

Design, Implementation, and Evaluation of a Hybrid DS/FFH Spread-Spectrum Radio Transceiver

Mohammed M. Olama, Stephen M. Killough, and
Teja Kuruganti
Oak Ridge National Laboratory
Oak Ridge, TN 37831
Email: {olamahussem, killoughsm,
kurugantipv}@ornl.gov

Thomas E. Carroll
Pacific Northwest National Laboratory
P.O. Box 999, MS-IN K3-12
Richland, WA 99352
Email: Thomas.Carroll@pnnl.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, implementation, and evaluation of a hybrid DS/FFH spread-spectrum radio transceiver using a single Field Programmable Gate Array (FPGA). The FPGA allows the various subsystems to quickly communicate with each other and thereby maintain tight synchronization. We also investigate various hopping sequences against robustness to interference and jamming. Experimental results are presented that show the receiver sensitivity, radio data-rate/bit-error evaluations, and jamming and interference rejection capabilities of the implemented hybrid DS/FFH spread-spectrum system under widely varying design parameters.

Keywords—Hybrid spread-spectrum; direct-sequence; frequency-hopping; interference; jamming; data rate; hopping sequence; Field Programmable Gate Array (FPGA); direct digital synthesizer; receiver sensitivity

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 jamming, and the security they provide against eavesdroppers [1]–[8]. 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 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) [9] 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]. The security of the classic PN-spreading codes for DS, FH, and HSS systems has been addressed in [7], and an initial design for a hardware prototypic hybrid spread-spectrum system has been presented in [8]. These works have shown that hybrid DS/FFH outperforms the existing standard DSSS and FHSS methods on wireless networks in terms of reliability (probability of bit-error) and security. In this paper, we present the efforts carried out at Oak Ridge National Laboratory toward exploring the design, implementation, and evaluation of a 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 quickly 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. We also investigate various hopping sequences against robustness to interference and jamming. Experimental results are presented that show the receiver sensitivity, data-rate/bit-error evaluations, and jamming and interference rejection capabilities of the implemented hybrid DS/FFH spread-spectrum system under widely varying design parameters.

II. ORNL SPECIFIC HYBRID DS/FFH DESIGN

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 [6] 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.

We decided to use the Software Defined Radio (SDR) method for hardware implementation of the hybrid DS/FFH system 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. 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.

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 (D/A) or analog-to-digital (A/D) converters. The SDR algorithms work over a designated 12.5-35.0 MHz frequency range.

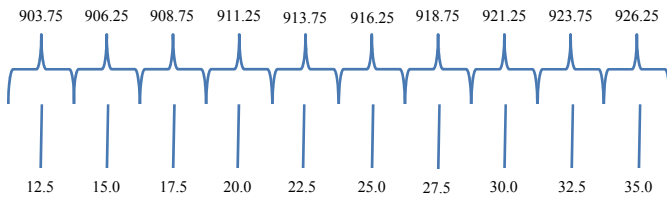


Fig. 1. The prototype hybrid DS/FFH FPGA radio frequencies in MHz.

Each DS signal is a 63-bit length maximal-length (ML) 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 vote determines the correct information even if one of the frequencies is completely blocked.

Of particular interest is the method 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 [10] 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.

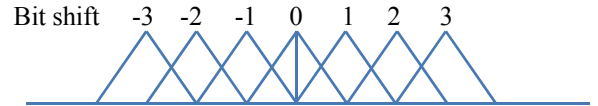


Fig. 2. Code-Phase-Shift-Keying modulation for the DS signal.

The bit-shift number refers to the number 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. [11] explores this method 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.

III. 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. 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. 6 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.

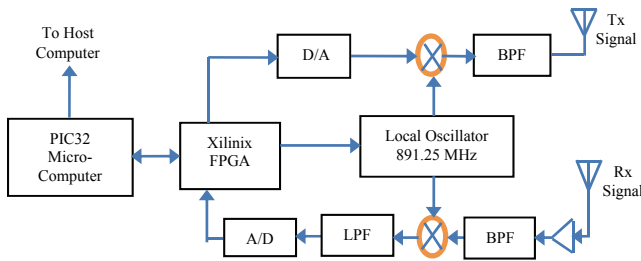


Fig. 3. Hardware setup for the hybrid DS/FFH prototype.

