A Practical Radio-Receiver Detector Using Correlated Stimulated Emissions

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

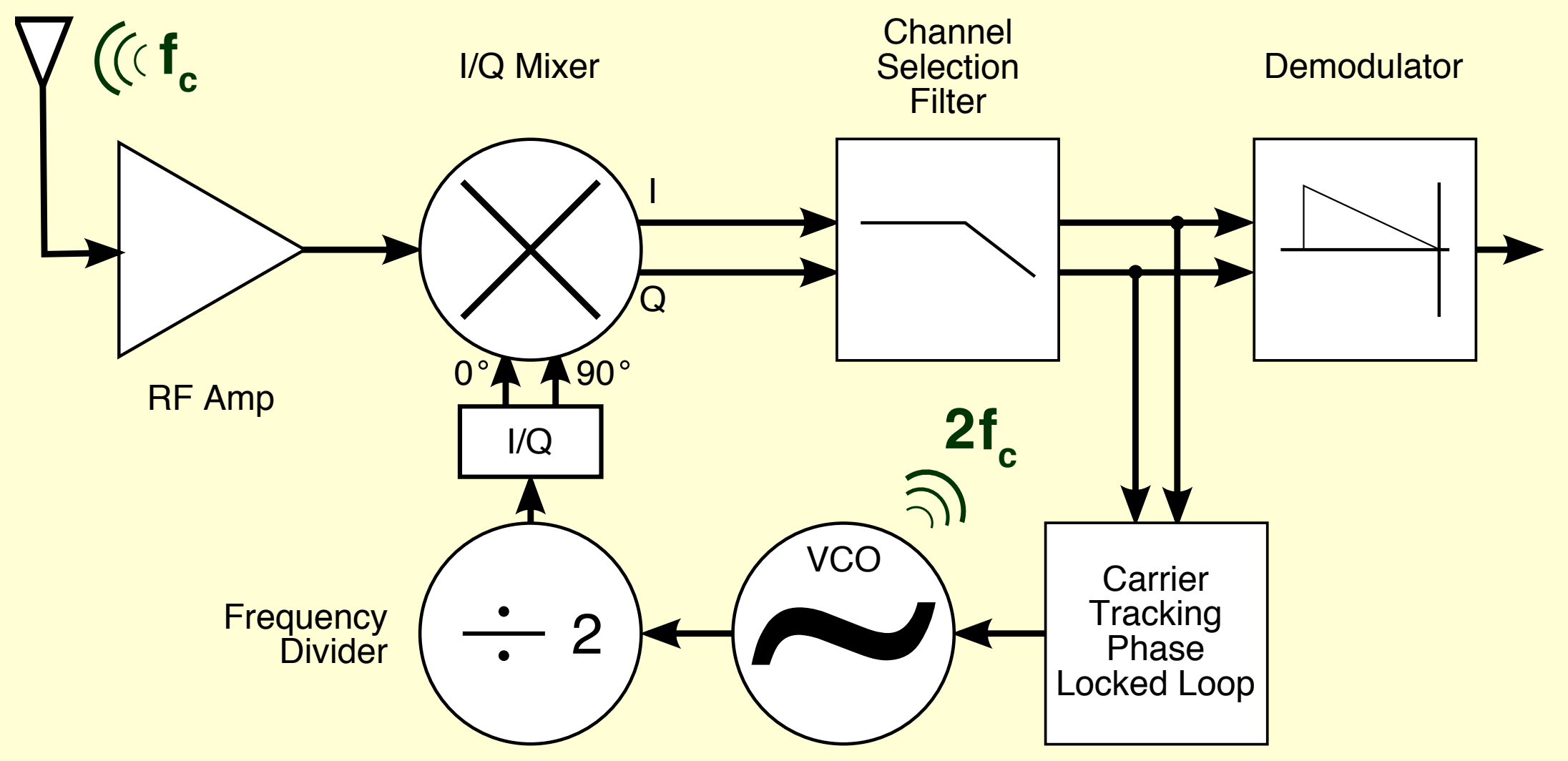
Introduction

While it is possible to detect many electronic devices by their unintended electromagnetic emissions, these emissions are often weak and intermittent. The Federal Communications Commission limits the power level of unintended emissions [FCC 1998], making 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 improve detection 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 small and easily concealed about a person or a device. In some situations, it may be a prudent security precaution 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.

