Interference Temperature Limits of IEEE 802.11 Protocol Radio Channels

John T. MacDonald
Sapient Systems Inc.
Northfield, IL 60093
Email: jtm@ece.iit.edu

Donald R. Ucci
Department of Electrical and Computer Engineering
Illinois Institute of Technology
Chicago, IL

***Abstract*—Interference temperature is a measure of how well a radio operating with a particular protocol and modulation scheme can tolerate interference in its spectrum space. We consider this tolerance metric for the IEEE 802.11 protocol for wireless networking. In experiments with off-the-shelf devices in the laboratory, we characterize the tolerance of the protocol to interference at various frequencies and power levels. Using the results of the experiment, we compute the interference temperature limit that the system will tolerate. We find that the interference temperature limit of the devices is much lower than the upper bound predicted by theory. The interference temperature limit of the protocols is not proportional to the data capacity, hence factors in the physical implementation play an important role in the robustness of the channel.**

I. Introduction

Many different communication applications and protocols share the unlicensed ISM band. A short list of examples includes: cordless phones, which utilize a narrow-band frequency modulation; Bluetooth, which utilizes a frequency hopping spread spectrum modulation; Microwave ovens, which generate broadband impulsive signals; and the well studied IEEE 802.11 wireless networking protocol. The later protocol has several variants including a low data rate QPSK modulation (the "b" variant), and a high data rate OFDM modulation scheme (the "g"variant). All of these operate in the same spectrum space: the unlicensed ISM band. In order to predict how well these disparate systems will inter-operate in the same spectrum space, it would be useful to understand to what degree each system is susceptible to noise and interference in the general case [2].

The study of interference tolerance of a particular wireless system is useful to know in terms of predicting the reliability of the communication channel and evaluating the quality of devices intended to operate under a particular protocol. It is also useful to understand the tolerance of all systems that share the same spectrum space so that new entrants to the crowded spectrum field can adapt to the environment to optimize the performance of its protocol and to avoid interfering with other, fixed wireless systems. Defining a useful metric for interference tolerance would aid the adoption of cognitive radio. One proposed metric is the interference temperature, T_I, that establishes a floor beneath which new users and protocols could be added to the spectrum space without degrading the legacy fixed channel radio systems [3].

The 2.4 GHz ISM band provides a good case study to consider the interoperability of disparate wireless systems in the same spectrum space. Although none of these communication systems reviewed was designed to accommodate the others, our experience in the Wireless Networks and Communications Research Center (WiNCOM) at the Illinois Institute of Technology is that they tend to work well together. An engineer must configure a wireless network and other devices in an elaborate scenario to force the wireless network to fail. The robustness of the system is perhaps the result of the fault tolerance designed into the wireless protocol, which has such features as error correction and collision avoidance [4]. These features also mean that it is immune to other systems that are transient in time, like Bluetooth and microwave ovens, and uncorrelated noise sources, like cordless phones [5].

In order to predict the behavior of the wireless protocol in the presence of interference, we have undertaken a simple experiment. A wireless network link is established between a client device and an access point. In between these, a narrow-band radiator is introduced at a specific frequency and constant power. This "tone jammer" is introduced in the bandwidth of the wireless channel. At several frequency points within the channel, the power of the radiator is increased until the client device disassociates from the access point. The power level at which the failure of the communication channel occurs provides a metric of the noise tolerance of the wireless device. This procedure is similar to that followed by others [6]. From this, we can compute the interference temperature limit to set boundaries for the operation of cognitive radios.

The paper is organized in the following manner: In Section II we review the concept of cognitive radios and the need for a consistent metric like the interference temperature limit to manage their operation. In Section III we review some of the features of the IEEE 802.11 wireless protocol that will impact the interference tolerance. In Section IV we review concepts of information theory that will allow us to set a theoretical upper bound on the interference temperature limit for the IEEE 802.11 protocol. In Section V we present the methods and results of our experiment to evaluate the interference tolerance of off-the-shelf (OTS) devices. In Sections VI we conclude with some remarks regarding applications of this work for interference tolerant cognitive radios.

II. Interference Temperature and Cognitive Radios

One definition for cognitive radio is [3]:

> Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e. outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g. transmit-power, carrier frequency, and modulation strategy) in real-time, with two primary objectives in mind:
>
> - highly reliable communications whenever and wherever needed;
> - efficient utilization of the radio spectrum.

