Hardware Trojans in Wireless Networks

Kiruba S. Subramani, Angelos Antonopoulos, Aria Nosratinia, and Yiorgos Makris
Department of Electrical Engineering, The University of Texas at Dallas, Richardson, TX 75080

I. Research Description

Wireless networks are now prevalent in most electronic systems, due to the rapid growth of telecommunications, sensor applications, and the Internet of Things. Though wireless devices use some form of encryption, the underlying hardware is still vulnerable to malicious modificiations (a.k.a hardware Trojans). Therefore, in this research work, we (i) theoretically analyze the risks posed by hardware Trojans in wireless networks, (ii) experimentally validate those risks and (iii) develop defense mechanisms to prevent such attacks.

Wireless devices inherently possess unused space, i.e. a *gap*, between their operating point and the physical limits of communication (Figure 1). A well crafted hardware Trojan, therefore, can be hidden within this gap and can be used to carryout malicious operations. Along this line, we have extensively studied the risks posed by two hardware Trojans in an IEEE 802.11a/g wireless network. The first Trojan attack is staged in the baseband part of the wireless device, more specifically in the Forward Error Correction Encoder. The second attack is staged in the RF front-end of the wireless device, namely at the power amplifier. After thorough experimental analysis to study the Trojan characteristics, we have implemented these malicious circuits on two experimental platforms, namely the Universal Software Radio Peripheral (USRP) and Wireless Open Access Research Platform (WARP). Using these two setups, we demonstrate the hardware Trojan attacks, as well as the ability of the rogue receiver to retrieve the leaked information, while an unsuspecting legitimate receiver continues to accurately recover the original message and remains oblivious to the attack. Finally, to thwart such attacks, we have developed two Trojan-agnostic detection mechanisms, namely channel noise profiling and matched filtering.

II. Baseband Attack

The first hardware Trojan attack studied in this work, exploits the Forward Error Correction (FEC) encoding used in an IEEE 802.11 a/g transmitters (TX) [1]. While FEC encoding seeks to protect the transmitted signal against channel noise, due to engineering conservativeness and design time uncertainties regarding operation variations, it offers more protection than what is needed by the actual channel. This margin is precisely where the exposed hardware Trojan finds room to stage an inconspicuous attack. To detect such a Trojan operation, we introduce a Trojan-agnostic defense mechanism (Channel Noise Profiling) which can be applied at the receiver (RX) end. This method monitors the noise of the transmission channel and based on noise distribution analysis, it identifies systematic inconsistencies which may be caused by the hardware Trojan.

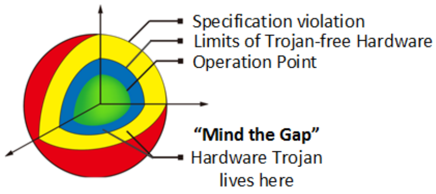

Fig. 1: The Gap

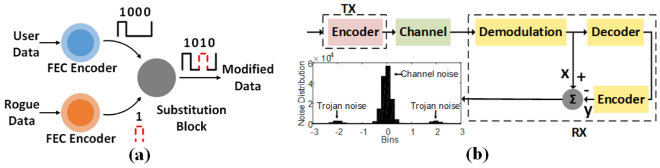

Fig. 2: FEC based Hardware Trojan (a) Overview, (b) Defense Mechanism (Channel Noise Profiling)

III. Analog / RF Attack

The second hardware Trojan is embedded in the power amplifier (PA) of an IEEE 802.11a/g transmitter's RF frontend. Here we highlight the Trojan's ability to discreetly leak sensitive information to a rogue RX by systematically varying the transmitted signal strength, while the legitimate receiver remains unaffected and oblivious to the attack. Since traditional tests fall short in detecting the exposed hardware Trojan, we propose a Trojan-agnostic detection method that leverages the channel estimation capabilities present in 802.11a/g receivers. The proposed method, shown in 3, employs an adaptive approach to robustly isolate possible trojan activity from channel and device noise, thereby exposing the Trojan's presence. The Adaptive Channel Estimation (ACE), presented in [2], is put to test against the power amplifier Trojan implemented on a printed circuit board and its performance is verified through experiments conducted in actual channel conditions.

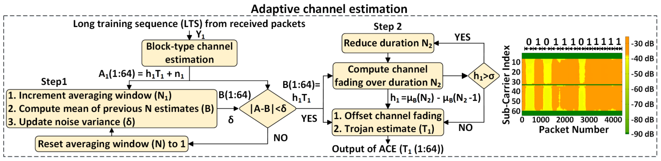
Adaptive channel estimation
Long training sequence (LTS) from received packets
Y1
Block-type channel estimation
A1(1:64) = h1T1 + n1
Step1
1. Increment averaging window (N1)
2. Compute mean of previous N estimates (B)
3. Update noise variance (δ)
B(1:64)
δ
|A-B|<δ
NO
Reset averaging window (N) to 1
B(1:64)= h1T1
YES
Step 2
Reduce duration N2
YES
Compute channel fading over duration N2
h1>σ
h1 =μB(N2) - μB(N2 -1)
1. Offset channel fading
2. Trojan estimate (T1)
NO
Output of ACE (T1 (1:64))
0 1 0 1 1 1 0 1 1 1 1 1
Sub-Carrier Index
10
20
30
40
50
60
0
1000
2000
3000
4000
Packet Number
-30 dB
-40 dB
-50 dB
-60 dB
-70 dB
-80 dB
-90 dB

Fig. 3: Adaptive Channel Estimation

References

[1] 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 *IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017*, 2017, pp. 90–94.

