ACE: Adaptive Channel Estimation for Detecting Analog/RF Trojans in WLAN Transceivers

Kiruba Sankaran Subramani, Angelos Antonopoulos, Ahmed Attia Abotabl, Aria Nosratinia, and Yiorgos Makris
Department of Electrical and Computer Engineering, The University of Texas at Dallas, Richardson, TX 75080, USA
Email:{kiruba.subramani, aanton, ahmed.abotabl, aria, yiorgos.makris}@utdallas.edu

***Abstract*—We propose a defense method capable of detecting hardware Trojans (HTs) in the analog/RF circuitry of wireless local area network (WLAN) transceivers. The proposed method, which is implemented on the receiver (RX) side and cannot be tampered with by the attacker, leverages the channel estimation capabilities present in Orthogonal Frequency Division Multiplexing (OFDM) systems. Specifically, it employs an adaptive approach to robustly isolate possible HT activity from channel and device noise, thereby exposing the Trojan's presence. The adaptive channel estimation (ACE) defense mechanism is put to the test using a HT which is implemented on a printed circuit board (PCB) and mounted on the Wireless Open-Access Research Platform (WARP). This HT, which is introduced through minute modifications in the power amplifier (PA), manipulates the transmission power characteristics of an 802.11a/g transmitter (TX) in order to leak sensitive data, such as the encryption key. Effectiveness of the proposed defense has been verified through experiments conducted in actual channel conditions, namely over-the-air and in the presence of interference.**

I. Introduction

Hardware Trojans seeking to interfere with the legitimate operation of an Integrated Circuit (IC) and/or steal sensitive information have been the topic of intense research over the last decade. Among the numerous attacks and defenses which have been developed [1]–[7], the majority targets digital logic. Recently, however, HT attacks on wireless networks have been considered, mostly focusing on simple physical links [8]–[11]. Indeed, wireless networks constitute an attractive and plausible target, as they exchange information over public channels, eliminating the need for physical access to the nodes.

For practical reasons, such as design conservatism to reduce cost and ensure high manufacturing yield in the presence of process variations, most wireless devices do not operate at the boundaries of their circuit and standards specifications. Rather, there typically exists a margin between their operating point and the aforementioned boundaries. This margin is precisely where HTs can find room to breathe. Towards addressing and mitigating the security risk introduced by this margin, we propose a method for monitoring the characteristics of the transmission channel and identifying inconsistencies which may be caused by HTs. Specifically, our *contributions* include:

- Development of a *Trojan-agnostic* detection method based on channel estimation, which leverages transmission power characteristics along with estimated channel coefficients to expose the presence of HTs in the TX.
- Demonstration of the effectiveness of the proposed method in detecting Trojan activity, using a wireless networking experimentation platform and custom-designed hardware which embeds a Trojan in the PA of a WLAN TX.
- Verification of the method's effectiveness: (i) in actual channel conditions, (ii) across various Trojan throughputs, and (iii) over a range of Trojan impact levels.

II. Defense Mechanism

The proposed detection method leverages an existing operation of WLAN transceivers, namely *channel estimation*. This operation uses transmitted pilot symbols, which are known to the RX, to estimate channel conditions in the form of coefficients. Knowledge of these coefficients enables robust interpretation of the noisy received data. Channel estimation, however, bundles together inherent channel non-idealities, such as fading and path loss, with potential transmission disturbances due to Trojan activity. To resolve this limitation, we propose an adaptive channel estimation method which exploits the slow-fading characteristics of indoor communication to distinguish between channel-induced and Trojan-induced impact on the estimated coefficients. Thereby, any HT imposing additional structure on the transmitted signal will be detected by ACE, regardless of the attack specifics.

A. Channel Estimation

Wireless networks are susceptible to a variety of transmission impediments such as path loss, fading and interference. These factors not only restrict the reliability and data rate of wireless communications but also create uncertainties in the transmission characteristics and leave margins wherein an adversary can operate.

