

GNSS 재밍신호 감시용 실시간 SDR의 IPC 기반 GUI 구현

박종일*, 박귀우*, 박찬식^o

Implementation of IPC-Based GUI for Real-Time SDR Software to Monitor GNSS Jamming Signals

Jong-Il Park*, Kwi-Woo Park*, Chansik Park^o

요 약

본 논문에서는 GNSS SDR에서 실시간 재밍신호 감시를 위한 GUI의 효과적인 구현을 위해 두 개의 프로세스를 활용한 구조를 제안하였다. SDR은 PVT를 얻기 위해 실시간으로 GNSS 신호를 처리 하고, GUI는 재밍 신호의 영향을 효과적으로 감지하기 위해 신호처리 과정에서 얻는 신호 스펙트럼, 상관 값, C/N_0 , 의사거리 및 PVT 등을 나타낸다. SDR 프로세스는 GNSS 신호의 실시간 처리를 위하여 C++과 CUDA를 이용해 구현했고, GUI 프로세스는 C#을 사용해 구현하고 두 프로세스 간 데이터 교환을 위하여 IPC의 Named pipe를 활용했다. 실제 GNSS 신호에 신호생성기로 만든 CW 재밍신호를 추가하여 SDR의 동작과 재밍 신호의 영향을 GUI를 통해 실시간으로 확인했다. 실시간으로 25개 위성 신호를 처리하는데 1.2MB의 버퍼와 288MB의 메모리 사용량을 사용하였으며, 연산시간은 0.88sec로 실시간으로 정상 동작하는 것을 확인했다. 제안한 GUI 구조는 실시간 재밍 감시 및 항재밍 시스템 등에서 활용가능 할 수 있을 것으로 기대된다.

Key Words : GNSS, SDR, Jamming monitoring, IPC, GUI

ABSTRACT

This paper proposes an efficient GUI structure to monitor jamming signal in real time for GNSS SDR. The proposed structure uses two processes. The SDR processes the GNSS signal in real-time to obtain PVT. The GUI was designed to effectively show using signal spectrum, correlation value, C/N_0 , pseudorange and PVT that can be obtained in signal processing to monitor the jamming signal. SDR process was implemented by C++ and CUDA for real-time processing of GNSS signal, GUI process was implemented by C# and named pipe of IPC was used to transmit and receive data between two processes. SDR operation and an effect of jamming signal were confirmed in real-time through GUI by GNSS signal that added CW jamming signal using the signal generator. GNSS SDR used 1.2MB of buffer and 288MB of memory usage to process 25 satellite signals in real time. We confirmed that the operation time is 0.88sec and it works in real time. The proposed GUI structure can be used in real-time jamming monitoring and anti-jamming system.

* 이 논문은 산업통상자원부 ‘산업전문인력역량강화사업’의 재원으로 한국산업기술진흥원(KIAT)의 지원을 받아 수행된 연구임. (2019년 임베디드SW 전문인력 양성사업, 과제번호 : N0001884)

♦ First Author : Dept. of Control and Robotics Eng., Chungbuk National University, whddlf915@naver.com, 학생회원

° Corresponding Author : Dept. of Control and Robotics Eng., Chungbuk National University, chansp@cbnu.ac.kr 정회원

* Dept. of Control and Robotics Eng., Chungbuk National University, zumbox@naver.com, 학생회원

논문번호 : 201905-070-A-RE, Received May 4, 2019; Revised June 21, 2019; Accepted June 21, 2019

I. 서 론

GNSS(Global Navigation Satellite System)은 전 세계 어디서나 정확한 3차원 위치와 속도를 제공하는 시스템으로 군사용 뿐 아니라 시각동기, 측지측량, 육상, 해양 및 항공 운항 등 다양한 응용에서 사용되고 있다^{1,2}. 그러나 지상에 도달하는 GNSS 신호의 세기는 -130dB로 주변 잡음 -110dB에 비하여 20dB나 낮고, 신호구조도 공개되어 있어 쉽게 재밍에 노출 된다².

가장 많이 사용되는 미국의 GPS(Global Positioning System) C/A(Coarse/Acquisition) 신호의 경우 처리이득(processing gain)을 고려하여 각 신호 처리가 정상적으로 동작하기 위한 JSR(Jammer-to-Signal Ration) 문턱 값은 코드 획득이 24dB, 코드 추적은 32dB, 반송파 추적은 41dB 이다. 그러나 GPS 신호가 워낙 약해서 재머의 전력이 1W 만 되어도 180Km 이내의 수신기가 신호를 획득할 수 없다^{2,3}.

인터넷을 통하여 민간도 쉽게 GNSS 재머를 구입할 수 있으며, 담배 갑 크기 정도로 자동차의 시가 책에 연결하는 저출력 재머 형태⁴, 자체 배터리를 내장하고 있어 어디에나 설치 가능한 형태⁴, 외양이 핸드폰과 거의 유사하여 발견이 힘든 형태⁴ 등 원하는 제품을 선택할 수 있다.

초창기의 재머는 GNSS C/A의 중심 주파수인 L1(1575.42MHz)에 CW(Continuous Wave) 신호를 송출하는 단순한 형태였으나⁵⁻⁷, L1 대역을 훑어가는 swept 형태^{5,8}, L1 대역 전체에 영향을 주는 WBFM(Wide Band Frequency Modulation) 가우시안 방식의 재밍^{4,7} 등의 복잡한 형태로 진화해 나가고 있다.

