2022 IEEE 22nd Annual Wireless and Microwave Technology Conference (WAMICON) | 978-1-6654-2195-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/WAMICON53991.2022.9786131

# Unanticipated Hardware Trojan Detection Technique Based on Antenna Reflection Coefficient Features Outside of its Operation Frequency

Noemí Miguélez Gómez, Eduardo A. Rojas Nastrucci
*Department of Electrical Engineering and Computer Science*
*Embry-Riddle Aeronautical University*
Daytona Beach, FL, USA
miguelen@my.erau.edu, rojas1@erau.edu

***Abstract*—The involvement of different entities in the life cycle of wireless electronics has increased the risk of adversary attacks, in particular, hardware Trojans (HTs). Wireless network hardware need to be compliant with a set of minimum security requirements to protect the data that these systems exchange and ensure the system reliability, however, HTs make them vulnerable. Hardware-based malicious attacks and defense mechanisms are continuously being analyzed to provide prevention and detection capabilities against them. Considering the unpredictability of HTs, there is a need for blind countermeasures that can detect and identify HTs without any previous knowledge of their characteristics: fingerprint-based methods. This paper presents a technique for the detection of unanticipated HTs based on antenna input reflection coefficient measurements ($S_{11}$) over a wide range of frequencies expanding far beyond the antenna operation frequency. This work includes the design, manufacturing and testing of printed circuit boards with a WiFi system-on-chip (ESP8285), a meandered inverted-F antenna, and a HT that shorts the antenna to disrupt the communication link. The effects of the insertion of the HT in both operational and non-operational modes are successfully used to detect its presence without anticipation of its characteristics using data similarity and distance measures (Pearson's coefficient, Euclidean and Manhattan distances) that can be extrapolated to machine learning algorithms for large scale analyses.**

***Index Terms*—Machine learning, physical-layer security, RF fingerprinting, Trojan detection, wireless networks.**

## I. Introduction

THE growth of RF technology and capabilities has enabled an increment in the quantity and quality of data that wireless networks are continuously sharing. Considering the global use of these systems, external attacks have been advancing at a fast pace, providing software and hardware tools to perform spoofing, jamming and eavesdropping attacks to these systems. Experienced changes in hardware design, fabrication, and distribution have increased the number of hardware vulnerabilities and attacks of wireless systems, presenting a threat for the data that these systems exchange [1].

The hardware supporting the security of communications technologies needs to be prepared against a wide variety of sources of attack. There are hardware-based operation and function vulnerabilities that can be introduced to integrated circuits (ICs) by untrusted entities that participate in their life cycle: hardware Trojans (HTs) [2],[3]. Hardware Trojans are a focused of concern due to the wide range of undesired behaviours that they can cause and how unpredictable they can be. The operational margins of wireless ICs are examples of wireless networks vulnerabilities that can facilitate HT activities. Among the different HT detection and prevention methods, fingerprint-based mechanisms are one of the main focuses proposed by the research community due to their unanticipated detection, low cost, low complexity and non-destructive characteristics [4]-[7].

In this work, a method that takes advantage of antenna features to detect hardware Trojan presence in wireless modules is presented. A printed circuit board (PCB) is designed based on commercial-off-the-shelf (COTS) modules that include a WiFi system-on-chip (SoC), a meandered inverted F antenna (MIFA), signal conditioning components, and a HT can be activated with the SoC and short-circuits the antenna, compromising the communications link. The design allows the measurement of the $S_{11}$ parameter of the antenna to analyze the effect of the HT during operational and non-operational phases. The measured data is exploited to detect the presence of HTs with straightforward statistical analyses using Pearson coefficient and Euclidean and Manhattan distances [8]. The results prove that without previous knowledge of the HT characteristics, the malicious hardware can be detected as an abnormal behavior of the antenna fingerprint beyond its resonance frequency. For large scale HT detection applications, this method allows the use of machine learning classifiers, such as one-class support vector machine (SVM), trained with data from Trojan-free modules, to detect Trojan-infected units [9].