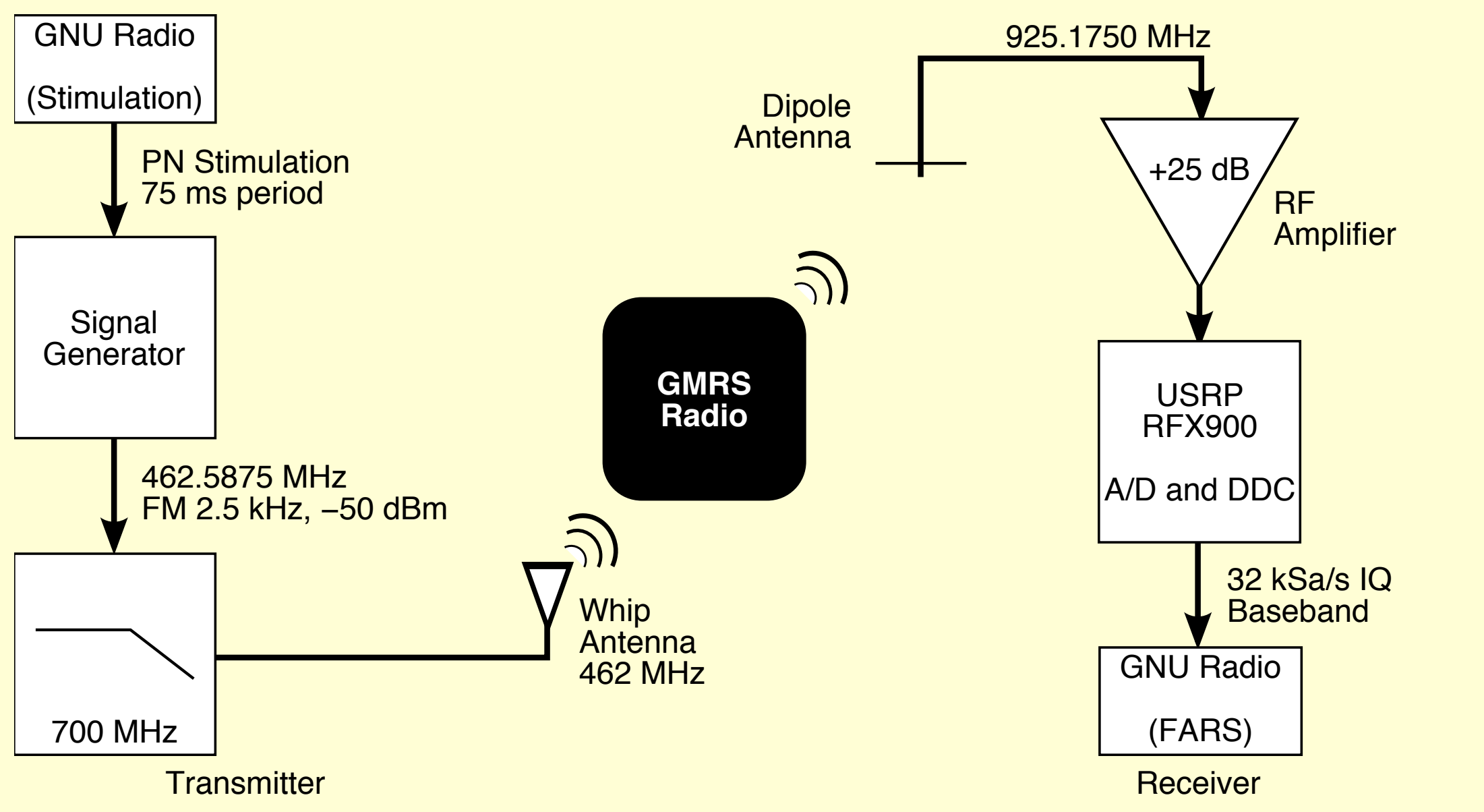
Direct-Conversion Receivers

Direct-conversion receivers use a single high-frequency oscillator to downmix incoming signals directly to complex baseband. The radio tunes to a carrier frequency of f_c Hz by essentially multiplying the radio signal with the complex exponential $e^{j2\pi f_c}$. However, it is difficult to generate an oscillator signal that is exactly f_c Hz—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 phased-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 $2f_c$ [Brueske 1999]. Thus, direct-conversion receivers may have spurious emissions at $2f_c$ Hz.

Detector Hardware

