ANALYSIS OF SPREAD-SPECTRUM ALGORITHMS TO PREVENT JAMMING ATTACKS IN SAFETY-CRITICAL APPLICATIONS

Aysegul Aglargoz, (German Aerospace Center (DLR), Braunschweig, Germany; Ayseguel.Aglargoez@dlr.de), Valentin Bartkowiak (German Aerospace Center (DLR), Braunschweig, Germany), Holger Spangenberg (German Aerospace Center (DLR), Braunschweig, Germany)

ABSTRACT

The introduction of wireless sensor networks in aircraft aims to reduce the cable weight, increase the ease of layout and maintenance, and enable easier addition of new systems. Despite these advantages over wired sensor networks, wireless technologies raise several problems in terms of safety and reliability. One of the significant threats in using wireless data-transmission in aircraft is the risk of jamming attacks by interfering radio-waves. For this reason, the reliability of spread-spectrum data-transmission methods against jamming is assessed for wireless intra-aircraft communications, especially for the safety-critical applications. This paper investigates the effectiveness of the spread-spectrum techniques, Frequency-Hopping Spread-Spectrum (FHSS) and Direct-Sequence Spread-Spectrum (DSSS), for wireless avionic intra-communication. Even though these methods are well-defined, the critical requirements of avionics do not allow the direct use of the methods. The FHSS and DSSS methods were implemented in a wireless flight control system concept. The implementation of the algorithm is based on the design constraints of the flight control systems. A Bit Error Rate (BER) analysis is used to compare the spread spectrum methods. Since the FHSS system is more robust against jamming, the FHSS algorithm is implemented and verified by means of Software-Defined Radio (SDR) on an FPGA-based testbed. The results show the feasibility of the successful implementation of the FHSS algorithm on the testbed, which was developed according to the system parameters.

1. INTRODUCTION

Since the invention of wireless telegraphy, the technologies for wireless transmission have developed rapidly. With the current advances, intense ongoing research and refined applications, wireless systems nowadays take the place of wired systems in several fields, such as telecommunication and monitoring networks. Due to their ease of installation and maintenance, advantages over the aging and damaging of cables, the market of wireless system and their applications expand greatly. One of the well-known application fields of wireless technologies is Wireless Sensor Networks (WSN), which can observe the environment, send the data to a related control unit and can also act accordingly. These networks are commonly used in agriculture, military, manufacturing and transportation, since they are easy to install, enable monitoring of physically-refined spaces, and reduce the limitations of network expandability after installation [1].

In the field of aviation, substitution of wired networks with wireless equivalents is a novel approach, which intends to reduce the cable weight, increase flexibility and ease the introduction of new functionality in aircraft environment. However, strict requirements have to be fulfilled in terms of safety and reliability, which is known as Design Assurance [2]. According to it, the Design Assurance Level (DAL) shows the criticality of a system and is associated with measure of rigor applied to the design process. Safety-critical systems are classified as DAL - A in the failure condition classification, because the failure of their functions might cause catastrophic failure conditions, as in the case of aircraft flight control systems. These failures would prevent continued safe flight and landing. Therefore, the assessment of interferences becomes crucial to evaluate the safety and reliability aspects of wireless systems in aircraft.

Interferences on wireless avionics intra-communication systems are classified in [3] as unintentional and intentional disturbances and the effects of unintentional interference are discussed. In this paper, the main focus is given to analyzing effects of jamming signals as an example of intentional interferences and examining the countermeasures against jamming.

Jamming attacks are the most common intentional disturbances, which are unpredictable and can interrupt the data transmission for an unknown time interval, which might cause catastrophic failure conditions for safety-critical systems. To overcome these threats, possible countermeasures depending on the jammer types are listed in [4], such as channel surfing, wormhole-based anti-jamming techniques and defeating energy-efficient jamming. One of the proposed strategies dealing with

jamming attacks is the spread-spectrum method, which is considered as a solution in this article, due to its Commercial Off-The-Shelf (COTS) availability and the compatibility with the current hardware.

Spread-spectrum methods aim to expand the transmission signal bandwidth in order to reduce the effects of noise and jamming. In addition, the spread-spectrum coded signal is difficult to demodulate by a receiver except an intended receiver, since the random spreading/hopping pattern is unknown to the adversary. This makes the system more secure due to its noise-like spectrum and required demodulation effort.

Spread-spectrum methods are commonly used for commercial applications, such as IEEE 802.15.4 standards for wireless personal area networks and IEEE 802.11b for Wi-Fi, as well as secure communication for military use such as to prevent eavesdropping during World War I - II. Ref. [5] explains the importance of spread-spectrum methods in burgeoning security market. Ref. [6] considers advanced hybrid spread-spectrum methods as robust and secure wireless communication techniques for harsh environments.