To mitigate inter-symbol interference caused by multi-path propagation, OFDM is commonly used in wireless networks. The transmitted data stream is sub-divided into symbols which are modulated onto orthogonal frequency sub-carriers, leading to a multi-carrier spectrum. Furthermore, OFDM inserts pilot signals and preamble within each packet to facilitate channel estimation by the RX, as depicted on the left part of Figure 1. As a result, the fading channel of an OFDM system can be viewed as a 2D lattice in a time-frequency plane, which is computed using known symbols at pilot positions and, subsequently, used to estimate the channel characteristics between pilots through interpolation. Depending on the channel characteristics (i.e., fast- or slow-fading), a block-type or comb-type pilot scheme is used to estimate the channel coefficients. Block-type channel estimation is used for slow-fading channels, where pilot symbols are inserted into all sub-carrier locations of a symbol and the channel condition is

978-1-5386-3093-8/17/$31.00 ©2017 IEEE

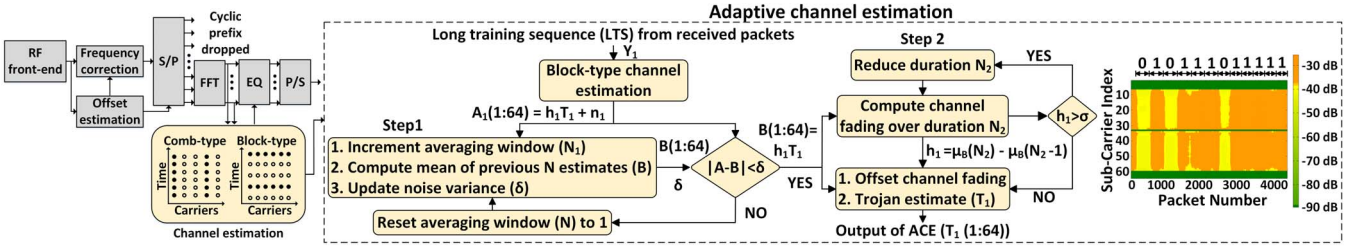

Fig. 1: Simplified OFDM RX and ACE-based detection method.

estimated once every M symbols. In contrast, a comb-type approach places pilot symbols within each symbol, thereby allowing us to estimate the channel characteristics on a per-symbol basis.

Given the slow-fading nature of WiFi, especially in indoor communications [12], we implement a block-type channel estimation algorithm, wherein the channel varies at a much slower rate as compared to the packet/symbol duration. The objective of this algorithm, which is described by Equation (1), is to estimate the channel attenuation matrix (**h**) given the matrix (**x**) containing the pilot signals - which is known to the RX - and the received signal matrix (**y**), in the presence of Gaussian white noise (**n**):

$$\mathbf{y} = \mathbf{hx} + \mathbf{n} \tag{1}$$

The RX, then, uses the estimated channel conditions to decode the received packet until the next pilot symbol arrives. The estimation can be based on least squares (LS), minimum mean-square error (MMSE), or modified MMSE [13].

B. Adaptive Channel Estimation

In a Trojan-free communication, the transmitted signal **x** is multiplied by the fading factor **h**. However, in the presence of a HT which systematically alters the transmitted signal to leak data, **x** is scaled by an additional factor **T**, which represents the impact of the Trojan, as described in Equation (2):

$$\mathbf{y} = \mathbf{hTx} + \mathbf{n} \tag{2}$$

Since channel fading matrix (**h**) and Trojan activity (**T**) are two unknown quantities which affect the transmitted signal, an unsuspecting legitimate RX estimates both factors together and considers them as a single entity in order to recover the user data. The additional capability required to separate Trojan activity from channel conditions and Gaussian noise is provided by the proposed ACE algorithm, which is shown in Figure 1 and explained next.

For each packet, the algorithm receives a long training sequence (LTS) from the packet preamble, which is processed in two steps in order to identify any Trojan activity (**T**). The first step involves removing the additive Gaussian noise (**n**), using adaptive averaging. Since the Trojan throughput is unknown to the legitimate RX, the algorithm computes the noise variance (δ) from the incoming channel estimates and uses it as a metric to adjust the averaging window duration (N_1). If the difference between the incoming estimate (A) and the mean of past channel estimates (B) is lower than δ, the window size is increased. On the other hand, if the difference is greater than δ, the algorithm considers this difference to be an anomaly and resets the window size. Once **n** has been removed, the next step is to separate **h** from **T**. To determine **h**, we compute the mean of the de-noised channel estimates over a duration (N_2), which is chosen to be large ($\sim$ 3ms). We point out that, due to slow fading, $N_2 >> N_1$. The computed mean values, μ_B in Figure 1, are compared between successive durations based on a threshold (σ), which is derived from a slow fading indoor channel model [12], to determine the rate at which the channel is varying. Accordingly N_2 can be adjusted to enhance the estimation of **h**. Once **h** has been determined, it is removed from the de-noised estimates computed in step 1, to reveal any Trojan activity (**T**).

