Analisador de Controle Remoto Utilizando RTL-SDR

Marcos Vinicios Pinho
<marcos.v.pinho@gmail.com>
Roberto Wanderley da Nóbrega
<roberto.nobrega@ifsc.edu.br>
Ramon Mayor Martins
<ramon.mayor@ifsc.edu.br>

Resumo- *Os controles remotos baseados em radiofrequência são largamente utilizados no dia a dia. Porém com o constante uso desses aparelhos surge a necessidade de realizar a manutenção dos mesmos. Em vista disso, é proposto um analisador de controle remoto baseado um dispositivo RTL-SDR, o qual usará a plataforma de desenvolvimento GNU Radio para criação dos blocos de processamento. O analisador tem como objetivo fornecer automaticamente informações sobre frequência de operação, taxa de transmissão, sequência transmitida e o codificador utilizado.*

Palavras-chave: GNU Radio. Rádio definido por software. Controle Remoto.

1 Introdução

Os controles remotos baseados em radiofrequência já é uma tecnologia bem consolidada há muitos anos, sendo geralmente empregados em variados sistemas de segurança, com a finalidade de travar/destravar portas, habilitar/desabilitar sistemas, etc (SUDA; LEHMER, 2004). Porém, com o uso constante desses aparelhos surge a necessidade de realizar a manutenção, ajustando a frequência de operação, a taxa de bits ou até realizando cópias do código desses dispositivos. No entanto, para realizar essas manutenções de forma correta e com a certeza de sucesso é necessário o uso de algum equipamento que auxilie e facilite o trabalho.

Atualmente existe no mercado aparelhos que realizam as medições necessárias para a aplicação dessas manutenções, como por exemplo o Analisador Digital de Controle Remoto, da empresa VTE Tecnologia Eletrônica[1], mas estes aparelhos possuem um valor muito acentuado e impossibilidade de atualizar o sistema já adquirido.

Em vista disso, é proposta a realização de um analisador de controle remoto empregando os conceitos de rádio definido por software e utilizando um *dongle* RTL-SDR (Realtek-based Software Defined Radio) de baixo custo.

O interesse em utilizar os conceitos de SDR está na substituição da tradicional implementação em hardware dos dispositivos de comunicação por uma implementação mais flexível, que faz uso de dispositivos programáveis controlados por software, como por exemplo, um computador pessoal ou um processador embarcado (SELVA et al., 2012).

[1] http://vtetecnologia.com.br

Esse dispositivo programável contém dois chips principais, um sintonizador digital e um processador Realtek RTL2832U (FANAN et al., 2015). O sintonizador mais comum é o Raphael Micro R820T, que tem um alcance de frequência entre 24 MHz e 1766 MHz (LAUFER, 2015). O RTL-SDR possui uma largura de banda máxima de 3.2 MHz, 8 bits de resolução e uma taxa de amostragem de 2.4 MS/s (MIYASHIRO et al., 2017).

Uma plataforma muito utilizada para a realização do software de controle é o GNU Radio, ela é utilizada para criação dos blocos de processamento. Essa ferramenta é um projeto de código aberto que provê um ambiente de desenvolvimento para implementar rádios definidos em software. As aplicações em GNU Radio são desenvolvidas utilizando a linguagem de programação Python, enquanto que os blocos de processamento são desenvolvidos em C++ por questões de desempenho (SELVA et al., 2012).

Este projeto possui como objetivo principal a realização do analisador de controles remotos utilizando um *dongle* RTL-SDR e inclui os seguintes objetivos específicos as serem realizados:

- Detectar a frequência do sinal transmitido.
- Detectar o codificador (chipset) utilizado.
- Detectar a taxa de bits do transmissor.
- Detectar a sequência de bits transmitida (informação).
- Desenvolver uma interface gráfica para o usuário.

2 Metodologia

2.1 Levantamento de dados

Nessa etapa serão realizados estudos sobre as informações necessários ao projeto. Para isso será realizada a fundamentação teórica sobre: codificadores utilizados, os tipos de modulações empregados nos controles remotos, os conceitos de rádios definidos em software, o funcionamento de um dispositivo RTL-SDR, a plataforma de desenvolvimento GNU Radio que será utilizada e técnicas de detecção de espectro.