To be both highly reliable and efficient in spectrum usage, cognitive radio systems must be aware of other radio channels that may interfere with its receivers. It must also be cognizant of the vulnerabilities of other radio systems to allow for maximum usage of the shared spectrum. To allow for the inter-operability of different radio users in the same spectrum space, interference temperature has been proposed as a new metric to limit the power and bandwidth available to new systems without degrading existing wireless systems [1].

The interference temperature derives from the receiver performance metric of the equivalent noise temperature

$$T_r = \frac{N}{Wk}, \tag{1}$$

where k is Boltzmann's constant, N is the noise power in the receiver circuit, and W is the receiver bandwidth. This provides a measure of the noise in the receiver and is a useful measure of the quality of the receiver. In designing radio receivers, engineers seek to minimize the receiver temperature in order to detect signals at the lowest possible power levels, thus improving the system range and signal fidelity. On the other hand, engineers design radio receivers with the knowledge that receiver quality comes at a cost and that there is a maximally tolerable noise level beyond which little is gained. Interference temperature is offered as a limit on the amount of interference that can be introduced into the receiver without degrading the channel,

$$T_i = \frac{I}{Wk}, \tag{2}$$

where I is the interference power. Contrary to the dictates of minimizing receiver temperature, an engineer would want to maximize the interference temperature limit of the receiver to tolerate the highest interference levels possible.

With a knowledge of the maximum tolerable interference temperature, cognitive radios can inter-operate with other radio systems in a reliable and efficient manner.

III. Protocol Features Impacting Interference Tolerance

The IEEE 802.11 protocol is well engineered with fault tolerance built in. On the transmitter side, there is a spectrum mask requirement intended to filter out noise from adjacent channels. On the receiver side, there is a matched filter which removes interference that may be present in the ISM band. The system incorporates a spread spectrum modulation scheme with a coding gain that reduces the impact of noise in the communication channel. The receiver also has a specification for carrier detection and clear channel assessment. This is used for collision avoidance, but may also be important in inter-operability with other transient interference sources, like Bluetooth devices and microwave ovens. The clear channel assessment functions as a "listen-before-talking" feature which prevents the radio from transmitting while the spectrum is occupied. At the network level, the protocol uses error correction and transaction control to assure integrity of the data. Such acknowledgments and repeated transmission cycles can negatively impact the actual data rates by trading off capacity for reliability, but the data quality is assured.

A. Transmit Spectrum Mask

Section 15.4.7.4 of the IEEE 802.11 specification dictates the amount of energy that a transmitter may leak into the adjacent channels. The "chipping rate" of the base-band encoded signal is 11 MHz. That means that the sampling rate is 11 MS/s and the base-band signal has an effective bandwidth of 11 MHz. A spectral mask is applied to the transmitted signal to limit the effective radio frequency energy to within 11 MHz of the carrier wave and suppressing side-lobes by -30 dBr below the peak signal power [4].

Because the signal energy is contained within this spectrum mask, the receiver can filter signals outside of this effective 22 MHz band. Any interference more than 11 MHz from the center frequency should have minimal impact on the channel.

A simple method to realize the spectrum mask is with the raised cosine filter which has the transfer function,

$$V(f) = \frac{\tau \text{sinc} 2f\tau}{1-(2f\tau)^2}, \tag{3}$$

where τ is the sampling period, the inverse of the chipping rate, $1/\tau$=11 MHz [10].

B. Clear Channel Assessment

Section 15.4.8.4 of the IEEE 802.11 specification describes the clear channel assessment (CCA) required to determine when the channel is free for transmission. Three modes of operation are defined in the IEEE 802.11 specification.

The three modes move from least interference tolerant to the most tolerant. The first mode allows that any detected interference, above an energy threshold, will prevent a CCA and restrict the device from accessing the channel. In *Mode 2*, the CCA will prevent transmission if another direct sequence spread spectrum (DSSS) signal can be detected in the presence of some competing interference. In the third mode, other interferers within the protocol and outside of the protocol can be ignored if they are judged to have no interference on the channel. It is hoped that the chip designers would incorporate *Mode 3* into their designs to maximize the performance and

the interference tolerance of their devices, but vendors rarely publish the implementation specifics.