Spread-spectrum techniques are also considered for safety-critical applications in railway communication. Ref. [7] presents a new spread-spectrum sequence for the enhancement of Communications-Based Train Control (CBTC) system, thereby overcoming jamming attacks. Ref. [8] explains the importance of security improvement mechanisms in the European Rail Traffic Management System and proposes several techniques, one of which is spread-spectrum for future railway communication to mitigate jamming attacks.

In this paper, two types of spread-spectrum methods are assessed: Frequency Hopping Spread Spectrum (FHSS) and Direct-sequence Spread Spectrum (DSSS), which are more viable for safety-critical applications due to their interference rejection potential [9]. FHSS method changes the carrier frequency swiftly and pseudo-randomly in several frequency channels. This makes FHSS resistant against interferences and due to its noise-similar characteristic, it prevents eavesdropping by adversary. DSSS expands the bandwidth of the data signal by using the Pseudo-Noise (PN) codes. PN codes are known by the transmitter and receiver, but unknown to a third-party user, which makes the transmission hard to intercept.

To analyze the feasibility of these two methods for safety-critical applications, the transceivers with FHSS and DSSS are simulated using Simulink. The transmission parameters of transceivers are based on wireless flight control concept and the design constraints of a flight control network are considered for simulations. Then, as intentional disturbances, jammers are modelled and introduced to the transmission channel. The resistance of each algorithm against jammers is measured by BER analysis and compared. According to the outcome of the simulations, the more resistant spread-spectrum algorithm is designed by using Xilinx System Generator, which is a tool to design systems in Simulink environment with a model-based approach. It enables HDL code generation, synthesizing and implementing the design on a FPGA. After the implementation of the transceiver on a FPGA-based SDR platform, it is validated with a testbed, which includes a host computer, an oscilloscope, Analog-to-Digital (AD) and Digital-to-Analog (DA) converters.

The paper is organized as follows. In Section 2, comparison of FHSS and DSSS algorithms is given. The comparison process is detailed by presenting the system parameters of flight control system concept, simulation method of FHSS and DSSS with Simulink, the jammer design methods and the simulation results. Section 3 is dedicated to the implementation and validation of FHSS on a FPGA-based SDR. In this section, the technical detail of the testbed, the implementation methods on the FPGA, validation and results of the implementation are explained. Section 4, Conclusion, concludes the paper and presents the possible improvement of the current design and the future directions of the work.

2. COMPARISON OF DSSS/FHSS TRANSCEIVERS

FHSS and DSSS transceivers are simulated to evaluate the immunity of transmission methods against jamming. Hence, firstly DSSS transmitter and receiver are simulated without any interference. After validating DSSS transceiver algorithm, FHSS transceiver is developed and verified without any intentional interference. In the last part of the simulations, jammers (J_k) are introduced to the transmission medium, as it is given in Figure 1. S_k stands for transmitted signal and R_k indicates received signal.

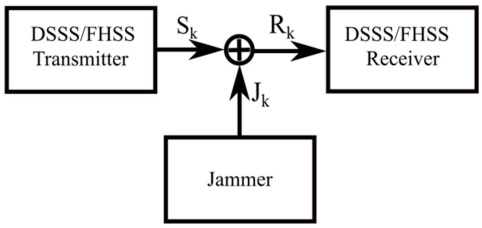

Figure 1. Transmission System Overview

2.1. System Parameters

As a case study, the wireless flight control system concept is chosen as a safety-critical system in an aircraft, which is presented in [3], to set the parameters of the simulations. The data-transmission rate up to 2 Mbits/s has to be supported, so that the necessary flight control system information can be sent in a certain time-interval. Due to the

lack of dedicated transmission band for wireless avionics intra-communication systems, the simulation is carried out in baseband with a bandwidth of 25 MHz. The transmission power is set to 10 dBm to keep the power level constant; however the crucial parameter for the simulations is the signal-to-jammer power ratio, which is also stated in Section 2.4.

2.2. DSSS Transceiver

The simulation of the DSSS transceiver can be divided into two main parts: transmitter and receiver. The transmitter consists of a Bernoulli binary generator, a PN sequence generator, a unipolar-to-bipolar converter and a mixer block. The Bernoulli binary generator produces flight-control data with a data rate of 2 Mbits/s, as set in Section 2.1. As PN sequence, the Kasami sequence is chosen due to its good cross-correlation characteristic. The Kasami sequence is generated at a chip rate of 32 Mchips/s, which is defined as the data rate multiplied by 16. The Kasami sequence generator is used to produce pseudo random sequence to modify the data to obtain a noise-apparent characteristic and spread the spectrum of the information data. After the data generation, the data signal and the Kasami sequence are converted into bipolar signals to obtain Non-Return-to-Zero (NRZ) signal behavior at the input of a multiplication block. Then the multiplication block is used as a mixer to modulate the data signal with the Kasami sequence to generate the DSSS data signal. The spreading signal is transmitted through the channel and fed into the receiver.

