EECS 3213

LAB 1 REPORT

NAME: MICHAEL WILLIAMS

STUDENT ID: 211087798

EECS USERNAME: MW1992

INTRODUCTION

In this lab, we explore line coding in real world examples. More specifically, we look at a given captured signal of a nonstandard infrared remote control and compare it to the established standard RC-5. RC-5 refers to a remote control communication protocol for electronic devices. It provides only a simplex direction of data, where information simply travels from the handset to the receiving unit. The specifics of the RC-5 protocol are further discussed below when comparing it to the nonstandard remote control signal contained in the WAV file.

This lab is broken into 3 different parts. In part 1, we discuss the specifics of the captured signal so that the reader may understand the characteristics of the wave. This includes deducing information such as the bit rate, the encoding of the bits, and the sequence transmitted. This information, along with the other characteristics specified below, act as the basis for drawing conclusions concerning both the standard RC-5 protocol and our captured signal in part 2 of this lab. We use the information gathered to compare our signal to standard RC-5 signals and make note of the differences and similarities, describing their properties, flaws, advantages, and other relevant technical differences. Lastly, in part 3 we use the information provided by the previous parts as well as other sources to examine the flaws of our captured signal in real life application, more specifically in terms of security. We also specify how these flaws may be corrected.

PART 1

We begin by observing the captured signal. We do so using the sound editing application, Audacity. Once open, the signal provided should look identical to figure 1. There should be 2 full periods of the signal and part of a third period present. It's worth mentioning that some prior information is provided concerning the signal. First, is that the peak to peak span of the signal is about 2 volts. Second, is that each spike in the waveform, which we will see more clearly later in the lab, refers to an infrared light flash of the transmitter's 870 nm LED.

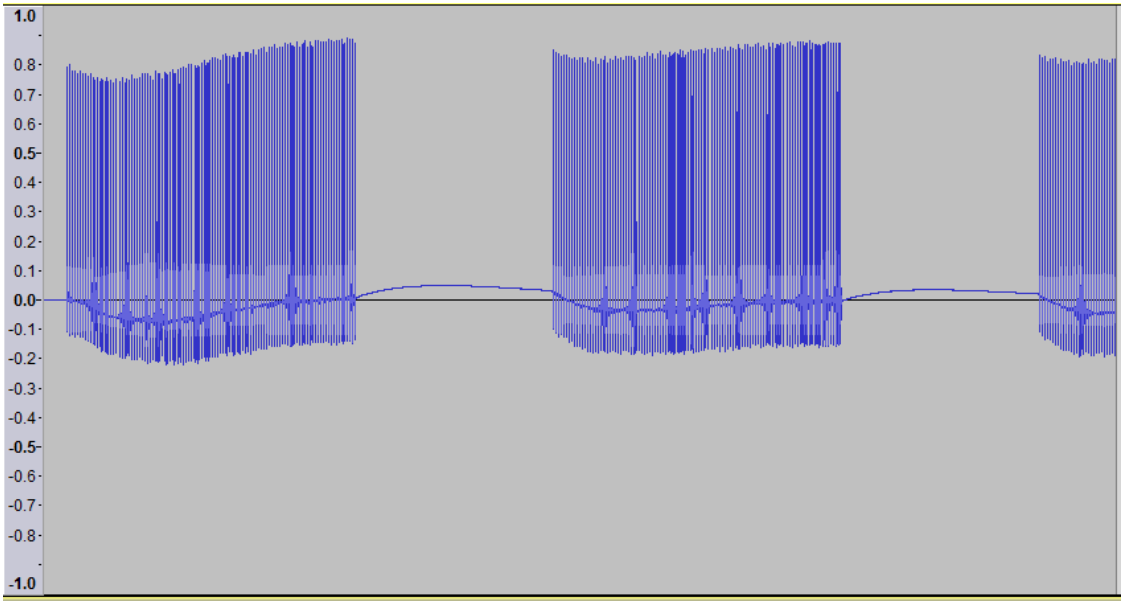

Figure 1: Entire signal from given WAV file.

We can already define important characteristics of the signal, from this level of magnification. We obtain 3 pieces of important information. The first is that the period of the signal is approximately 434 ms (milliseconds) long. The second is that the time lapse from the beginning of a period to the beginning of the subsequent period is approximately 733 ms. Last, the time between periods, or the time from the end of a period to the beginning of its subsequent period, is approximately 299 ms.