C. Data Rate and Coding Gain

The specification has several variants, the principal difference being the data rate. New variants have been added with increased data rates. The base variant operates a DSSS scheme with a fixed data rates of either 1 or 2 Mbps using a Barker code chipping sequence. The "b" variant specifies a complementary code keying (CCK) scheme with fixed data rate of either 5.5 or 11 Mbps data rates. The higher data rate is most often seen in practice. The "g" variant specifies an orthogonal frequency domain multiplexing (OFDM) scheme with variable data rates up to 54 Mbps. It would be expected that the higher data rate protocol would exhibit greater vulnerability to interference. The probability of error for a QPSK system subjected to a tone jammer is known in [11] and is approximated as

$$P_b = Q\left(\sqrt{\frac{P}{I}\frac{W}{R}}\right), \tag{4}$$

where P/I is the signal-to-interference ratio (SIR), and W/R is the bandwidth-to-data-rate ratio, or the coding gain. A large argument for the function Q results in a small probability of error; hence, a large SIR results in a small probability of error. On the other hand, a low coding gain, results in an increased probability of error. A sufficiently large error rate would compromise the digital channel.

IV. Theoretical Limits

The tolerance of the IEEE 802.11 protocol to interference can be evaluated analytically. The wireless channel can be viewed as a communication channel subject to some noise source. The noise will cause a distortion of the signal that will degrade the quality of the received signal. This will inhibit the signal detection and symbol estimation functions of the receiver. In the general case, Shannon's theorem proscribes a maximum limit on channel capacity given a Gaussian noise source [12]. As a corollary to Shannon's theorem, we can determine the worst case signal-to-noise (SNR) ratio that a channel can sustain, and still maintain a desired channel capacity.

Shannon's Theorem is given by:

$$C \leq W \log_2(1 + \frac{S}{I}). \tag{5}$$

By applying some algebra one can determine the upper bound on the noise that the channel can sustain give a desired capacity C, a minimal signal strength S, and the channel bandwidth W, that is,

$$I \geq \frac{S}{(2^{(C/W)} - 1}. \tag{6}$$

The factor in the denominator of (6) is the noise figure that the protocol can sustain based solely on the loading factor (C/W). The numerator is the signal strength in the channel. In wireless systems, S would be represented by the minimum receiver sensitivity, the minimum signal strength that the receiver can reliably detect. From the specification, we know that the minimum receiver sensitivity is -80 dBm. From that, we can compute the upper bound on the noise limit and approximate the interference temperature.

The theoretical bounds of the interference temperature are tabulated in Table II (together with the experimental results that will addresses in the next section.) The assumptions are that the channel bandwidth W is 20 MHz (as specified in the protocol), the minimum receiver S sensitivity is -80 dBm (from the protocol), and the data rates are variable. Theoretically, the lowest data rate protocol can sustain the most interference, and has the highest interference temperature limit.

V. Experimental Results

Our experimental test bed is as follows: we set up a wireless local area network (WLAN) with a laptop computer and an access point. The separation of the devices was approximately five meters. Between the laptop computer and the access point, one meter from the laptop, an interference source was introduced using an RF signal generator. This signal generator could be controlled to vary the frequency and power of the interfering tone. The experimental method was as follows:

1) Set up the laptop and access point in associated network mode.
2) Set the access point to Channel 6 (2.437 GHz), data rate 2 Mbps.
3) Set the signal generator to start at a frequency -15 MHz below the channel center frequency.
4) Set the signal generator power to -80 dBm.
5) Wait sixty seconds for the system to stabilize. If the connection failed, record the power level and frequency as tolerance limits, increase the interference frequency by one MHz. If the frequency is not greater than the center frequency, repeat Step 4. If the connection is sustained, increase the power by 1 dBm and repeat Step 5 until it fails.

After the experiment was finished for the base 802.11 protocol at 2 Mbps and the operational envelope was established, the experiment was then repeated for the "b" protocol at 11 Mbps, and the higher data rate "g" protocol at 54 Mbps.

