AN ULTRA HIGH SPEED SIGNAL INTERCEPTION FPGA CORE FOR FH MONITORING AND FOLLOW ON JAMMING

S. Krishna Prasad
Staff Engineer

krishnaprasad@nsscomm.com

16-11-781/40, NSS Communications, Hyderabad-36, INDIA

Abstract

Intercepting a communication signal is becoming challenging today with the advanced low SNR and LPI schemes. Interception of FH signal requires a low latency design right from antenna to jamming circuit so that we can intercept, extract parameters and jam the signal very quickly. In this paper, we proposed a FPGA based solution for ultra high speed signal interception of FH signals.

Keywords-frequency hopping spread spectrum, signal interception, jamming

I INTRODUCTION

Frequency Hopping Spread Spectrum, popularly known as FHSS protects against a jammer by increasing the bandwidth that the information signal occupies far more than required. By increasing the system's bandwidth, the jammer needs to spread its power over a wide frequency band W_T making it less effective. To give the basic introduction of the FH signal characteristics[6] the FH transmitter and its related analysis is presented in this section.

The main idea of frequency hopping spread spectrum is simply based on the multiplication of a conventional MFSK signal prior to transmission by an intermediate frequency. This frequency is generated by a frequency synthesizer [5] of the form:

$$p(t) = 2\cos(2\pi f_i t) = 2\cos\left\{2\pi\left[f_1 + (i-1)\Delta f_h\right]\cdot t\right\},\ i = 1,2,...,N \quad \text{-- (1)}$$

where N is the maximum number of possible frequency hop bins, Δf_h is the separation between the carrier frequencies of adjacent bins, and i changes pseudorandomly every T_h seconds. By doing this, the entire spectrum of the MFSK signal transmitted is shifted from its initial carrier frequency f_c to the new carriers frequencies:

$$f_{c_i} = f_c + f_1 + (i-1)\cdot\Delta f_h . \quad \text{-- (2)}$$

In Equation (1), there are N different frequency hop bins, each of bandwidth Δf_h The value of i is changed periodically every T_h seconds according to some predetermined (but apparently random to a third–party observer) noiselike spreading code, called a "pseudorandom" or "pseudonoise sequence.

A simplified block diagram of the transmitter of the FH/MFSK system is shown in Figure 1.

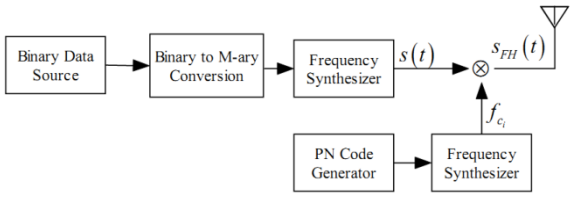


Figure 1. FHSS Transmitter

If we consider single hop, the signal bandwidth is identical to the conventional MFSK, which would be much smaller than W_T. But, when averaged over many hops, the FH/MFSK spectrum occupies the entire W_T bandwidth.

It is difficult to maintain phase coherence from hop to hop between the transmitter and the receiver, primarily because of frequency–dependent multipath and Doppler shifts [5]. Consequently, unless the hopping rate is very low compared to the transmitted symbol rate, practical frequency–hopping systems almost always require noncoherent or differentially coherent demodulation.

A conventional MFSK signal is described by

$$s(t) = \sqrt{2}A_c\cdot\cos\left\{2\pi\left[f_s + (m-1)\Delta f\right]\cdot t + \theta_i\right\}, m = 1,2,..,M \quad \text{-- (3)}$$

where M is the modulation order of the signal, θ_i is the symbol phase, and Δ_f is the frequency separation between each of the M signaling tones. The step Δf is chosen to be an integer multiple of the symbol rate R_s in order to achieve orthogonality. So, multiplying this signal by the frequency from the synthesizer (2.1) the signal becomes:

$$s'(t) = 2\sqrt{2}A_c \cos\{2\pi[f_s + (m-1)\Delta f]t + \theta_i\}\cos(2\pi f_i)$$
$$= \sqrt{2}A_c \cos\{2\pi[f_i + f_s + (m-1)\Delta f]t + \theta_i\} + \sqrt{2}A_c \cos\{2\pi[f_i - f_s - (m-1)\Delta f]t - \theta_i\}.$$

--(4)

The carrier frequencies of the first term are

$$f_i + f_s + (m-1)\Delta f = f_1 + (i-1)\Delta f_h + f_s + (m-1)\Delta f \ ,$$

-- (5)

which is smallest for i=1 and m=1. In this case, the carrier frequency becomes

$$f_1 + (N-1)\Delta f_h - f_s \, .$$

--(7)

If the smallest frequency of the first term is greater than the largest frequency of the second term, then from [5] the following condition has to be satisfied:

$$f_s > f_1 + B + \frac{N-1}{2}\Delta f_h$$

--(8)

where B is the required guardband above and below the high– and the low frequency signaling tones, respectively. In this case, a high pass filter is used to remove the frequency difference contribution, and the frequency hopped MFSK signal becomes

$$s_{FH}(t) = \sqrt{2}A_c \cdot \cos\left\{2\pi\left[f_i + f_s + (m-1)\Delta f\right]\cdot t + \theta_i\right\}.$$

-- (9)

The major advantage of frequency hopping systems against non–sophisticated jammers is that the jammer cannot jam the specific hop bin where the FH system operates at any instant time. The reason is the lack of information about the hopping pattern that the transmitter uses.

The frequency hopping technique also allows portions of the frequency band containing known narrowband interference to be avoided.

Another advantage of an FH system is that the power spectral density of the frequency–hopped signal is identical to that of the conventional MFSK signal in a

specific hop bin. However, since the signal hops from bin to bin, and assuming that the probability that any bin is occupied is equal to (1/N), the average power spectral density is

$$PSD = \frac{1}{N}\sum_{i=1}^{N} S_{FSK}(f \mid f_c = f_{c_i}) \, .$$

--(10)

One of the most popular jammers against frequency–hopping systems is the follower jammer [5]. The follower jammer is a sophisticated jammer that has the ability to intercept with an acceptable probability the instantaneous frequency of the FH system, and then it can generate an appropriate jamming in a narrow range about this frequency.

II FH SIGNAL INTERCEPTION

The signal search and interception is the subject of interest from decades. Even though the fundamental concept of spectrum estimation and signal detection is well discussed in theory with FFT, in practice there are technology limitations to be addressed to realize a system.

The typical radio meter based FH detection[1] is limited to its lesser number of hop interceptions and is useful for only declaring the presence of FH signal presence. The technique proposed in [1] is useful for detecting one FH signal at a time. The research in VLSI technologies and signal processing for fast hopping FH radios [2][3][4] resulted in very fast frequency hoppers which are difficult to intercept with conventional techniques. It is observed [5][6] that the single tone or multi ton jamming is most suitable for against fast hopping FHSS links. This motivates for the development of fast signal processing techniques on FPGAs for follow on jamming.

As the present ESM requirements is to perform full monitoring of the FH signal and also initiate follow on jamming on selected FH targets, there is a need to intercept the FH signal with maximum number of hops.

In this context an FPGA based reconfigurable IP is proposed which can be directly adopted to any Xilinx FPGA based ESM systems. The proposed architecture is advanced variant of the signal search architecture while is completely realized in Xilinx FPGAs. The core possesses two basic capabilities with respect to handling FH signals. The high speed spectrum estimation and FPGA based report generation feature is useful for signal intelligence and also follow on jamming applications. The multi channel filter bank based digital tuner is useful for FH signal monitoring applications. This filter banks with second level of DDC in them which are dynamically tuned as per the intercepted signal frequencies, can produce de-hopped signal for each

hop period. The final produced base band outputs can be stitched in time domain which can be given to monitoring or analysis modules. The below figure shows the high level block diagram of FH signal interception system.

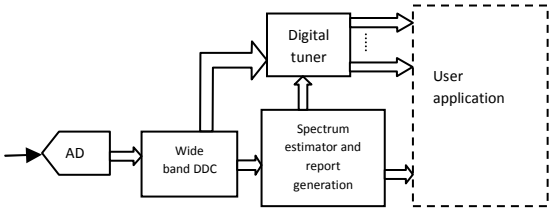


Figure 2. Signal interception system

In case of wideband FH handling multiple instances of the core can meet the requirements. Below figure shows the 4 parallel cores which are tuned to adjacent 40 MHz band each by the front end RF sections, to result in 160 MHz of aggregate bandwidth.

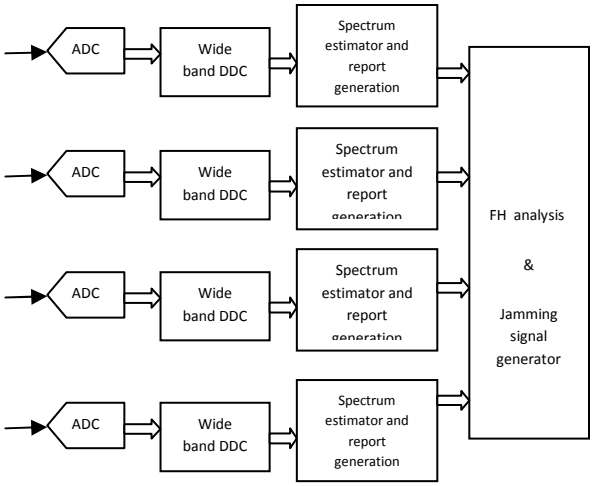


Figure 3. Wideband FH interception system

III PROPOSED DESIGN

To address the problem, an ultra high speed signal interception core is proposed. The design is capable of running upto 300MHz on Xilinx Virtex6 FPGAs. This design has the capability of processing instantaneous bandwidth of 150MHz. This solution can be used to intercept any complicated FH or combination of multiple FH signals. Signal interception core block diagram is shown in Figure-4. The heart of the signal interception core is a dynamic FFT engine.

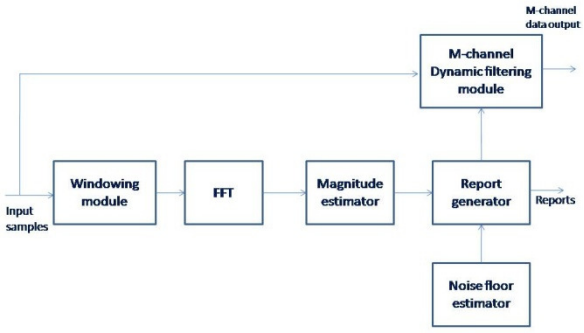


Fig 4. Block diagram of signal interception core

The design supports 4 different modes of operation namely

(a) Spectrum monitoring mode
(b) Signal interception and reporting mode
(c) Automatic interception and capturing mode
(d) Monitoring mode

Spectrum monitoring mode corresponds to monitoring the frequency band of interest. This is the direct application of Fourier transform. Signal interception and reporting mode is the main mode that is used for FH interception. This mode generates reports of various signals and their repetitions that can be used for identification of Frequency Hopping. Automatic interception and capturing mode is extension to signal interception mode, where we can even capture the signals also. Based on the interception information, signal capture happens by tuning NCO to appropriate frequency. Monitoring mode is an additional mode to monitor a particular signal through m-channel dynamic filtering module.

Signal interception core contains two data paths, one for signal interception and other for signal capture. Both paths are explained separately below.

3.1 *Signal interception data path*

Signal interception data path contains windowing module, FFT engine, magnitude estimator, noise estimator and report generator. Windowing module multiplies the input data with a window function. Various window functions supported are Rectangular, Triangular, Hamming, Hanning, Blackman, Gaussian, Barlett-Hann, Kaiser and Blackman Harris. The length of the window depends on the FFT size selected.

Core contains a dynamically configurable FFT engine which can be configured during compile time. FFT engine supports various FFT sizes ranging from 1K to 32K. Apart from FFT computation, the engine has 2 additional features also.

(a) Time domain overlapping: To increase the time domain resolution of computations, a time domain overlapping of 25% and 50% is provided
(b) Spectral averaging: FFT engine includes spectral averaging feature to take average of 2, 4 or 8 consecutive spectrums.

A CORDIC based magnitude estimation algorithm is implemented for calculating the magnitude of frequency spectrum. This magnitude value goes to the report generator.

Report generator analyzes the data produced by previous block and generates reports. Typical format of the report is shown in Figure 5.

Report format

Start freq IF band code	Centre frequency	Bandwidth	Magnitude	Signal lifetime	timestamp

Start freq IF band code: 16-bit value denoting current input frequency band
Centre freq: Centre frequency of reported signal (16-bit)
Bandwidth: Bandwidth of current reported signal (16-bit)
Magnitude: Magnitude of current reported signal (32-bit)
Signal lifetime: Number of repetitions of signal (16-bit)
Time stamp: Absolute time stamp of the current observation of signal (48-bit)

Figure 5. Report format

To calculate the bandwidth of the signal, we need to differentiate actual signal from noise. So, a robust noise estimation engine is incorporated in the core. This engine provides noise estimation that can be used for setting threshold. Signal amplitudes that cross this threshold are registered. Bandwidth and other parameters are calculated for these signals. A minimum bin criteria is also embedded sothat signals of sufficient bandwidth only are reported. Each signal is identified with a time stamp and the core has the capability to report repetition of signals through signal life time field in the report. The report generation and read logic are shown in Figure 6.

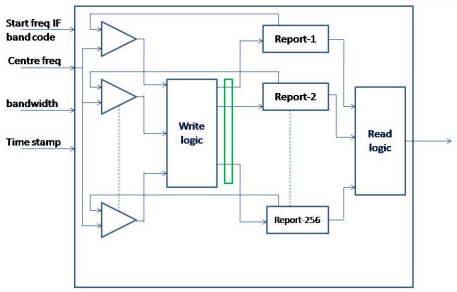


Figure 6. Report generation/read logic

As shown in Fig-6, each new signal interception is compared with existing reports and then only it is saved as new signal. If the signal exists in one of the reports, the lifetime field of that particular report is incremented. There are 1024 reports that can be saved. These reports can be read through a DPRAM based read interface.

3.2 *signal capture data path*

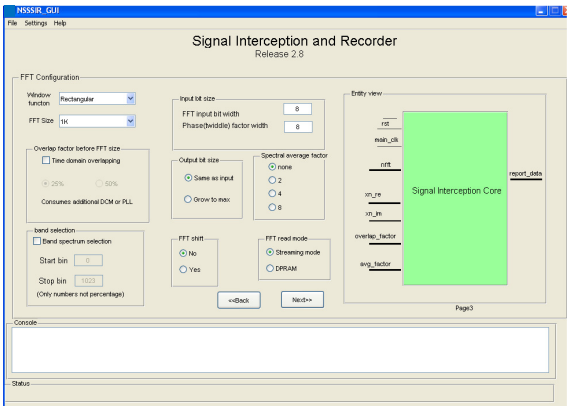
Signal data capture path contains an m-channel filter bank along with a pipeline. The core supports upto 5-channels. The m-channel filter bank contains NCOs that can be tuned to the intercepted signals in the interception data path. So, these 5 channels contain the functionality of narrow band DDCs also.

In case of automatic interception and capturing mode, these filter banks are used for signal capture. Initially, the interception path sweeps the frequency spectrum and identifies the required signals based on threshold. The NCOs are tuned to these frequencies and the data is captured. To adjust timing, a long pipeline is placed before the filters to cater for processing delay in interception path. The pipeline delay should be variable as the computation time depends on FFT size. The down converted samples are saved in FIFOs at the output of filters. The core has the facility to select the number of samples to be saved in the FIFO.

IV RESULTS

4.1 *Graphical user interface*

A front software GUI is developed for configuring the signal interception FPGA core. Different parameter like window function type, FFT parameters, m-channel filter bank parameters are set through this. Figure-7 shows GUI screen shot for setting FFT parameters.



Similarly Figure 8 shows the parameter selection for reports. The software has option to select the fields to be displayed in reports. The core has an option to synchronize with GPS signal and number of reports to be saved. The reports can be read out in streaming mode (sequential) or index based through DPRAM.

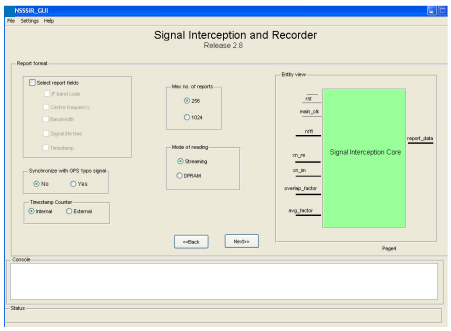


Figure 8. Reports parameter selection

The software GUI is designed in such a way that it generates direct simulation and synthesis scripts based on the parameters chosen.

4.2 *Simulation results*

The core is simulated with ModelSim software. A combination of 4 different sine waves is fed as input. Figure-9 shows the test input. The 4 sine waves are harmonics to each other.

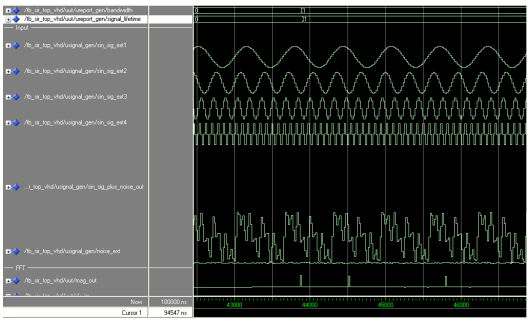


Figure 9. Test input for simulations

The corresponding outputs are shown in Figure 10. Figure shows state transitions of the core which indirectly shows the interception of signal.

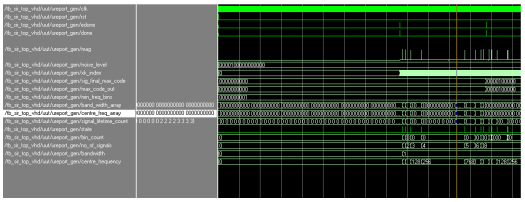


Figure 10. Simulation outputs

Figures (9) and (10) show the case of simplest simulation check. The core is fed with FH signal using a test bench and the results are verified. The core is able to intercept multiple simultaneous FH emissions as well.

V CONCLUSIONS

In this paper, we proposed a FPGA based solution for ultra high speed signal interception of FH signals. The proposed design occupies approximately 50% of Virtex5 SX240T FPGA operating at 300MHz of ADC sampling. The results demonstrate jamming effectiveness for 50% of the hop duration for FH radio operating at 2000 hops/sec. The solution could intercept 3 simultaneous emissions which are running at random hops.

REFERENCES

[1] JanneJ Lehtom aki, Markku Juntti, Harri Saarnisaari, "*Detection of Frequency Hopping Signals With a Sweeping Channelized Radiometer* ," IEEE 2004

[2] Jri Lee, *"A 3-to-8-GHz Fast-Hopping Frequency Synthesizer in 0.18-_m CMOS Technology,"* IEEE JOURNAL OF SOLID-STATE CIRCUITS, VOL. 41, NO. 3, MARCH 2006

[3] Sandner, C.Wiesbauer, A.;Grewing, C.;Winterberg, K.;van Waasen, S.;Friedrich, M.;Li Puma, A 3GHz to 7GHz Fast-Hopping Frequency Synthesizer for UWB, *G. 2004 International Workshop on Ultra Wideband Systems Joint with Conference on Ultra Wideband Systems and Technologies.* Joint UWBST & IWUWBS 2004 (IEEE Cat. No.04EX812)

[4] Jinhua SunJiandong Li;Lijun Jin;Xiaojun Wu ,"*A channel-estimation-based equalization algorithm for fast frequency hopping radio,"* 14th IEEE

Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.

[5] Konstantinos Karkatzounis, PERFORMANCE EVALUATION OF DIFFERENT JAMMING STRATEGIES OVER UNCODED NONCOHERENT FAST FREQUENCY HOPPING MFSK COMMUNICATION SYSTEMS, NPS, September 2004

[6] Amer A. Hassan, Wayne E. Stark, and John E. Hershey*,"Error Rate for Optimal Follower Tone-Jamming,"* IEEE TRANSACTIONS ON COMMUNICATIONS, VOL 44, NO 5, MAY 1996

BIO DATA OF AUTHOR

S. Krishna Prasad received B.Tech degree in year 2009 in Electronics and Communications Engineering from JNTU Hyderabad, INDIA. He completed his training at NSS Communication Labs for Electronic Warfare system design. Currently He is working for development of ESM systems on FPGA platforms.