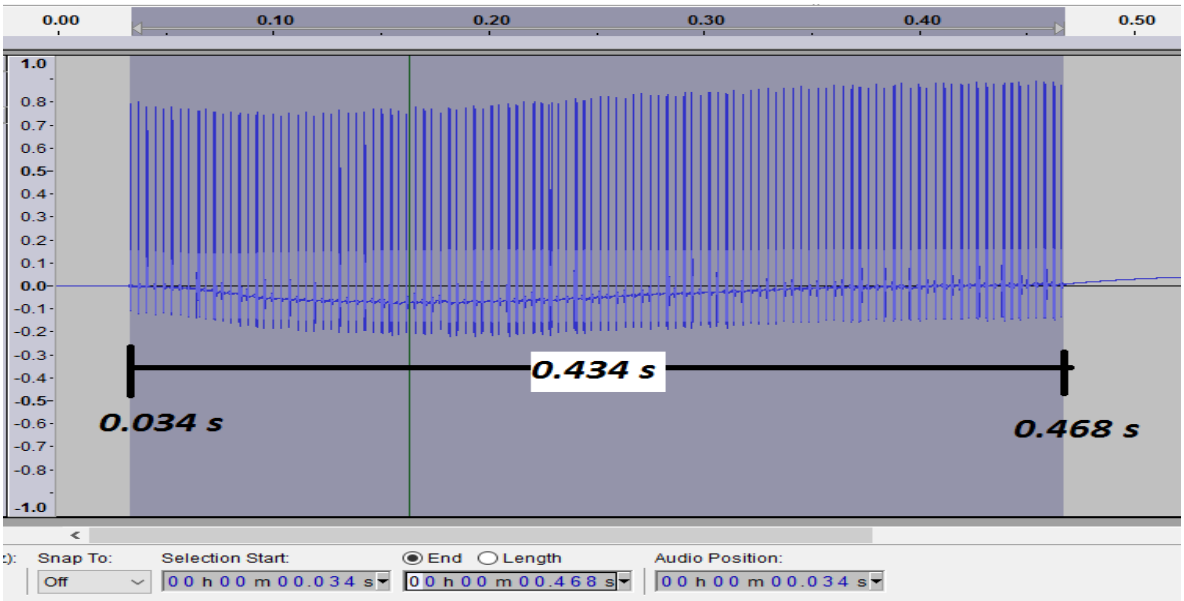

Figure 2: Signal period

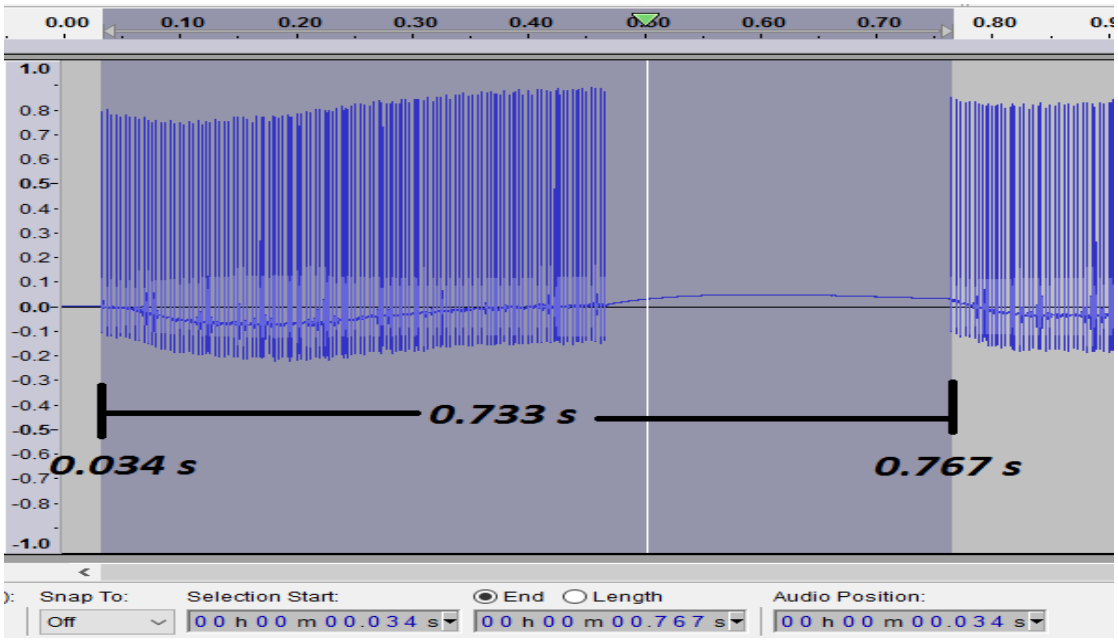

Figure 3: Time lapse from beginning of period to beginning of next period

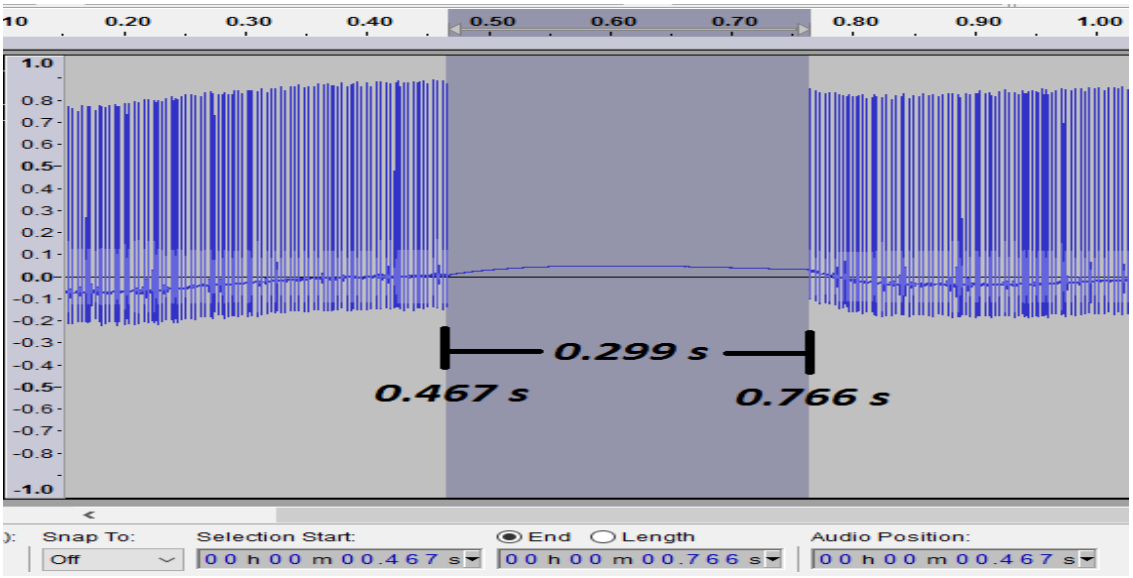

Figure 4: Time lapse between period finish and starting points

Each period contains a set of spikes or pulses. When we magnify any period, this becomes clear. We also notice a pattern amongst the pulses and for the time being, group these patterns into group A and group B. Group A will refer to a standalone pulse with no other pulses close to it. Group B will refer to two adjacent pulses that are relatively close to one another. Throughout the entire period, the pulses remain identical, no matter the group or period they belong to. Their amplitudes remain relatively the same, a claim of which is supported by the prior information given, described earlier in the lab.

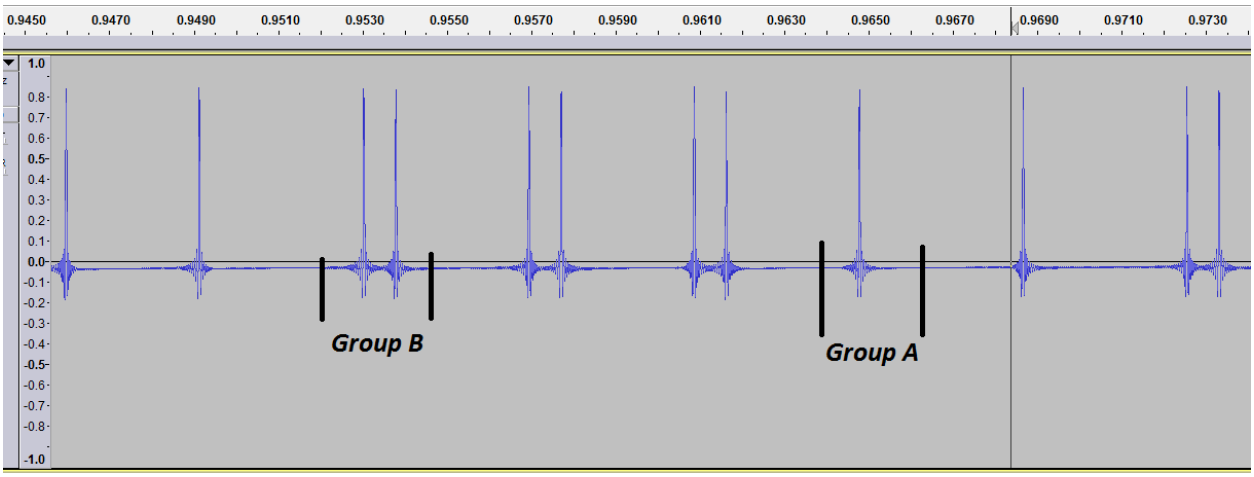

Figure 5: pulses of the signal period. The different types of pulses are described as Group A and Group B pulses.

For the remainder of the images below, it is important to note that all timing information is taken from the peak of a pulse, to the peak of an adjacent pulse. Doing so, we can more accurately describe the characteristics of each group of pulses. Furthermore, doing so for the remainder of the description will guarantee consistency in the values.

First we describe the characteristics of adjacent groups of pulses. The timespans from Group A pulse to another group A pulse, as well as the timespan of a group A pulse to the beginning pulse of group B are identical at approximately 3.85 ms. Similarly, the timespan from the beginning pulse of group B to the beginning of a group A pulse is also approximately 3.85 ms. This is important as it suggests that no matter the number of pulses in the group, the same time is allocated for each group of pulses. In other words, 3.85 ms is allowed for either a group A or B pulse to occur. This also supports the idea that there are two types or groups of pulses used in the signal.