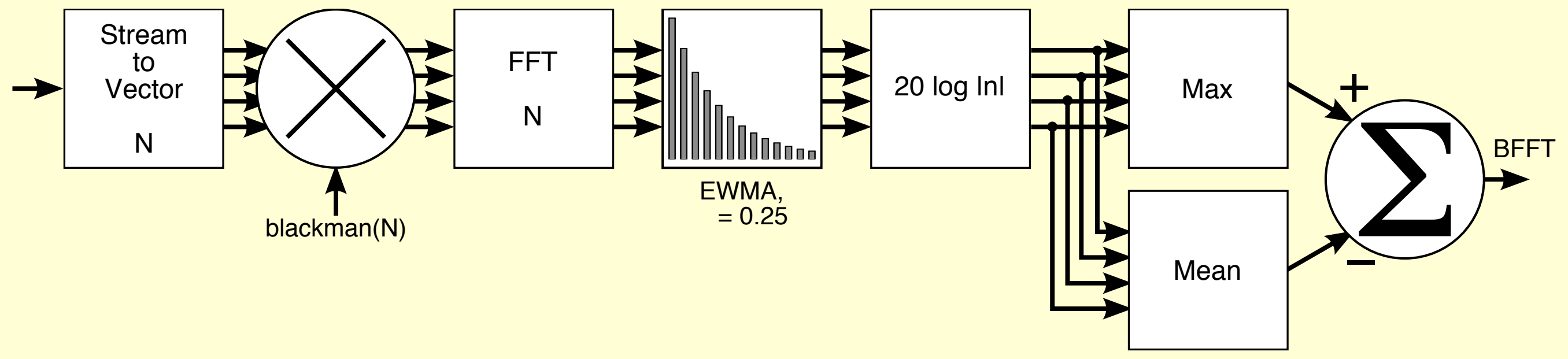


The radio detector is based around the Universal Software Radio Peripheral (USRP), a software-defined radio that uses an ordinary PC for digital signal processing. The USRP grants numerous advantages, such as:

- **Flexible:** The same hardware can run many different algorithms
- **Real-Time:** Instantaneous results make testing easier
- **Open Source:** Both the hardware and the software are readily and freely modifiable
- **Fast:** Does not require time-consuming hardware design
- **Inexpensive:** The USRP is substantially cheaper than an oscilloscope or similar high-speed hardware

