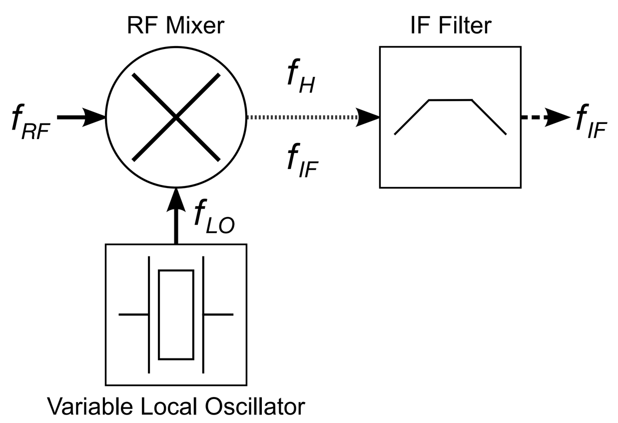
Real-Time Detection of Radio Receivers Using Stimulated Emissions

Colin Stagner, Christopher Osterwise, Daryl Beetner, and Steven Grant
Missouri University of Science and Technology

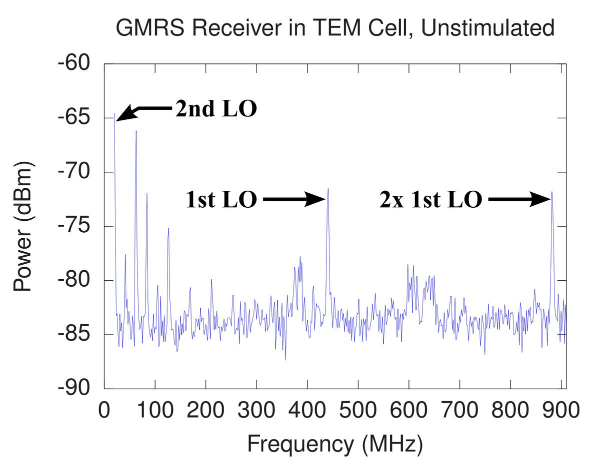
Introduction

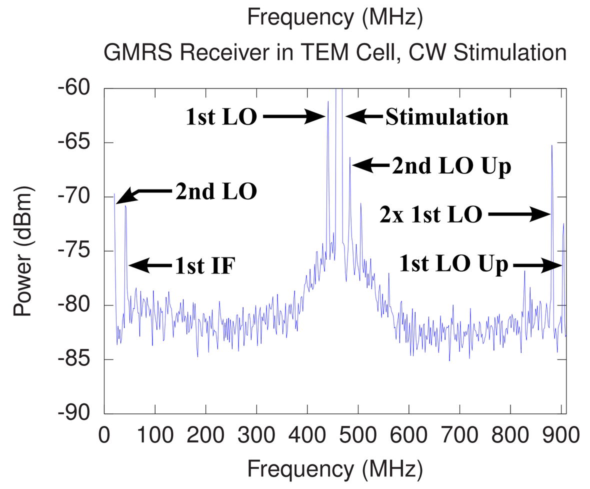
- Superheterodyne receivers can be used to initiate explosive devices
- Potential threats can be detected by locating radio receivers
- Receivers use high-frequency signals in their RF mixers
- These signals escape into the environment as unintended electromagnetic emissions [1, 2]



