Fall 2009

Detection of low cost radio frequency receivers based on their unintended electromagnetic emissions and an active stimulation

Sarah A. Seguin

Department: Electrical and Computer Engineering

DETECTION OF LOW COST RADIO FREQUENCY RECEIVERS BASED ON THEIR UNINTENDED ELECTROMAGNETIC EMISSIONS AND AN ACTIVE STIMULATION

by

SARAH ANN SEGUIN

A DISSERTATION

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

in

ELECTRICAL ENGINEERING

2009

Approved by

Dr. Daryl G. Beetner, Advisor
Dr. Todd Hubing
Dr. Richard DuBroff
Dr. Steven Grant
Dr. Matt O'Keefe

PUBLICATION DISSERTATION OPTION

This dissertation has been prepared in three papers for publication formatted in the style used at the Missouri University of Science and Technology. The first two papers have been submitted to the IEEE Transactions on Electromagnetic Compatibility while the third paper's publication venue has not been determined at the time of the submittal of this dissertation.

ABSTRACT

Detection of super-regenerative receivers using their unintended electromagnetic emissions at a significant distance is challenging due to high levels of ambient noise. The evolution of an approach used to solve this problem is chronicled within the three papers that combine to form this dissertation. First, a passive detection method was created for detecting devices based on the characterization of their unintended emissions and utilized a cascading correlation method to confirm detection. Using a simple sine-wave stimulation to modify these unintended emissions produced better results over passive detection techniques by improving the signal quality and the consistency of the unintended emissions, but was still rather limited in extending the reliable detection distance. Additionally, extensive characterization measurements of the target device were required.

If the response of the receiver to a stimulation is known, however, a more complex stimulation can be used to embed additional information into the unintended emissions which does not require the previously essential characterization data. For regenerative receivers, an amplitude modulated stimulation generates a corresponding modulation in the unintended emissions of the target device. The receiver may thus be detected from these modulated emissions by calculating the received signal energy and then correlating it with the amplitude of the stimulation. A high correlation indicates the presence of the device. The receiver may be detected even when its emissions are well below the noise floor. Results show that five super-regenerative receivers from three different manufacturers can be detected in a noisy environment to distances of over 100 meters with an area under the receiver operating characteristic (ROC) curve of 94%.

ACKNOWLEDGMENTS

Many thanks are owed to the people who helped me through this journey. Without their assistance, guidance and support, this Ph.D. never would have been completed.

First, I would like to thank my advisor, Dr. Daryl Beetner for his continued patience with me while I blundered through explaining my developments to him. His guidance and forbearance have been invaluable during my journey. Dr. Richard DuBroff has been crucial in my development as an engineer. Thanks are also owed to the rest of my committee and Dr. David Cunningham for their suggestions.

A university laboratory is a sum of its people and especially its students. I would like to thank Jianmin Zhang, Xioher Chen, Mauro Lai, Giuseppe Selli, and Yvonne Hardesty for their many years of camaraderie, but most of all for their willingness to help whenever I needed it. I would also like to thank Kristen O'Donnell for whipping me into shape for the qualifying exam. Do not forget to always, "beat it with a dead horse!" Michael and Amy Cracraft have been vital friends for so many years, that I can not imagine a time before knowing them. Thank you, Michael, for being such an interested sounding board and, thank you, Amy, for being such a close friend.

I would like to thank my immediate family for always believing that I could do it and not constantly asking that pesky question about graduation: Dad, Mom, Nancy, Jim, Jane, Brian and David.

Lastly, I would like to thank my spouse, John Louis Seguin. Mere thanks are not enough, but these words are all I can offer for the extraordinary support you have provided. He has been a steady foundation for the roller coaster journey that has been this Ph.D. He truly has earned somewhere between one tenth to one quarter of this degree.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

SECTION

1. INTRODUCTION

Virtually any switching electronic device emits unintended electromagnetic emissions. Many applications in defense and surveillance would benefit from the ability to detect these electromagnetic emissions and properly identify the corresponding device. The challenge is to measure the relatively weak signal, strip away the ambient noise, and differentiate between multiple devices in the same frequency spectrum. It would also be beneficial to detect a device at a particular frequency band from a great distance.

The evolution of an approach used to solve this problem is chronicled within the three papers that combine to form this dissertation. First, a passive method was created for detecting devices based on the characterization of their unintended emissions. Detection was accomplished using a cascading correlation method to obtain an ideal pulse that is then cross correlated with ambient electromagnetic measurements to determine the presence of the receiver. This novel method accounts for variations in pulse characteristics to improve the accuracy of detection. Results using simple laboratory equipment show these receivers can be detected in a noisy environment with an area under the receiver operator characteristic (ROC) curve of 98%.

While this discovery provided a method of identification, its range was still somewhat limited. It was discovered that the receivers under test respond consistently, however, to a radio frequency stimulation and their emissions can even be frequency and amplitude modulated to a certain extent. Using a stimulation improves the signal quality and consistency from these receivers, but the most important effect is the ability to modulate their emissions in a known manner. This modulation allows for the creation of a detection algorithm that looks for very specific characteristics in the emissions, potentially allowing detection of the emissions when they are below the noise floor and allowing detection of super-regenerative receivers as a class of devices. These advancements helped increase the reliability and distance of detection. A US patent was also awarded for the invention of this technique [1].

While using a stimulation to modify the emissions produced better results over passive detection techniques, the method was still rather limited in extending the reliable detection distance. Additionally, extensive characterization measurements of the target device were required. If the response of the receiver to a stimulation is known,

however, a more complex stimulation can be used to embed additional information into the unintended emissions which does not require the previously essential characterization data. For regenerative receivers, an amplitude modulated stimulation generates a corresponding modulation in the unintended emissions of the receiver. The receiver may thus be detected from these modulated emissions by calculating the received signal energy and then correlating it with the amplitude of the stimulation. A high correlation indicates the presence of the device. The receiver may be detected even when its emissions are well below the noise floor. Results show that five super-regenerative receivers from three different manufacturers can be detected in a noisy environment to distances of over 100 meters with an area under the receiver operating characteristic (ROC) curve of 94%.

PAPER

1. DETECTION AND IDENTIFICATION OF LOW-COST RF RECEIVERS BASED ON THEIR UNINTENDED ELECTROMAGNETIC EMISSIONS

1.1. ABSTRACT

Virtually any switching electronic device emits unintended electromagnetic emissions. Many applications in defense and surveillance would benefit from the ability to detect these electromagnetic emissions and properly identify the corresponding device. The challenge is to measure the relatively weak signal, strip away the ambient noise, and differentiate between multiple devices in the same frequency spectrum. The unintended emissions from super-regenerative receivers were examined and used to develop a detection scheme for these receivers. Detection was accomplished using a cascading correlation method to obtain an ideal pulse that is cross correlated with ambient electromagnetic measurements to determine the presence of the receiver. This novel method accounts for variations in pulse characteristics to improve the accuracy of detection. Preliminary results using simple laboratory equipment show these receivers can be detected in a noisy environment with an area under the receiver operator characteristic (ROC) curve of 98%.

1.2. INTRODUCTION

Electronic devices give off unique electromagnetic signals as a result of their board layout, circuit design, packaging, and other variables. These emissions may be used to detect and identify the device. The challenge is detecting the weak electromagnetic emissions from the device in the presence of other, sometimes very strong, intentional emissions sources.

A common method of detecting the presence of an electronic device is to use a "bug scanner", which stimulates an emission to detect non-linear junctions. These bug scanners work by illuminating a desired target with a known electromagnetic stimulation that is then modulated by non-linear junctions in the device, causing it to re-radiate harmonics of the original stimulation signal [9]. This technology is

difficult to use in practice due to the large number of non-linear junctions that respond to this type of stimulation, the relatively weak response from the device, and the high power levels required to trigger a measurable response. For example, the non-linear response from a rusty nail is similar to the response from an electronic device such as a radio receiver. The reflected power is typically about 90 dB below the incident power, requiring these detectors to either be used at very high power or at close range to be effective. Handheld devices that operate at "safe" levels of 1–3 W typically have a range of only a few meters.

Some work has already been done to passively detect and identify electronic devices based on their electromagnetic emissions. One system has been designed to determine if cell phones have been powered on while onboard an aircraft in flight by using knowledge of the intentional electromagnetic emissions from the phone as it communicates with a base station [2]. This technique, however, will not work for a device that does not intentionally radiate. Additional work has shown the potential of passively identifying wireless receivers based on their unintended emissions using simple matched filters [3]– [5] or using neural networks [7]. Other efforts have shown the possibility of detecting more sophisticated electronic devices such as automobiles [3], [6]. Here we present an advanced technique for passively detecting and identifying a regenerative receiver based on its unintended emissions. Unlike bug scanning devices, our technique enables us to successfully identify these devices while far from the device without using a stimulation source. In addition, because simple cross-correlation is insufficient due to erratic variations in the time and frequency characteristics of the signal, a consistent direct match would be impossible. The discussed technique, therefore, employs a cascading correlation to determine if an electronic device is present by analyzing specific characteristics of the emissions in both the time and frequency domain.

1.3. METHODS

The detection methodology can be broken down into three phases as illustrated in Fig. 1.1. First, a device is characterized by acquiring a series of measurements of its emissions in the time and frequency domain. These measurements are used in the second phase to develop an ideal pulse in the time domain. The third phase, device detection, utilizes all the data acquired during the device characterization phase in combination with the ideal pulse to determine the presence of the device in

an unknown environment. For the purposes of this study, a low-cost RF toy truck was utilized to represent a typical super-regenerative receiver. The mobility of the device had the added benefit of allowing the researchers an easy way to vary the distance from the target to the receiver.

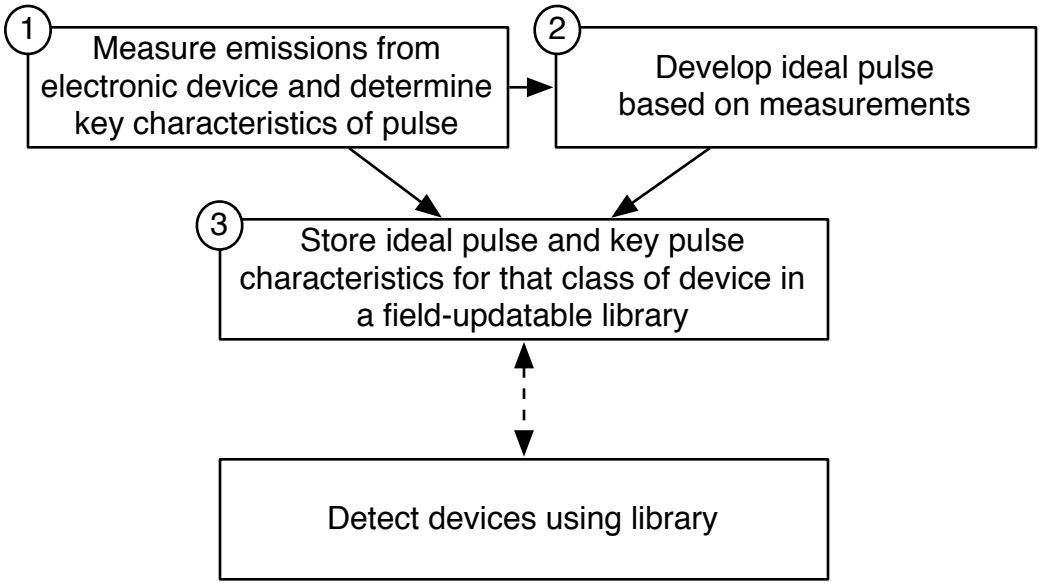


Figure 1.1 Procedure used to classify an electronic device.

Each device must be characterized before a detection algorithm can be developed. Devices are characterized by measuring their electromagnetic emissions and then determining key device radiation characteristics in the time domain. Figures 1.2 and 1.3 show typical emissions from a regenerative receiver for the frequency and time domains, respectively. While the characteristics of a pulse are generally well bounded, they may vary between measurements or within a single measurement. The pulse envelope and the pulse repetition rates both vary about some nominal value. The pulse repetition rate, though not consistently at 200 kHz, remains within reasonable boundaries. As will be discussed later in greater detail, the repetition rate and its boundaries are used to create a square wave template that will serve as one piece of the total detection algorithm. Individual pulses also change over time. To illustrate, Fig. 1.4 shows how an individual pulse is being frequency modulated to a lower frequency and then back to its original level. The duration and the individual

time-frequency characteristics taken from these first two steps is used to create a single ideal pulse for each device using a cascading correlation method.

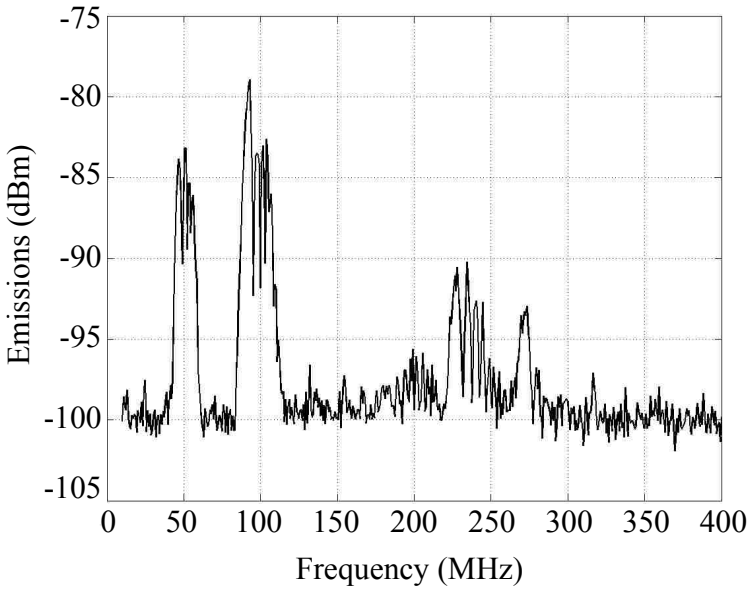


Figure 1.2 Unintended electromagnetic emissions from a super-regenerative receiver in the frequency domain.

Once characterized, the ideal pulse, pulse repetition rate, and repetition boundaries are then stored in a library and used as input parameters to the detection algorithm. Each step of this process is explained in detail in the following sections.

1.3.1. Electromagnetic Emission Measurements and Device Characterization. Several characteristics are determined from the radiation signature: the shape of the emissions pulse, the rate of the emissions pulse, the frequency content of the emissions pulses, the change in frequency content over time, and the change in emissions characteristics when subject to different noise conditions and environments. To characterize the emissions from a device, emissions were measured in a semi-anechoic chamber to minimize ambient noise. In our measurements we used a Sunol Sciences JB5 biconnilog antenna connected to an Agilent Infinium 54855A oscilloscope and a Rohde and Schwarz FSEB spectrum analyzer to measure the time domain and frequency domain radiation characteristics, respectively. Several measurements were obtained with resolution and video bandwidths of 10 kHz and a

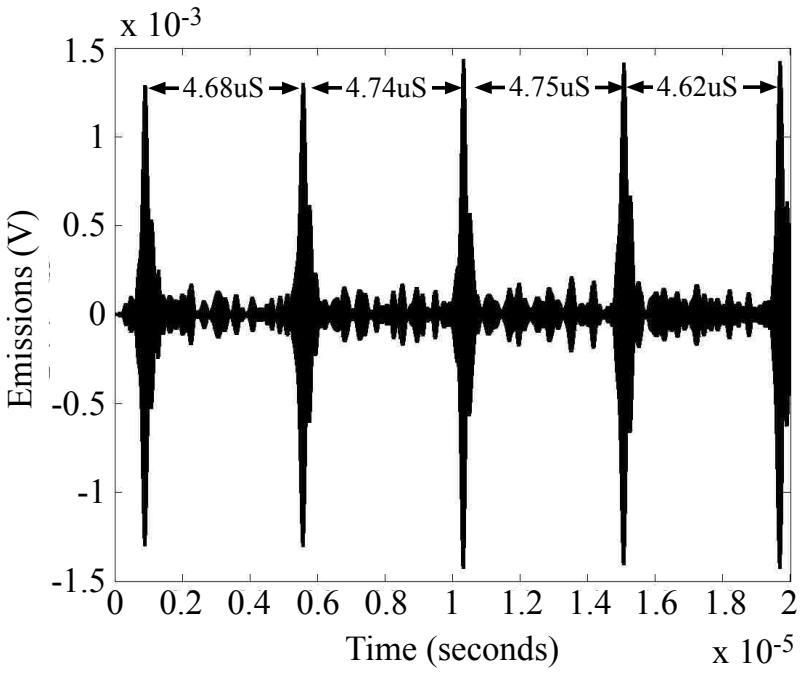


Figure 1.3 Unintended electromagnetic emissions from a super-regenerative receiver in the time domain.

