Final Project Report : Jamming and Anti-Jamming

Anubhav Mishra
IMT2017503

Pratyush Nandi
IMT2017518

I. Overview

Radio jamming is the deliberate jamming, blocking or interference with authorized wireless communications. Intentional communications jamming is usually aimed at radio signals to disrupt control of a battle. A transmitter, tuned to the same frequency as the opponents' receiving equipment and with the same type of modulation, can, with enough power, override any signal at the receiver. Digital wireless jamming for signals such as Bluetooth and WiFi is possible with very low power.

II. Motivation

As a part of the final project for the course on Principles of Communication this is an attempt to build a transmitter-receiver system with a protocol that minimizes jamming as well as takes care of the noise in the channel introduced as White-Gaussian noise. The whole system is simulated in Matlab.

III. Building the Anti-jammer system

One of the widely used techniques of Anti-Jamming an RF channel is FHSS(Frequency Hopping Spread Spectrum). FHSS is a transmission technology where the data signal is modulated with a narrow band carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. The transmission frequencies are determined by a spreading, or hopping, code. The receiver must be set to the same hopping code and must listen to the incoming signal at the right time and correct frequency in order to properly receive the signal.

In this project, the implementation focuses on using Frequency hopping Spread Spectrum to minimize jamming effects and then also tries to minimize the interference of noise of the channel in the signal. The removal of noise is the job of the receiver.

A. Transmitter

Firstly a set of carrier frequencies are selected which is known to both the transmitter and receiver. The transmitter selects one of these randomly and transmits the signal on the selected carrier frequency.

The time signal is divided into chunks. Each time division is transmitted at a different carrier frequency from the previous time division.

The selection of the carrier frequency is based on a random algorithm which is shared by the transmitter and receiver with the same random seed. Hence, given the transmitter and receiver start at the same point of time, the jumps are same and both stay at the same frequency at any point of time.

The Matlab code provided for the transmitter first divides the time signal into chunks of 2 seconds each. Then it chooses a frequency among the given list of carrier frequency to modulate the time signal on the selected carrier frequency using the *fmmod* function provided by Matlab.

These frequency modulated time divided chunks are then appended into one signal that is received by any receiver, ready to be demodulated.

B. Receiver

The receiver works on the basic principle of demodulating the given signal. The receiver, provided with the same randomising algorithm, the list of carrier frequencies, and the random seed, hops in the same order as the transmitter. So the receiver always demodulates the modulated signal on the carrier frequency the transmitter transmits on. The same hop duration is also shared by the receiver and the transmitter.

In the code, *fmdemod* function provided by Matlab provided a good demodulated signal imitating the original signal with a little reduction in amplitude.

We then introduced White Gaussian noise in the transmitted signal. The *fmdemod* function couldn't reduce the interference of noise.

Due to this another implementation of receiver was designed. A PLL was used as an FM demodulator. The PLL traced the frequency of the transmitted signal and reduced the noise. The PLL in the presence of zero-mean White Gaussian noise represents the optimum signal demodulator as it provides the maximum a-posteriori estimate and the minimum mean square error.

In the code, a PLL was implemented from scratch to use it as an FM demodulator.

During a hop from one frequency to the other, there occurs an audible high frequency audio along with the modulated signal. To avoid this the last 75 samples and the first 75 samples of each time frame is removed. This loss isn't visible in the signal as it contributes to a very small fraction of the signal.

IV. Further Improvements

The design provided in this report reduced the interference of the a jammer using FHSS and also reduced the interference of white noise from the channel using a PLL.

Although this is an improvement from not doing anything at all, there are other ways to ensure further improvements from this model.

One of the ideas is to have a particular "check" at the end of each time frame. This helps to know whether the given channel frequency is jammed. At the end of each time frame, a sine wave of the carrier frequency can be sent with no signal riding on it. This after the Fourier transform would show up as an impulse at that frequency. If we see other "noticeable" interference from other frequencies, we can remove this time frame as a junk. So the time frame should be of very less length. A time frame of 0.1 seconds can be considered.

One way to implement this in Matlab is to pad zeros an the end of each time frame for the same duration of time frame, i.e 0.1 seconds. This would ensure enough time to check the condition of the given channel in the receiver.

In the receiver end, the job of demodulation can be divided into two parts.

1) Demodulation of the signal.
2) Checking the status of the channel

At every time frame or at every halt in the frequency before a hop, the signal is first demodulated in the given carrier frequency. Then the second half of the signal is transformed in the frequency domain. This is then checked. If it has only one noticeable impulse at the carrier frequency, the signal demodulated is considered.