The main function of the DSSS receiver is to demodulate the incoming signal from the receiver and retrieve the information. Hence, the local replica of the PN sequence has to be generated and synchronized with the PN sequence which is used at the transmitter. Therefore, a two-stage synchronization process is carried out. The first step is for the coarse synchronization of the PN sequence, which is named as PN acquisition. When the signal is acquired, fine adjustments are done by PN tracking, in order to reach the best alignment of signals by means of a closed-loop [10].

The simulation of the receiver with the aforementioned synchronization stages is carried out as follows. The DSSS receiver contains a mixer, a correlator, a local PN sequence generator, an acquisition block, a tracking block and a search/lock clock generator [11]. The simplified block diagram of DSSS receiver and the connections of blocks are given in Figure 2.

The aim of the acquisition block is to sustain a coarse synchronization of the PN sequence; therefore, a cross-correlation is performed between the received signal and the locally generated Kasami sequence to obtain a measure of the similarities between two signals. The cross-correlation function contains a mixer and a bandpass filter, which is centered at 2 MHz. Then, a square law envelope detector is used to retrieve the envelope of bandpass-filtered signal.

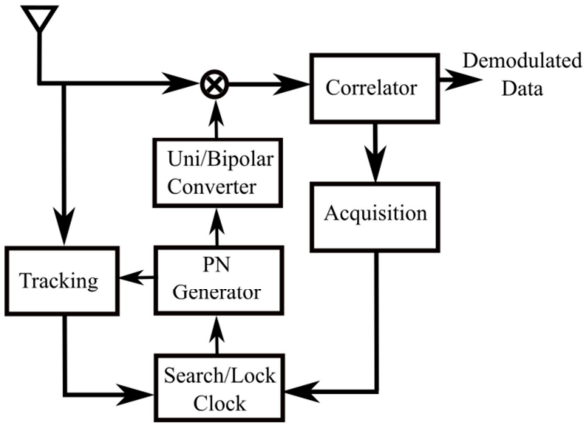

Figure 2. Overview of DSSS Receiver Architecture

After that the signal is integrated over the chip duration and sampled at the frequency of 2 MHz. A threshold is defined to determine if the signal is acquired. As an output, the acquisition decision signal is generated and fed into the Search/Lock clock generator.

The tracking block, in Figure 2, is designed according to the early/late gate method. The locally generated Kasami sequence and the received signal are used as inputs for the tracking block. In this block cross-correlations between the received signal and the early/late Kasami sequence are performed, and then the envelopes are retrieved with the square-law envelope detectors. The early envelope is subtracted from the late envelope to obtain an error signal. This error signal goes through a loop filter to retrieve the mean of the error signal and is fed into a Voltage-Controlled Oscillator (VCO). The VCO generates a sinus at 32 MHz. The sinus goes through a sign function to obtain a square signal and a bipolar to unipolar converter is used, so that the square signal takes values of 0 and 1 to perform logical operation. The output signal of the tracking block is fed into the Search/Lock clock generator.

The Search/Lock clock generator coordinates the output signals of acquisition and tracking blocks and generates the best possible synchronized clock to feed into the PN generator. When the signal is greater than the threshold, the phase of Kasami sequence is corrected. When the signal remains constant, above the threshold value, the acquisition block stops. The tracking block takes over control to keep the fine synchronization and correct phase error into the clock signal.

The Search/Lock clock block is an important part of the synchronization, which is shown in Figure 3. It consists of a clock generator, which uses a frequency of half the chip rate. This generated clock is combined with the acquisition signal with a NAND gate and fed into a J-K Flip-Flop for the phase correction.

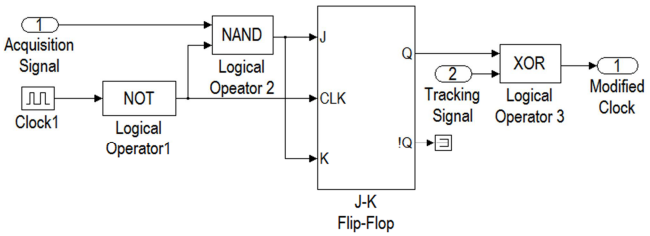

Figure 3. Simulink Block Diagram of Search/Lock Clock

J and the K input are tied together, which constructs a T Flip-Flop. The coarse corrected clock by acquisition is combined with the tracking corrected clock by a XOR gate. When the signal is acquired, the acquisition signal stays above the threshold and a constant value of 1 is sent to the search lock clock. When the acquisition process is finished, the tracking process starts and the clock signal, which is corrected by tracking, is used as a clock for the Kasami sequence generator.

Lastly, when the PN sequence is synchronized, the DSSS demodulator retrieves the information data with a mixer by multiplying the received signal and the synchronized Kasami sequence (half chip delayed).

2.3. FHSS Transceiver

The simulation of FHSS is based on two main parameters: dwell time and number of sub-channels. For the simulation, 39 sub-channels and a dwell time of 100 μs are used.