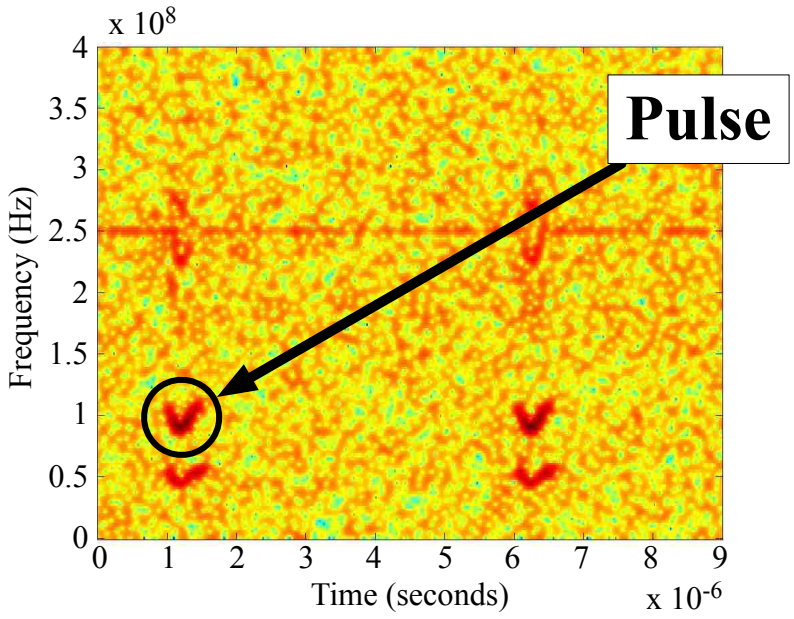


Figure 1.4 The time and frequency characteristics of a super-regenerative receiver.

sweep time of 9800 milliseconds. Example emissions measured using this setup from the regenerative receiver inside a toy truck were shown in Figs. 1.2 and 1.3. The unintended radiated emissions were sampled in the time domain at 2×10^9 samples per second. This long time period relative to the device's repetition rate was used to better understand the device's radiation characteristics. In this way, several radiated pulses were captured for analysis.

For the toy truck, 100 microseconds of data containing approximately 20 pulses was initially acquired during the characterization procedure. After extensive examination of the data it was determined for efficiency and speed that only 20 microseconds (approximately 4 pulses) of data was needed for accurate detection. The optimal digital or analog filter to be utilized was also determined from this data. For example, the toy truck had a pulse with a rate of emissions of 200 kHz; the primary frequency content of a single toy truck pulse was around 50 MHz and varied consistently by 10%. This results in a relatively broad band radiation at 50 MHz, as seen in Fig. 1.2. It was concluded that a digital filter centered at 50 MHz with a bandwidth of 20 MHz could be used to capture most of the radiation signature in the time domain. Fig. 1.3 shows the time domain emissions measured from the toy truck after being filtered digitally.

1.3.2. Development of an Ideal Pulse. For the device detection procedure, a template for a single time-domain pulse was created for the electronic device using a cascading correlation procedure. The definition of cross-correlation for two signals in the discrete-time domain is [11]

$$(f \star g)_i = \sum_j f_j^* g_{i+j}. \tag{1.1}$$

where f and g are two discrete-time signals to be cross-correlated, $\star$ indicates the cross-correlation process, and * represents the complex conjugate of f. An "ideal" pulse template is formed using successive cross-correlations. First, a statistically significant number of single pulses are randomly chosen from all the sets of measurement data. These pulses are then combined through correlation:

$$T(t) = [p_1(t) \star p_2(t) \star ... \star p_n(t)] / \max[p_1(t) \star p_2(t) \star ... \star p_n(t)]. \tag{1.2}$$

where $T(t)$ is the resulting pulse template, and $p_1(t)$ through $p_n(t)$ represent the n randomly chosen single pulses from the emissions measurements. Practically, these pulses are correlated iteratively until all pulses are combined by first correlating the

first two pulses, correlating the result with the next single pulse, and so on until all n pulses are combined. When all n pulses have been combined, the final result is normalized by the maximum value and stored as an "ideal" pulse as illustrated in Fig. 1.5.

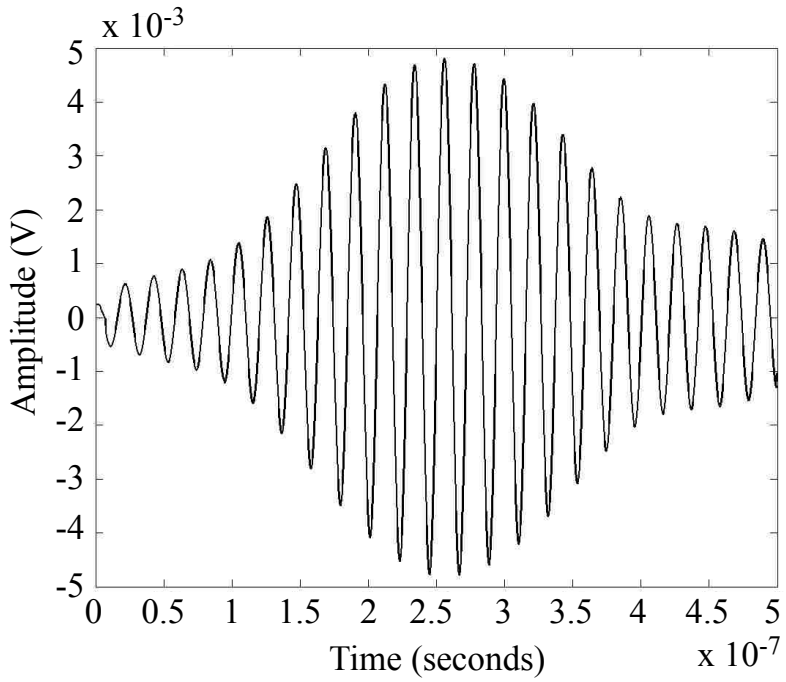


Figure 1.5 An ideal pulse developed for the toy truck using the cascading correlation procedure.

There is a smoothing effect on the pulse envelope since the envelope changes from pulse to pulse for most regenerative receivers. Comparing a single pulse chosen from the toy truck's emissions in Fig. 1.6 to the toy truck's "ideal" pulse in Fig. 1.5, one can see how the ideal pulse envelope has changed. The frequency modulation is preserved in the ideal pulse, however, since it is present in every single pulse of the emissions.

1.3.3. Detection. Detecting unintended emissions from many devices poses a significant problem due to the erratic nature of any unintended emissions. Unlike intended radiated emissions from intentional transmitters like a cell phone that are deliberately designed to radiate in a certain manner, unintended emissions have no such restrictions other than meeting regulatory requirements. As discussed earlier, for

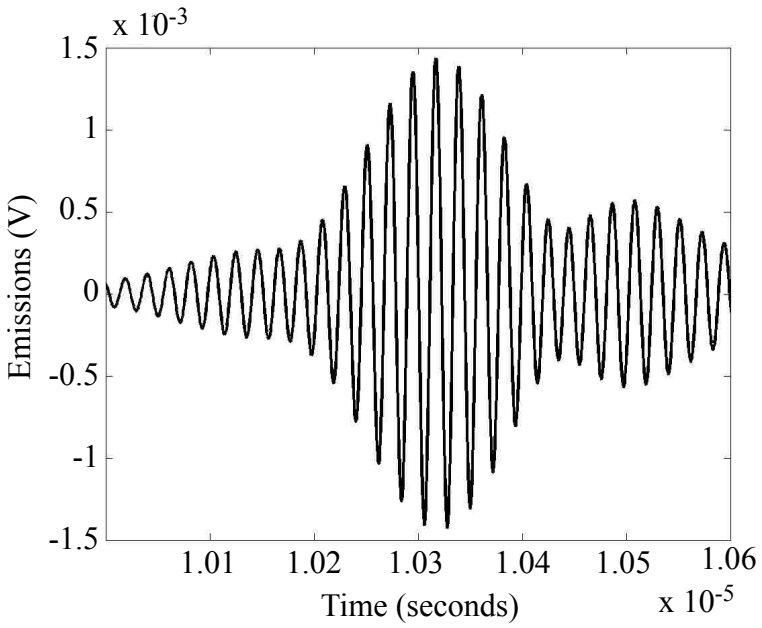


Figure 1.6 A single pulse from a toy truck in the time domain.

the super-regenerative receivers examined in this paper, the unintended emissions are measurable and, though erratic, can be placed within certain bounds. The detection procedure shown in Fig. 1.7 addresses the erratic nature of the unintended emissions of the regenerative receiver.

The detection process begins by measuring the ambient electromagnetic environment using a receiver attached to an antenna. The data is digitized and sent to a computer for digital signal processing. Once digitized, the signal is digitally band-pass filtered to analyze only the frequency band of interest. For example, the toy truck's emissions are filtered using a band-pass filter centered at 50 MHz with a 20 MHz bandwidth. The resulting signal is then examined for similarity to a template signal as discussed below.

Because of the erratic nature of unintended emissions, a two pronged approach was developed to bring specific unintended emissions from a device, if present, out of the ambient noise. For any characterized device two important pieces of information are stored in a library of devices: the ideal pulse and the pulse repetition rate. These two pieces of information are first retrieved from the library for a single device before beginning any signal processing.

After retrieving the ideal pulse from the library, the time-domain pulse is correlated with the ambient noise. This first correlation will bring out similar pulses from

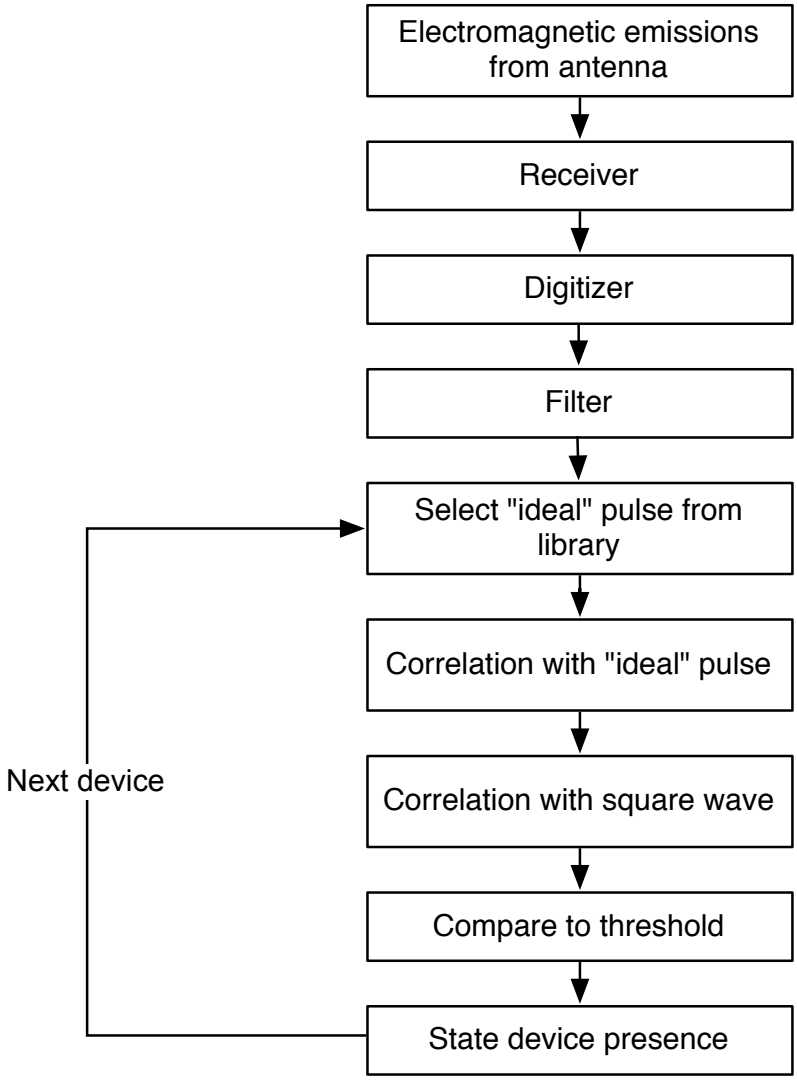


Figure 1.7 Procedure used to detect an electronic device.

the noise. However, this correlation is not enough to identify the device since there could be many devices, such as other regenerative receivers, that exhibit a similar pulse. Further signal processing must be completed using the pulse repetition rate information.

The pulse repetition rate depends on many factors, including not only device characteristics but electromagnetic energy within the receive band of the receiver. Since the repetition rate is nominally at one frequency, but can vary by as much as 20%, it is not possible to simply correlate with a pulse train using a basic matched

filter or perform the correlation in the frequency domain. It is still possible, however, to use this information for detection by correlating the measured signal with a square wave with the device's expected pulse repetition frequency. Variations in repetition rate are taken into account by changing the duty cycle of the square wave and by chaining several square waves together to correspond with different repetition rates. Each chained square wave has a slightly different frequency, varied from the nominal frequency. The number of square waves is determined by the expected variation in the pulse repetition rate. The duty cycle of the square wave is similarly determined from the pulse width and expected variation in repetition rate, as well as the total sample length.

Figure 1.8 shows an example square wave used to detect repetitive pulses with a repetition rate around 200 kHz. This square wave is zero mean, has a duty cycle of 10% and is chained with several square waves (not shown) that vary in repetition rate by plus or minus 10% from 200 kHz. A zero mean square wave was used so as not to add any additional energy to the correlation that was not associated with the periodicity. The duty cycle was set to 10% to correspond with the pulse duration time. The square wave correlation thus brings out periodicity of the signal while the ideal pulse correlation brings out each individual pulse from the background noise.

The result of these cascaded correlations is finally normalized and compared to an expected threshold value from the library to determine the presence of a device. A successful threshold match is determined by calculating the power in the signal after both correlations and comparing it to an expected threshold. The correlation output is normalized as:

$$Normalized\ Output = \frac{\sum_{n=N}^{n=0}(y_{out}[n])^2}{\sqrt{\sum_{n=N}^{n=0}(x_{in}[n])^2}} \tag{1.3}$$

where y_{out} is the output of the cascaded matched filters, x_{in} is the measured signal that is the input to the cascaded matched filters and N is the number of samples. An output of '1' indicates a perfect match between the input signal and the ideal signal. The threshold was determined statistically by examining results generated over many acquired measurements. Several measurements of the device were taken under numerous ambient conditions outside of the semi-anechoic chamber to develop the threshold. This threshold is based on the power in the signal and is stored in the library for reference during detection.

