SDR SYSTEM FOR GNSS SIGNAL PROCESSING

Larisa MONACU, Titus BĂLAN

Transilvania University, Brasov, Romania
(larisa.monacu@student.unibv.ro , titus.balan@unitbv.ro)

DOI: 10.19062/1842-9238.2018.16.3.9

Abstract: *Commercially available GNSS (Global Navigation Satellite System) receivers, where signal processing is done on the hardware side, are limited in terms of search frequency, PLL phase, noise bandwidth, or algorithms used to process the input GNSS signal and are not suitable for utilization in industrial or military applications. Thus, the most reliable solution is the usage of a software-configurable receiver. Satellite navigation allows accurate location services in vehicle, air and naval navigation systems But its precision can also be used in military services like delivering weapons to targets for military purposes, or in other applications in the IoT domain or people tracking services. This paper describes the implementation of real-time GNSS reception in the L1 band using Software Defined Radio (SDR) platforms and specific software implementations for signal processing, aiming to obtain a precise geographic position, as well as a method for the broadcasting of GNSS signals based on the SDR platform.*

Keywords: *SDR, GPS, Real Time tracking, GPS Spoofing, IoT*

1. INTRODUCTION

Finding position and location has remained a source of interest for the industry, which is trying to improve the quality and precision of location services. In the past, people have explored stellar constellations to establish their position. Since the US implementation of the GPS system and a similar GLONASS system by the Soviet Union, satellite positioning applications have grown globally, not only in the military area but also in the commercial market. Aircraft and ships use the GPS system to find out the current position and guide them to the destination without hitting obstacles. Farmers also use the GPS system for automatic farming equipment to ensure that they plant in the same place in the next season. Topography field uses GPS to analyze different surfaces of the earth. Telecommunications use GPS for social activities, including cross-country cycling, skiing, hiking skydiving, paragliding, geotagging photographs among others.

This paper describes the implementation of real-time GNSS reception in the L1 band, using the Hack RF One SDR platform, along with an ANT555 GPS antenna which processes the signal to obtain the geographic position.

The Global Navigation Satellite System GNSS is defined as a satellite system that provides the autonomous geo-spatial position with a global approach. GNSS receivers using GPS, GLONASS, Galileo, or BeiDou systems are used in many applications.

The US implementation, the GPS system, is a radio navigation and positioning system that provides accurate information about the position, speed and timing of the information to the GPS receiver. The NAVSTAR GPS system was launched in 1974 and since 1983 GPS has been used also for civil purposes.

The system functions based on the usage of minimum three GPS satellite signals, used to calculate position, speed and time information for users.

Accuracy of GPS determination can range from tens of meters to millimeters, depending on the equipment and method used.

The operating principle of the GPS antenna consists in the measurement of the signal propagation time between the satellites and a terrestrial receiver, thus determining the receiver's position. Software Defined Radio (SDR) technology grew between 1990-1995 with the SPEAK Easy Military Program, which aimed to build a US Air Force radio that could operate at frequencies between 2MHz and 2GHz.[1]

Software Defined Radio systems have parameters that can be reconfigured via software. In its original academic term, the term software radio refers to the reconfiguration of the radio interface through software, comprising reconfigurability at any OSI level through software. The concept has been introduced to migrate hardware components such as mixers, filters, amplifiers, modulators/demodulators, detectors, software to a personal computer, or an embedded architecture.[2]

SDR technology, applied to global satellite navigation (GNSS) reception, allows the implementation of a positioning device with a high level of flexibility. Hardware design is generally very costly and any significant improvements require a redesign of the hardware. Compared to a conventional GNSS hardware receiver, the use of an SDR provides greater flexibility for processing and analyzing in intermediate stage signals. Furthermore, a software receiver can also be configured as a GNSS multi-constellation receiver with small modifications. The SDR implementations, used in many domains, were also tailored for GNSS receiving platforms and analyzed in several research papers [3],[4],[5],[6].