재밍 신호의 영향을 극복하는 AJ(Anti-Jamming) 기법은 수신기 내부에서 신호처리를 통하여 영향을 줄이는 기법^{6,8}과 외부의 감시망을 이용하여 재머의 위치를 검출하는 기법으로 구분할 수 있다^{2,4,8}. 두 기법 모두 상관기 이전에서 처리하는 기법과 상관기 이후에서 처리하는 기법으로 구분할 수 있다. 상관기 이전에서 처리하는 기법은 다시 안테나 기반 기법과 적응필터를 사용하는 방법으로 나눌 수 있다. 안테나 기반 기법은 GPS가 RHCP(Right Hand Circular Polarized)임을 이용하는 단순한 방법에서 다중 CRPA(Controlled Reception Pattern Antenna)를 사용하는 STAP(Spaced Time Adaptive Processing)나 SFAP(Spaced Frequency Adaptive Processing)이 있

다^{3,9}. 적응필터는 주파수 영역, 시간 영역에서 설계할 수 있다^{2,8}. 상관기 이후에서 처리하는 기법은 다시 벡터 추적루프를 사용하는 방법²과 외부의 INS(Inertial Navigation System) 등의 도움을 받는 기법으로 나눌 수 있다.

재밍은 단순히 GNSS 수신기가 신호를 받지 못하게 하여 위치를 구하지 못하게 하는 것인데, 이에 반하여 기만(Spoofing)은 특정 수신기를 속여 기만기가 원하는 동작을 유도하는 진보한 전자전의 형태이다¹⁰. 단일 안테나를 사용하는 수신기에서 기만에 대응하는 AS (Anti-Spoofing) 기법은 크게 RF 프론트엔드에서 얻을 수 있는 값의 변화 확인과 신호처리 과정에서 얻을 수 있는 값의 일치도를 비교하는 방법이 있다⁸. 또한 CR(Cognitive Radio) 같은 접근으로 GNSS에서도 재밍을 감지하고 이들의 영향이 없는 새로운 주파수로 이동하여 항법을 수행하는 기법도 소개되었다¹¹.

이미 의도적인, 또는 의도적이지는 않은 GNSS 재밍 신호에 대한 많은 보고가 있었으며⁷, 특히 우리나라도 많은 재밍이 보고되었다¹². 이 때문에 통신분야, 항공기 및 선박 등의 분야에서 많은 피해를 입기도 했다. 점점 GNSS 교란 신호의 발신지가 확대되고 그에 따라 교란영향 범위에 들어가는 항공기, 선박 등의 수도 증가하고 있다. 교란신호의 범위가 넓어짐에 따라 재밍 혹은 기만 신호를 실시간으로 대응하고, 군사적, 사회적으로 피해를 줄이기 위해 실시간으로 재밍신호를 감지하는 기술이 요구된다.

재밍신호를 감지하기 위해 수신기에서 제공하는 C/N_0 , 스펙트럼, 위성위치 등의 재밍감시 요소를 확인해야한다. 상용 하드웨어 수신기의 경우 C/N_0 수신기의 위치 등의 신호추적 이후의 한정된 값을 얻을 수 있다. 반면에 본 연구에서 사용하는 SDR(Software Defined Radio)은 스펙트럼, 상관 값, 위성 위치 등 디지털 신호처리로 얻을 수 있는 다양한 재밍감시 요소 값을 얻을 수 있다^{7,13}. 또한 SDR은 수신기 구조 변경이 간단하기 때문에 성능분석 및 상태 감지에 많이 활용되고 있다¹³. 이러한 SDR의 특징으로 재밍신호 감지에 사용하기 적합하다.

본 논문에서는 재밍신호를 실시간으로 확인하고 대응하기 위해 연구실에서 구현한 실시간 SDR¹³에 적합한 재밍 감시 GUI(Graphic User Interface)를 구현한다. 재밍감시에 사용할 SDR은 실시간 동작을 위해 다중 스레드 등의 병렬연산으로 구현되었다¹³. 실시간 SDR에 GUI를 추가할 경우 더 많은 스레드를 운영

하고 동기화를 고려해야하기 때문에 소프트웨어의 복잡도가 증가한다. 또한 신호처리 연산능력에도 영향을 미쳐 정확한 재밍감시가 어렵다. 이를 해결하기 위해 GUI와 SDR 신호처리 프로세스를 분리하는 방법으로 소프트웨어를 설계하였다. 이때 두 프로세스의 데이터 교환을 위하여 IPC (Inter-processor Communication) 을 활용하였다. GUI는 SDR에서 얻을 수 있는 재밍감시 요소를 시각적으로 나타내도록 구현하였다.

본 논문의 구성은 다음과 같다. 2장에서는 신호처리 과정에서 얻을 수 있는 재밍감시 5가지 요소를 구체적으로 설명하였다. 3장에서는 다중스레드로 구현된 SDR에 적합한 GUI를 구현하는 방법에 대해 설명하였다. 4장에서는 전체적인 SDR의 동작 및 재밍신호 감시에 필요한 요소를 얻는 과정을 설명하고, 5장에서는 IPC 기반으로 GUI와 SDR의 프로세스 운영과정과 GUI와 SDR의 입출력 데이터 및 형식에 대해 정의하였다. 6장에서는 실시간 SDR에 적합한 IPC 기반 GUI가 SDR의 실시간 신호처리에 영향을 주지 않고 실시간으로 동작하는지를 확인하고, 마지막 7장에서 본 논문의 결론을 맺는다.