## II. Methodology and Procedures

### A. Wireless Module Design

The design of the PCB used in this work is based on commercially available COTS modules that include the WiFi Espressif ESP8285 system-on-a-chip (SoC). MIFA designs are included in these modules for their low-cost and high-efficiency capabilities, such as the 2.4 GHz MIFA presented in Fig. 1 and used in this work. Ansys HFSS Electronics Desktop 2021 is utilized to simulate the antenna performance, and to

978-1-6654-2195-9/22/$31.00 ©2022 IEEE

optimize its dimensions (Table I) to achieve resonance at 2.4 GHz. The substrate selected for the module is FR-4 with a dielectric constant of 4.5 and a loss tangent of 0.016, and the thicknesses of the substrate and the copper are 1.6 mm and 0.0356 mm, respectively, specified by the PCB manufacturer.

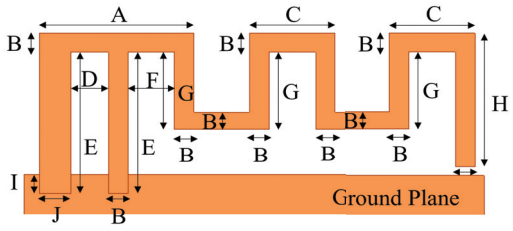


Fig. 1. Meandered inverted F antenna - baseline design.

TABLE I
MEANDERED INVERTED F ANTENNA DESIGN PARAMETERS

| Parameter | Value | Parameter | Value | Parameter | Value |
|---|---|---|---|---|---|
| $A$ [mm] | 5.0 | $D$ [mm] | 1.4 | $G$ [mm] | 2.65 |
| $B$ [mm] | 0.5 | $E$ [mm] | 4.9 | $H$ [mm] | 2 |
| $C$ [mm] | 2.7 | $F$ [mm] | 1.7 | $I$ [mm] | 0.5 |
| $J$ [mm] | 0.9 | | | | |

The ESP8285 SoC includes RF conditioning components (e.g., power amplifier, filters), WiFi functionalities (IEEE 802.11 b/g/n at 2.4 GHz), a 32-bit processor, and on-chip SRAM in a 32-pin QFN package. The compactness of the SoC minimizes the size (32.6 mm x 25.2 mm) and signal conditioning components of the 2-layers PCB design presented in Fig. 2. EAGLE electronic design automation (EDA) PCB software is used to create the schematic and board layout, which considers the tracing requirements to enhance the overall antenna performance and dimensions of the module. As it can be seen in Fig. 2, the design includes probing traces to measure the antenna parameters, and the inserted malicious hardware (HT). The HT includes the Analog Devices HMC550A switch, which allows to control signals from DC to 6 GHz with low insertion losses and very low current consumption. As it can be seen in Fig. 2, the switch is placed close to the end of the antenna, connecting it to ground (short-circuiting) in its "On" state, when it receives a control signal from the SoC.

### *B. Hardware Trojan Detection*

The hardware Trojan detection procedure presented in this work utilizes the $S_{11}$ parameter of the antenna, far beyond its operation frequency, as a fingerprint for the type of module under analysis to determine its trustworthiness. The preparation and validation of the procedure comprises the following steps: (1) measure the $S_{11}$ parameter of the antenna of populated boards without the HT for a wide frequency range (e.g., 0.1 GHz to 18 GHz) that expands far beyond the antenna operating frequency, (2) measure the $S_{11}$ parameter of the antenna of populated boards with the HT for a wide frequency range (e.g., 0.1 GHz to 18 GHz), (3) perform statistical analyses for

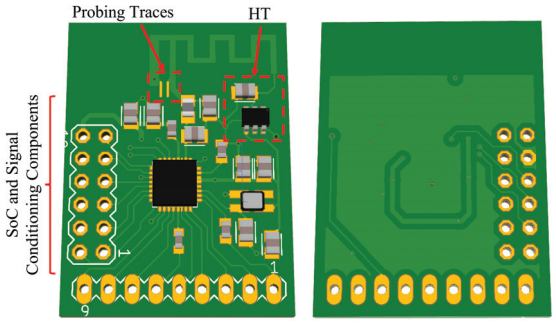


Fig. 2. EAGLE PCB design (3D View): (L) top and (R) bottom layers.

different combinations of the data to identify a measure that can detect anomalies from the Trojan-free cases, and (4) apply this measure to identify the Trojan-infected modules. These steps are common in machine learning algorithms for large-scale applications, which usually include data preparation, comparison and classification stages. Additionally, the $S_{11}$ parameter of the antenna is also measured when the board is completely populated and the HT is activated (i.e., antenna is short-circuited) for effect analyses and future considerations. All the $S_{11}$ parameters of the antenna are measured using a GGB Industries 40A-GS 750 $\mu$m pitch microwave probe, as presented in Fig. 3, and a Keysight N5227B 67 GHz PNA calibrated with a GGB Industries CS-11 calibration substrate.