In this paper, besides the usage of the multipurpose Hack RF One SDR hardware platform, we have used the GNSS-SDR software reception framework that provides implementation of various algorithms required by a GNSS receiver, from reading the first probe to conditioning and passing it through competing blocks that affect acquisition, coding and tracking phases, as well as demodulation of the signal. Having everything implemented in software brings two main advantages: first, the GNSS SDR receiver can be easily upgraded during its operational life, second, the SDR platform can be used for prototyping different signal processing and signal quality monitoring algorithms.

A Software Defined Radio platform can be used not only to accurately receive GNSS signals, but also to emulate GNSS signals and to transmit them, as a method for spoofing unauthorized access of devices that are navigating based on GNSS coordinates.

This paper is organized as follows: subsection 2 introduces the software and hardware elements used for our experimental platform, subsection 3 detail the blocks needed for signal processing, subsection 4 shows a way for results validation and visualization while subsection 5 details a method for GPS Spoofing using an SDR element, with possible military applicability.

2. SDR PLATFORM ELEMENTS

As software platform for the signal receiving and for the extraction of the geographical position we have used a GNSS-SDR platform that implements a software defined receiver with the help of C++ defined functions. GNSS-SDR is based on GNU Radio, a well-known framework that provides signal processing and processing blocks that can be used in a visually programmatic way. GNSS-SDR provides an easy code, completely reusable for RF fronts, and allows new implementation or personalization. It offers interfaces to all type of RF signals for different hardware SDR platforms.[7]

From the satellite positioning point of view, GNSS-SDR runs a C ++ program that reads data from a signal source (that can be a hardware device or a suitable prerecorded file) and which performs all signal processing until the geographical position is established.

We have run the software configurations in the software of a personal computer running Linux. As we have mentioned, for the "dry run" tests, to ensure that the system is working properly on the PC environment, we have used the option to process samples of raw data stored in a file, as we wanted to be sure that the system is not influenced by the real-time processing time constraints.

GNSS SDR provides interfaces through USB and Ethernet buses to a variety of commercially or customized front-ends by adapting processing algorithms to different sampling frequencies, intermediate frequencies, and sample rates [8].

We had several options to be used as hardware SDR platform for the effective data acquisition: USRP products from Ettus Research (National Instruments) that supports a wide variety of development environments for RF applications [9], Digilent Zedboard platform, based on the Xilinx Zynq that includes a processing system and a programable logical layer with connection to a RF daughterboard from Analog Devices [10] and Hack RF from Great Scott Gadgets capable of transmitting or receiving radio signals from 1 MHz to 6 GHz

After analyzing the hardware contained in various devices designed to demodulate the signals, we have chosen to use the Hack RF One due to its lower costs and simpler use then other products. It is recommended to install and use the device within the Linux distribution, which offers a wider range of continuously developing libraries.

Designed to enable the testing and development of the latest and next-generation technologies, Hack RF One is a hardware platform that can be used as an USB peripheral or programmed for autonomous operation and has the ability to digitize received or transmitted radio signals.[11]

3. GPS RECEPTION AND SIGNAL PROCESSING

After we have validated the software functionality by using pre-recorder satellite data, we have moved to the real solution so the SDR receiver is processing real-time GNSS signals. We have obtained the reception of GPS signal from the L1 Band, centered on 1.57542 MHz using the Hack RF ONE device, an ANT555 GPS antenna specific for GPS L1 signal reception and a software configuration file made using the GNSS-SDR implementation blocks.