II. 재밍신호 감시 요소 분석

SDR은 그림 1과 같이 크게 하드웨어로 구성된 RF 프론트엔드 부분과 소프트웨어로 구현된 신호처리 부분으로 나눌 수 있다. 안테나에서 얻은 아날로그 RF 신호는 국부 발진기와 곱 연산으로 IF 신호로 변조된다. 변조된 IF 신호는 ADC(Analog to Digital Converter)를 통해 신호처리 영역에서 사용하는 디지털 IF 신호로 변조된다. 신호획득에서 상관기를 이용하여 위성의 대략적인 코드위상과 도플러 주파수를

얻고, 신호추적을 통해 정밀한 코드위상과 도플러 주파수를 얻는다. 얻은 채널 파라미터를 이용하여 수신기의 위치를 추정할 수 있다^{[1],[13]}.

그림 1에서 재밍신호 감시요소 또한 RF 프론트엔드와 신호처리 과정에서 얻을 수 있는 요소로 나눌 수 있다. RF 프론트엔드에서 얻을 수 있는 재밍신호 감시 요소는 AGC(Automatic Gain Control)의 이득 값^[7]이 있고, 신호처리 과정에서 얻을 수 있는 재밍신호 감시 요소로는 스펙트럼 분포, 신호획득과 신호추적의 상관 값, 의사거리, C/N_0 , 수신기의 PVT(Position, Velocity and Time) 값이 있다^[7]. GUI에서는 이들 감시 요소를 감시하여 실시간으로 재밍신호를 검출할 수 있다.

스펙트럼 감시 기법은 GNSS 신호의 스펙트럼을 확인하여 재밍신호를 탐지하는 기법으로, 감시하기 위한 스펙트럼은 RF 프론트엔드에서 변환한 디지털 IF 신호를 FFT(Fast Fourier Transform)을 취해 얻는다. 지상에서 수신하는 GNSS 신호세기는 주변 잡음 세기보다 작으므로, 만약 재밍 신호가 존재하면 해당 주파수 성분의 크기가 증가하고 이를 감지하여 재밍을 검출할 수 있다^[7].

상관 값은 신호획득 부분과 신호추적 부분에서 얻을 수 있다. 일반적인 GPS 수신기에서 신호획득은 중심 주파수의 $\pm 5\text{kHz}$ 범위를 100Hz 간격으로 1/2 칩단위로 계산한 상관 값 중 임계치를 넘어가는 가장 큰 상관 값을 찾아 도플러와 코드 위상을 구한다. 그러나 재밍이 있는 경우 상관 값의 크기가 줄어들거나 왜곡이 발생하여 상관 값을 제대로 구할 수 없어 위성신호의 획득이 힘들어진다^{[1],[13]}.

신호 추적에서는 신호 획득에서 얻은 코드위상과 도플러 주파수를 더욱 정밀하게 찾는다. 신호 추적에

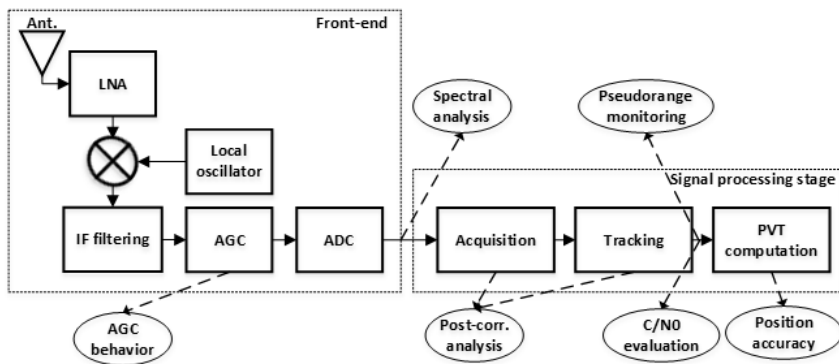


그림 1. GNSS 신호처리 과정 블록도
Fig. 1. Diagram of the GNSS signal processing block

서는 E(Early), P(Prompt), L(Late) 세 개의 상관기를 이용한다. 정상적인 신호를 수신하고 있으면 E와 L의 상관 값은 같고 P값은 E, L의 2배 값이 되는 삼각형 모양으로 나타난다. 만약 재밍이 있으며 이 삼각형 모양에 왜곡이 생기면 이를 확인하면 재밍을 검출할 수 있다^[7].

C/N_0 는 반송파 대 잡음 밀도 비율이며, SDR이 신호추적을 얼마나 정확하게 하고 있는지를 C/N_0 를 통해 알 수 있다. 재밍 신호가 존재하면 정확한 도플러 주파수와 코드 위상을 추적할 수 없기 때문에 C/N_0 값이 감소하며 이를 이용하면 재밍의 유무를 확인할 수 있다^[1,7].

PVT 값으로도 재밍신호의 유무를 확인할 수 있다. 재밍신호에 의하여 의사거리 오차가 증가하고, 수신기의 위치와 시각 오차가 증가한다. 같은 이유로 도플러 오차가 증가하여 수신기의 속도 오차도 증가한다.^[7].

III. GUI 설계

스펙트럼, 상관 값 특성, C/N_0 , 의사거리 및 PVT 등의 다양한 감시요소의 특징에 따라 시각적으로 표현해주면 쉽게 감시요소의 변화를 파악할 수 있다. 감시요소를 시각적으로 표현하기 위해서 막대그래프와 선 그래프, 산점도, 스카이플롯, 문자열 출력 방식의 5

개의 폼으로 GUI를 구성하였다.

그림 2 (a)는 스카이 플롯으로 위성데이터를 복조하여 구한 위성위치를 수신기를 원점으로 나타내는 그림이다. 미국의 GPS는 초록색, 중국의 BDS(BeiDou System)는 노란색으로 표기하여 위성 시스템을 구분하였다. 재밍 신호가 들어면 위성신호를 수신할 수 없어 위성의 개수가 급격히 줄어든다.