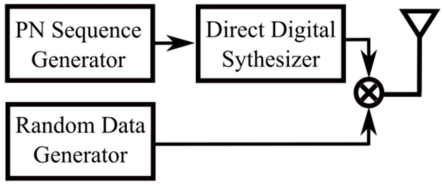

Figure 4. FHSS Transmitter

The transmitter of FHSS is similar to DSSS. The FHSS transmitter consists of a Bernoulli Binary generator as a random data generator, a PN sequence Generator, a Direct Digital Synthesizer (DDS) and a mixer block, which are connected as in Figure 4. PN sequence is generated by using nine D Flip-flops to create a random hopping pattern. To obtain a sequence with maximum length, the generating polynomial is chosen as $p(x) = x^9 + x^5 + 1$ [12]. The DDS generates different carrier waves according to the variable input. It is constructed with a two dimensional lock-up table, which contains the sub-channel information to hop. The sub-channel spacing is chosen as 5 kHz. A mixer is used to modulate the data signal with the hopping carrier to obtain the FHSS signal. The output power block adjusts the output power FHSS signal to 10 dBm, which is set in Section 2.1.

The FHSS receiver has a similar structure as the DSSS receiver for the synchronization, as shown in Figure 5. In comparison to the receiver of DSSS in Figure 2, the PN generator is connected to a frequency synthesizer. The other difference is the structure of the correlator. After the local hopping carrier, which is generated by frequency synthesizer, is conjugate, it is used to feed a mixer with the received signal. After that in the correlator, an integrator is used to integrate over a hop. A sampling is performed at 2 MHz and finally, a decision is taken to retrieve the information in the transmitter.

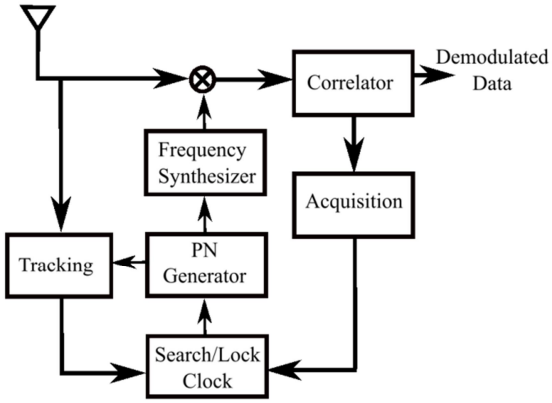

Figure 5. Overview of FHSS Receiver Architecture

2.4. Worst-case Jammer Design and Jamming Resistance Evaluation Method

Jammer waveforms are modeled and introduced into the transmission medium as given in Figure 1. Several jamming waveforms can be present in the transmission medium, which are classified according to their distribution in time and frequency. In simulations, different types of jammers are used: tone, multi-tone, narrowband, broadband and partial-band. According to [10], the system under broadband jamming is defined as baseline performance and the worst case jammers are indicated, which are multi-tone jammers and partial-band jammers.

In this paper, the performance of spread-spectrum methods under worst-case jamming is assessed. Therefore, a brief explanation of each jammer, partial-band and multi-tone jammer is given. Multi-tone jammer is implemented with a summation of several sinusoidal waves with different phases, which is given in Equation 1 [10].

$$J(t) = \sum_{l=1}^{N_t} \sqrt{2J/N_t}\ \sin(\omega_l t + \theta_l) \qquad (1)$$

Random phase θ_l is produced in the range of [0, 2π] and $N_t = 100$ tones are generated. J indicates the time averaged power of jammers waveform. The Power Spectral Density (PSD) of this multi-tone jammer signal is given in

Figure 5. As it is seen in this Figure, the signal spectrum is between 5 MHz and 15 MHz, and contains several tones.

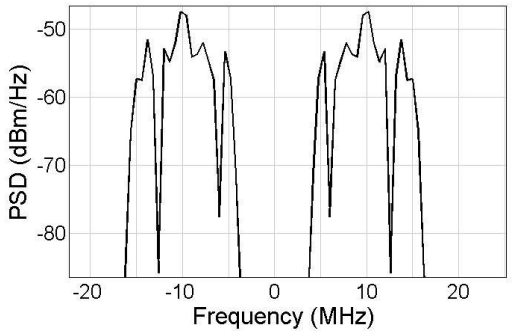

Figure 6. Spectrum of Multi-Tone Jamming Signal

The partial-band jammer is modelled with a random-noise generator and a band-pass filter to adjust the bandwidth of the signal. The Gaussian noise is distributed over a limited bandwidth. The bandwidth of partial-band jammer is chosen as 10 MHz. The cut-off frequencies of the filter are chosen as 5 MHz and 15 MHz.