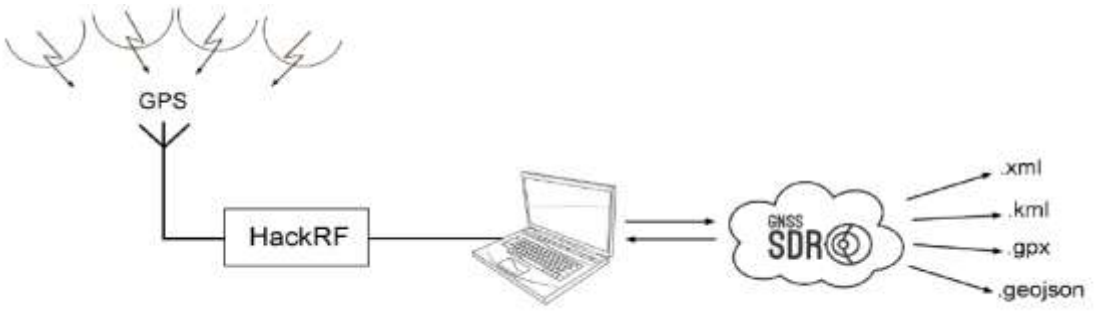

FIG.1 The block diagram for real-time GPS reception

Initially, we aimed to receive the L1 C / A GPS signal with the VERT2450 antenna, which has a bandwidth of up to 5.6 GHz. In order to receive and decode a GPS signal, a specific GPS antenna, which operates in the 1.5 GHz band, is required. It is also necessary for the antenna to have a built-in LNA amplifier to amplify the signal due to the losses, or an external amplifier connected between the antenna and the device. So we chose to use the ANT555 GPS antenna.

If one cannot track and acquire the signal, the terminal displaying "loss of lock in channel x", a parameter to be reconfigured is the one referring to the Doppler Effect. In this sense, the value of the Doppler parameter in Hz should be increased and the search step in the frequency grid decreased.

The software configuration performs the acquisition and tracking of the signal, decodes the navigation message and other variables required for the positioning algorithms, finally calculating the navigation solution.

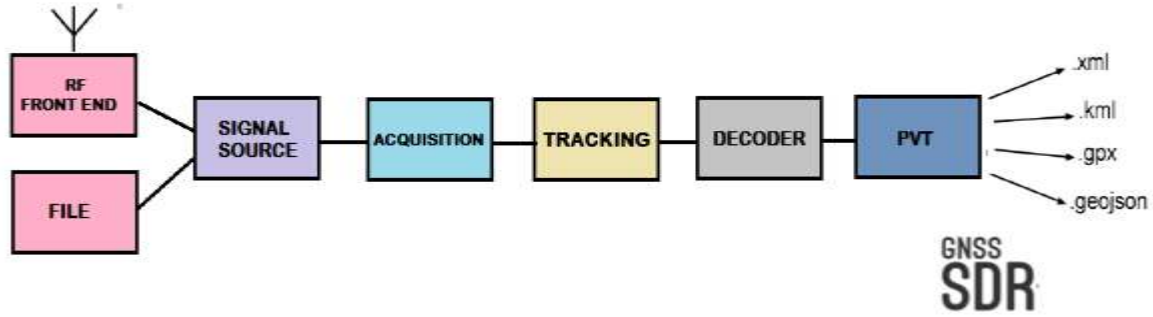

FIG.2 Block diagram describing the GNSS-SDR operation

Main functional blocks used for signal processing are described below:

- SIGNAL SOURCE

The signal source block is responsible for implementing the hardware driver, that communicates with the Hack RF One device and injects a continuous stream of raw GNSS signal samples into the processing flow graph. Inputs are the raw bits that come out of the analog-to-digital converter (ADC) of the Hack RF One, being read in real time with the ANT555 GPS ANTENNA. Also, the signal source may be a file that contains previously recorded signal rows, real or simulated.

- ACQUISITION

It contains blocks to convert the data type into the sample stream, to filter the noise and possible interference and to transmit the input data.

- TRACKING

The role of a tracking block is to track the evolution of the signal synchronization parameters: encoding phase, Doppler effect, and operator phase.

- DECODER

The role of the block is to get the data bits from the navigation message broadcast by GNSS satellites. The NAV GPS message is modulated at 50 bits / second. The entire message contains 25 frames of 30 seconds, forming the main frame. Each frame is divided into 5 sub-frames of 6 seconds each. Also, there are collected sync data from all processing channels in order to calculate GNSS fundamental measurements: pseudodistance, carrier phase and Doppler effect.

- POSITION- VELOCITY -TIME

The role of a PVT block is to calculate navigation solutions and provide information in appropriate formats for further processing or representation of data for geographic information: .KML, .GeoJSON, .XML and .GPX files are generated when calculating the first fixed position.

4. THE RESULTS OF POSITIONING SYSTEMS

Receiving the signal should be done in open spaces, preferably on a high building, to avoid interference and reflection introduced by the environment where the signal is propagated. Satellite signals do not propagate through the walls of the buildings or the foliage of the forests (trees), so the antenna must have direct view to the sky.