An example of the ACE output as a function of time and frequency is shown on the right part of Figure 1. For each received packet (x-axis), the algorithm estimates channel conditions corresponding to the 64 sub-carriers (y-axis) and depicts them using a heat-map. For example, the channel estimates corresponding to the guard-band and DC sub-carrier (sub-carrier index 1:6, 32 and 60:64) are depicted in dark green as their values are small (-90dB). Similarly, for the remaining 52 sub-carriers (data and pilots), the estimates are color-coded according to their magnitude levels.

Detection of Trojan activity is, subsequently, based on the amount of variance in the generated heat-maps. Specifically, when no suspicious activity exists, removing channel fading and Gaussian noise from the ACE output results in a uniformly colored heat-map. However, when a Trojan leaking information bits is present, the ACE output between successive leaked bits spans multiple levels and, thereby, reveals the Trojan's presence. We note that channel estimates are complex values, comprising amplitude and phase components. Therefore, ACE is a powerful, attack-independent defense, capable of detecting Trojans which manipulate transmission power characteristics (e.g., amplitude, frequency, phase, or combinations thereof).

III. Analog/RF Hardware Trojans

In order to evaluate ACE effectiveness, actual implementations of HTs are required. However, to date, there do not exist examples of analog/RF HTs operating in complex wireless networks. Rather, the available body of literature has only considered HTs operating in simple wireless links. For example, leakage of sensitive information through modifications in the RF front-end of an impulse radio-based wireless cryptographic IC was presented in [8], [11]. Similarly, HTs exploiting spread spectrum techniques to hide an unauthorized transmission signal within the ambient noise floor of a simple link were shown in [6], [10]. To address this limitation, we designed and implemented a HT in the PA of a WLAN

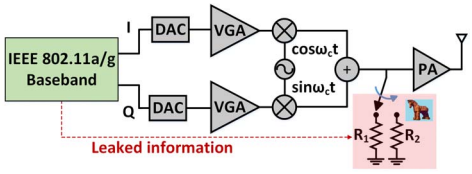

Fig. 2: Simplified model for the PA Trojan.

transceiver, which extends the principles of these methods to complex wireless networks. This HT embeds the rogue signal through imperceptible magnitude variations of the legitimately transmitted signal (which itself may have variations due to the structure of the transmission protocol), without violating the specifications of the 802.11a/g standard.

A. Threat Model

The threat model embodied in the designed HT assumes that attacks can be staged either in the design phase or during IC fabrication. The attacker has no control of the IC input space, hence the HT is always on and no trigger is required. The payload (i.e., the information to be leaked by the HT) is forwarded from the baseband domain of an 802.11a/g transceiver where it resides, to its analog/RF part, as shown in Figure 2, and may be either the encryption key or other sensitive data. Information is leaked through subtle manipulation in the transmission power characteristics, which are achieved through modifications in one or more blocks of the TX (in this case, the PA).

B. PA Attack

In a typical transceiver, I/O ports of an RF IC are terminated in a load that is matched to the output impedance of the previous stage to avoid signal reflection. The value of this impedance is typically 50Ω, which we use as a reference; we note, however, that the attack principles are independent of this value. Due to parasitics and imperfections, it is often impossible to achieve an exact impedance match. The tolerable mismatch is quantified by IC design specifications, such as input/output return loss. If an attacker manages to manipulate the termination impedance, data can be leaked by systematically varying the transmission profile.

