Demonstration of Hardware Trojan Attacks & Defenses in an IEEE 802.11a/g Network

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

I. Research Description

The widespread use of wireless networks, along with the outsourcing of integrated circuit (IC) design and manufacturing to third parties around the globe, have rendered wireless ICs vulnerable to hardware Trojan (HT) attacks. Towards understanding the corresponding risks and developing appropriate remedies, we present the implementation of two HTs in the baseband (BB) and radio-frequency (RF) domains of an 802.11a/g transceiver. Further, we present two Trojan-agnostic defense mechanisms to prevent such attacks.

II. Hardware Demonstration

The first HT attack presented in this demonstration, exploits the Forward Error Correction (FEC) encoding used in 802.11 a/g transmitters (TX). 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 needed by the actual channel. This margin is precisely where our HT 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 a HT.

The second HT is embedded in the power amplifier (PA) of an 802.11 a/g transmitters RF frontend. Here we highlight the Trojans ability to discreetly leak sensitive information to a rogue RX, while the legitimate receiver remains unaffected and oblivious to the attack. Since traditional test measurements and existing statistical approaches fall short in detecting the HT, we propose a Trojan-agnostic detection method based on matched filtering which is implemented on the receiver side.

A. Experimental Setup

HT attack on FEC is demonstrated using two USRP devices, shown in Figure 1(a), where one functions as rogue TX and the other as both legitimate and rogue RX. The two software defined radios are connected to respective PCs running BB operations in GNURadio. The leaked information is successfully retrieved by the rogue RX and is updated to a file in real-time.

The RF attack is demonstrated using two WARP boards and a custom designed PCB as shown in Figure 1(b). The signal transmitted by the legitimate WARP node is fed into the Trojan circuit that is implemented on a custom designed PCB and is mounted on TX node. The contaminated signal is then transmitted to the second WARP device which incorporates the functionality of both the legitimate and rogue RX.

B. Description of the observables

The following will be demonstrated to the audience:

1) Baseband Attack:

- Legitimate communication between two USRP platforms
- Successful reception of leaked data by a rogue RX
- Impact of HT on legitimate communication (Figure 1(c))
- Defense mechanism (Figure 1(e)) and its effectiveness

2) RF Attack:

- Legitimate communication between two WARP platforms
- Rogue data extracted from received signal strength
- Impact of RF Trojan on legitimate communication (Figure 1(d))
- Matched-filtering based defense (Figure 1(f)) and effectiveness

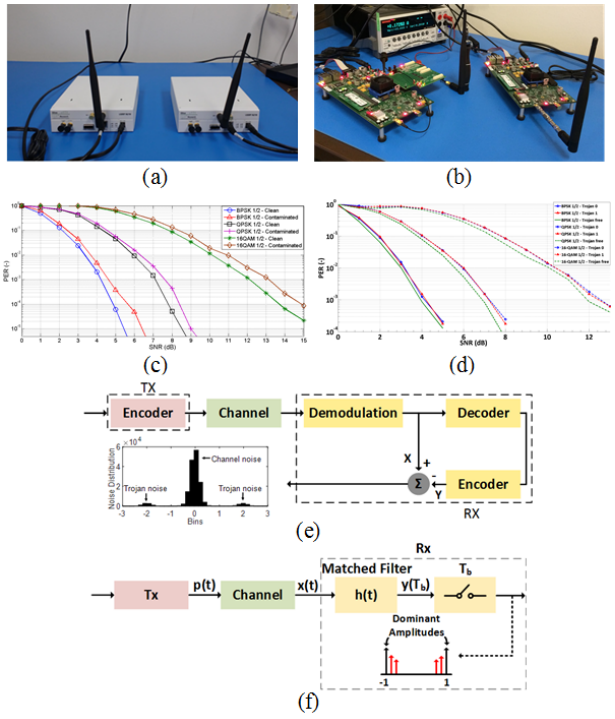

Fig. 1: (a) USRP Platform, (b) WARP Platform, (c) Impact of Baseband Trojan on Legitimate Communication, (d) Impact of RF Trojan on Legitimate Communication, (e) Channel Noise Profiling and (f) Matched-filtering based defense

References

[1] K. Subramani et. al., "INFECT: INconspicuous FEC-based Trojan: a Hardware Attack on an 802.11a/g Wireless Network," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2017 (to appear)