The jammed ratio of the signal spectrum, ρ, given in Equation 2, is a relevant measure for the performance evaluation of jammers, where W_{ss} is the signal bandwidth and W_j is the jammed bandwidth.

$$\boldsymbol{\rho = \frac{W_j}{W_{ss}} \leq 1} \qquad (2)$$

To analyze the effect of jammers, a BER analysis is carried out for several jamming powers and two types of jammers. Jammer power at the input of the receiver, N_j, is varied as 5, 10, 15, 20 dBm to obtain different signal-to-jammer power ratio. For simulations, the crucial measure is the signal-to-jammer power ratio, not the power of each of each system. 1000 bits are transmitted to evaluate the performance of the system under jamming attacks. The jammed ratio ρ is chosen as 0.4 to be consistent for each type of jammer. The variation in jammed ratio is directly related to BER. When the jammed ratio increases, the BER values also increase.

2.5. Simulation Results

The performance of DSSS and FHSS is evaluated with BER graphs in comparison to single-carrier data-transmission system, which is used as a reference system to measure the improvement by using spread-spectrum techniques. The immunity of each algorithm against multi-tone and partial-band jamming is summarized by Figure 7 and Figure 8.

Figure 7 is obtained to show the multi-tone jamming susceptibility of FHSS, DSSS and single-carrier transmitter. Therefore, the jamming power is changed, while keeping transmitted signal power E_b constant (10 dBm) according to the design requirement in Section 2.1; the BER analysis is carried out. With the varying jamming power, the transmitted and received bits are compared. As an outcome, the BER versus E_b/N_J (Signal-to-Jammer Power Ratio) graph is obtained, which is seen in Figure 7. The negative E_b/N_J values indicate jamming power is higher than transmitted signal power, while positive values reveal that the power of transmitted signal is higher than the jammer power.

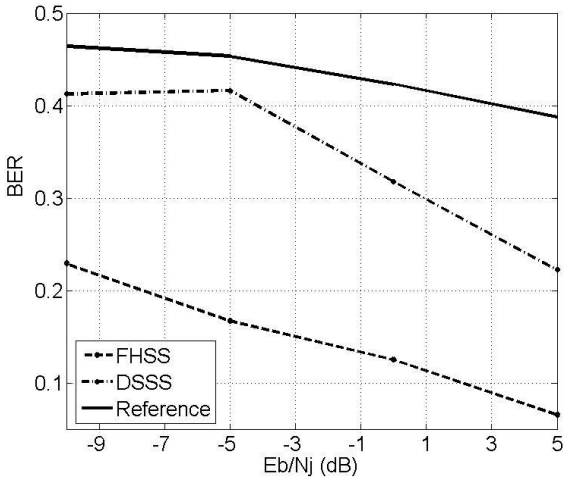

Figure 7. Evaluation of DSSS/FHSS against Multi-tone Jamming

The single-carrier scheme is indicated by the reference curve, which shows the worst-case conditions, when the data are transferred in a single frequency band. As a result, it is seen that the immunity of FHSS is higher than DSSS and single-carrier transmission techniques. If the DSSS and FHSS curves are compared, the FHSS jamming-tolerance is twice as that of DSSS in terms of BER. Furthermore, when the power of the jammer (N_j) is increased, the BER performance becomes very poor for each type of communication scheme.

In Figure 7, BER values are obtained which are greater than the jammed ratio of 0.4 in case of high jamming powers. The main reason of these BER values is that the data signal and the generated jamming signal do not show ideal flat characteristics and vary slightly in amplitude and frequency. Therefore the jammed ratio also changes, which results in changes in the BER with values greater than 0.4 being obtained.

Figure 8 shows the partial-band jamming susceptibility of transceiver implemented by means of FHSS, DSSS and single-carrier transmission schemes. The same method is followed to obtain the BER graph, as multi-tone jammer in Figure 7. BER values reach minimum for FHSS. It means the FHSS is more robust against partial-band jamming than DSSS and signal-carrier transmission schemes. The

improvement of DSSS according to reference is rather low, like in Figure 7, whereas the improvement of the FHSS in comparison to DSSS is more than twice in terms of BER. The graph also validates that the BER decreases when the jamming power is decreased, same as in Figure 7.

If Figure 7 and Figure 8 are compared, BER values are higher under multi-tone jamming. It is concluded that more bits are corrupted under multi-tone jamming than partial-band jamming. The multi-tone jammers are more effective, since the insertion of continuous-wave tones into a transmissions channel is the most influential way for a jammer to corrupt more bits.