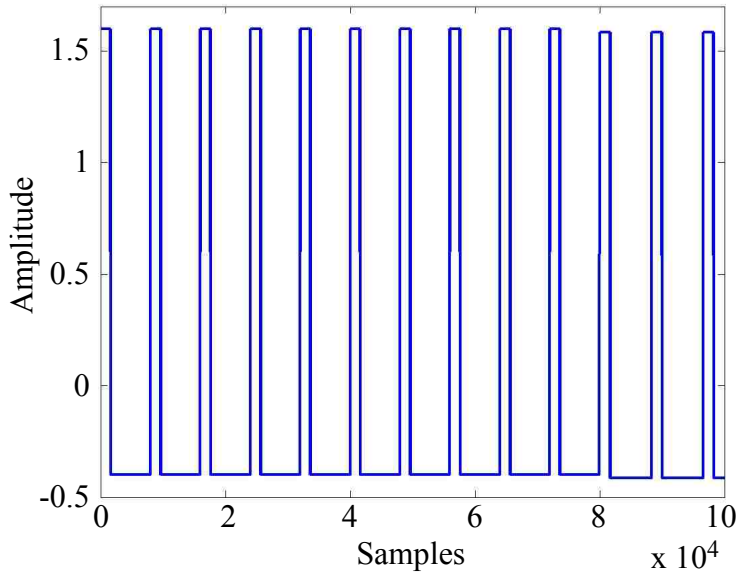


Figure 1.8 Example square wave used to bring out the periodicity of the signal in the second correlation.

1.4. RESULTS

The method discussed in this paper was tested in both a low ambient noise level environment– a semi-anechoic chamber– and a very noisy urban environment– the hallway outside our lab. Detection in a semi-anechoic chamber when the device was at a distance of 3 meters (the size of our chamber) was found to have an area under the receiver operator characteristic (ROC) curve of 99 %. However, since a semi-anechoic chamber is not a typical environment, we tested our detection algorithm in a noisy environment where it was consistently able to detect a device at a distance of 40 meters. Under these conditions, the algorithm proved especially robust as the signal to noise level at this distance was nearly equal to one and it is not possible to determine if the device was present through simple human observation.

Several ambient electromagnetic emissions measurements were acquired in the hallway without a target electronic device as well as measurements containing a target device for detection. Factors such as the battery charge, climate and ambient noise levels would cause the device's unintended emissions to alter. The data represented in the following plots represent average operating conditions for the toy truck. The measurements for these plots were taken over a period of days with varying battery charges. All of the data was then processed by our detection algorithm. At a close range of 3 meters, the device can be identified by simple observation. Increasing the

device's distance by only a few meters made it difficult to identify through observation alone. Correspondingly, the algorithm detection rate worsened. The two plots shown in Fig. 1.9 and Fig. 1.10 depict the unintended emissions of a toy truck at 5 meters and at 40 meters, respectively. These figures show that as the distance is increased from the antenna, the unintended emissions from the device are increasingly lost in the noise and the signal-to-noise ratio (SNR) decreases. The toy truck can be detected in both measurements, however, using the techniques previously discussed.

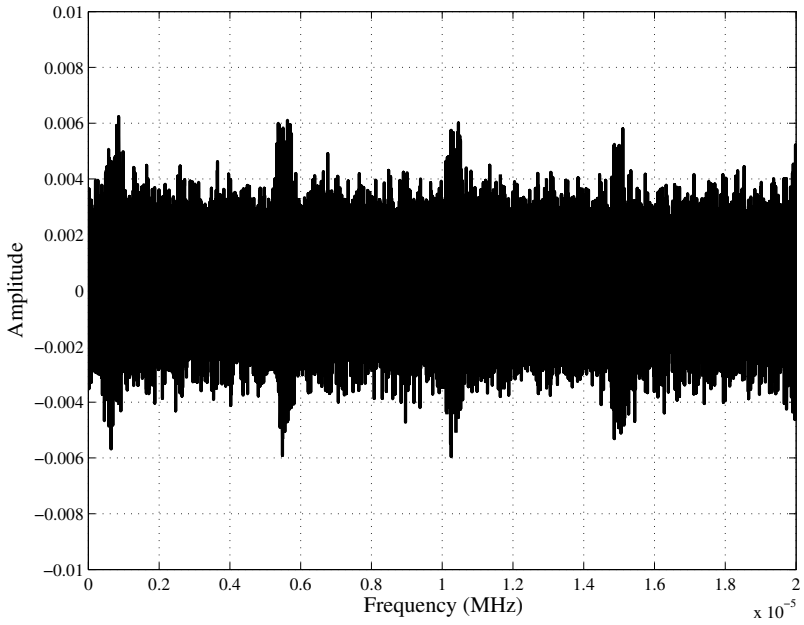


Figure 1.9 Unintended electromagnetic emissions of a toy truck in ambient noise, 5 meters from the antenna.

The outputs of the detection algorithm for a noisy urban environment are shown in Fig. 1.11. The three subplots in this picture represent the outputs at designated points of the algorithm. The top subplot shows the signal that has been captured and band-pass filtered. The middle subplot represents the output of the first correlation with the ideal pulse. The bottom subplot represents the final output of the correlation with the square waves. The dotted red line in the bottom subplot represents the detection threshold for the chosen device. The detection threshold was chosen so that the false alarm rate was reasonably low. Since the output of the algorithm,

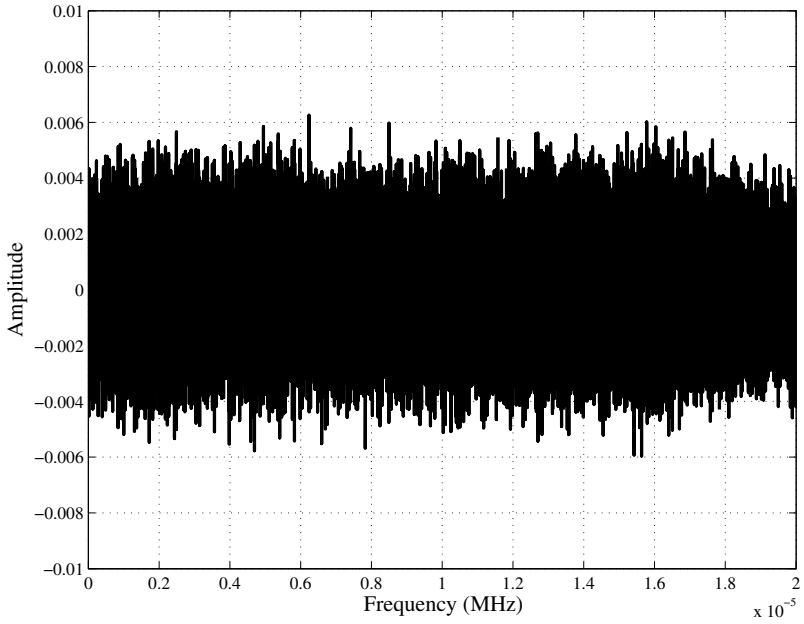


Figure 1.10 Unintended electromagnetic emissions of a toy truck in ambient noise, 40 meters from the antenna.

shown in the bottom subplot, is below the threshold, the device is clearly not present in the sample.

Plots of the algorithm output for a toy truck in a noisy urban environment at 3 and 25 meters are shown in Fig. 1.12 and Fig. 1.13. It is clearly shown in these figures that the energy is above the detection threshold and that the toy truck will be detected in both these cases. At 3 meters the truck's emissions are very strong and can easily be seen by visual inspection. When the truck is at a distance of 25 meters, it's emissions are not discernible above the noise, though it can still be detected after processing. At 40 meters the truck's emissions are completely lost in the noise though it can still be detected. The overall performance of the cascading correlation detection method in the ambient environment compared with a basic matched filter as described in [10] may be found in Fig. 1.14. 664 total measurements were included in this ROC curve that were taken at all times of the day. Of these measurements 334 sets contained the receiver, while 330 contained only noise. The cascading correlations yielded an area under the ROC curve of 98% compared with the matched filter performance of 74%.

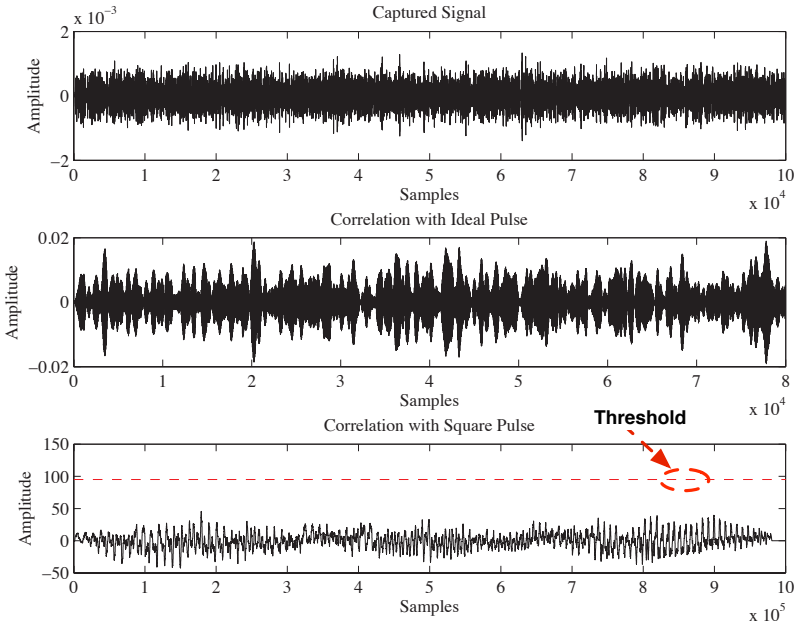


Figure 1.11 Example of the detection algorithm's output for a noisy urban environment measurement without a device for detection.

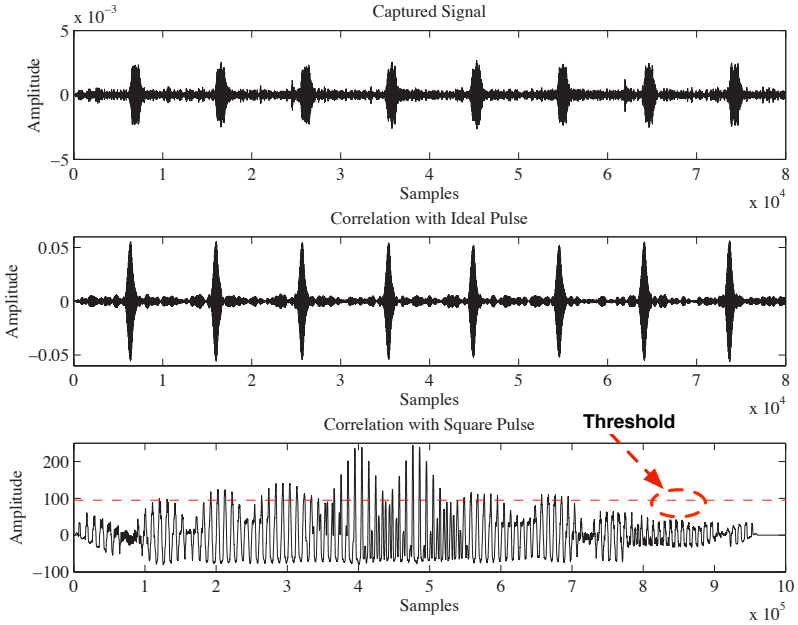


Figure 1.12 Example of the detection algorithm's output for a super-regenerative receiver at 3 meters.

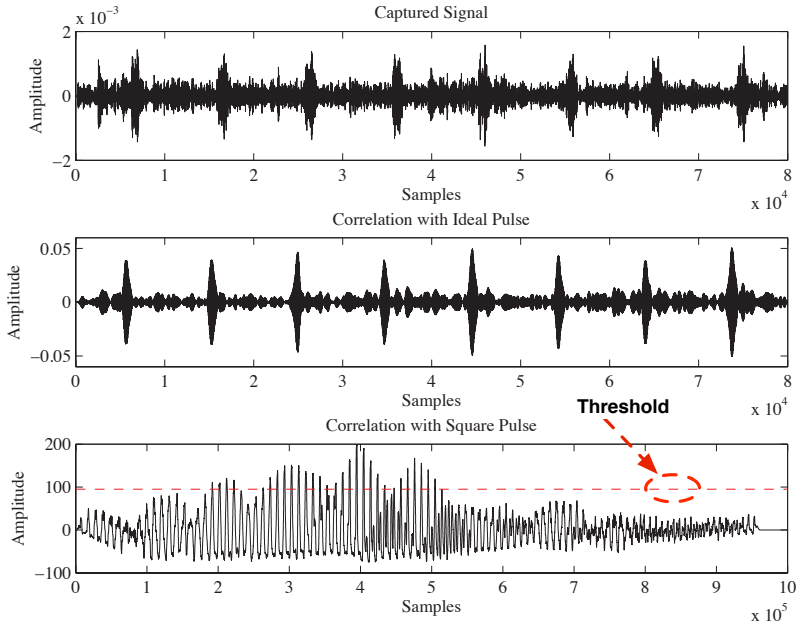


Figure 1.13 Example of the detection algorithm's output for a super-regenerative receiver at 25 meters.

1.5. DISCUSSION

The method of detection presented in this paper has the ability to detect low-cost RF receivers using their unintended electromagnetic emissions. Preliminary results show that this class of receivers exhibits many common characteristics suggesting it is possible to generically detect devices from this class, yet the emissions also differ from one device to another, allowing discernment even among different regenerative receivers. Specific results were included for a toy truck containing a low-cost super-regenerative receiver. To improve the detection at greater distances, either or both the prototype hardware and the processing algorithm need to be changed. If the SNR were improved by simply changing the hardware, the same algorithm would yield better results, detecting the receiver at a greater distance. Improved SNRs can be obtained by using pre-amplifiers and analog filters in the frequency band of interest. The analog filters improve SNR by allowing the oscilloscope to set its dynamic range according to the frequency band of interest rather than over the entire frequency band. The oscilloscope that was used in our study only has 8 bits of vertical resolution. Systems with resolutions as high as 12 or 16 bits can be purchased that would also improve the SNR. Receiver and digitizer combinations also exist that have band-selectable analog filters and high-resolution high-speed sampling that can greatly improve the SNR.

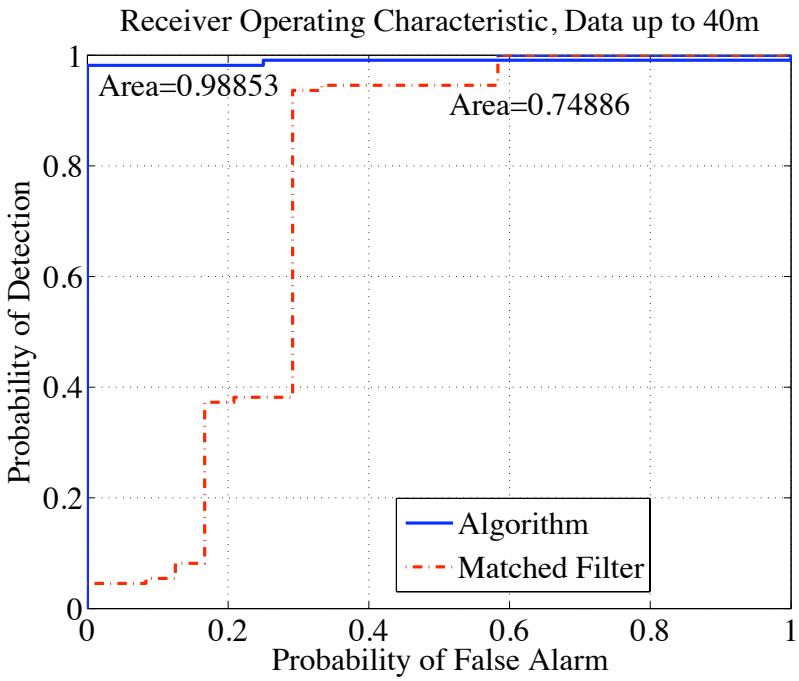


Figure 1.14 Receiver operator characteristic (ROC) of the detection algorithm compared with a basic matched filter.