Based on this principle, we introduce a HT circuit, which is depicted in Figure 2 and which consists of a pair of termination resistors and a Single Pole Double Throw (SPDT) switch that selects which resistor to connect to the input of the PA based on the value of the leaked bit. The information to be leaked is obtained from the baseband part of the TX and is used as the controlling signal for the HT. When connected, the termination resistor is in parallel with the input impedance of the PA, thereby modifying its value. The resistor values are chosen such that they cause subtle changes in the amplitude of the transmitted signal. In this work, resistor values of $R_1 = 0.8k\Omega$ and $R_2 = 30k\Omega$ are chosen to terminate for rogue bits "0" and "1", respectively. When terminated with 30kΩ, the signal amplitude is close to an ideal 50Ω condition, while when terminated with 0.8kΩ, there is a 5% reduction in the transmitted signal amplitude. The attacker can, then, exploit this variation to create a covert channel for transmitting data in an unauthorized fashion.

C. RX Modifications

In the implemented attack, the rogue data is introduced in the transmitted signal via amplitude variations induced by the HT. To sense these variations and obtain access to the leaked information, the rogue RX leverages the Received Signal Strength Indicator (RSSI) block. Specifically, the rogue RX, who is aware of the rogue throughput, tracks the received signal strength over the duration of one leaked Trojan bit and seeks to identify discrepancies in the power profile, beyond a certain threshold value. These subtle discrepancies are, then, translated to "0" or "1" bit values. If the environment gets noisier, the rogue transmissions must either use a higher power differential or spend a longer time on each rogue bit, while the rogue RX's integrators collect the rogue signal strength and increase its signal-to-noise ratio (SNR).

D. Trade-offs

There exists a trade-off between three key quantities involved in the operation of the HT: the rogue data rate, the reliability of the rogue reception, and how inconspicuously the HT can operate. In general, for a fixed rogue data rate, the more reliable we want the rogue reception to be, the more perceptible the HT signal will have to be (e.g., in this case the amplitude variation will have to be higher). Similarly, at a fixed rogue reception reliability level, the higher the rogue data rate, the more perceptible the HT signal. Finally, at a fixed HT signaling level, the higher the data rate, the lower the rogue reception reliability.

IV. Experimental Results

To experimentally assess the proposed defense, we built a testbed, shown in Figure 3, consisting of two WARP boards, one acting as the WiFi TX and the other as the WiFi RX, along with a custom-designed PCB implementing the PA Trojan. To characterize both the Trojan-free and the Trojan-infested transmissions, the PCB harboring the PA Trojan, which is mounted on the TX WARP board, consists of two PAs: the first PA aims to characterize the Trojan-free transmission, whereas the second PA is connected to an SPDT and two variable resistors, which are used to terminate its impedance according to the incoming leaked bit, as described in Section III-B. The input of the PA (either clean or contaminated) is connected to the output of the WARP RF front-end, whose gain is appropriately adjusted.

The PCB-based implementation of the proposed attack constitutes a proof-of-concept of the feasibility and effectiveness of HT attacks in the RF front-end of wireless networks. When integrated in a WLAN transceiver, the overhead of the HT becomes negligible compared to the overall circuit, both in terms of area and power. To verify this, we designed a Class-A PA and the Trojan circuit in GLOBALFOUNDRIES' 130nm RF CMOS process in Cadence. The HT occupies $9.56\mu m^2$ and consumes $0.72nW$, thus leaving a negligible area and power footprint as compared to the $0.57mm^2$ and $415.8mW$ of the PA. This footprint becomes even smaller when compared to the overall transceiver area and power consumption.

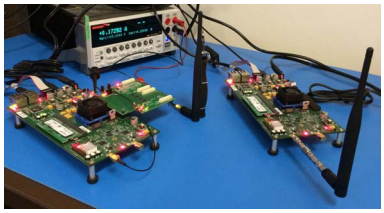

Fig. 3: WARP-based experimental testbed.

A. Attack Effectiveness

In order to retrieve the leaked data, the adversary who is aware of the attack implementation details uses a rogue RX which exploits the information available in the RSSI block, as explained in Section III-C. Figure 4 shows the signal strength of the received contaminated signal, i.e., the signal conveying both the legitimate and the leaked information for multiple packets over a duration of 3s. Within this period, the SPDT switch contaminates the transmission with rogue bits "0" and "1", reflecting the leaked information. The adversary averages the received signal strength over the duration of one rogue bit (a duration which is known to the adversary) and attributes an increase/decrease in the signal power above/below a target threshold to a leaked "0"/"1", respectively. In Figure 4, this variation corresponds to 1.5dB. However, this value can be further adjusted since the variable resistors that were used in our implementation to terminate the input impedance of the PA have a wide range between 100Ω and $50k\Omega$. When a rogue "0" bit is leaked, the PA is terminated with a lower impedance as compared to the case where a rogue "1" bit is leaked. This impacts the S_{11} performance (i.e., reflection coefficient) and, in turn, the transmitted and received power. Therefore, leaked information corresponding to higher power can be attributed to a rogue "1" bit. As demonstrated in Figure 4, all 24 rogue bits are successfully retrieved in our example.

