Voltage Controlled Oscillator for Wi-Fi Jamming

Alex Gabourie, Arjun Seshadri, Robert Wagner
Electrical Engineering Department
University of Wisconsin - Madison

Submitted for ECE 447
Professor Daniel van der Weide
December 16, 2013

Abstract

A Wi-Fi jammer is a device that interrupts data transmission in a wireless local area network. The proposed design will interfere with Wi-Fi signals using IEEE 802.11b/g/n wireless protocols and any other signal in the 2.4-2.5GHz range. To achieve the desired signal interference, a voltage controlled oscillator (VCO) was deemed to be appropriate. The final design was based upon a common base configured BJT with inductive feedback. The terminating network was designed such that the input reflection coefficient indicated a net gain, and the load network was designed to maximize power generation in the oscillator. Additional design considerations included: tuning the terminating matching network to reduce the probability of oscillation outside of the desired frequency range, and creating a Schmitt trigger to tune the varactor on the load network. The project was designed in Agilent's Advanced Design System (ADS).

Introduction

As a group, our first exposure to analysis or design of microwave transistor amplifying systems has been in ECE 447. Oscillators were a topic introduced near the end of the course and presented a mechanism to convert DC power to AC power. An interesting device, which would be easily testable and allow us to further explore oscillator design, was a Wi-Fi jammer. Building a Wi-Fi jammer presented a challenge that our group did not have experience with: designing for a band of frequencies. Up until the start of the design project, the course content was focused on tuning a circuit to work at a single frequency. To achieve oscillation over the 2.4-2.5 GHz band, the load network of the oscillator needed to be tuned continuously. Using *Microwave Transistor Amplifiers: Analysis and Design* by Guillermo Gonzalez for guidance, we discovered that a signal-fed VCO would be able to provide the continuous tuning needed for the load network.

Theory/Concepts

The main concept for operation of an oscillator is overall positive loop gain. This means that a signal will continue to grow inside the oscillating network until the transistor powering the circuit saturates. A way to visualize the operation of an oscillator is by using the S-plane of the Laplace transform. Initially, the poles of the oscillating circuit are on the right half plane, which indicate an unstable, negative loop resistance circuit. As the signal grows, the transistor cannot provide enough power and the poles move closer, and eventually to, the imaginary axis. At this point, steady oscillation has been achieved.

In a two-port negative-resistance oscillator, as shown in Figure 1, creating an overall positive loop gain entails creating a $|\Gamma_{IN}| > 1$. This is equivalent to creating a negative input resistance (R_{IN}), and having a load resistance (R_L) such that $| R_{IN}| > R_L$. Meeting these conditions creates an unstable circuit, which has poles in the right half of the S-plane. A VCO would allow us to rapidly sweep the frequency range of 2.4-2.5 GHz in order to create a poor signal to noise raito, and ultimately a high enough bit error rate to jam the signal. To get an appreciable amount power out of the oscillator when sweeping frequencies, oscillation must begin quickly. A larger $|\Gamma_{IN}|$ causes the poles to move farther into the right half of the S-plane and increases the positive loop gain, resulting in faster oscillation start up times.

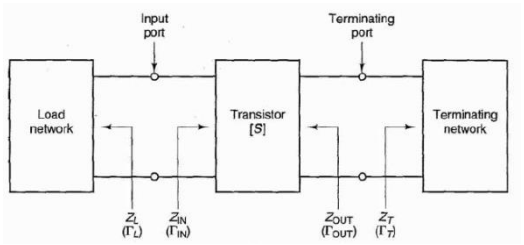


Figure 1: A diagram of a two port oscillator model

To create a $|\Gamma_{IN}| > 1$, an RF engineer may modify the circuit in several ways: choice of transistor, transistor configuration, transistor bias network, and termination network. The first three design considerations help control the S-parameters of the transistor, which is the device powering the circuit. These parameters are important as they directly define what Γ_{IN} is. Equation 1 below shows the relationship between the S-parameters and Γ_{IN}.

$$\Gamma_{IN} = S_{11} + \frac{S_{12}S_{21}\Gamma_T}{1 - S_{22}\Gamma_T} \qquad (1)$$

Some transistors are specifically designed to be used in oscillating circuits by facilitating $\Gamma_{IN}>1$. Therefore, selecting the proper transistor for your design is a critical choice, and must not be overlooked. In addition, selecting the transistor's configuration can greatly improve stability or create instability. For a BJT, a negative-resistance oscillator in the common base configuration is most effective for creating an oscillator. The configuration, as well as the feedback inductor can be seen in Figure 2.

