# Hardware Trojans in Wireless Networks: Risks & Remedies

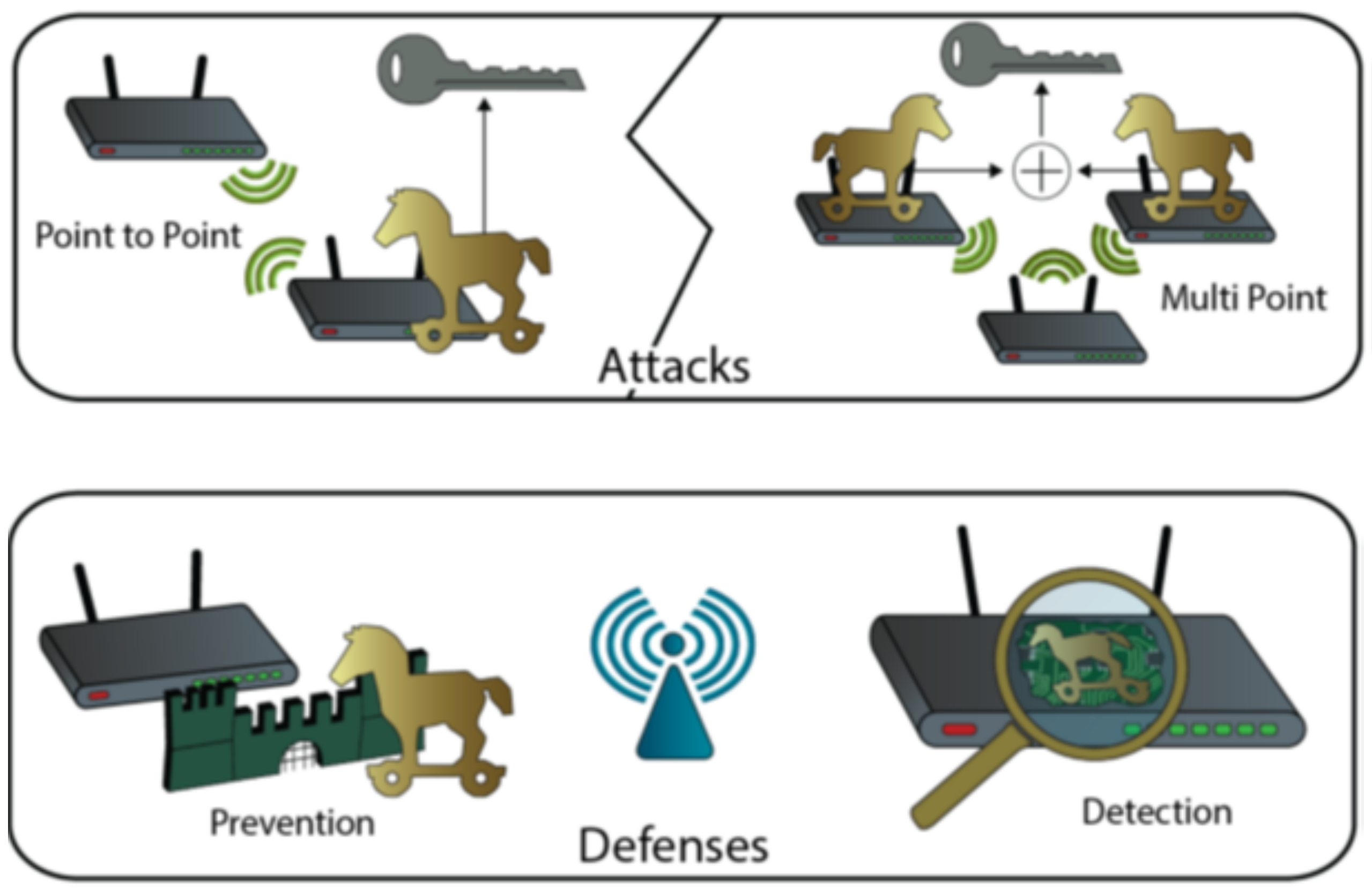
Yiorgos Makris & Aria Nosratinia
{yiorgos.makris, aria}@utdallas.edu
Department of Electrical Engineering, The University of Texas at Dallas