Similar improvements in the SNR might be obtained by using long sample times. Long sample times allow averaging effects to be exploited, but requires a consistent signal over time.

Since several factors, such as battery charge, climate, and ambient noise level affect a low-cost receiver's unintended emissions, the detection algorithm should account for these changes. Modifying the hardware addresses problems with the ambient noise level, but factors such as signal fluctuations among devices or with battery wear and climate conditions cannot be addressed with simple hardware changes. Incorporating these changes in the detection algorithm is under investigation.

This paper discusses the results for a single super-regenerative receiver, however, this algorithm has been tested with several different super-regenerative receivers and yielded similar results. All of the characteristics discussed above, such as the pulse repetition rate, etc., must be determined for each individual device for the algorithm to work correctly, as these characteristics may vary significantly. For example, one receiver may have a pulse repetition rate of 200 kHz compared with another receiver that has a slower pulse repetition rate of 150 kHz. These differences could be used to distinguish between the two receivers.

1.6. CONCLUSION

Unintended emissions from electronic devices are measurable and detectable in an ambient noise environment using a targeted detection algorithm. Though detecting unintended emissions of electronic devices can be a challenge due to their erratic nature, it is possible to do so by characterizing these emissions first in a low noise environment and then using a detection algorithm that accounts for typical variation in the emissions.

Here, a method to detect and identify super-regenerative receivers based on their unintended electromagnetic emissions was presented. Emissions were characterized by their emissions bands, pulse shape and pulse repetition rate. An ideal pulse based on the time domain signal was created using several cascaded correlations of pulses measured in the semi-anechoic chamber. This ideal pulse was then correlated with measured emissions data to find similar "pulses" in the measured data. This result was followed by another correlation with one or more square waves. A threshold based on the energy of the output from the signal-processing algorithm was calculated and used to determine if a device was present. Using this algorithm, a toy truck containing a super-regenerative receiver was detected to 40 meters with an area under the ROC curve of 98%.

1.7. REFERENCES

[1] P. Dourbal, "Method and apparatus for detecting and locating a concealed listening device," U.S. Patent 5,717,656, Feb. 10, 1998.

[2] M. Kroll, "Aircraft internal EMI detection and location," U.S. Patent 6,580,915, Sept. 24, 1999.

[3] D. Beetner, S. Seguin, T. Hubing, "Electromagnetic emissions stimulation and detection system," U.S. Patent 7,464,005, Dec. 9, 2008.

[4] T. Hubing, D. Beetner, X. Dong, H. Weng, M. Noll, H. Göksu, B. Moss, and D. Wunsch, "Electromagnetic detection and identification of automobiles," presented at *EuroEM*, Magdeburg, Germany, Jul. 2004

[5] A. Shaik, H. Weng, X. Dong, T. H. Hubing, and D. G. Beetner, "Matched filter detection and identification of electronic circuits based on their unintentional radiated emissions," in *Proc. IEEE Int. Symmp. Electromagn. Compat.*, Aug. 14-18, 2006, vol. 3, pp. 853–856

[6] T. Hubing, D. Beetner, S. Seguin, B. Moss, M. Schmidt, "Improvised explosive device detection based on unintentional electromagnetic emissions," presented at *IEEE Ant. and Prop. Soc. Int. Symp.* Piscataway, NJ, 2006, pp. 202

[7] H. Weng, X. Dong, X. Hu, D. G. Beetner, T. Hubing, and D. Wunsch, "Neural network detection and identification of electronic devices based on their unintended emissions," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 8-12, 2005, vol. 1, pp. 245-249.

[8] X. Dong, H. Weng, D. Beetner, T. Hubing, D. Wunsch, M. Noll, and H. Göksu, "Detection and Identification of Vehicles Based on Their Unintended Electromagnetic Emissions," IEEE Trans. Electromagn. Compat., vol. 48, no. 4, pp. 752–759

[9] A. Oppenheim and R. Schafer, *Discrete-Time Signal Processing*. New Jersey: Prentice-Hall, 1999.

[10] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*. New York: McGraw-Hill, 2002.

2. CONTROLLING UNINTENDED EMISSIONS FROM REGENERATIVE RECEIVERS TO IMPROVE DETECTION AND IDENTIFICATION

2.1. ABSTRACT

Detection of low-cost regenerative receivers using their unintended radio-frequency emissions can be difficult because of the erratic nature of these emissions and their tendency to drift in frequency. The biggest problem comes when trying to detect these devices in a noisy environment when the signal level of these unintended emissions is well below the ambient noise. These receivers respond consistently, however, to a radio frequency stimulation and their emissions can even be frequency and amplitude modulated to a certain extent. Using a stimulation improves the signal quality and consistency from these receivers, but the most important effect is the ability to modulate their emissions in a known manner. This modulation allows for the creation of a detection algorithm that looks for very specific characteristics in the emissions, potentially allowing detection of the emissions when they are below the noise floor and allowing detection of super-regenerative receivers as a class of devices. Early results show significant improvements in detection over a traditional passive approach.

2.2. INTRODUCTION

Electronic devices give off unique electromagnetic signals as a result of their printed circuit board layout, circuit design, packaging and other variables. These electromagnetic emissions have been used to passively detect and identify these devices [1] [2]. The challenge is detecting the weak and inconsistent electromagnetic emissions from one device in the presence of other, sometimes very strong, intentional and unintentional emissions sources, or detecting new devices whose emissions have not previously been observed.

Prior work has explored how to passively identify wireless receivers based on their unintended electromagnetic emissions using simple matched filters [3]- [5], using neural networks [6]- [7] and using algorithms that exploit both time and frequency domain characteristics of the signals to detect specific devices [1] [2]. Each of these methods only passively listens to the unintended emissions from a device. Without

a stimulation, the emissions can be erratic and inconsistent. Using an active method for detection often leads to better results because it makes the unintended emissions more consistent and because the unintended emissions respond in a predicable way to the stimulation such that they can be deliberately manipulated for easier detection.

A common active method of detecting the presence of an electronic device is to use a "bug scanner". These bug scanners work by illuminating a target with a strong electromagnetic stimulation that is rectified by non-linear PN junctions in the device, causing the device to re-radiate harmonics of the original stimulation signal [9]. The observation of harmonics indicates the presence of an electronic device. This technology is not ideal in many environments, however, due to the large number of non-linear junctions that respond to this type of stimulation, the relatively weak response from the device, and the high power levels required to trigger a measurable response. Many metal-to-metal junctions will rectify the stimulation much like a PN junction. For example, the non-linear response from a rusty nail can be confused with the response from an electronic listening device. Re-radiated emissions are typically 60-90 dB or more below the stimulation, so even with a strong stimulation typical bug scanners only work to a distance of several meters or less.

Another active detection and location technique includes radio-frequency identification (RFID). RFID is an automatic identification method that uses two elements, a transponder and a tag. Relevant information is stored in the tag that is read by the transponder. Tags can be either passive devices that re-radiate energy from a stimulation or active devices that radiate their own energy [9]. The simplest of RFID systems consists of a passive tag that works similarly to the bug scanner where the passive tag is designed to re-radiate energy from the transponder [9] and the transponder listens for an expected response.

Here we present a technique that uses a weak stimulation for detecting and identifying regenerative receivers based on their unintended emissions. This technique can generate a much stronger response with lower stimulation power than traditional bug scanning methods. The response of regenerative receivers to a stimulation will be shown experimentally and two detection algorithms will be proposed. One of the detection algorithms simply uses the stimulation to make the signal more consistent and employs a cascading correlation technique to detect the device [2]. This technique requires prior knowledge of the unintended emissions in the time and frequency domains to determine if the device is present. The second technique uses the stimulation signal to deliberately change a regenerative receiver's unintended emissions over time. Since all regenerative receivers are expected to show a similar change in

emissions with stimulation, these manipulated emissions can then be used detect any member of the class of regenerative receivers and only requires the knowledge of the response frequency.

2.3. METHODS

An algorithm to passively detect and identify regenerative receivers was developed in [1] – [2]. In [1] and [2], a three step detection algorithm was introduced. In this algorithm, the emissions from a device are first characterized by acquiring a series of measurements of the emissions in the time and frequency domain. These measurements are used to develop an "ideal" emissions signal in the time domain. The data acquired during the device characterization phase is then utilized to determine the presence of the device in an unknown environment. Detection is accomplished by using the shape of the emissions pulse from the receiver, the repetition rate of emissions pulses, and the expected bandwidth of emissions, as well as other information.

The detection methodology presented here uses a weak electromagnetic stimulation to modify the unintended emissions from an electronic device. Each device must first be characterized in a semi-anechoic chamber to determine its response to an electromagnetic stimulation. Devices are characterized by measuring their electromagnetic emissions, by determining key device radiation characteristics in the time and frequency domains, and by determining their response to different types of electromagnetic stimulation. A low-cost RF toy containing a 50 MHz receiver was utilized here to represent super-regenerative receivers. It was found experimentally that this regenerative receiver responded to a stimulation in a predictable manner, causing the signal to be more consistent and easier to detect. Once the device has been characterized, the key features of their unintended emissions, the response of their emissions to stimulation, and the preferred stimulation signal are stored in a database for later reference during detection of the device.

2.4. ELECTROMAGNETIC EMISSIONS

Figs. 2.1 and 2.2 show typical emissions from a regenerative receiver in the frequency and time domains. The characteristics of the pulse tend to be well bounded, but may vary between measurements or within a single measurement. The pulse envelope, pulse repetition rate and the pulse magnitude all vary about some nominal

value and can change drastically depending on the ambient electromagnetic environment or, in the absence of a stimulation, may vary depending on random processes within the receiver. These parameters become more consistent when subjected to an appropriate RF stimulation.

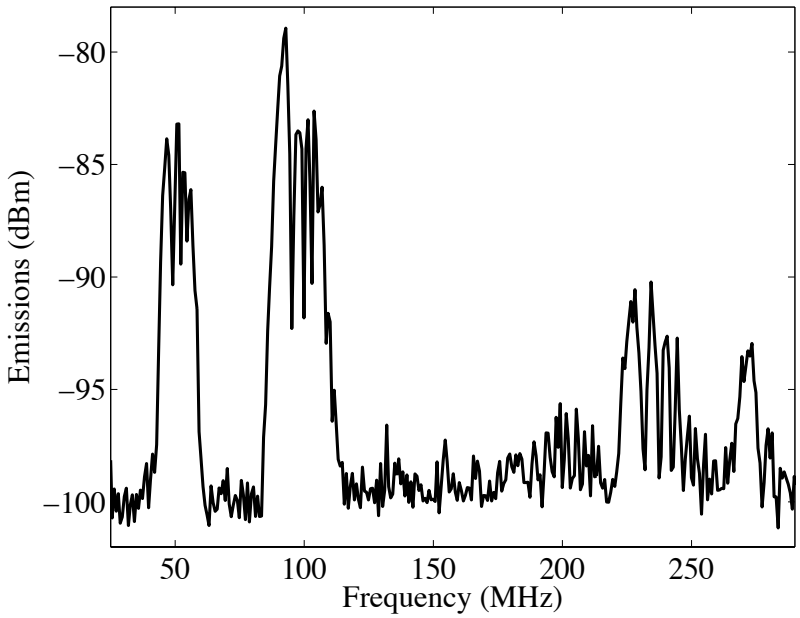


Figure 2.1 Unintended electromagnetic emissions from a super-regenerative receiver in the frequency domain.

To understand how a super-regenerative receiver reacts to a stimulation, it is useful to examine the circuit diagram, shown in Fig. 2.3 [10]. A super-regenerative receiver is an RF amplifier with enough positive feedback to cause oscillations that can be damped by a quench signal. In this simplified schematic, the field-effect transistor (FET) is the main amplifier in the regenerative receiver. The gate circuit is designed to be resonant at the receiver's operating frequency. The devices we used in this study are resonant at 50 MHz. The gate circuit is coupled into the antenna or source, V_i, as shown. Mutual coupling, M, between the drain coil and gate circuit allows oscillations to build up when the gate bias is raised above a cutoff value. The circuit is designed to oscillate in two ways. First, ignoring the self-quench part of the circuit (R_1 and C_1), the other resistors, capacitors and inductors are chosen in the circuit to specify the amplification such that there is large positive feedback in the

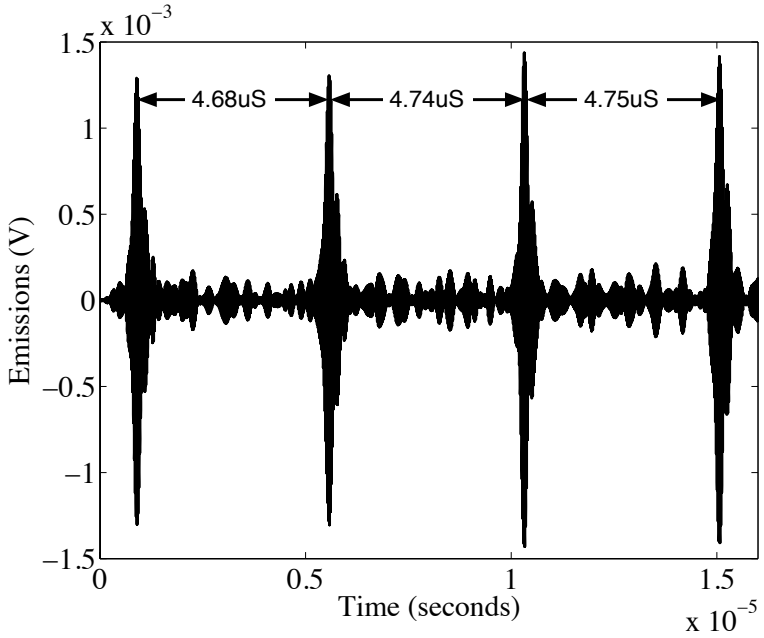


Figure 2.2 Unintended electromagnetic emissions from a super-regenerative receiver in the time domain.

circuit and to create the 50 MHz resonant frequency. The positive feedback allows the 50 MHz oscillation to build up over time. The amplification is controlled by the FET gate bias. When it builds above a threshold, a quench signal is imposed and the amplification (and the size of the 50 MHz oscillation) decreases. As the output decreases, the quench signal is removed and the process repeats. The device used in this study has a pulse repetition frequency of 200 kHz. When turned on and listening for a transmitted signal, these regenerative receivers will thus contain two oscillations, in this case 50 MHz "pulses" occurring at a 200 kHz rate, as shown in Figs. 2.1 and 2.2.

Super-regenerative receivers will respond to RF energy at their resonant frequency from the antenna input (V_i in the circuit diagram) even if the energy is not in the form intended to activate the device. Applying RF energy at the resonant frequency of the super-regenerative receiver increases the repetition rate and the amplitude of the pulse.