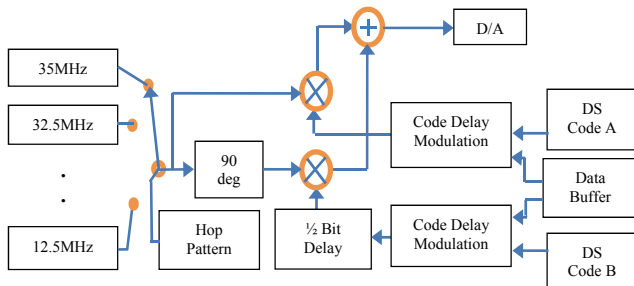


Fig. 4. Transmitter portion of the FPGA code.

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. 7.

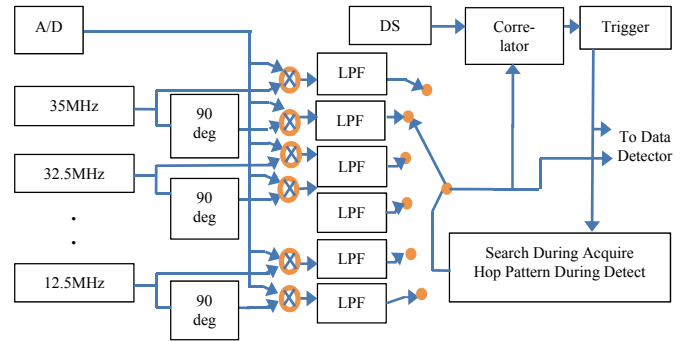


Fig. 5. Preamble-detection section of the receiver.

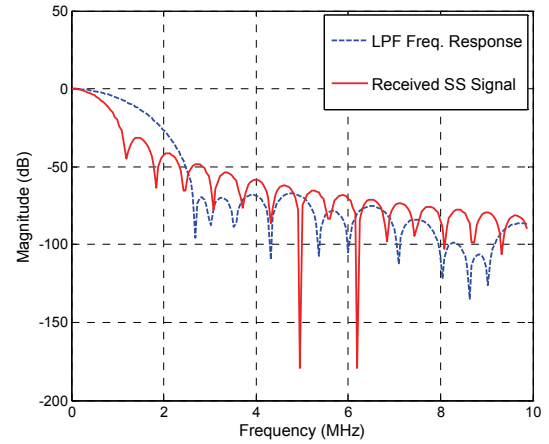


Fig. 6. The frequency response of the digital LPF implemented in the FPGA, superimposed on the frequency spectrum of the received SS signal.

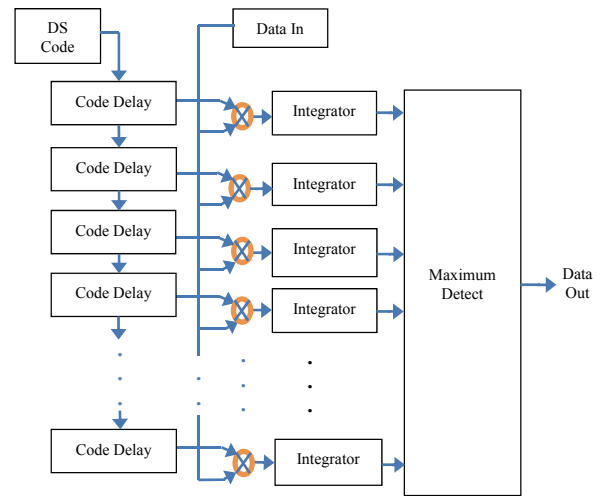


Fig. 7. Data-detection section of the receiver.