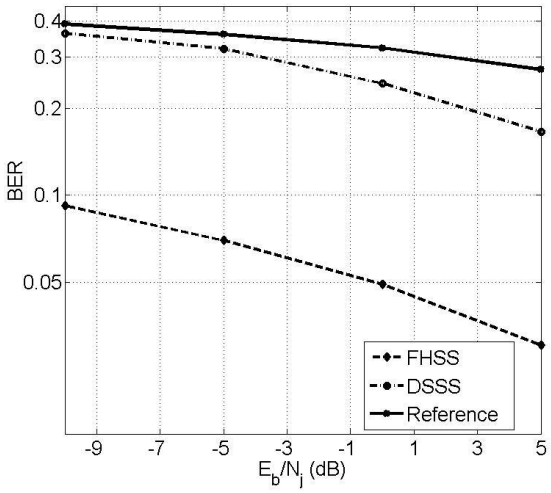

Figure 8. Evaluation of DSSS/FHSS against Partial-band Jamming

To show the improvement of the system only with spread-spectrum techniques, the transceiver is isolated from the other data enhancement/protection methods. To measure the effects of spread spectrum algorithms, BER values are obtained only using these techniques. The BER values that are seen in Figure 7 and 8 do not reflect the overall performance of the system. They are rather high for safety-critical applications but they show the enhancement of the system. The overall performance also depends on additional methods, such as modulation, channel and error-correction coding. According to outcome of the simulation, it is concluded that FHSS is a promising method to improve the overall system performance.

3. IMPLEMENTATION AND TEST OF FHSS TRANSCEIVER WITH A SDR

In this section, the hardware development stages of FHSS algorithm are explained. The implementation method of the FHSS with a SDR testbed, required software and setup components are briefly presented. Finally, the results of the validation and implementation are given.

3.1. SDR Specifications and Xilinx System Generator

The SDR of Nutaq, Perseus 601X [13], is chosen as a development platform for the FHSS implementation. It is Xilinx Virtex 6 LXT FPGA based SDR, which provides high-logical performance and low power consumption, as well as being suitable for telecommunication applications [14]. Besides the FPGA, SDR consists of a memory, testing and several debugging interfaces, such as Joint Test Action Group (JTAG) FPGA, USB Universal Asynchronous Receiver/transmitter (UART). The connection with a host computer is established via Gigabit Ethernet (GigE) [13]. It provides reconfigurable I/O pins for connection of FPGA Mezzanine Card (FMC) cards. In this application, Analog-to-Digital-to-Analog Converter (ADAC) FMC card, ADAC250, is used for simplicity. ADAC250 has high speed converters, which are two 14-bit 250 MSPS Analog-to-Digital Convert (ADC) and two 16-bit 1 GSPS Digital-to Analog Converter (DAC) [15]. This FMC card supports multiple clock configurations and integrated programmable gains.

The FHSS algorithm is developed by using high-level hardware development tool, Xilinx System Generator. It provides libraries to Simulink, which reduces the development time, provides functional blocks for telecommunication applications and simplifies the hardware co-simulation. In addition, Nutaq libraries are used to communicate with Perseus, modify several parameters of ADAC250, configure the registers, test and debug the algorithm. More information is given in section 3.3 about the development of test environment with Nutaq blocks.

3.2. FHSS Algorithm Implementation

FPGA development is based on Xilinx System Generator, thereby the FHSS transceiver is developed by using Xilinx blocks, which provide DDS, Linear Feedback Shift Register (LFSR), filter design and mathematical blocks for this design. Firstly, the transmitter part of the transceiver is designed, which includes two LFSRs as random data generation, given in Figure 9. One of the LFSR blocks with degree of 7 is used to generate hopping pattern. The feedback polynomial of it is chosen to reach maximum length sequence, $p(x) = x^7 + x^6 + 1$. Then, an algorithm is developed to limit the number of sub-channels up to 39. The pseudo random sub-channel index is fed as an input to the Direct-Frequency Synthesizer (DFS) to generate carrier with the given sub-channel index.

The DFS contains a DDS block, which generates sinus carrier signal. The sub-channel spacing is chosen as 5 kHz. The random information data are generated by LFSR and converted to a bipolar signal and modulated by means of a carrier signal. At the output of the frequency hopping modulator, a signal with a dwell time of 100 μs is obtained.

An efficient hopping pattern is observed, if all the sub-channels are in use. The design parameters are summarized in Table 1.

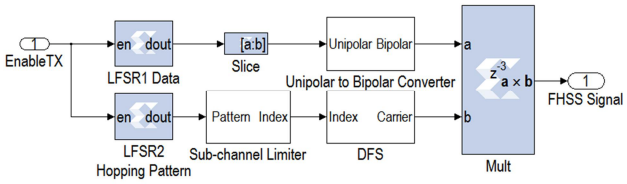

Figure 9. Structure of FHSS Transmitter with Xilinx Blocks

The second part of the transceiver is the FHSS receiver. For simplicity of the design, it is assumed that PN sequences are synchronized. The FHSS receiver contains multiplication, integrator, sampling and decision blocks. The received signal and the carrier signal are multiplied. Under the given assumption, the locally generated carrier signal and the carrier that is generated in the transmitter are identical. After the multiplication, the output signal is integrated over one symbol duration. After integration, the signal is sampled at 10 kHz to detect data bits. The sampling is done by an embedded Hardware Description Language (HDL) code and a clock generated by a free-running counter with a bit of output. The resampled data are compared with zero data to obtain binary data at the output of the receiver.