Another idea is to minimize the loss in information we will decrease the size frames of channel to a minimum where it will be just more than the length of bits which we replace while overlapping. In this way whenever one of the channel gets jammed we will not concatenate those particular bits. The catch is here that there are so many channels and the length of each frame is very less so een if we don't concatenate the bits, the loss in information will be very less and another advantage is that the probability of channel getting jammed also decreases significantly.

V. Results

The audio file used is 9 seconds long while the audio file used for inter-channel interference is 6 seconds. We used an frame of 2 seconds interval. The audio-file is being sampled at 44.1 Khz. The audio is being sent in 5 different channels of lowest frequency channel at 10 Khz and highest frequency channel at 14 Khz with a difference of 1 khz between each channel. The original audio signal is up-sampled by a factor of 5 to satisfy the nyquist criterion ie $fs >= 2Xfc$. We have considered that the channel has awgn so we have added awgn with a snr of 50. Further we have also considered the case where the one of the channels gets jammed by another audio signal. This phenomenon is called inter-channel interference. So one of the channels of original audio file gets jammed and the audio which has more power will dominate the channel. Below are the graphs of audio signal, modulated audio signal and demodulated audio signal. At last we would like to thank Prof Jyotsna Bapat and Teaching Assistants for guiding us through the project.

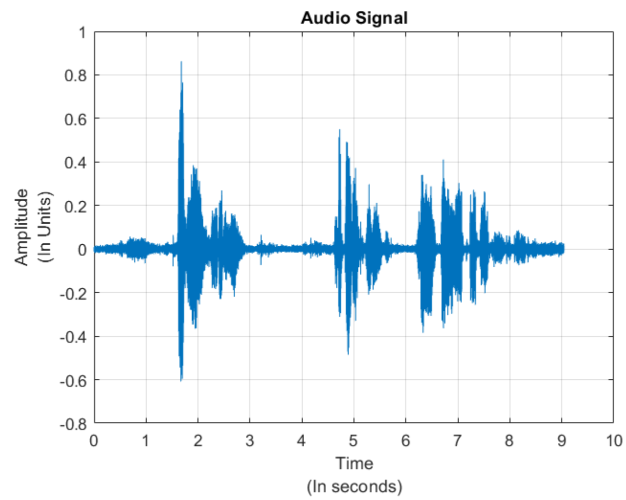

Fig. 1. Original Audio Signal

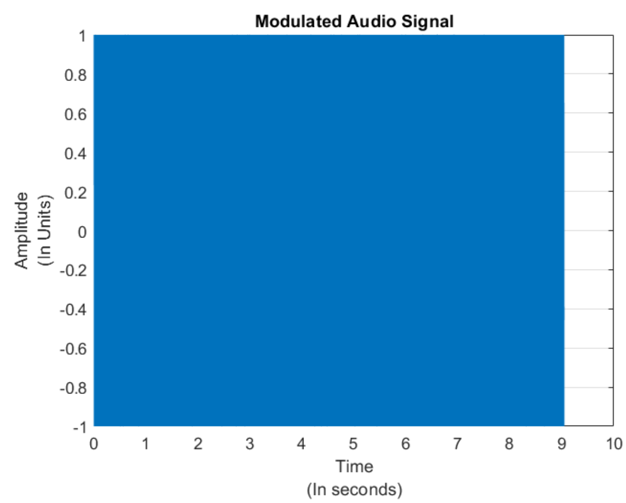

Fig. 2. Modulated Audio Signal

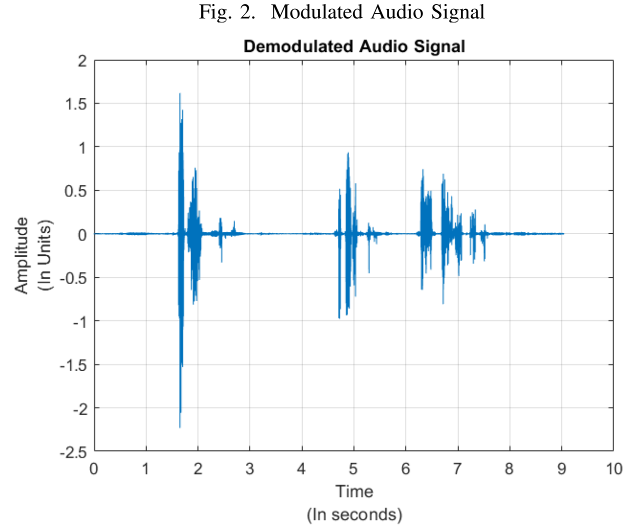

Fig. 3. Demodulated Audio Signal

VI. References

1) H.R. Swanepoel ; S. Sinha, ”Design of a frequency hopped spread spectrum (FHSS) transceiver for cellular systems”. https://ieeexplore.ieee.org/document/1406742/authors