IV. EXPERIMENTAL EVALUATIONS AND 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.

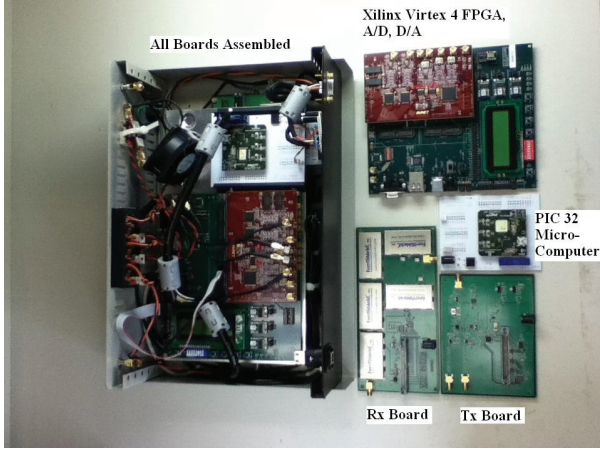


Fig. 8. The implemented hybrid DS/FFH prototype.

A. Experiment 1: Data Rate Evaluation

We designed and implemented a test harness to perform unidirectional throughput testing. The testing began by pseudo-randomly generating a stream of 100,000,064 bits. The test harness divided the stream into units of 32 octets, packaged and formatted the units as packets, and signaled the transmitter to send them. On the receiver side, the test harness read the decoded bit stream and verified the correctness of the payload by comparing the transmitted stream with the received stream. Both bit errors and packet errors were identified and noted.

Table 1 below shows the data rate theoretical limits. In testing, the radios demonstrated a sustained data rate of 37.8 kbps, which is 90.4% of the achievable data rate. The raw over-the-air data rate that considers the total data transmitted, including the octets for preamble and error correction, is 139.6 kbps, which is quite near the design objective of 150 kbps. Also, the radios demonstrated a bit error rate of less than 10^{-6} . The performance is comparable to the 40 kbps offered by IEEE 802.15.4, 915 MHz BPSK PHY specifications [12].

Table 1: The hybrid DS/FFH prototype data rate theoretical limits.

Task	Data Rate
MAC-to-PHY communication	92.2 kbps
Transmit	84.2 kbps
Receive	41.8 kbps

B. Experiment 2: Jamming Rejection Evaluation

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 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.

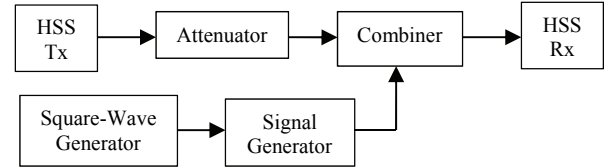


Fig. 9. Experimental setup for testing hybrid DS/FFH jamming resistance.

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 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.

Figure 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.

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. Theoretical investigation of different hopping sequences (or patterns) on the performance of the system is illustrated in the next section.

Figure 12 shows the hybrid DS/FFH jamming susceptibility versus frequency. Two receiver gain versions of the HSS were evaluated in this scenario. The difference in gain between the low-gain and high-gain version is 5 dB. Eventually an automatic adjustment will be developed to choose the best value for a particular environment. It is noticed in Fig. 14 that the smaller signal has less distortion and is able to better reject the undesired frequencies.

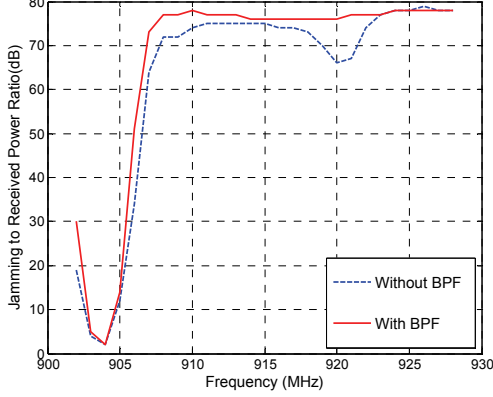


Fig. 10. The hybrid DS/FFH prototype performance while the frequency-hopping feature is disabled and with no jamming.