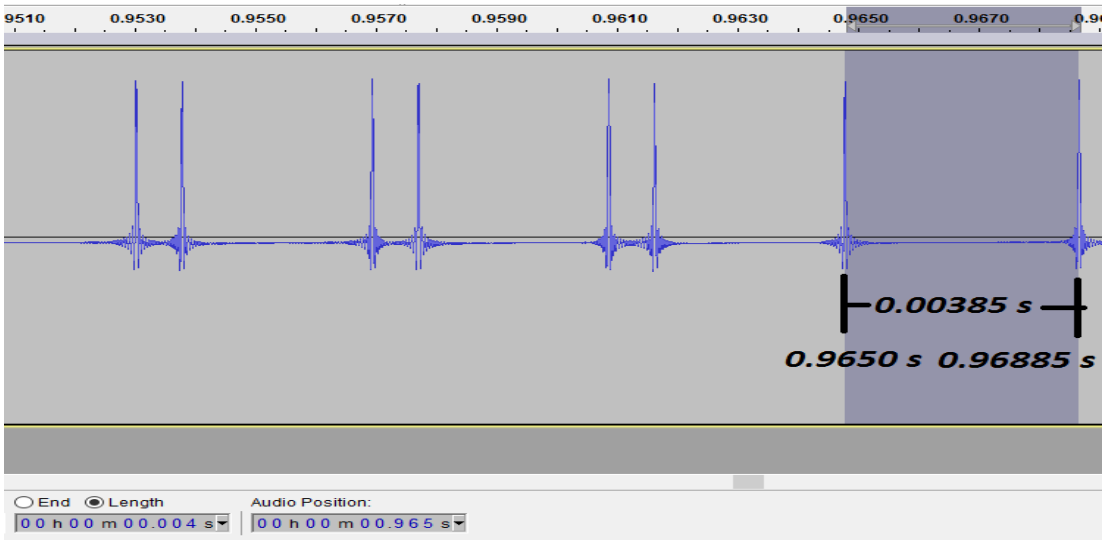

Figure 6: Timespan from group A pulse to adjacent group A pulse

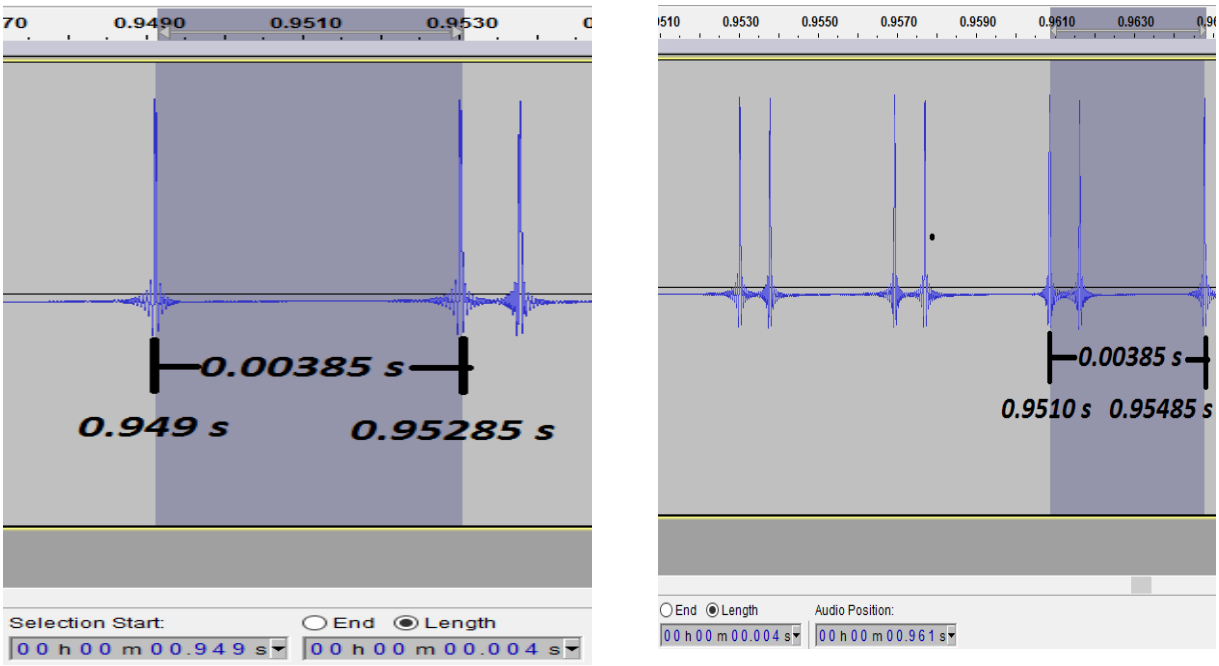

Figure 7: On the left is the timespan from a group A pulse to the beginning of the adjacent group B pulse. On the right is the timespan from the beginning of a group B pulse to the adjacent group A pulse

The time between the second pulse of group B and the group A pulse is approximately 3.2 ms. From the above, it makes sense that this distance is smaller than the distance between groups. Specifically looking at figure seven and figure 8 timespans, one would expect the distance between the group B pulses to be approximately 0.75 ms apart. The recorded timespan between both pulses of group B is approximately 0.8 ms. This matches up relatively accurately with the above values.

