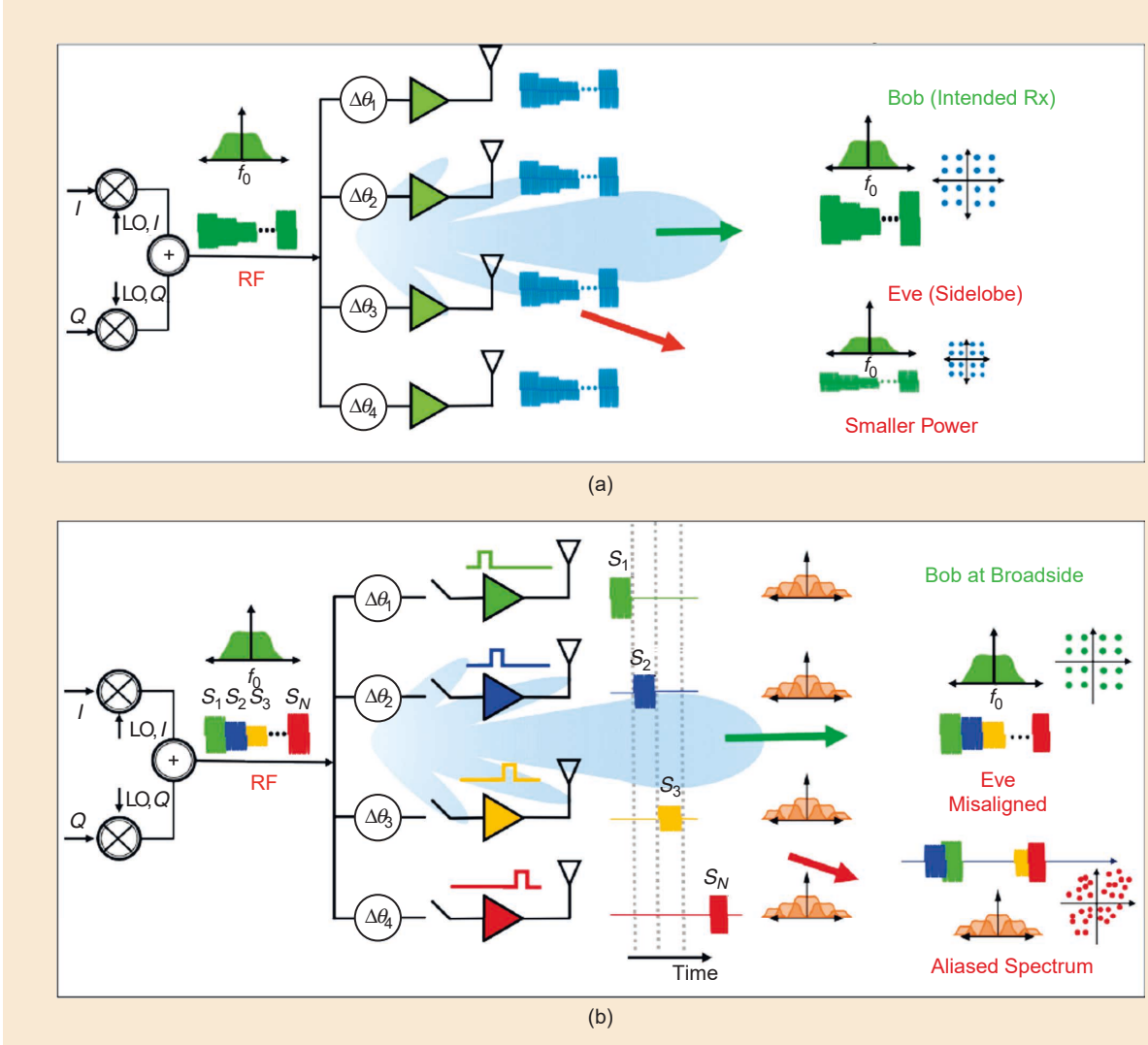

Figure 23. *The measurement of a quaternary phase-shift keying data constellation of intermediate frequency with a data bandwidth equal to 200 MHz, and the received spectrum as a function of spatial elevation angles at a center frequency of 76 GHz. (a) Measurements for a conventional phased array, showing preservation of the SS and constellation in space. (b) Measurements for a spatiotemporal modulated array, preserving signal spectrum and constellation at the broadside while spectrally aliasing at other angles [57]. Rx: receiver; LO: local oscillator; I: in-phase.*

signal spectrum and the data constellation are preserved only in the direction of interest (broadside).

