TOWARD COGNITIVE VECTOR NETWORK ANALYZERS FOR CONDUCTING WIRELESS STIMULUS-RESPONSE MEASUREMENTS IN OPEN-AREA ENVIRONMENTS

by

Robert Douglas White

B.A.Sc., The University of British Columbia, 2009

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF APPLIED SCIENCE

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

(Electrical and Computer Engineering)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

April 2015

Abstract

Vector network analyzers (VNAs) are often used to measure antenna performance, channel response, and shielding effectiveness in open-area environments. In such applications, external interference from other users may sporadically occupy portions of the frequency band of interest and thus compromise the integrity of the measurements. The simple strategies for avoiding such interference that are commonly employed may be ineffective because: 1) clear channels within the band may not be available, 2) it may be difficult to find suitable antennas for use in adjacent clear bands, 3) the other users in the band may be uncooperative, 4) the interference encountered in the band may be intolerable even during off-peak hours or 5) it may not be possible or convenient to move to a different measurement location. Here, we show that the reliability and accuracy of VNA-based wireless measurements performed under such circumstances can be significantly improved by applying cognitive radio concepts where uncooperative wireless systems are cast as primary users and the VNA is cast as the secondary user. For the case of long-burst interference, i.e., scenarios dominated by voice and video transmissions that are much longer than the VNA measurement dwell time, we propose and demonstrate a scheme that uses carrier sensing to: 1) avoid collisions between VNA and primary user transmissions and 2) identify and reject corrupted measurements. For the case of short-burst interference, i.e., scenarios dominated by data packet transmissions that are much shorter than the VNA measurement dwell time, we show that identification and rejection of corrupted measurements is more difficult but can be accomplished by modifying the interference-aware VNA to apply robust estimation to the results. The main limitation of the second scheme is the time required to collect the additional measurement data required. In both cases, re-purposing existing hardware within the VNA and making relatively minor enhancements to the firmware would both simplify implementation and significantly decrease the data collection time. Both cases represent an important step toward realizing a fully cognitive VNA that is capable of sensing its environment and configuring itself to conduct interference-free wireless measurements as quickly and effectively as possible.

Preface

This thesis is based on work conducted in UBC's Radio Science Laboratory (RSL) by Prof. David G. Michelson and Robert D. White. This work followed a brief earlier exploration of the interference-aware vector network analyzer (VNA) concept by Prof. Michelson and Dr. Nikola Stanchev (then a postdoctoral research fellow in UBC RSL.)

Both Prof. Michelson and Mr. White contributed to the literature survey, development of the two variants of the interference-aware VNA concept, the research plan and the structure of the thesis. Mr. White was solely responsible for the development of the spectrum occupancy measurement system and collection and reduction of the corresponding measurement data, and development of the interference-aware VNA prototypes and collection and reduction of the corresponding performance data. Prof. Michelson and Mr. White both contributed to editing and refinement of the text and figures in the thesis.

Table of Contents

List of Tables

List of Figures

Acknowledgements

I thank my supervisor, Prof. David Michelson, for suggesting a thesis project that so closely aligns with my interests while having the potential for considerable industry impact.

I gratefully acknowledge the funding provided to me by NSERC and Bell Canada through a Collaborative Research and Development Grant entitled "Towards Fourth Generation Wireless Networks Incorporating Cognitive Radios" (CRDPJ 395689 – 09).

The interest expressed in our interference-aware VNA concept and feedback provided to us by the following people were particularly helpful:

- Dennis Lewis, *Technical Fellow - RF / Microwave and Antenna Metrology*, The Boeing Co., Seattle, WA
- Parminder Singh, *Division Manager - Electromagnetic Compatibility Department,* QAI Laboratories, Coquitlam, BC.
- Dr. John Lodge, *Chief Technical Officer,* Communications Research Centre Canada, Ottawa, ON (in his former capacity as *Research Program Manager of the Communications Signal Processing Group*)
- Garth D'Abreu, *Director of RF Engineering – Test Solutions Group*, ETS-Lindgren, Cedar Park, TX

The Spectrum Explorer software provided by the Communications Signal Processing Group of the Communications Research Centre (CRC) Canada, along with their efforts to develop a software driver for the Agilent/Keysight N6841A RF Sensor, provided us with an important and unique capability to measure spectrum occupancy.

The Infiniium DSO7034B Oscilloscope provided to us by Agilent Technologies (now Keysight Technologies) under a special grant greatly assisted in the development and validation of the hardware prototypes of our interference-aware VNA.

The responses received from hardware vendors regarding their product lines and instrument capabilities in the context of this research enhanced the completeness of this thesis. Thanks to:

- Steve Hall, *RF Applications Specialist*, Keysight Technologies (formerly Agilent Technologies), Vancouver, BC
- Pui Him Wai, *Account Manager*, Rohde and Schwarz Canada, Vancouver, BC

Dedication

I dedicate this thesis to all of my family and friends. Their friendship and support during the course of my studies were both essential and very much appreciated.

Chapter 1
Introduction

Since the earliest days of wireless communication, it has been recognized that the wireless spectrum is a finite resource that must be managed carefully and shared equitably [1]. Much of the effort devoted to the advancement of wireless technology during the past century has been devoted to increasing the number of simultaneous users that can coexist and maximizing the amount of information that they can exchange within a specified portion of the wireless spectrum. While ensuring that wireless communications applications can coexist is already challenging, ensuring that wireless communications and wireless measurement applications can coexist is particularly difficult given the sensitivity of most wireless measurement applications to noise and interference [2].

Vector network analyzers (VNAs) are stimulus-response test sets that are used to characterize the complex frequency response of an unknown system [3]. They generally offer higher resolution and dynamic range than alternative wireless stimulus-response measurement techniques. For this reason, test setups based upon VNAs are often used to characterize wireless channels in open-area environments despite the inconvenience of requiring a direct connection between the transmitter and receiver. The types of wireless measurements conducted using such equipment are diverse. For example: 1) Antenna designers often use VNAs to characterize the radiation pattern or polarization response of an antenna by measuring the signal received by the antenna when it is illuminated from various aspects [4], [5], 2) Wireless system designers often use VNAs to characterize channel impairments by measuring channel frequency response or channel impulse response [6], [7], and 3) Electromagnetic compatibility (EMC) engineers often use VNAs to characterize the shielding effectiveness of an enclosure, vehicle or building by measuring the excess path loss [8], [9], [10].

The integrity of VNA-based wireless measurements may be compromised by external interference from other users who may occupy portions of the frequency band of interest. In the frequency domain, it is useful to characterize external interference as *broadband*, *narrowband*, or *point-like* depending on the bandwidth of the interfering signals compared to

the frequency span of interest and the interval between measurement points in the frequency span. In the time-domain, it is useful to characterize external interference as *continuous*, *long-burst*, or *short-burst* depending on the duration of the interfering signals compared to the time that the VNA must wait for the IF filter to charge at each measurement point in its sweep, i.e., the measurement dwell time.

Common strategies for avoiding external interference include: 1) identifying clear channels in which measurements can be conducted, either within the frequency band of interest or possibly within adjacent frequency bands, 2) making suitable arrangements with the interfering users to share the band or conducting measurements during off-peak hours when the interference is greatly reduced, or 3) conducting the measurements in a different location that is free from interference. However, such avoidance strategies are often inconvenient and may be ineffective if: 1) clear channels within the band are not available, 2) antennas suitable for use in adjacent bands are not available, 3) the other users in the band are uncooperative or unaware, 4) the interference encountered in the band is intolerable even during off-peak hours, or 5) it is impractical to move the device or scenario under test to another location. In such cases, alternative strategies are required.

The objective of this thesis is to show that the reliability and accuracy of VNA-based wireless measurements performed in open-area environments where continuous, long-burst, and short-burst interfering signals of various bandwidths are encountered can be significantly improved by applying cognitive radio concepts where uncooperative wireless systems are cast as primary users and the VNA is cast as the secondary user. We refer to our proof-of-concept implementation as an *interference-aware* VNA. It represents the first step towards a *cognitive* VNA that is capable of monitoring the wireless environment and configuring itself as required to conduct interference-free wireless measurements quickly and effectively.

The remainder of this thesis is organized as follows:

In Chapter Two, we begin by reviewing previous work and essential concepts including: 1) essential aspects of VNA function and operation, 2) the major applications of VNAs in wireless measurements, 3) alternatives to VNAs for wireless stimulus-response measurements, 4) recent progress in spectrum occupancy measurement and modeling, 5) recent progress in interference avoidance and wireless coexistence techniques used in

wireless measurements and a summary of cognitive radio concepts. We conclude by suggesting that the interference-aware or cognitive VNA is a natural next step in the evolution of VNAs for wireless measurement applications.

In Chapter Three, we describe how we conceived, implemented and verified the performance of an interference-aware VNA suitable for conducting wireless measurements in typical long-burst interference environments, i.e., those dominated by voice and video transmissions that are much longer than the VNA dwell time. We demonstrate that it is a relatively simple matter to add an external sensing receiver, external logic and external control software to a modern high-performance VNA with direct access to certain elements of the hardware and use carrier sensing to: 1) avoid collisions between VNA and primary user transmissions and 2) identify and reject corrupted measurements. However, we conclude that while our scheme is practical, the cost and effort required to realize an interference-aware VNA would be greatly reduced if manufacturers would implement the functionality internally by using one of the reference receivers as a spectrum-sensing receiver and making relatively minor enhancements to the firmware and internal connections. This would also avoid the large latencies associated with conventional schemes for external instrument control.

In Chapter Four, we describe how we modified the interference-aware VNA described in the previous chapter to perform well in typical short-burst interference environments, i.e., those dominated by data packet transmissions with durations that are much shorter than the measurement dwell time. We demonstrate that identification and rejection of corrupted measurements is more difficult than in the long-burst case but can be accomplished with high effectiveness by post processing the data using robust estimation techniques. The main limitation of the scheme is the longer time required to collect the required measurement data. Collecting the minimum necessary data for robust estimation to be effective can reduce measurement times, but the statistics to aid operators with identifying the minimum amount needs to be developed. Once again, we conclude that our scheme is practical but that implementing the functionality internally could vastly reduce the cost and effort required to realize such an instrument.

In Chapter Five, we summarize our contributions and offer recommendations for further work.

Chapter 2

Background and Motivation

2.1 Introduction

Our interference-aware or cognitive vector network analyzer draws from several bodies of previous work. Here, we summarize relevant work in five areas: 1) fundamental aspects of VNA function and operation, 2) the major applications of VNAs in wireless measurements, 3) alternatives to VNAs for wireless stimulus-response measurements, 4) recent progress in spectrum occupancy measurement and modeling, 5) recent progress in interference avoidance and wireless coexistence, including cognitive radio. We conclude by suggesting that the *interference-aware* or *cognitive* VNA is a natural next step in the evolution of VNAs for wireless measurement applications.

2.2 Vector Network Analyzers

2.2.1 VNA Architecture and Operation

A vector network analyzer (VNA) is a swept-frequency stimulus-response test set used to characterize RF/microwave devices or networks. It functions by sweeping or stepping a single carrier across a *frequency span* comprising numerous points in quick succession and applying that signal to the input port of a device or network under test (DUT or NUT). It determines the reflection and transmission response of the DUT or NUT by comparing the amplitude and phase of the reflected and transmitted signals, respectively, with those of the incident signal. The set of points that comprise the response across the frequency span is called a *trace*. Developed by Hewlett-Packard during the mid 1960's, VNAs transformed RF/microwave engineering by making characterization of devices and networks rapid, reliable and reproducible. They were among the first widely used RF/microwave measurement systems to rely on a computer-based controller and external control bus (HPIB, later GPIB) to automate configuration, calibration, measurement and error correction. Most VNAs are designed to characterize one- and two-port devices and networks; certain specialized VNAs are capable of measuring additional ports [11].

A block diagram of a typical VNA is shown in Figure 1. During a typical measurement sequence, the controller causes the RF source to emit a single carrier of specified frequency and amplitude. The signal is passed through a pair of directional couplers then applied to the input port of the device or network under test. A fraction of the incident signal is sampled by the forward directional coupler and is referred to as the reference signal, *R*. A fraction of the signal reflected from the input port is sampled by the reverse directional coupler and is referred to as the reflected signal *A*. In the case of a two-port device or network under test, the signal that emerges from the output port is referred to as the transmitted signal *B*.

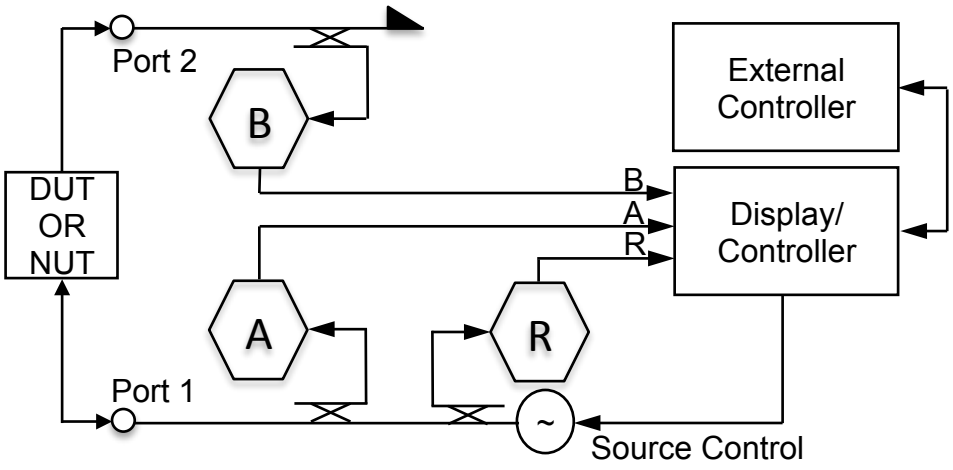


Figure 1 - Block diagram of a typical vector network analyzer.

In the most common VNA configuration, the signals *A* and *R* are applied to a two-port measurement receiver that returns both the magnitude ratio $|A/R|$ and the phase difference between *A* and *R*. The complex quantity A/R is the reflection coefficient Γ from which the input impedance of the input port can be determined by a well known bilinear transformation. Similarly, the signals *B* and *R* are applied to a two-port measurement receiver that returns the ratio $|B/R|$ and the phase difference between *B* and *R*. The complex quantity B/R is the transmission coefficient τ. Not only are such *ratioed* measurements physically meaningful, they effectively cancel any errors associated with fluctuation of the strength of the source signal as the frequency of the source is stepped across the span of interest [3], [12]. Applying the inverse Fourier transform to the complex frequency responses in both transmission and reflection yields corresponding impulse responses.

2.2.2 VNA Calibration and Error Correction

The responses measured by a VNA are usually corrupted by systematic errors including: 1) directivity and crosstalk errors associated with signal leakage, 2) source and load impedance mismatches associated with reflections and 3) frequency response errors associated with the measurement receivers. Multi-term error models capture these effects in the form of a error terms in a signal flow graph. The most common error model uses six terms to account for errors in the forward direction and six additional terms to account for the error terms when the input and output port are reversed. The process of determining the coefficients of the individual error terms is referred to as *calibration* [13].

Calibration of a VNA typically involves measuring the complex responses *A/R* and *B/R* of a set of one and two-port devices with precisely known responses. These devices are commonly referred to as *calibration standards*. The point at which the responses of the calibration standards are measured is referred to as the *calibration plane*. A typical set of calibration standards includes a short, open, and matched load and a through-line connection. Comparing the measured values of the standards at each frequency point with the actual values allows one to estimate the coefficients of the error terms. Once the error term coefficients are known, the model can be inverted and the actual value of the reflection or transmission coefficient of the device or network under test can be recovered from the measured values [14].

When only the transmission coefficient is of interest, as in the case of most wireless measurements performed using VNAs, only the *through-line response* needs to be measured during the calibration process. Dividing the measured complex transmission response, $H'(j\omega)$ (expressed in linear units), of an unknown network or device under test by the measured value of the complex transmission response, $H_t'(j\omega)$, of the through-line connection then multiplying the result by the true value of the complex transmission response of the through-line connection, $H_t(j\omega)$, will yield the actual complex transmission response of the unknown network or device under test, $H(j\omega)$ [15], i.e.,

$$H(j\omega) = H'(j\omega)\frac{H_t(j\omega)}{H_t'(j\omega)} \ .$$

During the late 1970's, it was recognized that useful insights concerning reflections and impedance discontinuities within a test fixture or measurement scenario could be gained by taking the inverse Fourier transform of the complex transmission response to yield the impulse response of the device or network under test. However, the process was normally performed offline using a standalone computer, not in real time on the VNA as the measurement data was collected.

During the early 1980's, engineers at Hewlett-Packard incorporated the capability to compute the inverse Fourier transform of a transmission response trace in real time (using a Chirp-Z transform to accommodate trace lengths that are not powers of 2) into the pioneering HP 8510 VNA. This allowed operators to view the impulse response of the network or device under test in real time for the first time. By the late 1980's, time-domain gating of the impulse response was used routinely to remove the effects of delayed replicas of the transmitted signal that arise due to reflections or echoes in the measurement setup. This typically involves eliminating elements of the impulse response that exceed a certain delay then Fourier transforming the result back into the frequency domain to yield the pristine result [16].

Random and drift errors vary over time and cannot be characterized or corrected by calibration. While some random and drift errors are due to low signal to noise levels or temperature-related effects, others arise from movement of cables and related mechanical issues. Ensuring adequate RF source levels, maintaining adequate temperature control, and using fixtures that minimize cable torsion and flexion are effective measures for controlling such errors. Multiple traces may be averaged to reduce the effect of random errors to an acceptable level but should only be regarded as a last step.

External interference is another type of unpredictable and therefore random error. The nature of this interference determines its impact on VNA-based channel measurements. For example, strong and sustained wideband interference will completely corrupt the measured channel response. Short bursts of wideband interference or any length of narrowband interference will only corrupt short portions of the channel frequency response. When the corrupted response is inverse Fourier transformed to yield the channel impulse response, the short bursts of interference in the frequency response will increase the overall noise floor in the time (delay) domain and reduce the dynamic range of the measurement.

When the interference occurs randomly and sporadically, some relief can be obtained by averaging the channel frequency response measured across many successive sweeps. If the interference is confined to a fixed portion of the response over successive sweeps, steps may be taken to either manually or automatically remove the offending portions then replace the missing values by interpolation. *However, techniques for avoiding or mitigating external interference that degrades VNA-based measurements have not been demonstrated or reported previously in the literature*.

2.2.3 Measurement Time and Efficiency

The performance metrics usually associated with VNAs include the maximum frequency span, the maximum number of frequency points, the noise floor (as a function of IF bandwidth), dynamic range, measurement accuracy, and so forth. Because the sweep will always take a finite time to complete, it is generally understood that only devices or network with responses that are static over a sweep, i.e., which present quasi-static responses, can be reliably characterized. However, the length of time required to conduct a measurement is also important when: 1) the measurements are automated and conducted in quick succession or 2) time-critical instrument state changes must be made in response to external triggers.

Sweep time is the most obvious delay that affects measurement time and efficiency. During a measurement at a particular frequency point, the VNA must wait long enough for the IF filter to fully respond to the applied signal. This wait time is inversely proportional to the IF filter bandwidth and is referred to as the *measurement dwell time*. Selecting a higher IF bandwidth will reduce the dwell time but raise the noise floor and decrease the dynamic range. Other considerations that affect sweep time include the complexity of the error correction model and the time required to execute the associated error correction software, the impact of band switching for wider frequency spans, and so forth [17]

Measurement automation involves exchange of commands and data between a controller and the instrument. GPIB and Ethernet are the two most common communication buses for external instrument control. Ethernet, while offering higher throughput, also incurs longer latency than GPIB which may be problematic in instrument control applications [18],[19]. Also, the multiple layers of software and protocol stacks that commands and data must traverse in either case introduce additional latencies that may not be acceptable when

instrument state changes and measurement actions must be made in response to external triggers in real time. High end VNAs usually provide external trigger inputs and outputs that allow certain functions, such as stepping from frequency point to point, to be performed under external control but with minimal software overhead.

2.3 Application of VNAs in Wireless Measurements

The first generation VNAs that were introduced during the 1960's and 70's were complex measurement systems that were composed of several large pieces of test and measurement equipment installed in one or more equipment racks. The second and third generation VNAs that were released during the early and late 1980's transformed VNAs into standalone instruments that were also suitable for use under field conditions.

Until the mid 1980's, VNAs were used almost exclusively to characterize the frequency response of devices such as cables, connectors, filters and amplifiers. Often such devices are completely contained within a shielded enclosure and therefore reasonably isolated from interfering signals in the outside world. By the late 1980's and continuing until the present, VNAs have replaced test setups based upon spectrum analyzers and remote tracking generators as the preferred instruments for use in systems for measuring the radar cross section of targets [20],[21], the radiation pattern of antennas [22],[23], the shielding effectiveness of enclosures [24] and the response of wireless channels [25],[26].

The principal advantages of VNAs in wireless measurement applications include their abilities to: 1) return response measurements with high dynamic range, high sensitivity and high resolution in both time and frequency, 2) return complex ratioed transmission responses that make calibration and error correction more accurate and 3) use time domain gating to remove delayed replicas of the transmitted signal that arise due to reflections or echoes in the measurement setup. Their principal disadvantages include: 1) the requirement for an RF cable connection between the receiver and transmitter, 2) the requirement that the channel be static over the duration of a measurement sweep and 3) the susceptibility of the receiver to external interference.

2.4 Alternatives to VNAs for Wideband Wireless Channel Measurements

There are two principal alternatives to VNAs for wideband characterization of wireless channels: 1) spectrum analyzers with remotely located tracking generators and 2) vector signal analyzers with remotely located vector signal generators.

2.4.1 Spectrum Analyzers with Remotely Located Tracking Generators

A swept-frequency spectrum analyzer equipped with a remotely located tracking generator is capable of returning wideband transmission response measurements over a frequency span of interest. As in the case of VNAs: 1) the measurements have high dynamic range, high sensitivity and high resolution in frequency, 2) the receiver is extremely susceptible to interference, and 3) the channel must be static over the duration of the measurement sweep. The duration of the sweep is proportional to the number of points and inversely proportional to the IF or resolution bandwidth. Although an RF link between the transmitter and receiver is not required, some method for synchronizing the start of the transmitter and receiver frequency sweeps is needed. Because a spectrum analyzer does not return phase response information, the options available for calibration, error correction and time domain processing are greatly reduced compared to a VNA.

2.4.2 Vector Signal Analyzers with Remotely Located Vector Signal Generators

A test set based upon a vector signal analyzer and a vector signal generator can overcome some of the limitations of the swept-frequency spectrum-analyzer-based scheme. Here, the vector signal generator is configured to emit a signal that occupies the frequency span of interest, e.g., 1) a single carrier signal that has been modulated by a pseudo random binary sequence with a specified chip rate or 2) multi-carrier signals similar to those used in OFDM-based signalling.

In the first case, correlating the received signal with a replica of the original transmitted signal will reveal the power delay profile. Variants include the sliding correlator channel sounder and the stepping correlator channel sounder. In the second case, the amplitude and phase of each carrier is compared to a replica of the transmitted signal to yield a coarsely

sampled estimate of the complex frequency response. Only relative phase response can be characterized, however. As a result, absolute delay measurements are not possible.

The principal advantages of these systems include their abilities to: 1) operate without a direct connection between the transmitter and receiver and 2) reject significant amounts of interference due to the relatively low cross-correlation (typically as low as -30 dB) between the original pseudorandom signal and most practical interfering signals. However, they deliver far less temporal resolution, dynamic range and sensitivity than VNA or spectrum analyzer-based instruments.

In the case of multi-carrier systems, the transmitted power is distributed between all of the carriers. Not only does this reduce the power available per carrier proportionately, but the resulting signal no longer has a constant envelope. The potentially high ratio of peak to average power generally requires that a fairly robust (and expensive) power amplifier that can handle the peak power levels that appear at the final stage of the transmitter.

2.5 Measurement & Modelling of Spectrum Occupancy

Spectrum occupancy is a field of study concerned with measuring and modelling of the observable behaviour of wireless devices transmitting signals over the radio frequency spectrum in real-world deployments of wireless infrastructure. The concepts of spectrum occupancy and a number of definitions date back to the earliest days of radio but were codified in the 1970s after large-scale measurement campaigns were conducted to characterize spectrum occupancy in land mobile radio bands in the VHF and UHF portions of the wireless spectrum. However, the best practices proposed and recommended during this time were limited by the technology of the time and the nature of the signals of interest: narrowband analog signals that cover wide areas and which accessed the channel under human control [27].

Regulatory bodies responsible for the management and regulation of the radio spectrum have been using spectrum occupancy measurements and models for a variety of purposes, such as gaining insight into the utilization of wireless spectrum, providing information and feedback to policy makers, and influencing allocation of licenses. In many instances, regulatory agencies set up spectrum-monitoring stations that are capable of recording spectrum occupancy measurement data for months or even years [28]. More recently,

Dynamic Spectrum Access (DSA) researchers have used measurement-based spectrum occupancy models to simulate the performance of their spectrum sensing techniques and spectrum access algorithms and protocols.

While the published spectrum occupancy studies by spectrum regulators tend to focus on wide-area land mobile radio bands, the DSA community's interest of frequency bands is much wider and even includes license-exempt short-range device bands, which are seldom studied by regulatory agencies. Measuring, modelling, and understanding how wireless devices occupy the radio spectrum will continue to be critical for making informed spectrum management decisions and intelligently accessing spectrum.

The hardware used to conduct spectrum occupancy measurements has significantly evolved over the past few decades and has increased the resolution and quantity of collected measurement data. Models have evolved from first order models that provide a general indication of spectrum usage to second order models that capture the temporal and spatial behaviour of spectrum occupancy.

There are three common types of signals that occupy spectrum in modern wireless environments. In this thesis, we refer to them as: 1) Continuous, 2) Long-burst, and 3) Short-burst. Continuous signals generally result from broadcasting applications, like television and radio, or monitoring applications such as those using closed circuit video. Long-burst signals generally result from human centric communications using voice or video and tend to last of the order of seconds or tens of seconds. Short-burst signals generally result from packet oriented digital transmissions and tend to last for hundreds of microseconds. Many modern spectrum occupancy studies have sought to characterize the behaviour of these types of signals [29],[30],[31].

2.6 Interference Avoidance and Mitigation

2.6.1 Wireless Measurements

As mentioned in Chapter 1, the practical strategies for avoiding interference in wireless channel measurements that are commonly used to ensure clear channels for wireless measurements are often impractical or ineffective. The simplest active scheme for avoiding interference to others is to provide the channel sounder with a spectrum-sensing receiver and adopting a carrier sense (listen before transmitting) protocol. Although no commercial VNA

of which we are aware has this capability, we believe that a VNA-based channel sounder that is used to measure transmission response only could, in principle, use one of its unused reference receivers as a spectrum-sensing receiver if the appropriate internal connections were made and its internal firmware was suitably modified.

More sophisticated techniques for either avoiding or mitigating interference in wireless channel measurements have been reported in recent years. Schemes based on spread spectrum probing signals are inherently resistant to interference and cause minimal interference to other spread spectrum and narrowband systems. However, such an approach doesn't offer unlimited performance; the degree of suppression rarely exceeds 30 dB.