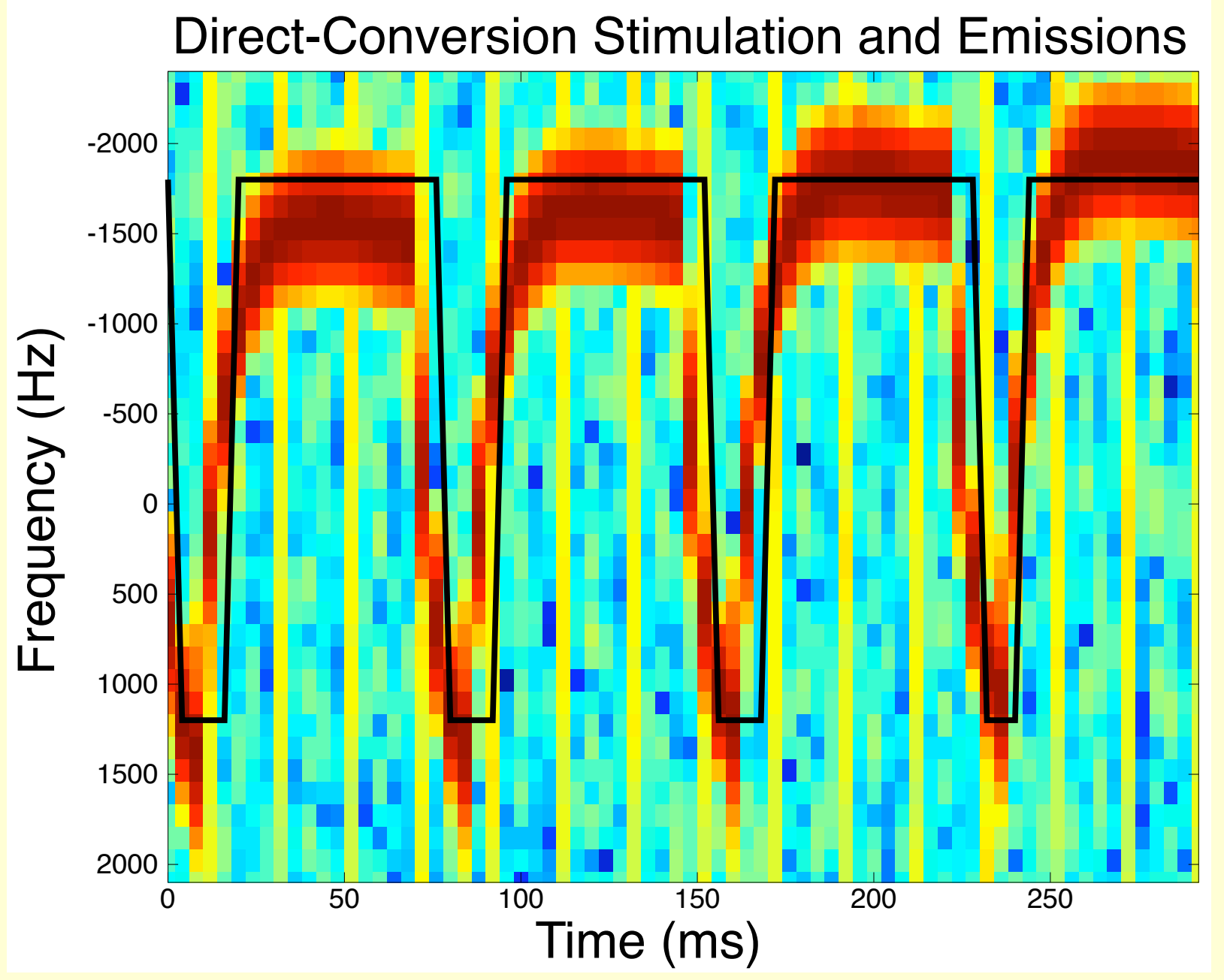
The naïve Approach

Others have documented working methods for detecting radio receivers, but these existing methods do not utilize stimulated emissions. Wild and Ramchandran demonstrated that the superheterodyne radios in many television sets have strong local oscillator emissions, and they successfully used a Fast Fourier Transform (FFT) to detect them [2005]. FFT algorithms can detect GMRS receivers as well, but most GMRS receivers deactivate their local oscillators when they are not receiving a call. This power-saving feature leaves little for the FFT to detect, limiting its effectiveness. The FFT algorithm will also detect any signal on the frequencies of interest—not just local oscillators—making it prone to false positives. Nonetheless, this approach is a good example of a naïve detection algorithm, and it is included for the sake of comparison.