Conclusions

This article discusses the most common HT attacks and countermeasures in wireless systems. The systems that are continuously sharing data wirelessly are becoming completely vulnerable to these types of hardware attacks, especially considering the unpredictability of HTs and the increase in the number of entities that are a part of the lifecycle of wireless ICs. Even the most common attacks can present different designs that can be hidden in several parts of wireless components and take advantage of a variety of undetectable features. Widely used countermeasures present costly, time-consuming, and even destructive procedures that detect or prevent HTs. In contrast, RF fingerprinting techniques provide detection aspects without previous knowledge about the HT's design, position, or even main function, at a low cost with little complexity and time consumption, thus providing promising capabilities to enhance the future of hardware security in wireless systems.

References

[1] S. Bi, R. Zhang, Z. Ding, and S. Cui, "Wireless communications in the era of big data," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 190–199, Oct. 2015, doi: 10.1109/MCOM.2015.7295483.

[2] E. Halepovic, C. Williamson, and M. Ghaderi, "Wireless data traffic: A decade of change," *IEEE Netw.*, vol. 23, no. 2, pp. 20–26, Mar. 2009, doi: 10.1109/MNET.2009.4804332.

[3] Cisco Systems, "Cisco annual internet report (2018–2023) white paper," Cisco, San Jose, CA, USA, 2022. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[4] Cisco Systems, "Cisco visual networking index: Forecast and trends, 2017–2022," Cisco, San Jose, CA, USA, 2022. [Online]. Available: https://twiki.cern.ch/twiki/pub/HEPIX/TechwatchNetwork/HtwNetworkDocuments/white-paper-c11-741490.pdf

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, doi: 10.1109/JPROC.2016.2558521.

[6] A. Antonopoulos, C. Kapatsori, and Y. Makris, "Trusted analog/mixed-signal/RF ICs: A survey and a perspective," *IEEE Des. Test*, vol. 34, no. 6, pp. 63–76, Dec. 2017, doi: 10.1109/MDAT.2017.2728366.

[7] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, Aug. 2014, doi: 10.1109/JPROC.2014.2335155.

[8] S. Bhunia and M. Tehranipoor, *Hardware Security – A Hands-On Learning Approach*. Morgan Kaufmann, 2019.

[9] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. Adv. Cryptol. (CRYPTO)*, 1996, 104–113.

[10] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan./Feb. 2010, doi: 10.1109/MDT.2010.7.

[11] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan attacks: Threat analysis and countermeasures," *Proc. IEEE*, vol. 102, no. 8, pp. 1229–1247, Aug. 2014, doi: 10.1109/JPROC.2014.2334493.

[12] K. Subramani, G. Volanis, M.-M. Bidmeshki, A. Antonopoulos, and Y. Makris, "Trusted and secure design of analog/RF ICs: Recent developments," in *Proc. IEEE 25th Int. Symp. On-Line Testing Robust Syst. Des. (IOLTS)*, 2019, pp. 125–128, doi: 10.1109/IOLTS.2019.8854461.

[13] N. Miguélez-Gómez and E. A. Rojas-Nastrucci, "Antenna additively manufactured engineered fingerprinting for physical-layer security enhancement for wireless communications," *IEEE Open J. Antennas Propag.*, vol. 3, pp. 637–651, 2022, doi: 10.1109/OJAP.2022.3181325.

[14] D. Chang, B. Bakkaloglu, and S. Ozev, "Enabling unauthorized RF transmission below noise floor with no detectable impact on primary communication performance," in *Proc. IEEE 33rd VLSI Test Symp. (VTS)*, 2015, pp. 1–4, doi: 10.1109/VTS.2015.7116257.

[15] K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia, and Y. Makris, "Amplitude-modulating analog/RF hardware Trojans in wireless networks: Risks and remedies," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3497–3510, Apr. 2020, doi: 10.1109/TIFS.2020.2990792.

[16] L. Lin, W. Burleson, and C. Paar, "Moles: Malicious off-chip leakage enabled by side-channels," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Des. – Dig. Tech. Papers*, 2009, pp. 117–122.

[17] K. S. Subraman, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "Demonstrating and mitigating the risk of an FEC-based hardware Trojan in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2720–2734, Oct. 2019, doi: 10.1109/TIFS.2019.2900906.

[18] K. S. Subramani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "ACE: Adaptive channel estimation for detecting analog/RF Trojans in WLAN transceivers," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Des. (ICCAD)*, 2017, pp. 722–727, doi: 10.1109/ICCAD.2017.8203848.

[19] Y. Liu, Y. Jin, A. Nosratinia, and Y. Makris, "Silicon demonstration of hardware Trojan design and detection in wireless cryptographic ICs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 4, pp. 1506–1519, Apr. 2017, doi: 10.1109/TVLSI.2016.2633348.

[20] M.-M. Bidmeshki, A. Antonopoulos, and Y. Makris, "Information flow tracking in analog/mixed-signal designs through proof-carrying hardware IP," in *Proc. Des., Automat. Test Eur. Conf. Exhib. (DATE)*, 2017, pp. 1703–1708, doi: 10.23919/DATE.2017.7927268.

[21] M. M. Bidmeshki, A. Antonopoulos, and Y. Makris, "Proof-carrying hardware-based information flow tracking in analog/mixed-signal designs," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 2, pp. 415–427, Jun. 2021, doi: 10.1109/JETCAS.2021.3075098.

[22] N. Hu, M. Ye, and S. Wei, "Surviving information leakage hardware Trojan attacks using hardware isolation," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 253–261, Apr./Jun. 2019, doi: 10.1109/TETC.2017.2648739.

[23] C. Bao, D. Forte, and A. Srivastava, "On reverse engineering-based hardware Trojan detection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 35, no. 1, pp. 49–57, Jan. 2016, doi: 10.1109/TCAD.2015.2488495.

[24] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008, doi: 10.1109/TWC.2008.070194.

[25] H. Fang, X. Wang, and L. Xu, "Fuzzy learning for multi-dimensional adaptive physical layer authentication: A compact and robust approach," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5420–5432, Aug. 2020, doi: 10.1109/TWC.2020.2993175.

[26] H. Fang, X. Wang, and L. Hanzo, "Adaptive trust management for soft authentication and progressive authorization relying on physical layer attributes," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2607–2620, Apr. 2020, doi: 10.1109/TCOMM.2020.2965451.

[27] R. Rad, J. Plusquellic, and M. Tehranipoor, "A sensitivity analysis of power signal methods for detecting hardware Trojans under real process and environmental conditions," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 12, pp. 1735–1744, Dec. 2010, doi: 10.1109/TVLSI.2009.2029117.

[28] H. Zhao, L. Kwiat, K. A. Kwiat, C. A. Kamhoua, and L. Njilla, "Applying chaos theory for runtime hardware Trojan monitoring and