There are many factors that will affect the characterization of the tolerance envelope. The interference power is measured not at the device under test, the laptop computer, but rather at a nearby spectrum analyzer with its own separate antenna to sense the signal and the interfering field. Hence, power measurements approximate the power realized in the device under test. It would be ideal to test the receiver tolerance of the device under test alone; however, in this test case, the access point and laptop form a communication pair and it is difficult to differentiate which device failed. We can only conclude that the link between the two devices failed. The parameters of the room in which the experiment took place may exhibit some frequency power fading in the bandwidth in question, so it is

TABLE I
DEVICES EMPLOYED IN THE EXPERIMENT

Laptop	Dell Inspiron Model 600m, Intel(R) PRO/Wireless 2200BG chip-set.
Access Point	Linksys model WAP55AG.
Signal Generator	Hewlett Packard HP8556A RF Signal Generator
Transceiver	Down East Microwave 2304-144 Mixer/Transceiver
Antenna	Kent Electronics, 900-2600 MHz, Log Periodic Array

difficult to make general conclusions given the specific spatial arrangement of the experiment. Other outside interference was minimized to the extent possible in our low noise facility.

Because of the limitations listed, it is difficult to make general statements about the interference tolerance and the interference temperature of the IEEE 802.11 protocol from one set of laptop/access point pairs in the multitude of vendors combinations, but this provides an interesting first step. The devices utilized in this experiment are cataloged in Table I.

The graph of the interference tolerance of the three IEEE 802.11 (2.4GHz) variants is plotted in Figure 1. It shows the SIR at a particular interference frequency that resulted in failure of the channel as the interference is swept across the bandwidth of the radio channel. A high point on the curve indicates frequencies where the particular protocol variant is most susceptible to the narrow band interference source. All the protocols have a higher tolerance for noise the farther away the interference frequency deviates from the channel center frequency. This is to be expected if we assume that the receiver incorporates a bandpass filter similar to the raised cosine filter mentioned previously. Also, all the variants had a high tolerance for noise at the center frequency. This is due the fact that the protocol requires -15 dB of carrier suppression which explains the accommodation for noise at the carrier frequency.

The theory predicts that the noise tolerance is inversely proportional to the channel capacity, but this did not bear out in the experiments. Both the "g" variant at 54 Mbps, and the "b" variant at 11 Mbps have similar interference tolerance characteristics, with the "b" variant only marginally better then the higher data rate "g" variant (the theory predicts that because the coding gain of "b" is 5 times higher, the noise tolerance should be 7 dB higher). The base variant at 2 Mbps was the most susceptible to the interference (it required a higher SIR.) Since this is so much worse than the other variants, we can only infer that the electronics were optimized for the higher data rates to the detriment of the lower data rates. Thus, contrary to popular wisdom, these devices are best operated at the higher data rates for the best quality of service.

To compute the interference temperature limit for each of the different protocol variants, we determine the worst case SIR that resulted in the channel failure. With this figure we can compute the maximum tolerable interference power level relative to the minimum specified receiver sensitivity. With the highest tolerable interference power ($I = -80\text{dBm} - SIR_{\max}$) we can compute the interference temperature as stated in (2). These figures are tabulated for both of the protocol variants in Table II. Counter to our intuition, the "g" protocol has a higher measured interference temperature then either the "b" or the base protocols and thus can sustain higher interference levels. The numbers are also significantly lower then the theoretical upper bound, indicating that the channels are more sensitive to the interference than the theory would predict.

Why are the measured temperatures so much lower than then theoretical upper bounds? The receiver implementation incorporates real world components which may include lossy devices, may have poor synchronization, or may have their own high receiver temperature (these are inexpensive off the shelf components). Obviously, there are more important limiting factors to the quality of the receiver than the data rate of the channel.

VI. CONCLUSIONS

Returning to our discussion of the interference temperature metric as a tool for cognitive radio: A cognitive radio monitors its environment and makes some decision about what is the most reliable and efficient manner to operate a communication channel. In this example, if a cognitive radio is limited to operating in the unlicensed ISM band, it can detect the presence of IEEE 802.11 networks and make an accommodation for them. A radio can detect IEEE transceivers talking to each other, estimate their distance based on the received signal strength indication, and can then transmit at a level that will not interfere with the channel at the determined distance. Alternatively, if one were to operate an IEEE 802.11 channel in the presence of noise, one would select a channel that had the lowest noise, and adjust the transmit power in order to accommodate the presence of the noise.