In [32], the ITU-R acknowledged the value of swept-frequency sounding to provide real-time channel evaluation (RTCE) for adaptive HF communications but cautioned that equipping individual stations with this capability could reduce the overall capacity of the system. Instead they recommend that a centralized network of a limited number of FMCW channel sounders linked to centralized spectrum management networks be operated on an intermittent, low-power basis. The real-time spectrum management information so obtained should be shared with multiple users. In this manner, interference to other users in the band will be limited.

In [33], Bryant et al. present a method for implementing a high resolution channel sounder that causes only low levels of wideband interference and is therefore suitable for use in the bands currently used by global navigation satellite systems (GNSS) where high levels of interference caused by a probing signal would have safety of life implications. It determines the step response of the channel using a single period of the narrowband pseudorandom probing signal then takes the derivative to obtain the channel impulse response. Their scheme requires that: 1) the chip period t_{chip} exceeds the duration of the impulse response and 2) the channel being measured remains stationary over the period of the m-sequence.

In [34], Chen et al. propose a novel channel sounding technique that uses multicarrier modulation (MCM) to achieve frequency agility and time domain spreading to minimize interference to the primary user. They refer to their scheme as *multicarrier direct sequence swept time delay cross-correlation* or (MC-DS-STDCC). Their scheme is intended to

minimize the interference with incumbent licensed transmissions within the context of a dynamic spectrum access (DSA) network.

In [35], Gokalp et al. use Prony modeling, a high-resolution spectral estimation method, to extract the average power delay profiles (APDP) and Doppler spectrum from FMCW channel response data that has been corrupted by interference. The process is modeled by an infinite impulse response (IIR) filter with *P* poles and *M* zeroes. As described by the authors, the procedure has five steps: 1) determine the passband for prefiltering by observing the spectral content of a section of the sweep that is known to be free from interference, 2) specify the order of polynomials for a section of the sweep that is known to be corrupted by interference, 3) apply a sixteenth-order FIR prefilter, 4) obtain the ARMA coefficients by Prony's method, 5) obtain the frequency response of the filter. Steps 3-5 are repeated for every sweep prior to estimating the APDP. In the test cases considered, the authors were able to lower the noise floor of APDPs by 15-20 dB.

In [36], Sugizaki et al. describe a UWB spatio-temporal channel sounder that combines a 500-MHz-wide OFDM probing signal and a virtual array antenna based on an eight-element collinear subarray with a novel method for estimating the time-of-arrival and angle-of-arrival of the UWB OFDM signals. In addition to sounding the UWB channel of interest, their channel sounder is capable of estimating the spectrum and angle of arrival of an in-band (narrowband) interfering signal. To avoid interference, the channel sounder can create: 1) a spectrum hole within the OFDM probing signal by nulling the subcarriers that correspond to the interference and 2) a null in the antenna array pattern that lies in the direction of the interference.

In [37], Li et al. propose a novel methodology for visual assisted electronic channel sounding that uses non-uniform sampling in the frequency domain to reduce the level of interference caused by the channel sounder. It uses: 1) a computer vision system to construct three-dimensional models of the propagation environment, 2) ray tracing to predict the most likely propagation paths in the environment and construct a trial version of the channel impulse response (CIR), and 3) a statistical technique for selecting the fewest number of frequency samples required to verify and improve the estimated CIRs from the pool of frequencies not currently being used by incumbents.

2.6.2 Cognitive Radio

Cognitive radio is a concept based upon the notion that wireless devices would be more responsive to their users' needs and make more efficient use of both their own hardware and the wireless spectrum if they could sense their environment and reconfigure themselves appropriately. The original concept, as proposed by Mitola and Maguire [38] in 1999, foresaw software-based wireless devices that would learn about all aspects of their environment and users' behaviour, exchange information with other cognitive devices through a Radio Knowledge Representation Language (RKRL), and be able to adjust all aspects of their behaviour and performance through self-modification of their software including various aspects of their protocol stacks, modulation and coding schemes and RF frequency and power. Mitola believes that cognitive radio is a natural extension of the software defined radio concept that he pioneered several years previously [39],[40].

Within a fairly short time, researchers narrowed their focus to spectrum-sensing cognitive radio with the sole aim of making more effective use of the wireless spectrum. Measurement data collected over the previous decade in various locales have shown that many portions of the wireless spectrum are fully occupied at peak times while adjacent bands are mostly idle. However, the conventional regulatory schemes for frequency assignment do not permit users who are authorized to operate in one band to operate in another band simply because it is clear. Spectrum-sensing cognitive radio is based upon the notion that secondary users equipped with spectrum-sensing receivers can access wireless spectrum in such a way that primary users are neither aware of nor affected by their presence. Ultimately, deployment of cognitive radio systems will require significant changes to the regulatory environment [41].

There are three main cognitive radio paradigms: underlay, overlay and interweave. The *underlay paradigm* allows the secondary user to transmit simultaneously with the primary user provided that the interference experienced by the affected primary receiver does not exceed an acceptable limit. This implies that the secondary user can predict the relative strengths of the primary and secondary signals present at the primary receiver. The *overlay paradigm* also allows the secondary user to transmit simultaneously with the primary user and at any power level provided that the secondary user offsets interference experienced by the primary receiver by relaying the primary user's message. The *interweave paradigm* restricts

the secondary user to transmitting when the channel is idle and no primary user traffic is present. It tacitly assumes that the secondary transmitter has access to a spectrum occupancy data from a suitable spectrum-sensing receiver. The secondary transmitter's output power is practically limited by the range of the spectrum-sensing receiver. In practice, the gain and height of the receiving antenna above ground, the sensitivity of the receiver front end and the nature of the intervening propagation environment determine the range of the receiver [42].

2.7 Discussion

Interest in using VNAs to collect wideband transmission response measurements in open area environments for antenna measurement, wireless channel characterization and assessment of shielding effectiveness has increased markedly in recent years. VNAs provide stimulus-response measurements with lower noise floor, larger dynamic range and higher resolution in both time and frequency than most competing techniques. Techniques for: 1) correcting systematic errors associated with imperfections in the VNA hardware or test setup, 2) improving VNA measurement throughput during automated testing, 3) controlling drift and random errors associated with temperature effects or flexion and torsion of RF cables through both control of the physical environment and temporal averaging and 4) using time-domain gating to eliminate unwanted multipath, are well developed and routinely applied. However, techniques for avoiding or mitigating external interference have not been demonstrated previously in the literature.

Only a few previous studies have proposed techniques for collecting useful channel measurement data in the presence of interference or reducing the impact of channel measurement transmissions on wireless users. Previous studies of spectrum occupancy suggest that VNAs used to characterize wireless channels in open area environments will encounter two types of interference scenarios where the interference is intermittent and cognitive radio interweave techniques can be applied. In the first, interference is dominated by voice and video transmissions with durations much longer than the time that the VNA requires to measure channel response at a single frequency point, i.e., the measurement dwell time. We refer to this as *long-burst interference*. In the second, interference is dominated by data packet transmissions with duration much shorter than the VNA dwell time. We refer to this as *short-burst interference*.

Considerable effort has been devoted to development of spectrum sensing cognitive radio techniques that allow secondary users to access wireless spectrum in such a way that primary users are neither aware nor affected by their presence. This suggests that a *cognitive* or *interference-aware* VNA is a natural next step in the evolution of VNAs for wireless measurement applications. In the next two chapters, we consider the proposition that the reliability and accuracy of VNA-based wireless measurements performed in the presence of external short- and long-burst interference, respectively can be significantly improved by applying cognitive radio concepts where uncooperative, external wireless systems are cast as primary users and the VNA is cast as the secondary user.

Chapter 3

An Interference-Aware Vector Network Analyzer for Conducting Wireless Stimulus-Response Measurements in Land Mobile and Public Safety Bands

3.1 Introduction

Vector network analyzer (VNA) based measurement systems generally offer higher resolution and higher dynamic ranges than competing wireless measurement techniques and are often used by antenna designers, channel modelers and EMC engineers to characterize the response of antennas, wireless channels and shielded enclosures in open-area environments. Because VNAs are both extremely vulnerable to external interference and capable of disrupting communication between others, such measurements have traditionally been conducted in clear channels within the frequency band of interest or possibly in adjacent frequency bands if the primary band is not available. As clear channels become increasingly rare, test engineers have sometimes found it necessary to work with other users to develop informal protocols for sharing the channel. In other cases, they tolerate small amounts of interference and deal with it using manual techniques. Sometimes they arrange to conduct the measurements in an alternative location that suffers from less interference. While often helpful, such schemes are frequently impractical or ineffective and more effective approaches are required.

As described in more detail in the previous chapter, a variety of other techniques for ensuring that wireless channel measurements can coexist with other users have been reported in the literature. Several of the schemes focus on the need to avoid interference to primary users. In [32], the ITU-R recommend that a small number of FMCW channel sounders linked to centralized spectrum management networks be operated on an intermittent, low-power basis and used to obtain real-time spectrum management information for multiple users in order to limit the interference to regular communications users. In [33], Bryant et al. present a method for implementing a high resolution channel sounder that causes only low levels of wideband interference and is therefore suitable for use in the bands currently used by global

navigation satellite systems (GNSS) where high levels of interference caused by a probing signal would have safety of life implications. In [34], Chen et al. propose a novel channel sounding technique that uses multicarrier modulation (MCM) to achieve frequency agility and time domain spreading to minimize interference to the primary user.

Other schemes focus on techniques for obtaining high quality measurement data in interference environments. In [35], Gokalp et al. use Prony modeling, a high-resolution spectral estimation method, to extract the average power delay profiles (APDP) and Doppler spectrum from FMCW channel response data that has been corrupted by interference. In [36], Sugizaki et al. describe a UWB spatio-temporal channel sounder can create: 1) a spectrum hole within the OFDM probing signal by nulling the subcarriers that correspond to the interference and 2) a null in the antenna array pattern that points in the direction of the interference. In [37], Li et al. propose a novel methodology for visual assisted electronic channel sounding that uses non-uniform sampling in the frequency domain to reduce the level of interference caused by the channel sounder. However, to the best of our knowledge, no previous efforts to develop interference mitigation techniques that can be applied to commercial-off-the-shelf (COTS) VNAs has been reported in the literature. This is surprising considering that many of the working engineers with whom we have spoken have assured us that such a capability would be of immediate and considerable value to several sectors of the wireless industry.

Here, we show that the reliability and accuracy of VNA-based wireless measurements performed in the presence of external interference can be significantly improved by applying cognitive radio concepts where uncooperative, external wireless systems are cast as primary users and the VNA is cast as the secondary user. In particular, we devise and demonstrate hardware and software that can augment commercial-off-the-shelf VNAs and make them more resistance to such interference. Scenarios of interest divide into two types. In this chapter, we focus on cases where the interference is dominated by voice and video transmissions with duration much longer than the time that the VNA requires to measure a single frequency point, i.e., the measurement dwell time. In the next chapter, we focus on cases where the interference is dominated by data packet transmissions with duration shorter than the VNA dwell time.

The remainder of this chapter develops as follows: In Section 3.2, we present our system-level design of an interference-aware VNA suitable for use in long-burst interference environments. In Section 3.3, we describe our implementation of such an interference-aware VNA based upon external hardware and software add-ons. In Section 3.4, we demonstrate the performance of the unit and identify any shortcomings. In Section 3.5, we conclude that the scheme is eminently practical but that relatively minor enhancements to the firmware and internal connections found in high end commercial VNAs would greatly simplify implementation and eliminate the need for external instruments and hardware.

3.2 Concept

We began our efforts to develop an interference-aware VNA begin with the observation that a VNA characterizes a channel by applying a tone of given frequency to the channel input and comparing the amplitude and phase of the version that appears at the channel output to the original signal. The measurement is repeated at successive points across a specified frequency span until the complex frequency response of the transmission channel is completely characterized. However, when wireless measurements are conducted in open areas, the measured frequency response is susceptible to corruption by interference from other users. As noted in Chapter 1, there are three main cognitive radio paradigms: underlay, overlay and interweave. Here, we adopt the interweave paradigm.

A block diagram that presents a conceptual design of an interference-aware VNA is shown in Figure 2. The portions in blue indicate the components and connections that have been added to a conventional VNA to realize an interference-aware VNA. Our first task is to provide the VNA with a spectrum-sensing receiver. Since most wireless measurements in open areas only concern the forward or transmission path, the measurement and reference receivers normally used on the reverse or reflected path are potentially available. If the outputs from those receivers cannot be accessed quickly enough because direct connections aren't available and software access incurs excessive latencies, an external spectrum-sensing receiver must be supplied.

Using a spectrum-sensing receiver, the VNA can detect interference before (or after) each measurement and inhibit (or reject) the measurement if interference is, in fact, detected. When the primary users transmit voice and video with durations much longer than the VNA

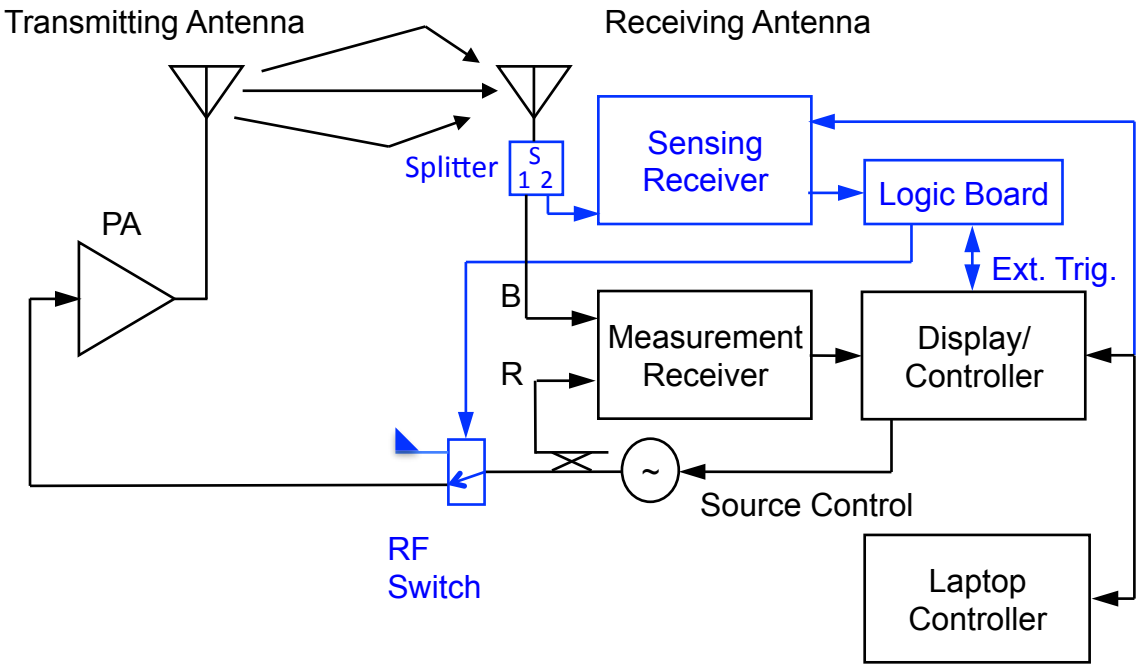


Figure 2 - Conceptual hardware architecture diagram of an interference-aware VNA

measurement dwell time, such a scheme is virtually guaranteed to yield channel measurements that are pristine. Overlap between the primary users and VNA can only occur when a primary user begins transmitting while the VNA is measuring a frequency point. Given that the measurement dwell time is of the order of a millisecond, the resulting interference to the primary user will be imperceptible. It is therefore reasonable to expect that the interference-aware VNA will easily achieve its goals for neither influencing nor being influenced by primary users' transmissions.

As the frequency and duration of primary user transmissions increase, the measurements will be inhibited or rejected more often and the length of time needed to complete the measurements will increase. The main problems are to minimize both the measurement collection time and the cost and complexity of the implementation. In cases where certain frequency points are occupied by transmissions of unusual duration, it may be appropriate to omit those points and use interpolation to fill in. In so doing, we are trading off measurement accuracy for measurement speed.

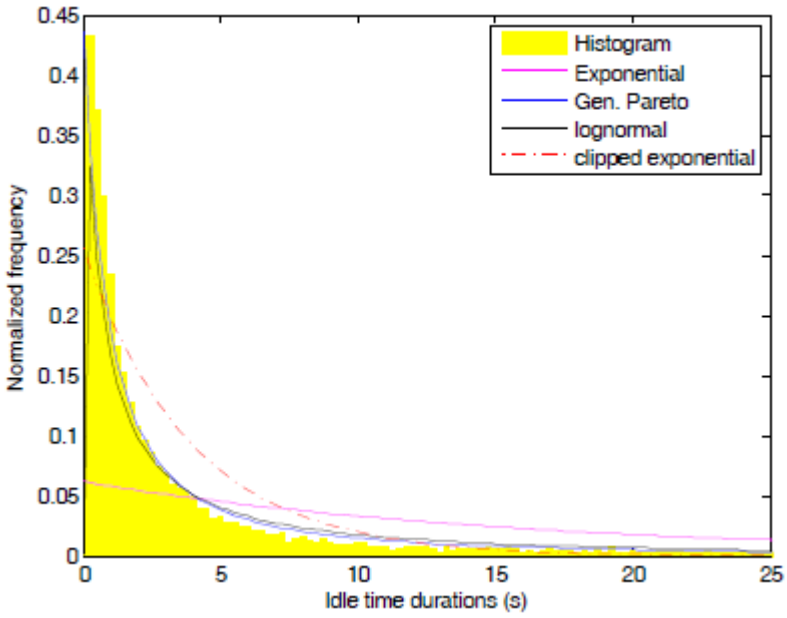
3.2.1 Classification of Primary User Transmissions

In the frequency domain, primary user transmissions may be classified as: 1) *broadband* if they occupy the entire frequency span of interest, 2) *narrowband* if they occupy only a portion of the frequency span of interest and 3) *point-like* if they occupy a bandwidth which is less than the interval between successive frequency points. In the time domain, primary user transmissions divide into three types depending on whether they occupy the spectrum: 1) continuously, 2) in long bursts of length $\Delta t_i > \Delta t$, and 3) in short bursts of length $\Delta t_i < \Delta t$, where Δt is the measurement dwell time.

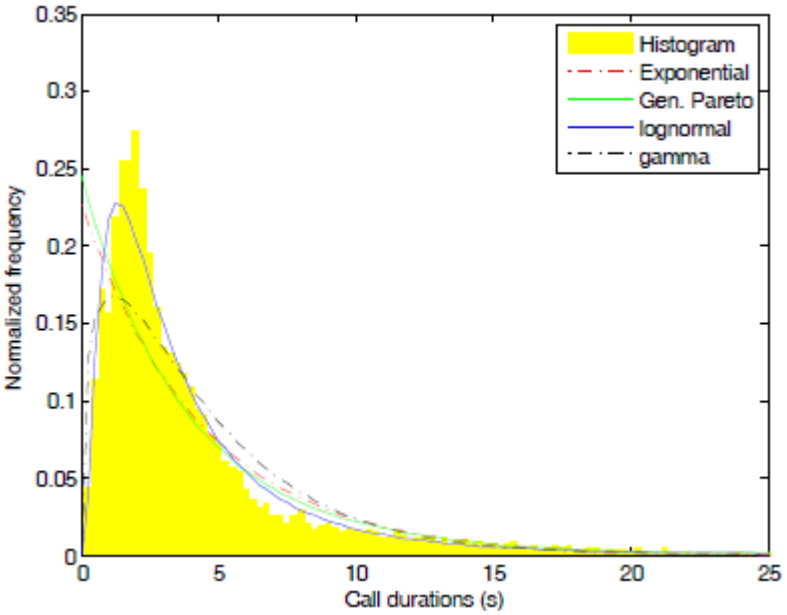
For our purposes, a primary user transmission is effectively continuous if, due to its length, it would be unreasonable to wait for the transmission to cease before completing a measurement. Such transmissions are generally the result of broadcast or monitoring undertakings. A long-burst transmission is short enough (up to tens of seconds) that it is reasonable to wait for it to cease before completing a measurement but is longer than the measurement dwell time. Such transmissions are generally the result of human-centric voice or video transmissions. Many researchers have presented statistical descriptions of the frequency and duration of such transmissions [43], [44], [45]. Examples are given in Figure 3. By contrast, a short-burst transmission is shorter than the measurement dwell time. Such transmissions are generally associated with packet-oriented wireless data transmissions. For wireless standards such as Wi-Fi, Bluetooth and ZigBee, transmission durations are very short and may last for only 100s of microseconds. This scenario will be considered in Chapter Four.

3.2.2 Modes of Operation

We propose three methods by which an interference-aware VNA could function. The first, which we call *stepping mode,* represents a relatively simple modification to conventional VNA operation but incurs substantial sweep completion times in the face of heavy interference. The second, which we call *step and skip mode*, allows certain frequency points to be skipped if the wait for them to become clear exceeds a certain threshold. The third, which we call *random sampling mode*, allows the frequency response at different points to be



(a)



(b)

Figure 3 – Histogram of a) idle times and b) hold times with model fits (week long data) from [43]

collected opportunistically and thereby reduce waiting times but requires a much more flexible VNA. It has the potential to operate much more efficiently in a heavy interference environment, however.

In principle, modern VNAs are sufficiently flexible and programmable that any of these operating modes could be realized using an external controller. In practice, however, instrument commands delivered via GPIB, USB or Ethernet must traverse a fairly complex software stack and the delays between a command being issued and actually occurring are significant. In practice, the external controller requires access to signals that are as close to the hardware as possible.

3.2.2.1 Stepping Mode

Stepping mode represents only a minor departure from the conventional mode of operation of VNAs. Here, the frequency span, IF bandwidth and number of points for the VNA and the spectrum-sensing receiver are set to identical values on both instruments. At a given moment, the output from the spectrum-sensing receiver is compared to a threshold value. The output of the comparator (Occupied) indicates whether the channel is occupied or not. Both are configured to operate in a point sweep mode in which the instrument steps from one frequency point to the next in response to an external trigger (Trigger In) from an external controller. If a trigger occurs while the measurement is in progress, the external trigger is ignored. Once the measurement is complete, each instrument generates a trigger (Trigger Out) that indicates to the external controller that it is ready to move to the next frequency point. The output level from the spectrum-sensing receiver is compared to a threshold value to determine whether interference is present after the measurement at each frequency point is complete.

A frequency sweep is measured as follows. Let the spectrum-sensing receiver and VNA both be initialized to the same frequency point. If the external controller senses that the channel at that frequency point is occupied, i.e., Occupied is high, operation of the VNA is halted and no measurement is undertaken. Once the frequency point is clear, the external controller applies a signal to Trigger In that causes the VNA to measure the response at that point. Immediately upon completion of the measurement, the VNA generates a signal via Trigger Out that causes the spectrum-sensing receiver to once again determine whether the channel is now occupied. If the channel is clear, both the spectrum-sensing receiver and the VNA advance to the next frequency point and the process is repeated. If the channel is occupied, it is assumed that the channel measurement was corrupted and the measurement is

retaken without advancing to the next frequency point. The process is repeated until the frequency sweep is complete.

Stepping mode makes use of capabilities and signals that are already available in most high-end VNAs. Because primary user transmissions are always much longer than VNA dwell times, an interference-aware VNA that operates in sequential mode will always return a pristine channel frequency response even in the presence of interference. However, the time required to complete the sweep will increase greatly as the number of interfering transmissions and their duration increases.

3.2.2.2 Step and Skip Mode

Step and skip mode is very similar to stepping mode but allows a given frequency point to be skipped if the wait for it to become clear exceeds a certain threshold. If the number of points that are skipped falls below a given threshold, the missing points are estimated through interpolation. If the number exceeds that threshold, the sweep is retaken and merged with results obtained during previous sweeps. This requires a more sophisticated external controller than stepping mode requires, but is ultimately more practical in environments in which a few long or very long transmissions could otherwise impractically delay the sweep.

3.2.2.3 Random Sampling Mode

Random sampling mode represents a significant departure from the conventional mode of operation of VNAs. It assumes that the VNA is capable of switching to any frequency point within the frequency span of interest on command. In this mode of operation, a frequency sweep is measured as follows. Let the spectrum-sensing receiver and VNA both be initialized to the same frequency point. If the external controller senses that the channel at that frequency point is occupied, i.e., Occupied is high, operation of the VNA is halted and no measurement is undertaken. Instead, the external controller advances the VNA to the next clear frequency point detected by the spectrum-sensing receiver and the measurement process continues. The process is repeated until the end of the span is reached at which time the external controller causes the VNA to advance to the closest frequency point that is both clear and required to complete the frequency response. If the number of points that are skipped falls below a given

threshold, the missing points are estimated through interpolation. If the number exceeds that threshold, the sweep is retaken and merged with results obtained during previous sweeps.

Random sampling mode requires a more sophisticated external controller than stepping mode or step and skip mode require, and requires greater flexibility in moving from point to point than most current VNAs currently offer. In the end, it likely offers the best performance and may be quite practical if implemented using internal VNA hardware rather than external add-ons.

3.2.3 Relative Performance

When the duration of the primary users' transmissions is much, much greater than that of the VNA measurement dwell time, all three modes are capable of delivering pristine channel response measurements while having negligible impact on the primary users. However, the total measurement time will increase as primary user occupancy increases and the VNA is forced into an idle state for increasing lengths of time. The simplest algorithm, stepping mode, will be idled most often and sometimes excessively and therefore take longest. By timing out after a certain wait time, step and skip mode will avoid excessive delays and take less time to complete a sweep. As long as the number of missing points falls below a specified threshold, they can be filled in by interpolation albeit at the cost of some accuracy. The most complex algorithm, random sampling mode, will look for other frequency points to measure if the current point is occupied. It will be idled least often and therefore complete the measurement in the shortest time.

A more complete understanding of the performance trade-offs associated with each operating mode as the level of primary user traffic increases can best be appreciated by conducting simulation-based studies. Such simulations will be based upon knowledge and understanding of the frequency and duration of primary user transmissions and the limitations of practical implementations. We explore the latter in the next section.

3.3 Proof of Concept Implementation

This proof of concept implementation demonstrates that the interference-aware VNA concepts shared in the previous section can be implemented today by augmenting a COTS VNA with external hardware. This implementation is not a final product and commercial products should be designed from the ground up with proper integration and reduced reliance

on external components. The architecture, hardware, and software of the implementation are designed for operation in the presence of long-burst interference and discussed in this section.

Architecture & Block Diagram. A diagram of the implementation can be found in Figure 4 and a photo of it can be seen in Figure 5. An Agilent E8362C PNA series VNA is selected as the core of the implementation and everything else is based around it. An HP 8594E Spectrum Analyzer (SA) is used as a dedicated spectrum sensor for continuous detection of primary user transmissions. A Narda S123D PIN-diode switch is used for the RF switch to control VNA transmissions. All of these components interface to the logic board, which consists of an Arduino Uno board and series of integrated circuits where decisions on when to take measurements are made. A Dell Vostro 1500 laptop running Matlab was used as the laptop controller to configure and coordinate the hardware.

3.3.1 Hardware

VNA Configuration. The VNA is configured to perform wireless channel measurements with a few differences from typical configurations. Port 1 of the VNA is connected to a transmitting sleeve dipole antenna through a Narda S123D PIN-diode RF switch using RF coaxial cable. Port 2 of the VNA is connected to a receiving sleeve dipole antenna through a splitter that also feeds the received signal into the SA RF input using RF coaxial cable. The VNA is setup to perform a linear frequency sweep S21 measurement between the start frequency and stop frequency, which is the most traditional VNA mode of operation. However, the VNA's Point Trigger mode is used so that only one measurement point is taken for each trigger that is received instead of the entire sweep. External triggering is also used with the external trigger output enabled, so that the device triggering the VNA knows when the measurement is complete. An IFBW setting of 1 kHz is selected as a reasonable compromise between measurement receiver sensitivity and VNA measurement dwell time. It is important to set the VNA's number of sweep-points to 401 because the SA has a fixed number of 401 points in a sweep.