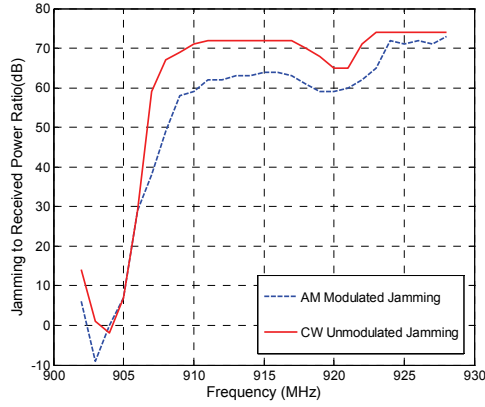


Fig. 11. The hybrid DS/FFH prototype performance while the frequency hopping feature is disabled and in the presence of jamming.

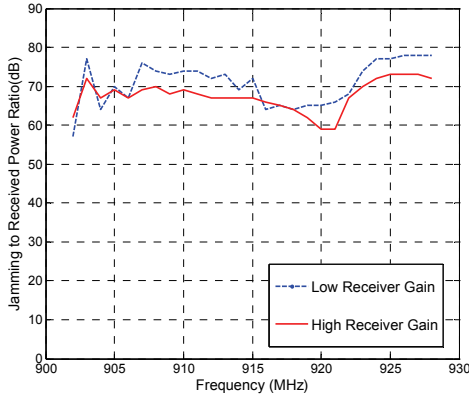


Fig. 12. The hybrid DS/FFH prototype performance in the presence of jamming.

C. Experiment 3: Interference Rejection Evaluation

In this experiment, we evaluate the robustness of the hybrid DS/FFH prototype against interference. Two transceivers were positioned 5 meters apart on either side of a Faraday cage. On each of the radios' SMA connectors, we attached an omnidirectional, 900-960 MHz-tuned, 3 dBi-gain vertical antenna. A bi-conical antenna, placed at the midway point, was attached to a spectrum analyzer. We positioned another antenna at the quarter point to emit our interfering signals. The radios were entered into a requester-responder (i.e., echo reply) mode that generated a request every second and a response, in turn, by the receiver.

We measured transmission power no greater than -35 dBm, 25 dBm over the noise floor. We purposely limited the power of the interference during the evaluation to no more than 30 dBm (1024 times) greater than the power level of the HSS transmissions. We did this for two reasons. First, any receiver can be overpowered and swamped out. This result is not indicative of the protocol but the receivers themselves. Second, we did not desire to damage the receivers or any other sensitive testing equipment.

We began the evaluation by using a signal synthesizer. We generated a continuous wave signal, approximately 600 kHz in width, from 902 to 928 MHz, stepping one kHz at power levels ranging from 10-30 dBm greater than the power level of the HSS as observed on the spectrum analyzer. This method did not interfere with the transmissions. Our hypothesis is that DS provides sufficient protection from this type of interference.

The second evaluation method consisted of generating white noise interference. Using an SDR, we transmitted a 20 MHz wide Gaussian signal centered at 915 MHz with peak power of 30 dBm greater than the HSS transmissions. This signal disrupted both transceivers from receiving coherent messages. Currently, we are working on generating a narrower 2 MHz wide interference signal and testing the reception performance at both transceivers. In the next section, we investigate the effect of different hopping sequences on the performance of a hybrid DS/FFH system.

V. HOPPING SEQUENCE EVALUATION

We investigate in this section the impact of different hopping sequences on the system robustness against noise, interference, and jamming. We consider the same system parameters as described in Sections II and III (10 hopping channels, 3 hops per symbol, and the logical layer protocol data unit size is 32 octets). We examine three channel selection strategies:

- Strategy S_0 : Choose each and every channel c , uniformly at random.
- Strategy S_1 : Choose a channel c_i , uniformly at random, that is different from the previous two channels, c_{i-1} and c_{i-2} .
- Strategy S_2 : For each triad of symbols, choose three distinct channels c_1 , c_2 , and c_3 such that $c_1 \neq c_2$, $c_1 \neq c_3$, and $c_2 \neq c_3$. Channel selection follows a uniform Dirichlet process.