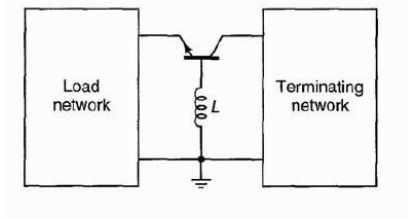


Figure 2: Common base, negative feedback oscillator configuration.

Lastly, in terms of modifying Γ_{IN} with changes on behalf of the transistor, the bias network must be appropriately set. The bias network determines the power and frequency limitations of the circuit, which modify the S-parameters.

To check if the aforementioned choices lead to a potential oscillating network, reviewing the conditions for unconditional stability can be instructive. The necessary and sufficient conditions for unconditional stability are as follows:

$$K > 1 \qquad K = \frac{1 - |S_{11}|^2 - |S_{22}|^2 + |\Delta|^2}{2|S_{12}S_{21}|}$$

where

$$|\Delta| < 1 \qquad \Delta = S_{11}S_{22} - S_{12}S_{21}$$

If these conditions are satisfied, then it is not possible to create $|\Gamma_{IN}| > 1$, and a different transistor, configuration, or bias network should be considered.

Additional control over Γ_{IN} comes from modifying the termination network. If the oscillator is terminated in a 50 Ω antenna, such that the jamming signal can be propagated, a network of lumped elements or transmission lines can be constructed to change Γ_T. Referring back to Equation 1, Γ_{IN} is dependent on Γ_T. In order to guide the selection of Γ_T such that $|\Gamma_{IN}| > 1$, stability circles may be used. On the Γ_T plane, the $|\Gamma_{IN}| = 1$ circle can be drawn and the regions of stability and potential instability can be seen visually. For an oscillator in a passive termination network, Γ_T will be restricted to the region of potential instability and $|\Gamma_T| < 1$.

For the Wi-Fi jammer, we are only concerned with the frequencies in the 2.4-2.5 GHz range. To restrict our device to only oscillating in that range, tuning of the termination network, feedback inductor, and biasing networks can reduce the number of frequencies in which $|\Gamma_{IN}| > 1$. At frequencies outside of the ideal range, $|\Gamma_{IN}|$ should be less than one to guarantee that oscillation does not occur. This way, power is being sent in the desired spectrum and devices operating on other frequencies are not affected.

Another aspect of an oscillator that must be considered is the load network, as shown in the left half of the oscillator in Figure 1. Using the approximation that there is linear variation of the negative resistance as a function of current, a conclusion about the load resistance for maximum oscillator power can be made. It can be shown that $R_L = R_o/3$, where R_o is the negative value of R_{IN} when the amplifier gain is zero, creates the maximum power in the oscillator. The other condition necessary for oscillation is for $X_L = -X_{IN}$. The problem with the last two considerations is that Z_{IN} changes with frequency which would require Z_L to change in response to Z_{IN}. R_{IN} does not change significantly over the range of frequencies so selecting an average value for R_L is sufficient to create good power in the oscillator. The same cannot be said for the reactive part of Z_{IN}. By having an appropriate LC load matching network and using a varactor to achieve dynamic capacitance, it is possible to achieve $X_L = -X_{IN}$ over the desired range of frequencies.

In the LC load matching network, the varactor is tuned using a Schmitt trigger. The Schmitt trigger uses an op-amp and the time constants of an RC circuit to create a triangle wave. For the use in the oscillator, the Schmitt trigger will be used to reverse bias the varactor over a range of voltages. As the voltage of the trigger increases, the depletion region of the pn junction varactor increases which decreases the capacitance. By choosing the correct sweeping voltages for the Schmitt trigger, correct capacitances can be achieved to meet the conditions for oscillation at all frequencies between 2.4-2.5GHz.

Experiments/Simulations

During the design process, the order in which steps were completed was similar to the order of material presented in the theory/concepts section of this paper. Selecting a transistor optimal for our application demanded a great deal of attention to a variety of parameters. The foremost of these parameters was the transition frequency of the device, or the frequency at which the transistor would operate at unity gain. To ensure that the negative resistance condition necessary for oscillation could be guaranteed, and to additionally ensure that a suitable amount of power could be delivered to the antenna load, the transition frequency needed to be well above the desired range of operation. While a high transition frequency granted optimal transistor performance, the transistor's performance at this optimal condition needed to meet a certain gain criteria for a meaningful amount of power to be broadcasted, leaving high gain being yet another important factor in decision making. Finally, our unique 'jamming' application demanded that we have a high noise output to increase the effectiveness of our device's operation. After extensive searching, a transistor that met all of these requirements was found, the BFP405 NPN BJT by Infineon Technologies. The transistor, designed specifically for oscillators, not only exceeded the required specifications with a transition frequency of 25 Ghz, a max gain of 23 dB, and a noise figure of 1.25 dB, but also possessed the additional benefits of high maximum collector current, and a low single unit cost of $.79.