Spectrum Analyzer Configuration. The HP 8594E spectrum analyzer is configured to be a dedicated spectrum sensor for detecting primary user transmissions that may cause harm to VNA measurement results. The RF input of the SA is connected to a receiving sleeve dipole antenna through a splitter that also provides the signal to the VNA measurement receiver. The

start frequency and stop frequency are selected to match those of the VNA. A resolution bandwidth (RBW) value larger than the VNA IFBW is chosen (30 kHz) to accommodate for frequency alignment error in the analog sweep control. The amplitude reference level and scale of the display are important because they correspond to the performance of the video output and comparator threshold level. The noise floor location on the display should be far enough below the threshold level so that noise does not frequently trigger false alarms. The amplitude scale determines the interfering signal amplitude level that corresponds with a 1 volt increase on the video output, which contributes to the SNR needed to cross the comparator threshold. Internal attenuation is set to 0 dB to maximize the sensitivity of the SA spectrum sensor. External triggering is also used to allow the Arduino to start a sweep.

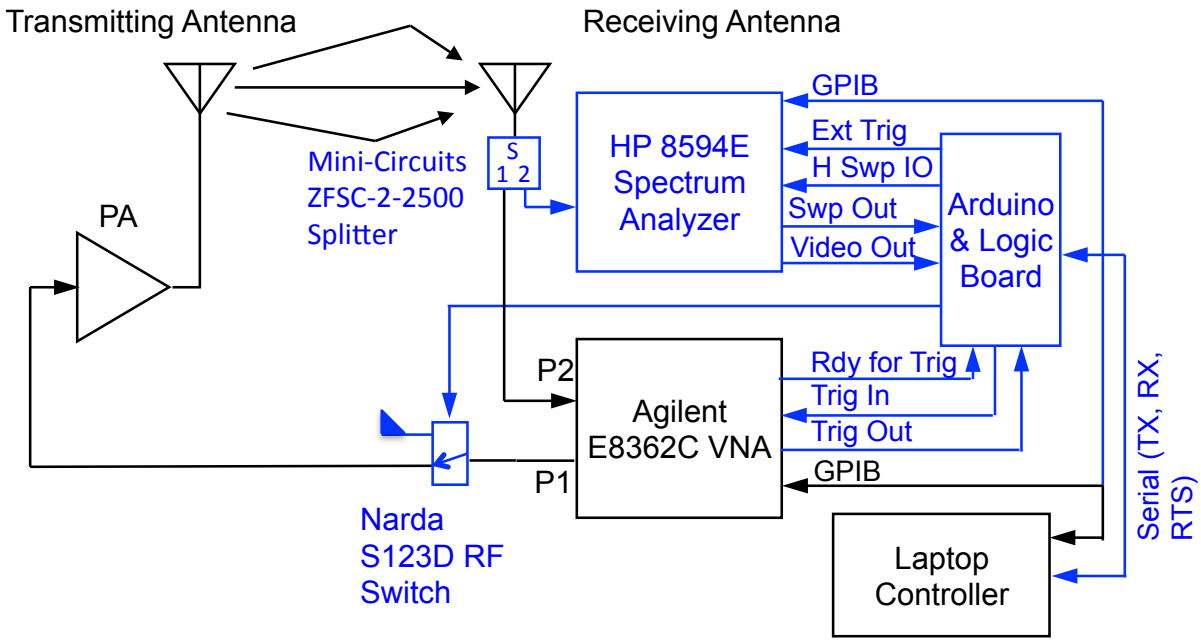


Figure 4 - Hardware block diagram of implemented long-burst interference-aware VNA

Arduino and Logic Board Configuration. The Arduino and Logic board, which comprise the decision-making element of the implementation, interface to nearly every other component of the implementation. A wiring diagram of the Arduino and Logic Board can be seen in Figure 6. It has four connections to the spectrum analyzer, three connections to the VNA, one connection to the RF switch, and one connection to the laptop. Through these various interfaces, the Arduino and logic board fulfill 3 roles: 1) Synchronize the sweeps of

the VNA and SA, 2) Inhibit VNA measurements while interference is present, and 3) Detect and log occurrences of interference.

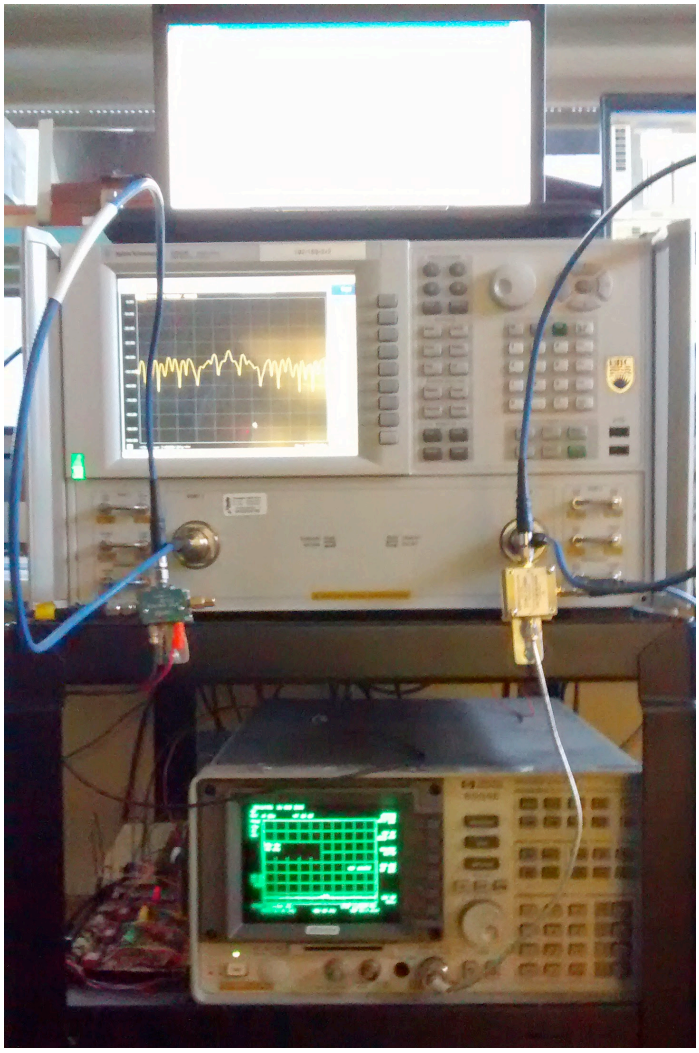


Figure 5 - Photo of implemented long-burst interference-aware VNA

The Arduino board facilitates a synchronized sweep between the VNA and SA by acting as a man in the middle man of two different sweep control techniques. The Agilent E8362C PNA is capable of performing a stepped sweep with other instruments using the external Trigger In and Trigger Out connectors to move across the sweep one points at a time together. An event on the Trigger In connector starts a VNA measurement and an event on the Trigger Out connector is sent once the VNA measurement is complete. However, the HP 8594E is an older analog spectrum analyzer without a stepped sweep feature, but still allows external

control of its sweep via the External Trigger, Sweep Out, and High Sweep Input Output connectors.

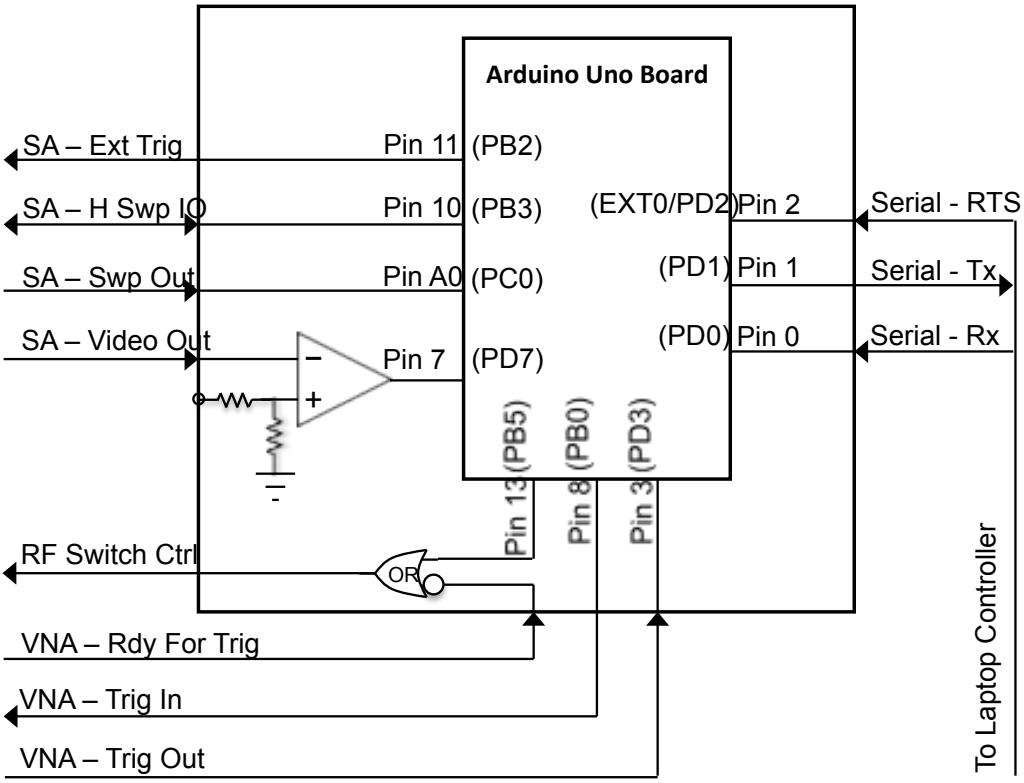


Figure 6 - Input/Output connections to/from the Arduino and Logic board

The External Trigger connector starts a sweep when an event is received, the Sweep Output indicates the progress of the sweep using a ramp generator between 0 and 10 Volts, and the High Sweep Input Output stops and starts the sweep when pulled low and high. A diagram of the microcontroller signaling required to perform a synchronized sweep between these two instruments can be seen in Figure 7. Synchronizing the sweeps of the VNA and SA is crucial for detecting interference at the current measurement point, and any significant deviation would compromise the entire implementation.

Medium access by the VNA transmitter is controlled by the Arduino and Logic board that controls both the RF switch and VNA measurement triggers. A PIN diode switch is used as the RF switch because it is capable of switching states in a number of nanoseconds, whereas mechanical switches change states in a number of microseconds and can be too slow compared to measurement times. The Video Output from the spectrum analyzer and the

Ready For Trigger signal from the VNA are the inputs that determine the RF switch state and the VNA Trigger In line. The Video Output of the HP 8594E outputs a voltage from 0 to 10

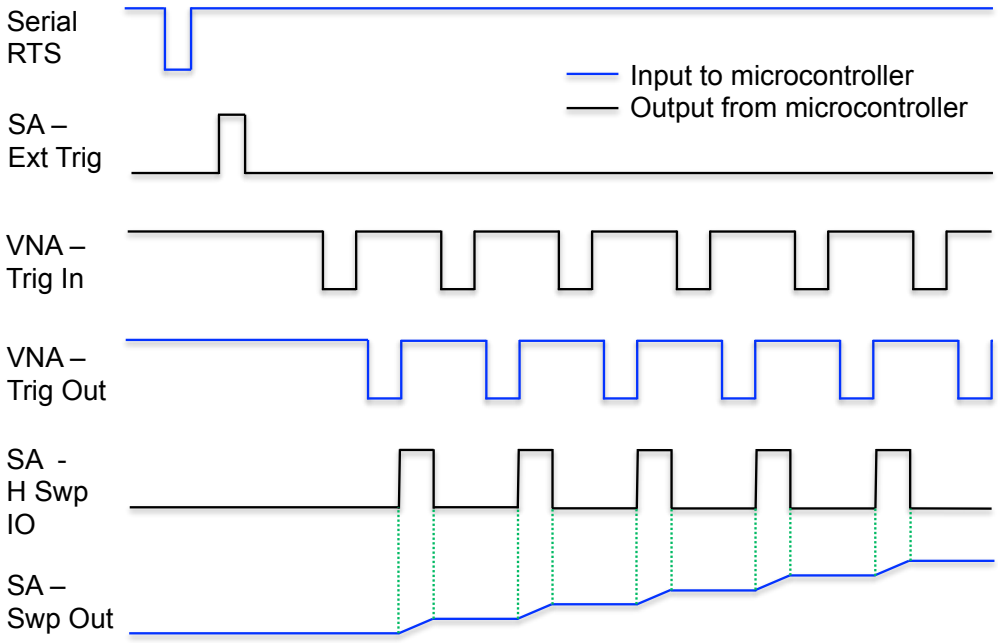


Figure 7 - Signal diagram of Arduino input/output lines for sweep synchronization

volts that corresponds to the amplitude level of the signal on the units display and serves as a low-latency energy detector.

A comparator is used to determine when the amplitude of the Video Output line exceeds a threshold, and the digital output of the comparator indicates whether the spectrum is considered occupied by interference or clear for transmission. The VNA's Ready For Trigger signal goes low to indicate it is waiting to receive a trigger for the next measurement and goes high when the VNA is taking a measurement. The Arduino queries the state of the comparator output before sending the VNA a trigger, and will only send the trigger once either 1) the comparator output is low or 2) a timeout occurs while waiting for the comparator output to go low. The Arduino allows an inverted Ready For Trigger Signal to control the switch state when sending a trigger in the first instance, and forces the switch to remain open and withhold the VNA transmission when sending a trigger in the second instance.

Immediately following each VNA measurement, the Arduino and Logic board detects if primary user signals are occupying the spectrum. The Arduino queries the state of the

comparator output and determines the VNA measurement to be clean or corrupt if the comparator output is low or high, respectively. The Arduino keeps an array of corrupt data points and sends the array to the laptop controller when queried after the measurement sweep. This corrupt data array is used to identify corrupt measurement data at the receiver, so the data points can be re-collected or omitted from the data set.

3.3.2 Software

Microcontroller Software. The software for the microcontroller on the Arduino board can be found in Appendix A. The software was written in the C programming language and compiled within the Arduino IDE. The microcontroller is used to synchronize the sweep of the SA with the VNA as the VNA steps through each point of the sweep. The SA is not capable of directly interfacing to the VNA Trig In and Trig out lines. The microcontroller is needed to move the SA sweep to the next point where the VNA is going to take a measurement before a trigger is sent to the VNA. The microcontroller also waits for interference to disappear before triggering a VNA measurement, as well as check the interference state after the measurement to flag interference occurrences. The Microcontroller software is interrupt driven by three events: 1) receiving a Start Sweep signal from the Computer serial port RTS line, 2) receiving a Move to next point signal from VNA Trigger Out, and 3) receiving a request for the corrupt-data-index from the computer serial port.

Instrument Control. The computer controller runs a MATLAB script that facilitates the whole measurement process. The MATLAB program begins by initializing the instrument state of both the VNA and SA by sending SCPI commands over the GPIB bus. GPIB is used because; 1) it is the only option for the SA, and 2) GPIB is faster than LAN for small data payloads because of its lower latency. After the instruments are initialized, the measurement is started and the computer waits for the VNA measurements to finish the sweep. The measurement data is read from the VNA and the corrupt data array is read from the Arduino microcontroller before processing begins.

Data Processing. MATLAB is used to perform data processing to the VNA measurement data once the computer controller has received the VNA measurement data and the corrupt data vector from the Arduino board. The corrupt data vector identifies all of the measurement points where either interference was measured immediately following the measurement point

or a timeout occurred from waiting for interference to disappear. The flagged data points in the corrupt data vector can be removed from the VNA measurement data and replaced by using techniques such as interpolation to reduce the impact of the missing measurement data. The CIR is generated by applying a Kaiser window with a beta of 7 to the CFR data and performing an inverse Fourier transform on the data. A beta value of 7 for the Kaiser window is chosen to suppress side-lobes levels for better dynamic range.

3.4 Results

In this section, a series of tests are performed on the described interference-aware VNA implementation to characterize its performance and the factors that impact performance. The performance of the proof-of-concept implementation was assessed by a series of tests. The test results demonstrate the interference-aware VNA's ability to collect accurate measurements while operating in the presence of long-burst interference, where traditional VNA measurement techniques cannot operate reliably. The additional time required to conduct the measurements in an interference-aware manner are quantified and further tests are performed to characterize the key contributing sources, VNA dwell time and instrument control communications overhead. Tests to assess the impact of the interference-aware VNA on long-burst interference producing primary users are discussed.

3.4.1 Measurement of Dwell Time

Description of the Test Setup. The test setup used to measure VNA dwell times is the same as is described in Section 3.3 and shown in Figure 4, except an Agilent Infiniium DSO7034B Oscilloscope is used to probe the Ready For Trigger signal output from the E8362C VNA Auxiliary IO Port. The Ready for Trigger signal is driven low when the VNA is ready to accept a trigger for a measurement, and goes high when the VNA is taking a measurement and when the sweep is complete. The duration of time that the Ready For Trigger signal remained high between low states of sequential measurements was measured as the VNA measurement time, which includes the dwell time, setup time, and processing time of the instrument. Oscilloscope markers were placed on the rising and falling edge of the high state and the measured delta between the two oscilloscope markers was noted.

Description of the Results. Measurements of the Ready For Trigger signal durations were conducted for IFBW values from 50 Hz to 40 kHz to compare the conventional practice of

approximating the VNA dwell time as 1/IFBW with actual VNA measurement times. The actual VNA measurement time includes factors in addition to the dwell time, such as setup time, data processing time, error correction and other contributing sources. Accounting for all of the various factors when predicting measurement time can be inconvenient, which is why the simple estimate of IFBW filter charge time, 1/IFBW, is the most commonly used predictor. The relationship between the calculated dwell time and the VNA measurement time are compared in Figure 8. This plot reveals that the calculation, dwell time = 1/IFBW, is a good approximation of VNA measurement time when the IFBW setting is from 1Hz-1kHz, but is not very accurate when set above 1 kHz. This information should be considered by interference-aware VNA operators when determining the IFBW setting for their measurements because the deviation between the calculated and measured values may come as a surprise.

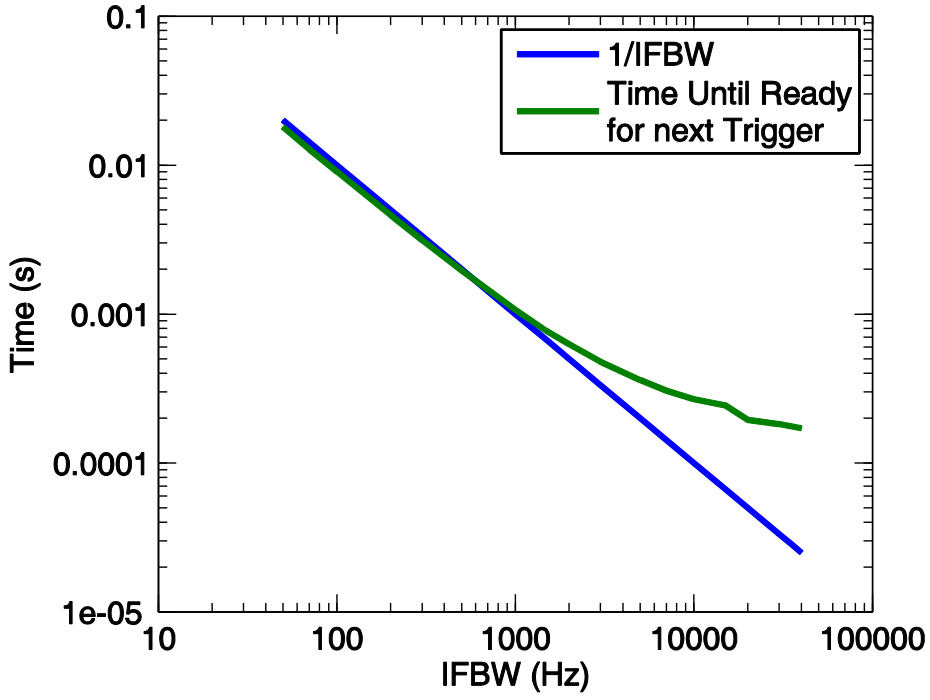


Figure 8 - Comparison of predicted VNA dwell time to VNA measurement time

3.4.2 Measurement of Communications Overhead

Description of the Test Setup. The test setup used to measure the communications overhead associated with instrument control buses is the same as is described in Figure 4,

except 3 different instrument control adapters were used to interface to the VNA: 1) LAN, 2) USB-GPIB, and 3) PCI-GPIB. Seven different sets of commands were used to test the instrument control adapters and each test consisted of sending a unique command or query that generated different amounts of data on the instrument control bus. The test commands were sent from MATLAB and the 'tic toc' tool was used to measure the duration of the tests. The seven test commands used were: 1) FREQ:CENT, 2) CALC:FORM:REAL, 3) *OPC? and response, 4) SENS:SWE:MODE? and response, 5) CALC:DATA? FDATA with 54 byte response, 6) CALC:DATA? FDATA with 214 byte response, and 7) CALC:DATA? FDATA with a 414-byte response. For each test, 1 instance, 10 instances, 100 instances, and 1000 instances of the test command were sent and cumulative time was recorded.

Description of the Results. A table of the communication overhead measurement results can be seen in Table 1. The fastest instrument control adapter across the seven test commands is the PCI-GPIB card, the second fastest was the USB-GPIB adapter, and the LAN adapter was the slowest in most cases. For sending commands and receiving data with small data payloads, latency plays a larger role in contributing to instrument control overhead than bandwidth does. The measured results are consistent with the results provided by National Instruments in [18] and [19]. Selecting the fastest instrument control bus and adapter is one way to reduce the measurement time. However, integrating the interference-aware VNA concept into the VNA firmware would be the ideal solution because it would completely eliminate the instrument control overhead times experienced over external buses.

Table 1 - External instrument control bus communication overhead

MEASURED VALUES	Adapter	T_1 com (s)	T_10 com (s)	T_100 com (s)	T_1000 com (s)
FREQ:CENT	PCI-GPIB	3.72E-3	8.67E-3	44.55E-3	294.25E-3
	USB-GPIB		62.80E-3	182.60E-3	1.61E+0
	LAN	2.63E-3	6.00E-3	31.20E-3	285.30E-3
CALC:FORM:REAL	PCI-GPIB	4.89E-3	8.56E-3	36.13E-3	243.75E-3
	USB-GPIB	7.24E-3	33.75E-3	173.00E-3	1.54E+0
	LAN	5.02E-3	7.48E-3	27.80E-3	230.00E-3

*OPC? And Result	PCI-GPIB	4.46E-3	17.03E-3	118.75E-3	1.17E+0
	USB-GPIB	9.70E-3	62.38E-3	470.00E-3	4.56E+0
	LAN	33.20E-3	174.20E-3	1.60E+0	15.78E+0
SENS:SWE:MODE?	PCI-GPIB	4.60E-3	18.48E-3	123.50E-3	1.27E+0
	USB-GPIB				
	LAN	29.05E-3	94.88E-3	439.25E-3	4.04E+0
CALC:DATA? FDATA (54 bytes/10 time points)	PCI-GPIB	9.58E-3	39.75E-3	259.00E-3	2.47E+0
	USB-GPIB	23.00E-3	133.20E-3	1.10E+0	11.88E+0
	LAN	31.00E-3	170.83E-3	1.61E+0	15.73E+0
CALC:DATA? FDATA (214 bytes/50 time points)	PCI-GPIB	9.72E-3	42.73E-3	306.00E-3	2.91E+0
	USB-GPIB	24.40E-3	126.00E-3	1.11E+0	11.07E+0
	LAN	24.40E-3	171.60E-3	1.53E+0	15.56E+0
CALC:DATA? FDATA (414 bytes/100 time points)	PCI-GPIB	9.66E-3	50.00E-3	351.00E-3	3.38E+0
	USB-GPIB	24.67E-3	145.40E-3	1.22E+0	11.88E+0
	LAN	32.00E-3	169.20E-3	1.57E+0	15.63E+0

3.4.3 Measurement Performance in the Presence of Interference

Description of the SR5500 Chanel Emulator. A block diagram of the test setup that was used to evaluate the performance of the proof-of-concept implementation of the interference-aware VNA is shown in Figure 9. A photograph of the test setup is shown in Figure 10. The Spirent SR 5500 wireless channel emulator was used: 1) to emulate both the fading and dispersive channel being measured by the VNA (Channel 1) and 2) to introduce various degrees of path loss and shadow fading into the simulated interference (Channel 2). The Sprint SR5500's Dynamic Environment Emulation (DEE) feature was used to vary the strength of the interfering signal according to a predefined script. The distorted replica of the VNA RF test signal and the interfering signal were combined and returned to the VNA receiver input. Performing such tests on a test bench is more cost effective and convenient than field measurement for particular types of tests because there is no need to transport

measurement equipment to the field and all lab resources are readily available during testing. A standard GSM channel model for typical urban environments was used for both of the wireless channels.

