The Center for Cyber Defenders

Expanding computer security knowledge

SAND2016-6901C

A Foray into Wi-Fi Timing

Defending Networks through Frequency Analysis

Evan Roncevich, University of Colorado Boulder
Matthew Ghormley, New Mexico Institute of Mining and Technology

Project Mentor: Ian Zedalis, Org. 5623

Problem Statement:

Wi-Fi networks can leak a significant amount of physical information. This can reveal the location, activity, and other bits of information about devices on the network.

Our goal is to be able to use this information to protect and prevent malicious activity on Wi-Fi Networks. We need to change how the system sends signals to defend against these attacks.

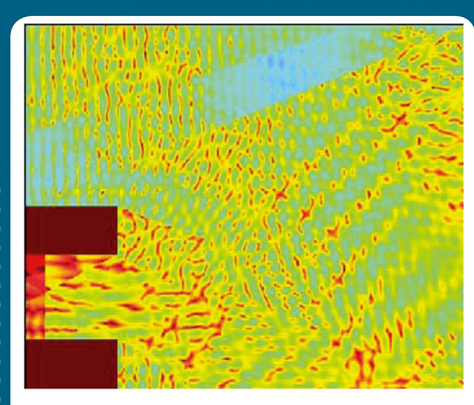
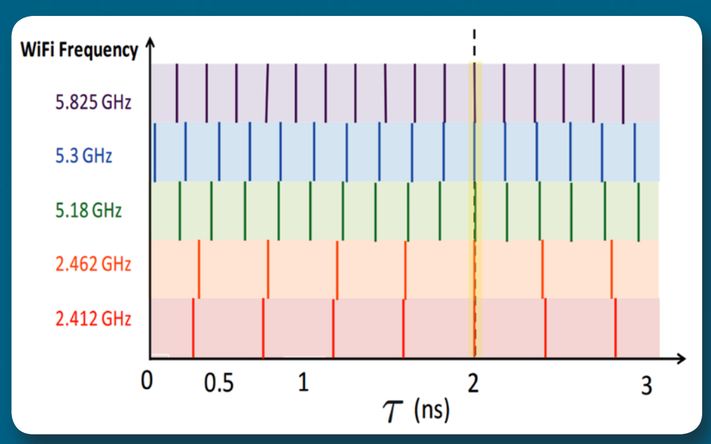


Figure 4-5—A representative signal intensity map

Wi-Fi intensity over a room.

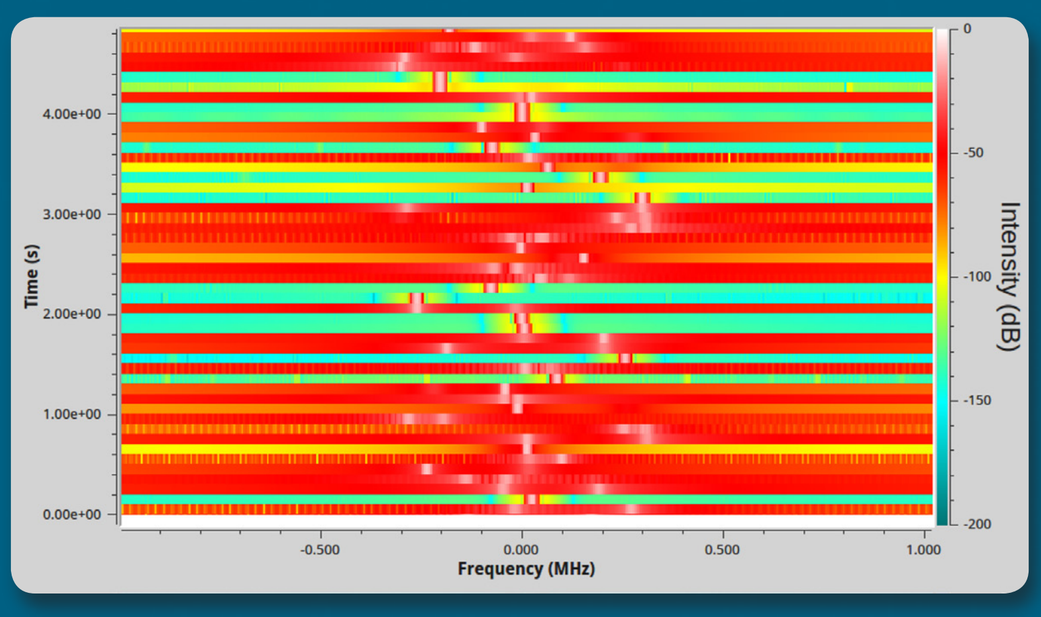


Wi-Fi sending over multiple bands.

Objective and Approach:

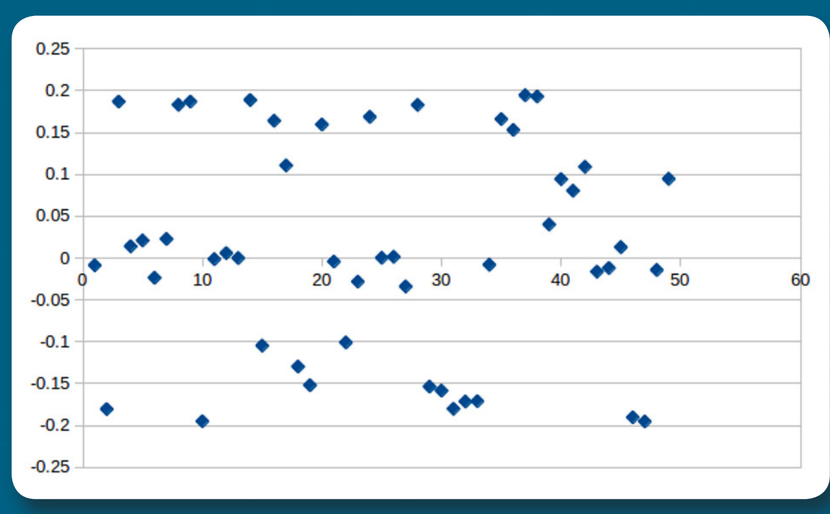
- Acquire hardware with open-source software and modifiable hardware to help us control how Wi-Fi packets are sent. This is mainly in IoT devices.
- Create a statistical classification technique for identifying a Wi-Fi device through certain physical signal characteristics. Certain patterns can be picked up in how the signal changes to determine this classification.
- Develop a model to statistically manipulate Wi-Fi to prevent traffic classification.

A Wi-Fi-enabled lightbulb with modifiable firmware.



Results:

- We developed several simple classification techniques for devices sending Wi-Fi packets.
- We used captured packet and radio signal information to perform an analysis on several different Wi-Fi devices.



- We will work on introducing statistical randomness into the Wi-Fi packet transmissions to prevent information from inadvertently being leaked from the network.

Impact and Benefits:

- Performing security scans on networks for detecting certain types of information leakage.
- Adding sufficient randomness into the system to prevent further leakage of information.
- Creating network fingerprinting to detect when foreign or inauthentic connections are added to a Wi-Fi network.

Overall, we have determined where vulnerabilities lie from physical properties in a network. These properties can reveal critical information and need to be controlled.

With this analysis technique, we can help build Wi-Fi networks that prevent information leakage while protecting themselves from malicious or foreign devices.

Sandia National Laboratories
LOCKHEED MARTIN
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-84AL8500. SAND2016-XXXXC.
U.S. DEPARTMENT OF ENERGY
NNSA National Nuclear Security Administration