After the transistor was chosen, the next step in our design was to choose the configuration of the transistor, and the corresponding DC biasing network that would best take advantage of the transistor's unstable behavior. As explained previously, the transistor configuration was chosen to be common base, with an added destabilizing feedback inductor. We opted for this arrangement for its high power gain as well as its great degree of instability when the inductor was properly tuned. An inductor value that maximized the transistor's performance at the 2.4-2.5 Ghz range was 18.25 nH, and we selected this for our design.

Next, the DC Biasing network was specified. Here, the key parameters that were optimized for were high voltage swing to prevent the formation of harmonics and low quiescent power consumption, with the additional criteria of remaining under all the absolute maximum values provided in the transistor specification sheet. Since the Collector Emitter voltage was limited to 4.5V, a quiescent value well under this point, 2V was chosen to ensure both a large and harmonic-free signal swing with a low possibility of

reaching the critical maximum. While the current limitations were relatively lax, the Q-point here was set at 5 mA primarily to limit the DC power consumption of our transistor. Power was quite an important factor since our proposal aims for the device to be powered using a mere two 9V DC batteries. Finally, since the only voltage source powering the device was a 9V battery, resistor 'voltage-dividing' networks of were chosen to ensure the proper V_{CE} and I_C for the quiescent point.

The termination matching network was designed in attempt to maximize the power delivered to the 2.4-2.5 GHz band of frequencies. Here, the key design challenge was band limiting the power that was output by the transistor to ensure that the frequencies produced by the transistor could precisely be controlled and no devices outside the vicinity of the Wi-Fi range would be harmed. This was achieved after an extensive effort, where a series capacitor, a shunt capacitor, and an inductor of unique values produced a band limited output from roughly 1-4.5 Ghz. The resulting matching network can be seen in Figure 4 below. The design was then optimized to maximize the S parameters within the range of interest, to ensure that the oscillator starts-up quickly and needs less time [allows for a greater frequency with respect to our VCO triangle waveform] to output power at each specific frequency:

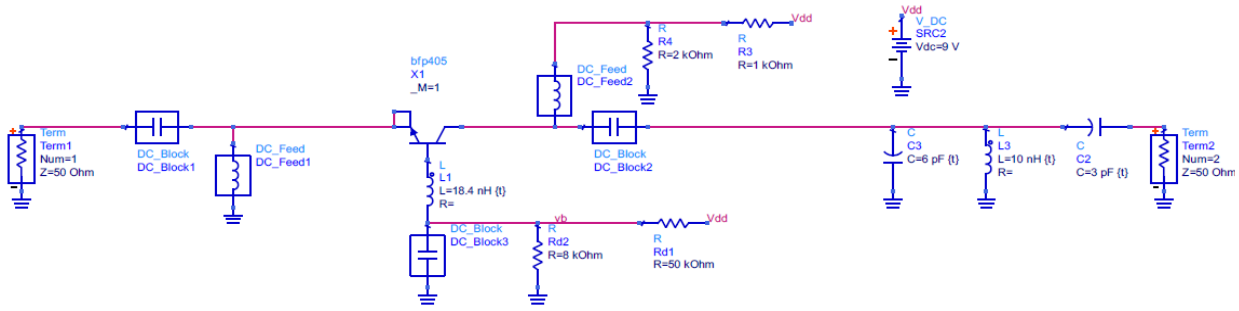


Figure 4: Termination matching network

The design we settled with produces the Γ_{IN} characteristics as seen in Figure 5 below:

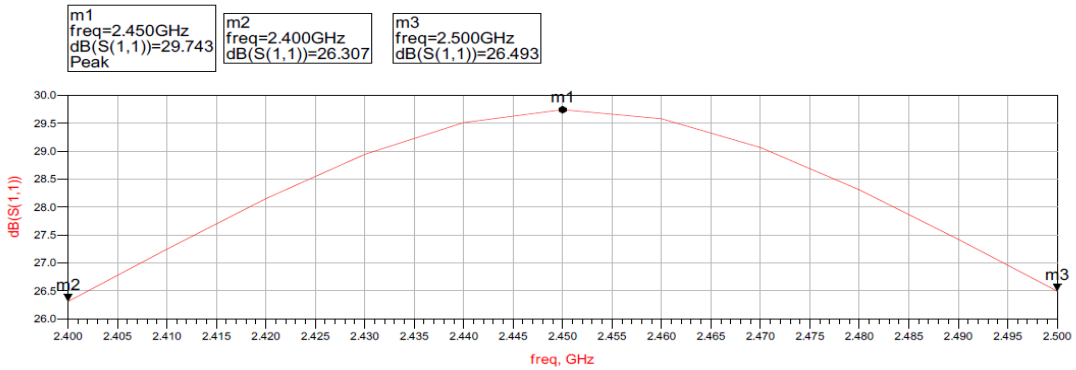


Figure 5: Γ_{IN} gain in relation to frequency.