2.2 Realizar o modelo do receptor

Nessa etapa será realizado o modelo para a recepção do sinal na plataforma de desenvolvimento GNU Radio. Esse modelo deverá receber e identificar sinais para modulação OOK e FSK, e fornecer os bits de informação para os blocos decodificadores.

2.3 Detectar a frequência do sinal transmitido

Com base nos estudos realizados no levantamento de dados será escolhida a técnica de detecção de espectro que melhor se adequar ao projeto. Então será desenvolvido os blocos de processamento para a detecção do sinal nas faixas de frequências mais utilizadas pelos controles remotos.

2.4 Detectar as características do codificador

Para realizar essa tarefa é necessário o conhecimento detalhado sobre o codificador utilizado. Nessa etapa serão realizados três blocos decodificadores baseados nos *datasheets* dos mesmos. Os três codificadores escolhidos foram o HT6026, HT12E e o HT6P20B, todos produzidos pela Holtek Semicondutor Inc. Os decodificadores servirão como base para todas as detecções apresentadas a seguir.

1. Detectar a sequência de bits transmitida

   Com os blocos decodificadores já implementados, será realizada efetivamente a decodificação do sinal transmitido, passando o sinal de entrada aos decodificadores existentes. Os codificadores que não forem compatíveis com a codificação do sinal transmitido não conseguirão realizar a decodificação. Apenas será apresentado a sequência detectada de um codificador compatível.

2. Detectar o codificador utilizado

   Após a detecção da sequência de bits transmitida é detectado qual o codificador foi utilizado e como seus pinos de entradas foram conectados.

3. Detectar a taxa de transmissão

   Para realizar essa etapa é necessário que o detector do codificador utilizado já esteja concluído. Pois é necessários saber o formato da informação transmitida, seus períodos de sincronismo e como cada bit de informação é codificado, para poder detectar as taxas dos bits de informação e de codificação.

2.5 Desenvolver uma interface gráfica para o usuário

Após a realização de todos os blocos de processamento necessários para o analisador de controle remotos, será desenvolvida uma interface gráfica para o usuário de modo a facilitar o uso e realizar a escolha da função desejada de forma simples.

3 Resultados e Discussão

Para uma visão do funcionamento de um controle remoto, foi realizada a análise de um sinal transmitido que utiliza codificador HT6026. Esse codificador é capaz de codificar 9 entradas de informação em três estados lógicos diferentes, sendo 3^9, resultando em 19.683 sequências diferentes. O sinal transmitido consiste em duas sequências da mesma informação e dois períodos piloto, o primeiro período piloto possui 18 clocks de duração, já o segundo possui 24 clocks. Esses pilotos representam a ausência da portadora (HOLTEK SEMICONDUCTOR INC, 2009). A Figura 1 apresenta a duração e como estão organizados esses períodos.

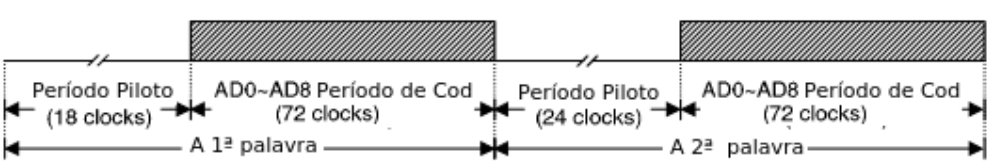

Figura 1 - Formato de ciclo de transmissão - HT6026.

Cada trit[2] de informação é codificado conforme apresentado na Figura 2. Como pode ser observado nessa figura, um trit de informação tem duração de 8 clocks. A frequência de oscilação f_{OSC} depende de resistores e capacitores inseridos entre as entradas do oscilador (HOLTEK SEMICONDUCTOR INC, 2009). Em vista disso, para um mesmo codificador pode existir diferentes valores de f_{OSC} e consequentemente de taxa de transmissão.

A análise da transmissão foi realizada utilizando a ferramenta Inspectrum[3] e está apresentada na Figura 3. É possível observar nessa figura os 9 trits de informação e o período piloto transmitido, além disso, é possível fazer a detecção visual dos trits transmitidos conforme os formatos de onda apresentados na Figura 2. É possível observar também a modulação OOK na transmissão com seus períodos com ausência da portadora.