In the Linux terminal, after setting the configuration files and initiating the configuration, satellites were detected for the number of channels set. After a few seconds of the L1 C / A GPS signal has been detected, navigation messages were received for each channel. To decode the location, it is necessary to receive the signal from at least four satellites. After approximately 10 seconds of signal acquisition and tracking, real-time location determination and coordinate display in the terminal were performed.

The advantage of using GNSS-SDR is the ability to generate .xml, .kml, .geojson, .gpx files that contain the coordinates. These files can be opened with the help of appropriate tools to verify the correct location and determine the accuracy of the geographic position. For example, we have opened the resulting .kml file with the Google Earth application.

FIG.3 Viewing real-time geographic location in Google Earth application

We have observed in our tests that the method used provides a 3-4 meter accuracy of user location, which is a pretty good estimate given the weather conditions and the reflections on the surrounding buildings at the moment of receiving the data.

Also the coordinates resulting from the decoding of the location can be transmitted in a cloud or a data base over the internet for further processing or monitoring and thus accessible at all times. Stored data can be used in IoT applications, such as tracking services for people, vehicles or devices.

5. GPS SPOOFING WITH APPLICABILITY IN THE MILITARY DOMAIN

Another way to use the SDR platform is not only to receive GNSS signals, but also to transmit GNSS signals, emulating a real GNSS system. A GPS spoofing attempts to deceive a GPS receiver by broadcasting incorrect GPS signals, structured to resemble a set of real GPS signals. In case of protecting critical infrastructures against unauthorized unmanned vehicles, like drones, that navigate based on GNSS positioning, the GPS spoofing is a valid countermeasure.

We have used the SDR platform to simulate a GPS signal from the L1 band (C / A data) using a script [12] based on a file containing ephemeris GPS data to specify the GPS satellite constellation. The ephemeris data file is available to the public, updated daily on the site: http://cddis.gsfc.nasa.gov/

These files are then used to generate simulated pseudo-distance and Doppler effect for GPS satellites in view, and then used to generate digital I / O samples to simulate the L1 C / A GPS signal. To obtain the simulated GPS signal, a file containing the modified data is generated

To test that the broadcasted GPS signal is received by surrounding elements, we used the Android GPS Test application, available for free, with which can display the signals from different available satellites and the current location of the user. The simulated GPS signal was transmitted using the Hack RF One device and a VERT2450 antenna. After a few tens of seconds, we were able to receive the data transmitted using the fake broadcast signal.

In order to receive the new signal, it is necessary to set the Location Mode - GPS Only and to restart the smartphone to correctly apply the setting. Otherwise, the mobile device will estimate the geographic position using the Internet.

FIG.4 View of the fake data received by the GPS Test application

FIG. 4 shows the reception of the simulated GPS signal, the reception power for each simulated satellite and the accuracy with which the location was calculated (on the left side). It also shows the coordinates of the current location received by the mobile device, the coordinates that were specified when creating the transmitted file, as well as its positioning on a map. The current time is different from the time displayed by the GPS Test application as the time at which the processed ephemeris data was processed.

The development of the GPS application system by the US Defense Department led to the use of the system as a defense mechanism during the war. Today, military applications have grown to be used in the mapping of missile location or equipment, monitoring of areas of military interest, guiding soldiers in reconnaissance or rescue operations. GPS Spoofing can be used in falsely guiding enemy equipment in case of war or deviation of airplanes and ships to other targets or strategic locations.[13]

6. CONCLUSIONS

This paper presents a method for real-time GNSS signal reception from the NAVSTAR GPS system via a Software Defined Radio platform. The received data is processed using the implemented software blocks from GNSS-SDR in order to obtain the real-time geographic position of the receiver. A software reception system has more flexibility compared to the conventional off-the-shelf hardware receiver because intermediate signals are available for processing and analysis at each stage.

Real-time reception using the GPS antenna and the Hack RF SDR platform with GNSS-SDR software configuration was tested to provide a 3-4 meter accuracy of user location. New algorithms can be added and tested in the modular structure of the software receiver.