In estimating the tolerance of devices to interference, theoretical bounds based on the protocol specification are a poor guide. The factors that most affect the tolerance of the devices are most likely peculiar to the implementation choices of the engineers rather than the dictates of the specification. We have shown the measured tolerance to noise is much lower than we could have predicted theoretically. It would be a mistake for cognitive radios to make theoretical assumptions about the noise tolerance of radio channels without more specific knowledge of the devices in question.

We have presented the calculation of the interference temperature of the IEEE 802.11 protocol with the caveat that this is a preliminary study of a single device pair. An empirical study of interference temperature would require many more combinations of OTS devices. It may be more fruitful to study the specification and the FCC regulations of the ISM band to determine what are the opportunities for cognitive radios in the unlicensed band.

In future work in the Wireless Interference Laboratory, we will consider other devices and protocols. Our focus will

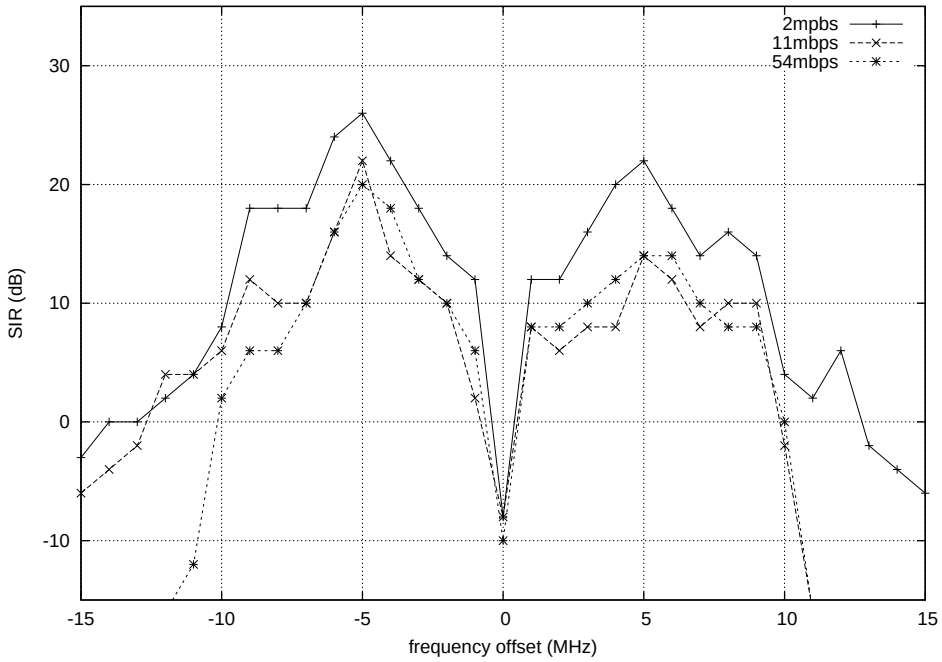

Fig. 1. Interference Tolerance of the IEEE 802.11 variants. The horizontal axis is the interference frequency offset from the center frequency of the channel. The vertical axis is the signal to interference ratio (SIR) that resulted in channel failure when the interference source was a tone at the frequency overlaying the bandwidth of the IEEE 802.11 signal. The top curve (with the worst susceptibility) is the base protocol transmitting at 2 Mbps. The "b" and "g" protocol variants exhibit better interference tolerance.

IEEE 802.11 Protocol	Worst Case SIR (dB)	Interference I (dBm)	Interference I (watts)	Interference Temperature T_I measured (K)	Interference Temperature T_I upper bound (K)
base (2 Mbps)	26	-106	2.5×10^{-14}	91	5.1×10^{5}
"b" (11 Mbps)	22	-102	6.3×10^{-14}	230	7.8×10^{4}
"g" (54 Mbps)	20	-100	1.0×10^{-13}	360	6.2×10^{3}

TABLE II
INTERFERENCE TEMPERATURE MEASUREMENTS FOR THE IEEE 802.11 WIRELESS PROTOCOL VARIANTS

continue on the ISM band which provides a fertile incubator for new inter-operative radio systems.

ACKNOWLEDGMENT

The authors would like to thank our associates in the Wireless Interference Laboratory for their encouragement and assistance.