B. Impact on Legitimate Transmission

While the adversary is capable of correctly decoding the rogue information, the impact of the HT on the legitimate transmission remains negligible. Indeed, as we demonstrate in this subsection, both TX characteristics and RX error probability remain unaffected. As previously described, the HT slightly modulates the power amplitude of the PA. This is verified in Figure 5, wherein the reflection coefficient, S_{11}, of the Trojan-free and Trojan-infested communication is plotted in a Smith chart. In comparison to the clean case, there exists only a slight shift in S_{11} when a Trojan bit is leaked. Such minute shift and variance is well-within the margins of process variation and device noise, respectively, and cannot be uniquely attributed to the presence of a HT.

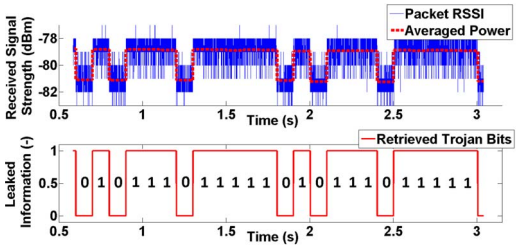

Fig. 4: Decodability of the leaked information.

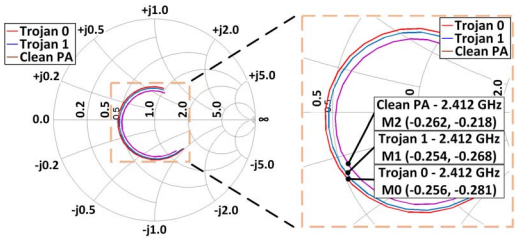

Fig. 5: Impact of the PA Trojan on S_{11}.

Similarly, the impact of the PA Trojan on the legitimate RX is also minute, as corroborated by Figure 6, wherein the error probability, expressed via packet-error-rate (PER) of the legitimate RX, is plotted versus the RX SNR. PER measurements have been performed for binary phase shift keying (BPSK), quadrature phase shift keying (QPSK) and quadrature amplitude modulation (16-QAM), all with a coding rate of 1/2, and have been repeated for Trojan-free and Trojan-infested transmissions. When the Trojan is active, a slight increase in the SNR is required in order to achieve a target PER. For example, for BPSK and a PER value of 10^{-2} this increase is less than 0.2dB and is actually sensed by the unsuspecting legitimate RX as an increase in background noise. The same trend and shift is observed for QPSK and 16-QAM. Therefore, the HT is robust across modulation schemes, demanding an imperceptible increase in power, which given the many uncertainties of wireless communications cannot be uniquely attributed to existence of a Trojan.

C. Detection Evasion

Before evaluating effectiveness of the proposed defense, we examine the ability of existing methods in detecting this HT. In WLAN transceivers, specification tests that rely on spectral mask and Error Vector Magnitude (EVM) measurements are typically applied after the IC has been fabricated. The spectrum of our PA Trojan was measured with a Tektronix MD04104-6 spectrum analyzer and is shown in Figure 7. Evidently, independent of the leaked information value, the transmitted signal power, which is centered at 2.412GHz and occupies a 20MHz bandwidth, is within the margins allowed by the 802.11a/g standard [14]. Figure 8 depicts the EVM of the Trojan-infested communication versus the transmission power for BPSK, QPSK, and 16-QAM along with the 802.11a/g specifications. The Trojan evades detection, since the measured EVM value for all modulation schemes is well below the value specified by the protocol.

Another method which has been successful in detecting HTs in ICs is statistical side channel fingerprinting [8], [15], [16]. To evaluate effectiveness of this method in detecting our attack, we performed Principal Component Analysis (PCA)

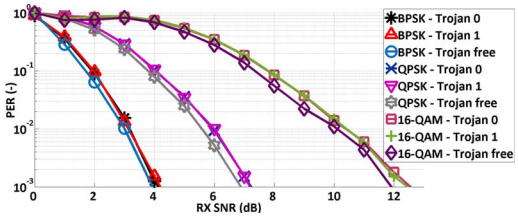

Fig. 6: PER vs. SNR of the legitimate RX.