$$f_{IF} = f_{RF} - f_{LO}$$
$$f_H = f_{RF} + f_{LO}$$

Unintended Emissions

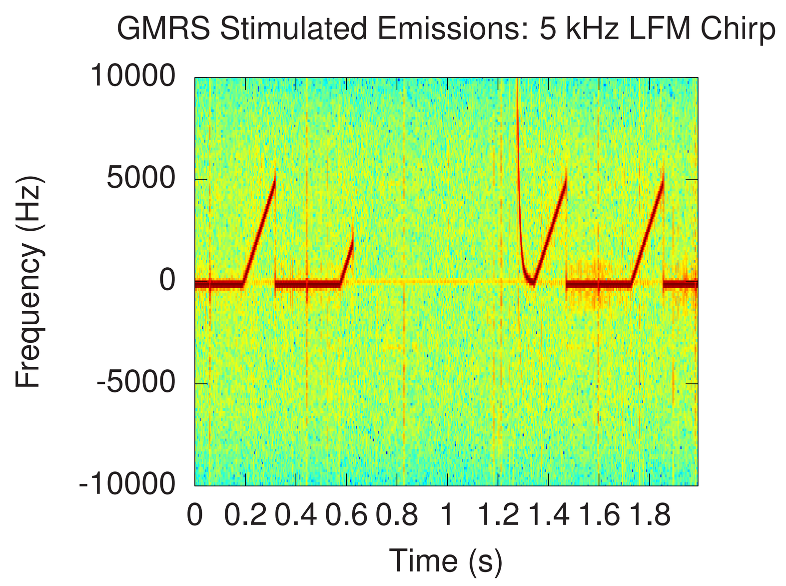




- Superheterodyne radios use mixers to perform frequency translation [3]
- Mixers have multiple unintended emissions signals
- All signals are either:
  - Local oscillators: locally-generated sinusoids
  - Mixer outputs: a frequency-translated copy of the signal the radio is receiving
- The mixer outputs consist of:
  - f_{IF} Intermediate frequency
  - f_H Up-mixing frequency
- Mixer outputs only occur when the radio is receiving a signal

Stimulated Emissions

- The stimulated emissions effect:
  - Mixer outputs (f_H) contain the original stimulation signal
  - Mixer outputs radiate back into the environment as unintended emissions
- Can use this method to inject a known signal into the f_H emissions
  - Example: linear frequency modulated (LFM) chirp
  - Works for arbitrary FM signals

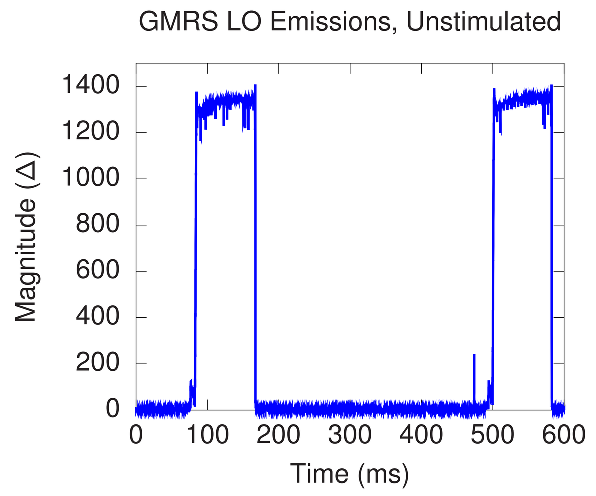


- Known signals are easier to detect than unknown signals

Challenges to Detection

Local Oscillator Duty Cycle

- Two-way radios are designed for intermittent use
- Receiver deactivates its local oscillator (LO) to conserve power
- There are no emissions of any kind when the LO is inactive
- Stimulation improves the duty cycle
  - 20% when unstimulated
  - 60% when stimulated



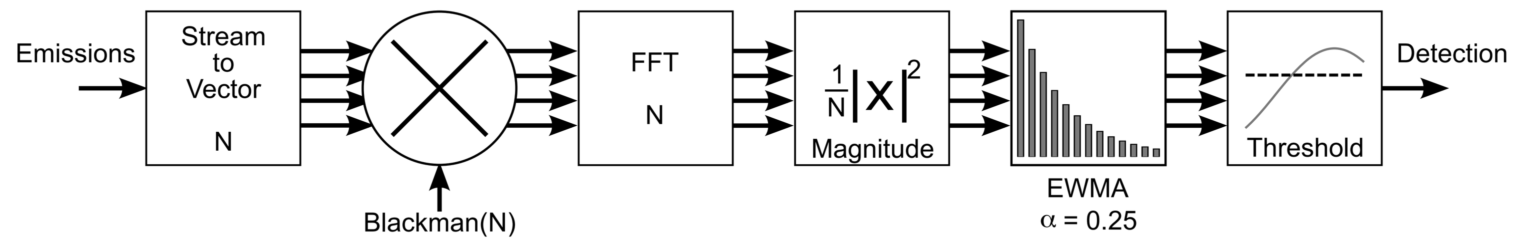
Name	Freq Range (MHz) Min	Max	Bandwidth (MHz)
f_{IF}	21.4	21.7	0.3
f_{LO}	440.8	446.3	5.5
f_{RF}	462.6	467.7	5.2
f_H	903.4	914.0	10.7