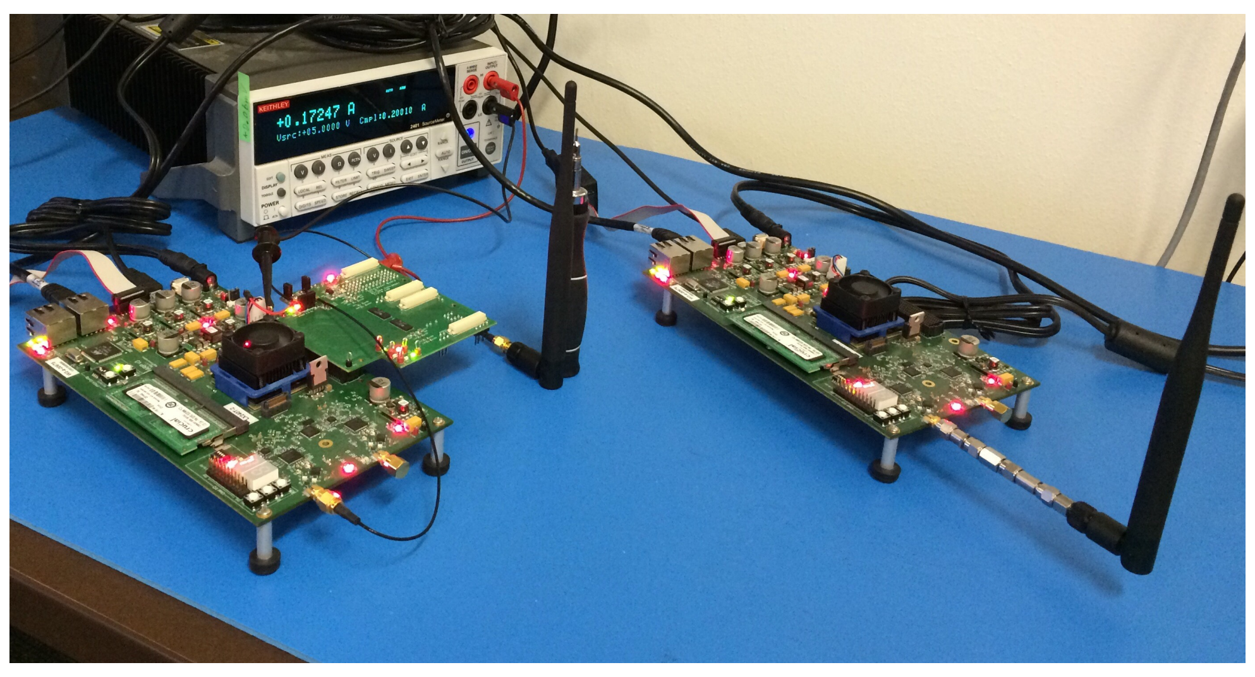
## Motivation

"Gap" between wireless transceiver operating point and physical limits of communication introduces opportunities for hardware Trojans to compromise security of wireless networks

### Project Objectives:

- Model the risk posed by hardware Trojans in wireless networks
- Elucidate feasibility of hardware Trojan attacks in an 802.11a/g network
- Develop detection and prevention methodologies
- Experimentally evaluate attacks and defenses