The paper also describes a way of simulating the GPS signal in order to obtain a fictive geographic position and user data, by transmitting using the SDR platform of a file which contains a set of fake coordinates, usable in defense scenarios based on GPS spoofing.

The use of a common radio platform for multiple markets, significantly reduces the logistical support and operating expenditure. In the high-performance military and government communications market, radio system designers and integrators are often incorporating SDR elements, that allow for the addition of new features and capabilities without requiring major new infrastructure expenditures.

REFERENCES

[1] O. Croitoru, *Terrestrial and Space Radiocommunications*, Chapter 14, Transilvania University of Brasov, 2018

[2] About SDR *http://www.rtl-sdr.com/about-rtl-sdr/* , accessed on 22 October 2018

[3] H. Heikki, R. Jussi, A. Tapani, N. Jari, *Multicore software-defined radio architecture for GNSS receiver signal processing*, Published in journal: *EURASIP Journal on Embedded Systems - Special issue on design and architectures for signal and image processing archive*, Volume 2009

[4] A. Brown, J. Redd and M.-A. Hutton , *Simulating GPS Signals: It Doesn't Have to Be Expensive* , GPS World, Vol. 23, No. 5, May 2012

[5] M. Rao1, G. Falco, *SDR Joint GPS/Galileo Receiver from Theory to Practice,* International Journal of Aerospace Sciences 2012, 1(1): 1-7

[6] T. Pany, N. Falk, B. Riedl, T. Hartmann, G. Stangl, and C. Stöber , *Software GNSS Receiver: An Answer for Precise Positioning* Research in *GPS World*, Vol. 23, No. 9, September 2012

[7]GNSS-SDR: https://www.researchgate.net/publication/233380791_GNSS_SDR_An_open_source_tool_for_researchers_and_developers

[8] About GNSS-SDR *https://gnss-sdr.org/docs/* , accessed on 22 October 2018

[9] A. Marwanto, M. Sarijari, A. Fisal, N. Yusof, R. Rashid,. (2009, December). *Experimental study of OFDM implementation utilizing GNU Radio and USRP-SDR* in *communications (MICC)*, 2009 IEEE 9th Malaysia International Conference on (pp. 132-135). IEEE.

[10] S. Gvozdenovic, *System Level Design of Software-Defined Radio Platform https://digitalcommons.wpi.edu/cgi/viewcontent.cgi?article=4152&context=mqp-all*

[11] About HACKRF ONE *https://greatscottgadgets.com/hackrf/* accessed on 22 October 2018

[12] Script created by Takuji Ebinuma available at https://github.com/osqzss/gps-sdr-sim

[13] D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, *Unmanned Aircraft Capture and Control via GPS Spoofing* , https://pdfs.semanticscholar.org/c9d8/5878c56390b614a891d477b90d1b35ceb21b.pdf
[14] L. Presti, L. di Torino, P. Falletti, E. Nicola, M, M. Gamba,. *Software defined radio technology for GNSS receivers*, (2014, May).
[15] M. Z. H. Bhuiyan, S. Söderholm, S. Thombre, L. Ruotsalainen, H. Kuusniemi,
A multi-GNSS software-defined receiver: design, implementation, and performance benefits, 2016, ed. Spring
[16] T. Pany , *Navigation signal processing for GNSS software receivers*, 2010, Artech House.
[17] M. H. S Malik, M. A Malik, U. I. Bhatti, M. S. Z Farooq, M. Iqbal, *Global Navigation Satellite System Software Defined Radio*, 2014
[18] A. S. H. Ghadam**,** M. Renfors, B. Soltanian, *Utilization of multi-rate signal processing for GNSS-SDR receivers*, 2014, ed. Spring
[19] T. Ren, M. Petovello, *An analysis of maximum likelihood estimation method for bit synchronization and decoding of GPS L1 C/A signals*, Ed Spring 2014
[20] M. Pini, E. Falletti, M. Fantino, *Performance evaluation of C/N0 estimators using a real time GNSS software receiver. In Spread Spectrum Techniques and Applications*, 2008 IEEE 10th International Symposium on (pp. 32-36).