$$f_H = 2f_{RF} - f_{IF}$$

Emissions' Frequency Range

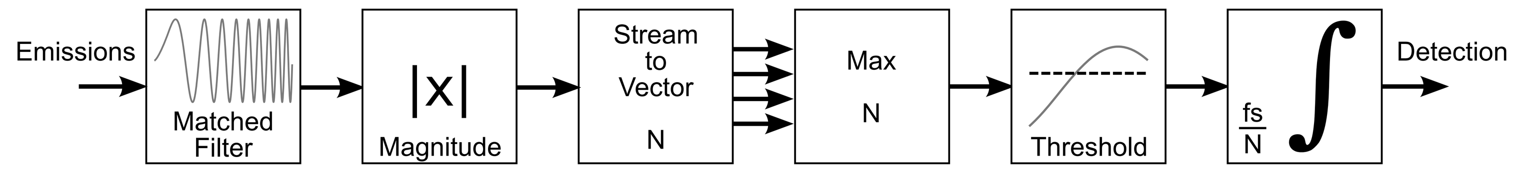
- The f_H frequency depends on
  - The channel the radio is tuned to
  - The radio's intermediate frequency
- For GMRS radios, this range is about 10 MHz wide

Periodogram Detector



- Passive detector: does not require a stimulation signal
- First proposed in [4] for detecting television sets
- Searches for sinusoidal local oscillator emissions
- Uses periodogram averaging to improve sensitivity
- The local oscillator duty cycle makes the emissions non-stationary, decreasing the effectiveness of this approach

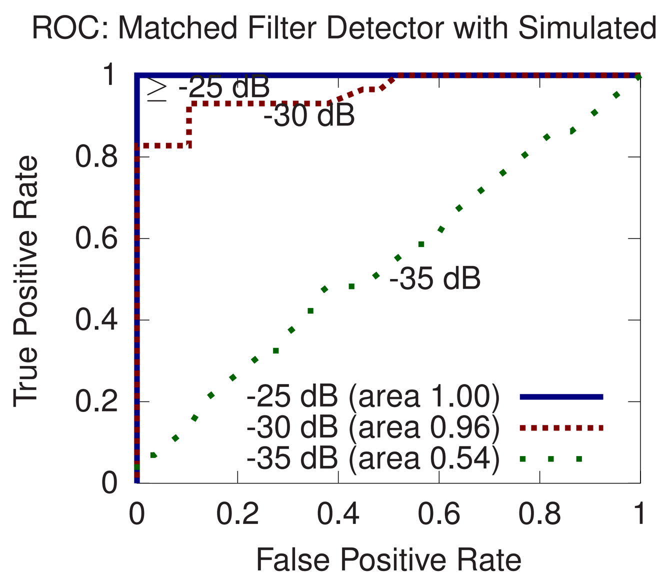
Matched Filter Detector



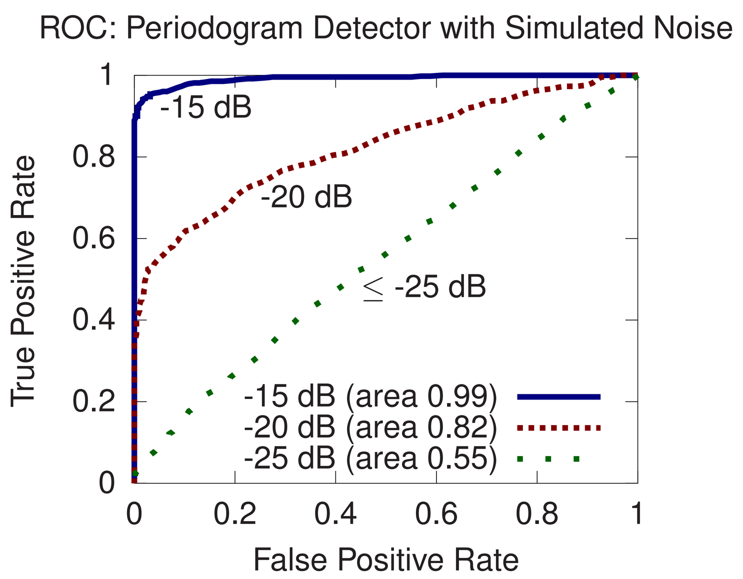
- Active detector: uses stimulated emissions
- Transmits an LFM chirp to the radio receiver
- Searches for the transmitted chirp with a matched filter [5]
  - Optimal linear filter for detecting a known signal in noise
  - We know what the unintended emissions signal is
- Key advantages:
  - Integration period is not limited by the LO duty cycle
  - Shift-immunity: LFM chirps are resistant to frequency shift