Table 1. Implemented FHSS Transmitter Parameters

FHSS Parameters	Value
PN Generator Type	LFSR
LFSR Length	7
Sub-channel Spacing	5 kHz
Dwell Time	100µs
Number of Channels	39
ADAC Rate	200 MHz

After completing transceiver simulation, the maximum path delay is calculated to compensate the delay between transmitted and received signal. To verify the algorithm, BER analysis is carried out.

3.3. Testbed Development and Testing

The validation of the algorithm is followed by including Nutaq data communication blocks, which are used to configure registers and parameters of ADAC.To receive real-time signals after FPGA implementation by the host computer, the RTDEX block is appended to the design. According to the design in Figure 10, the signal after ADC is retrieved to observe errors due to ADAC. Two enable signals are introduced to control the transmitter and the ADAC250.

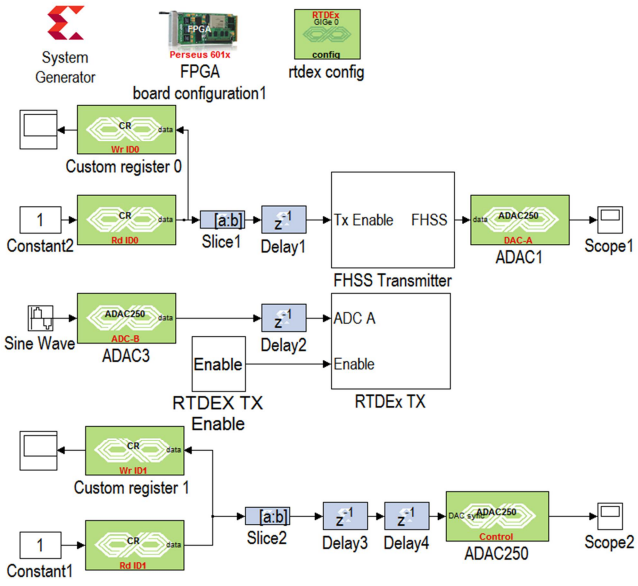

Figure 10. FHSS Transmitter Design

After including necessary blocks for communication, the design is synthesized. Then, the design is implemented, which includes translation, mapping and placement & routing. Register-Transfer Level (RTL) schematic is obtained and it is verified that the timing constraints are fulfilled. After verifying, the generated .bit file is used to configure FPGA by using iMPACT tool.

After the configuration of the FPGA, signals are validated in two different ways. By the first method, the output signal of transmitter is obtained by an oscilloscope with a sampling rate of up to 4 GSa/s. The second way of the validation is done by transferring the real-time signal to a host computer via GigE; thereby a host application has to run on the computer. In addition, the contents of registers are also modified through host application according to needs, such as the enable signal in custom register 0, which is seen in Figure 10. Moreover, some properties of DAC/ADC can be chosen through the host application interface. The sampling rate of DAC is chosen as 200 MHz. The interpolation parameter is chosen as the highest possible, which is 4 in this case. An amplifier is used to retrieve higher power at the oscilloscope input to distinguish transmitted signal from other signals.

3.4. Implementation Results

After completing the design of FHSS transceiver including Nutaq communication blocks, the design is implemented on

a Perseus 601X AMC. The results of implementation can be classified into two parts.

The first part is the verification of design constraints by checking compilation reports, which are generated during synthesis, place & route by Xilinx Platform Synthesis (XST). The timing reports show the clock frequency of the system reaches 100 MHz and the timing constraints are met. The resource utilization shows only 2 % of the resources are used, therefore parallel implementation of more complex algorithms, such as Multiple-Input and Multiple-Output, (MIMO) SDR transceiver, is feasible for improvements of the algorithm.

The second part is the validation of the generated waveform by the oscilloscope. The output of DAC is connected with a Micro-Miniature Coaxial (MMCX) to SubMiniature Version A (SMA) cable to the oscilloscope. Figure 11 shows the single run of the output. The X-axis indicates the relative time and the Y-axis shows the voltage level of the waveform. As it is seen in Figure 11, on a randomly chosen time-interval, waveforms with 4 different frequencies are observed. It is verified that the frequency is changed every 100 μs, which is stated at the beginning of the design as a dwell-time. In addition, the amplitude of the signal changes for different frequencies because of the characteristic of DAC. DAC is DC coupled and shows slight change at the amplitude for low and high frequencies.

4. CONCLUSION

In this paper, the simulation of wireless transceivers is demonstrated with two types of spread-spectrum algorithms, DSSS and FHSS, validated using BER analysis. After introducing a jamming signal into the transmission channel, BER analysis is performed and the effects of multi-tone and partial-band jammers on the transmitted signal are observed. The result of the BER analysis indicates that FHSS is two times more resistant than DSSS against multi-tone and partial-band jamming attacks. With this outcome of simulations, the FHSS transceiver is designed with Xilinx System Generator in Simulink environment and implemented on a Virtex-6 FPGA-based SDR platform.

The prototype is validated by a testbed of Nutaq communication blocks, host computer and an oscilloscope. It is concluded that the transmitter works according to design requirements of the case-study. The receiver is validated with BER analysis without additional interference. The jamming-resistance of FHSS shows that the FHSS technique can be considered to enhance the security and reliability of wireless systems, especially wireless avionics intra-communications. However, to assess the overall safety and reliability of the wireless data-transmission, modulation, channel coding and the encryption methods should be also considered and added to the hardware implementation.

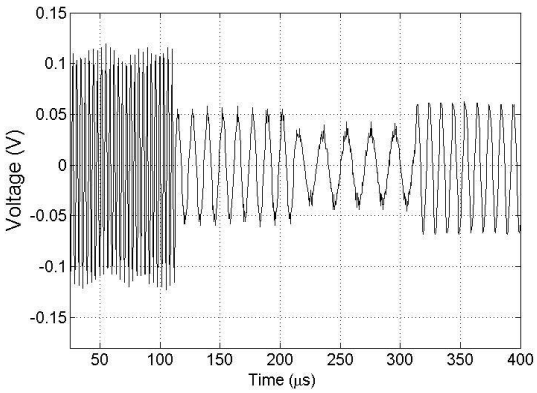

Figure 11. FHSS Transmitter Output Waveform

As further research, the improvement of synchronization algorithm in FPGA development is considered to obtain more precise synchronization. Furthermore, to implement a dynamic frequency-hopping system, a spectrum-sensing module will be developed; thereby an unknown hopping-pattern can be obtained to increase the security and reliability of the systems. In addition, hybrid spread-spectrum techniques will be also developed to assess the performance against jammers and compare with the current FHSS implementation.

5. ACKNOWLEDGMENT

This work is supported by German Federal Ministry for Economic Affairs and Energy (BMWi).

6. REFERENCES

[1] M.A Labrador. Smith and P.M. Wightman, Topology Control in Wireless Sensor Networks, Springer, USA, 2009.

[2] RTCA, SC-180, DO-254, Design Assurance Guidance for Airborne Electronic Hardware, April 2000.

[3] A. Aglargoz and H. Spangenberg, “Safety and reliability analysis of wireless data communication concepts for flight control systems,” in Digital Avionics Systems Conference (DASC), 2014 IEEE/AIAA 33rd, pp.2E2-1-2E2-12, Oct 2014.

[4] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, “A Survey on Jamming Attacks and Countermeasures In WSNs”, Communications Surveys & Tutorials, IEEE , vol.11, no.4, pp.42,56, Fourth Quarter 2009.

[5] B. Gaston, “Applications of Spread-Spectrum Radio Technology for the Security Market,” Security Technology, 1994. Proceedings of IEEE, 28th Annual 1994 International Carnahan Conference on, pp.86,91,Oct 1994.

[6] M.M Olama, X. Ma; T.P. Kuruganti, S.F: Smith, S.M. Djouadi, "Hybrid DS/FFH spread-spectrum: A robust, secure transmission technique for communication in harsh environments," in Military Communications Conference, pp.2136-2141, Nov. 2011.

[7] Z. Peng, G. Li, H. Wang and Q. Wu, "A Wireless Transmission Mechanism of the Wireless CBTC System and Performance Analysis," International Conference on Audio,

Language and Image Processing (ICALIP), pp.443-448, July 2008.

[8] I. Lopez and M. Aguado, "Cyber Security Analysis of The European Train Control System," in Communications Magazine, IEEE , vol.53, no.10, pp.110-116, Oct 2015.

[9] D.T. Magill, F.D. Natali and G.P. Edwards, "Spread-spectrum Technology for Commercial Applications," Proceedings of the IEEE, vol.82, no.4, pp.572-584, April 1994.

[10] M. Simon, J. K Omura, R. A. Scholtz, B. K. Levitt, "Spread Spectrum Communications Handbook", Revised Edition, Mc-Graw Hill, 1994.

[11] N. Shirude, M. Gofane, and M. Panse, "Design and simulation of radar transmitter and receiver using direct sequence spread spectrum," Electronics & Communication Engineering Journal, vol. 9, no. 3, pp. 56–65, Jun. 2014.

[12] J. Proakis and M. Salehi, Digital Communications, Third edition, McGraw Hill, New York, 1995.

[13] Nutaq, Nutaq Persus 601X, Virtex-6 AMC with FMC site, Product Sheet.

[14] Xilinx, Virtex-6 Family Overview, Product Specification, Aug 2015.

[15] Nutaq, ADAC250, High-speed dual A/D and D/A FMC module, Product Sheet.