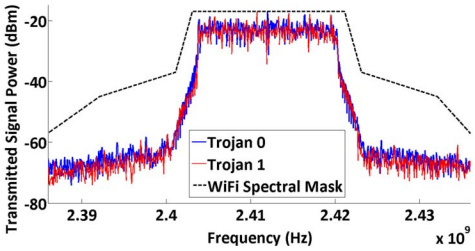

Fig. 7: Measured WiFi spectral mask.

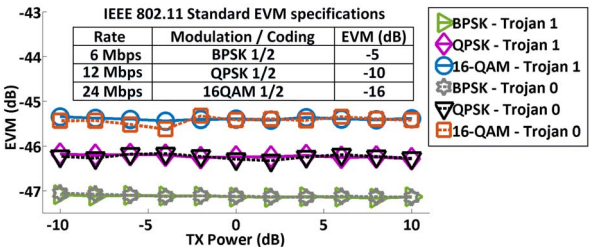

Fig. 8: Measured EVM across modulation schemes.

on data collected from the implemented PA Trojan-infested circuit. Since the malicious circuit leaks information by modifying transmission power, we measured the PA's output for six different input levels between -15dBm and +15dBm. Figure 9(a) shows three dimensions of the collected transmission power for a population of devices, where Trojan-0 and Trojan-1 correspond to termination by a 0.8kΩ and 30kΩ resistor, respectively. Evidently, the Trojan-free and Trojan-infested signatures are inseparable in the raw data. The Trojan-free data was used to generate PCA coefficients, which were later used to project the signatures onto the principal components. As shown in Figure 9(b), PCA falls short in separating the Trojan-free devices from their Trojan-infested counterparts, as the populations have only slightly shifted. Hence, it is not possible to use a one-class classifier, such as the Minimum Volume Enclosing Ellipsoid used in [8], [15], to enclose the Trojan-free measurements and separate them from the Trojan-infested ones. We also repeated this experiment with 12-dimensional data. However, as shown in Figure 9(c), PCA was still unable to separate Trojan-free from Trojan-infested signatures.

D. Defense Effectiveness

Unlike traditional functional tests and existing statistical methods which fail to detect the proposed HT, ACE is able to effectively uncover the Trojan's presence. An example of applying this method on Trojan-infested transmissions is shown in Figure 10 for BPSK modulation. Experiments were conducted in a multi-user environment to account for interference from other wireless devices. Specifically, the following setups were used to characterize the effectiveness of the defense method: (i) line of sight (LoS) between wireless nodes under various distances, (ii) non-line of sight (nLoS) with nodes positioned in adjacent rooms, (iii) varying Trojan throughput, and (iv) different Trojan impact levels.

LoS: Figure 10(a) shows the output of ACE for a clean TX. Since ACE removes channel fading and Gaussian noise from the detected channel estimates, the variations in the output of the algorithm remain uniform in the absence of malicious transmission manipulation. The experiment was repeated in the presence of the Trojan and over two distances between the communication nodes, i.e., 0.5m and 3m, and results are plotted in Figure 10(b) and Figure 10(c), respectively. In this setup, the Trojan throughput is 1bps, and the code word that is leaked is "0101 1101 1111". In this case, the channel estimation values in the presence of the Trojan are clearly distinguishable, as reflected in the different colors of the heat-maps in both plots. Thereby, the Trojan activity is successfully detected, independent of the node seperation distance.

nLoS: ACE is also capable of effectively exposing the Trojan under nLoS. This is shown in Figure 10(d), where wireless nodes have been positioned in adjacent rooms and are separated by a distance of 7m. Again, the malicious circuitry is configured to have a throughput of 1bps and the leaked code word is "0101 1101 1111". Despite the significant impact of fading and path loss on the received signal, which is represented by the minor disturbances between the detected Trojan bits, ACE is able to reveal the Trojan's presence through the variance of the heat-map.