### Initial Demonstrations:

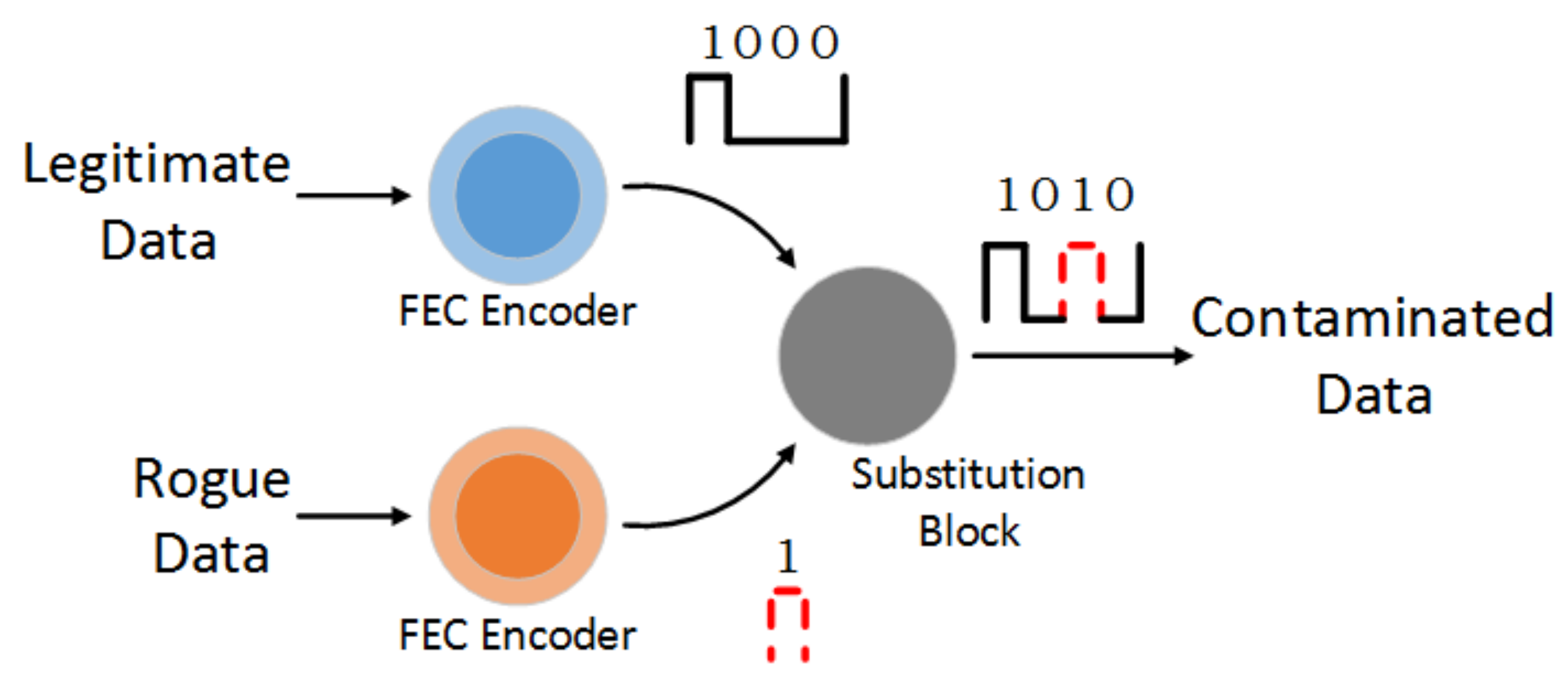
**Baseband Trojan**

- FEC-based Trojan
- Negligible overhead
- Inconspicuous
- Robust
- High rogue data rate