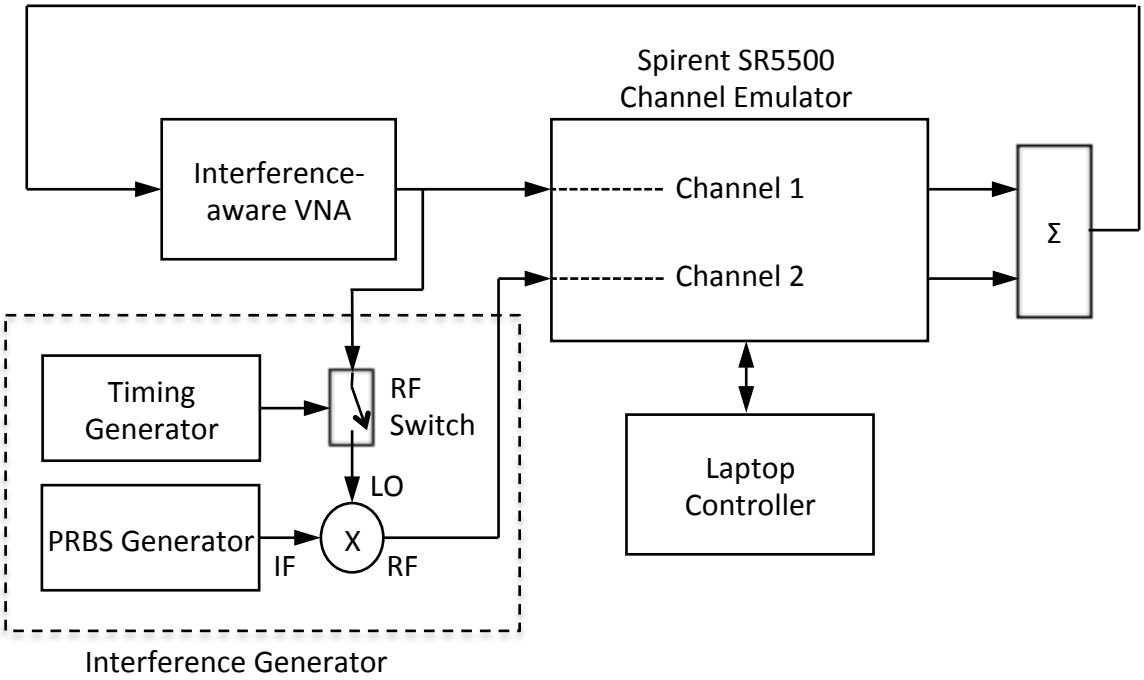


Figure 9 - Performance Test Setup Diagram

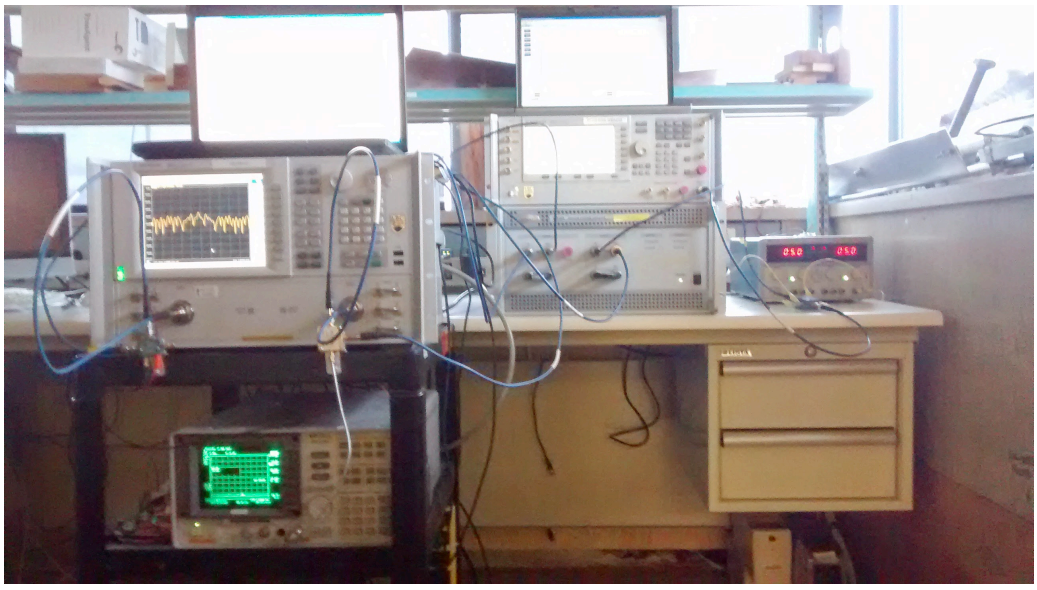


Figure 10 - Photo of Performance Test Setup

*Description of the Interference & PRBS Generators***.** The interference generator comprised: 1) a PRBS (pseudo random binary sequence) generator that produced an interfering signal that occupied a bandwidth typical of a land mobile radio transmitter and 2) a timing generator that turned the interference on and off so that the channel occupancy and idle times followed a predefined distribution. The output of the PRBS generator was upconverted to the current frequency point being measured by the VNA by a mixer that was driven by a sample of the VNA RF test signal. The timing generator controls the on-off pulsing of the interference signal by way of a python script running on a Raspberry Pi Model B single board computer. The python script toggles a digital GPIO pin that controls the Mini-Circuits ZMSW-1211 PIN-diode RF switch according to an appropriate statistical distribution that accurately models the idle and busy durations of the desired interference. The lognormal distribution models used to approximate idle and busy duration histograms of public safety voice traffic collected over a week long measurement campaign in [43] were used to generate the random interference durations.

Illustration of Performance in the Time and Frequency Domains. We assessed the accuracy of the interference-aware VNA by comparing the CFR and CIR of the wireless channel it measures to those measured by traditional VNA techniques. CFR and CIR plots are generated for four scenarios and compared in Figure 11 and Figure 12 respectively. The four measurement scenarios are: 1) linear frequency sweep without interference, 2) linear frequency sweep with interference, 3) averaged linear frequency sweep with interference, and 4) interference-aware channel sounder with interference. The CFR and CIR demonstrate that the interference-aware VNA is capable of performing clean measurements while operating in long-burst interference environments. The interference-aware technique performs more reliably than traditional techniques in interference environments. The effect of corrupt measurement data is visible as increased noise floor and decreased dynamic range in the CIR as well as spurs in the CFR. The ability of the interference-aware VNA to attain accurate measurement results in the presence of interference comes at the cost of increased measurement time. Steps to reduce the measurement time should be taken without sacrificing the requisite accuracy.

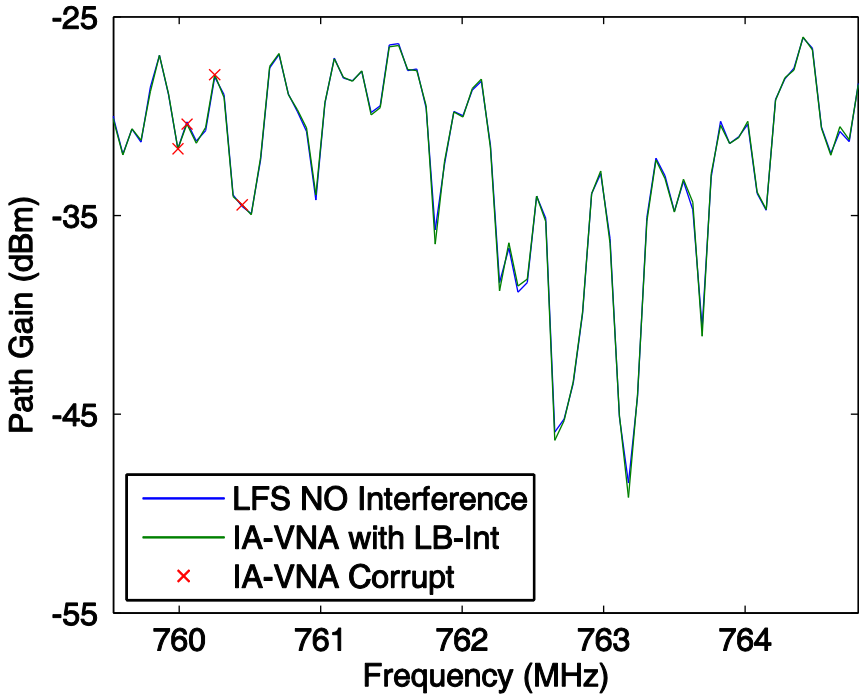


Figure 11 - Comparison of CFR plots produced by different VNA techniques

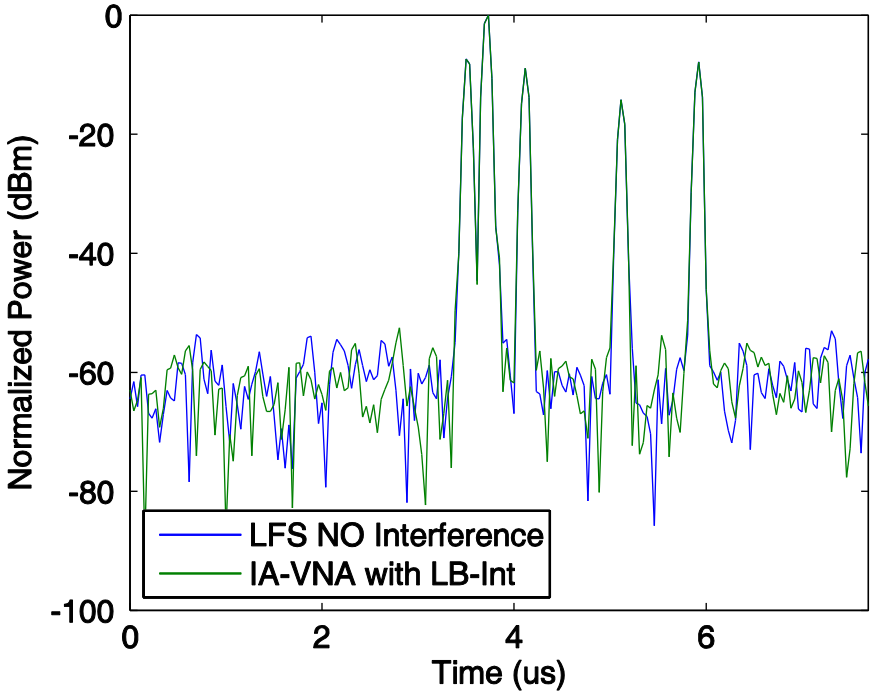


Figure 12 - Comparison of CIR plots produced by different VNA techniques

Illustration of Improvement of Measurement Time. The interference-aware VNA implementation is significantly slower than traditional VNA measurement techniques even when there is no interference present because of the external hardware and measurement control. When interference is present, the measurement time can rise considerably if the primary user transmissions are of long duration and occur frequently. Such situations are not uncommon and the increased time due to spectrum occupancy can be combatted by implementing the step and skip mode, where a timeout occurs after waiting a specified amount of time and the current measurement point is skipped. The step and skip mode is used in the implementation. Implementing the random access mode discussed earlier would further reduce the wait time by avoiding situations where signal with a bandwidth that covers multiple points causes waiting at sequential frequency points. Unfortunately, implementing a random access mode using external hardware and control software would end up increasing measurement time due to the increased communications overhead time. Integrating interference-aware techniques into VNA firmware would allow for more efficient implementation of a random access mode.

*Impact on Primary Users – Possible Test Setups***.** IEEE Standard 1900.2-2008 – IEEE Recommended Practice for the Analysis of In-band and Adjacent Band Interference and Coexistence between Radio Systems – provides guidance on setting up tests to quantify the impact that coexisting wireless devices have on one another. The focus of this standard is on wireless systems that are deployed and operational around the clock, but the principles and framework can be applied to test and measurement equipment that is temporary as well.

> "Depending on the service, performance degradation [due to interference] can be manifested in many ways … [such] as lower data throughput, lower voice quality, video distortions, decreased battery life, increased incident of blocked or dropped links, delay, reduced system capacity, reduced interference margin, or reduced capability of the recipient system to adapt to new condition or advance with new technology. An individual interference event may not in itself be deemed harmful" [46].

In situations where primary user transmissions are classified as long-burst interference and last on the order of seconds, a short transmission from the interference-aware VNA before it detects the primary user and ceases transmission will have only a minor impact on the

primary user. We verified this by operating handheld voice radios in the vicinity of the interference-aware VNA and demonstrating that the people operating the radios could not detect any issues.

3.5 Discussion

We have demonstrated that it is possible to transform a commercial-off-the-shelf VNA into an interference-aware VNA by applying cognitive radio concepts. We have cast the external interferers as primary users and the VNA as a secondary user that is equipped with a spectrum-sensing receiver. Of the three cognitive radio paradigms, we concluded that interweave is the most appropriate for use here because of the CW nature of the VNA stimulus signal.

In this work, we have focused on the case when the duration of the primary users' transmissions is much, much greater than that of the VNA measurement dwell time and have proposed three increasingly sophisticated modes of operation for an interference-aware VNA: stepping mode, step and skip mode and random access mode. All three modes are capable of delivering pristine channel response measurements while having negligible impact on the primary users. However, as primary user occupancy increases and the VNA is forced into an idle state for increasing lengths of time, the total time required to measure a complete frequency response will increase. As operating mode becomes more sophisticated, the VNA will be forced into an idle state less often and total measurement time will decrease.

We implemented a proof-of-concept demonstrator and transformed a Keysight (Agilent) PNA into an interference-aware VNA by adding: 1) a spectrum-sensing receiver, 2) suitable logic for responding to state changes and triggers and initiating triggers, and 3) an external controller to configure the instruments and to oversee operation of the entire measurement system. We demonstrated that such a system is capable of recovering clean estimates of the channel frequency response even in the presence of moderately heavy interference. We conclude that our scheme is practical but that the cost and effort required to realize an interference-aware VNA would be greatly reduced if vendors would implement it using components internal to the VNA and making relatively minor enhancements to the firmware and internal connections used in commercial VNAs instead of relying on external hardware and software.

Chapter 4
An Interference-Aware Vector Network Analyzer for Conducting Wireless Measurements in Short Range Device Bands

4.1 Introduction

In the previous chapter, we demonstrated that it is possible to transform a commercial-off-the-shelf VNA into an interference-aware VNA by applying cognitive radio concepts. We cast the external interferers as primary users and the VNA as a secondary user that is equipped with a spectrum-sensing receiver. Unlike a conventional VNA, an interference-aware VNA must: 1) avoid transmitting while another user occupies the frequency point of interest and 2) reject measurements collected in the unlikely event that another user begins transmitting after the measurement begins.

We previously focused on the case when the duration of the primary users' transmissions is much, much greater (of the order of seconds) than that of the VNA measurement dwell time (of the order of milliseconds). As the number and duration of primary users transmissions increase, the interference-aware VNA will be blocked more often and the length of time required to complete the measurement will increase. In response, we proposed three increasingly complex modes of operation: stepping mode, step and skip mode and random access mode. We showed that all three modes are capable of delivering pristine channel response measurements while having negligible impact on the primary users. The more complex modes introduce flexibility and adaptability that allow the interference-aware VNA to proceed to other frequency points rather than wait for an occupied frequency point to clear. In this manner, the interference-aware VNA will be forced into an idle state less often and the total measurement time will decrease.

Short-range device bands present a unique challenge because the primary users in these bands tend to emit data packets that are much shorter (of the order of hundreds of microseconds) than the VNA measurement dwell time (of the order of milliseconds). We refer to such interference as *short-burst interference*. As a consequence, it is possible for a primary user transmission to begin and end while the VNA is in the process of measuring a single

frequency point. We refer to such transmissions as *latent transmissions*. This greatly reduces the effectiveness of the listen-measure-listen strategy employed in the previous chapter to prevent: 1) communications between primary users from corrupting VNA measurements and 2) VNA emissions from interfering with communications between primary users.

Given that VNA-based wireless measurements are generally conducted using low transmit power and over brief periods, preventing communications between primary users from corrupting VNA measurements is our primary concern. Here, we propose a statistical method for eliminating corrupted measurements that does not require manual intervention. When short-burst interference is either expected or detected, the interference-aware VNA is tasked with measuring the same frequency point multiple times during the measurement sequence. Carrier sensing prevents the VNA from measuring the response at a particular frequency point as long as part of the packet is detected before the measurement is triggered. If we can assume that the probability of a latent transmission is low, then it is reasonable to conclude that corrupted measurements will appear as outliers against a background of several pristine channel measurements. In that case, applying robust estimation techniques in order eliminate the outliers that result from the interference will significantly improve the reliability and accuracy of the channel measurements in the presence of such interference.

The remainder of this chapter is organized as follows: In Section 4.2, we present our system level design of an interference-aware VNA based on a combination of spectrum sensing to detect channel occupancy and robust estimation to eliminate outliers that result from latent transmissions. In Section 4.3, we summarize our efforts to collect and interpret spectrum occupancy data collected in the ISM2450 band in a WiFi-dominated indoor environment and determine the characteristics of the busy and idle time distributions in such cases. In Section 4.4, we describe our implementation of a proof-of-concept demonstration of an interference-aware VNA. Much of the design was driven by the need to avoid measurement delays and results in an implementation that is quite different from the implementation described in the previous chapter. In Section 4.5, we conclude that the proposed scheme is both effective and practical. Its most serious limitation is the additional time required to collect multiple measurements at each frequency point. The effectiveness of the scheme would be greatly improved by real time estimation of the minimum number of

measurements required to successfully apply robust estimation of the true response at each frequency point.

4.2 Concept

4.2.1 Mode of Operation

The mode of operation used for the short-burst interference-aware VNA is a slightly modified version of the stepped sweep mode. The mode used here has two steps: 1) carrier sense before each of a set of measurement at each frequency point and 2) robust estimation is applied to the set of measurements collected in the first step before moving on to the next frequency point. This mode can be referred to as the stepped-point stepped-frequency mode.

The objective of the first step of our algorithm is to avoid interference between the VNA and primary users while taking measurements because interference is negative for both parties. Avoiding interference allows the VNA to collect accurate measurements and prevents causing harm to the primary users. Our algorithm consists of three states: 1) sense state, 2) measure state, and 3) wait state.

The 'measure state' collects measurement data that can range from a single data-point to a set of data-points and is chosen by the user according to the interference characteristics. Once selected, the number of data points collected and the measurement time is constant for each time the 'measure state' is entered during the measurement. The 'measure state' transitions to the 'sense state' after each completed measurement.

The 'sense state' monitors the channel for a fixed time before each measurement and determines if interference is present or not. The 'sense state' transitions to the 'wait state' if interference is present or it transitions to the 'measure state' if there is no interference. The time spent in the 'sense state' is set by the user according to a ratio of sense time to measure time and is constant for each time the 'sense state' is entered during the measurement.

The 'wait state' continuously senses the channel until the interference ceases and is only entered when the 'sense state' detects interference. The 'wait state' transitions directly to the 'measure state' as soon it determines the interference has disappeared. The amount of time spent in the 'wait state' will be a result of the characteristics of the interference environment.

*The objective of the second step of our algorithm is to identify data points that incurred interference and made it through the first step of the algorithm, and remove them from the dataset***.** We identify corrupt data points by taking several measurements at each frequency point and assume that any outliers of the statistical distribution are corrupt data points. Any outlying data points are then removed by using robust estimation. The closest sample to the estimated mean value is selected as the measurement value for that frequency point.

4.2.2 Performance

*Measurement Time***.** The benefits of our multi step algorithm are offset by increased measurement time due to the increased number of data points required for statistical confidence. It is therefore imperative to understand what contributes to the overall measurement time so appropriate action can be taken to offset the increase as much as possible. Each state of our algorithm will be held for a finite amount of time before moving to the next state. An example of how the first step of our algorithm interacts with an active channel is illustrated in Figure 13 and has the state times 1) measurement time (t_m), 2) sensing time (t_s), and 3) waiting time (t_w) labelled.

Both t_m and t_s are constant for each measurement point for the duration of the measurement. This makes it easy to calculate the total time spent in these two states because the number of measurement points is the only variable that affects their contribution. If we are required to collect N data points at each of F frequency points for our measurement, then the total time spent in the measurement and sensing states are determined by

$$t_M = N \times F \times t_m$$

and

$$t_S = N \times F \times t_s ,$$

where t_M and t_S are the total time spent in the measurement state and sensing state, respectively.

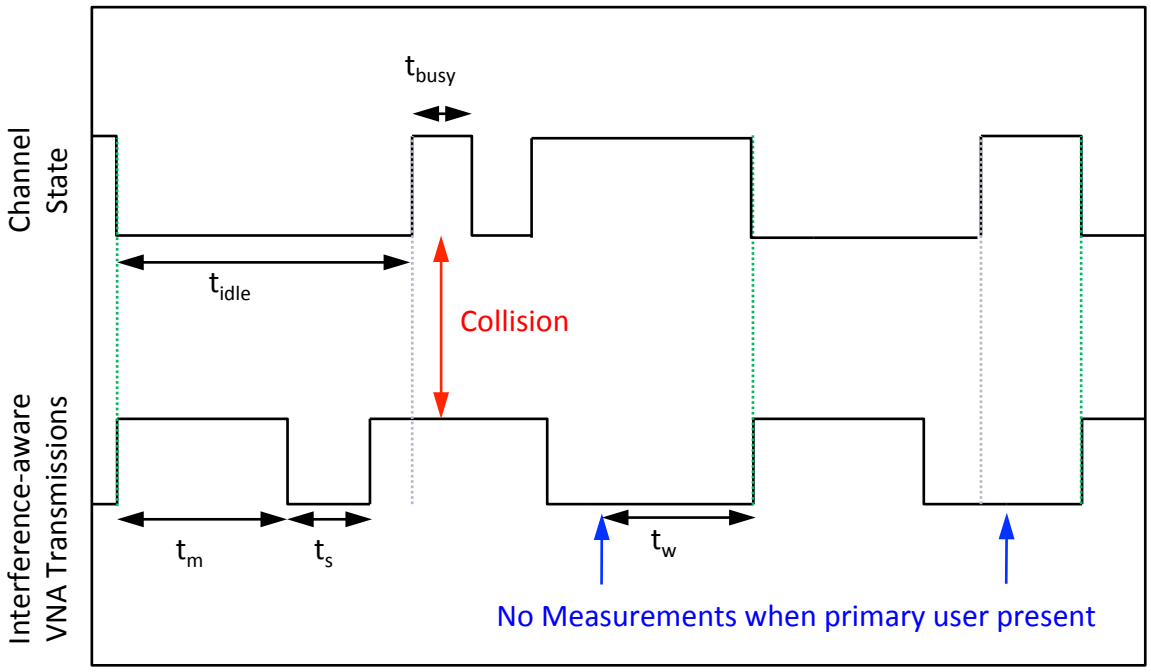


Figure 13 – Short-burst interference-aware VNA carrier-sense and medium access timing diagram

Let the amount of time in the measure state and sensing state required to complete the measurements be represented by t_{acq} so that,

$$t_{acq} = t_M + t_S$$

and

$$t_{acq} = N \times F \times (t_m + t_s) \ .$$

The total measurement time, T_{TOT}, is equal to the amount of time the channel was idle during the measurement, t_{idle}, plus the amount of time the channel was busy during the measurement, t_{busy}, i.e.,

$$T_{TOT} = t_{idle} + t_{busy} \ . \qquad (1)$$

The idle time and busy time also determine the spectrum occupancy as a percentage of time, SO,

$$SO = \frac{t_{busy}}{t_{idle} + t_{busy}} \ . \qquad (2)$$

Because our algorithm acquires data when the spectrum is idle and waits when the spectrum is busy, the measurement completes once t_{idle} is equal to t_{acq} , and the time spent waiting, t_{wait}, will be equal to t_{busy}. Therefore equations (1) and (2) above become

$$T_{TOT} = t_{acq} + t_{wait} \qquad (3)$$

and

$$SO = \frac{t_{wait}}{t_{acq}+t_{wait}} \quad . \qquad (4)$$

Reorganizing equation (4) to isolate t_{wait} , and substituting it into equation (3) yields the total measurement time T_{TOT},

$$T_{TOT} = \frac{t_{acq}}{(1-SO)}.$$

When spectrum occupancy is zero, the measurement time is equal to t_{acq} and as spectrum occupancy approaches 100% our measurement time approaches infinity.

The waiting time, t_{wait} , is determined by multiplying SO by T_{TOT} and can range from no time when the channel is vacant to a large amount of time when the channel is highly occupied, i.e.,

$t_{wait} = SO \times T_{TOT}$.

4.3 Spectrum Occupancy in Short Range Device Bands

Spectrum Occupancy of Short Range Device (SRD) frequency bands is unique from the majority of allocated frequency bands because of the emitter characteristics, variety of wireless systems sharing common spectrum, and the license-exempt status of most of these bands. Emitters in SRD bands generally transmit low-power spread-spectrum digital burst signals that can be difficult to capture without proper equipment and configuration. These bands most often support numerous homogenous and heterogeneous wireless systems that are forced to coexist in shared spectrum without regulator allocated channels, which challenges the traditional channel-based spectrum occupancy approach where only one type of emitter is expected in a defined bandwidth. License-exempt transmitters that operate in SRD bands are

not documented in databases and there is nowhere to consult on what to expect in a particular location or area. These unique characteristics make conducting spectrum occupancy measurements in SRD bands more challenging than other traditionally allocated frequency bands.

There are a number of published studies that explore spectrum occupancy of SRD bands and the types of devices that operate in them, but there are limitations due to the measurement equipment, instrument configuration, and test setups. Many studies are only able to produce first-order models or coarse time-binned first order models because the measurement equipment couldn't sample the spectrum fast enough to capture the short-burst behaviour of SRDs [47] [48]. Other studies that do use measurement equipment capable of capturing the short-burst behaviour are conducted in controlled test environments where the primary user traffic is not reflective of the coexistence nature of SRD bands in uncontrolled environments [49]. In order to understand and characterize the short-burst spectrum occupancy behaviour of SRD devices operating in realistic uncontrolled wireless environments, further measurements need to be conducted.

4.3.1 Hardware

The spectrum occupancy measurement setup consists of an Agilent N6841A RF Sensor, a computer to control and communicate with the RF Sensor, and a sleeve dipole antenna. A diagram of the measurement system can be seen in Figure 14 and a photo of it can be seen in Figure 15. The RF Sensor is configured to perform continuous time measurements of a WiFi channel so the temporal behaviour of transmissions in the channel is captured. The IQ-stream mode of the RF Sensor is used to stream the measurement data as it is being collected, and the stream stops when the deep capture memory first-in-first-out (FIFO) buffer becomes full. The sampling rate of the RF Sensor is set to the maximum sample rate of 28 MSa/s in order for the usable frequency span to cover the 20MHz WiFi channel at 2.412 GHz. In this configuration, it takes about 11.8 seconds for the FIFO buffer to fill and for the data collection to stop. No attenuation or pre-amp was used as a compromise between receiver sensitivity and signal distortion. The stream is also configured to send the maximum allowable block size so that the maximum throughput of the Ethernet link is achieved, and therefore the measurement duration is maximized. The IEEE-1588 standard was used for time synchronization because

GPS signals are not easily picked up indoors. The computer controller executes C programs that call functions in the RF Sensor Application Libraries (SAL), which are then relayed to the RF sensor over a 100BaseT Ethernet connection. The sleeve dipole antenna is selected for its omnidirectional pattern so that transmissions from all directions can be detected. The spectrum occupancy measurement setup was installed on a cart to provide an indoor mobile measurement solution.

4.3.2 Software

RF Sensor software – SMS SMT SAL. The RF Sensor comes with a suite of software tools to manage communications and to support user development of applications. The tools include the Sensor Management Tool (SMT), the Sensor Management Server (SMS), and the Sensor Application Library (SAL). The SMS needs to be installed on the computer that will run programs to communicate with the RF Sensors and it can be used to coordinate measurements between multiple RF Sensors. The SMT is an application that allows easy management of the RF Sensors and enables users to verify that the RF Sensors are configured and are running correctly. The SAL is a library of function calls that can be made to the RF Sensors and allows the development of custom software programs to fully interact with the RF Sensors.

Data Acquisition Software. A windows terminal application was written in C to make function calls to the SAL and acquire data according to the parameters passed into the application from the terminal command line. The acquired data is written to a file in its binary format so that it can be post-processed in the data processing environment. The terminal applications do not have a GUI and rely on text being written to the terminal to inform the user on the program's status. The major limitation imposed on the data collection software is the 100BaseT Ethernet port of the RF Sensor which can act as a bottleneck when transferring measurement data with a bandwidth larger than 2 MHz.

