Open Thesis / Project

Evaluation of Monitor Mode Capabilities in different Wi-Fi Cards

Thesis Type

Master Project / Master Thesis / Bachelor Thesis

Motivation

Although the majority of applications use Wi-Fi in the commonly known Access Point (AP) and Station modes (also called "Managed" mode), there are some other modes most Wi-Fi cards support. One such mode is Monitor mode, in which the card can listen to every packet on the wireless channel without knowing the password of the AP (albeit without understanding the encrypted payload) or without the need to join the network. With support from certain firmwares and drivers, monitor mode also allows to inject hand-crafted frames. For this reason, monitor mode has been extensively used in ethical hacking (e.g., for beacon spoofing and `DeAuth` attacks), to create jammers, in projects like `Wifibroadcast` to stream video data uninterrupted regardless of association to an AP, and more.
Since the firmware of Wi-Fi chips is usually closed source and since basic functions like sending and receiving frames and controlling rate/modulation scheme is done by the physical layer, monitor mode provides a breakthrough as it allows us to control these from user space. Using applications like `Scapy` and `dpkt`, it is possible to craft and send frame with desirable PHY attributes. We therefore want to expose the capabilities that monitor mode can provide us. Since these can vary from chip to chip and depend on the drivers used, this project focuses on experimenting with Wi-Fi cards from different manufacturers to see what is viable in monitor mode. The outcomes of this work would be of great contribution to the community and can serve as a basis for future research on wireless networking.

Goals and Tasks

The project includes the following tasks:

- Benchmark the capabilities of monitor mode in Wi-Fi chip variants such as MT76xx, RTL88xx, AX200, and others.
- Evaluate and test parameters such as achievable throughput, range of operation, latency in transmission and reception, and other features.

Target Group

- Students of ICE/Telematics;
- Students of Computer Science.

Required Prior Knowledge

- Good programming skills
  (e.g., in Python and/or C)
- Good knowledge of Linux operating system
- Good knowledge of embedded systems
- Experience in porting drivers is desirable

Contact Person

- MSc. MSc. BE Sonali Deo
  sdeo@tugraz.at
- Dr.techn. Markus Schuss
  markus.schuss@tugraz.at
- Assoc.Prof. Carlo Alberto Boano
  cboano@tugraz.at

Institute of Technical Informatics
Networked Embedded Systems Group