The process used to characterize the emissions of regenerative receivers is outlined in Fig. 2.4. A general characterization was completed first that determines the unintended emissions when the device is not subjected to a stimulation. Emissions

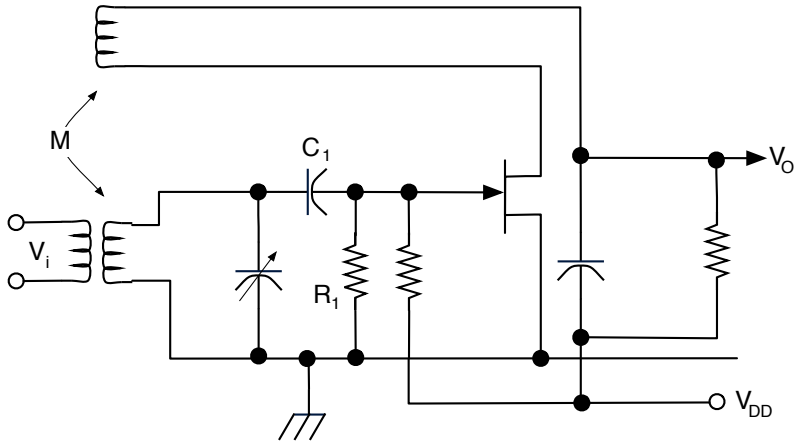
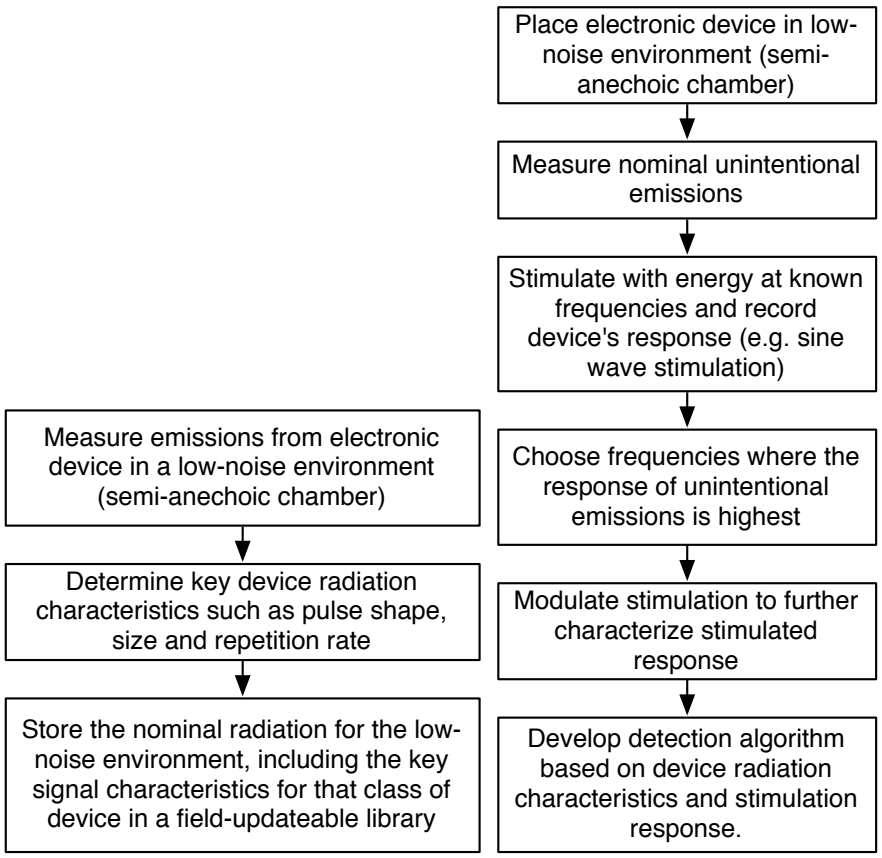


Figure 2.3 Schematic of a self-quenched super-regenerative receiver.

were measured in a semi-anechoic chamber to minimize ambient noise. In our measurements we used a Sunol Sciences JB5 biconilog antenna connected to an Agilent Infinium 54855A oscilloscope and a Rohde and Schwarz FSEB spectrum analyzer to measure the time and frequency domain characteristics, respectively. Several measurements were obtained with resolution and video bandwidths of 10 kHz and a sweep time of 9800 ms. The unintended emissions were sampled in the time domain at 2×10^9 samples per second. 100 microseconds of data containing approximately 20 pulses were initially acquired during the characterization phase. Nominal attributes of the emissions were determined from the measurements, including the shape of the pulse, the rate of the pulses, the frequency content of the pulses, and the change in frequency content over time. After determining the nominal radiation characteristics of the device, emissions were measured while applying an electromagnetic stimulation.

Various stimulation frequencies were tested and the frequency with the best response was recorded for later use. In many cases, the receivers will be susceptible to an RF signal in the same frequency range where the device has radiated emissions. For example, the device used in this study had emissions primarily around 50 MHz and a stimulation signal at 50 MHz will yield the best response. Fig. 2.5 shows the unintended emissions of a regenerative receiver in the frequency domain in response to a simple 50 MHz sine wave stimulation compared with the device's nominal emissions when it was not stimulated. The stimulation produced a noticeable change in the emissions, but was sufficiently different from the signal expected by the receiver that it did not activate the device (it only changed the unintended emissions). Note



(a) General characterization

(b) Stimulation response characterization

Figure 2.4 Procedure used to characterize an electronic device.

that the peak at 50 MHz is due to the actual stimulation and is not part of the device's response. The emissions with a stimulation show a series of peaks in the frequency domain separated by 280 kHz compared to emissions without a stimulation, because the rate of 50 MHz pulses is more consistent with a stimulation. Essentially, the frequency domain characteristics of the emissions results from a multiplication of the frequency domain characteristics of a impulse waveform representing the pulse repetition rate. When the repetition rate is constant, the frequency domain representation of the impulse waveform is a comb filter and one expects a series of peaks in the overall emissions. The stimulation needed to illicit this response is relatively weak, only about -30 dBm of output from the signal generator was required.

In addition to making the pulse rate more consistent, the device's pulse repetition rate may also be modulated by varying the stimulation power as shown in

Fig. 2.6. The pulses for the frequency modulated portion of this drawing are exaggerated for demonstration purposes. The pulse repetition rate increases with the amplitude of the stimulation. Since the size of individual pulses does not change but there are a different number of pulses over a given time segment, the total energy in the emissions is also modulated by the amplitude of the stimulation. The change in the repetion rate with stimulation power, as determined experimentally for one device, is show in Fig. 2.7.

2.5. DETECTION

Detecting unintended emissions from most regenerative receivers may be challenging due to the erratic nature of the unintended emissions as well as the low signal strength. Unlike intended radiated emissions from intentional transmitters like a cell phone that are designed to radiate in a certain manner, unintended emissions have no such restrictions, other than meeting regulatory requirements. As discussed earlier, for the super-regenerative receivers examined in this paper, the unintended emissions are erratic, but are measurable and their characteristics can be placed within certain bounds. The application of a stimulation signal has the benefit of forcing the unintended emissions into a more predictable pattern, increasing detectability.

In [2] a passive detection method that did not use any stimulation to find specific regenerative receivers was presented. Because of the erratic nature of unintended emissions, a two pronged approach was developed to bring specific unintended emissions, if present, out of the ambient noise. First, an ideal pulse was developed and correlated with the ambient noise to bring similar pulses out of the noise. Then, a series of square waves varying in frequency corresponding with the device pulse repetition rate were used in a second correlation with the ambient noise to take into account the frequency variation and the erratic nature of the unintended emissions. By simply using this algorithm in conjunction with a weak stimulation, the detection distance can be extended. The detection algorithm in [2] was found to be ineffective at a long distance in a particularly noisy environment. By applying a sine-wave stimulation with an output power of -28 dBm and using the same algorithm, detection at the maximum tested distance was vastly improved. Table 2.1 shows the results. The probability of detection was increased from 17% without a stimulation to 96% when using a stimulation. The false alarm rate was also improved. These results contain a larger set of data than was used in [2], including many outlying data sets, which

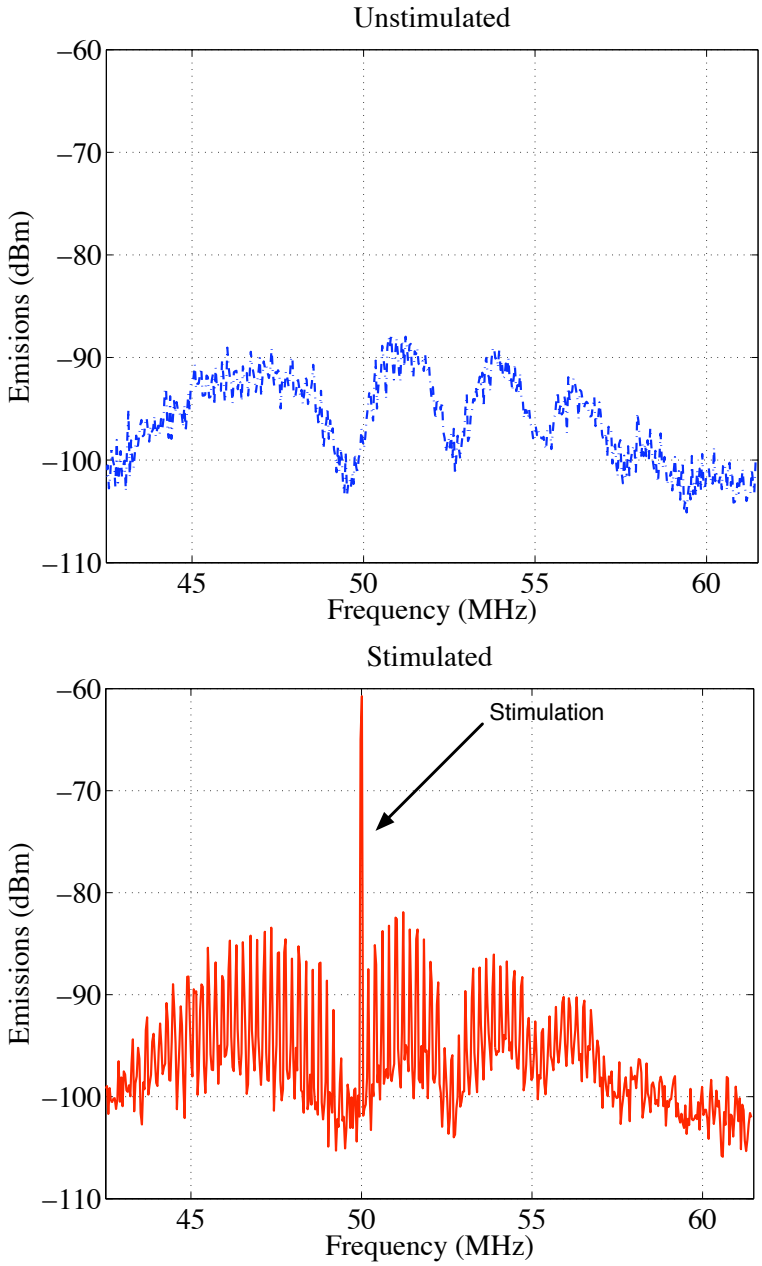


Figure 2.5 Emissions from a super-regenerative receiver without (top) and with (bottom) a stimulation

accounts for the difference in the performance between the present results and those in [2]. Outlying data sets were data with unusually poor signal-to-noise ratios that was a result of the receiver not being line of site to the antenna, such as behind a wall, etc.

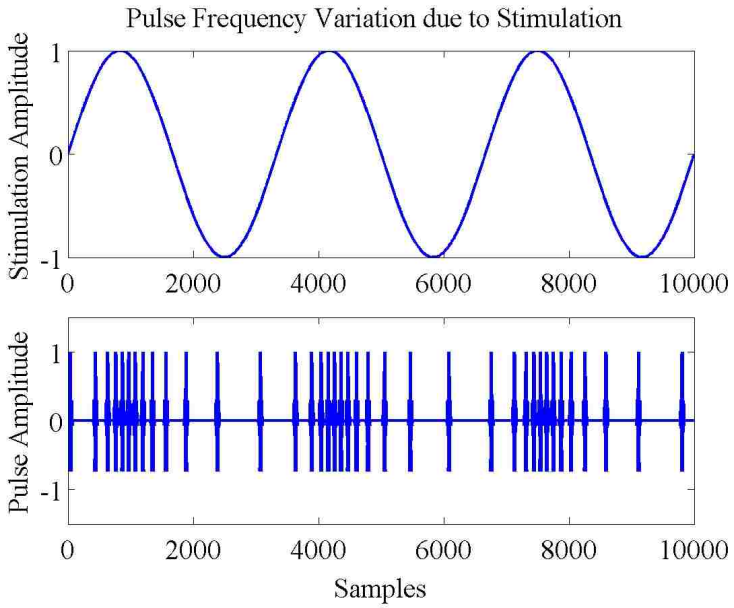


Figure 2.6 Exaggerated differences between the nominal and the stimulated response of the unintended electromagnetic emissions of a super-regenerative receiver.

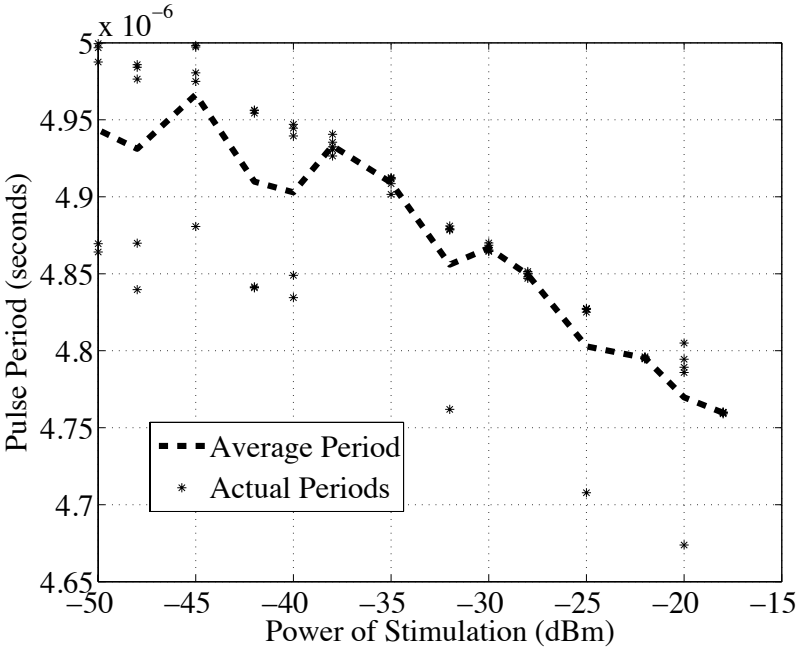


Figure 2.7 Pulse period variation with respect to stimulation power.

Table 2.1 Cascading correlation algorithm results with and without stimulation for 400 sets of data

	Average Normalized Energy	Probability of Detection	Probability of False Alarm
Stimulation:	151	96%	10%
No Stimulation:	34	17%	18%

Due to the erratic nature of the unintended emissions, the passive detection approach used in [2] could only perform the correlation with a small number of pulses. Also, since the pulse repetition rate could vary over time significantly the method presented in [2] required a correlation with many square waves of different frequencies to obtain good results. Using a weak stimulation can improve performance by making the signal more stable and thus allowing correlation with a longer pulse train. A stimulation can also reduce detection time by reducing the number of square waves that must be used. It was determined that only half of the original square waves were needed when a stimulation signal was present. This reduced the total algorithm execution time in MATLAB from an average of 1.8 seconds without stimulation to 0.9 seconds with stimulation. When a stronger stimulation signal was used, even less square waves were required during the square wave correlation step. Reducing the number of square waves required reduces the overall correlation time, and, thus, reduces the total algorithm execution time. These square waves were reduced without any change to the detection results.

Performance can potentially be further improved by modulating the amplitude of the stimulation. For example, comparing the radiated energy with the stimulation on to the radiated energy with the stimulation off allows a comparison of energy emitted in the two states. A change in energy in sync with the stimulation indicates the presence of a regenerative receiver. Since only regenerative receivers are expected to respond to the stimulation in this way, this scheme allows the detection of the receiver in the presence of interfering noise that does not respond to the stimulation and, in effect, paves the way for a generalized method for detecting these receivers, even when they have not previously been characterized. Both the cascading correlation algorithm used with and without stimulation are device specific. These algorithms require that each individual regenerative receiver be characterized in order to implement the algorithm correctly.

An algorithm that uses only how a regenerative receiver responds to a certain stimulation, but nothing that is device specific, was developed by pulsing a stimulation signal on and off continuously. Two signal generators were used in a chain to produce a 50 MHz sine wave mixed with a 1 kHz square wave, resulting in a 50 MHz sine wave stimulation for 0.5 milliseconds and no 50 MHz stimulation (stimulation was off) for another 0.5 milliseconds. Detection can be accomplished by comparing the energy of the emissions during stimulation to that without. The combined average normalized energy difference for five different devices for when the stimulation was "on" was 254 with a standard deviation of 104 and 15 when the stimulation was "off" with a standard deviation of 14. Results are given for a filtered signal containing a regenerative receiver and for a signal containing only the stimulation (no receiver present). Both signals were band-pass filtered from 40 to 60 MHz and then notch filtered to remove the stimulation signal at 50 MHz. After the filters, each signal was correlated with an expected pulse for a set of regenerative receivers, to further bring the signal out of the noise. There were 20 stimulation measurement sets taken consecutively for each of the five devices.

The consistent difference between the energy in the filtered signal when the device is present compared with the energy in the filtered signal when the device is not present shows that it is possible to use this algorithm to determine if a regenerative receiver that responds to a 50 MHz stimulation is present.

Based on these results, a detection algorithm was developed using the change in energy in emissions with stimulation. The algorithm first applies a notch filter at 50 MHz to the entire signal, whether the stimulation was on or off. To further bring the signal out of the noise the measured signal was correlated with an expected pulse for a range of regenerative receivers. The energy in the emissions was calculated as follows for both the stimulated signal and the signal without the stimulation present:

$$\text{NormEnergy} = \frac{\sum_{n=0}^{n=N} (y_{out}[n])^2}{\sqrt{\sum_{n=0}^{n=N} (x_{in}[n])^2}} \tag{2.1}$$

where y_{out} is the output of the correlation with an ideal pulse (after being notched filtered to remove the stimulation), x_{in} is the measured signal after being notch filtered that is the input to the matched filter, and N is the number of samples. An output of '1' indicates a perfect match between the input signal and the matched filter.

To find the energy difference with and without stimulation, the average normalized energy is calculated as:

$$Y_{\text{StimON}} = \frac{\sum_{i=0}^{i=I-1} (\text{NormEnergy}_{\text{StimON}_i})}{I} \tag{2.2}$$

$$Y_{\text{StimOFF}} = \frac{\sum_{j=0}^{j=J-1} (\text{NormEnergy}_{\text{StimOFF}_i})}{J} \tag{2.3}$$

where Y_{stimON} is the average normalized energy over an entire measurement set when the stimulation is on, $Y_{stimOFF}$ is the average normalized energy over an entire measurement set when the stimulation is off, I is the number of times the stimulation is on in a single measurement, J is the number of times the the stimulation is off in a single measurement and $\text{NormEnergy}_{\text{StimON}_i}$ and $\text{NormEnergy}_{\text{StimOFF}_i}$ are the normalized energy in the emissions as in (2.1), each time the stimulation was on or off. The detection algorithm simply used the average normalized energy difference:

$$\text{AvgEnergyDiff} = Y_{\text{StimON}} - Y_{\text{StimOFF}} \tag{2.4}$$

to determine if the device is present.

Table 2.2 shows the performance of this detection algorithm for five different receivers purchased from different manufacturers. Emissions were initially measured in a low-noise semi-anechoic chamber and then white noise was added as a percentage of emissions signal power to simulate ambient noise. The average normalized energy difference between the energy when the stimulation was on minus the energy when the stimulation was off, Avg Energy Diff, was averaged for 100 sets of data that contained 20 pulses for each set ($I = J = 20$. That is, the stimulation is turned on and off 20 times). A single receiver was present in each of the 100 sets of data. All five of the receivers tested were measured for 20 sets of data, for the total of 100 sets of data. For each of the 100 sets of data, the average normalized energy difference was consistently higher when the regenerative receiver was present than the average normalized energy difference when no receiver was present. In 96 out of 100 sets of data the regenerative receiver was detected using this method. When no receiver was present the algorithm did not produce any false alarms for the 100 sets of data. The addition of white noise did not affect the number of sets of data detected until 100% white noise was added.

Table 2.2 Results of the energy difference detection algorithm for five different receivers

	Average Normalized Energy Difference	Sets Detected
	No White Noise Added	
Regenerative Receiver Present:	254	96/100
No Receiver:	15	0/20
	50% White Noise Added	
Regenerative Receiver Present:	243	96/100
No Receiver:	16	0/20
	75% White Noise Added	
Regenerative Receiver Present:	241	96/100
No Receiver:	20	0/20
	100% White Noise Added	
Regenerative Receiver Present:	220	92/100
No Receiver:	19	0/20

2.6. CONCLUSION

Unintended electromagnetic emissions can be used to detect electronic devices. Even though detecting regenerative receivers can be a challenge due to the erratic and irregular nature of their emissions, it is possible to stabilize these emissions and predict them more consistently using a known, weak stimulation given some specific knowledge of receiver. These devices must first be characterized in a low noise environment to obtain their nominal unintended emissions and the response of these emissions to a known stimulation signal. A stimulation signal is chosen that causes a significant change in the device's unintended emissions. The stimulation can be relatively weak and still illicit a response from the device, even at long distances. One advantage of using a stimulation to change emissions is that it may be used to generally detect a regenerative receiver, because the response described in this paper is unique to regenerative receivers.

In this paper, two methods to detect and identify regenerative receivers using a stimulation to modify their unintended electromagnetic emissions were presented. The passive cascading correlation method that was presented in [2] was improved significantly by the introduction of stimulation when the receiver was far away in a noisy envrionment. In the tested scenario, the probability of detection was improved from 17% to 96% compared to the normal passive method. This improvement in detection

occurs because the stimulation makes the unintended emissions more consistent and predictable.

The second method presented might be used to detect a regenerative receiver even if that receiver had not previously been characterized. This method pulsed the stimulation signal on and then off. By comparing the difference in the energy in the unintended emissions with the stimulation on and with the stimulation off, it is possible to determine if a regenerative receiver that is resonant at that stimulation frequency is present without having to extensively characterize that receiver.

2.7. REFERENCES

[1] D. Beetner, S. Seguin, T. Hubing, "Electromagnetic emissions stimulation and detection system," U.S. Patent 7,464,005, Dec. 9, 2008.

[2] S. A. Seguin, D. Beetner, T. Hubing, "Detection and Identification of Low-Cost RF Receivers Based on their Unintended Electromagnetic Emissions," in IEEE Trans. Electromagn. Compat., under review

[3] T. Hubing, D. Beetner, X. Dong, H. Weng, M. Noll, H. Göksu, B. Moss, and D. Wunsch, "Electromagnetic detection and identification of automobiles," presented at *EuroEM*, Magdeburg, Germany, Jul. 2004

[4] A. Shaik, H. Weng, X. Dong, T. H. Hubing, and D. G. Beetner, "Matched filter detection and identification of electronic circuits based on their unintentional radiated emissions," in *Proc. IEEE Int. Symmp. Electromagn. Compat.*, Aug. 14-18, 2006, vol. 3, pp. 853–856

[5] T. Hubing, D. Beetner, S. Seguin, B. Moss, M. Schmidt, "Improvised explosive device detection based on unintentional electromagnetic emissions," presented at *IEEE Ant. and Prop. Soc. Int. Symp.* Piscataway, NJ, 2006, pp. 202

[6] X. Dong, H. Weng, D. Beetner, T. Hubing, D. Wunsch, M. Noll, and H. Göksu, "Detection and Identification of Vehicles Based on Their Unintended Electromagnetic Emissions," IEEE Trans. Electromagn. Compat., vol. 48, no. 4, pp. 752–759.

[7] H. Weng, X. Dong, X. Hu, D. G. Beetner, T. Hubing, and D. Wunsch, "Neural network detection and identification of electronic devices based on their unintended emissions," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 8-12, 2005, vol. 1, pp. 245-249.

[8] P. Dourbal, "Method and apparatus for detecting and locating a concealed listening device," U.S. Patent 5,717,656, Feb. 10, 1998.

[9] F. Dowla, ed., *Handbook of RF and Wireless Technologies*. Burlington, MA: Elsevier, 2004.

[10] L. J. Giacoletto, ed., *Electronics Designer's Handbook*, 2nd ed. New York, NY: McGraw-Hill Inc., 1977.

3. DETECTION OF REGENERATIVE RECEIVERS BASED ON THE MODULATION OF THEIR UNINTENDED ELECTROMAGNETIC EMISSIONS

3.1. ABSTRACT

Detection of super-regenerative receivers using their unintended electromagnetic emissions at a significant distance is challenging due to high levels of ambient noise. Using a simple sine wave stimulation to modify these unintended emissions has shown to produce better results over passive detection techniques by improving the signal quality and the consistency of the unintended emissions, but is still rather limited in extending the reliable detection distance. If the response of the receiver to a stimulation is known, however, a more complex stimulation can be used to embed additional information into the unintended emissions. For regenerative receivers, an amplitude modulated stimulation generates a corresponding modulation in the in the unintended emissions. The receiver may thus be detected from these modulated emissions by calculating the received signal energy and then correlating it with the amplitude of the stimulation. A high correlation indicates the presence of the device. The receiver may be detected even when its emissions are well below the noise floor. Results show that five super-regenerative receivers from 3 different manufacturers can be detected in a noisy ambient environment to distances of over 100 meters with an area under the receiver operating characteristic (ROC) curve of 94%.

3.2. INTRODUCTION

Electronic devices, when active, often unintentionally radiate measurable levels of electromagnetic emissions. These emissions have previously been analyzed to passively detect and identify these devices [1] [2]. The procedure of identifying devices by their emissions is complex when performed in a semi-anechoic environment, but the real challenge is identifying devices from a substantial distance and picking out the target emissions from within a noisy urban environment that may contain similar and potentially stronger emissions sources.

Previous research has worked with wireless receivers to identify them based on their unintended electromagnetic emissions using simple matched filters [3] – [5],

using neural networks [6] – [7] and using algorithms that utilize both the time and the frequency domain attributes of the signals from devices [1] [2]. In [1] and [2], a three step detection algorithm was introduced whereby the emissions from a device are first characterized by acquiring a series of measurements of the emissions in the time and frequency domains. These measurements were used to develop an "ideal" emissions signal in the time domain that was specific to a single device. The data acquired during the device characterization phase was then utilized in a detection algorithm that determined if that specific device was present in an unknown noisy ambient environment. Detection was accomplished by using the shape of the emissions pulse from the receiver, the repetition rate of the emissions pulses, and the expected bandwidth of the emissions.

Each of these prior methods passively listens to the unintended emissions from a device. A "bug scanner" represents one common method for actively detecting electronic devices. Bug scanners operate by radiating a target with a strong stimulation signal that is rectified by non-linear PN junctions in the device, resulting in a re-radiation of the harmonics of the original stimulation signal [9]. Measured harmonics indicate the presence of an electronic device. This is not an ideal technique for several reasons. First, since a large number of non-linear junctions respond to this type of stimulation, false positives are common. Secondly, the radiation of the harmonics is fairly weak dictating that a close proximity between the scanner and the device is needed for accurate detection. Finally, the high power levels required to trigger a measurable response are often impractical.

In [8], the authors used an active stimulation approach to detect super-regenerative receivers that has produced better results than when not using a stimulation. The weak stimulation used in [8] generates a much stronger response from the device than typical bug scanning methods and makes the unintended emissions from the device more consistent allowing better performance of the detection methods introduced in [2] and [8]. An algorithm was also introduced in [8] to generically detect not a single device, but any member of the class of regenerative receivers by comparing the energy in the emissions when the stimulation was turned on compared to when it was turned off.

Here we present a technique that improves the range of detection of super-regenerative receivers in a noisy environment by introducing a pseudo-random modulated stimulation signal to modify the receiver's unintended emissions. The response of the regenerative receivers to a stimulation will be discussed and a new detection algorithm will be presented. This algorithm requires only the knowledge of how a

class of devices, such as super-regenerative receivers, responds to a known stimulation and the frequency band of the device's emissions. The specific characteristics of the device's unintended emissions that were needed for the algorithm in earlier approaches are not necessary for the algorithm presented here. The algorithm presented here simply uses the fact that all regenerative receivers are expected to show a similar change in emissions with a stimulation. This approach improves the detection range from 40 meters in [8] to over 100 meters. The exact distance is not given for security reasons.

3.3. METHODS

The detection method introduced here uses a weak pseudo-random modulated sine-wave stimulation to modify the unintended emissions from a regenerative receiver, causing the emissions to be modulated according to the same pseudo-random sequence. Knowledge of how a class of devices respond to a particular stimulation must be obtained through a device characterization procedure in a semi-anechoic chamber. During this characterization, key device radiation characteristics are determined by measuring electromagnetic emissions in the time and frequency domains so that the optimal stimulation signal can be devised and used in conjunction with a detection algorithm. Five different low-cost RF toys from three different manufacturers containing 50-MHz super-regenerative receivers were studied in this paper.

3.3.1. Electromagnetic Emissions. Figures 3.1 and 3.2 illustrate the typical emissions from the five studied regenerative receivers in the frequency and time domains. Each of these receivers was tuned to receive a signal at 50 MHz. The similarity among the five devices is apparent in the plots presented. The characteristics of the pulses seen in the time domain tend to be well constrained for all of the devices, but may differ between measurements or even within a single measurement. For all five devices, the pulse envelope, pulse repetition rate and the pulse magnitude all vary around some nominal value that is different for each device and can change drastically depending on the ambient noise or, in the absence of stimulation, may vary depending on random processes within the receiver. These parameters become more consistent when subjected to a targeted radio-frequency (RF) stimulation [8].

The process we used to characterize the emissions from regenerative receivers can be found in Fig. 3.3. A general characterization was performed first to determine

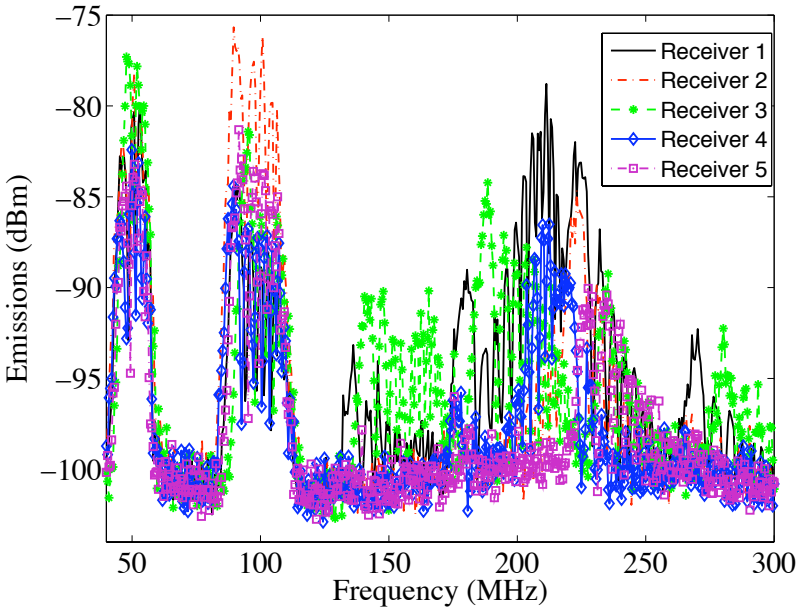


Figure 3.1 Unintended electromagnetic emissions from five different super-regenerative receivers in the frequency domain.

the unintended emissions when the device is not in the presence of a stimulation signal. Emissions were measured in a semi-anechoic chamber to minimize any ambient noise. In our measurements we used a Sunol Sciences JB5 biconilog antenna connected to an Agilent Infinium 54855A oscilloscope and a Rhode and Schwarz FSEB spectrum analyzer to determine the time and frequency domain characteristics, respectively. Several measurements for all devices were obtained with resolution and video bandwidths of 10 kHz and a sweep time of 9800 ms. The unintended emissions were sampled in the time domain at 2×10^9 samples per second. 100 microseconds of data containing approximately 20 pulses were initially acquired during the characterization phase. Nominal attributes of the emissions were derived from the measurements, including the shape, rate and frequency content of the pulses, and the change in frequency content over time. After determining the nominal radiation characteristics of the device, emissions were measured while applying an electromagnetic stimulation.

Various stimulation frequencies were tested and the frequency with the best response was recorded. In most cases, the receivers were susceptible to an RF stimulation signal in the same frequency range where the device had radiated emissions. For example, all of the devices used in this study were 50 MHz receivers that also had

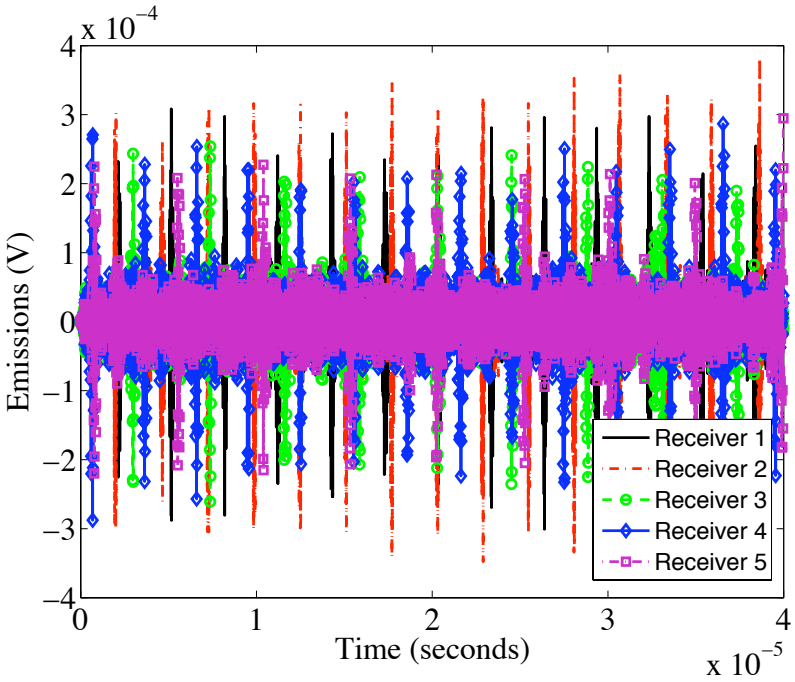


Figure 3.2 Unintended electromagnetic emissions from five different regenerative receivers in the time domain.

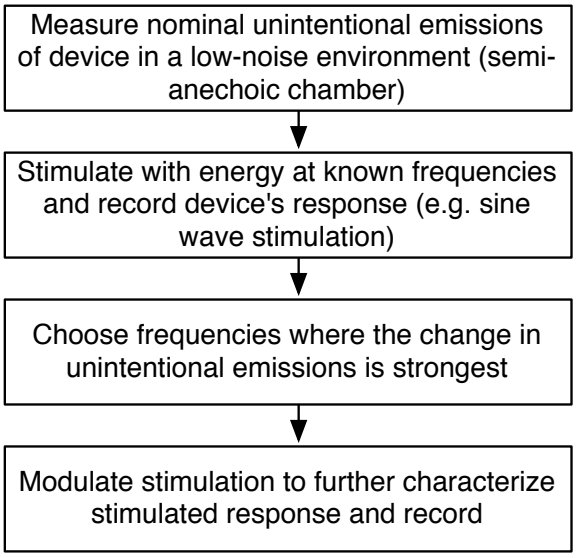


Figure 3.3 Stimulation characterization procedure.

emissions around 50 MHz. Not surprisingly, a stimulation signal at 50 MHz delivered the strongest response. Although the stimulation produced a noticeable change in the emissions, as shown in a representative plot measured from one of the five receivers in Fig. 3.4, it was sufficiently different from the signal expected by the receiver that it did not activate the device (it only affected the unintended emissions). The stimulation power is relatively weak, with only about -45 dBm of output from the signal generator needed to illicit a detectable response for this measurement setup.

In addition to making the pulse rate more consistent, the device's pulse repetition rate increases with the level of stimulation [8]. Thus, as illustrated in Fig. 3.5, the emissions can also be modulated by varying the stimulation power. The pulses for the frequency modulated portion of this plot were exaggerated for demonstration purposes. Increasing the amplitude of the stimulation results in a different number of pulses over a given time segment. Since the pulses themselves (and the energy in each pulse) remains largely unchanged, the energy in the emissions changes in proportion to the level of the stimulation [8].

3.3.2. Detection. The passive detection algorithm presented in [2] did not use any stimulation and as a result was found to be ineffective at a long distance in a particularly noisy environment. Detection was drastically improved in [8] by applying a sine-wave stimulation of -28 dBm while still employing the passive algorithm from [2], however, it did not significantly increase the detection distance. Detection can potentially be improved by embedding additional known information in the emissions. The detection scheme shown in Fig. 3.6 was developed using knowledge of how the unintended emissions of a regenerative receiver can be modified using an active stimulation signal. A pseudo-random sine-wave that varied from 1–20 kHz was used to amplitude modulate a 50-MHz sine-wave to generate an information-rich stimulation. A pseudo-random signal maximizes the information in the signal [10].

The stimulation signal was created by using a combination of MATLAB's pseudo-random number generator to create a string of sine-waves that was then sent to an Agilent 33250A function/arbitrary waveform generator to create the pseudo-random amplitude modulated 50 MHz stimulation signal. A chain of four different sine-waves that could be one of 20 sine-waves in the set of $[1, 2, ..., 19, 20]$ kHz was chosen at random by MATLAB and was sent to the arbitrary waveform generator via GPIB. The length of the pseudo-random amplitude modulation was 4 milliseconds, which is 4 cycles of a 1 kHz sine-wave or 80 cycles of a 20 kHz sine-wave. The amplitude modulation part of the signal essentially had four bits of information, meaning that four different sine-waves were combined together one after the other, within the

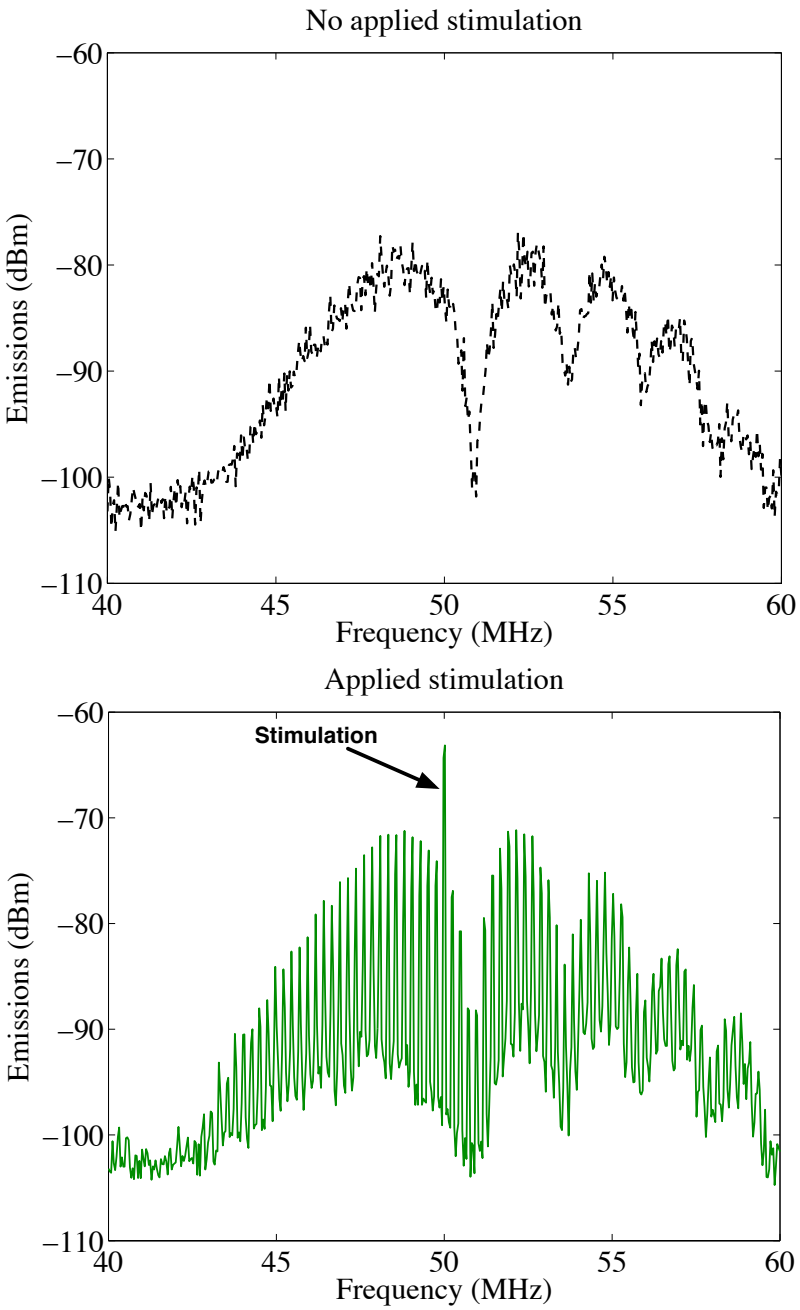


Figure 3.4 Unintended electromagnetic emissions from a super-regenerative receiver that is representative without (top) and with (bottom) stimulation.

4 millisecond message, so that each randomly chosen sine-wave cycled for roughly 1 millisecond. The sine-waves were carefully combined so that only integer-multiple periods were used for each randomly chosen sine-wave in the chain of sine-waves to avoid discontinuities that could lead to frequency domain leakage errors. Despite the

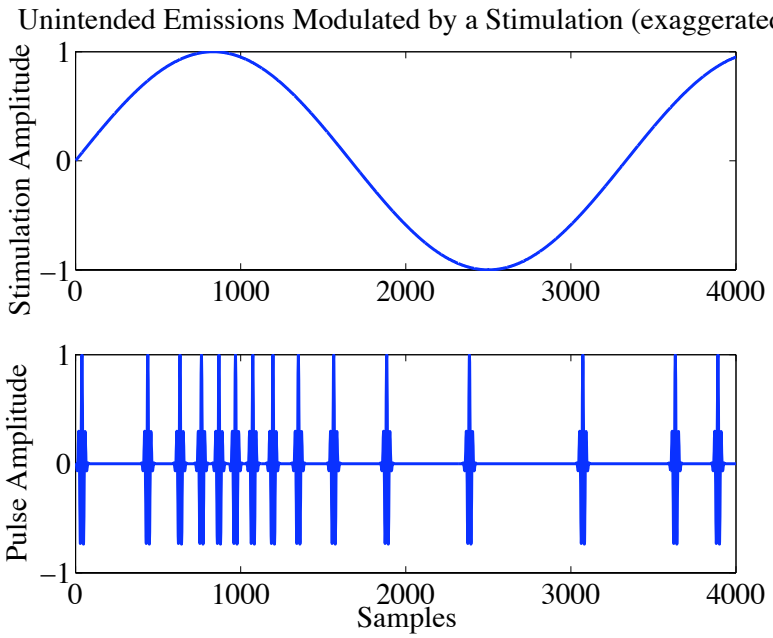


Figure 3.5 An exaggerated example of modulated stimulation unintended emissions.

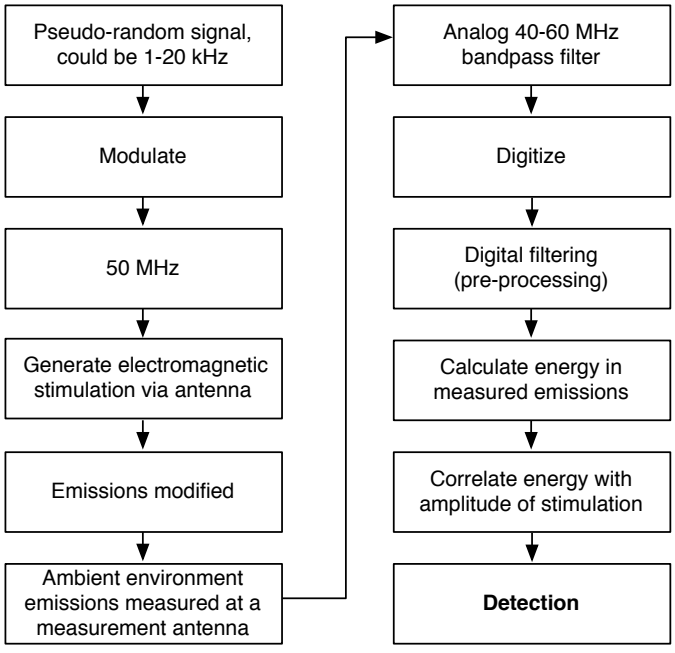


Figure 3.6 Detection algorithm.

bit length, (i.e. one of the four chosen sine-waves) being not exactly 1 millisecond depending on the frequency of the sine-wave, the 4 millisecond total message time was always maintained. Each created stimulation signal was recorded for every measurement as well as the actual stimulation sent to the antenna by the waveform generator before it was radiated.

The pseudo-random signal was delivered to the device via an ETS 3142B hybrid log-periodic antenna (frequency range 26 MHz – 2GHz), resulting in the unintended emissions of the regenerative receiver being modulated in-step with the known stimulation signal. The stimulation output from the generator was -10 dBm. The ambient emissions were measured at a second antenna, the CD CLP5130-1 log-periodic (a directional antenna at 50 MHz), using an analog 40–60 MHz bandpass filter attached to an oscilloscope to digitize the emissions and send them to a computer for digital signal processing. The antenna was a directional antenna that provided The emissions were sampled at a rate of 1×10^9 samples per second. 5 milliseconds total of data was collected with a LeCroy wavemaster 8600A oscilloscope that was triggered by the stimulation signal. The extra 1 millisecond of data beyond the 4-millisecond stimulation was not used.

Once digitized, the signal was again filtered digitally with a steep notch filter to remove the stimulation frequency at 50 MHz, as well as a steep low pass filter with a cut-off frequency of 60 MHz followed by another steep high pass filter with a cut-off frequency of 40 MHz. The short-time energy in the resulting signal was then calculated as follows

$$E[n] = \sum_m (x[m]w[n-m])^2 \tag{3.1}$$

where E is the short-time energy calculation, x is the measured signal, and w is a Hanning window with a varying length, depending on the amplitude of the stimulation. Though the actual window shape (e.g. Hanning, Blackman) is not as important as the window length, the Hanning window was chosen to obtain a smooth short-time energy that would better correlate with the amplitude of the stimulation. The Hanning window is written in the time domain as

$$w[n] = 0.5\left[1 + \cos\left(\frac{2\pi n T_s}{T_H}\right)\right] \quad -\tfrac{1}{2}T_H \leq nT_s \leq \tfrac{1}{2}T_H \tag{3.2}$$

where w is the Hanning window, T_s is the sampling period, and T_H is the Hanning window length. T_H is selected for each sine-wave in the chain of sine-waves according to the following

$$T_H = \frac{1}{f_{stim}K} \text{ where } K \geq 4 \tag{3.3}$$

where f_{stim} is the amplitude stimulation frequency and K is an integer number greater than or equal to 4. If a regenerative receiver is present, it will respond to the the stimulation with an increased pulse repetition frequency when the amplitude of the stimulation is greatest and a decreased pulse repetition rate when the amplitude is lowest. Thus, it is important to choose the Hanning window length so that it is some fraction of the sine-wave amplitude stimulation to capture these changes in the receiver's emissions. It is not difficult to change this length while calculating the short-time energy, since the stimulation signal is known.