Finally, our load network was chosen to guarantee the Barkhausen Oscillation conditions. Because our design resulted in an R_{IN} that varied insignificantly with frequency in the 2.4-2.5 Ghz range, an RLC circuit was selected for its constant R_L and its easily controllable X_L. This R_L was then chosen to be a third of the magnitude of our R_{IN} value to optimize for the power criteria detailed by Gonzalez. The capacitor within our RLC circuit was varactor-based, as explained previously, and configured with a DC network that forced it to sweep across the capacitance range plotted below in Figure 6.

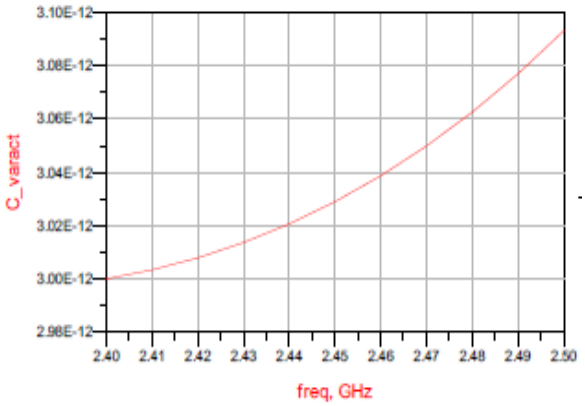


Figure 6: Varactor capacitance in relation to frequency

These capacitances resulted in $X_L = -X_{IN}$ for every frequency within our band of interest. In Figure 7, the left plot illustrates X_{IN} over our desired frequency range, and the right plot shows X_L needed for oscillation.

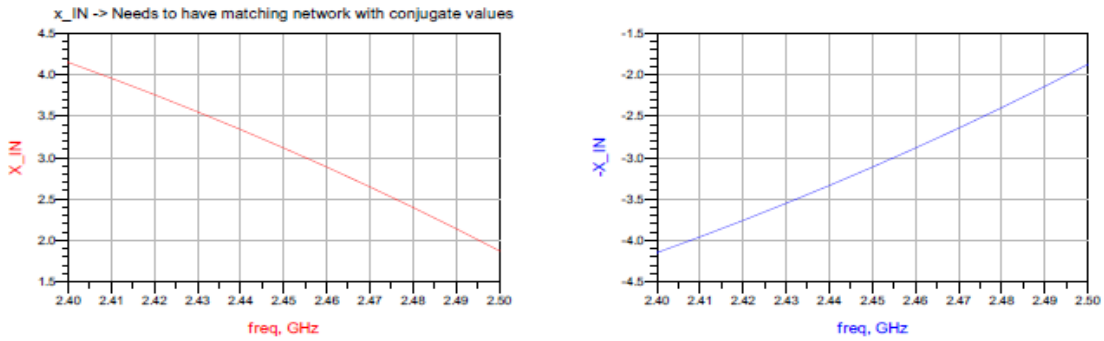
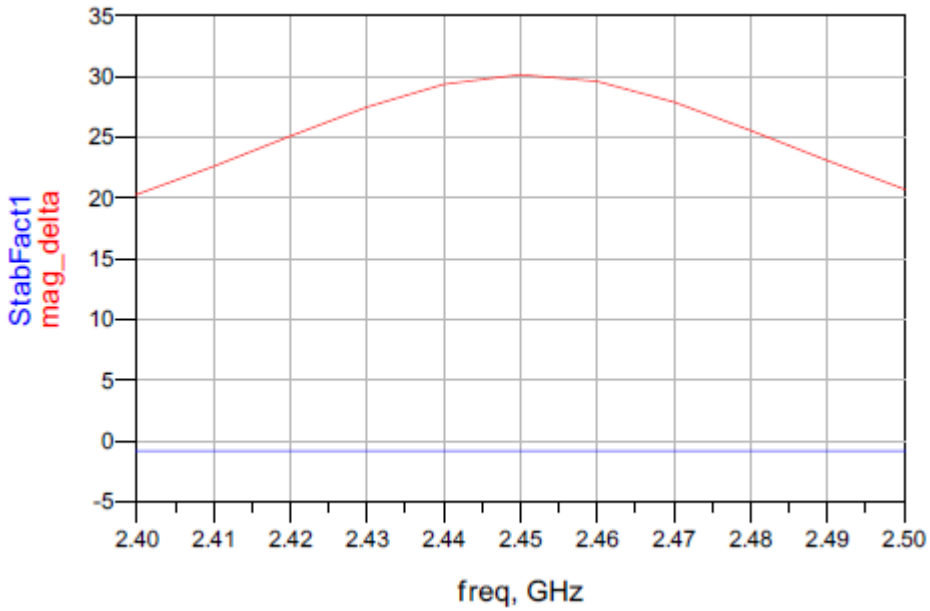