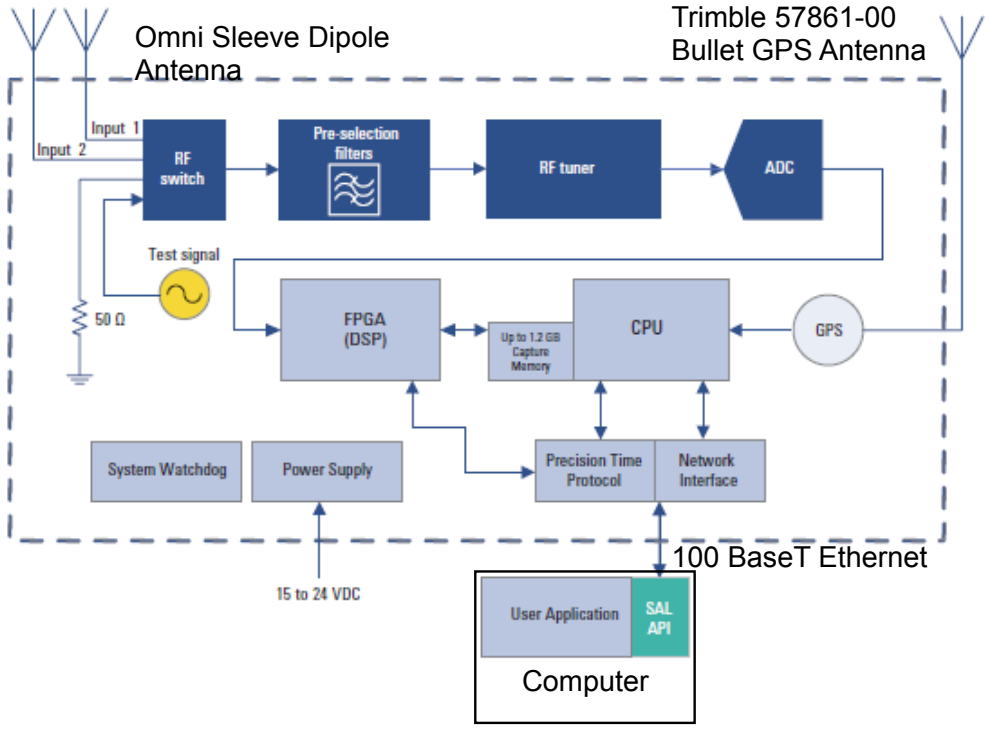


Figure 14 – Block diagram of N6841A-based spectrum occupancy measurement system from [47]

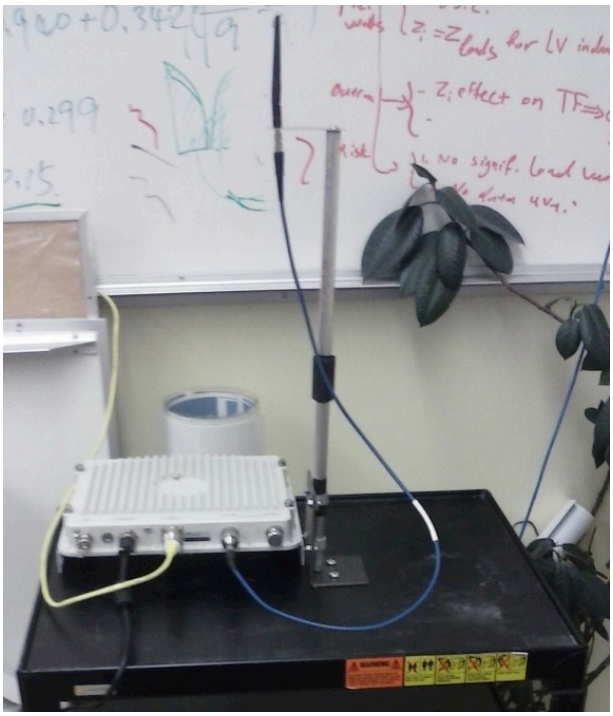


Figure 15 - Photo of N6841A-based spectrum occupancy measurement system

The IQ Stream application records the IQ time data being sampled by the RF Sensor to a file. The measurement is configured according to the user inputs that include centre frequency, sample rate, antenna port, number of samples per TCP packet, and filename for the data. Using the IQ Stream mode of the SAL effectively extends the signal capture memory by adding the 630 Megabytes of DMA memory to the 512 Megabyte FIFO buffer and clearing up memory by sending data out of the sensor during acquisition. The number of samples per TCP packet should be set to the maximum value of 32768 to maximize the data payload to packet header byte ratio and ensure that the payload data from the RF Sensor is being read out at the maximum rate. Using the IQ Stream mode instead of using the lookback feature of the time mode increases the continuous capture time at full sample rate from 4.8s to 11.8s.

Data Processing Software. MATLAB is used as the data processing software environment because of the rich suite of toolboxes and libraries it provides as well as the flexibility that it offers. A series of MATLAB functions were written to perform spectrum occupancy analysis of the measurement data. Functions were written to read the data files produced by the acquisition software, determine a threshold value, determine the channel state, determine the state holding times and determine the percent spectrum occupancy. Various plots of the metrics and statistics are presented by these functions so the researcher can visually analyze the data to spot trends and patterns in the data and ensure data integrity. In addition to the spectrum occupancy processing functions, a function was written to create a MPEG4 video of spectrum snapshots for the duration of the measurement so complete visual analysis of the measurement data can be performed using almost any video player software. Researchers can swap out any of these functions with a replacement function that uses a different technique or algorithm with little effort and without having to start their programming from scratch.

The threshold function applies a user defined Probability of False Alarm to the statistical distribution of the instrument noise power and selects the corresponding power level as the threshold. Noise power measurement files can be created by performing a measurement with a matched load connected to the RF input of the RF Sensor and should be performed under the same thermal conditions the RF sensor will be exposed to during data collection so the thermal noise in all the measurements is comparable.

The channel state is determined by comparing the power level of the measurement data to the power level determined by the threshold function. The spectrum is considered to be occupied where the measurement data values exceed the threshold and is otherwise considered idle. The state holding times are determined by counting the number of consecutive channel state values and then multiplying those values by the time between samples. The percent spectrum occupancy is calculated by dividing the total number of samples that are above the threshold by the total number of samples in the data set.

The user can specify the FFT overlap and number of FFT points to use for the spectral analysis of the IQ data, while the spectrum data collected by the FFT acquisition program had the number of FFT points (limited to maximum of 16384 points) determined at the time of measurement and the FFT overlap is fixed at 50% when using averaging.

4.3.3 Data Collected

Spectrum occupancy measurement data was collected to characterize the temporal behaviour of Wi-Fi transmissions in the ISM 2450 band. The measurements were conducted at a single location in an indoor office environment, the MacLeod Building at UBC, because the desired outcomes were strictly temporal and not spatial. Measurement data was collected over a 48 hour period with a measurement taking place every 15 minutes. Each measurement was an 11.8 second continuous-time IQ data capture that produced a 1.2 GB file. A total of 236 GB of data and 2265 seconds of observation time was generated by the measurement campaign. This data set contains enough information to provide over three-hundred-thousand duration time samples for both the WiFi channel's busy and idle time durations.

4.3.4 Results

Plots of the busy duration and idle duration histograms are provided in Figure 16 and Figure 17 respectively. The histograms show that the transmission durations do not occur randomly, but rather are heavily influenced by the protocols. Modelling the durations of transmissions and gaps between transmissions with commonly used random distributions is unlikely to produce a good fit to the measurement data, unless the time resolution is destroyed by using larger bins. However, this may defeat the goal of producing a realistic simulation model. As a result of the heavy influence of the protocols, information about the access point configuration can be extracted by comparing the measurement data to the details of the IEEE-

802.11 standard. The most commonly encountered values in the busy duration histogram are likely to correspond to the various combinations of data transmission rates and data payload sizes. Wi-Fi device are frequently adjusting their data-rates and modulation scheme to minimize bit errors and maximize throughput as the condition of the wireless channel changes. The most commonly encountered values in the idle duration histogram are found to correspond to the inter-frame spacing durations. The values show that in addition to the Short Inter-frame Spacing (SIFS) being common, that the Arbitration Inter-frame Spacing (AIFS) is also common. The presence of AIFS values in the idle duration histogram indicates that the access point is configured to use wireless quality of service. Other values in the idle duration histogram that are not linked to the inter-frame spacing can be attributed to other access point settings, like the Beacon Interval. A meeting with UBC IT Services confirmed some of the insights gained analyzing the measurement data.

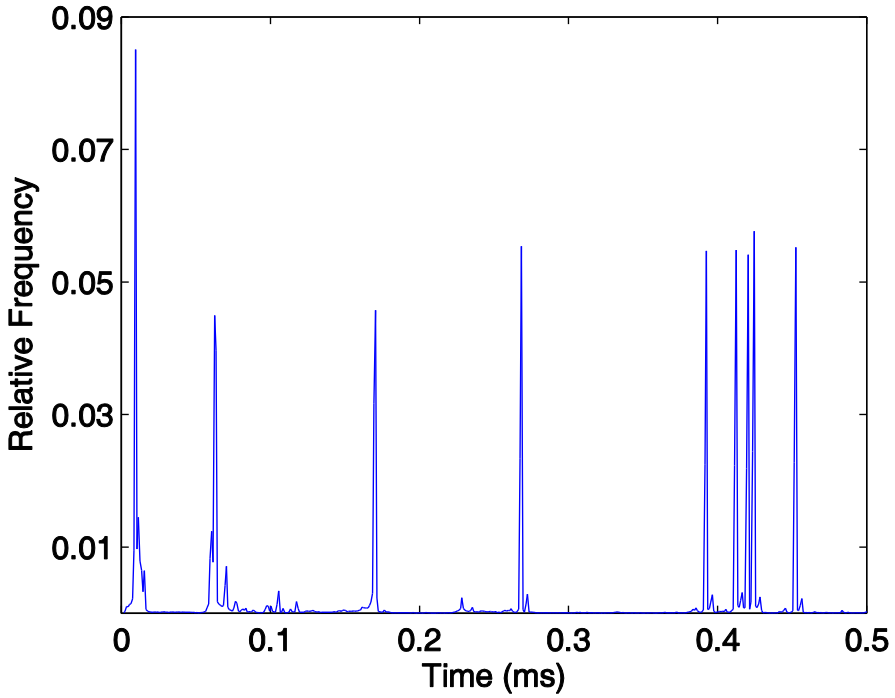


Figure 16 - Histogram of Wi-Fi channel busy durations, cut off at 0.5ms

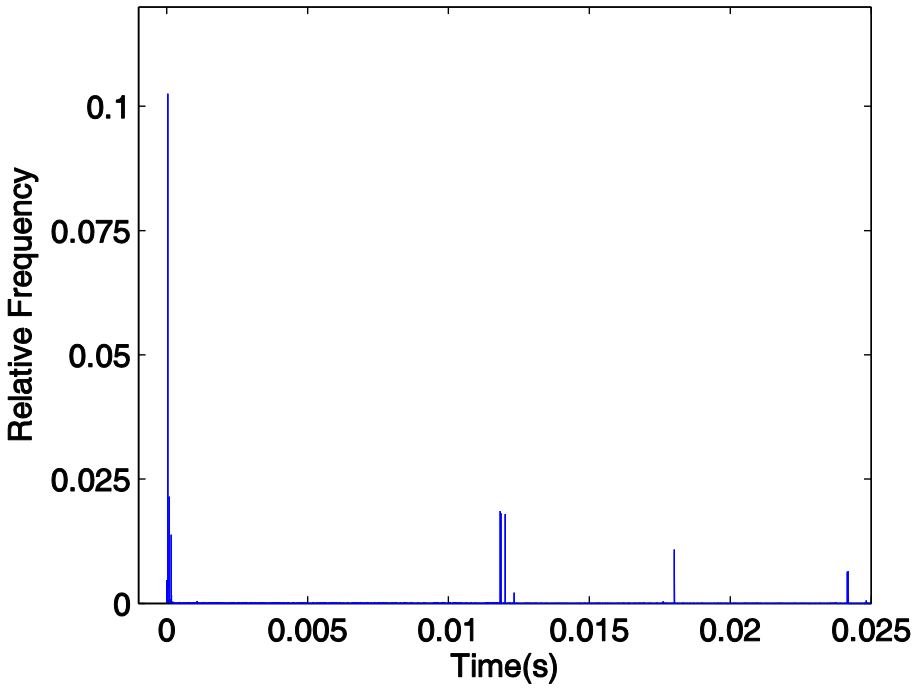


Figure 17 - Histogram of Wi-Fi channel idle durations, cut-off at 25ms

The Cumulative Distribution Functions (CDF) of busy and idle durations are shown in Figure 18 and Figure 19. The CDFs provide an easy means to determine what percentage of the transmissions and idle durations fall below a particular time value. The busy duration CDF can be used to select an optimal timeout value that prevents excessive waiting for the spectrum to clear. The idle duration CDF can be used to predict what percentage of interference-aware VNA transmissions will be interfered with by the primary user once the VNA measurement duration is known, as well as how long the sense state duration should be. The CDFs and PDFs provide tremendous insight into the spectrum occupancy behavior and allow interference-aware VNA operators to tune the configuration for better performance.

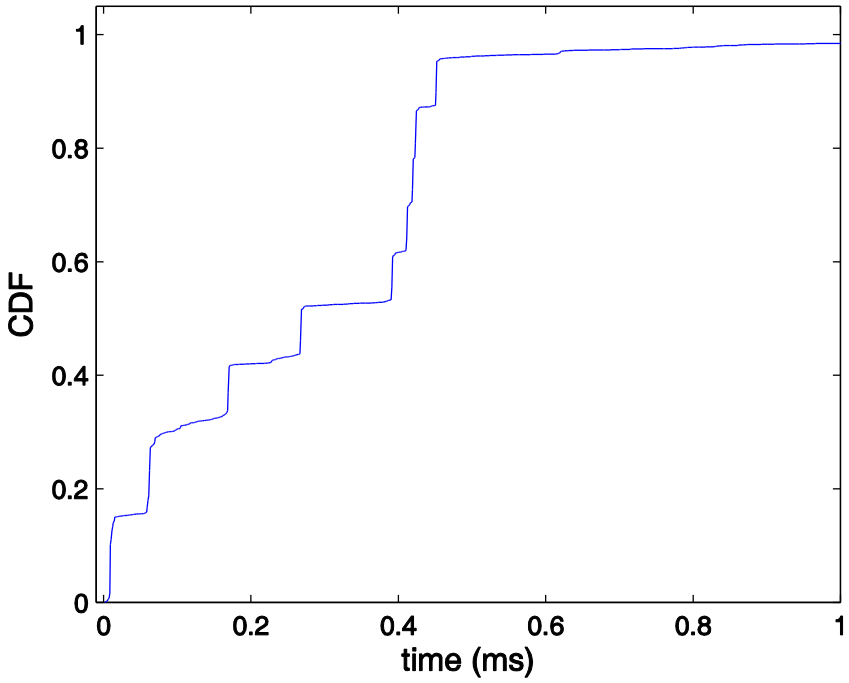


Figure 18 - Cumulative distribution function of Wi-Fi busy durations, cut-off at 1ms

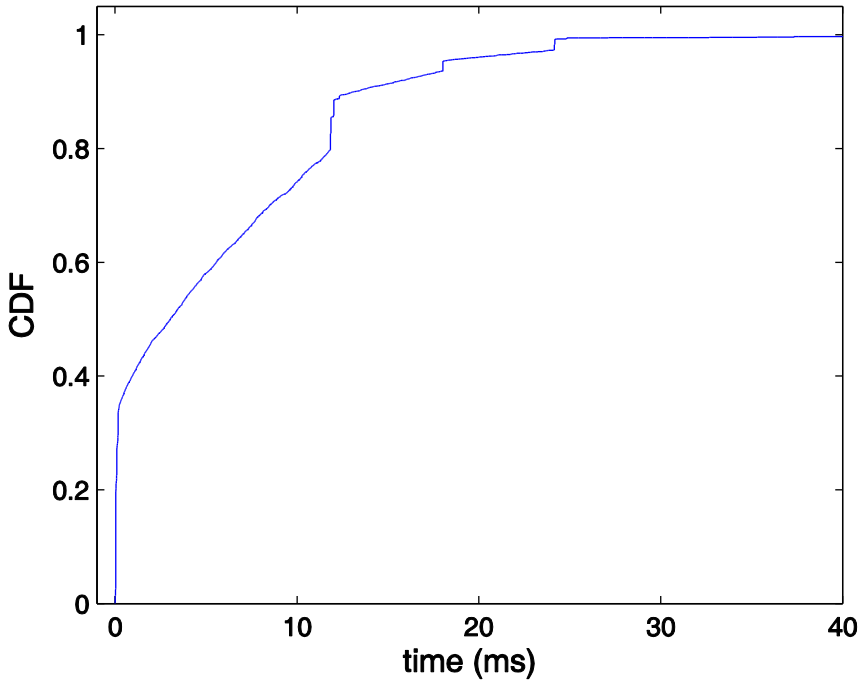


Figure 19 - Cumulative distribution function of Wi-Fi channel idle durations, cut-off at 40ms

4.3.5 Discussion

Though the 802.11 protocols are well defined in IEEE standards, there is no easy way to use the available information to accurately predict the occupancy because the spectrum is shared by homogenous and heterogeneous coexisting devices. It is common to find numerous license-exempt devices operating in the same spectrum such as WiFi devices from various networks and non-WiFi devices like Bluetooth transmissions. Performing a measurement campaign is the only way to observe the real occupancy behaviour of WiFi and other signals operating in license-exempt SRD bands. The spectrum occupancy measurement results will be used to tune the interference-aware VNA for operation in the ISM 2450 band in the next section.

4.4 Proof-of-Concept Implementation

This proof of concept implementation demonstrates that interference-aware VNA concepts for short-burst interference environments can be implemented today by augmenting a COTS VNA with external hardware. This implementation is not a commercial product and its intended use is to test the performance of the interference-aware VNA techniques. The architecture, hardware, and software of the implementation are designed for operation in the presence of short-burst interference and discussed in this section.

The previously discussed short-burst interference-aware VNA concepts are implemented using as much commonly available COTS equipment and as little custom hardware as possible. The first step of the proposed algorithm that applies carrier sense is implemented in hardware, while the second step of the proposed algorithm that applies robust estimation is implemented in software. All of the hardware in addition to the VNA is used to add a carrier-sense MAC to the VNA. At the core of this implementation is an Agilent E8362C PNA-series VNA, which is a reasonably high end but commonly used instrument with standard and non-standard input/output ports. The VNA is augmented with a HP 8594E spectrum analyzer to act as a dedicated spectrum sensor, a custom designed logic board to inhibit and trigger VNA measurements, and a laptop to configure the instruments and process the measurement data.

4.4.1 Hardware

VNA Configuration. The VNA is directly interfaced to a number of other components using a number of input/output connectors, as shown in Figure 20. The two standard RF ports are each connected to an antenna using coaxial cable to execute a single direction S21 measurement, except there is an RF switch along the transmission output path and the receiver path is split to go to the SA as well. The GPIB connector is used to interface the VNA to the computer controller, which configures and extracts measurement data from the VNA. The external trigger input BNC connector is interfaced to the logic board to enable the logic board to trigger VNA measurements. The Ready For Trigger pin on the DB-25 Auxiliary IO connector is used to provide the logic board with updates on the VNA measurement state. A photo of the hardware is shown in Figure 21.

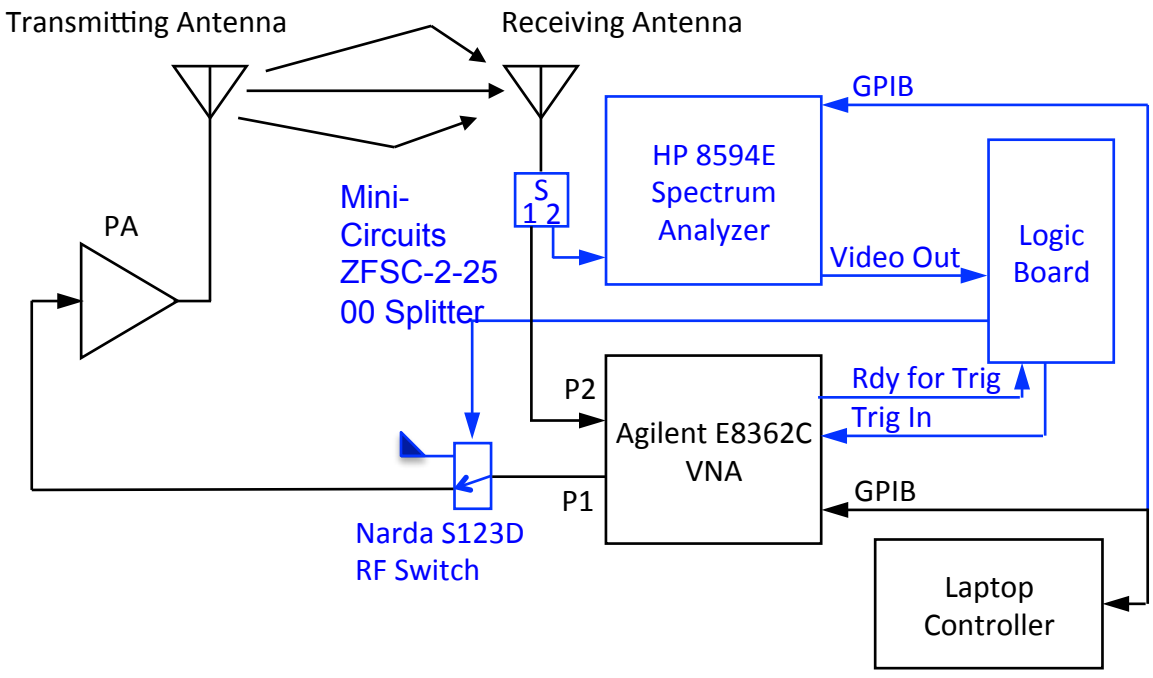


Figure 20 - Hardware block diagram of implemented short-burst interference-aware VNA

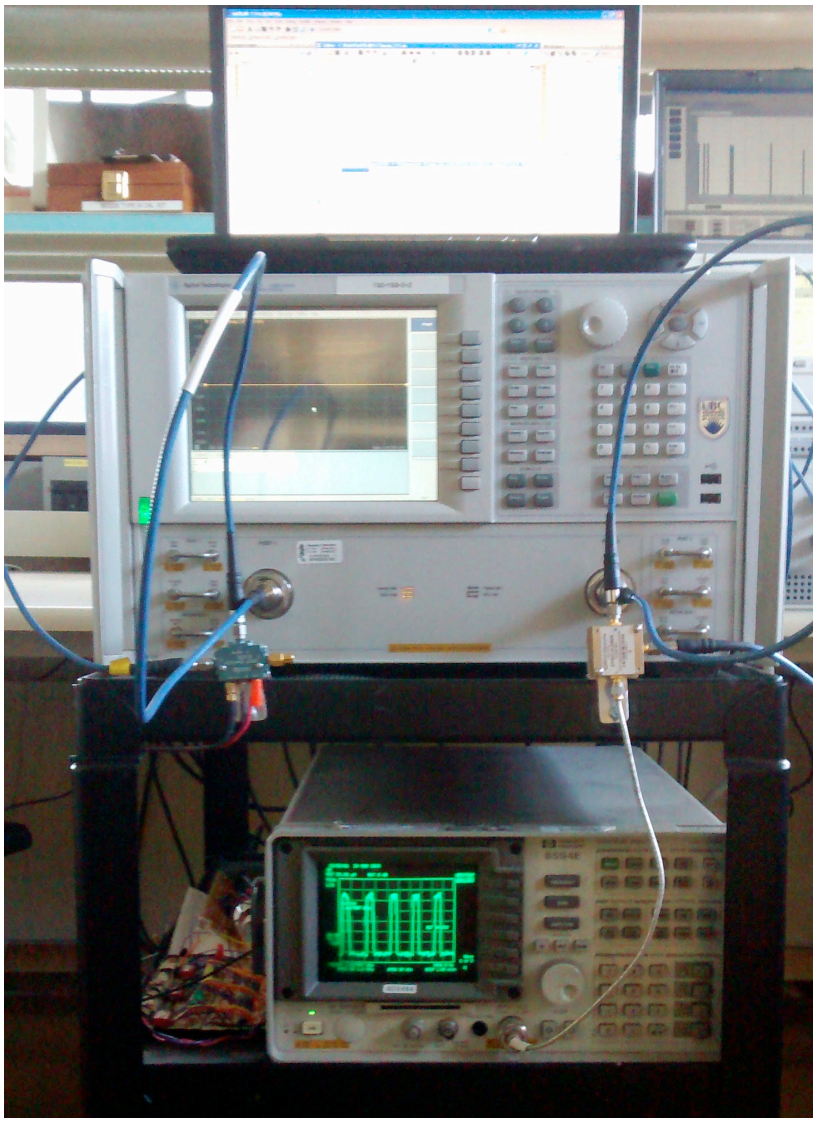


Figure 21 - Photo of short-burst interference-aware VNA implementation

The interference-aware VNA is configured in an unusual manner compared to traditional VNA measurements in order to cooperate with the external components and realize the concept. Frequency synchronization between the VNA and SA is essential, and the most practical way to accomplish this for the short-burst interference concept is by using the Continuous Wave (CW) or Zero-Span mode of both instruments and having a computer control the centre frequency by sending commands over GPIB. Operating the VNA in CW mode means spectrum opportunities can only be exploited at the current frequency setting. Point-trigger mode of the VNA is used to reduce VNA transmission durations by having each trigger measure only a single point instead of an entire sweep. The IFBW is set to the

maximum value of 40 kHz in order to minimize the VNA measurement time, t_m, to 171us. Even at this minimum measurement time, 42% of primary user transmissions will be shorter according to the spectrum occupancy measurements conducted in the previous section. Reducing the VNA measurement time will reduce the probability of interference with short-burst primary user transmissions. External triggering is used to enable the logic board to decide and control when measurements are taken.

Segmented Sweep Mode. After the completion of a CW mode measurement series, the VNA no longer accepts triggers and it drives the Ready For Trigger line high. During measurements, this indicates the VNA is transmitting and the RF switch passes the VNA stimulus signal through. After measurements are complete, however, this causes the VNA to transmit energy continuously. The Auto Source feature that turns the source on for a measurement sweep and off after sweep completion in linear frequency sweep mode would fix this problem, but it does not work in CW mode. To overcome this without adding additional hardware, the VNA is put into Segmented Sweep mode where the first segment is a single point in a vacant license-exempt frequency band and the second segment is setup as a CW measurement series in the frequency band of interest. Using segmented sweep mode in this manner causes the leaked RF energy between measurement series to be transmitted outside the frequency band of interest where it won't cause interference to licensed primary users.

SA Configuration. A HP 8594E spectrum analyzer is used as a continuous spectrum sensor to detect the presence of signals at the frequency that the VNA is collecting measurements. This spectrum analyzer was selected because its analog video output acts as a low latency energy detector that is input to the logic circuit to determine if the channel is busy or idle. Using a spectrum analyzer to sense the spectrum means we are limited to energy detection and cannot easily implement feature based spectrum-sensing techniques. The RF input is connected to a splitter that receives a signal from the receiver antenna and splits it to both the VNA receiver and SA. The spectrum analyzer is interfaced to the computer controller via GPIB and is initialized and configured using SCPI commands. The Video Output signal from the SA is fed into the logic circuit where the voltage level is compared to an energy detection threshold.

The SA is specifically configured to act as a spectrum sensor for the interference-aware VNA by way of the video output signal. The SA is operated in zero-span mode and sweeps continuously with free run triggering so it is able to continuously sense the spectrum. To enhance sensitivity to weaker interfering signals, the amplitude scale on the spectrum analyzer display is set to linear and the reference level is adjusted to position the noise floor near the bottom of the display. The RBW is selected as a compromise between receiver sensitivity, filter charge time, and bandwidth over which detected energy is spread. The VBW is set so the filter charge time, over which energy is averaged, corresponds to the sense time t_s. The spectrum occupancy measurement results from the previous section revealed that the sense time should exceed the Wi-Fi SIFS duration of 40us in order to avoid starting measurements in between successive data packets where interference will almost certainly occur.

RF Switch. The Narda S123D RF Switch is a pin-diode switch that is used to turn the continuous wave signal that is output from the VNA on while in the measure state and off while in the sense state. A pin-diode switch is used because using mechanical switches or sending instrument control commands takes too long to transition states relative to the sense time and measure time of this implementation. External control of the VNA RF source is required because the VNA leaves the source power on while in-between measurement points and sweeps in CW mode while waiting for a trigger. If the VNA source is not turned off in between measurement points, the leaked RF energy causes the spectrum sensor to rightfully declare the channel is busy and prevents any further measurements. The interference-aware VNA would cause self-interference if it didn't have an RF switch to turn its source off in between measurements.

Logic Circuit. The logic circuit schedules VNA transmissions when the channel is free from interference according to the status of the VNA Ready For Trigger output and the SA Video Output. A diagram of the Logic Circuit is shown in Figure 22. The SA Video Output is fed into a comparator circuit to determine if the measured energy level exceeds the predetermined energy threshold. The threshold is adjustable and set by a variable-resistor that is part of a voltage divider feeding the positive input of the comparator. The VNA Ready For Trigger output indicates when the VNA is transmitting so the logic circuit can determine if the energy detected by the spectrum sensor is being caused by the interference-aware VNA, or

primary user transmissions. The logic circuit uses the VNA External Trigger Input to trigger VNA measurements when the channel is determined to be free from interference, and controls the state of the RF Switch to prevent the VNA source from leaking while in the sense state and allow the VNA source to transmit when in the measure state.

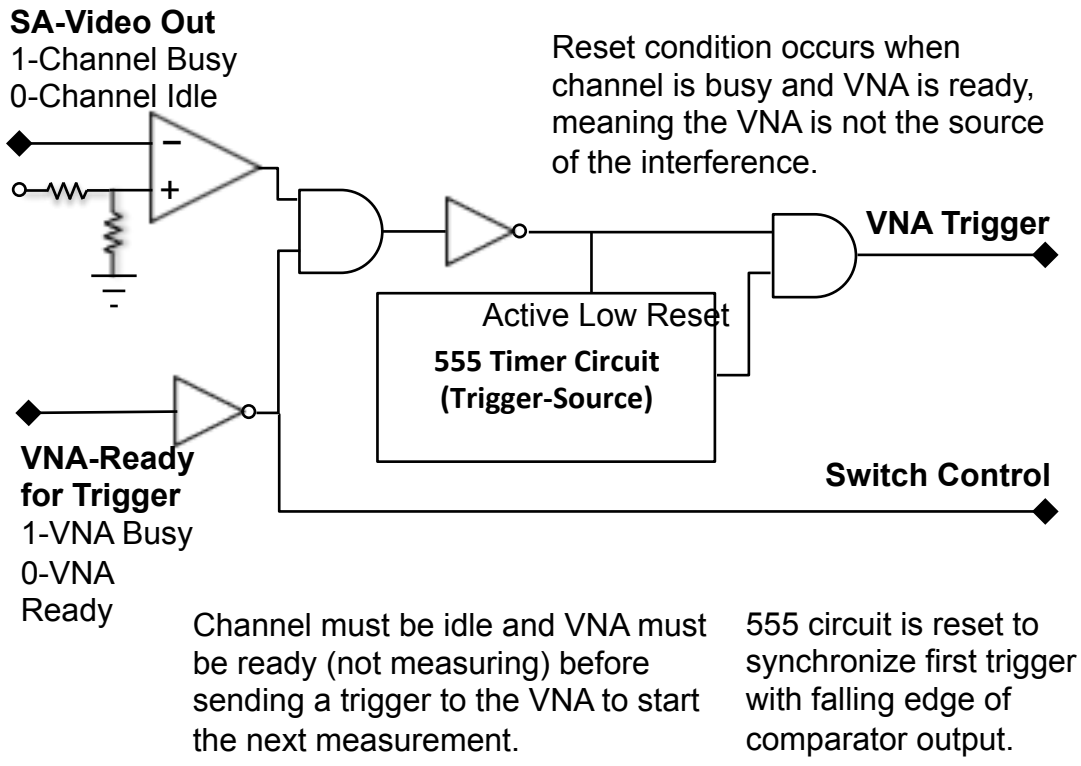


Figure 22 - Diagram of Logic Board for short-burst interference-aware VNA implementation

The 555 timer circuit on the logic board is where the time spent in the sense state after each measurement is set and VNA measurement triggers originate. The sense state time, t_s, is set by the difference between the period of the astable 555 timer circuit and the VNA measurement state time, t_m. The period of the astable 555 timer circuit is set to be to the sum of the desired t_m and t_s. The periodic pulses transmitted by the 555 timer circuit are only received by the VNA when the spectrum is determined to be clear and the VNA is ready to accept the next trigger. If the spectrum is determined to be busy or the PNA is currently taking a measurement, no triggers make it to the VNA. Each time the spectrum is determined to be busy by a source other than the VNA, the 555 timer is reset so the rising edge of 555

timer coincides with the falling edge of the comparator output (spectrum going from busy to idle).

4.4.2 Software

Instrument Control. The computer controller runs a MATLAB script that facilitates the whole measurement process. The MATLAB program begins by initializing the instrument state of both the VNA and SA by sending SCPI commands over the GPIB bus. GPIB is used because; 1) it is the only option for the SA, and 2) GPIB is faster than LAN for small data payloads because of its lower latency. After the instruments are initialized, the measurement is started and the computer waits for the VNA measurements to finish at the current frequency point. The measurement data is then read from the VNA before stepping the VNA and SA to the next frequency point until all of the measurements have been completed at all of the frequency points. Data processing is then started upon reading the measurement data from the final frequency point.

Data Processing. After collection of the measurement data, data processing begins by applying robust estimation to the datasets collected at each frequency point. Outlying data points, considered to be those beyond 3 standard deviations, are removed from the dataset and a new estimation of the mean value is calculated. It was discovered that doing at least two iterations of this was far more effective than a single one because of the large skewing effect a single corrupt data point can have on the initial estimation of the mean value. In several trials where only a single iteration was used, there were no actual data points within 1 standard deviation of the estimated mean after removing the initial outliers beyond 3 standard deviations. This occurred because significant outliers were still in the data set and not removed because of the drastic skewing effect of a few extreme outliers. The larger the ratio of clean data points to corrupt data points, the better robust estimation performed. Upon completion of robust estimation, the data-point closest to the estimated mean value at each frequency point is used to construct a CFR. Applying a Kaiser window with a beta of 7 to the CFR data and performing an inverse Fourier transform on the data yielded the CIR.

4.5 Results

The performance of the short-burst interference-aware VNA implementation and the impact of important parameters on its performance are characterized in this section. The

performance of the proof-of-concept implementation was assessed using accuracy of the CFR and CIR, the time required to complete the measurement, and the impact on primary user networks. The test results demonstrate the interference-aware VNA's ability to collect accurate measurements while operating in the presence of short-burst interference, where traditional VNA measurement techniques cannot operate reliably. The additional time required to conduct the measurements in an interference-aware manner are quantified and the key contributing factors are discussed. Primary user throughput tests are used to quantify the level of harm caused by the transmissions of the short-burst interference-aware VNA.

4.5.1 Accuracy and Timing

Accuracy and Timing Test Setup. The same test equipment used in Section 3.4 to test the performance of the long-burst interference-aware VNA is used again to test the performance of the short-burst interference VNA with a few important changes. The most significant change is that the interference-aware mode of the VNA is changed to short-burst mode instead of the long-burst mode used in the previous chapter. A standard 802.11 indoor channel model for commercial environments is emulated by the SR5500 on both channels to accurately simulate Wi-Fi channel conditions in the ISM 2450 band. The interference generator is also changed to be more representative of the 2.4 GHz band by modifying the timing generator to use different distributions to generate the short-burst idle and busy durations. Idle and busy durations were modelled using the discrete distributions depicted in Figure 16 and Figure 17.

Accuracy Measurements. A series of measurements were conducted to determine the accuracy of the interference aware VNA operating in the presence of short-burst interference. The baseline pristine channel response, which all other methods are compared to, was generated using a traditional VNA Linear Frequency Sweeps (LFS) with no interference present on the channel. Then, interference was injected into the channel and three more series of measurements were taken: 1) traditional linear frequency sweep with interference present, 2) Averaging N traditional linear frequency sweeps with interference present, and 3) interference-aware VNA measurements with N points collected at each frequency with interference present.

The CFR produced by each of the measurement techniques are superimposed in Figure 23 to highlight where deviations due to interference occur. The interference observed in the CFR at affected frequency points looks like superimposed noise with a standard deviation proportional to the amplitude difference of the interfering signal and VNA signal. No significant deviations on the interference-aware VNA CFR are observed like there are on the LFS and averaged LFS CFR plots. The individual CFR plots combined in the comparison figure are individually plotted in Figure 24, Figure 25, Figure 26, and Figure 27.

Figure 28 plots the amplitude of the data collected using the three measurement techniques against the amplitude measured by the clean linear frequency sweep at the same frequency. The residual values from the clean CFR indicate the effect of short-burst interference on the accuracy for each of the measurement techniques. It is visible in the figure that the interference-aware VNA has much smaller residual values compared to the single LFS and averaged LFS.

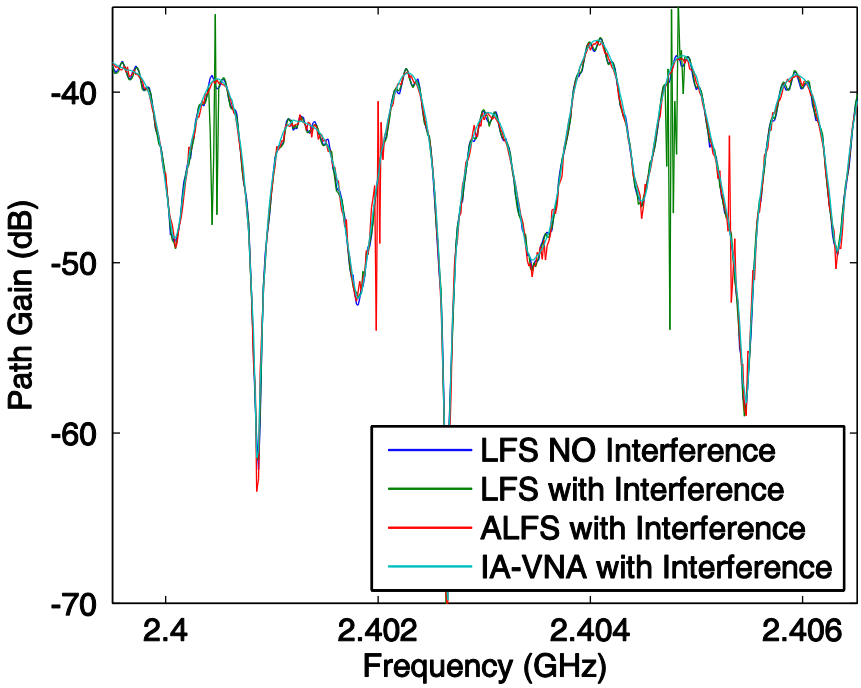


Figure 23 - Comparison of CFRs generated by different VNA techniques

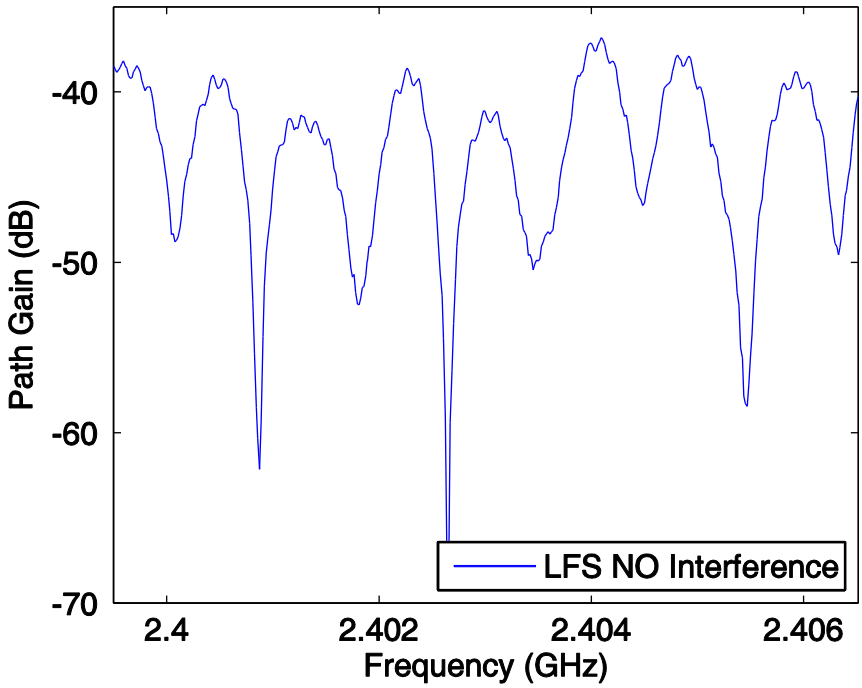


Figure 24 - CFR produced by linear frequency sweep without interference present

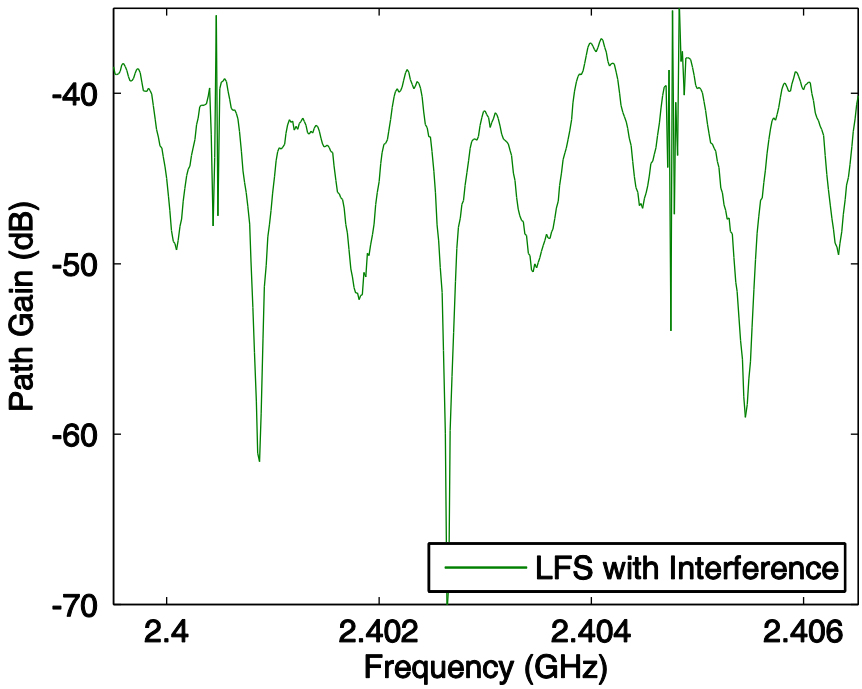


Figure 25 - CFR produced by linear frequency sweep with short-burst interference present

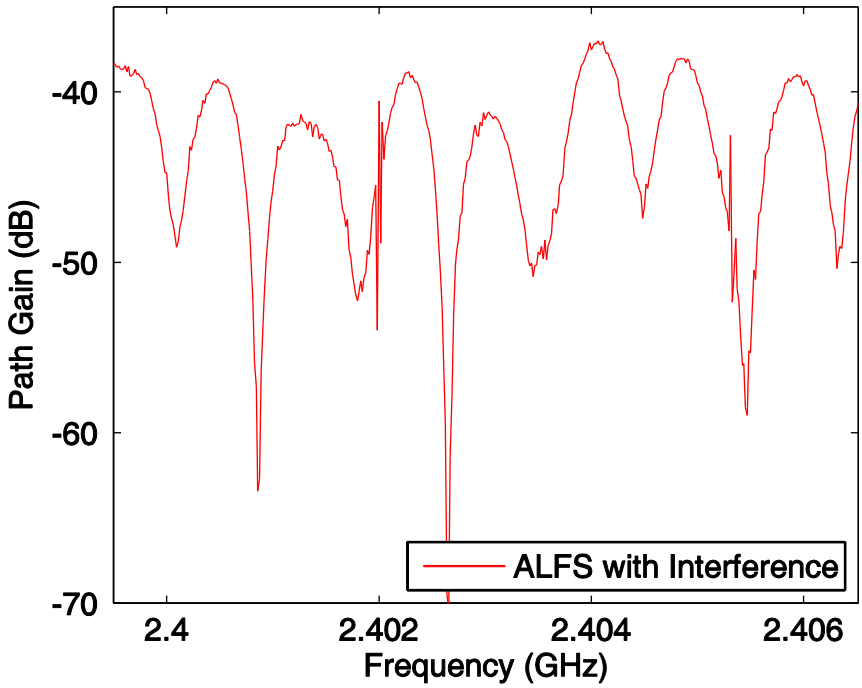


Figure 26 - CFR produced by averaged linear frequency sweep with short-burst interference present

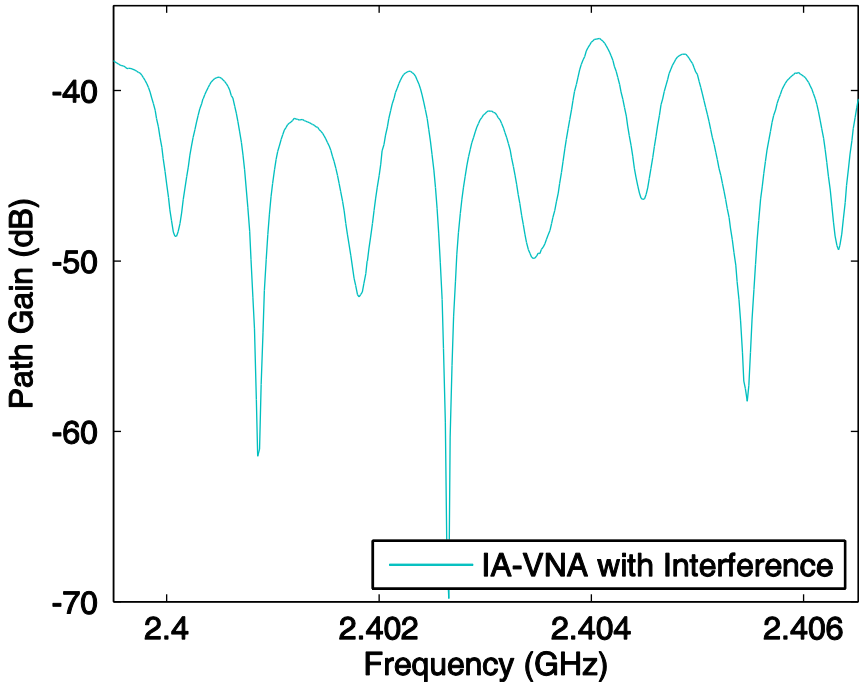


Figure 27 - CFR produced by interference-aware VNA with short-burst interference present

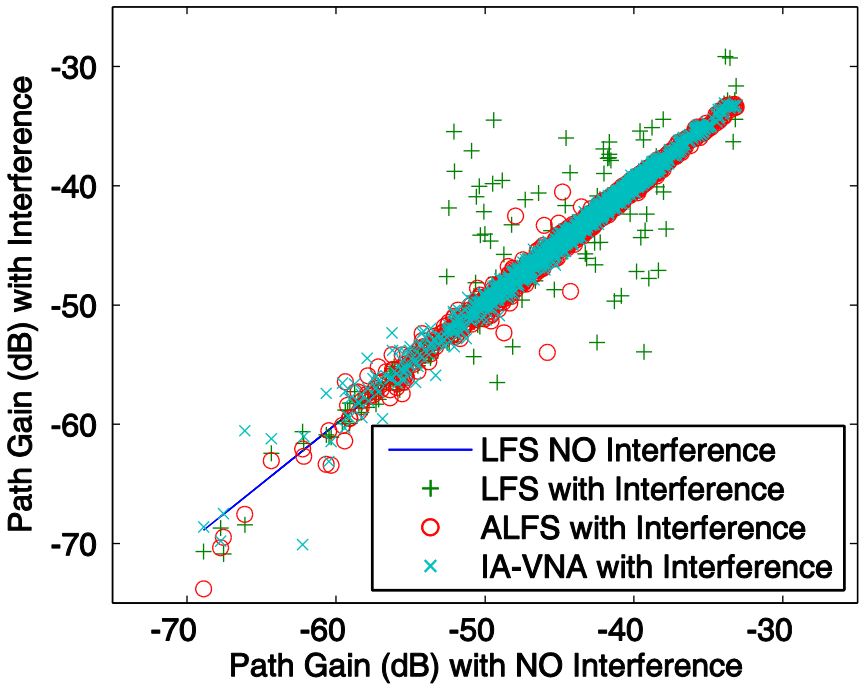


Figure 28 - Residual CFR values produced by different VNA techniques

The CIR produced by each of the measurement techniques are superimposed in Figure 29 to highlight the impact of incurred interference. The plot clearly demonstrates that errors in the CFR measurements appear as an increased noise-floor in the CIR. The more significant the errors in the CFR are, the higher the noise-floor of the CIR gets and the greater the reduction in dynamic range. The individual CIR plots combined in the comparison figure are individually plotted in Figure 30, Figure 31, Figure 32, and Figure 33.

Figure 34 plots the amplitude of the CIR data from the three measurement techniques against the amplitude of the data from the clean CIR at the same time point. This plot displays the difference in CIR noise level obtained from each of the measurement techniques. The interference-aware VNA technique outperforms the other two traditional techniques in terms of dynamic range by several dB.

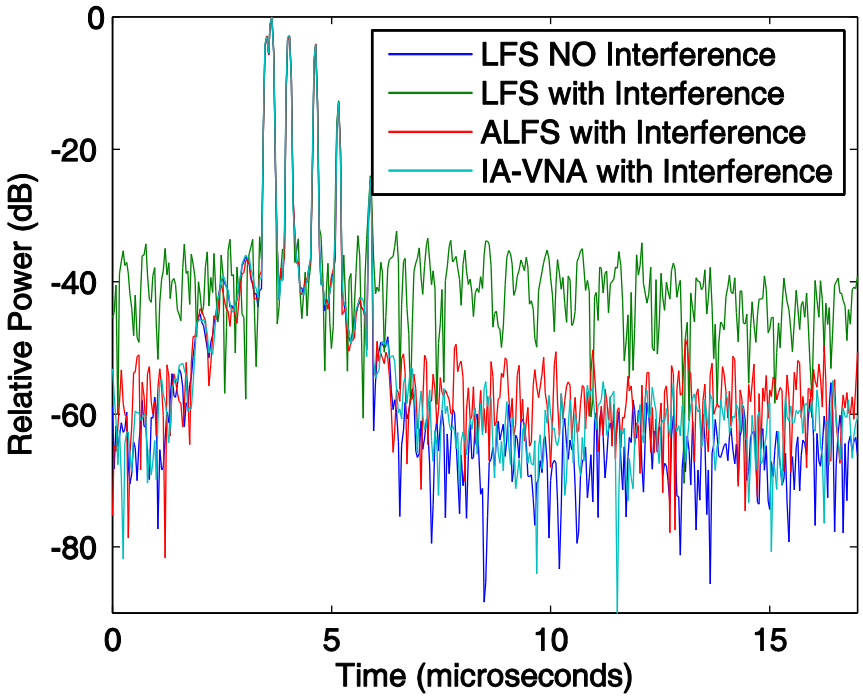


Figure 29 - Comparison of CIRs generated by different VNA techniques

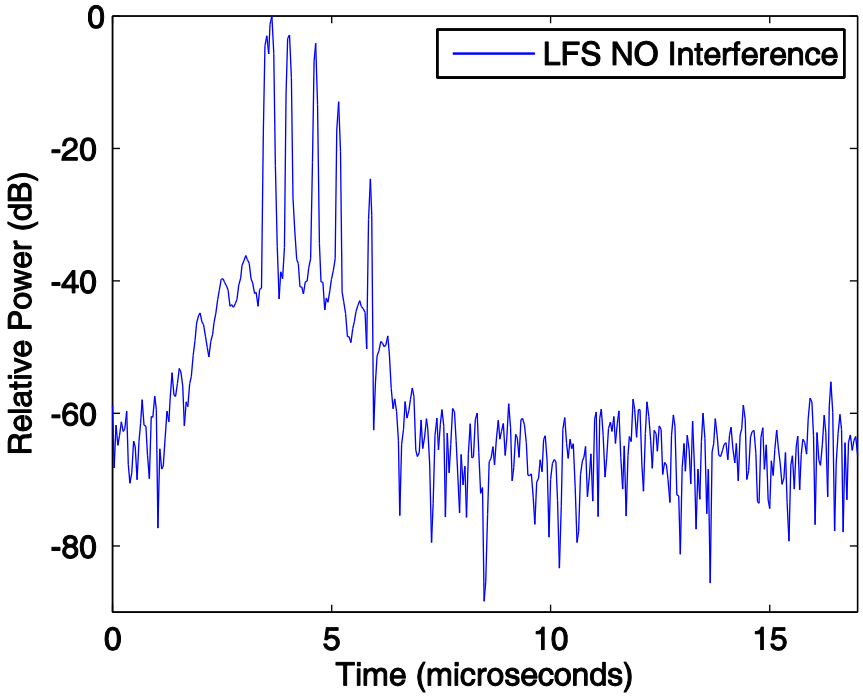


Figure 30 - CIR produced by linear frequency sweep without interference present

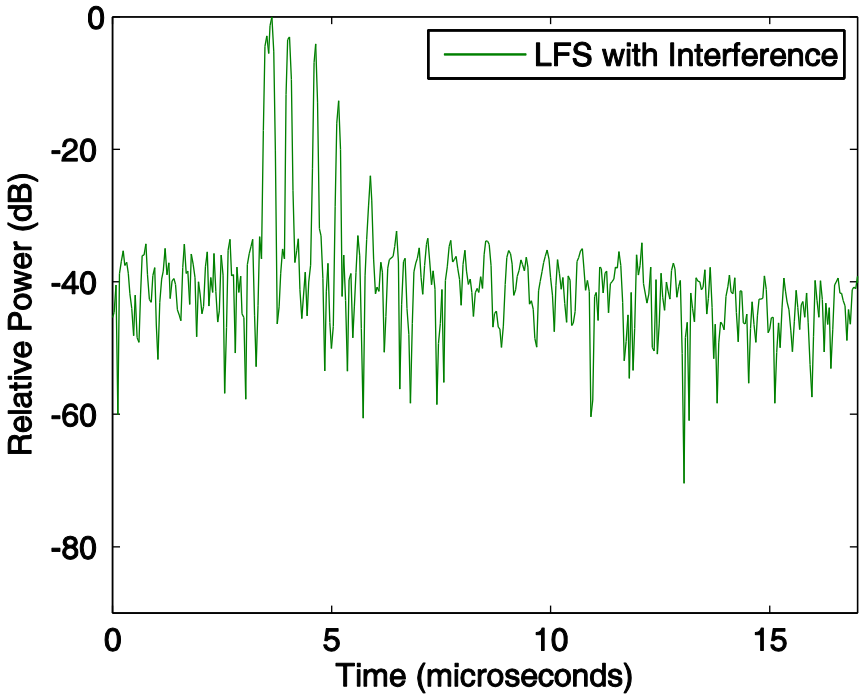


Figure 31 - CIR produced by linear frequency sweep with short-burst interference present