수신기 위치는 그림 2.(b)와 같이 산점도로 표현하였다. 수신기의 위치는 ECEF(Earth-Center Earth-Fixed) 좌표계에서 2차원 수평면으로 표현하였다. 1초 마다 계산된 수신기의 위치를 누적하여 붉은 점으로 표시하며 재밍이 발생하면 위치 분산이 급하게 변한다.

상관 값은 그림 2.(c)의 격자그래프와 그림 2.(f)의 선 그래프의 두 가지로 나타내었다. 그림 2.(c)에서 x축은 코드위상, y축은 도플러 주파수, 이며, 해당 도플러와 코드 위상의 격자에 상관 값의 크기를 색으로 나타내었다. 재밍이 발생하면 상관 값 피크의 크기와 위치가 변한다. 그림 2.(f)는 신호추적 단에서 구한 상관 값으로 1/2칩 간격인 E, P, L 상관기의 상관 값을 나타낸다. 정확하게 추적을 하면 E와 L의 상관 값은 동일하고 P의 상관 값은 E, L보다 2배 큰 상관 값을 가져 이등변삼각형 모양을 가진다. 칩 간격과 상관기의 개수는 변경 가능하며, 칩간격이 좁을수록 개수가 많을수록 더 정확하게 파악할 수 있다.

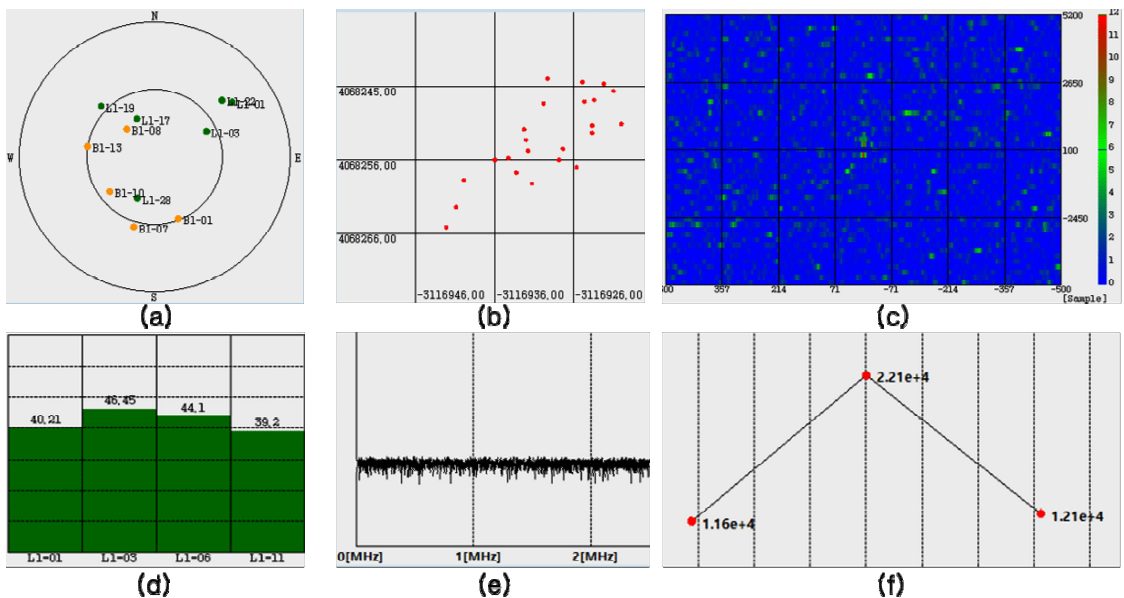


그림 2. 재밍신호를 감시하기 위한 GUI 폼

Fig. 2. GUI form for monitoring jamming signal

(a) Satellite position form, (b) SDR position form, (c) Doppler map, (d) C/N_0 form, (e) IF signal Spectrum, (f) E, P, L form

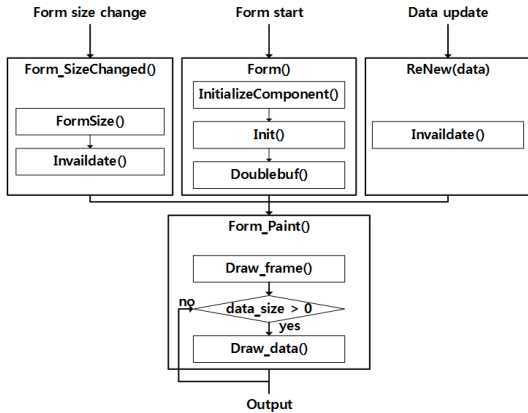


그림 3. 폼 동작 블록 순서도
Fig. 3. Form activity block diagrams

C/N_0 는 그림 2.(d)와 같이 막대그래프 형식으로 나타내었다. C/N_0 크기에 따라 막대의 색과 크기를 다르게 표현하였다. 신호 수신 상태가 좋아 C/N_0 값이 큰 경우(39dB-Hz 이상) 초록색으로 그렇지 않은 경우 붉은색으로 표현해 수신 상황을 한 눈에 알아 볼 수 있도록 하였다.

IF 신호의 스펙트럼 값은 그림 2.(e)와 같이 표시하였다. 스펙트럼 표시 범위는 중심 주파수부터 10MHz 대역이며, 정상적인 경우 GNSS신호 세기는 주변 잡음 세기보다 낮기 때문에 스펙트럼은 평평한 모양을 가진다. 만약 재밍신호가 있으면 해당 대역의 크기가 증가해 이를 GUI에서 확인할 수 있다. 추가로 GUI로 재밍 신호의 대역폭도 확인할 수 있다.