Once calculated, the energy, E, is then correlated with the amplitude of the stimulation signal [11]

$$y_{out}[n] = \frac{\sum_k E[k]s^*[k-n]}{\sqrt{\sum_n \left(E[n]\right)^2 \sum_n \left(s[n]\right)^2}} \tag{3.4}$$

where E is the calculated energy of the emissions, s is the amplitude of the known stimulation, y_{out} is the normalized output of the cross-correlation, and $*$ represents the complex conjugate. The energy is correlated with the amplitude of the stimulation to capture the change in the emissions with the strength in the applied stimulation. A higher stimulation amplitude results in a higher pulse repetition rate [8], and a higher amplitude for those pulses in the unintended emissions of the regenerative receiver and, thus, a higher energy. These changes in the energy coincide with the amplitude variation of the amplitude modulated stimulation.

The result of the normalized correlation, y_{out}, which was computed in the time domain is compared to an expected threshold value to determine the presence of a device. A successful threshold match was determined by calculating the detection statistic, γ, after the correlation and comparing it to an expected threshold. The detection statistic was calculated as,

$$\gamma = \texttt{max}\{|y_{out}[n]| : n \in [0, N]\} \tag{3.5}$$

where γ is the detection statistic, y_{out} is the output of the correlation with the stimulation, and N is the total number of samples. A large peak in the cross-correlation indicates a high correlation with the amplitude of the stimulation and, therefore, is why γ was chosen as the maximum over the normalized correlation. The detection statistic is compared in the last step of the algorithm with a stored threshold to determine if a device is present. A higher value for the detection statistic indicates that it is more probable that the target device is present. Note that no information except the receive band and the expected band of emissions are required to use this algorithm.

3.4. RESULTS

The method discussed in this paper was tested in a very noisy urban environment – on the lawn outside our laboratory. Detection in the noisy urban environment at 40 meters is shown in Fig. 3.7 using a receiver operating characteristic (ROC) curve. Fig. 3.7 shows the comparison between the ROC's of the algorithm discussed in [2], called the cascading correlation algorithm, and the proposed modulated stimulation algorithm. These results reflect the detection of only one of the five tested receivers, since the cascading correlation algorithm is a device specific algorithm it can not be used to detect all five devices at the same time. Both algorithms yielded similar results using data up to 40 meters. The cascading correlation and the modulated stimulation algorithms produced areas under their ROC curves of 98% and 97%, respectively. Each ROC curve included 650 measurements that were taken at all times of the day over 12 days. Of these measurements, 325 sets contained the receiver, while 325 contained only noise.

Extending the distance to over 100 meters and including measurements of 5 regenerative receivers generated the ROC curve shown in Fig. 3.8. 3,015 total measurements were included in this ROC curve that were composed of emissions from five target devices (only one device per measurement) and were taken at all times of the day over 18 days. These measurements included 1,510 measurements containing one of the five receivers (divided roughly 5 ways, about 300 measurements per device) and 1,505 measurements containing only ambient noise. The modulated stimulation algorithm produced an area under the ROC curve of 94%.

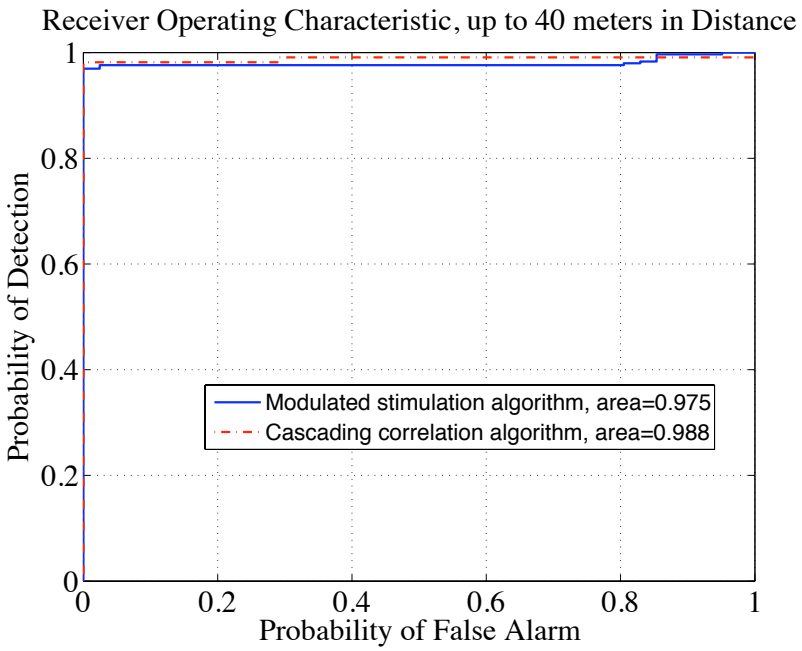


Figure 3.7 Receiver operating characteristic (ROC) of the modulated stimulation algorithm compared with the cascading correlation algorithm for a single device at distances of up to 40 meters.

Comparing the modulated stimulation algorithm with the cascading correlation algorithm from [8] at distances over a 100 meters in, in Fig. 3.9, these algorithms produced an area under the ROC curves of 93% and 85.1%, respectively and a probability of detection with no false alarms of 87% and 9.6% respectively. The modulated stimulation algorithm yielded improved results over the cascading correlation algorithm at the greater distances when the signal-to-noise ratio was low. Both algorithms were tested using the same data that consisted of 1,401 total measurement sets (705 sets containing a single receiver and 695 containing noise data only). The results for the modulated stimulation algorithm are different than those shown in Fig. 3.8, because the ROC curve for Fig. 3.9 was calculated with data that only included one device. Using only one device was necessary for this comparison, since the cascading correlation algorithm is device specific and can not be used for multiple devices at the same time, in contrast to the modulated stimulation algorithm. The improved range over those in [8] for the cascading correlation algorithm likely resulted from the use of a highly directional receiving antenna. In addition, better results could be expected with the modulated stimulation algorithm using a longer stimulation or one with a higher bandwidth, since more information could be encoded in the signal to result in

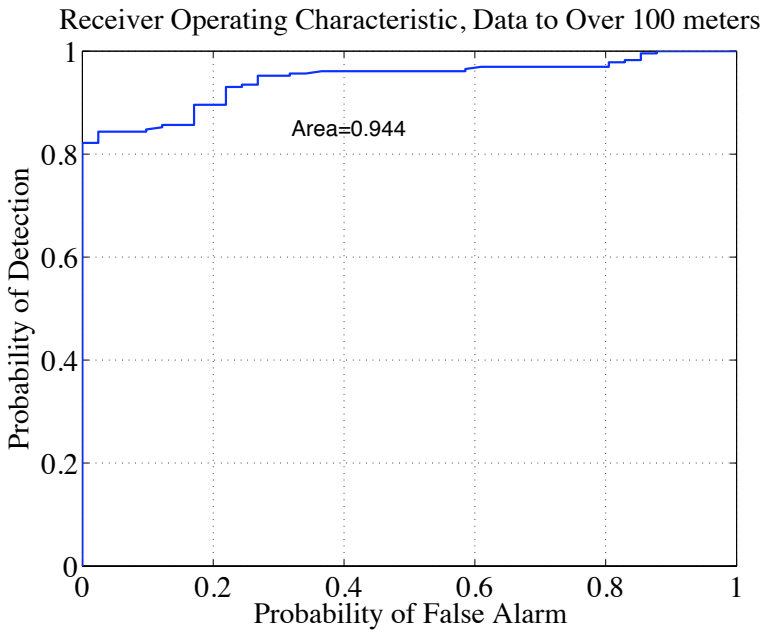


Figure 3.8 Receiver operating characteristic (ROC) of the modulated stimulation algorithm for 5 different devices at distances of over 100 meters.

a higher correlation. These tests were not conducted here because of limits with the test equipment.

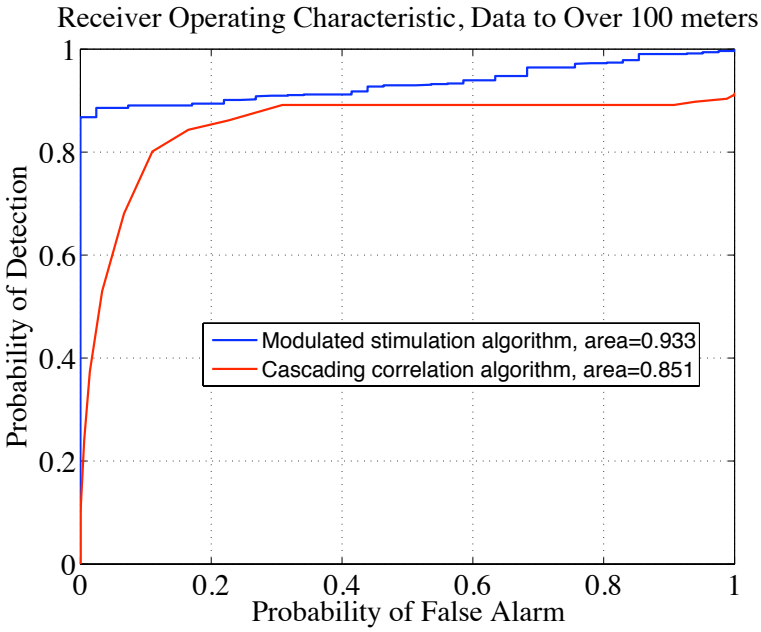


Figure 3.9 Receiver operating characteristic (ROC) of the modulated stimulation algorithm compared with the cascading correlation algorithm for a single device at distances of over 100 meters.

3.5. CONCLUSION

In this paper, a method was presented to detect super-regenerative receivers by imposing known information on the receiver's unintended electromagnetic emissions. An amplitude-modulated signal with significant information content - in this case a band-limited pseudo-random sequence - is delivered as an electromagnetic signal to the device and the resulting ambient electromagnetic emissions are measured. The energy in these emissions are then correlated with the known amplitude-modulated signal. The result of the correlation is used to determine if a device is present. Using this algorithm, five different regenerative receivers were detected at over 100 meters with an area under the ROC curve of 94%. Note that while the cascading correlation algorithm was able to detect the devices at over 100 meters with an area under the ROC curve of 85%, the modulated stimulation algorithm had a significantly better detection rate at 0% false alarms, had a higher area under the ROC curve, and does not require highly specific information about the device, as is required when using the cascading correlation algorithm. The approach has the additional advantages that very little information is required about the device - only the receive and emissions bands - so that new receivers might be detected even if they had not previously been encountered and the advantage that only regenerative receivers are expected to respond to the stimulation in the described way, so that false alarms may be minimized.

3.6. REFERENCES

[1] D. G. Beetner, S. Seguin, T. Hubing, "Electromagnetic emissions stimulation and detection system," U.S. Patent 7,464,005, Dec. 9, 2008.

[2] S. A. Seguin, D. G. Beetner, T. Hubing, "Detection and Identification of Low-Cost RF Receivers Based on their Unintended Electromagnetic Emissions," in IEEE Trans. Electromagn. Compat., under review.

[3] T. Hubing, D. G. Beetner, X. Dong, H. Weng, M. Noll, H. Göksu, B. Moss, and D. Wunsch, "Electromagnetic detection and identification of automobiles," presented at *EuroEM*, Magdeburg, Germany, Jul. 2004.

[4] A. Shaik, H. Weng, X. Dong, T. H. Hubing, and D. G. Beetner, "Matched filter detection and identification of electronic circuits based on their unintentional radiated emissions," in *Proc. IEEE Int. Symmp. Electromagn. Compat.*, Aug. 14-18, 2006, vol. 3, pp. 853–856.

[5] T. Hubing, D. G .Beetner, S. Seguin, B. Moss, M. Schmidt, "Improvised explosive device detection based on unintentional electromagnetic emissions," presented at *IEEE Ant. and Prop. Soc. Int. Symp.* Piscataway, NJ, 2006, pp. 202.

[6] X. Dong, H. Weng, D. G. Beetner, T. Hubing, D. Wunsch, M. Noll, and H. Göksu, "Detection and Identification of Vehicles Based on Their Unintended Electromagnetic Emissions," IEEE Trans. Electromagn. Compat., vol. 48, no. 4, pp. 752–759, 2006.

[7] H. Weng, X. Dong, X. Hu, D. G. Beetner, T. Hubing, and D. Wunsch, "Neural network detection and identification of electronic devices based on their unintended emissions," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 8-12, 2005, vol. 1, pp. 245-249.

[8] S. A. Seguin, D. G. Beetner,T. Hubing, "Controlling Unintended Emissions from Regenerative Receivers to Improve Detection and Identification," in IEEE Trans. Electromagn. Compat., under review.

[9] P. Dourbal, "Method and apparatus for detecting and locating a concealed listening device," U.S. Patent 5,717,656, Feb. 10, 1998.

[10] D. G. Manolakis, D. Manolakis, V. Ingle and S. M. Kogon, *Statistical and Adaptive Signal Processing: Spectral Estimation, Signal Modeling, Adaptive Filtering and Array Processing.* Massachusetts: Artech House Publishers, 2005.

[11] A. Oppenheim and R. Schafer, *Discrete-Time Signal Processing.* New Jersey: Prentice-Hall, 1999.

SECTION

2. CONCLUSIONS

In this dissertation, unintended emissions from electronic devices were studied for the purposes of remote identification. Through a series of experiments and discoveries, the methods used to identify devices was refined and improved. First, a passive detection was presented based on particular characteristics of the target device's unintended emissions. These emissions were then analyzed using a cascading correlations method that yielded positive detection at a distance of 40 meters with an area under the ROC curve of 98%.

This technique was taken a step further when the addition of a stimulation signal at the receiver's frequency band was shown to react with the receiver making it easier to detect the device at greater distances. A US patent was awarded for this unique detection method. Additionally, this method may also be used as a generic regenerative receiver even if the device had not been previously characterized.

Finally, an additional method was designed building on the previous efforts which integrated a pseudo-random sequence into the stimulation signal. The detection algorithm works by detecting the induced change in the target device's unintended emissions. This technique also can be performed without characterization of the device as was needed in previous methods as long as the general frequency band of the device to be detected is known. The result produced detection at over 100 meters with an area under the ROC curve of 93%.

BIBLIOGRAPHY

[1] D. Beetner, S. Seguin, T. Hubing, "Electromagnetic emissions stimulation and detection system," U.S. Patent 7,464,005, Dec. 9, 2008.

VITA

Sarah Ann Seguin was born as Sarah Ann Hartleben on 21 October 1977 in St. Paul, Minnesota. She graduated magna cum laude with her B.S in Electrical Engineering from the Missouri University of Science and Technology (Missouri S&T) in 1999. As an undergradraduate, she held a recurring internship over summers and vacations at Guidant Corporation in Arden Hills, Minnesota. At Missouri S&T, Seguin was an active member of the Institute of Electrical and Electronics Engineers, holding positions as the Chairperson, Treasurer, Computer Society Chair, Power Society Chair and Web Master. In addition, she was permitted membership of Eta Kappa Nu and held the Bridge Correspondent position. After receiving her B.S. she took a hiatus from electrical engineering to write patents at the law firm of Schwegman, Lundberg, and Woessner L.L.C. in Minneapolis, MN and to attend law school for one semester. After her semester of law school, Seguin returned to the field of electrical engineering and held a full-time engineering position at Guidant Corporation before returning to graduate school. As a graduate student at Missouri S&T, she worked in the Electromagnetic Compatibility Laboratory of the Electrical and Computer Engineering Department, guided by her advisor Dr. Daryl Beetner while earning her Ph.D. Her M.S. was awarded in August 2005 and her Ph.D. in 2009 both of them from Missouri S&T.