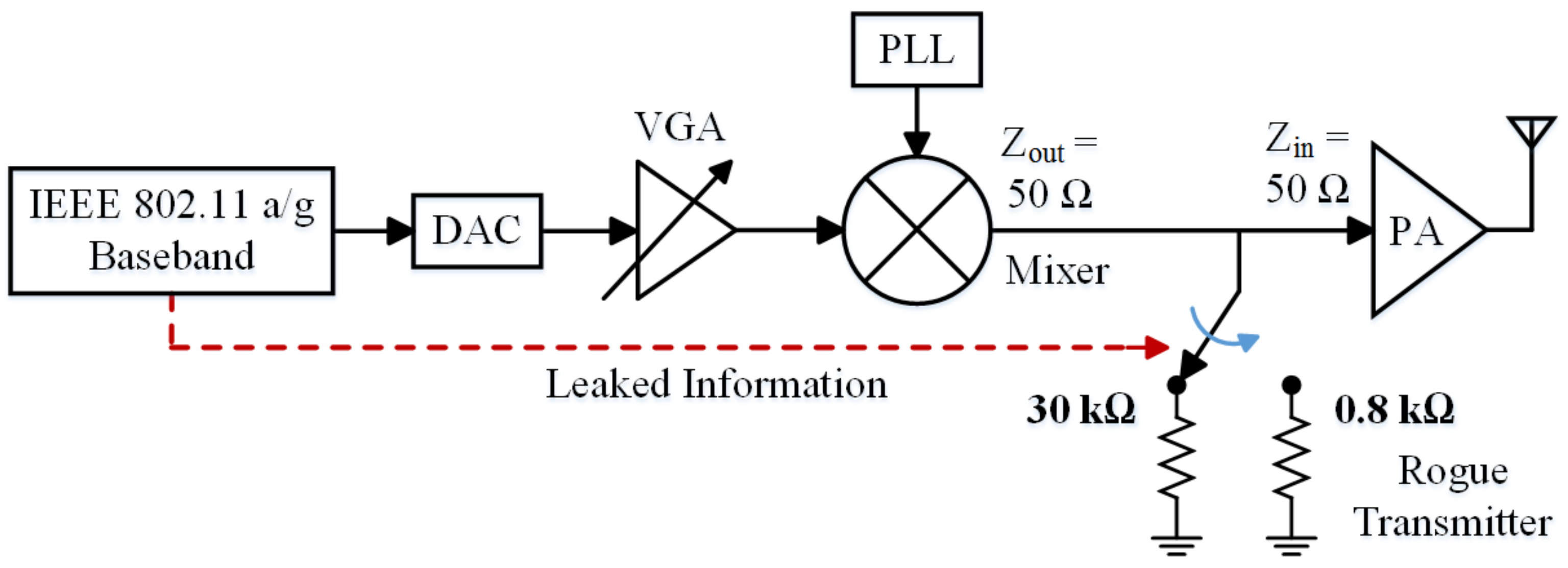
**RF Trojan**

- Modifies termination impedance
- Minute power variations
- Stealthy and robust

### Trojan Model

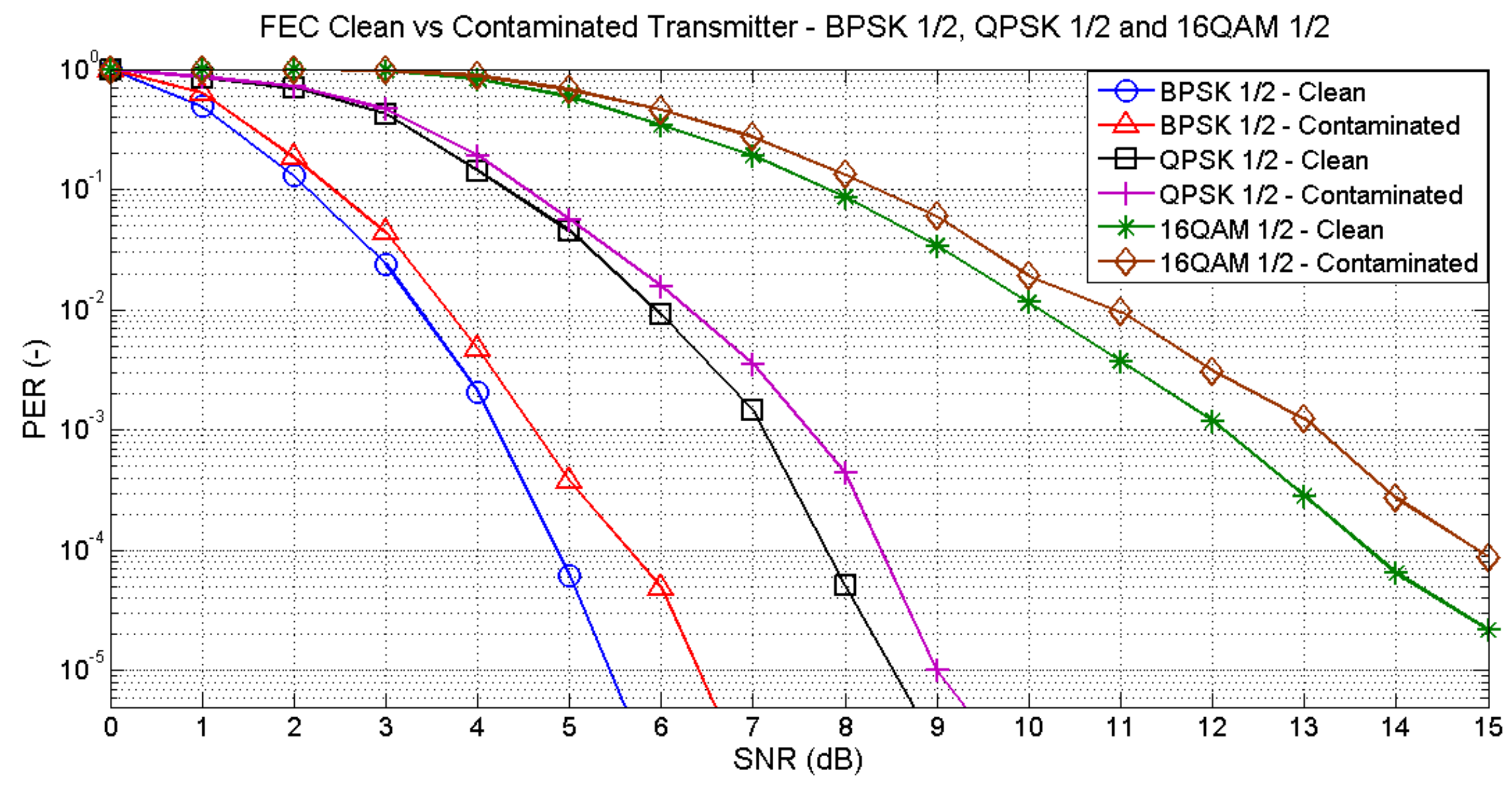