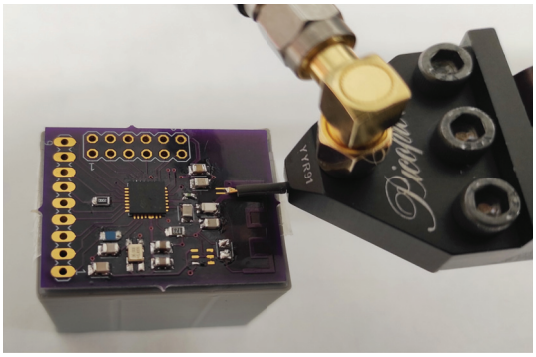

Fig. 3. Populated PCB antenna $S_{11}$ measurement - probing.

To analyze the $S_{11}$ measurements, data similarity and distance metrics are used. While the dimension of the data used in these cases can vary depending on the number of points selected for our measurements and methods, it is important to note that each "Frequency - $S_{11}$" pair of values are a distinct feature used to extract information for the antenna/module fingerprint. For the large frequency range, a total of 201 data points/features are used in the analyses. Among other metrics, Pearson coefficient, and Euclidean and Manhattan distances are considered in this work, widely used in learning algorithms to classify data. Pearson coefficient or correlation coefficient (equation I) measures the linear correlation between two different sets of data. In this case, the data from two identical PCB designs is assumed to be as linearly similar as possible, manufacturing and components imperfections con-

sidered. Manhattan (equation II) and Euclidean (equation III) are the most commonly used distances for vector comparison, presenting similar formulas to determine the total difference among the set of features of the measurements.

$$\rho_{x,y} = \frac{cov(x,y)}{\sigma_x \sigma_y} \tag{1}$$

$$d\left(x,y\right) = \sqrt{\sum_{i=1}^{n}\left(x_i - y_i\right)^2} \tag{2}$$

$$d\left(x,y\right) = \sum_{i=1}^{n}\left|x_i - y_i\right| \tag{3}$$

These metrics are used for:

- Measure the similarity/distance between Trojan-free PCBs. The PCBs are populated, but the HT is not included, to obtain the fingerprint of the Trojan-free module or commonly known as golden module/reference.
- Measure the similarity/distance between Trojan-free and Trojan-infected PCBs. The PCBs are populated but one of them includes the HT components.
- Set a threshold to classify data from new modules.

In terms of distances, a threshold for automatic classification can be more complex and time consuming to set than with the correlation coefficient. However, they present great qualities to be considered as tools for analysis and comparison purposes.

## III. Tests and Results

The PCB design, manufacturing and soldered components can alter the parameters of the antenna. Fig. 4 presents the simulated and measured antenna $S_{11}$ parameters, using a populated PCB for the measured data. As it can be seen, the simulated and measured results agree, with difference in bandwidth likely due to effects of additional devices around the antenna not accounted in the simulations.

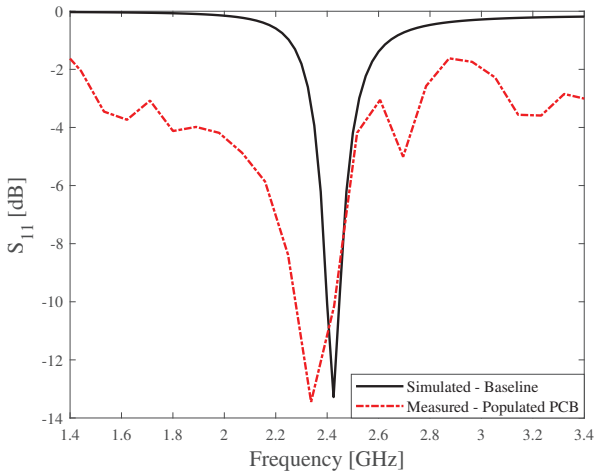


Fig. 4. Simulated and measured MIFA performance.