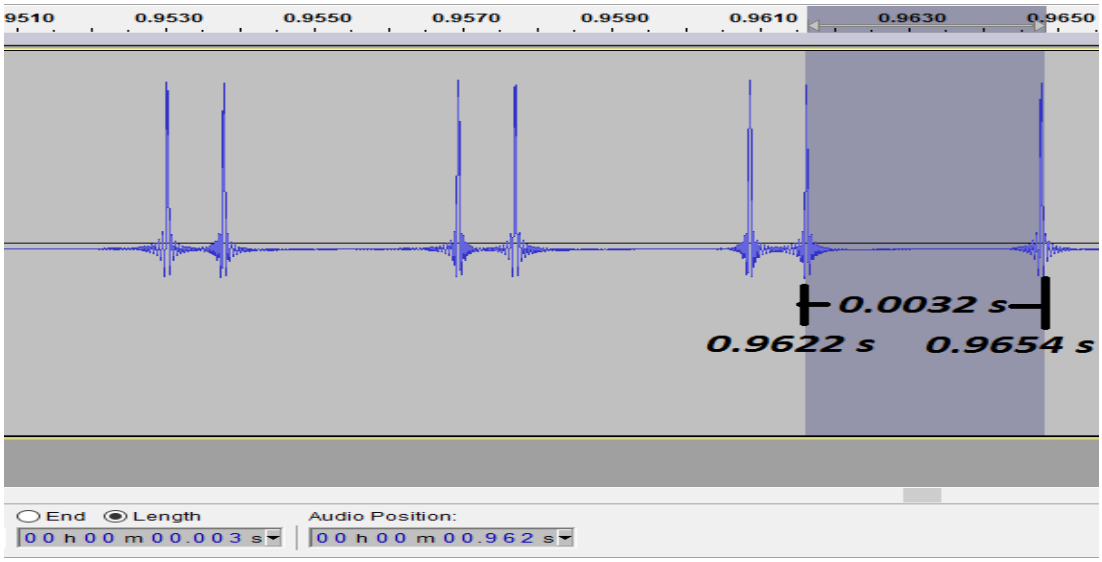

Figure 8: Timespan from the second pulse of group B to the adjacent group A pulse

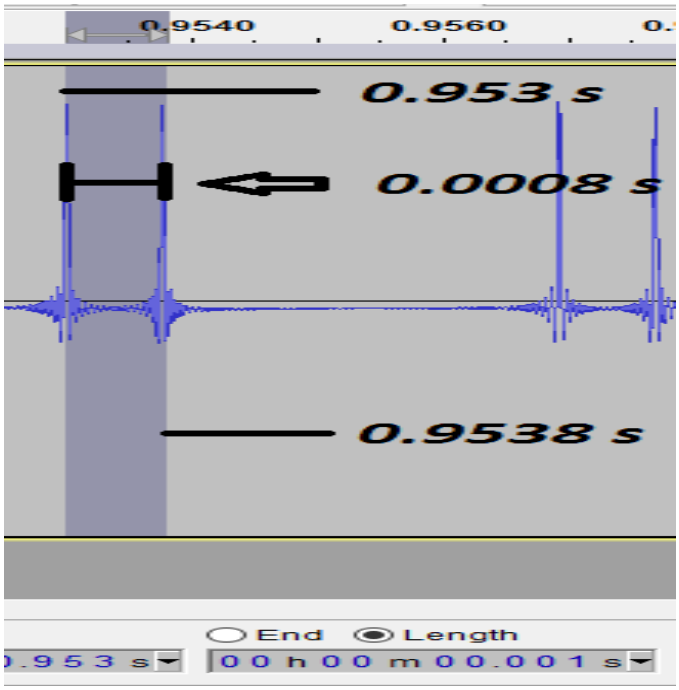

Figure 9: Timespan between the two pulses of group B

Last, we compare timespans associated directly between adjacent B groups, as to address the last timespans and to ensure that they remain consistent with the information above. The timespan from the beginning of group B to the beginning of another adjacent group B is approximately 3.85ms. The timespan from the beginning of group B to the end of an adjacent group B is approximately 4.7 ms. The difference between the two spans is approximately 0.85 ms, which is fairly consistent with the distance between the 2 pulses of a

group B, as expected. Lastly, the timespan between the second pulse of group B to the beginning pulse of an adjacent group B is approximately 3.2 ms, as expected from figure 8.