For each strategy we compute *success* as the ratio of the messages correctly received to the total number of messages transmitted. First we consider the scenario that the adversary wideband jams access to one channel. Let us start by considering strategy S_0 . The success for strategy S_0 under one denied channel, denoted S_0^1 , is given by

$$S_0^1 = \frac{\sum_{n=0}^{32} \binom{32}{n} \left(\binom{3}{2} 9^{2.1} \right)^n (9^3)^{32-n}}{(10^3)^{32}} \quad (1)$$

which evaluates to $S_0^1 = 0.6994$.

Now, consider S_1 , where the current channel cannot be the same as the previous two channels, and S_2 , where a triad of symbols is transmitted on three channels. For both cases, it is trivial to see that $S_1^1 = S_2^1 = 1$ as the interference will at most result in one error per triad.

Now consider a more advanced adversary that denies two channels. Under this constraint, the success rate of strategy S_0 is expressed as

$$S_0^2 = \frac{\sum_{n=0}^{32} \binom{32}{n} \left(\binom{8}{2} 8^{2.2} \right)^n (8^3)^{32-n}}{(10^3)^{32}} \quad (2)$$

which evaluates to $S_0^2 = 0.02978$.

For S_1 , deriving the closed-form equation for success from the Markov chain is nontrivial. Using a Monte Carlo simulation for this case, we find $S_1^2 = 0.1014$.

For S_2 , success is computed as

$$S_2^2 = \frac{\sum_{n=0}^{32} \binom{32}{n} \left(\binom{8}{2} \binom{2}{1} \right)^n \left(\frac{10}{3} \right)^{32-n}}{\left(\frac{10}{3} \right)^{32}} \quad (3)$$

giving $S_2^2 = 0.1099$. We summarize the results in Table 2.

While S_1 and S_2 are effective when one channel is denied, none of the three strategies we evaluated are robust against an adversary denying two or more channels. Increasing the number of hops per symbol and/or employing frequency hopping patterns with minimal collisions would further enhance the robustness of the system against two or more denied channels.

Expressions (1)-(3) are for either fixed or unfixed interference (the frequency of the interfering signal changes with respect to time or position). If the interference is fixed, avoiding the affected channels provides an optimal strategy.

Table 2. The success rate of the hopping strategies.

Strategy	Deny One Channel	Deny Two Channels
S_0	0.6993908	0.02977531
S_1	1.0	0.101405
S_2	1.0	0.1099453

VI. CONCLUSIONS

A hardware FPGA-based hybrid DS/FFH prototype was implemented successfully and optimized for a typical SG utility application. Experimental results indicate that high resistance of hybrid DS/FFH systems to other jamming and interference signals allows the possibility of intentionally operating several HSS radios in the band simultaneously. For SG 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.

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 Conf. (MILCOM'90)*, pp. 410-414, 1990.
- [5] 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 Conf. (MILCOM'11)*, pp. 2136-2141, 2011.
- [6] X. Ma, M.M. Olama, T.P. 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 Conf. (MILCOM'12)*, pp. 1888-1893, Nov. 2012.
- [7] X. Ma, M.M. Olama, T. Kuruganti, S.F. Smith, and S.M. Djouadi, "Security of Classic PN-Spreading Codes for Hybrid DS/FH Spread-Spectrum Systems," *Proc. of the IEEE Military Communication Conf. (MILCOM'13)*, pp. 957-962, Nov. 2013.
- [8] S.M. Killough, M.M. Olama, T. Kuruganti, and S.F. Smith, "FPGA-Based Implementation of a Hybrid DS/FFH Spread-Spectrum Transceiver," *Proc. of the World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'13)*, July 2013.
- [9] A Technical Tutorial on Digital Signal Synthesis, Technical Report, Analog Devices, Inc., 1999.
- [10] D. Taylor "Introduction to synchronous communications, a classic paper by J. Costas," *Proc. of the IEEE*, vol. 90, no. 8, pp. 1459-1460, 2002.
- [11] 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.
- [12] IEEE Std. 802.15.4-2006, "A wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)," IEEE Computer Society, 2006.