To compare Trojan-free and Trojan-infected PCBs and be able to extract the classification metrics, it is essential that the PCB modules present $S_{11}$ parameters as similar as possible. Fig. 5 presents the comparison of these parameters for two PCBs that are not populated. As it can be seen, the results match presenting most part of the differences for frequencies higher than 12 GHz. When both PCBs are populated strictly using the same method, some additional differences may appear. Manufacturing and soldering defects can be the major cause of differences in these measurements, but both empty and populated PCBs can be considered golden modules if a high level of similarity is maintained.

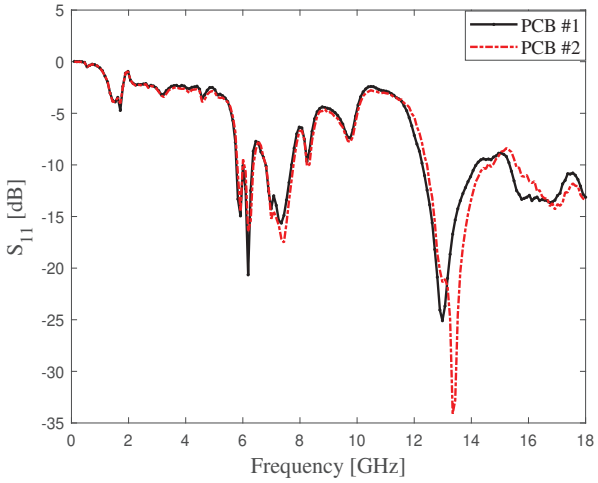


Fig. 5. $S_{11}$ measurement comparisons of empty/not populated PCBs.

The differences caused by the presence of the HT can be seen in Fig. 6, in which the data from two populated PCBs, with and without HTs, is presented. As it can be seen, the measurements are slightly different in all the considered frequency range, specially between 4 GHz and 6 GHz. The scatter plot presented in Fig. 7 confirms the aforementioned assumptions: the relationship between data from boards without HT presents a high positive correlation, and the relationship between data from boards with and without HT presents a low positive correlation. For classification and general application purposes, it should be considered that these differences are specific for this HT design.

Based on the presented results, when compared with the data of a golden module, the selected metrics are expected to provide higher correlation coefficients and lower distances when the new board under analysis is Trojan-free, as confirmed in Table II. Considering Fig. 6 results, the metrics are also evaluated in the frequency range where the differences are higher, from 4 GHz to 6 GHz, enhancing the classification capabilities of the used metrics. It is important to highlight that the values obtained for the distances cases differ more than the ones obtained for the correlation coefficient, specially due to manufacturing and soldering defects, which demonstrates in which case it would be easier setting a threshold for classifi-

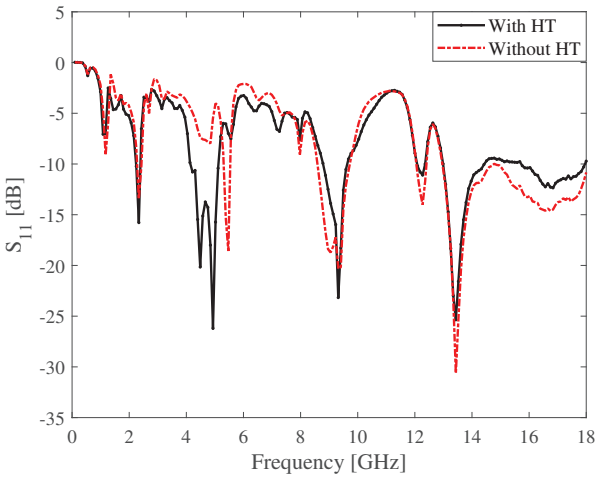


Fig. 6. $S_{11}$ measurement comparison of PCB with and without HT.

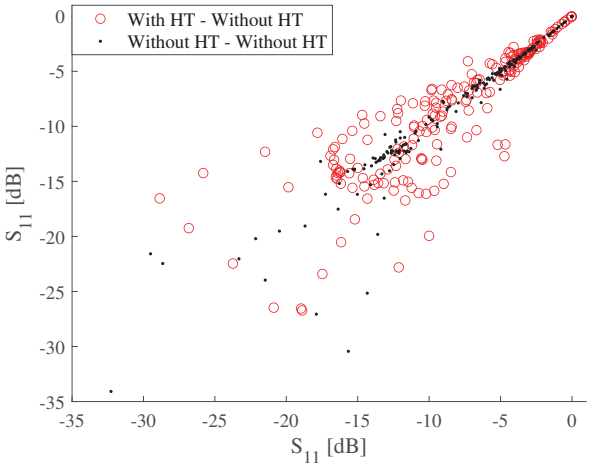


Fig. 7. Scatter plot comparison of $S_{11}$ measurements for PCBs without HT and PCBs with and without HT.

cation. For the presented cases, using the Pearson coefficient as the classification measure, the data presenting a coefficient lower than approximately 0.85-0.90 when compared to the golden module data can be considered from an untrustful module.