Varying Trojan throughput: The third setup analyzes the defense effectiveness against throughput varying Trojans. Here the Trojan circuit leaks information bits "0101" at a rate of 100 bps, followed by code word "1101" at a rate of 1bps and "1111" at 100bps. Figure 10(e) shows the ACE output corresponding to this experiment. Again, the proposed method is able to isolate Trojan activity in the presence of unknown channel fading rates. This becomes evident from the distinct colors in the heat-map representation.

Varying Trojan impact levels: In the final setup the Trojan encodes leaked information using multiple impact levels. Instead of leaking a single bit at a time, the HT can increase its throughput by leaking P bits which are encoded into 2^P levels. Effectiveness of the proposed defense against such Trojan attacks is demonstrated in Figure 10(f), where the four Trojan impact levels have a different representation. The gain variance between these levels is 0.5dB. The gradient from the smallest to the biggest Trojan impact level verifies the trade-off between rogue reception reliability and HT inconspicuousness, which was described in Section III-D.

We note that the defense mechanism we proposed and evaluated: (i) is performed at the RX side, hence its effectiveness cannot be reduced by the attacker, (ii) does not rely on Trojan-free chips, and (iii) is based on general principles and does not assume knowledge of the HT attack specifics.

V. Conclusions

The margin between the operating point of a wireless transceiver and the boundaries defined by circuit specifications and network standards introduces an opportunity for HTs to compromise security of wireless networks. Towards mitigating this serious threat, we introduced a Trojan-agnostic defense mechanism based on adaptive channel estimation and we verified its effectiveness on a HT implemented on a PCB and embedded in the PA of a WLAN transceiver. Our experiments corroborate that ACE is capable of detecting the presence of malicious circuitry in WLANs, in actual channel conditions and over various Trojan impact levels and throughputs.

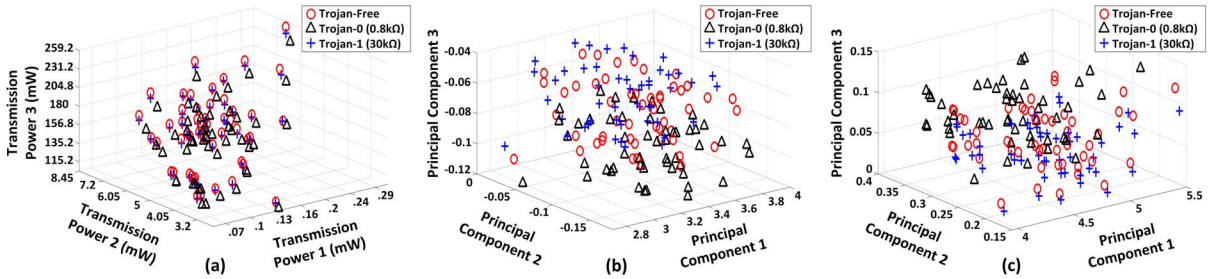

Fig. 9: PCA of: (a) Trojan-free and Trojan-infested devices projected in a three dimensional transmission power space, (b) output of PCA showing the three maximum variant principal components for a six dimensional data, (c) output of PCA showing the three maximum variant principal components for a twelve dimensional data.