Simulated Performance

Matched Filter Detector

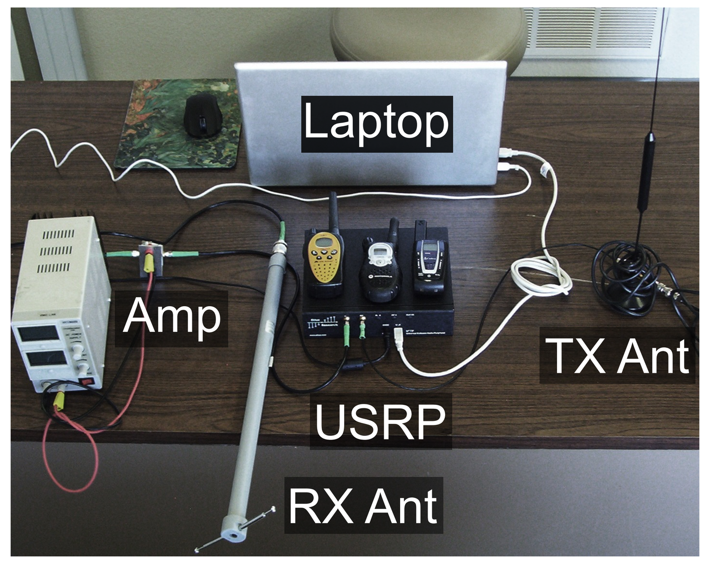


Periodogram Detector



- Quantitative improvements
  - Difficult to compare algorithms experimentally
    - Different initial emissions power
    - Different RF propagation
  - Tested receiver operating characteristics using a MATLAB simulation
  - The matched filter detector is more sensitive than existing techniques
- Qualitative improvements
  - High-frequency oscillators are not unique to radio receivers
  - If a device has a clock or other sinusoidal output near f_{LO}
    - Periodogram detector will detect it, causing a false positive
    - Matched filter detector only reacts to stimulated emissions
  - Matched filter ensures that the detected device is a radio receiver

Research to Reality



- Assembled working detector using a Universal Software Radio Peripheral (USRP)
  - Software-defined radio uses an ordinary computer for baseband signal processing
  - Low power transmitter (200 mW)
  - Completely off-the-shelf components
  - Demonstrates feasibility of constructing a hand-held detector
- The USRP System is capable of detecting nearby superheterodyne receivers in real-time

References

(1) D. Beetner, S. Seguin, and H. Hubing, "Electromagnetic emissions stimulation and detection system," United States Patent 7 464 005, 2008
(2) S. Seguin, "Detection of low cost radio frequency receivers based on their unintended electromagnetic emissions and an active stimulation," Ph.D dissertation, Missouri S&T, 2009. [Online] Available: `http://scholarsmine.mst.edu/thesis/pdf/Seguin_09007dcc80708216.pdf`
(3) R. Oki and T. Ebisawa, "Double Superheterodyne Receiver," United States Patent 4 395 777, 1983
(4) B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," *Proc. First IEEE Int'l Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, Nov. 2005, pp. 124–130
(5) G. Turin, "An introduction to matched filters," *IRE Trans. Inf. Theory*, vol. 6, no. 3, pp. 311–329, June 1960

Department of Electrical Engineering - Missouri University of Science and Technology - Rolla, MO
Mail: `cbsfg8 <at> mst.edu`