Baseband Trojan Model



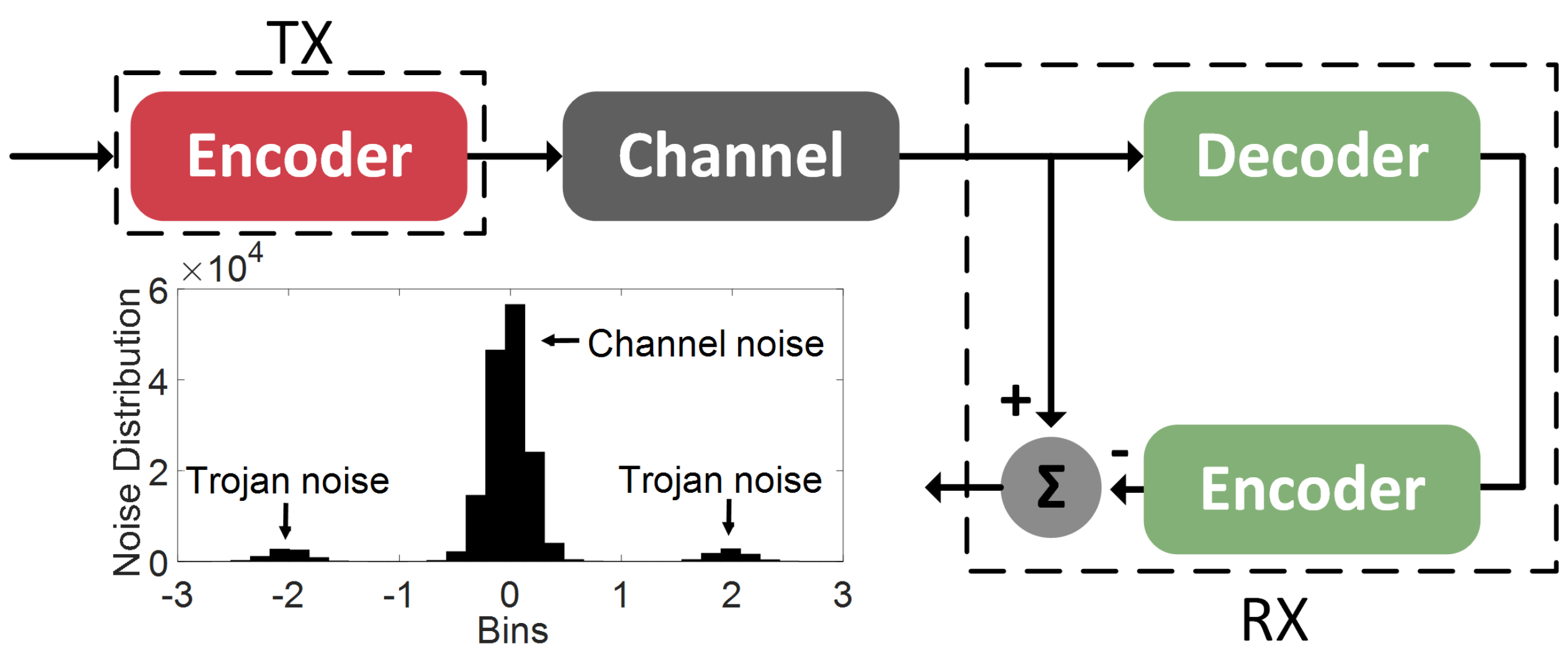
RF Trojan Model

### Baseband Trojan Results

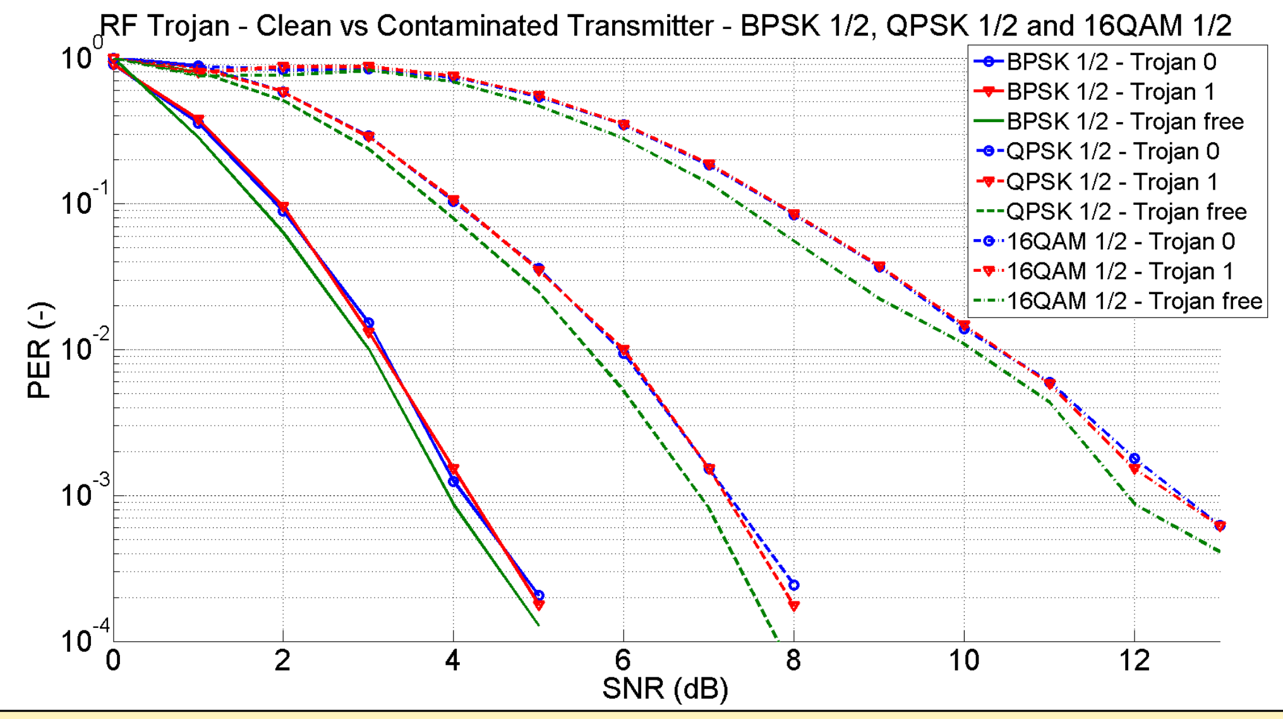


