A Practical Radio-Receiver Detector Using Correlated Stimulated Emissions

Colin Stagner and Dr. Daryl Bechter
cbsfg8@msst.edu, daryl@msst.edu
MS&T Electromagnetic Compatibility Laboratory, Missouri University of Science and Technology

INTRODUCTION

While it is possible to detect many electronic devices by their unintended electromagnetics emissions, these emissions are often weak and intermittent. The Federal Communications Commission limits the power level of unintended emissions (ICs) that make most devices difficult to detect at long range. Some devices that intentionally capture ambient signals, such as radio receivers, may also radiate these signals back into the environment as unintended emissions. It is possible to detect a number of these devices by stimulating specific changes in their unintended emissions. This approach is known as stimulated emissions detection. Using stimulated emissions offers substantial quantitative and qualitative benefits over existing algorithms.

One class of receivers of particular interest are General Mobile Radio Service (GMRS) transceivers. GMRS radios are popular, “walkie-talkie” style radios with a range of roughly five miles (Nguyen p.6). Their low cost, long battery life, built-in squelch codes, and long range make them ideal for any number of uses, but they are also easily corrupted by devices which can be used to locate these radios—regardless of whether or not they are actively transmitting a signal. GMRS radios often incorporate direct-conversion receivers that have strong stimulated emissions, making them an ideal candidate for stimulated emissions research.

Direct-Conversion Receivers

Direct-conversion receivers use a single high-frequency oscillator to downmix incoming signals directly to baseband. The radio tunes to a carrier frequency of f1 by essentially multiplying the radio signal with the complex exponential exp(i2\pi f1 t) . However, it is difficult to generate an oscillator signal that is exactly f1; therefore, there will always be some amount of frequency drift—and high radio frequencies exacerbate this problem. At the GMRS radio frequency of 462 MHz, a frequency drift of just 0.005% will result in a tuning error of approximately 25 kHz—an entire channel away from the intended frequency. Direct-conversion receivers solve this problem by actively tracking the carrier frequency with a phase-locked loop (PLL), as shown below.

The phase-locked loop drives a voltage controlled oscillator (VCO), and this in turn provides the local oscillator signal to the downmixer. In order to improve signal isolation, most receivers use VCOs that operate at some multiple of the carrier frequency, such as 2f1 [Bruene 1999]. Thus, direct-conversion receivers may have spurious emissions at 2f1 Hz.

The radio receiver is based around the Universal Software Radio Peripheral (USRP), a software-defined radio that uses an ordinary PC for digital signal processing. The USRP grants numerous advantages, such as:

- **Flexibility:** The same hardware can run many different algorithms
- **Fast:** Does not require time-consuming hardware design
- **Open Source:** Both the hardware and the software are readily and freely modifiable

**REFERENCES**


This material is based upon work supported by the U.S. Department of Homeland Security under Award Number 2008-IT-061-ED0003. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

**NOTES**

1. **Real-Time:** Instantaneous results make testing easier
2. **Open Source:** Both the hardware and the software are readily and freely modifiable