REFERENCES

[1] Federal Communication Commission, "Spectrum Policy Task Force," Report ET 02-135, November 2002

[2] D.A.Roberson, *et.al*, "Spectral Occupancy and Interference Studies in Support of Cognitive Radio Deployment", **Proceeding of the IEEE Workshop on Networking Technologies for Software Defined Radio Networks**, Reston VA, USA, Sept. 25 2006

[3] S.Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications", **IEEE Journal on Selected Areas in Communications**, vol.23, no.2, pp.201-20, February 2005

[4] **ANSI/IEEE Std.802.11, 1999, Edition (R2003)**

[5] T.M.Taher, *et.al.*, "Characterization of an Unintentional Wi-Fi Interference Device - The Residential Microwave Oven", **Proceedings of the IEEE Military Communications Conference**, Arlington, VA, USA, October 23, 2006

[6] K.Pietikainen, *et.al.*, "IEEE802.11G Tolerance to Narrowband Jamming", **Proceedings of the IEEE Military Communications Conference**, Baltimore, MD, USA, October 18, 2005

[7] Y.M.Shobowale and K.A.Hamdi, "Interference Characterization in the Unlicensed Band", **IEEE Communication Letters**, vol.10, no.6, pp. 450-3, June 2006

[8] E.S.Sousa, "Performance of a Spread Spectrum Packet Radio Network Link in a Poison Field of Interferers", **IEEE Transactions on Information Theory**, vol.38, no.6, pp. 1743-54, November 1992

[9] T.Lee, *et al*, "Spectral Singatures and Interference of 802.11 Wi-Fi Signals with Barker Code Spreading", **Proceedings of the IEEE Conference on Dynamic Spectrum Allocation**, DySpan 2005, Reston VA

[10] A.B.Carlson, P.B.Briley, J.C.Rutledge, **Communication Systems, An Introduction to Signals and Noise in Electrical Communication, 4th Ed.**, McGraw Hill, Boston, MA, USA, 2002

[11] R.L.Peterson, R.E.Ziemer, D.E.Borth, **Introduction to Spread Spectrum Communication Systems**, Prentice Hall, Upper Saddle River, NJ, USA, 1995

[12] Robert B. Ash, **Information Theory**, John Wiley and Sons, New York, 1965

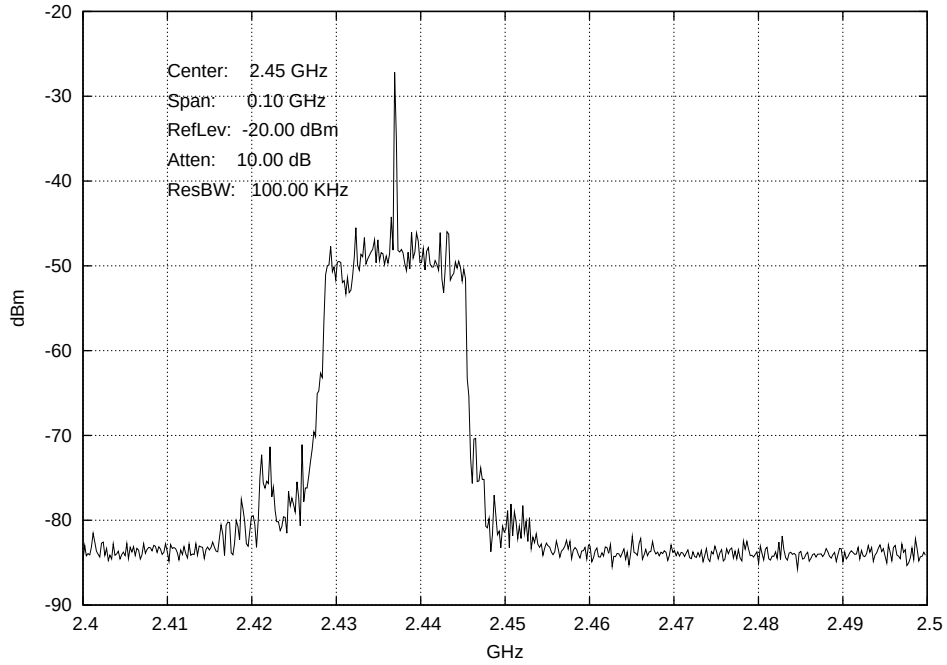

Fig. 2. A spectrum graph of a tone jammer interference overlaid on a IEEE 802.11G channel. The tone jammer corresponds to the carrier frequency and due to carrier suppression of the OFDM signal, no degradation was seen in the channel.