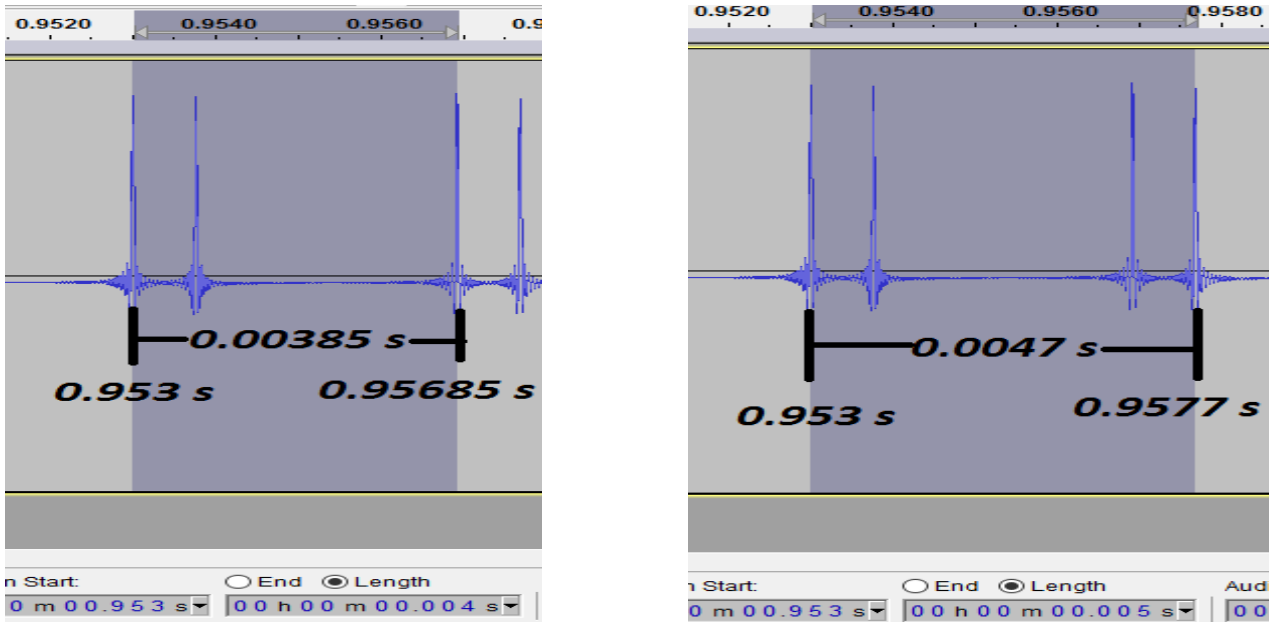

Figure 10: On the left is the timespan from the beginning of group B to the beginning of the adjacent group B. On the right is the timespan from the beginning of group B to the end of the adjacent group B.

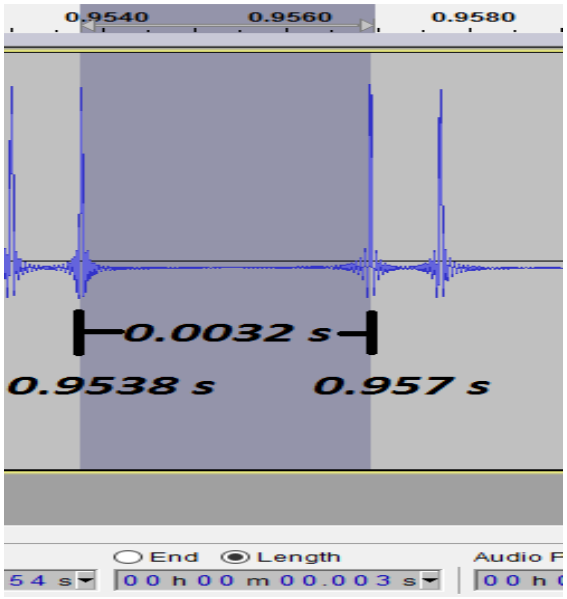

Figure 11: Timespan from the end of group B to the beginning of an adjacent group B

Lastly, we magnify the signal even more to get a better approximation of each individual spike or pulse. As previously stated, they are identical to each other, no matter the group they belong to. We can determine the effective pulse width of each wave by approximation. The effective pulse width is the approximate width of the peak to peak amplitude signal. The effective pulse width is a value of about 0.035 ms long.