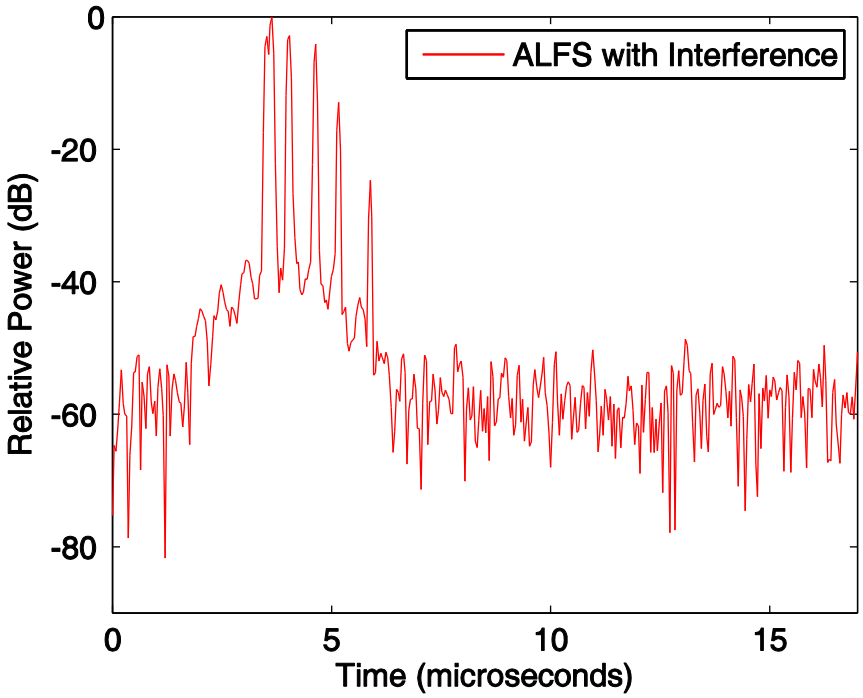


Figure 32 - CIR produced by averaged linear frequency sweep with short-burst interference present

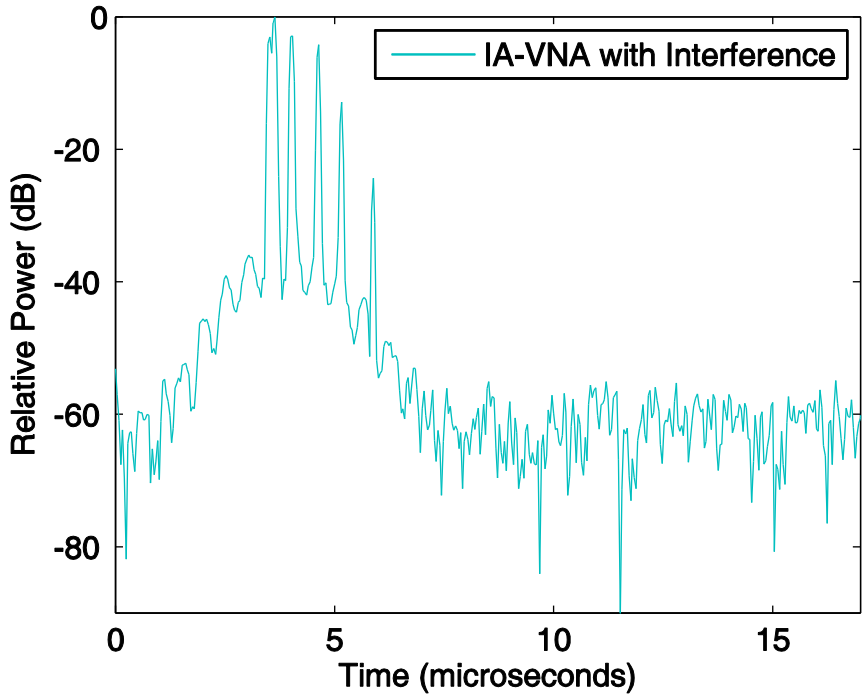


Figure 33 - CIR produced by interference-aware VNA with short-burst interference present

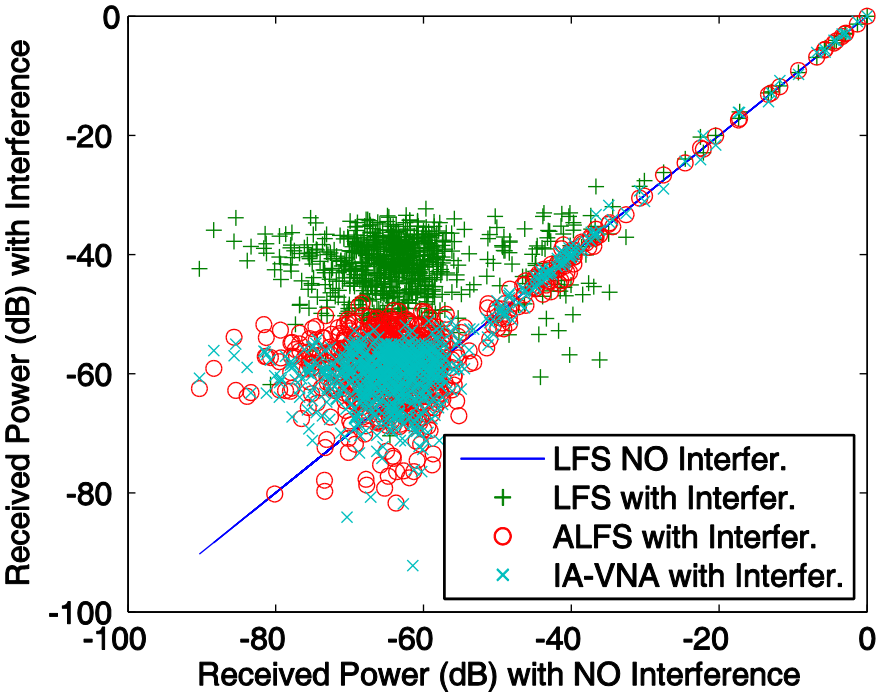


Figure 34 - Residual CIR values produced by different VNA techniques

The devastating impact of short-burst interference on measurement results when no mitigating action is taken are clearly shown in the measurement results. The traditional single LFS lost about 30dB of dynamic range in the CIR due to interference and the averaged LFS lost about 10dB dynamic range due to interference. The interference-aware VNA outperformed the other measurement techniques, but still incurred a penalty of a few dB reduction in CIR dynamic range.

*Measurement Time***.** A series of the interference-aware VNA measurements were conducted where test parameters were adjusted to observe the effect on measurement time. The number of frequency points, the number of points at each frequency, the IFBW, and the level of spectrum occupancy are the parameters that influence the overall measurement time. It is apparent that the number of frequency points and points at each frequency are multipliers of the IFBW time and spectrum occupancy wait time. In real world conditions, spectrum occupancy is an uncontrolled parameter and cannot be reduced. The other parameters that are controllable should be optimized for each use case.

The IFBW can be adjusted to reduce the VNA measurement dwell time, and whatever reduction in measurement time that can be achieved will be further multiplied by the total number of measurement points. Reducing the VNA dwell time by 1ms when there are 801 frequency points and 30 points at each frequency will save 24.03 seconds. The measurement time equations provided in the concept section can be used to determine how much time will be saved by reducing the single point measurement time, t_m. Figure 8 in Chapter 3 Section 4 provides actual values for t_m when using the E8362C VNA and shows how they differ from commonly used approximate calculation.

The recorded measurement times while operating the interference-aware VNA were drastically longer than the predicted measurement times. The surprisingly large difference came from a factor present in this implementation that is not present in an ideal implementation, instrument control communication overhead. Sending SCPI commands over the GPIB bus to configure both the VNA and SA at each frequency point added up to be the most significant contributor of measurement time. Over 80% of the measurement time can be attributed to instrument control communication overhead where SCPI commands are sent and measurement data is transferred. The best way to reduce measurement time of this

implementation is to reduce the number of frequency points. Reducing the number of points collected at each frequency also has an effect, but it is not nearly as significant in this implementation. The relationship between number of frequency points and number of points at each frequency is plotted in Figure 35. Doubling the number of frequency points doubles the overall measurement time, while multiplying the number of points at each frequency is only incremental due to the configuration of the implementation. Eliminating the instrument control communication overhead would bring measurement times closer in line with the calculated ideal implementation.

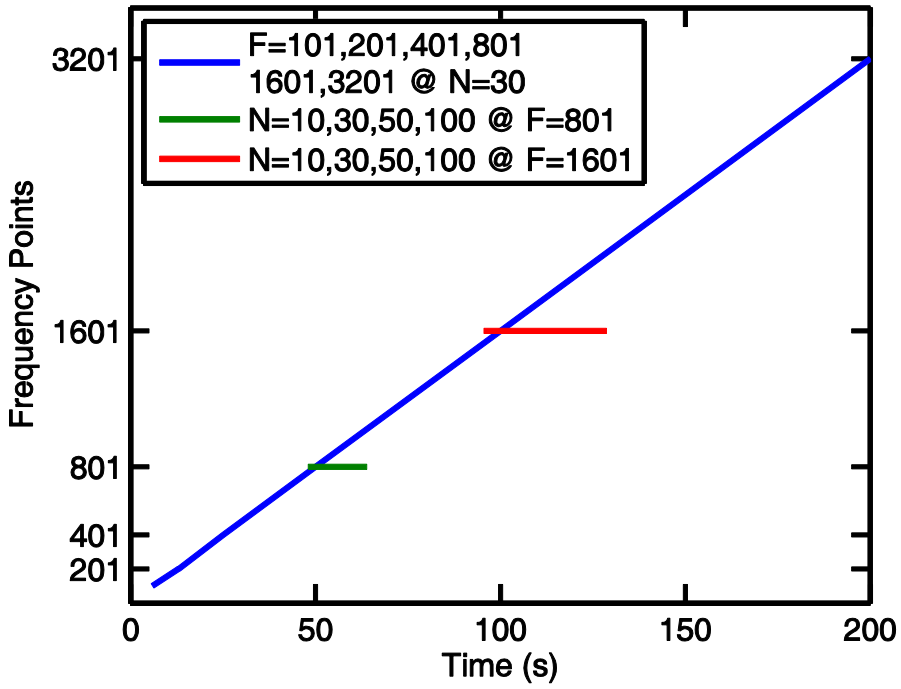


Figure 35 - Interference-aware VNA measurement times as a function of measurement points

4.5.2 Impact on Primary Users

Test Setup. The impact of the VNA on primary users is an important performance metric of the interference-aware VNA, and the results will differ when operating in different frequency bands that are occupied by different wireless services. In the case where the PU is generating short-burst interference, there is a high likelihood that the VNA will cause some harm to the PU. We referred to IEEE 1900.2-2008 as we created a test setup where the impact of the interference-aware VNA on primary users could be quantified by a measurable metric.

The impact of the interference-aware VNA on PU networks was tested by creating a controlled PU network, performing VNA measurements during the operation of the controlled PU network, and measuring the reduction in throughput of the PU network while the VNA was operating. The controlled PU network used for testing consists of two Cisco Aironet 1200 access points configured as a point-to-point wireless bridge with a computer connected to each. Each computer runs iperf throughput software to generate traffic over the wireless bridge and measure the throughput achieved by the link. A diagram of the test setup is provided in Figure 36 and a photo of the test setup is provided in Figure 37. First, throughput measurements are conducted without the operation of the VNA to establish a baseline throughput value. Then throughput measurements were conducted while 1) operating the VNA in traditional linear frequency sweep mode on the same channel as the wireless bridge, and 2) operating the VNA in interference-aware mode on the same channel as the wireless bridge.

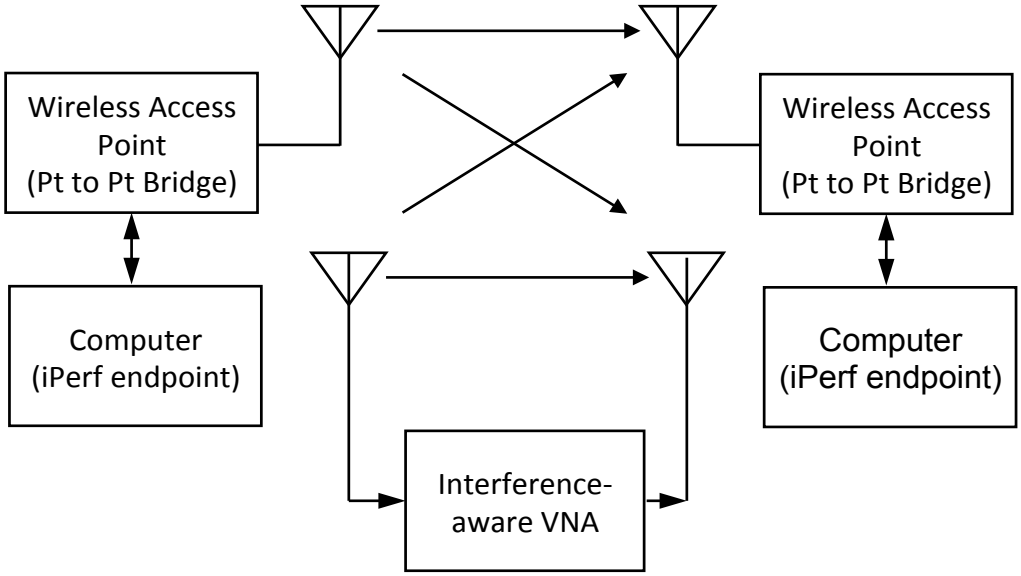


Figure 36 – Diagram of test setup for measuring impact of interference-aware VNA on primary users

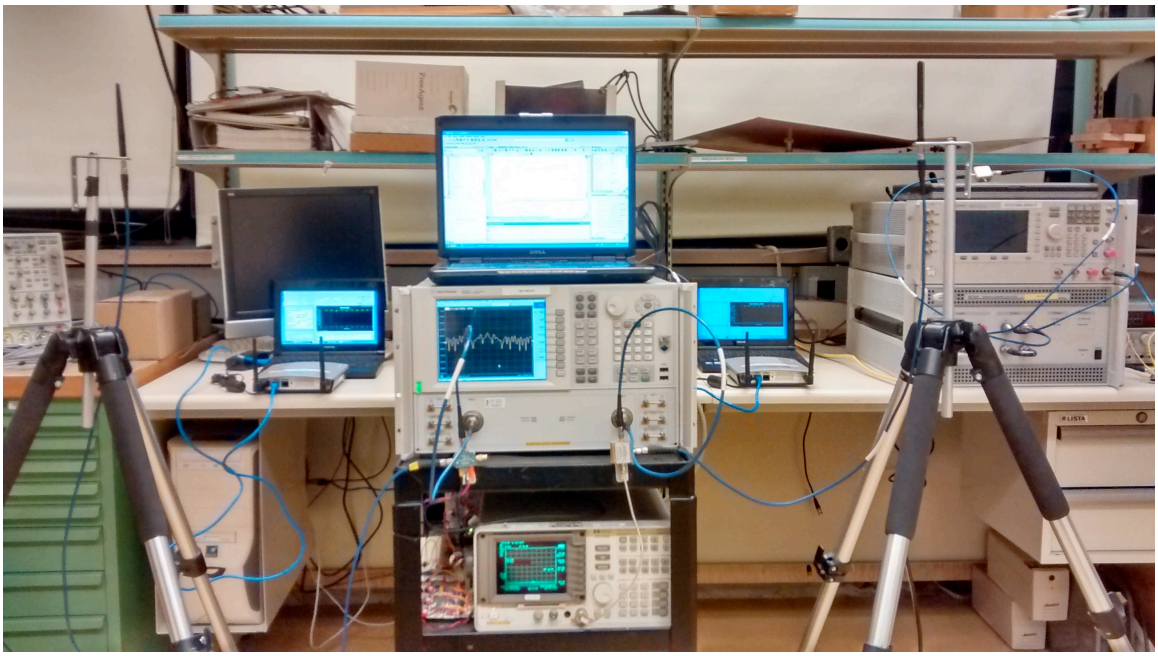


Figure 37 - Photo of test setup for measuring impact of interference-aware VNA on primary users

Impact on Primary Users. The VNA parameters with potential impact on primary users include the transmit power level, the IFBW and the total number of frequency points. Stronger VNA transmissions emitted near primary user receiver locations will cause more severe interference. The VNA dwell time, which is controlled by the IFBW setting, determines the length of the VNA stimulus signal. As the VNA dwell time increases, the probability that a short-burst interference event will occur during that transmission also increases. The total number of measurement points the VNA needs to collect determines how many transmissions are sent that can possibly cause interference. As the number of measurement points increases, the number of interference events will increase, even though the probability remains the same. Minimizing VNA dwell time and number of measurement points is the best way to reduce interference caused to primary users.

The measured primary user reduction in throughput caused by the interference-aware VNA is shown in Table 2. The average reduction in throughput across several measurements taken with varied primary user parameters was about 6.5%. Even though a 6.5% reduction in throughput is noteworthy, the nature of throughput measurements cause a worst-case scenario in terms of spectrum occupancy, and it is expected that the impact would be less severe in more ordinary spectrum occupancy conditions.

Table 2 - Primary user throughput reduction cause by VNA measurements

	54Mbps Source: 5 dBm				12Mbps Source: 5 dBm			
	Int. Power: 15dBm		Int. Power: 7dBm		Int. Power: 15dBm		Int Power: 7 dBm	
Test Num	LFS (Kbps)	IA-VNA (Kbps)	LFS (Kbps)	IA-VNA (Kbps)	LFS (Kbps)	IA-VNA (Kbps)	LFS (Kbps)	IA-VNA (Kbps)
1	21432	20175	21589	20094	8380	7839	8157	7804
2	21587	20428	21085	18392	8074	7841	8384	7736
3	21410	19946	20928	19421	8179	7821	8373	7531
4	21906	19636	20596	19136	8199	7762	8092	7677
5	20995	19206	20454	20286	8101	7745	8166	7817
6	21563	19549	20727	20642	8225	6813	8129	7806
7	21687	19832	21150	17857	8170	7863	8157	7634
8	21314	20378	22303	20483	8205	7913	8144	7542
9	21388	20681	21288	20097	8186	7514	8162	7490
10	20893	20267	21840	19843	8159	7926	8166	7614
Average	21418	20010	21196	19625	8188	7704	8193	7665
Throughput Reduction		6.57%		7.41%		5.91%		6.44%

4.6 Discussion

Once again, we have demonstrated that it is possible to transform a commercial-off-the-shelf VNA into an interference-aware VNA by applying cognitive radio concepts. In this chapter, we have focused on the case when the duration of the primary users' transmissions is less than that of the VNA measurement dwell time. In such cases, there is a high probability that latent transmissions by primary users will corrupt the measurement point but can't be as reliably detected as in the long burst case. We have proposed that multiple sweeps be collected and either linear averaging or robust estimation be used to suppress the interference. The latter was found to be more effective and is our recommended approach.

We implemented a proof-of-concept demonstrator and transformed a Keysight (Agilent) PNA into an interference-aware VNA by adding: 1) a spectrum-sensing receiver, 2) suitable

logic for responding to state changes and triggers and initiating triggers, and 3) an external controller to configure the instruments and to oversee operation of the entire measurement system. We demonstrated that a system that uses carrier sensing to reject the majority of interference and robust estimation to eliminate the interference that remains, is capable of recovering clean estimates of the channel frequency response even in the presence of moderately heavy short-burst interference. Elimination of outliers using robust estimation proved to perform better than linear averaging in all of the cases considered. The main limitation of the scheme is the time required to collect the required measurement data.

As in the previous chapter, we conclude that our scheme is practical but that the cost and effort required to realize an interference-aware VNA would be greatly reduced if vendors would make use of internal hardware and make relatively minor enhancements to the firmware and internal connections used in commercial VNAs instead. The greatest contributor to the overall measurement time of our implementation was the communication overhead associated with sending commands from the system controller to the VNA and spectrum analyzer. Lower latency proved to be more important than bandwidth for transferring commands and small sets of data. GPIB was faster than USB, which was faster than LAN.

•

Chapter 5
Conclusions and Recommendations

5.1 Conclusions

The overarching goal of this thesis has been to develop techniques that will allow VNAs to coexist with other wireless users within a frequency band of interest when conducting wireless measurements in open-area environments. In order to mitigate such interference, we have proposed techniques based on cognitive radio concepts in which uncooperative wireless systems are cast as primary users and the VNA is cast as the secondary user. In such a scheme, primary users can operate in their usual way with neither knowledge nor awareness of the wireless probing signals that are being broadcast in their band while the wireless measurements delivered to the end users are free of corruption due to interference from primary users.

In cases where the duration of the interfering signals exceeds the measurement dwell time, i.e., long-burst interference, we have shown that it is sufficient to: 1) inhibit VNA transmission and wait when an interfering signal is detected and 2) reject and possibly retake a measurement if an interfering signal is detected immediately after a measurement is completed. If the transmission duration of the interfering signals is less than the measurement dwell time, i.e., short-burst interference, the signals could corrupt the VNA measurement without being detected either before or after the measurement. We refer to these as latent transmissions. In that case, we have proposed that several channel response measurements be collected at a given frequency point and robust estimation be used to reject the outliers caused by measurement corruption. Such a technique is more effective than simple averaging.

By adding an external sensing receiver, external logic and external controller and control software to a Keysight/Agilent E8362C VNA, we implemented two types of interference-aware VNAs. The first was suitable for suppressing long-burst interference. The second was a more sophisticated version suitable for suppressing short-burst interference. We demonstrated that both systems allow pristine channel frequency response measurements to be obtained even in environments with relatively heavy interference. The presence of any interference will

block the measurement process and increase the total measurement time. When the interference is short-burst, much more additional measurement data is required in order to ensure statistically reliable results.

5.2 Recommendations for Further Work

With the concept proven and the possibility of obtaining pristine channel measurements in interference environments demonstrated, the next goal will be to reduce measurement time without sacrificing accuracy. The strategies for accomplishing this goal will involve a combination of: 1) better and more sophisticated frequency sampling strategies that reduce blocking due to primary user transmissions and allow for incomplete frequency sampling in cases where blocking times at specific frequencies are excessive and 2) better and more sophisticated statistical strategies that reduce the amount of data required to successfully conduct robust estimation. A longer-range goal is to devise a scheme that will allow the interference-aware VNA to draw conclusions about the interference environment within which it is working and to reconfigure itself appropriately. In this way, the interference-aware VNA would become a truly cognitive VNA.

Although the external logic circuits and controllers that we developed to transform a commercial VNA into an interference-aware VNA have proven the viability and practicality of the concept, the relatively cumbersome and inflexible instrument interfaces available on most commercial VNAs limit the speed and performance that can be achieved. Accordingly, there will almost certainly be significant advantages to realizing an interference-aware VNA by using one of the commercial VNA's internal reference receivers as a spectrum-sensing receiver and incorporating the relevant control software into the existing controller.

Internal implementation could also help us avoid communications and software execution overhead and thereby allow us to significantly decrease the data collection time. By reusing existing functionality within the VNA, simplify implementation and reduce the cost. Integrating such functionality into the firmware also unlocks the ability to implement modes of operation that are not practical to implement externally, such as the random sampling mode described in Chapter 3, and thereby speed up measurement times.

The industry colleagues with whom we have shared our vision have assured us that such a capability would greatly benefit the antenna, electromagnetic compatibility and wireless

communications communities. We hope that VNA manufacturers such as Keysight Technologies (formerly Agilent Technologies), Anritsu, and Rohde & Schwarz will consider introducing such interference-aware enhancements into future versions of their products in order to better serve their channel modeling, antenna design and EMC customers.

References

[1] Joint Technical Advisory Committee, *Radio spectrum conservation; a program of conservation based on present uses and future needs*. New York: McGraw-Hill, 1952.

[2] S. Heuel and A. Roessler, "Coexistence of S-Band radar and 4G mobile networks," in *15th International Radar Symposium, 2014*, Gdansk, 2014, pp. 1–4.

[3] Agilent Technologies, "Understanding The Fundamental Principles Of Vector Network Analysis." Agilent Technologies, 01-Aug-2000.

[4] Y. Cui and S. Hao, "A novel approach for radiation pattern measurement of short wave phased array," in *10th International Symposium on Antennas, Propagation & EM Theory, 2012*, Xian, 2012, pp. 398–401.

[5] S. Licul and W. A. Davis, "Ultra-wideband (UWB) antenna measurements using vector network analyzer," in *IEEE Antennas and Propagation Society International Symposium, 2004*, Monterey, CA, 2004, vol. 2, pp. 1319–1322.

[6] Chang Lian, "Indoor wireless channel measurement and analysis at 6.25GHz based on labview," in *10th International Conference on Electronic Measurement & Instruments, 2011*, Chengdu, 2011, vol. 1, pp. 252–257.

[7] T. Dammes, W. Endemann, and R. Kays, "Frequency domain channel measurements for wireless localization - practical considerations and effects of the measurement," in *18th European Wireless Conference European Wireless, 2012*, Poznan, Poland, 2012, pp. 1–8.

[8] B. D. Cordill, S. A. Seguin, and M. S. Ewing, "Shielding effectiveness of composite and aluminum aircraft, model and measurement comparison," in *IEEE Instrumentation and Measurement Technology Conference, 2011*, Binjiang, 2011, pp. 1–5.

[9] D. Senic and A. Sarolic, "Shielding effectiveness measurements in resonant enclosure using mode-tuned and mode-stirred method," in *21st International Conference on Applied Electromagnetics and Communications, 2013*, Dubrovnik, 2013, pp. 1–4.

[10] D. Micheli, A. Delfini, F. Santoni, F. Volpini, and M. Marchetti, "Measurement of Electromagnetic Field Attenuation by Building Walls in the Mobile Phone and Satellite Navigation Frequency Bands," *IEEE Antennas Wirel. Propag. Lett.*, vol. 14, pp. 698–702, 2015.

[11] G. Simpson, "Vector Network Analysis and ARFTG: A Historical Perspective," in *50th ARFTG Conference Digest-Fall*, Portland, OR, 1997, vol. 32, pp. 41–41.

[12] Agilent Technologies, "Exploring the Architectures of Network Analyzers." Agilent Technologies, 06-Dec-2000.

[13] Agilent Technologies, "Applying Error Correction To Network Analyzer Measurements." Agilent Technologies, 27-Mar-2002.

[14] National Instruments, "Introduction to Network Analyzer Measurements Fundamentals and Background." National Instruments, 05-Mar-2014.

[15] A. Henze, N. Tempone, G. Monasterios, and H. Silva, “Incomplete 2-port vector network analyzer calibration methods,” in *IEEE Biennial Congress of Argentina, 2014*, Bariloche, 2014, pp. 810–815.

[16] J. Dunsmore, “Expert Advice: Network Analyzers Not Just for S-Parameters Anymore,” *Microwave Journal*, no. March 2008, 04-Mar-2008.

[17] Agilent Technologies, “Improving Throughput In Network Analyzer Applications.” Agilent Technologies, 01-May-2000.

[18] A. McCarthy, “Instrument Bus Performance – Making Sense of Competing Bus Technologies for Instrument Control.” National Instruments, 01-Oct-2012.

[19] A. McCarthy, “GPIB and Ethernet: Selecting the Better Instrument Control Bus,” *Evaluation Engineering*, no. August 2005, Aug-2005.

[20] G. Schone, S. Riegger, and E. Heidrich, “Wideband polarimetric radar cross section measurement,” in *AP-S. Digest Antennas and Propagation Society International Symposium, 1988*, Syracuse, NY, 1988, vol. 2, pp. 537–540.

[21] Hewlett-Packard, “Radar cross section measurements with the HP8510 network analyzer.” Hewlett-Packard, Apr-1985.