The Bartlett FFT (BFFT) algorithm searches for peaks on a Bartlett periodogram, as shown above. A Blackman window is used to improve amplitude resolution, and an exponentially-weighted moving average filter (EWMA) averages multiple FFTs together to improve frequency resolution. The algorithm uses a straightforward peak detector that computes the difference between the mean and the maximum values of the periodogram.

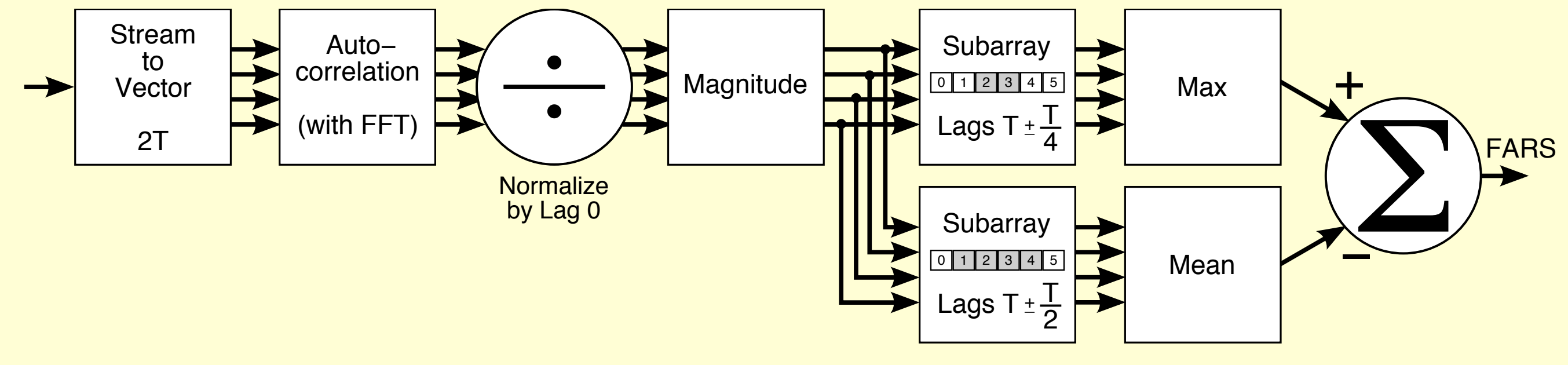
Changing the Emissions



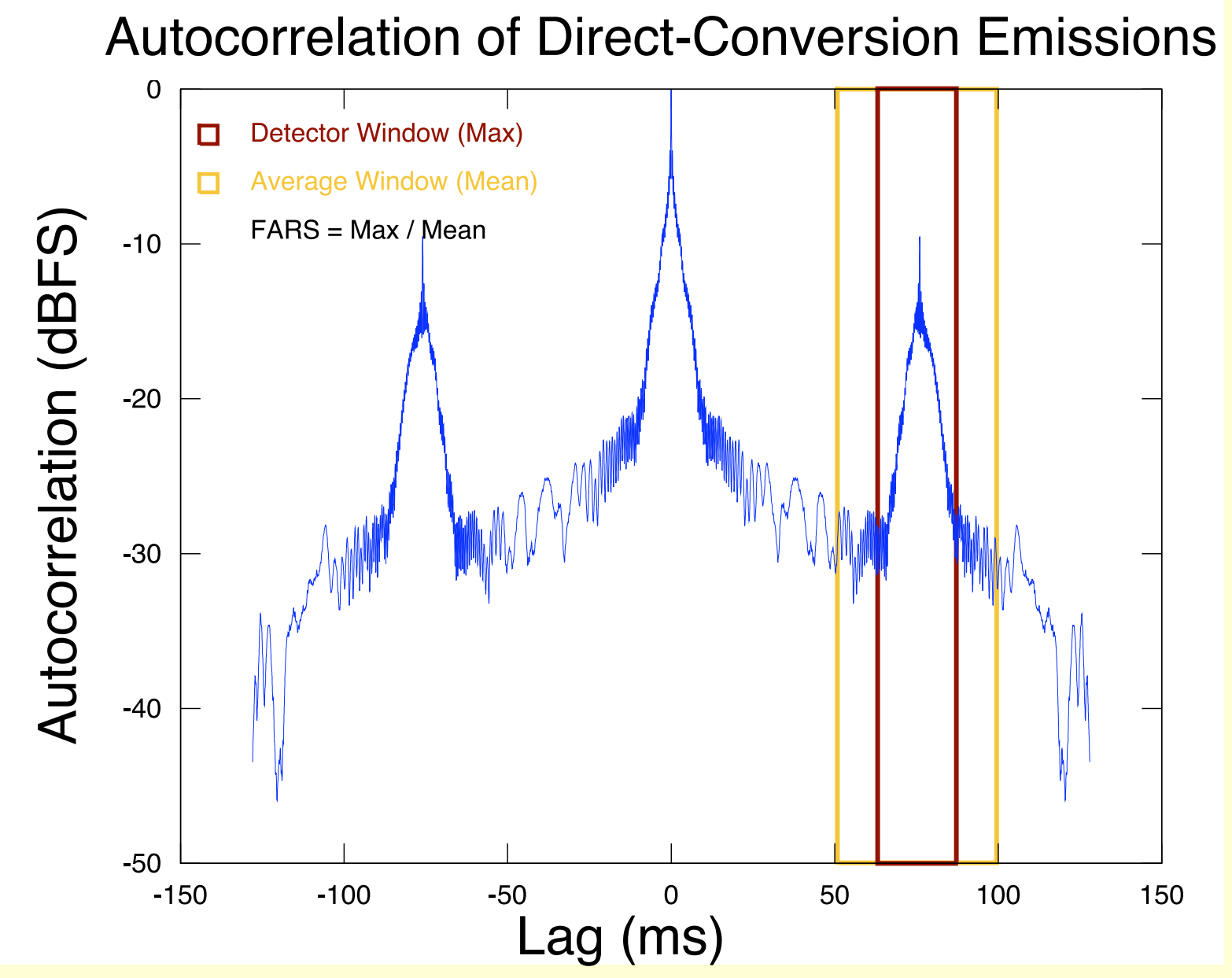
Since the emissions originate from a phase-locked loop that follows the carrier frequency, it is possible to change the PLL's frequency by changing the carrier frequency. Previous research demonstrated that varying the carrier frequency causes a corresponding change in the emissions' frequency [Conrad 2009]. As the spectrogram on the left shows, transmitting a periodically varying carrier frequency—i.e., a periodic frequency-modulated (FM) signal—will produce emissions with the same period. The stimulation signal, plotted as a thin black line, is a 75 ms FM square wave with an 80% duty cycle. The emissions' frequency changes at nearly identical rate, indicating that the phase-locked loop is tracking the stimulation signal. It is possible to utilize the periodic nature of these stimulated emissions to detect the radio receiver.

Stimulated Emissions Algorithm

Fast Autocorrelation Radio Sensing (FARS) is an algorithm for stimulating and detecting periodic emissions. FARS takes advantage of a well-known property of the autocorrelation function: the autocorrelation of a periodic signal is periodic. If the stimulation signal is approximately uncorrelated and has a length of T samples, its autocorrelation function will have sharp peaks at $\pm T$, $\pm 2T$, $\pm 3T$... lags. Since the PLL's emissions closely resemble the stimulation signal in both relative frequency and period, the autocorrelation of the emissions will have similar peaks. The complete FARS algorithm, along with a block diagram, is listed below.



1. Transmit a periodic stimulation to the radio receiver that has a period of T samples
2. Record the emissions and compute their autocorrelation.
3. Normalize the emissions by dividing each lag by the 0th lag. This makes the maximum value of the autocorrelation equal to 1.0.
4. Take the magnitude of each lag.
5. Find the maximum value of the autocorrelation in the “vicinity” (detector window) of T.
6. Find the mean value of the autocorrelation in the “vicinity” (average window) of T.
7. Subtract. The FARS statistic is a real number in the range [0, 1] that indicates how strongly the autocorrelation peaks near T. Values closer to 1 indicate a higher confidence that a direct-conversion receiver is present.