detection," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 4, pp. 716–729, Jul./Aug. 2020, doi: 10.1109/TDSC.2018.2864733.
[29] S. Narasimhan et al., "Hardware Trojan detection by multiple-parameter side-channel analysis," *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2183–2195, Nov. 2013, doi: 10.1109/TC.2012.200.
[30] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop Hardware-Oriented Secur. Trust*, 2008, pp. 51–57, doi: 10.1109/HST.2008.4559049.
[31] Y. Wen and W. Yu, "Combining thermal maps with inception neural networks for hardware Trojan detection," *IEEE Embedded Syst. Lett.*, vol. 13, no. 2, pp. 45–48, Jun. 2021, doi: 10.1109/LES.2020.3000008.
[32] C. Bao, D. Forte, and A. Srivastava, "Temperature tracking: Toward robust run-time detection of hardware Trojans," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 10, pp. 1577–1585, Oct. 2015, doi: 10.1109/TCAD.2015.2424929.
[33] M. Yan, H. Wei, and M. Onabajo, "On-chip thermal profiling to detect malicious activity: System-level concepts and design of key building blocks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 3, pp. 530–543, Mar. 2021, doi: 10.1109/TVLSI.2020.3047020.
[34] R. Shende and D. D. Ambawade, "A side channel based power analysis technique for hardware Trojan detection using statistical learning approach," in *Proc. 13th Int. Conf. Wireless Opt. Commun. Netw. (WOCN)*, 2016, pp. 1–4, doi: 10.1109/WOCN.2016.7759894.
[35] H. P. Romero, K. A. Remley, D. F. Williams, and C. Wang, "Electromagnetic measurements for counterfeit detection of radio frequency identification cards," *IEEE Trans. Microw. Theory Techn.*, vol. 57, no. 5, pp. 1383–1387, May 2009, doi: 10.1109/TMTT.2009.2017318.
[36] J. He, X. Guo, M. Tehranipoor, A. Vassilev, and Y. Jin, "EM side channels in hardware security: Attacks and defenses," *IEEE Des. Test*, vol. 39, no. 2, pp. 100–111, Apr. 2022, doi: 10.1109/MDAT.2021.3135324.
[37] 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, doi: 10.1109/TVLSI.2017.2727985.
[38] H. Huang, A. Boyer, and S. B. Dhia, "The detection of counterfeit integrated circuit by the use of electromagnetic fingerprint," in *Proc. Int. Symp. Electromagn. Compat.*, 2014, pp. 1118–1122, doi: 10.1109/EMCEurope.2014.6931070.
[39] L. N. Nguyen, C. Cheng, M. Prvulovic, and A. Zajic, "Creating a backscattering side channel to enable detection of dormant hardware Trojans," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 7, pp. 1561–1574, Jul. 2019, doi: 10.1109/TVLSI.2019.2906547.
[40] G. Li, K. Itou, Y. Katou, N. Mukai, D. Pommerenke, and J. Fan, "A resonant E-field probe for RFI measurements," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 6, pp. 1719–1722, Dec. 2014, doi: 10.1109/TEMC.2014.2354018.
[41] E. Song and H. H. Park, "A high-sensitivity electric probe based on board-level edge plating and LC resonance," *IEEE Microw. Compon. Lett.*, vol. 24, no. 12, pp. 908–910, Dec. 2014, doi: 10.1109/LMWC.2014.2361433.
[42] F. Fiori and F. Musolino, "Comparison of IC conducted emission measurement methods," *IEEE Trans. Instrum. Meas.*, vol. 52, no. 3, pp. 839–845, Jun. 2003, doi: 10.1109/TIM.2003.814685.
[43] S. Adibelli, P. Juyal, L. N. Nguyen, M. Prvulovic, and A. Zajic, "Near-field backscattering-based sensing for hardware Trojan detection," *IEEE Trans. Antennas Propag.*, vol. 68, no. 12, pp. 8082–8090, Dec. 2020, doi: 10.1109/TAP.2020.3000562.
[44] J. Balasch, B. Gierlichs, and I. Verbauwhede, "Electromagnetic circuit fingerprints for hardware Trojan detection," in *Proc. IEEE Int. Symp. Electromagn. Compat. (EMC)*, 2015, pp. 246–251, doi: 10.1109/ISEMC.2015.7256167.
[45] S. Mi, Z. Zhang, Y. Zhang, and A. Hu, "A non-destructive method for hardware Trojan detection based on radio frequency fingerprinting," *Electronics*, vol. 11, no. 22, Nov. 2022, Art. no. 3776, doi: 10.3390/electronics11223776.
[46] M. Sabri, A. Shabani, and B. Alizadeh, "SAT-based integrated hardware Trojan detection and localization approach through path-delay analysis," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 68, no. 8, pp. 2850–2854, Aug. 2021, doi: 10.1109/TCSII.2021.3074549.