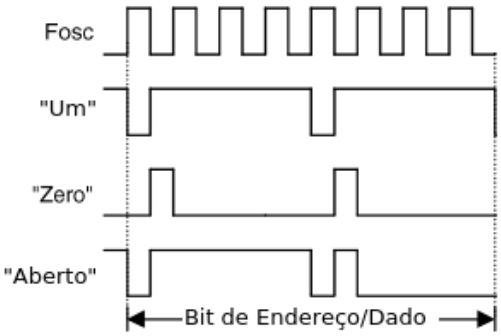

Figura 2 - Formato de onda na saída - HT6026.

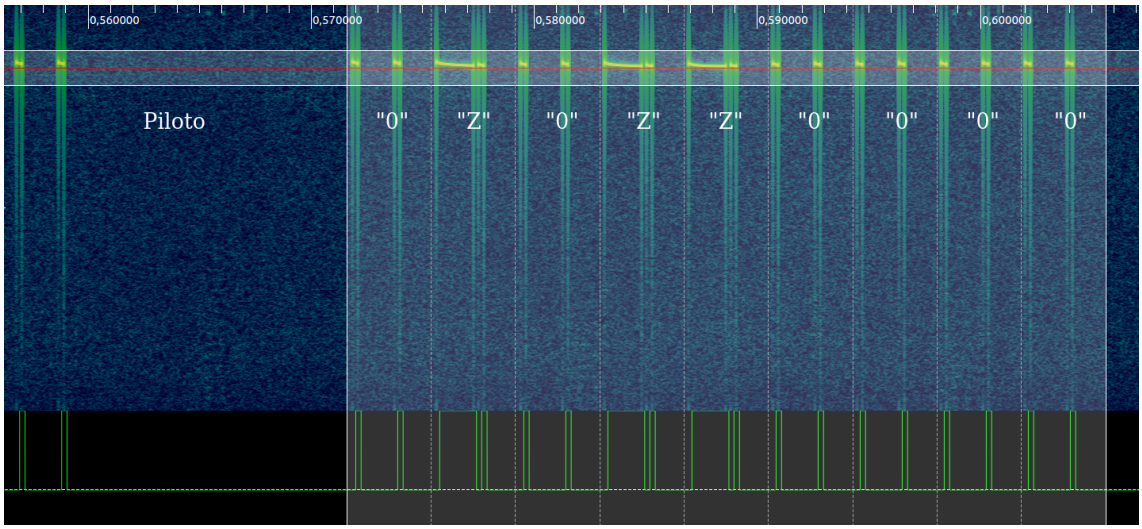

Figura 3 - Exemplo de transmissão utilizando o HT6026.

4 Considerações Parciais/Finais

Referências

FANAN, A. et al. *Comparison of Spectrum Occupancy Measurements using Software*

[2]Um trit é a menor unidade de informação que pode ser armazenada em um sistema que faz uso da lógica ternária, ou seja, um trit faz referência a três estados lógicos possíveis. Para esse trabalho os três estados possíveis são: um, zero e aberto.

[3]https://github.com/miek/inspectrum

Defined Radio RTL-SDR with a Conventional Spectrum Analyzer approach. [S.l.], 2015.

HOLTEK SEMICONDUCTOR INC. *HT6026 Remote Control Encoder*. [S.l.], 2009. Rev. 1.10.

LAUFER, C. The hobbyist's guide to rtl-sdr. In: ____. [S.l.]: Pearson, 2015. cap. 1.

MIYASHIRO, H. et al. *Software Defined Radio for hands-on Communication theory*. [S.l.], 2017.

SELVA, A. F. B. et al. *Introduction to the Software-defined Radio Approach*. [S.l.], 2012.

Hirohide Suda e Matthew J. Lehmer. *REMOTE KEYLESS ENTRY SYSTEM*. 2004. US 6,718,240 B1. Disponível em: <https://patentimages.storage.googleapis.com/ae/8a/3f/8df7ef2c8104f4/US6718240.pdf>.