GUI의 각 폼은 실시간으로 재밍 신호 감시를 위해 SDR의 동작에 따라 화면을 갱신해야한다. 본 연구에서는 그림 3과 같이 3가지 조건에서 GUI를 갱신하였

다. 첫 째, 폼이 새로 생성될 때 변수와 데이터를 초기화하고 초기화한 값을 갱신한다. 두 번째는 사용자가 폼 크기를 변경할 때이며, 폼 크기에 맞춰 그래프 크기도 수정하여 갱신한다. 세 번째로 SDR에서 데이터를 받았을 때 이며, 데이터를 받을 때 마다 갱신한다.

IV. SDR의 재밍감시 요소 출력 과정

재밍감시 요소 출력을 위한 SDR의 동작구조와 동작과정은 그림 4와 같다. 그림에서 흰색 상자는 SDR의 동작, 회색 연결부는 전달되는 데이터 종류를, 회색 상자에는 회색 연결부에 적혀있는 번호의 데이터를 나타낸다.

먼저 안테나에서 아날로그 RF신호를 USRP(Universal Software Radio Peripheral) 및 증폭기를 이용하여 디지털 IF신호로 변환한다. 얻은 IF신호 데이터는 신호 버퍼에 저장한 후 3가지 방법으로 사용한다.

첫째, FFT를 수행하여 스펙트럼 값을 획득한다. 획득한 스펙트럼 값은 출력 값 갱신부분으로 넘어가고 갱신주기마다 IPC를 이용해 GUI로 출력한다. 둘째, 신호획득에 사용한다. 신호획득을 통해 도플러 주파수와 코드위상에 대한 상관 값을 얻을 수 있다. 신호획득의 상관 값은 그림 2.(c)의 도플러 맵으로 표현한다. 도플러 맵을 통해 채널의 코드 위상과 도플러 주파수를 확인할 수 있다. 셋 째, 신호추적 상관기에 사용한다. 추적 상관기를 이용하여 상관 값과 반송파 주파수 오차, 코드 주파수 오차 등과 같은 채널정보를 갱신, 비트 추출하고 C/N_0 를 구한다.

얻은 비트를 복조하여 위성위치를 구하고, 의사거리를 계산한다. 얻은 위성위치와 의사거리를 이용하여

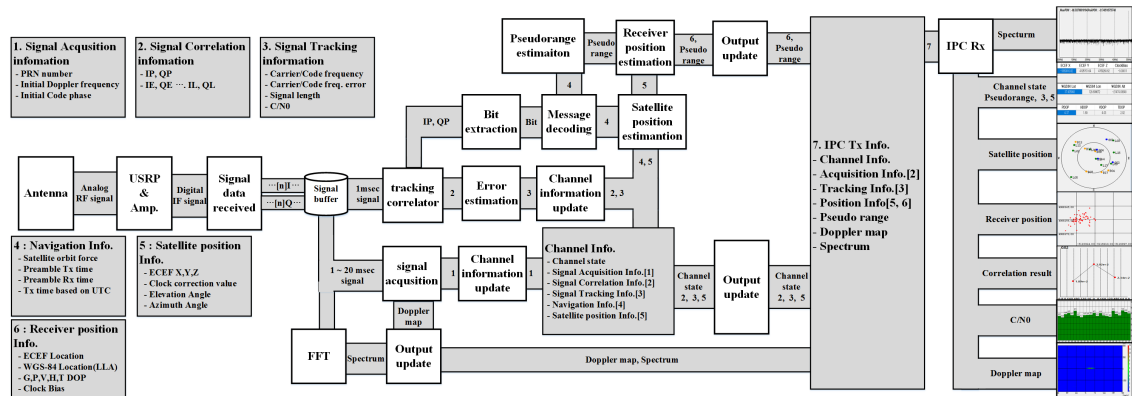


그림 4. SDR 동작 흐름도
Fig. 4. Flowchart of SDR

수신기의 위치를 추정한다. 추정한 결과는 IPC 출력 정보로 넘겨준다. IPC를 이용해 구현한 GUI로 채널 상태, 상관 정보, 위성위치 정보 등 재밍신호 감시에 필요한 데이터를 송신한다. GUI는 받은 정보를 이용해 각 데이터마다 시각적으로 표현한다.

V. SDR과 GUI 프로세스 통신 방식

실시간 SDR^[13]은 고속 신호처리를 위하여 다중 스레드와 CUDA를 이용해 병렬연산을 C++로 구현했다. 여기에 GUI가 추가된다면 다중스레드 관리와 동기화 문제로 인해 소프트웨어가 복잡해진다. 또한 동기화와 스레드 관리를 하지 못하면 SDR의 신호처리 연산능력에 영향을 미친다.

소프트웨어의 복잡성을 해결하기 위해 SDR과 GUI는 서로 다른 프로세스에서 동작하도록 구현했다. 프로세스는 운영체제에 의해 리소스를 할당받는다. 운영체제가 적절한 리소스를 각각의 프로세스에 할당해 주기 때문에 SDR과 GUI 프로세스간의 동기화를 개발시 고려하지 않아도 되는 장점이 있다.

실시간 SDR에 적합한 GUI를 구현하기 위해 이식이 쉽고 GUI구현에 적합한 .Net Framework 기반인 C#으로 구현했다. SDR에서 재밍감시 요소를 받아오기 위해 IPC의 Named pipe로 구현했다.

5.1 IPC를 이용한 GUI와 SDR 소프트웨어 구성 두 프로세스의 기능과 동작 흐름은 그림 5와 같다. 먼저 GUI 프로세스는 사용자에게 의해 실행된다. 사용자는 GUI의 입력 폼을 사용하여 SDR 동작과 관련된 파라미터를 입력하고 SDR 동작 명령을 내린다. SDR의 프로세스를 실행시키면서 입력한 파라미터를 함께 전달한다.

프로세스 실행명령을 받은 SDR 프로세스는 전달

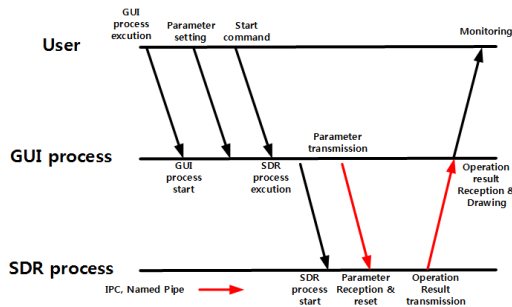


그림 5. GUI와 SDR 프로세스 운영과정
Fig. 5. GUI and SDR process operation

받은 파라미터를 바탕으로 동작 파라미터 및 메모리를 초기화한다. SDR의 신호처리 동작 중 재밍신호 감시에 필요한 요소 데이터를 GUI에 전달한다. GUI는 전달받은 데이터를 파일로 출력하거나 구현된 폼으로 시각화한다. 사용자는 이 결과를 통해 재밍신호를 감시한다.

GUI 프로세스와 SDR 프로세스가 파라미터 데이터를 전송하거나 재밍신호 감시에 필요한 요소 데이터를 전달받는 과정에 FIFO(First Input First Output) 방식의 IPC가 활용된다.

5.2 입출력 데이터 및 형식 정의

다양한 통신시스템의 프로토타이핑과 감시, 평가환경 등에 활용되는 SDR은 사용자의 요구조건에 따라 데이터의 형식, 크기, 순서만을 정의하여 사용자가 쉽게 입출력 데이터를 재 정의할 수 있도록 설계했다. 데이터 형식은 그림 6과 같다.

그림 6.(a)는 SDR 프로세스에서 GUI 프로세스로 데이터를 전달하는 출력데이터 형식을 나타냈다. 수신기의 채널정보와 수신기 동작정보는 기본으로 포함되며 사용자가 데이터를 추가할 수 있다.

한 데이터 패킷은 각 데이터의 크기와 데이터로 구성했다. 먼저 수신기 채널정보는 수신기 채널 수와 데이터로 구성했다. 수신기 채널정보는 채널번호, 채널 상태, C/N_0 , 도플러 주파수, PLL 및 DLL 오차, 코드 주파수, 의사거리, BER(Bit Error Rate) 등이 포함된다. 10byte의 채널이름을 포함하여 한 채널당 54byte로 구성했다.

수신기 동작정보는 동작시간, 연산상태 등 수신기 동작과 관련된 정보와 수신기 목적에 따른 측정치 정보가 포함된다. GNSS 수신기의 목적으로 사용하기 위해 측정치 정보는 위치, 시각정보 등을 포함했다. 한 정보 데이터마다 4byte씩 할당되어 있으며 동작정보 길이는 모든 데이터의 개수를 의미한다. 채널정보와 수신기 동작정보 이후에는 사용자가 정의한 데이터가 이어서 전송된다.

Number of receiver Ch.	Channel data of receiver	Number of receiver operation data	Receiver operation data	Number of User defined data	User defined data
------------------------	--------------------------	-----------------------------------	-------------------------	-----------------------------	-------------------

(a)

Number of Flag bit	Flag bit	Number of Parameter data	Parameter data	Number of Channel setting	Channel setting	Number of Filepath	Filepath
--------------------	----------	--------------------------	----------------	---------------------------	-----------------	--------------------	----------

(b)

그림 6. 입출력 데이터 형식

Fig. 6. Input & output data form (a)output data (b)input data

GUI에서 SDR로 전달하는 입력데이터의 형식은 그림 6.(b)와 같다. 플래그 bit는 시작, 정지, 일시 정지 등과 같이 SDR 동작에 관련된 1bit의 데이터를 의미한다. 파라미터는 수신기 동작에 필요한 IF 주파수, 표본화 주파수 등을 의미한다. 한 파라미터 데이터마다 4byte로 표현했다. 채널설정은 각 채널의 동작 단계인 신호획득, 추적 등을 임의로 설정할 수 있다.

VI. GUI 구현 및 실험

그림 7과 같이 실시간 SDR에 적합한 IPC 방식의 재밍감지 GUI를 구현했다. 그림 7은 재밍신호가 들어왔을 때 GUI 결과를 나타내며 BDS신호와 GPS신호를 수신 중에 재밍신호가 들어왔을 때의 모습을 자세히 보여준다. 재밍신호는 1573.6MHz 주파수, -50dBm의 전력의 CW 방식으로 신호 생성기를 이용해 생성했다. 동작 확인을 위해 실시간 동작가능성을 확인하고 GUI 출력 값을 통해 재밍신호를 감지할 수 있는지 확인했다.

실시간 동작가능성을 확인하기 위해 25개 위성신호를 약 540초 동안 수신했다. 실험에 사용한 PC 사양은 실시간으로 재밍신호 감지요소를 얻고 출력하기 위해 GPU(Graphics processing unit)로 GTX 1080Ti 2개, CPU는 Intel core i7-6950x 10core 1개를 사용했다^[13].

표 1은 수신과정에서 측정된 메모리 사용량, 신호

표 1. 실시간 연산능력
Table 1. Real-time operation performance

Buffer size	Memory usage	Operation time
1.2 MB	288 MB	0.88 sec

버퍼의 크기, 1초 단위로 측정된 연산시간을 기록한 것이다. 만약 실시간 동작에 문제가 있다면 실시간으로 입력되는 신호가 쌓여 버퍼크기는 계속 증가할 것이다. 그러나 버퍼크기는 6ms의 신호 길이에 해당하는 1.2MB 수준을 유지하여 실시간으로 동작함을 확인하였다.

메모리는 평균 288MB가 할당되며 시간에 따른 증가 없이 유지되었다. 프로세서간 통신에 문제가 생겨 데이터가 쌓이게 되면 사용되는 메모리가 증가하지만 그런 현상이 없어 실시간 동작이 가능함을 확인하였다. 항법해를 구하는데 까지의 연산시간은 약 880ms로 1초 주기 출력에 대하여 120ms의 여유를 가진다. 따라서 SDR과 GUI는 실시간으로 정상 동작함을 알 수 있다.

재밍신호 감지를 확인하기 위해 재밍신호가 들어오기 전과 후의 동작결과를 비교하였다. 그림 7.(f)를 보면 IF 신호로 변조된 재밍신호가 들어오는 부분인 6.6MHz 부근에 스펙트럼 결과가 증가한 것을 확인할 수 있다.

재밍신호 추가 전 그림 7.(e)의 빨간색 상자의 빨간 점이 신호획득한 위성의 도플러 주파수와 코드위상의

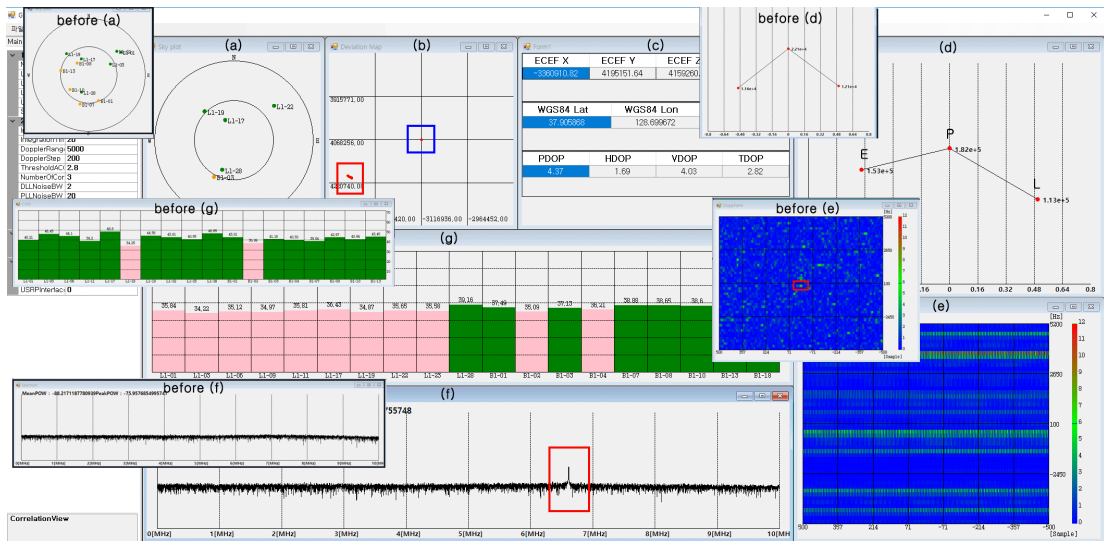


그림 7. IPC 방식의 GUI를 이용한 재밍신호 감지 결과

Fig. 7. Jamming signal monitoring using implemented GUI by IPC method Before : Results of before GNSS adding a jamming signal

값을 나타낸다. 여기서 x축은 코드위상 y축은 도플러 주파수를 나타낸다. 재밍신호가 들어오면 그림 7.(e) 이 나타내는 신호획득 상관 결과처럼 x축과 평행한 여러 개의 초록색 줄로 나타난다. DSSS(Direct Sequence Spread Spectrum) 복조로 인해 재밍신호가 넓게 퍼져 사이드 로브의 값이 평행한 줄로 나타난다.

신호추적의 상관 값을 나타내는 두 개의 그림 7.(d) 를 보면 P 값이 E, L값의 2배에 한참 못 미치는 결과로 E, P, L값이 왜곡 된 삼각형이 생기는 것을 확인할 수 있다. C/N_0 는 보통 정상적으로 수신할 때는 C/N_0 가 38-45db의 값을 가진다. 추적결과가 좋지 않기 때문에 C/N_0 값을 나타내는 그림 7.(g)에서 L1신호는 재밍신호로 인해 붉은색으로 표시된다. BDS는 GPS 보다 중심주파수가 약 14MHz 낮지만 GPS 신호와 동일한 프론트엔드에서 수신하기 때문에 C/N_0 값이 평균 약 42dB에서 평균 약 38dB로 낮아진다.

그림 7.(a)와 그림 7.(b)는 위성위치와 수신기 위치를 나타낸다. 재밍신호 추가 전 결과인 그림 7.(a)에서 나타나는 위성 개수는 12개인데, 재밍 신호로 인해 그림 7.(a)에서 나타나는 위성의 개수가 4개로 줄어든 것을 확인할 수 있다. 그림 7.(b)의 파란 사각형은 재밍신호가 들어오기 전의 수신기 위치이다. 빨간 사각형은 재밍신호가 들어온 후의 수신기 위치이며, 재밍신호의 영향으로 수신기 위치가 변화한 것을 확인할 수 있다.

재밍신호의 영향으로 재밍신호 감시요소 값이 바뀌는 것을 GUI를 통해 확인할 수 있었다. 따라서 실시간 SDR의 IPC 방식의 GUI가 정상적으로 설계, 구현됨을 알 수 있다.

VII. 결 론

본 논문에서는 GNSS SDR에서 재밍신호 실시간 감시를 위하여 IPC 기반 GUI를 구현하고 실험을 통하여 그 동작과 성능을 확인하였다. 제안한 구조는 SDR과 GUI 두 개의 프로세스를 활용하며, 두 프로세스 간 데이터 교환을 위해서 IPC 의 Named pipe를 활용하였다. 재밍신호를 감시하기 위해 필요한 요소를 분석하였으며 신호 획득과 추적의 신호처리 과정에서 얻을 수 있는 요소를 활용하여 GUI 폼을 설계하였다. GUI의 각 폼은 신호처리 과정에서 얻을 수 있는 요소를 막대 그래프와 선 그래프, 산점도, 스카이프롯, 문자열 출력 방식을 이용하여 표현하였으며 실시간으로 내용을 갱신하여 재밍신호 유무를 시각적으로 판단할

수 있도록 하였다.

실제 GNSS 신호에 재밍 신호를 추가하여 실행한 실험 결과, 메모리 사용량 및 버퍼 크기가 증가하지 않고 일정하게 유지되어 실시간으로 동작하며, PVT 를 구하는 연산시간은 약 880msec 로 1초 주기로 출력력을 충분히 제공할 수 있음을 확인하였다. GUI를 이용하여 재밍신호 추가 전과 후를 비교하면 재밍신호의 유무를 판단 할 수 있음을 확인하였다.

제안된 구조는 실시간 재밍신호 감시 뿐 아니라 재머의 탐지 및 항재밍 시스템 등에서 활용 할 수 있을 것으로 기대된다.

References

- [1] E. D. Kaplan and C. J. Hegarty, *Understanding GPS/GNSS principles and applications*, 3rd Ed., Artech House, 2017.
- [2] K. Kim, "Analysis of anti-jamming techniques for satellite navigation systems," *J. KICS*, vol. 38C, no. 12, pp. 1216-1227, Dec. 2013.
- [3] I. M. Weiss and A. W. Morrison, "GPS protection toolbox: Picking the right technology for interference suppression," *PLANS 2002 tutorials*, Apr. 2002.
- [4] R. H. Mitch, M. L. Psiaki, B. W. O'Hanlon, and S. P. Powell, "Civilian GPS jammer signal tracking and geolocation," in *Proc. ION GNSS 2012*, pp. 2901-2920, Nashville, Tennessee, Sep. 2012.
- [5] Y. T. Chen and K. J. Lin, "Assessing and counteraction the effects of interference on GNSS signals," in *Proc. 2015 GCCE*, pp. 427-428, Osaka, Japan, Feb. 2016.
- [6] R. Di, S. Peng, S. Taylor, and Y. Morton, "A USRP-Based GNSS and interference signal generator and playback system," in *Proc. IEEE/ION PLANS 2012*, pp. 470-478, Myrtle, South Carolina, Apr. 2012.
- [7] E. Falletti and B. Motella, *GNSS Interference Threats and Countermeasures, Chapter 5 Interference Detection Strategies*, Artech House, 2015.
- [8] F. Dovis, L. Musumeci, B. Motella, and E. Falletti, *GNSS Interference Threats and Countermeasures, Chapter 2 Classification of*

Interfering Sources and Analysis of the Effects on GNSS receivers, Artech House, 2015.

- [9] M. Petovello and G. Lachapelle, "GNSS Solutions: Adaptive antenna arrays, multi-GNSS tropospheric monitoring and high-dynamic receivers," *insideGNSS*, Apr. 2006.
- [10] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. J. Navig. and Observation*, vol. 2012, article ID 127072, 2012.
- [11] K. W. Park, M. J. Lee, and C. Park, "A design of anti-jamming method based on spectrum sensing and GNSS software defined radio," in *Proc. ISGNSS 2018*, Bali, Indonesia, Nov. 2018.
- [12] S. K. Jeong, T. H. Kim, C. S. Sin, and S. U. Lee, "Technical trends of smart jamming for GPS signal," *Electron. and Telecommun. Trends*, vol. 27, no. 6, pp. 75-82, 2012.
- [13] K. W. Park, J. Yang, and C. Park, "A Design and implementation of software defined radio for rapid prototyping of GNSS receiver," *J. Positioning Navig., and Timing*, vol. 7, no. 4, Dec. 2018.

박종일 (Jong-Il Park)



2018년 2월 : 충북대학교 전자공학부 졸업
2018년 3월~현재 : 충북대학교 제어로봇공학과 석사과정
<관심분야> GNSS, SDR
[ORCID:0000-0003-4885-2221]

박귀우 (Kwi-Woo Park)



2013년 2월 : 충북대학교 전자공학부 졸업
2015년 2월 : 충북대학교 제어로봇공학과 석사
2015년 3월~현재 : 충북대학교 제어로봇공학과 박사과정

<관심분야> GNSS, SDR, 항법
[ORCID:0000-0002-0338-2599]

박찬식 (Chansik Park)



1984년 2월 : 서울대학교 제어계측공학과 졸업
1986년 2월 : 서울대학교 제어계측공학과 석사
1997년 2월 : 서울대학교 제어계측공학과 박사
1997년 2월~현재 : 충북대학교 전자정보대학 교수

<관심분야> GNSS, PNS, SDR, 미지정수결정, 오차해석
[ORCID:0000-0003-2650-4947]