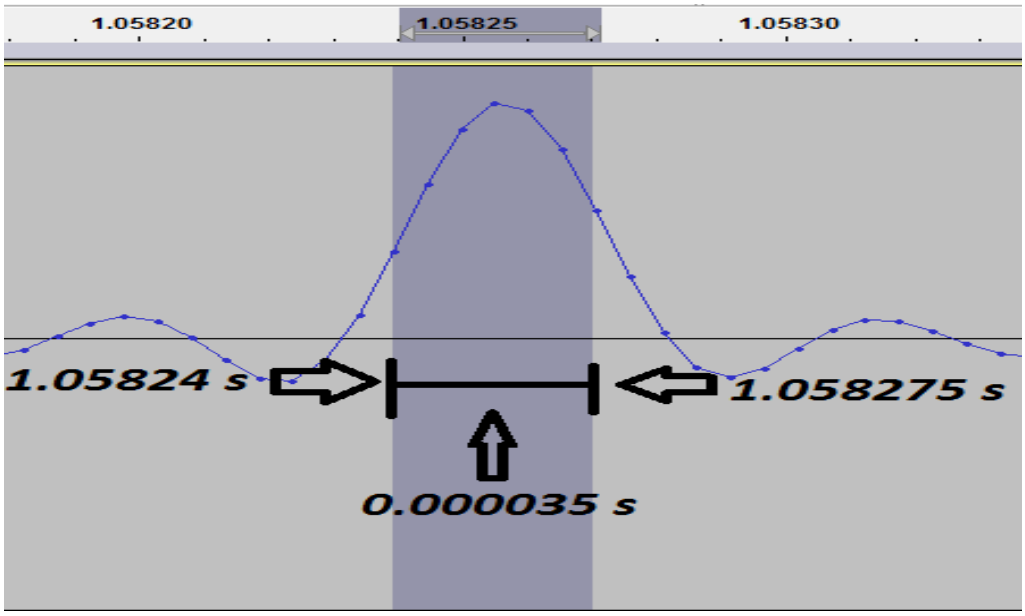

Figure 12: Effective pulse width

From all of these various timespans, we can conclude a few things. First, we have proof that the signal is comprised of the two types of pulses, group A and group B. We know this because the timing from the beginning of the first group to the beginning of the second group is the same, no matter the combination of groups used. This means that the same time is allotted for every group. This also suggests that each group conveys its own meaning. With only two types of groups, this means there are only two types of conveyed meaning. This leads me to conclude that the meanings or values conveyed are actually 0 and 1 bit values. Bursts of the same amplitudes are sent within time allocations per bit signal of 0.385 ms. In that time, depending on the pulses sent, the bit signal represents either a 1 or a 0 bit. If 1 signal pulse exists, the bit value is 0. If 2 pulses are present in the time frame, the bit signal represents a 1. In other words, group A represents a bit value of 0 and group B represents a bit value of 1. The diagram provided below describes this process

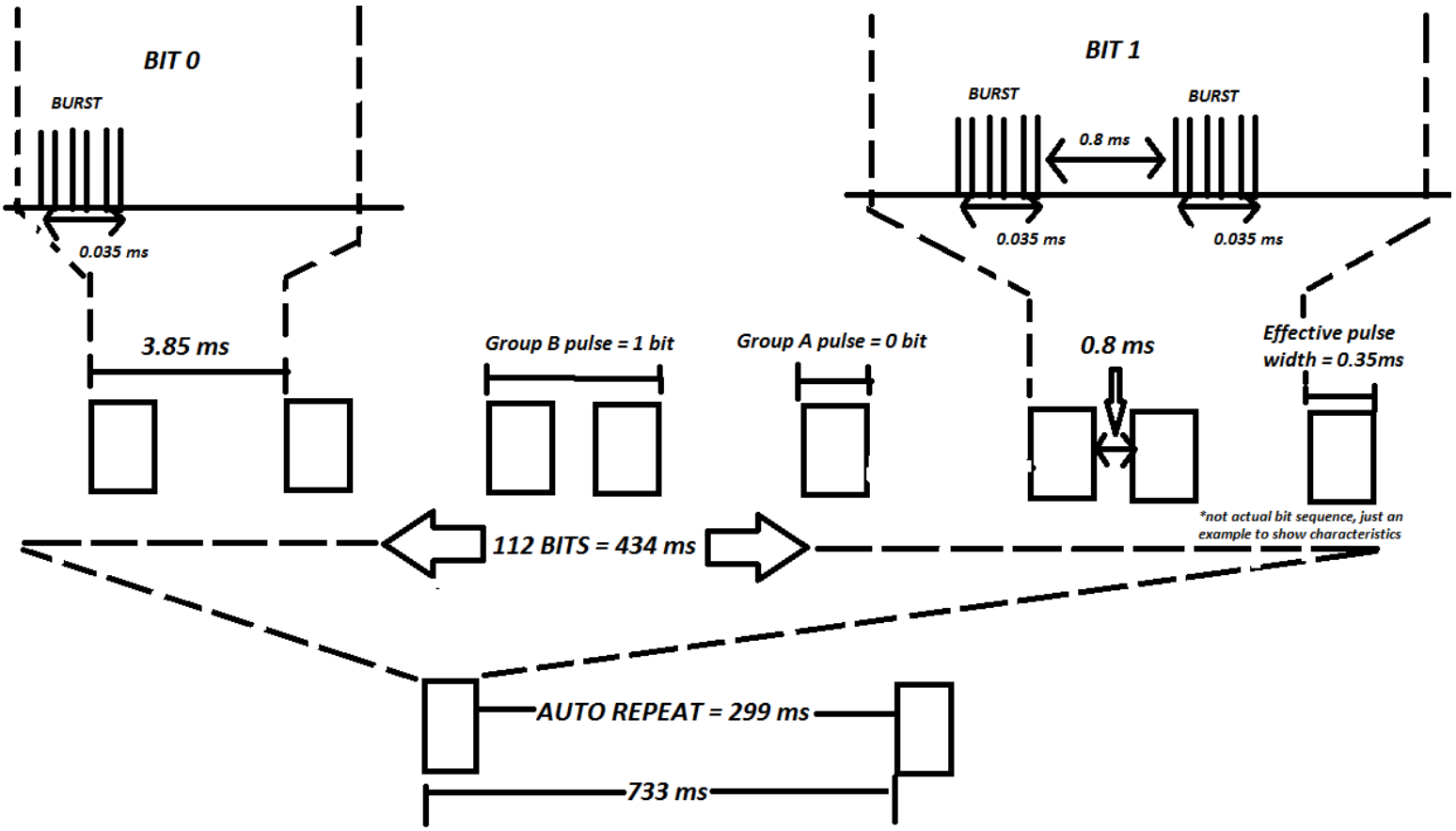

Figure 13: Diagram of captured signal protocol details

Bit rate of transmission = 1 s / 0.00385 s

= 259.74 bps

= 260 bps

The bit rate of transmission is equivalent to the number of bits sent over the course of 1 second. Each bit value is given a time frame of 0.00385 seconds. Thus, the bit rate is approximately 260 bps, or bits per second.