[2] 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 *International Conference on Computer-Aided Design (ICCAD), 2017*, 2017, pp. 722–727.

Demo: Performance Randomization for Preventing Hardware Trojan Attacks in Analog/RF Circuits

Kiruba S. Subramani, Angelos Antonopoulos, Aria Nosratinia, and Yiorgos Makris
Department of Electrical Engineering, The University of Texas at Dallas, Richardson, TX 75080

I. Research Description

In this hardware demonstration, we present a novel hardware Trojan defense technique that can be used against a variety of Trojan implementations in wireless networks. Traditional wireless devices are designed to operate within a bounded space, whose margins are controlled by the Integrated Circuits (IC) specification limits, wireless standards, device operating conditions, conservative design etc. However, for any single device in a manufactured lot, the operation region is centered around a single point in this bounded space, leaving unused area (aka GAP) for a knowledgeable attacker to exploit and stage a hardware Trojan attack. The proposed defense technique exploits concepts from chaos theory, wireless communication and tunable circuits to prevent the existence of this gap, thereby hindering Trojan operation. Essentially, the defense algorithm guides the device to operate in this bounded space in a chaotic manner, leaving no room for systematic Trojans to establish a covert communication channel. The proposed technique is Trojan-agnostic and can be easily integrated into existing platforms. Effectiveness of the defense technique will be demonstrated against two hardware Trojans that are found in literature.

II. Hardware Demonstration

In this demonstration, we will present the defense's effectiveness against two hardware Trojan attacks in an IEEE 802.11a/g network. The first attack is a timing channel spyware that manipulates the inter-packet timing of an IEEE 802.11a/g legitimate communication to establish a timing channel based covert communication link with an adversary to leak information. The second Trojan attack exploits the specification margins of ICs and the attack is staged in the Analog/RF front-end of a wireless transmitter. The introduced hardware Trojan will systematically vary the transmitted signal strength according to the leaked information.

A. Experimental Setup

The experimental setup consists of two WARP nodes and a custom designed PCB as shown in Figure 1. The timing channel spyware is implemented in the baseband logic of the transmitter. The PA Trojan is implemented on a printed circuit board and is mounted on the transmitter node. The contaminated signal from the Trojan-infested transmitter is sent to the second WARP device, which incorporates the functionality of both the legitimate and the rogue receiver.

B. Description of the observables

The following will be demonstrated to the audience:

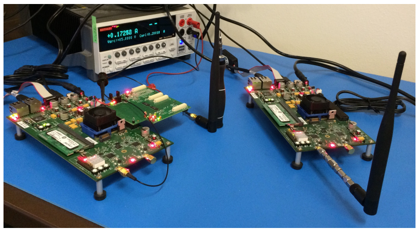

Fig. 1: Experimental Platform

1) A graphical user interface, shown in Figure 2, allows complete control over the experimental setup and displays the output plots from the experiment
2) GUI will have the option for the user to define the covert channel's message (Leaked information)
3) Received signal strength from a PA Trojan infested communication, representing the Trojan activity. Users will be able to see the leaked information (defined in the previous step) embedded in the received signal
4) Received signal strength for the PA Trojan infested communication when the defense is enabled. Users will observe that the covert communication channel no longer exists
5) Timestamps from a communication affected by the Timing channel attack, representing the spyware activity. Users will be able to see the leaked information (defined in step 2) embedded in the received signal
6) Timestamps from a Timing channel spyware circuit after the defense is enabled. Users will observe that the covert communication channel no longer exists

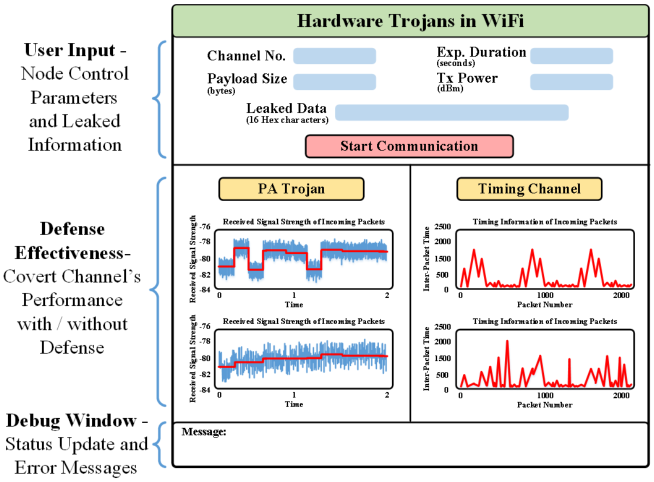

Fig. 2: Node Control GUI