TABLE II
$S_{11}$ SIMILARITY AND DISTANCE MEASURES

| Measure | Freq. Range | Golden Mod. | With-Without HT |
|---|---|---|---|
| Pearson Coeff. | 0.1-18 GHz | 0.92 | 0.82 |
| Euclidean Dist. | 0.1-18 GHz | 33.05 | 44.5 |
| Manhattan Dist. | 0.1-18 GHz | 214.7 | 386.2 |
| Pearson Coeff. | 4-6 GHz | 0.99 | 0.77 |
| Euclidean Dist. | 4-6 GHz | 2.94 | 21.8 |
| Manhattan Dist. | 4-6 GHz | 9.4 | 77.2 |

## IV. Conclusions and Future Approaches

In this paper, a method that uses antenna $S_{11}$ parameters far beyond its operation frequency, as a module fingerprint to detect hardware Trojan presence in wireless modules is presented. To validate the method, a PCB is designed based on COTS modules that include a WiFi SoC, a MIFA, signal conditioning components, and a HT that can short-circuit the antenna. Similarity and distance metrics are used to compute a classification threshold to identify modules that are not reliable. The results present capabilities to use a correlation coefficient threshold of approximately 0.85-0.90 to identify the untrustful modules for the case under study, considering low manufacturing and PCB preparation errors to maintain a high correlation coefficient between golden modules. The application range of this method is limited by the effect of the HT insertion on the fingerprint of the antenna, which it is highly dependent on the type of HT used, the footprint of the hardware or its position in the PCB design, among other considerations.

To evaluate the accuracy of this method, future work includes the testing of a large set of PCBs and the implementation of a one-class classifier to classify the modules with malicious hardware. Future work also includes the analysis of the transmission parameters when the HT is activated to create additional features to be considered to improve the generated fingerprint of the module and the classifier.

## References

[1] A. Antonopoulos, C. Kapatsori, and Y. Makris, “Trusted analog/mixed-signal/RF ICs: A survey and a perspective,” IEEE Design Test, vol. 34, no. 6, pp. 63–76, 2017.

[2] M. Rostami, F. Koushanfar, and R. Karri, “A primer on hardware security: Models, methods, and metrics,” Proceedings of the IEEE, vol. 102, no. 8, pp. 1283–1295, 2014.

[3] 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 Transactions on Dependable and Secure Computing, vol. 16, no. 1, pp. 18–32, 2019.

[4] S. Narasimhan et al., ”Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis,” in IEEE Transactions on Computers, vol. 62, no. 11, pp. 2183-2195, Nov. 2013, doi: 10.1109/TC.2012.200.

[5] S. Adibelli, P. Juyal, L. N. Nguyen, M. Prvulovic and A. Zajic, ”Near-Field Backscattering-Based Sensing for Hardware Trojan Detection,” in IEEE Transactions on Antennas and Propagation, vol. 68, no. 12, pp. 8082-8090, Dec. 2020, doi: 10.1109/TAP.2020.3000562.

[6] J. Balasch, B. Gierlichs and I. Verbauwhede, ”Electromagnetic circuit fingerprints for Hardware Trojan detection,” 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), 2015, pp. 246-251, doi: 10.1109/ISEMC.2015.7256167.

[7] M. Köse, S. Taşcioğlu and Z. Telatar, ”RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum,” in IEEE Access, vol. 7, pp. 18715-18726, 2019, doi: 10.1109/ACCESS.2019.2896696.

[8] Veera Brahmam M. et al., ”Pearson Correlation Based Outlier Detection in Spatial-Temporal Data of IoT Networks,” in: Innovative Data Communication Technologies and Application, vol 96. Springer, Singapore, 2022, doi: 10.1007/978-981-16-7167-8_75.

[9] Y. Liu, Y. Jin, A. Nosratinia, and Y. Makris, “Silicon demonstration of hardware trojan design and detection in wireless cryptographic ICs,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 25, no. 4, pp. 1506–1519, 2017.