### Baseband Trojan Defense

Channel Noise Profiling

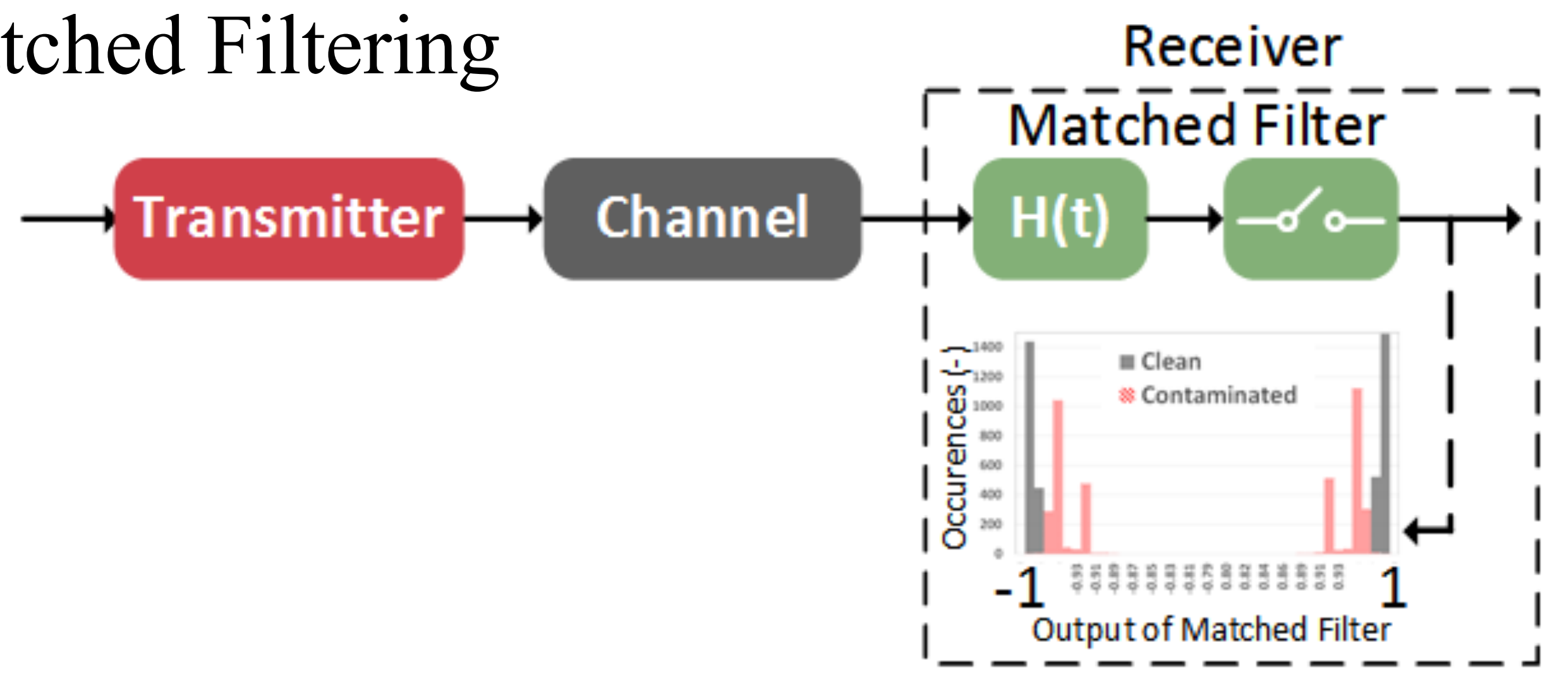


### RF Trojan Results



### RF Trojan Defense

Matched Filtering



Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Third Biennial Principal Investigator Meeting
Jan. 9th - 11th 2017
Arlington, VA

National Science Foundation
WHERE DISCOVERIES BEGIN