[47] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *Proc. Int. Conf. Inf. Process. Sensor Netw.*, 2009, pp. 25–36.
[48] M. Köse, S. Taşcioğlu, and Z. Telatar, "RF fingerprinting of IoT devices based on transient energy spectrum," *IEEE Access*, vol. 7, pp. 18,715–18,726, Jan. 2019, doi: 10.1109/ACCESS.2019.2896696.
[49] S. K. Haider, C. Jin, M. Ahmad, D. M. Shila, O. Khan, and M. van Dijk, "Advancing the state-of-the-art in hardware Trojans detection," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 1, pp. 18–32, Jan./Feb. 2019, doi: 10.1109/TDSC.2017.2654352.
[50] D. Merli et al., "Localized electromagnetic analysis of RO PUFs," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, 2013, pp. 19–24, doi: 10.1109/HST.2013.6581559.
[51] M. Ahmed et al., "Robust and noninvasive IC authentication using radiated electromagnetic emissions," *J. Hardware Syst. Secur.*, vol. 3, pp. 273–288, Sep. 2019, doi: 10.1007/s41635-01900072-y.
[52] M. M. Ahmed et al., "Radiated electromagnetic emission for integrated circuit authentication," *IEEE Microw. Compon. Lett.*, vol. 27, no. 11, pp. 1028–1030, Nov. 2017, doi: 10.1109/LMWC.2017.2750078.
[53] S. Ghosh and K. Roy, "Parameter variation tolerance and error resiliency: New design paradigm for the nanoscale era," *Proc. IEEE*, vol. 98, no. 10, pp. 1718–1751, Oct. 2010, doi: 10.1109/JPROC.2010.2057230.
[54] N. M. Gómez and E. A. R. Nastrucci, "Unanticipated hardware Trojan detection technique based on antenna reflection coefficient features outside of its operation frequency," in *Proc. IEEE 22nd Annu. Wireless Microw. Technol. Conf. (WAMICON)*, 2022, pp. 1–4, doi: 10.1109/WAMICON53991.2022.9786131.
[55] A. Al-Shawabka et al., "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2020, pp. 646–655, doi: 10.1109/INFOCOM41043.2020.9155259.
[56] Q. Zhou, Y. He, K. Yang, and T. Chi, "12.3 exploring PUF-controlled PA spectral regrowth for physical-layer identification of IoT nodes," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2021, pp. 204–206, doi: 10.1109/ISSCC42613.2021.9365941.
[57] S. Venkatesh, H. Saeidi, K. Sengupta, and X. Lu, "Millimeter-wave physical layer security through space-time modulated transmitter arrays," in *Proc. IEEE 22nd Annu. Wireless Microw. Technol. Conf. (WAMICON)*, 2022, pp. 1–4, doi: 10.1109/WAMICON53991.2022.9786152.
[58] S. Venkatesh, X. Lu, K. Sengupta, and B. Tang, "Spatio-temporal modulated millimeter-wave antenna arrays for secure wireless links," in *Proc. IEEE Int. Symp. Antennas Propag. North Amer. Radio Sci. Meeting*, 2020, pp. 1565–1566, doi: 10.1109/IEEECONF35879.2020.9330046.
[59] J. Guo, L. Poli, M. A. Hannan, P. Rocca, S. Yang, and A. Massa, "Time-modulated arrays for physical layer secure communications: Optimization-based synthesis and experimental assessment," *IEEE Trans. Antennas Propag.*, vol. 66, no. 12, pp. 6939–6949, Dec. 2018, doi: 10.1109/TAP.2018.2870381.
[60] J. Classen, M. Schulz, and M. Hollick, "Practical covert channels for WiFi systems," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, 2015, pp. 209–217, doi: 10.1109/CNS.2015.7346830.
[61] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret agent radio: Covert communication through dirty constellations," in *Information Hiding*, M. Kirchner and D. Ghosal, Eds. Berlin, Germany: Springer-Verlag, 2013, pp. 160–175.
[62] K. Sankhe et al., "Impairment shift keying: Covert signaling by deep learning of controlled radio imperfections," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, 2019, pp. 598–603, doi: 10.1109/MILCOM47813.2019.9021079.
[63] A. R. Díaz-Rizo, H. Aboushady, and H.-G. Stratigopoulos, "Leaking wireless ICs via hardware Trojan-infected synchronization," *IEEE Trans. Dependable Secure Comput.*, early access, 2022, doi: 10.1109/TDSC.2022.3218507.
[64] A. R. Díaz-Rizo, H. Aboushady, and H.-G. Stratigopoulos, "Anti-piracy design of RF transceivers," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 1, pp. 492–505, Jan. 2022, doi: 10.1109/TCSI.2022.3214111.