[22] R. J. Langley and D. Papaioannou, “Microcomputer Controlled Antenna Radiation Pattern Measurements,” in *13th European Microwave Conference, 1983*, Nurnberg, Germany, 1983, pp. 851–856.

[23] E. T. Calazans, H. D. Griffiths, A. L. Cullen, R. Benjamin, and D. E. N. Davies, “Antenna pattern measurement using a near-field wire scattering technique,” in *Sixth International Conference on (Conf. Publ. No.301) Antennas and Propagation, 1989*, Coventry, 1989, pp. 341–344 vol.1.

[24] J. P. Blanchard, F. M. Tesche, S. H. Sands, and R. H. Vandre, “Electromagnetic shielding by metallized fabric enclosure: theory and experiment,” *IEEE Trans. Electromagn. Compat.*, vol. 30, no. 3, pp. 282–288, Aug. 1988.

[25] S. J. Howard and K. Pahlavan, “Measurement and analysis of the indoor radio channel in the frequency domain,” *IEEE Trans. Instrum. Meas.*, vol. 39, no. 5, pp. 751–755, Oct. 1990.

[26] H. Zaghloul, G. Morrison, D. Tholl, M. G. Fry, and M. Fattouche, “Measurement of the frequency response of the indoor channel,” in *33rd Midwest Symposium on Circuits and Systems, 1990*, Calgary, AB, 1991, pp. 405–407.

[27] A. Spaulding and G. Hagn, “On the Definition and Estimation of Spectrum Occupancy,” *IEEE Trans. Electromagn. Compat.*, vol. EMC-19, no. 3, pp. 269–280, Aug. 1977.

[28] ITU-R, *ITU-R Handbook on Spectrum Monitoring*, Edition 2011. Geneva, 2011.

[29] M. Wellens, J. Riihijärvi, and P. Mähönen, “Empirical time and frequency domain models of spectrum use,” *Phys. Commun.*, vol. 2, no. 1–2, pp. 10–32, Mar. 2009.

[30] M. Lopez-Benitez and F. Casadevall, “Discrete-time spectrum occupancy model based on Markov Chain and duty cycle models,” in *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2011*, Aachen, 2011, pp. 90–99.

[31] A. J. Gibson and L. Arnett, “Statistical modelling of spectrum occupancy,” *Electron. Lett.*, vol. 29, no. 25, p. 2175, 1993.

[32] ITU-R, “Recommendation ITU-R F.1337 : Frequency management of adaptive HF radio systems and networks using FMCW oblique-incidence sounding,” Sep. 1997.

[33] E. B. Bryant, G. J. Brodin, and A. H. Kemp, “High resolution channel sounder with narrowband low interference characteristics,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 42, no. 2, pp. 514–526, Apr. 2006.

[34] Q. Chen, A. Wyglinski, and G. Minden, “Frequency Agile Interference-Aware Channel Sounding for Dynamic Spectrum Access Networks,” in *IEEE Global Telecommunications Conference, 2007*, Washington, DC, 2007, pp. 3144–3148.

[35] H. Gokalp, G. Y. Taflan, and S. Salous, “In-band interference reduction in FMCW channel data using Prony modelling,” *Electron. Lett.*, vol. 45, no. 2, p. 132, 2009.

[36] D. Sugizaki, N. Iwakiri, and T. Kobayashi, “Ultra-wideband spatio-temporal channel sounding with use of an OFDM signal in the presence of narrowband interference,” in *4th International Conference on Signal Processing and Communication Systems, 2010*, Gold Coast, QLD, 2010, pp. 1–10.

[37] G. Li, J. Teng, F. Yang, A. C. Champion, D. Xuan, H. Luan, and Y. F. Zheng, “EV-sounding: A visual assisted electronic channel sounding system,” in *IEEE INFOCOM, 2014*, Toronto, ON, 2014, pp. 1483–1491.

[38] J. Mitola and G. Q. Maguire, “Cognitive radio: making software radios more personal,” *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[39] J. Mitola, “The software radio architecture,” *IEEE Commun. Mag.*, vol. 33, no. 5, pp. 26–38, May 1995.

[40] J. Mitola, “Software radios: Survey, critical evaluation and future directions,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 8, no. 4, pp. 25–36, Apr. 1993.

[41] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, “NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey,” *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006.

[42] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, “Breaking Spectrum Gridlock With Cognitive Radios: An Information Theoretic Perspective,” *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[43] T. M. Taher, R. B. Bacchus, K. J. Zdunek, and D. A. Roberson, “Empirical modeling of public safety voice traffic in the land mobile radio band,” in *7th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Stockholm, 2012, pp. 230–235.

[44] L. Mendes, L. Goncalves, and A. Gameiro, “GSM downlink spectrum occupancy modeling,” in *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications, 2011*, Toronto, ON, 2011, pp. 546–550.

[45] M. Lopez-Benitez and F. Casadevall, "Time-Dimension Models of Spectrum Usage for the Analysis, Design, and Simulation of Cognitive Radio Networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2091–2104, Jun. 2013.

[46] "IEEE Recommended Practice for the Analysis of In-Band and Adjacent Band Interference and Coexistence Between Radio Systems," *IEEE Std 19002-2008*, pp. 1–94, Jul. 2008.

[47] D. Kumar, G. Kalaichelvi, D. Saravanan, and T. K. Loheswari, "Spectrum opportunity in UHF-ISM band of 902-928 MHz for cognitive radio," in *Third International Conference on Advanced Computing, 2011*, Chennai, 2011, pp. 282–286.

[48] M. Biggs, A. Henley, and T. Clarkson, "Occupancy analysis of the 2.4 GHz ISM band," *IEE Proc.-Commun.*, vol. 151, no. 5, pp. 481 – 488, Oct. 2004.

[49] S. Geirhofer, L. Tong, and B. Sadler, "A Measurement-Based Model for Dynamic Spectrum Access in WLAN Channels," in *IEEE Military Communications Conference, 2006*, Washington, DC, 2006, pp. 1–7.

Appendix A - Long-burst Interference Arduino Board Code

The software written to control the microcontroller on the Arduino board is described in this appendix. The software was written in the C programming language and compiles when built using the Arduino Integrated Development Environment (IDE). The Arduino libraries provided with the IDE were useful for initial implementation, but were ultimately replaced with custom code that accessed the microcontroller registers directly to eliminate the extra clock cycles executed by the library functions in order to reduce latency. The software is interrupt driven by 4 events: 1) start sweep event, 2) next sweep point event, 3) timeout event, and 4) corrupt data query event.

The start sweep event occurs when the External Interrupt 0 (EXT0) pin, which is pin 2 on the Arduino Uno Board, is driven low by the Serial RTS line of the Laptop Controller. The interrupt service routine (ISR) sets the global variable *startFlag* and then exits, leaving the infinite loop in the main function to take appropriate action. When the *startFlag* is detected by the main function, a sequence of actions is taken. The first action is to reset the *count* value *targetADC* value and *corruptData* array that keep track of the current frequency point in the sweep, the expected analog voltage at the ADC when the spectrum analyzer (SA) reaches the next frequency point, and what points experienced a timeout or interference respectively. Then the SA is set up to start a new sweep by ensuring the previous sweep is complete, sending a new trigger, and pausing the sweep once it has started. All of the flags are then cleared and the first VNA measurement is triggered. The validity of the VNA measurement is checked upon completion, and flagged if a timeout occurred.

The next sweep point event occurs when the External Interrupt 1 (EXT1) pin, which is pin 3 on the Arduino Uno board, is driven low by the Trigger Output line of the VNA. The ISR sets the global variable *nextPtFlag* and then exits, leaving the infinite loop in the main function to take appropriate action. When the *nextPtFlag* is detected by the main function, a sequence of actions is taken. The first action is to wait for the VNA transmission to cease and then check if there are any external sources of interference present that may have started during the VNA measurement. If an external source of interference is detected, the frequency point is flagged as corrupt in the *corruptData* array. The frequency point *count* is incremented and the SA is swept until the ADC detects it has reached the next frequency point, and the

sweep is paused. The *targetADC* variable is set for the next frequency point and the *nextPtFlag* is cleared. Finally, a VNA measurement is triggered and the *corruptData* array flags the point if a timeout occurs.

The timeout event occurs when the Timer 1 16-bit counter overflows after the counter is started prior to sensing the spectrum before a measurement. The Timer 1 16-bit counter register overflows on the 65536th timer clock period. A clock divider of 256 is used with the 16 MHz clock frequency of the microcontroller to generate a timer clock frequency of 62.5 kHz, which generates an overflow interrupt every ~1.05 seconds. The timeout value defined at the beginning of the code *(# define timeoutValue X)* specifies how many timeout events need to occur before setting the global variable *timeout* as a flag to trigger appropriate action in the infinite loop in the main function. The Timer 1 ISR increments the global count variable *to_count* and compares it to the value of *timeoutValue* to determine whether or not to set the *timeout* flag.

The corrupt data query event occurs when a character is received by the serial port RX register. The ISR sets the global variable *txCorruptData* and exits, leaving the infinite loop in the main function to take appropriate action. When the *txCorruptData* flag is detected by the main function, the *corruptData* array is transmitted on the serial port TX line to the laptop controller who requested the data. The format of the transmitted *corruptData* array is comma separated ASCII characters terminated with a new line feed. The value of each character is either '0' or '1' indicating whether the VNA measurement was clean or corrupt respectively.

Main Function Source Code

```
#include <avr/io.h>
#include <avr/interrupt.h>

#define sweepPoints 401 // number of trace points of SA sweep
#define channelADC  0   // sets ADC channel to ADC0
#define timeoutValue 5  // sets interrupt time to 1sec * integer value 5 = 5s

// Global Variables
  volatile byte startFlag = 0;
  volatile byte nextPtFlag = 0;
  volatile byte txCorruptData = 0;
  volatile byte timeout = 0;
  byte to_count = 0;

int main(void) {
  // put your setup code here, to run once:
  // static variables
  float static stepMultiplier = 2.5575;  // 1023/400=2.5575
```

```
// variables
int count = 0;
long targetADC = 0;
int measADC = 0;
byte occupied = 0;
byte corruptData[sweepPoints] = {0};


// Configure and Initialize sweep control pin that connects to SA (HP 8590E) HIGH SWEEP IN/OUT
DDRB |= 0b00111111;  // Set pins 8-13 as outputs (PB0-PB5)
DDRD &= 0b00000011;  // Set pins 2-7 as inputs (PD2-PD7)
PORTD |= 0b00001100; // Set pull-up resistors on external interrupt pins (pin 2&3)

//  PORTB |=  _BV(PORTB2);  // set High Sweep In Out High [PIN 10 on Arduino]
DDRB &= ~_BV(DDB2);    // Set as input
PORTB &= ~_BV(PORTB2); // Turn off pull-up

// Configure and Initialize donePin that connects to PNA (Agilent E8362C) TRIGGER IN
PORTB |= _BV(PORTB0);  // set Trig Out (to PNA Trig In) high [PIN 8 on Arduino]

// Configure and Initialize sweep start pin that connects to SA (HP 8590E) EXT TRIG INPUT
PORTB &= ~_BV(PORTB3);  // set SA Ext Trig low [PIN 11 on Arduino]

// ADC Analog input pin that connects to SA (HP 8590E) has default config of ANALOG INPUT
DDRC = 0b00000000;  //Set PortC to input
DIDR0 |= 0b00111111;  // Disable digital input buffer on PORT C analog input pins

ADMUX |= 0b01000000;    // set voltage reference to AVCC (5V)
ADCSRA |= 0b00000111;  // ADC clock prescaler (16 MHz / 128 = 125 kHz) must be below 200 kHz for 10-bit sample
ADCSRA |= _BV(ADEN);    // Enable the ADC
ADMUX &= 0b11110000;    // Select ADC channel 0;

// Configure interrupt_0 pin for each negative pulse coming out of the PNA (Agilent E8362C) EXT TRIG OUT
EICRA = 0b00001010;  // Set to Int0 and Int1 to interrupt on falling edge
EIMSK = 0b00000011;  // Enable Int0 and Int1

UBRR0H = 0;
UBRR0L = 103;
UCSR0B = 0;
UCSR0B |= _BV(RXEN0);
UCSR0B |= _BV(TXEN0);
UCSR0B |= _BV(RXCIE0);

// Clear External interrupt flags
EIFR = 0b00000011;

// enable global interrupts
sei();

while(1){
  if(startFlag != 0) {
     count = 1;
     targetADC = 0;

    // Reset all variables
     // initialize corrupt data vector for upcoming sweep
     for(int i=0; i<sweepPoints; i++){
       corruptData[i] = 0;
     }

    // Move SA to first measurement point by
     // finish past sweep if incomplete
     DDRB &= ~_BV(DDB2);  // set as input
     PORTB &= ~_BV(PORTB2); // Turn off pull-up

     // send sweep trig to SA
```

```
  trigSA();

  // wait for sweep to finish
   while(((PINB &= _BV(PINB2)) >> 2) == 1);

  // wait for SA to start sweep
  while((PINB &= _BV(PINB2)) == 0){
    _delay_ms(1);
    trigSA();
  }

  // Pause sweep
  DDRB |= _BV(DDB2);      // Set as output
  PORTB &=  ~_BV(PORTB2);  // drive low

 // set target ADC value for second sweep point
  targetADC = (count*stepMultiplier);

  // RESET FLAGS
  startFlag = 0;
  nextPtFlag = 0;
  txCorruptData = 0;

 // Perform measurement at first point
  trigPNA();

  if(timeout){
    corruptData[count-1] = 1;
  }

} else if(nextPtFlag != 0) {
 _delay_us(500);  // wait for PNA to get ready for next trigger (it takes extra 100us after sending trig out)
 occupied = readSO();
  if(occupied){
    corruptData[count-1] = 1;
  }

  count = count + 1;  // increment count of triggers received

 // get initial ADC voltage reading
  measADC = readADC(channelADC);

 // move SA to next sweep point
   if(measADC < targetADC) {
   // Move to next point by setting H SWP IO high and send trigger to SA to get it moving
   DDRB &= ~_BV(DDB2);  // set as input
   PORTB &= ~_BV(PORTB2); // Turn off pull-up

   trigSA();

    // wait for sweep to get to next point
    while(measADC <= targetADC){
    measADC = readADC(channelADC);
    }

    // stop SA at current sweep point by putting SA -HIGH SWP INOUT to a low state
    DDRB |= _BV(DDB2);      // set as output
    PORTB &= ~_BV(PORTB2);  // drive low

  }

  // setup for next interrupt call
    if(count < sweepPoints) {
      // set voltage for next sweep point
      targetADC = (count*stepMultiplier);
      // RESET FLAG
```

```
        nextPtFlag =0;

        // send trigger to PNA to take measurement (negative Pulse) now that SA is at next point
        _delay_us(100);  // wait for PNA to get ready for next trigger (it takes extra 100us after sending trig out)

        trigPNA();

        if(timeout){
          corruptData[count-1] = 1;
        }
       }else if(count==sweepPoints){

        // RESET FLAG
        nextPtFlag =0;

        trigPNA();

        if(timeout){
          corruptData[count-1] = 1;
        }

}else{
        DDRB &= ~_BV(DDB2);  // set as input
        PORTB &= ~_BV(PORTB2); // Turn off pull-up
        // RESET FLAG
        nextPtFlag =0;
       }

   } else if(txCorruptData != 0){

     for(int i=0; i<(sweepPoints-1); i++){
       while(!(UCSR0A & _BV(UDRE0))){};
       UDR0 = (char)(corruptData[i]+48);
       while(!(UCSR0A & _BV(UDRE0))){};
       UDR0 = ',';
       }
       while(!(UCSR0A & _BV(UDRE0))){};
       UDR0 = (char)(corruptData[sweepPoints-1]+48);
       while(!(UCSR0A & _BV(UDRE0))){};
       UDR0 = '\n';
       txCorruptData=0;
   }
  }
return 0;
}

////////////////////////////////////////////////////////////////////////////////////////////
unsigned int readADC(byte channel) {
  ADMUX |= (0b00001111 & channel);  // select ADC channel
  ADCSRA |= _BV(ADSC);              // ADC start conversion

  while ( (ADCSRA & _BV(ADSC)) );

  byte lowerByte = ADCL;
  byte upperByte = ADCH;

  unsigned int valueADC = (unsigned int)((upperByte << 8) | lowerByte);
  return valueADC;
}
```

Appendix B – Long-burst Interference VNA Laptop Controller Software

The laptop controller coordinates the whole measurement by running a MATLAB script that configures the instruments, starts measurements, retrieves data, and processes the data. The VNA and SA are configured and controlled by sending SCPI commands over the GPIB instrument control bus. The script begins by setting user variables to values entered by the operator and creating the instrument communication objects. The VNA is configured into an initial state where calibration measurements and traditional linear frequency sweep measurement can be conducted. The script prompts the operator to acknowledge that the RF connections are correct for the calibration measurement before executing the measurement and retrieving the trace data from the VNA. Additional prompts are issued prior to each of the remaining measurements for the operator to acknowledge that the RF connections, interference generator, and channel emulator are configured appropriately for the upcoming measurement. Prior to each measurement, further instrument control commands can be issued to change the instrument configurations for the upcoming measurement. A series of measurements are conducted to capture 1) a pristine channel frequency response using a linear frequency sweep without interference present, 2) a corrupt linear frequency sweep with interference present, and 3) an interference-aware measurement in the presence of interference. Upon completion of all the measurements, calibration is applied to the collected data and further data processing is performed to generate CFR and CIR response plots.

Main Script Data Acquisition Code

```
% Parameters
startFreq = 757E6;
stopFreq = 783E6;
rfPower = -5;
IFBW = 1E3;
SA_RBW = 30E3;
SA_RL = 15; % uV units  60uV for 100kHz
sweepPoints = 401;
freqVect = startFreq:(stopFreq-startFreq)/(sweepPoints-1):stopFreq;

% create Arduino, vna and SA communication objects
ard = serial('COM11','baudrate',9600, 'timeout',5, 'inputbuffersize',900,
'requesttosend','off');
sa = gpib('ni',0,18,'timeout',5,'inputbuffersize',1700);
vna = gpib('ni',0,15,'timeout',50,'inputbuffersize',3400);

% open communication objects
```

```
fopen(ard);
fopen(sa);
fopen(vna);

% initialize VNA
fprintf(vna, 'SYST:PRES');                          % Factory presets
fprintf(vna, 'CALC:PAR:DEF My_S21, br1, 1');     % Create a measurement
fprintf(vna, 'CALC:PAR:SEL My_S21');    % Sets the selected measurement
fprintf(vna,'DISP:WIND:TRAC:DEL');      %Deletes specified  trace window
fprintf(vna, 'DISP:WIND:TRAC:FEED My_S21'); %Creates a new trace and
associates a measurement to the specified window
fprintf(vna, 'DISP:WIND:TRAC:Y:RLEV -50');  % Adjust scale ref level

fprintf(vna, ['SENS:SWE:POIN ' num2str(sweepPoints)]);  % sweep points
fprintf(vna, ['SENS:BWID ' num2str(IFBW)]);       % if bandwidth in hz
fprintf(vna, ['SENS:FREQ:STAR ' num2str(startFreq)]);   % center freq in hz
fprintf(vna, ['SENS:FREQ:STOP ' num2str(stopFreq)]);         % span in hz

fprintf(vna, 'SENS:SWE:TIME:AUTO ON');              % automatic sweep time
fprintf(vna, ['SOUR:POW ' num2str(rfPower)]);       % Set RF Output Power

fprintf(vna, 'FORM REAL,32');      % Sets the data format for data transfers
fprintf(vna, 'FORM:BORD SWAP');    % Set byte order for GPIB data transfer

% Get calibration data
    input('Setup for through line calibration, then hit enter');
    % Arm VNA for single sweep
    fprintf(vna,'SENS:SWE:MODE SING');

    % get sweep data from VNA
    calData = acquireData_f(vna);

% Get Pristine sweep
    input('Setup pristine sweep (inteference off), then hit enter');
    fprintf(vna,'SENS:SWE:MODE SING');

    % get sweep data from VNA
    data_lfs = acquireData_f(vna);

% Setup external triggering
fprintf(vna, 'TRIG:SOUR EXT');
fprintf(vna, 'CONT:SIGN BNC1,TIENEGATIVE');       %Set external trigger to
BNC 1 and rising edge
fprintf(vna, 'SENS:SWE:TRIG:MODE POINT');           %Measure 1
point/trigger
fprintf(vna, 'TRIG:CHAN:AUX1:ENAB ON');                  % Enable external
trigger on BNC IO2

% initialize SA
fprintf(sa, 'IP');                              %Instrument Preset
fprintf(sa, ['FA ' num2str(startFreq) ] );          %Start Freq
fprintf(sa, ['FB ' num2str(stopFreq) ] );          %Stop Freq
fprintf(sa, ['RB ' num2str(SA_RBW)]);             %Set Resolution
Bandwidth
% fprintf(sa, ['VB ' num2str(SA_VB)]);              %Set Video Bandwidth
```

```
fprintf(sa, 'LN');                              %Set Linear Units
fprintf(sa, ['RL ', num2str(SA_RL) 'uV']);              %Set Reference
Level
fprintf(sa, 'AT 0');
fprintf(sa, 'TM EXT');
fprintf(sa, 'DONE');
opc = fscanf(sa);

% start measurement
    % Arm VNA for single sweep
    fprintf(vna,'SENS:SWE:MODE SING');
    input('Turn on interference for IA-VNA, then hit enter');

    % Send trigger to Arduino
    ard.RequestToSend = 'off';
    pause(0.0001);
    ard.RequestToSend = 'on';
    pause(0.0001);
    ard.RequestToSend = 'off';

mode = 'SING';
while(~strcmp(mode,'HOLD'))
    fprintf(vna,'SENS:SWE:MODE?');
    mode = fscanf(vna,'%s');
    pause(0.001);
end

% get sweep data from VNA
data = acquireData_f(vna);

% Apply calibration
data_corrected = data./calData;

% get corrupt data vector from Arduino
fprintf(ard,'?');
input = fscanf(ard);
temp = regexp(input,',','split');
temp2 = cell2mat(temp);
corruptVector = str2double(temp);

index = find(corruptVector == 1);
```

Appendix C – Short-burst Interference VNA Laptop Controller Software

The laptop controller coordinates the whole measurement by running a MATLAB script that configures the instruments, starts measurements, retrieves data, and processes the data. The VNA and SA are configured and controlled by sending SCPI commands over the GPIB instrument control bus. The script begins by setting user variables to values entered by the operator and creating the instrument communication objects. The VNA is configured into an initial state where calibration measurements and traditional linear frequency sweep measurement can be conducted. The script prompts the operator to acknowledge that the RF connections are correct for the calibration measurement before executing the measurement and retrieving the trace data from the VNA. Additional prompts are issued prior to each of the remaining measurements for the operator to acknowledge that the RF connections, interference generator, and channel emulator are configured appropriately for the upcoming measurement. Prior to each measurement, further instrument control commands can be issued to change the instrument configurations for the upcoming measurement. A series of measurements are conducted to capture: 1) a pristine channel frequency response using a linear frequency sweep without interference present, 2) a corrupt linear frequency sweep with interference present, and 3) an interference-aware measurement in the presence of interference. Upon completion of all the measurements, calibration is applied to the collected data and further data processing is performed to generate CFR and CIR response plots.

Main Script Data Acquisition Code

```
% =======Load input Parameters
    inputParameters;
% == Save variables ==
    saveFolder = ['C:\RobW\CCS2\' date '\'];
    saveFigures = [saveFolder 'Figures\'];
    mkdir(saveFolder);
    mkdir(saveFigures);

% =======Open Communication with Instruments
    % Setup the connection with PNA
        pna = gpib(vendor, boardNumber, deviceNumber);
    % Configure VNA buffer size and timeout
        set(pna, 'InputBufferSize', PNAInputBufferSize);
        set(pna, 'Timeout', PNATimeout);
    % Open PNA GPIB connection
        fopen(pna);
```

```
    %Setup the connection with SA
        sa = gpib(vendor, boardNumber, SA_address);
    % Configure SA Timeout
        set(sa, 'Timeout', SATimeout);
    % Open SA GPIB connection
        fopen(sa);

% =======Create Data Variables
    dataLFS   = zeros(1,SweepPoints);
    t_LFS     = zeros(1,1);
    dataLFSi  = zeros(1,SweepPoints);
    t_LFSi    = zeros(1,1);
    avgLFSi   = zeros(1,SweepPoints);
    t_ALFSi = zeros(1,1);

% ======Perform Measurements
    % Perform Linear Frequency Sweep WITHOUT interference
        % Initialize PNA

initPNA_LFS(pna,rfPower,'My_S21',SweepPoints,IFBandwidth,centreFreq,span);

        %Collect Calibration Data
%             input('Calibration - Connect Bullet-Adaptor between cables
and then Press Enter');
%             fprintf(pna, 'INIT');
%             fprintf(pna, '*OPC?');                          % wait until
init complete
%             opc = fscanf(pna);
%             calData = acquireData_f(pna).';
%             mkdir('C:\RobW\CCS2\calData\')
%             save('C:\RobW\CCS2\calData\calData.mat', 'calData');
load('C:\RobW\CCS2\calData\calData.mat');

        input('Measurements - Connect cables to antennas/channel emulator
for pristine LFS and then Press Enter');
        disp('LFS Measurement Started');
        % measure LFS
        tic
            fprintf(pna, 'INIT');
            fprintf(pna, '*OPC?');                          % wait until
init complete
            opc = fscanf(pna);
            dataLFS(1,:) = acquireData_f(pna).';
            t_LFS = toc;
            disp('LFS Measurement Done');

    % Perform Linear Frequency Sweep with Interference
        input('Measurements - Connect cables to antennas/channel emulator
for LFS with Interference and then Press Enter');
            pause(1);

            disp('LFSi Measurement Started');
            tic
```

```
        % measure LFS
            fprintf(pna, 'INIT');
            fprintf(pna, '*OPC?');          % wait until init complete
            opc = fscanf(pna);
            dataLFSi(1,:) = acquireData_f(pna).';
            t_LFSi = toc;
            disp('LFSi Measurement Done');

    % Perform Averaged Linear Frequency Sweep with Interference
         % Initialize PNA
        initPNA_ALFS(pna,Traces);

        input('Measurements - Connect cables to antennas/channel emulator
for Averaged LFS and then Press Enter');

        disp('ALFSi Measurement Started');

        tic
        % measure average LFS
        for k=1:Traces
        fprintf(pna, 'INIT');
        fprintf(pna, '*OPC?');          % wait until init complete
        opc = fscanf(pna);
        end

        dataALFSi = acquireData_f(pna).';
        t_ALFSi = toc;
        disp('ALFSi Measurement Done');

    % Perform CCS Measurement
        % Initialize SA
            initSA_CCS(sa,SA_Start_Freq,SA_RB,SA_VB,SA_ST,SA_RL);
        % Initialize PNA
      initPNA_CCS(pna,rfPower,'My_S21',Traces,IFBandwidth,startFreq,cw);
            input('Measurements - Connect cables to antennas/channel
emulator for IA-VNA and then Press Enter');
            disp('CCSi Measurement Started');
            tic
        % call CCS measurement function
            dataCCSi =
CCSmeasure_f(pna,sa,startFreq,FreqStep,SweepPoints,Traces);
            t_CCSi = toc;
            disp('CCSi Measurement Done');

% Close communication ports
            fclose(pna);
            fclose(sa);
```