Each period of the signal send 112 groups of signals. In other words, 112 bits, or 14 bytes of information are transmitted per period. Following the bit encoding described above, we can translate the sequence of pulses sent, into a segment of binary code. The sequences of bits are broken into bytes so that they may more easily be analyzed:

1) 0000 0000
2) 1010 0101
3) 0000 0000
4) 0000 0011
5) 0001 0010
6) 0101 0110
7) 1110 0110
8) 0000 0000
9) 1010 0101
10) 0000 0000
11) 0000 0011
12) 0001 0010
13) 0101 0110
14) 1110 0110

Immediately we notice that the sequence of bits is actually repeated twice in each period. That is, the unique sequence is only 7 Bytes or 56 bits long. We can also see that the beginning of these sequences contain 8 zero bits, 8 bits of information, and then another 14 bits of zero. I believe this could either be for header or control information that is being sent to the receiver. Another possibility could be that the zeros represent a special sequence of idle bits and between them header information needed by the receiver. However, what is certain is that after the trail of 14 zero bits, the RC-5 sequence provided in the lab is transmitted. More specifically, the value 50325 is represented in binary by the sequence of bits that are highlighted yellow. This proves that the bit encoding is accurate. At the end of this sequence is another set of 10 bits. It is possible that these bits contain footer information needed by the receiver, or that they refer to, even partially, the end of the sequence.

PART 2

In our implementation of the bit encoding for our captured signal, I believe the encoding is based on the Manchester line coding scheme. I believe it these signals use the same premise of Manchester encoding, but take up at least double necessary signalling elements to convey the signal. The reason for this is because of the existence of 2 pulses. One pulse can be described in Manchester encoding through 2 signal elements, as such in the RC-5 protocol diagram. However, because there are two pulses in the encoding for a 1 bit, I believe the encoding for this bit uses double the signal elements to describe this change. This has the potential to double the signalling rate. However, under this scheme, there would still exist no DC component and would allow synchronization to occur, much like the RC-5 standard.

However, the line encoding of the signal captured contains many flaws, some of which are shared by the standard. First, both encoding schemes contain security issues that leave the

information sent susceptible to interception from unwanted sources. In other words, the signal transmitted may be recorded or copied. This is evident from the RC-5 Wiki page that states that a device may be used to control any brand of CD player using the RC-5 protocol, so long as it also uses an RC-5 protocol. Another problem with the captured signal is that the distance between periods is 733 ms, whereas the standard RC-5 protocol spaces their periods by only 144 ms. In addition, the period of the captured signal takes up a duration of 434 ms while carrying 112 bits, where as the standard protocol only takes up 24.9 ms while carrying 14 bits. Using this information, we can determine that the captured signal bit rate is also slower at 260 bps, whereas the standard protocol's bit rate is 562 bps. Furthermore, the time needed to convey 1 bit of information on the captured signal is 3800 microseconds, whereas the protocol takes only 1778 microseconds. Finally, our larger signal rate adds complexity to the encoding. Because the encoding is more complex, this increases the toll on the receiver's end and requires the receiver to be more sophisticated to properly receive and decode the information. This reduces the reliability of our signal.

PART 3

In terms of security, if the captured signal were to be used as an electronic key, one major flaw is that it would have the very real potential to be copied. Certain devices, in particular those using similar protocols, might be able to intercept and record the signal information. This is evident from the RC-5 Wiki page that states that a device may be used to control any brand of CD player using the RC-5 protocol, so long as it also uses an RC-5 protocol and the fact that our captured signal is similar to it. This is even more so a problem because the same sequence of bits is constantly repeated. This suggests that the receiver waits for a fixed code to be transmitted, which means that there is an even greater risk of having one's security compromised.

One could solve this issue by applying two different security features. The first of which is adapting a more security-friendly protocol such as the NEC protocol, which assigns each of the brands using it, its own unique header info. This may take away some of the functionality of the signal's protocol, but could at least reduce the potential number of devices that could be used to intercept sensitive information. Second and more importantly, one could use a rolling code implementation, instead of using the same fixed code for the receiver. This could prevent replay attacks, where someone may intercept and record the transmission for later use. Rolling codes are implemented using pseudorandom number generators, in which every time it is used; the electronic key randomly generates a new transmission sequence. The code is also encrypted to protect against any intercepting receivers. Rolling code always send out a code different from its previous one and the receiver checks to see if the code sent matches the calculated and expected code, after decrypting the transmission.