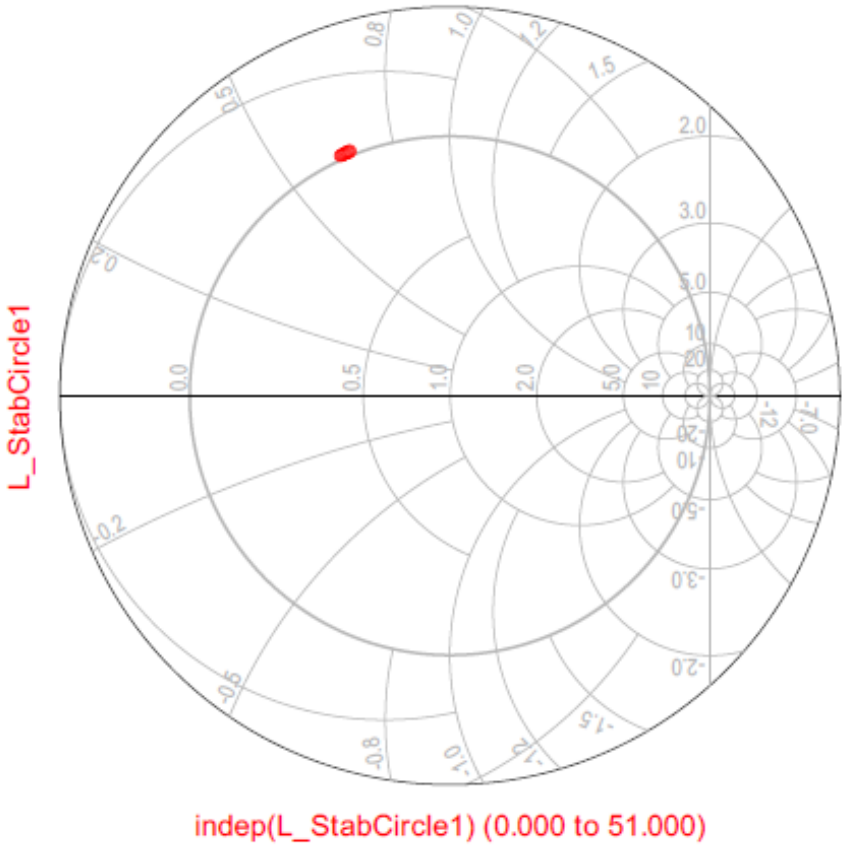
Figure 7: XL = -XIN for the 2.4-2.5GHz frequency band

Conclusion:

After extensive thought was put forth in designing every facet of our device, the Wi-Fi Jammer was optimized to be a well-functioning, band limited, low power noise source. Towards the conclusion of the design, we noted that the power output of the device may not be fully sufficient to jam signals lengthy distances away from the device, due to the lack of an additional power amplifier stage. This, however, was marked as a goal for future improvement and will be pursued in the next iteration of the device. Furthermore, a device is rather plain described in just theoretical terms, and we are determined to construct the device and test its operation in a limited and legal environment in the near future. The knowledge we gained from this project was diverse, and demonstrated to us one noteworthy fact: that the real 'RF world' is very much unlike that described in Gonzalez's text - it provides not simple numbers meant to be pushed through equations but rather a host of tradeoffs, challenges, and optimizations.

Supplemental Plots Attached: Stability graphs, Final matching network, $|\Gamma_{IN}|$ over 0-5GHz


StabFact1
mag_delta
35
30
25
20
15
10
5
0
-5
2.40
2.41
2.42
2.43
2.44
2.45
2.46
2.47
2.48
2.49
2.50
freq, GHz


L_StabCircle1
indep(L_StabCircle1) (0.000 to 51.000)

Our final design, including the matching network, is as follows: