FPGA-Based Implementation of a Hybrid DS/FFH Spread-Spectrum Transceiver

Stephen M. Killough[1], Mohammed M. Olama[2], Teja Kuruganti[2], and Stephen F. Smith[1]
[1]Measurement Science & Systems Engineering Division
[2]Computational Sciences and Engineering Division
Oak Ridge National Laboratory
Oak Ridge, TN 37831, USA
Email: {killoughsm, olamahussemm, kurugantipv, smithsf}@ornl.gov

***Abstract*—In recent years there has been great interest in using hybrid spread-spectrum (HSS) techniques for commercial applications, particularly in the Smart Grid, in addition to their inherent uses in military communications. This is because HSS can accommodate high data rates with high link integrity, even in the presence of significant multipath effects and interfering signals. A highly useful form of this transmission technique for many types of command, control, and sensing applications is the specific code-related combination of standard direct-sequence modulation with "fast" frequency-hopping, denoted hybrid DS/FFH, wherein multiple frequency hops occur within a single data-bit time. In this paper, we present the efforts carried out at Oak Ridge National Laboratory toward exploring the design and implementation of a hardware prototypic hybrid DS/FFH spread-spectrum radio transceiver using a single Field Programmable Gate Array (FPGA). The high integration within a single FPGA allows the various subsystems to easily communicate with each other and thereby maintain tight synchronization. Experimental results are presented to show the receiver sensitivity and jamming-rejection capability of the implemented hybrid DS/FFH spread-spectrum system under widely varying design parameters.**

Keywords—Hybrid spread-spectrum; direct-sequence; frequency-hopping; jamming; Field Programmable Gate Array (FPGA); Phase-Locked Loop (PLL)

I. INTRODUCTION

Hybrid spread-spectrum (HSS) systems, which combine direct-sequence (DS) and frequency-hopping (FH) spread-spectrum (SS) techniques, are attractive for their strong multiple-access capabilities, resistance to multipath fading and intentional/unintentional jamming, and the security they provide against eavesdroppers [1]-[6]. In recent years there has been great interest in using HSS systems for commercial applications, particularly in the Smart Grid (SG).

Based on the hopping rate, an HSS system is classified into a hybrid direct-sequence/slow frequency hopping (DS/SFH) system or a hybrid direct-sequence/fast frequency hopping (DS/FFH) version. In hybrid DS/FFH systems, multiple frequency hops occur within a single data-bit time. Specifically, each bit is represented by chip transmissions at multiple frequencies. If one or more chips are corrupted by multipath or interference in the RF link, statistically a majority should still be correct. Standard or slow frequency hopping, in contrast, transmits at least one (and usually several) data bits in each hopping interval. DS/FFH systems have not been previously widely implemented in many commercial or industrial applications since fast frequency-hopping rates were limited by the technology of frequency synthesizers. Today's extremely fast hopping speed direct-digital synthesizers (DDSs) [7] are rapidly becoming an alternative to the traditional frequency-agile analog-based phase-locked loop (PLL) synthesizers. Output frequencies with micro-Hertz resolution and sub-degree phase tuning capabilities can thus be readily achieved using a single integrated circuit (IC).

Most of the works related to HSS in the literature have addressed evaluating its performance under different modulation techniques [1], channel conditions [2], multi-user interference [3], jamming [4], and their combinations [5], [6]. These works have shown that hybrid DS/FFH outperforms the existing standard DSSS and FHSS methods on wireless networks. In this paper, we present the efforts carried out at Oak Ridge National Laboratory toward exploring the design and implementation of a hardware prototypic hybrid DS/FFH spread-spectrum radio transceiver using a single Field Programmable Gate Array (FPGA). The high integration in a single FPGA allows the various subsystems to easily communicate with each other and thereby maintain tight synchronization. The hybrid DS/FFH prototype is optimized for a typical SG utility application. We present the challenges we faced in the design and implementation stages and how we overcome them. Experimental results are presented to show the receiver sensitivity and jamming-rejection capability of the implemented hybrid DS/FFH spread-spectrum system under widely varying design parameters.

II. TECHNIQUES FOR HYBRID DS/FFH IMPLEMENTATION

The hardware implementation of a hybrid DS/FFH system requires more advanced programing techniques such as Software Defined Radio (SDR) to allow the various subsystems to be implemented in a single Field Programmable Gate Array (FPGA). This high integration allows the various subsystems to easily communicate with each other and maintain good synchronization. Implementation on a single

FPGA also allows the various local oscillators and other timing circuits to be coherently locked in phase thus insuring proper phase alignment for the radio signals. This is especially important for the various circuits that turn on and off between frequency hops.

Although the FPGA maintains good alignment among the various segments within the transmitted packet, the analog circuitry associated with the radio causes phase discontinuities when the radios hop to a different frequency. This is because the antennas, analog filters, and outside terrain all have a phase-versus-frequency characteristic that will cause the radio signal to have a different carrier phase relationship compared to operation on the previous frequency. Although it is technically possible to calibrate for this effect, the hybrid DS/FFH system is specially designed to use a modulation method that does not depend on a consistent phase relationship between frequency hops. An additional advantage to this methodology is that the carrier phase only needs to be consistent within a single DS sequence and not long term, therefore circuitry to maintain long term phase coherence, such as a Costas loop [8], is not necessary.

There are two major hardware methods for implementing the FH portion of the system: **(1)** those being a conventional receiver with a hopped local oscillator (LO) and conventional detector, or **(2)** a fixed LO and wide receiver with the channel separation and detection performed in software. There are particular cost and performance advantages with each technique. The hopped LO enables a conventional radio except for the agile LO frequency. Off-channel interference can be thoroughly rejected with additional analog filtering and dynamic range is only limited by the linearity of the input stage transistors. Achieving rapid switching to a new LO frequency precludes the use of a single Phase Lock Loop (PLL) since the loop cannot lock to a new frequency quickly enough. An alternative is to have two separate PLL oscillators that hand off the LO task to each other, with one oscillator performing the LO task while the other one is locking to the next frequency. Another alternative is to use a direct digital-synthesis oscillator because of its rapid switching frequency. Another advantage of the conventional radio approach is that the intermediate frequency can be lower, which would enable a slower analog-to-digital converter to be used. However, the slower sample rate would not significantly reduce the size or speed of the FPGA, since the computational limitation of the FPGA is from the correlation algorithms that are required for both of the two FH methods. A significant disadvantage of the hopped-LO approach is that the receiver will only be able to listen on one frequency at a time. Although a specific frequency can be prearranged for the radios to make their initial contact via the packet preamble, there would be no provision for making contact on another frequency if the intended frequency is being jammed. However, if a very precise time reference is available on both the transmitter and receiver, it would be possible to coordinate a changing initial contact frequency.

We decided to use the SDR methodology because of its flexibility in changing the system to evaluate new concepts. The methodology has also proven to be very powerful in that the vast majority of the signal processing components can be placed in a single FPGA, which enables tight synchronization and communication between the subsystem components. The entire HSS band is down-converted to an intermediate frequency, digitized, and sent to the FPGA. Within the FPGA, look-up-table based local oscillators down-convert the individual FH channels to baseband. These baseband signals are then decoded using DS correlators and stored in a buffer for subsequent delivery to a host computer.

Software implementation of the detection and second down-conversion algorithms enable very stable and consistent performance between the individual FH channels. Although phase consistency between FH channels is not required at this time, the availability of this consistency would be useful for higher performance versions of hybrid DS/FFH in the future. The SDR implementation also allows the receiver to receive more than one radio at the same time. This is useful for high-throughput systems, but this has also been a crucial feature on the present radio implementation because it allows redundant detection of the packet preamble. To provide jamming resistance, the receiver must listen on several channels at once, since any prearranged channel could be jammed.

Because of the wider bandwidth required to digitize the entire band, the SDR system requires a higher speed analog-to-digital converter and extra circuitry in the FPGA to perform digital filtering that would normally be performed in analog hardware. Since digital computing hardware is continually becoming more cost effective, the SDR implementation will not necessarily be more expensive than a traditional analog intermediate frequency system. SDR implementations still have fundamental limitations in that the dynamic range and interference rejection capability of the system will be limited by the resolution of the analog-to-digital converter. Conversely, analog systems can add more filtering to obtain very high overall performance levels.

III. ORNL Specific Hybrid DS/FFH Implementation

The hybrid DS/FFH prototype was designed to demonstrate the fundamental advantages of the HSS system, such as jamming resistance, difficulty of unwanted interception, robust performance, and reasonable cost. The prototype operates in the unlicensed 902-928 MHz ISM band, although target applications such as the SG may ultimately use a dedicated frequency band.

The work in [9] discusses the optimal selection of hybrid DS/FFH parameters, such as DS code length, frequency hopping rate, and packet length. These parameters can be optimized with respect to jamming resistance, channel capacity, interference to other users, and difficulty in eavesdropping. The parameters chosen for the hybrid DS/FFH prototype are considered to be nearly optimal at this time, based on the available ISM bandwidth and FPGA capabilities, although more optimum values may be chosen in the future.

As shown in Fig. 1, the HSS unit splits the 902-928 MHz band into ten separate FH channels, each of which sends a DS spread spectrum signal with a 1.25-MHz chipping rate. An analog mixer converts these frequencies up or down for the transmitter or receiver, respectively, for use by the digital-to-analog or analog-to-digital converters. The SDR algorithms work over a designated 12.5-35.0 MHz frequency range.

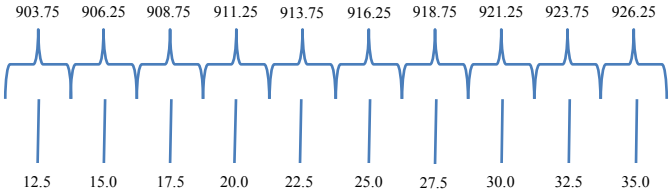

Fig. 1. The prototype hybrid DS/FFH FPGA radio frequencies in MHz.

Each DS signal is a 63-bit length Maximal Length Linear Feedback Shift Register code, although more advanced Gold or Kasami codes could also be used. After each 63-bit length code is transmitted, the system hops to a new frequency. The same data in the DS signal is repeated three times on three different frequencies, and at the receiver a two-of-three majority voting decision scheme determines the correct information even if one of the frequencies is completely blocked.

Of particular interest is the methodology for modulating the DS signal. Traditional PSK modulation requires a preamble at the beginning of the packet to determine the reference phase and a Costas Loop or similar mechanism to maintain this phase reference. With HSS in multipath channels, this phase reference is lost after each frequency hop, so HSS performs its DS modulation by shifting the start time of the code. The incoming signal is correlated with local copies of the shifted code pattern and an early-late voting system determines the amount of shift of the received signal. The correlation algorithm is independent of the carrier phase of the signal. The number of bits that can be encoded by this method is demonstrated by the early-late diagram described in Fig. 2.

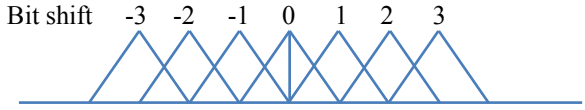

Fig. 2. Code-Phase-Shift-Keying modulation for the DS signal.

The bit-shift number refers to the amount of bits that the local DS code has been shifted for performing the correlation. To prevent ambiguous results from a correlation being between two bits, only every other bit position is used, which results in 31 positions available for each code word. The HSS prototype has a separate in-phase (I) and quadrature (Q) channel within each DS sequence, with a different DS code used for the I and the Q phases. For convenience, only 16 of the 31 positions are used for each of the I and Q. This results in an even 8 bits, per DS sequence. The I and Q channels are combined in an offset QPSK arrangement to provide a near constant-envelope signal. Four bytes of blank data are sent at the beginning of the packet as a preamble to set the reference DS start time.

A different interpretation of this methodology would be that the DS code is shifted because of a different time-of-flight, similar to GPS or continuous wave radar. Similar to the way GPS can achieve precise time-of-flight resolution, it can be expected that this methodology can be further developed to obtain higher bit capacity. Ref. [10] explores this methodology for multiple users occupying a channel simultaneously.

The HSS channel capacity is calculated by dividing the chip rate, or 1.25 MHz, by the 63-bit code length to get 19,841 DS sequences per second. Since the data is replicated three times for redundancy, the actual throughput is 6,613 DS sequences per second. Since each DS sequence contains 8 bits of data, the data throughput is 52,910 bits per second. The HSS prototype is optimized for reading household utility meters for SG applications and thus only requires 32 bytes, although the system has operated successfully with 256-byte packets.

IV. SDR Implementation

The prototype hybrid DS/FFH system is based on a Xilinx Virtex-4 FPGA for performing the digital signal processing. The hardware setup is described in Fig. 3. The FPGA, A/D, and D/A operate synchronously together at 100 MHz to allow operation on analog signals to a practical limit of 40 MHz. The D/A has 16-bit resolution for a dynamic range of 96 dB, and the corresponding A/D has 14-bit resolution for a dynamic range of 84 dB. The microcomputer loads and unloads data to the FPGA and communicates with sensors and other computers using Ethernet, RS232 or analog signals.

Fig. 4 describes the transmitter portion of the FPGA code, which consists of the data buffer, modulator, and ten local oscillators for generating the hopping carriers. Raised-cosine waveshaping is used to reduce the spectral sidebands. The receiver uses the same local oscillators for detecting signals, and all ten channels must be simultaneously received to detect the preamble during jamming situations. To acquire the packet preamble, a spread-spectrum correlator continually looks for the initial DS pattern on all channels. Once the preamble is detected, an internal timing sequence compares the signal with shifted copies of the DS code via a simple correlator. The shifted copy of the DS code that provides the strongest correlation then demodulates the actual data.

The preamble-detection section of the receiver is shown in Fig. 5. To make the signal detection independent of the carrier phase, both phases of the carrier (I and Q) are correlated with the preamble's DS code. However, the phase relationship must remain consistent during the duration of the DS sequence.

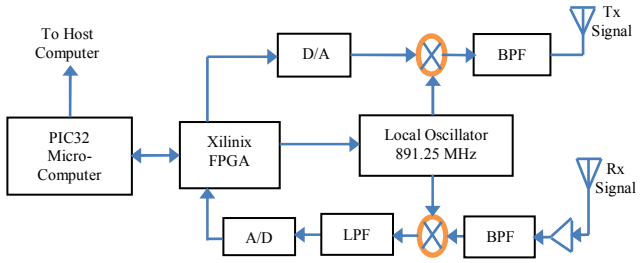

Fig. 3. Hardware setup for the hybrid DS/FFH prototype.

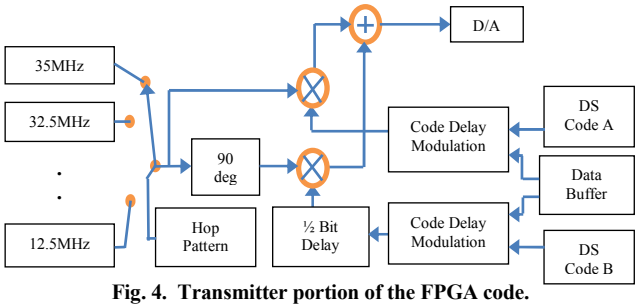

Fig. 4. Transmitter portion of the FPGA code.

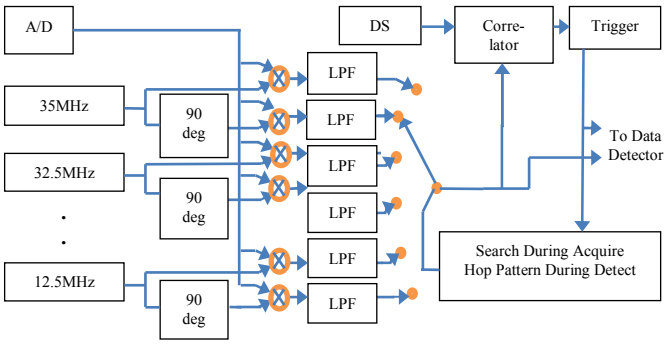

Fig. 5. Preamble-detection section of the receiver.

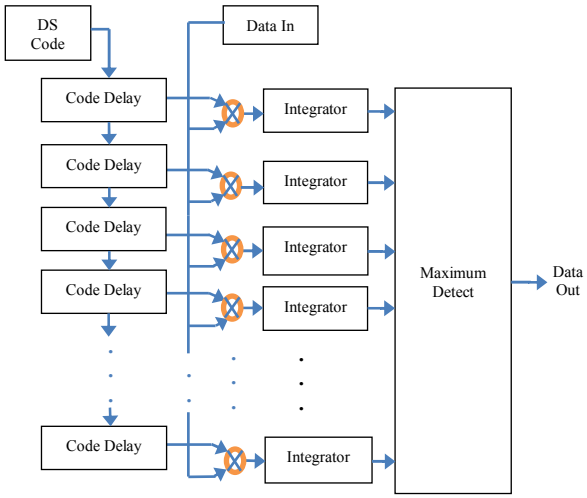

Fig. 6. Data-detection section of the receiver.

A key limitation of the radio's selectivity is the digital low-pass filter (LPF) implemented in the FPGA. Because we were limited to integer arithmetic in the FPGA, the filter was implemented as a simple square-window FIR LPF, with four of the filters connected in series. A future implementation of HSS could use a newer generation FPGA with floating-point arithmetic to achieve a filter with better rolloff characteristics and higher ultimate rejection. Fig. 7 is an analytically generated plot of the low-pass filter response, superimposed on the frequency spectrum of the spread-spectrum signal. The ultimate rejection level of 70 dB will be apparent in the experimental results presented in the next section.

Once the packet start has been established, the receiver begins listening on specific channels instead of all channels. A simple multiply-and-integrate correlator system is used for signal detection. This system is described in Fig. 6.

V. Experimental Results

Four bi-directional hybrid DS/FFH radio transceivers have been built and are performing well. The hardware prototype is shown in Fig. 8. The sensitivity for the units is –110 dBm to produce an approximately 80% success rate at the packet level. This is 5 dB less sensitive than theoretically possible, but it is expected that the detection algorithms in the SDR could be significantly improved for better overall sensitivity.

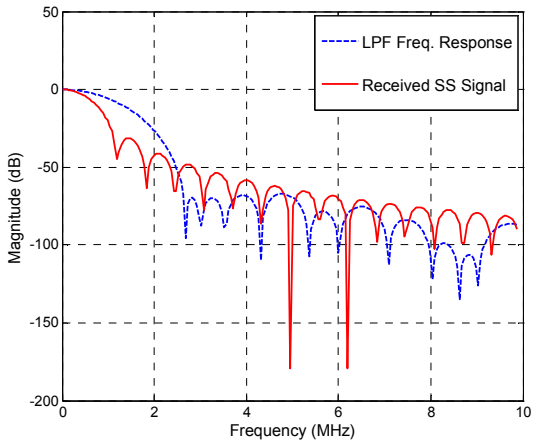

Fig. 7. The frequency response of the digital LPF implemented in the FPGA, superimposed on the frequency spectrum of the received SS signal.

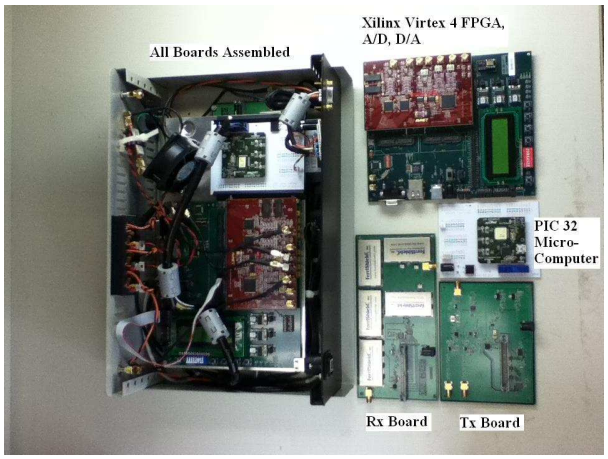

Fig. 8. The implemented hybrid DS/FFH prototype.

The jamming performance of the system was measured directly with laboratory equipment. The testing method used for the HSS evaluation is shown in Fig. 9. The square-wave generator is used at 20 kHz to modulate the signal generator at 100% AM modulation. The test procedure consists of initially transmitting data from the transmitter to the receiver with the signal generator turned off and the attenuator adjusted such that the receiver is operating at an 80% success rate. The attenuator is then reduced 20 dB so the system has a 20-dB margin. Then the signal generator is turned on and ramped up in power until the receiver has degraded to an 80% success rate. The difference in power between the signal generator (jamming) and the transmitter and attenuator combination (at the 20-dB margin point) is then recorded. This is repeated for signal generator frequencies from 902 to 928 MHz. Versions of the test are performed with and without the AM modulation. This methodology stresses the radio by exposing clipping and other non-linear effects that are expected in the A/D converter, SDR arithmetic, and analog front-end components.

A very interesting discovery during the tests was that the system performed better when the analog automatic gain-control (AGC) function was turned off. Normally the AGC

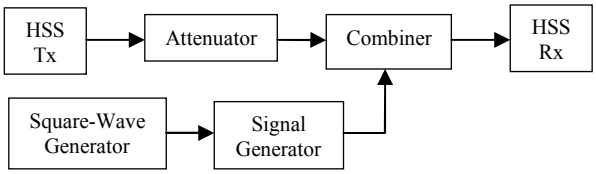

Fig. 9. Experimental setup for testing hybrid DS/FFH jamming resistance.

sets the signal strength such that the full range of the A/D is being used. This occurs since the AGC responds to the stronger interfering signal, which causes an undesired amplitude modulation of the desired signal. It is fortunate that the SDR system has enough dynamic range to detect weak signals when they are not boosted by an AGC amplifier. The following tests were thus conducted with the AGC turned off.

Since an AGC is not being used for this version of HSS, it is important to choose a proper amount of amplifier gain in the receiver. To reach a compromise between sensitivity and non-linear distortions caused by strong signals, two gain versions of the HSS were evaluated for performance. The difference in gain between the low-gain and high-gain version is 5 dB, and eventually an automatic adjustment will be developed to choose the best value for a particular environment.

The first test involved operating the HSS with the hopping feature turned off, so that the filtering capability of the SDR could be measured independently from the hopping benefits. For this test the intermediate frequency was always 12.5 MHz, which also allowed us to insert an analog 12.5 MHz, 3-pole bandpass filter (BPF) in line. This filter lets us operate the radio as a standard analog radio and allows us to do a direct selectivity comparison between the analog and SDR approaches. This comparison was made with the lower-gain version of the radio and the generator AM modulation turned off. The net results are shown in Fig. 10.

From the filtered version of the results, we still see the dynamic range limitations of the analog components ahead of the filter, which include the front-end amplifiers, surface acoustic wave (SAW) bandpass filters, and first mixer.

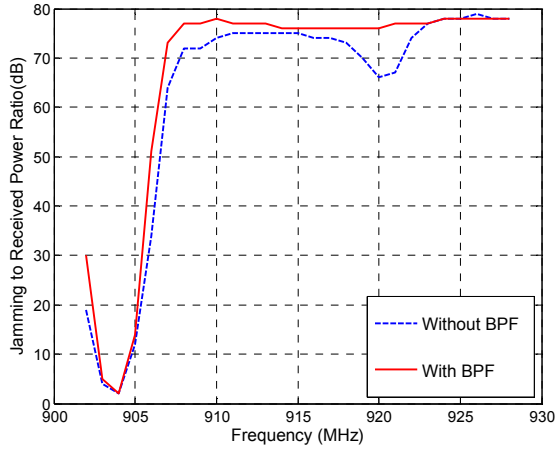

Fig. 10. The hybrid DS/FFH prototype performance while the frequency-hopping feature is disabled and with no jamming.

As a side note, the weak performance at 920 MHz can be explained by the corresponding IF signal being at 29 MHz. If this signal is strong enough to cause clipping in the A/D, the third harmonic at 87 MHz will produce a signal at 13 MHz and will thus jam the desired signal. For the SDR results, we can see that the SDR portion of the system has a dynamic range capability that is comparable to the analog portion, thus the SDR methodology causes only moderate performance degradation as compared to an analog system.

Also noteworthy is the 2-dB result (at 903.75 MHz) when the jammer is directly on the operating frequency. Typical QPSK systems require about a 6 dB signal-to-noise ratio (SNR) to operate, but since the HSS system works with random carrier phase it cannot reject the noise from the other quadrature phase, so the noise is doubled. This means that the HSS will require a 9-dB SNR. The process gain from the 63-bit length spread spectrum code is 16 dB; therefore, the HSS should theoretically tolerate a signal 7 dB stronger than the intended signal. Thus the HSS is within 5 dB of the theoretical.

Fig. 11 demonstrates the effect of AM modulation on the jamming signal. Peak values of the jammer signal are used for the comparison. In general, the modulation makes the radio 10 dB more susceptible to jamming. Although the analog gain stages do not use an AGC, the preamble detection correlator sets a threshold based on the overall signal strength and would thus have some susceptibility to AM jamming.

Sensitivity curves were generated for both the low- and high-gain versions of the radio and are shown in Fig. 12. The results are the percentage success rate at the packet level, averaged over 150 packets, with no error correction used.

These curves are unusual compared to typical digital radios because of their abrupt change from failure to success over a narrow power level range. This is due to the spread spectrum nature of the signal and in particular because of the asynchronous correlator used to detect the packet preamble. Typically for HSS, if the preamble is found, the rest of the packet is received error-free. Determining thresholds for the preamble detection was a particular challenge, and this is an area where there is potential for improving the HSS design.

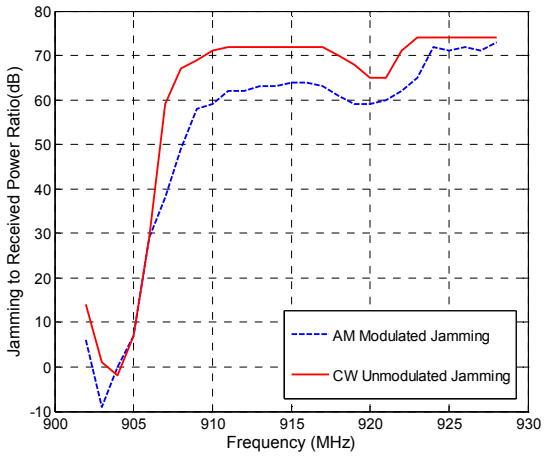

Fig. 11. The hybrid DS/FFH prototype performance while the frequency hopping feature is disabled and in the presence of jamming.

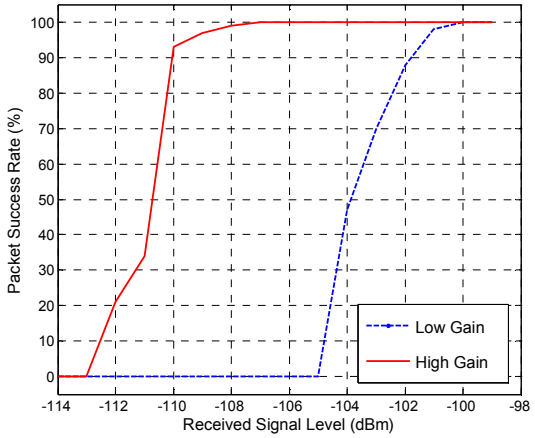

Fig. 12. Receiver sensitivity of the hybrid DS/FFH prototype performance.

The main test for HSS is to show that its FH will make the system jam-resistant at all jamming frequencies. Experiments showed that the hopping frequencies have to be judiciously chosen such that within a redundant triplet, no two of the three frequencies would be near each other, since this would let a single jammer jam both frequencies. Therefore the pattern could not be truly random but would need somewhat of a trend. Another limitation was caused by the characteristics of the analog first mixer. Since it was a double-balanced mixer, the second and fourth harmonics in the output were suppressed but the third and fifth harmonics were significant. For example, when the jamming frequency is 10.8 MHz at the A/D (902 MHz radio frequency), both the 12.5-MHz channel and the 32.5-MHz channel would be jammed with this single frequency. This issue will be solved in future HSS versions, but at this time the HSS is set to not use the top two channels. Using the analog version of HSS with the hopped LO would be a potential solution to this issue.

Fig. 13 shows the hybrid DS/FFH jamming susceptibility versus frequency. It is noticed that the smaller signal has less distortion and is able to better reject the undesired frequencies.

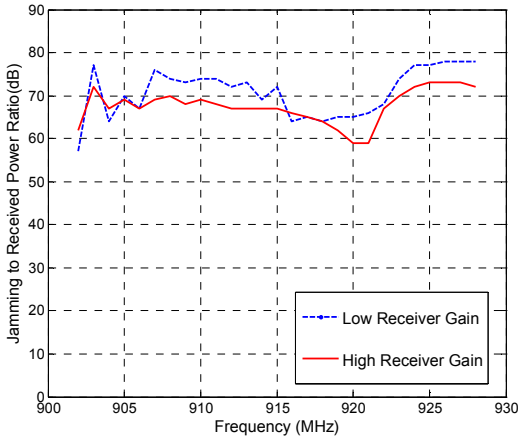

Fig. 13. The hybrid DS/FFH prototype performance in the presence of jamming.

VI. Conclusion

A hardware FPGA-based hybrid DS/FFH prototype was implemented successfully and optimized for a typical Smart Grid utility application. Experimental results indicate that high resistance of hybrid DS/FFH systems to other jamming signals allows the possibility of intentionally operating several HSS radios in the band simultaneously. For Smart Grid applications, this would enable a base station to service several clients at the same time, provided the system arranged for different clients to use different hop patterns and DS codes, and possibly even coordinated transmission time windows. The absence of an AGC in the receiver and the wide dynamic range also indicates the system will have quite good near-far performance.

Acknowledgment

This paper has been authored by employees of UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the U.S. Department of Energy. Accordingly, the United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

References

[1] E. A. Geraniotis, "Noncoherent hybrid DS-SFH spread-spectrum multiple-access communications," *IEEE Transactions on Communications*, vol. 34, no. 9, pp. 862-872, 1986.

[2] J. Zhang, K. C. Teh, and K. H. Li, "Error probability analysis of FFH/MFSK receivers over frequency-selective Rician-fading channels with partial band noise jamming," *IEEE Transactions on Communications*, vol. 57, no. 10, pp. 2880-2885, 2009.

[3] M. P. Pursley, "Direct sequence spread spectrum communications for multipath channels," *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, no. 3, pp. 653-661, 2002.

[4] J. H. Lee, B. S. Yu, and S. C. Lee, "Probability of error for a hybrid spread spectrum system under tone jamming," *Proc. of the IEEE Military Communications Conference (MILCOM'90)*, pp. 410-414, 1990.

[5] M. M. Olama, S. F. Smith, T. Kuruganti, and X. Ma, "Performance study of hybrid DS/FFH spread-spectrum systems in the presence of frequency-selective fading and multiple-access interference," *Proc. of the IEEE International Workshop on Communications Quality and Reliability (CQR)*, pp. 1-5, May 2012.

[6] M. M. Olama, X. Ma, T. Kuruganti, S. F. Smith, and S. M. Djouadi, "Hybrid DS/FFH spread-spectrum: A robust, secure transmission technique for communication in harsh environments," *Proc. of the IEEE Military Communications Conference (MILCOM'11),* pp. 2136-2141, Nov. 2011.

[7] A Technical Tutorial on Digital Signal Synthysis, Technical Report, Analog Devices, Inc., 1999.

[8] D. Taylor "Introduction to synchronous communications, a classic paper by John P. Costas," *Proc. of the IEEE*, vol. 90, no. 8, pp. 1459–1460, Aug. 2002.

[9] X. Ma, M. M. Olama, T. Kuruganti, S. F. Smith, and S. M. Djouadi, "Determining system parameters for optimal performance of hybrid DS/FFH spread-spectrum," *Proc. of the IEEE Military Communication Conference (MILCOM'12)*, pp. 1-6, Nov. 2012.

[10] Y.-R. Tsai, "M-ary Spreading-Code-Phase-Shift-Keying modulation for DSSS multiple access systems," *IEEE Transactions on Communications*, vol. 57, no. 11, pp. 3220-3224, Nov. 2009.