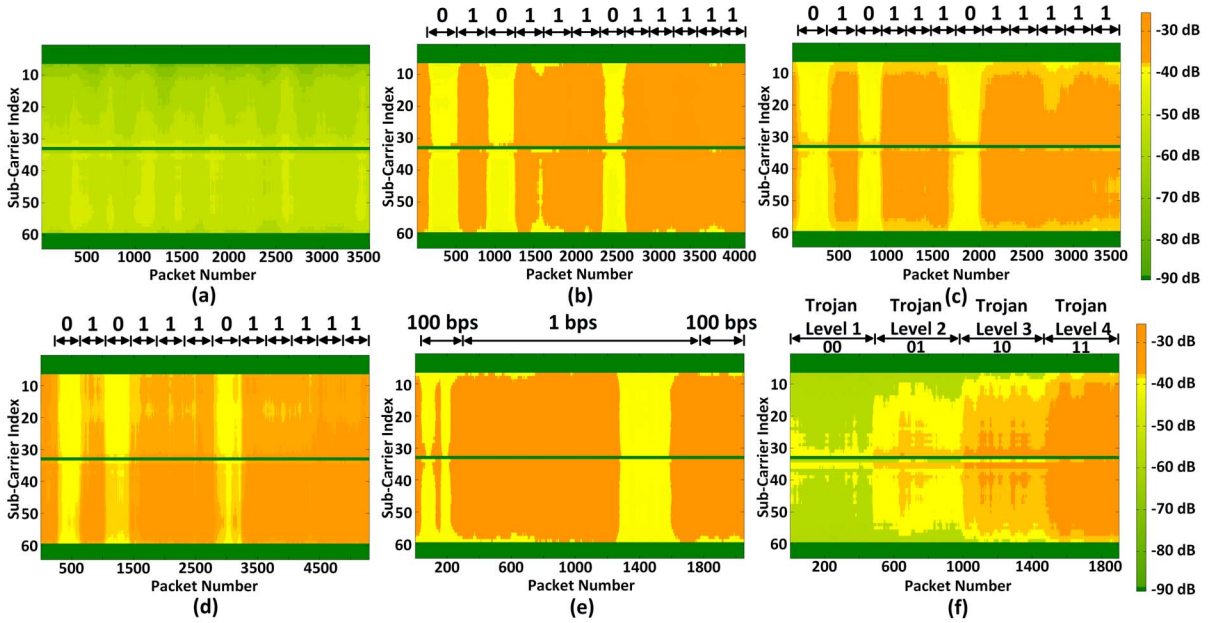

Fig. 10: ACE output for the following transmissions: (a) Trojan-free, (b) Trojan-infested over 0.5m, (c) Trojan-infested over 2m, (d) Trojan-infested nLoS, (e) Trojan-infested for varying throughput, and (f) Trojan-infested for different impact levels.

VI. AKNOWLEDGMENT

This work is funded by the National Science Foundation under grant 1514050.

REFERENCES

[1] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware Trojans: Lessons Learned after One Decade of Research," *ACM Transactions on Design Automation of Electronic Systems*, vol. 22, no. 6, pp. 1–23, 2016.

[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] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 10–25, 2010.

[4] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

[5] Y. Liu, K. Huang, and Y. Makris, "Hardware Trojan Detection Through Golden Chip-Free Statistical Side-Channel Fingerprinting," in *Design Automation Conference (DAC)*, pp. 155:1–155:6, 2014.

[6] L. Lin, W. Burleson, and C. Paar, "MOLES: Malicious Off-chip Leakage Enabled by Side-channels," in *International Conference on Computer-Aided Design (ICCAD)*, pp. 117–122, 2009.

[7] K. S. Subramani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "INFECT: INconspicuous FEC-based Trojan: A Hardware Attack on an 802.11 a/g Wireless Network," in *Hardware Oriented Security and Trust (HOST)*, pp. 90–94, 2017.

[8] Y. Liu, Y. Jin, and Y. Makris, "Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration & Detection Method Evaluation," in *International Conference on Computer-Aided Design (ICCAD)*, pp. 399–404, 2013.

[9] N. Kiyavash, F. Koushanfar, T. P. Coleman, and M. Rodrigues, "A Timing Channel Spyware for the CSMA/CA Protocol," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 477–487, 2013.

[10] D. Chang, B. Bakkaloglu, and S. Ozev, "Enabling Unauthorized RF Transmission Below Noise Floor with no Detectable Impact on Primary Communication Performance," in *VLSI Test Symposium (VTS)*, pp. 1–4, 2015.

[11] 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 Systems*, vol. 25, no. 4, pp. 1506–1519, 2017.

[12] F. Peng, J. Zhang, and W. E. Ryan, "Adaptive Modulation and Coding for IEEE 802.11n," in *IEEE Wireless Communications and Networking Conference*, pp. 656–661, 2007.

[13] Y. Liu, Z. Tan, H. Hu, L. J. Cimini, and G. Y. Li, "Channel Estimation for OFDM," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1891–1908, 2014.

[14] *IEEE 802.11-2012 Standard for Information Technology (https://standards.ieee.org/findstds/standard/802.11-2012.html).*

[15] Y. Jin and Y. Makris, "Hardware Trojans in Wireless Cryptographic ICs," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 26–35, 2010.

[16] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan Detection using IC Fingerprinting," in *Symposium on Security and Privacy*, pp. 296–310, 2007.