ABSTRACT

Paul Elijah Setiasabda (03220120007)

SOFTWARE-DEFINED RADIO IMPLEMENTATION WITH HACKRF ONE: FM TRANSCEIVER, JAMMER AND GSM RECEIVER
(xvi + 70 pages: 75 figures; 3 tables; 1 appendix)

Various communication systems have emerged in the last two decades where each of the system needs different equipments for testing and usage. The inefficient usage of resources led to an idea for Joseph Mitola who introduced the term Software Radio. Software Radio is the term used for an equipment that is capable of processing a signal wholly on the software for an unlimited amount of bandwidth. ADC/DAC and antenna are the main hardware needed for this. Currently, the idea of software radio cannot be fully implemented yet. Instead, a few compromises were made resulting in software-defined radio, where a huge part of the processing is done through a processor and software while some parts are done through hardware and the hardware can be adjusted by the software. One of the popular software-defined radio available in the market is HackRF One. The aim of this thesis is to demonstrate that HackRF One is a software-defined radio by implementing a few different communication systems on a wide range of frequencies. The systems are FM receiver, FM transmitter and GSM Receiver. A jammer was also implemented. The FM Receiver shows a good signal reception from commercial FM Radio stations and is able to extract the music from those FM channels. The FM transmission was checked with a spectrum analyzer. The frequencies used in the experiment were 84 MHz, 850 MHz, 1.9 GHz and 2.5 GHz. At 84 MHz, the sound sent from the computer's microphone was heard when tested using a commercial radio receiver showing that HackRF One is truly capable of transmitting FM Radio. HackRF One is also able to receive data from GSM transmission but it needs a software called wireshark to decode the data. With a few GSM information such as Kc and TMSI, the data of SMS and Phone calls can be extracted from the decoded data. Jammer was also implemented for FM, GSM and WiFi. FM radio can be jammed depending on the power, while it is more difficult to jam GSM and WiFi. A phone can get receptions from different base stations. HackRF one is able to block the frequency of one base station. If there is only a base station available to the phone, HackRF one can jam the phone's connection. Jamming WiFi is similar with GSM, because in some WiFi systems, they can reconnect to other WiFi channels, HackRF one can jam one channel, but not all WiFi channels.

References : 33 (1997 – 2016)

ABSTRAK

Paul Elijah Setiasabda (03220120007)

SOFTWARE-DEFINED RADIO IMPLEMENTATION WITH HACKRF ONE: FM TRANSCEIVER, JAMMER AND GSM RECEIVER
(xvi + 70 halaman: 75 gambar; 3 tabel; 1 lampiran)

Berbagai sistem komunikasi telah muncul dalam 2 dekade terakhir di mana masing-masing sistem memerlukan peralatan yang berbeda untuk melakukan pengujian dan penggunaan. Penggunaan peralatan yang tidak efisien ini memberikan ide kepada Joseph Mitola yang memperkenalkan istilah *Software Radio*. *Software Radio* adalah istilah yang digunakan untuk peralatan yang mampu memproses sinyal sepenuhnya pada perangkat lunak dengan jumlah *bandwidth* yang tidak terbatas. ADC / DAC dan antena adalah satu-satunya perangkat keras yang diperlukan untuk *Software Radio*. Saat ini, ide *Software Radio* tidak dapat sepenuhnya di-implementasikan. Sebaliknya, beberapa kompromi dilakukan yang memunculkan *Software-Defined Radio*, di mana sebagian besar dari pengolahan dilakukan pada prosesor dan perangkat lunak sementara beberapa bagian lain dilakukan melalui perangkat keras dan perangkat keras yang dapat diatur melalui perangkat lunak. Salah satu *Software-Defined Radio* populer yang tersedia di pasar adalah *HackRF One*. Tujuan dari skripsi ini adalah menunjukkan beberapa kemampuan *HackRF One* sebagai *Software-Defined Radio* dengan menerapkan tiga sistem komunikasi yang berbeda pada berbagai frekuensi. Tiga sistem tersebut adalah penerima *FM*, pemancar *FM* dan penerima *GSM*. Sebuah *Jammer* juga di-implementasikan. Penerima *FM* menunjukkan penerimaan sinyal yang baik dari pemancar *FM Radio* komersial dan mampu mengekstrak musik dari saluran-saluran *FM*. Transmisi *FM* dilakukan dan diperiksa dengan *spectrum analyzer*. Frekuensi yang digunakan dalam penelitian ini adalah 84 MHz, 850 MHz, 1,9 GHz dan 2,5 GHz. Pada 84 MHz, suara yang dikirim dari mikrofon komputer terdengar saat diuji menggunakan penerima radio komersial menunjukkan bahwa *HackRF One* benar-benar mampu melakukan transmisi *FM Radio*. *HackRF One* juga dapat menerima sinyal dari *GSM*, tetapi memerlukan perangkat lunak bernama *Wireshark* untuk membaca data dari *GSM*. Dengan beberapa informasi seperti *Kc* dan *TMSI*, data dari *SMS* dan panggilan telepon dapat diekstraksi dari data. *Jammer* juga diterapkan untuk *FM*, *GSM* dan *WiFi*. *Radio FM* dapat di blok tergantung dari kekuatan sinyal, sementara lebih sulit untuk *jamming* sistem *GSM* dan *WiFi*. Sebuah ponsel yang menerima sinyal dari beberapa *base station* yang berbeda akan sulit untuk di-blok oleh *HackRF* yang hanya mampu mem-blok satu frekuensi base station, tetapi jika hanya ada satu *base station* yang tersedia untuk telepon, *HackRF* dapat mem-blok sambungan telepon itu. *WiFi* Jammer mirip dengan *GSM*, karena dalam beberapa sistem *WiFi*, frekuensi sinyal dapat terkoneksi ulang ke saluran *WiFi* lain, *HackRF* dapat memblok satu *channel*, tetapi tidak semua *channel WiFi*.

Referensi : 33 (1997 – 2016)