Example Autocorrelation

Detector Comparison

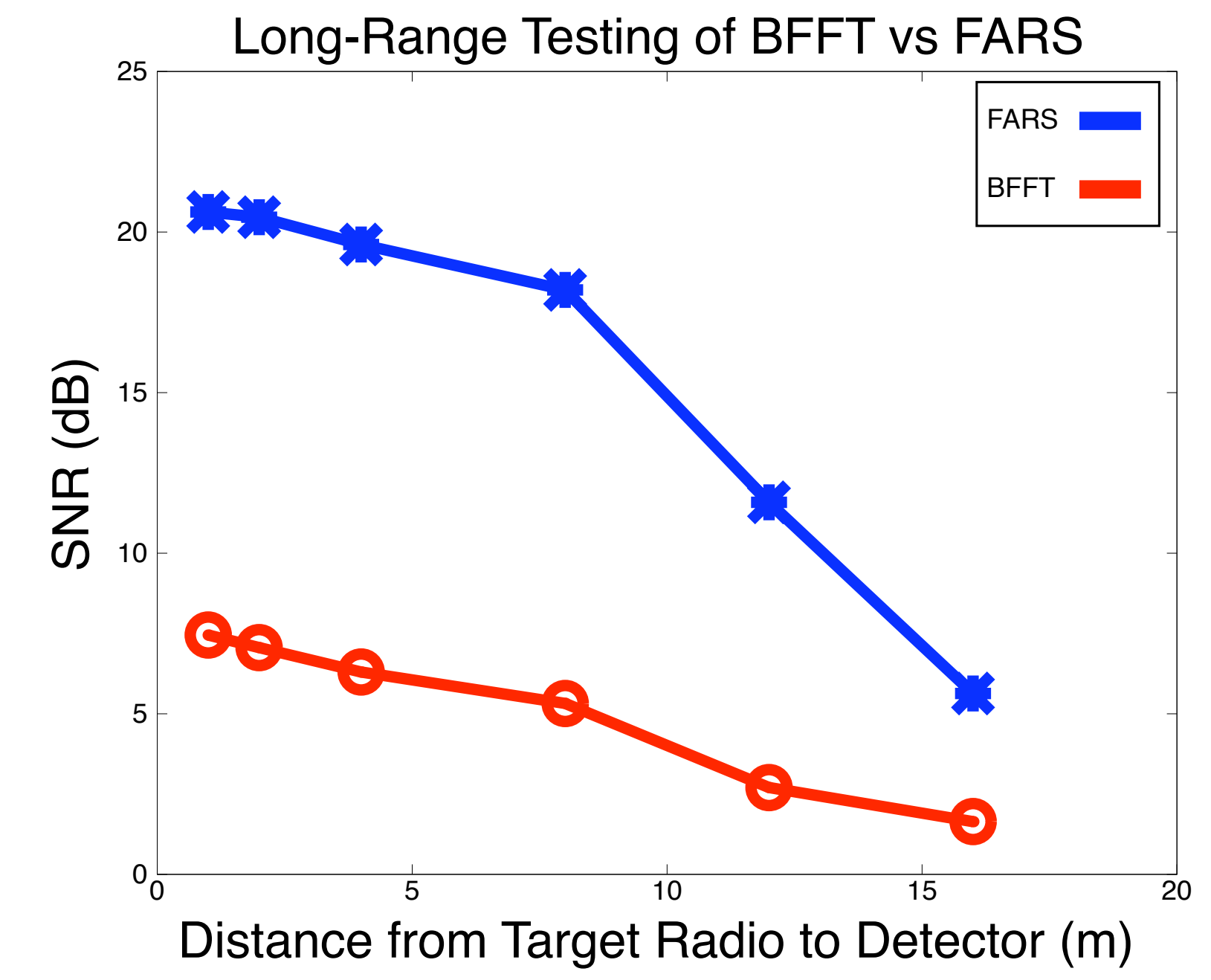
Test Procedure

The stimulated emissions algorithm (FARS) was tested against the naïve approach using the Motorola T6250, a portable GMRS walkie-talkie. Both tests were conducted using the USRP over distances ranging from 1 meter to 16 meters. The following measures were taken in order to ensure an accurate comparison:

- **Repetitions:** Both FARS and the BFFT used 15 seconds of data at each distance, resulting in over 100 statistic outputs
- **Time/Place:** Both tests were conducted indoors, in an office setting, at approximately the same time
- **Position:** The radios were kept in exactly the same position and orientation for all tests at the same distance
- **Peak Detection:** Both FARS and the BFFT use the same peak detector algorithm
- **Stimulation:** The BFFT used a continuous wave (CW) stimulation signal in order to force the radio out of power-saving mode

The signal-to-noise ratio of both algorithms was measured by finding the root mean squared (RMS) average of the test statistics when the radio was on ($S[n]$), the RMS average of the test statistics when the radio was off ($s[n]$), and calculating

$$SNR = 20\log_{10}(\mathrm{RMS}\{S[n]\}) - 20\log_{10}(\mathrm{RMS}\{s[n]\})$$



FARS Distance Test

Results

The stimulated emissions algorithm, FARS, consistently outperformed the Bartlett FFT by 9 dB at 16 meters and 13 dB at 1 meter. In addition to the quantitative signal-to-noise ratio improvement, FARS offers significant improvements in false positive rejection and frequency drift immunity. Since neither random noise nor communications signals tend to be precisely periodic, FARS will reject almost any signal that does not match the stimulation signal. FARS is a time-domain algorithm, not a frequency-domain algorithm, and as a result it can detect devices without accurately knowing their emissions' frequencies.

Conclusion

It is possible to detect the presence of direct-conversion radio receivers by using stimulated emissions—even when the radio is not deliberately transmitting any signals. Direct-conversion receivers actively track the incoming signal using a phase-locked loop (PLL), and it is possible to manipulate this PLL with a frequency-modulated signal. Fast Autocorrelation Radio Sensing (FARS) is an algorithm for detecting direct-conversion receivers using stimulated emissions. FARS transmits a periodic stimulation signal and searches for emissions with the same period using an autocorrelation. Careful testing with GMRS radios indicates that FARS performs favorably compared to existing methods, and FARS provides an improved signal-to-noise ratio and superior false-positive elimination. Despite these improvements, FARS is not a coherent detection algorithm, and it discards a great deal of time domain and phase information. Future research will explore coherent detection algorithms, which may offer superior performance, and methods for detecting superheterodyne receivers using stimulated emissions. While stimulated emissions is still a very new concept, it has the potential to form the basis of next-generation detection systems that will protect against electronic security threats.

References

D.E. Brueske, G.A. Kurtzman, and R.B. Meador. Wideband frequency synthesizer for direct conversion transceiver, April 13, 1999. US Patent 5,894,592.

A.P. Conrad. Improved detection of radio receivers by manipulating their unintended emissions through external electromagnetic-stimulation. Master's thesis, *Missouri S&*T, 2009.

FCC. Title 47–Telecommunication §15. In Code of Federal Regulations. GPO, Oct 1998.

T.X. Nguyen, S.V. Koppen, J.J. Ely, R.A. Williams, L.J. Smith, M.T.P. Salud, L. Martin, and V. Hampton. Portable wireless LAN device and two-way radio threat assessment for aircraft VHF communication radio band. *NASA Langley Res. Center, NASA/TM-2004-213010*, 2004.

B. Wild and K. Ramchandran. Detecting primary receivers for cognitive radio applications. *In New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, pages 124–130, 2005.

This material is based upon work supported by the U.S. Department of Homeland Security under Award Number 2008-ST-061-ED0001. 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.