Olama et al. EURASIP Journal on Advances in Signal Processing (2015) 2015:25
DOI 10.1186/s13634-015-0208-z

EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

Analysis, optimization, and implementation of a hybrid DS/FFH spread-spectrum technique for smart grid communications

Mohammed M Olama[1*], Xiao Ma[2], Stephen M Killough[1], Teja Kuruganti[1], Stephen F Smith[1] and Seddik M Djouadi[2,3]

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, error-probability analyses are performed for a hybrid DS/FFH system over standard Gaussian and fading-type channels, progressively including the effects from wide- and partial-band jamming, multi-user interference, and varying degrees of Rayleigh and Rician fading. In addition, an optimization approach is formulated that minimizes the bit-error performance of a hybrid DS/FFH communication system and solves for the resulting system design parameters. The optimization objective function is non-convex and can be solved by applying the Karush-Kuhn-Tucker conditions. We also present our efforts toward exploring the design, implementation, and evaluation of a hybrid DS/FFH radio transceiver using a single field-programmable gate array (FPGA). Numerical and experimental results are presented under widely varying design parameters to demonstrate the adaptability of the waveform for varied harsh smart grid RF signal environments.

Keywords: Hybrid spread-spectrum; Direct sequence; Frequency hopping; Smart grid communications; Non-convex optimization; Receiver sensitivity; FPGA

1 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.

User requirements for the next generation wireless communication system have been specified for the Smart Grid advanced metering infrastructure (AMI) and distribution automation systems [7]. These requirements demonstrate the need for high capacity and highly secure networks for Smart Grid applications. There is a significant gap between commercially available communications systems and those needed to satisfy the demanding requirements associated with electric utility industry. HSS systems are a promising candidate for Smart Grid applications since they provide high data rates with excellent signal security.

Spreading the signal over a relatively wide bandwidth allows transmission with relatively low power density, leading to low probabilities of detection and interception. HSS systems also provide an inherent security against eavesdroppers because knowledge of the spreading codes is required. The choice of appropriate pseudo-noise (PN) codes and dynamic altering of signal parameters provides the opportunity for a strong security scheme in the

* Correspondence: olamahussemm@ornl.gov
[1]Computational Sciences and Engineering Division, Oak Ridge National Laboratory, P.O. Box 2008, MS 6085, Oak Ridge, TN 37831, USA
Full list of author information is available at the end of the article

physical (PHY) layer of the network [5]; details of these techniques will be addressed in future works. This specific paper will focus on implementation, exploration, and optimization of the parameter space of the HSS system for adapting the technique for application-level requirements in Smart Grid.

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) [8] 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 [2], channel conditions [1,3], multi-user interference [2,3], and jamming [4]. However, little research has yet evaluated the performance of a hybrid DS/FFH system under all combinations of the aforementioned cases. Moreover, few efforts have to date attempted to address the design and selection of the HSS system parameters that achieve optimal performance. The work in this paper extends the one in [9] and [10] from a DS system to a hybrid DS/FFH system, in addition to taking jamming impacts into consideration. In [11], the performance of a SFH system was considered. In [2] and [12], the performance of a DS/SFH system over an AWGN channel and with multi-user interference was considered. The performance of an FFH system over fading channels was examined in [13] and extended in [3] to include the effects of partial-band noise jamming. Although [4] and [14] computed the error probability of DS/SFH under jamming tones in both AWGN and Rician fading channels, only a single user was considered. In [15], the optimal spreading sequences for chip-synchronous CDMA are derived by minimizing the average bit error rate under the standard-Gaussian-approximation condition. The work in [16] presents a simulation-based study for evaluating the performance of a hybrid DS/FFH scheme. Some preliminary performance analysis and hardware designs for the hybrid DS/FFH scheme were initially presented in [17-19].

In this paper, error-probability analyses are performed for a hybrid DS/FFH system over standard Gaussian and fading-type channels, progressively including the effects from wide- and partial-band jamming, multi-user interference, and varying degrees of Rayleigh and Rician multipath fading. We present analytical derivations for evaluating the performance in terms of probability of bit error. In addition, an optimization approach is formulated that minimizes the average bit-error probability of a hybrid DS/FFH communication system and solves for the system design parameters that achieve an optimal performance level. The optimization objective function is non-convex and can be solved by applying the Karush-Kuhn-Tucker (KKT) conditions [20]. We also present our efforts toward exploring the design, implementation, and evaluation of a hybrid DS/FFH radio transceiver using a single field-programmable gate array (FPGA). Numerical and experimental results are presented under widely varying design parameters to demonstrate the adaptability of the waveform for varied harsh smart grid RF signal environments.

2 System model

Assume that there are a total of K nodes that represent smart meters or data aggregation points in the Smart Grid wireless network. For the kth node, the transmitted signal is given as

$$s_{\mathrm{k}}(t) = \sqrt{2P} b_{\mathrm{k}}(t) a_{\mathrm{k}}(t) cos\left\{2\pi\left(f_{\mathrm{c}} + f_{\mathrm{h}}^{\mathrm{k}}(t)\right)t\right\} \tag{1}$$

where P is the common transmitted signal power, f_{c} is the carrier frequency, $\left\{f_{\mathrm{h}}^{\mathrm{k}}(t)\right\}$ denotes the hopping frequency of the kth node, the data signal $b_{\mathrm{k}}(t)$ is a sequence of statistically independent, unit-amplitude positive, and negative rectangular pulses of duration T_{b}, and $a_{\mathrm{k}}(t)$ is the PN-code waveform for the kth node in DSSS and is given as $a_{\mathrm{k}}(t) = \sum_{n=-\infty}^{\infty} a_{\mathrm{n}}^{\mathrm{k}} P_{\mathrm{T_c}}(t - nT_{\mathrm{c}})$, where $\left\{a_{\mathrm{n}}^{\mathrm{k}}\right\}$ is the discrete periodic signature sequence assigned to the kth node and $P_{\mathrm{T_c}}(t)$ is a rectangular pulse that starts at $t = 0$ and ends at $t = T_{\mathrm{c}}$.

Consider M frequency hopping channels with L (assume L is odd) hops per bit. Let $T = T_{\mathrm{b}}/L$ denote the duration of each hop and $T_{\mathrm{c}} = T_{\mathrm{b}}/NL$ denote the chip duration for the PN-code sequence, where N is the period of the PN-sequence and is also assumed to be odd. The wide-band jamming fully corrupts W hopping channels and another single channel partially (let $W_{\mathrm{j}}^{\mathrm{p}}$ be the part of the channel affected by the partial jamming).

The fading channel considered here is modeled as a general wide-sense-stationary uncorrelated scattering (WSSUS) channel [9]. Following [10,21,22] , the received signal can be described as:

$$y(t)=\sum_{k=1}^{K}\mathrm{Re}\left\{r_k(t-\tau_k)exp\left\{2\pi\left(f_c+f_h^k(t)\right)(t-\tau_k)\right\}\right\}+J(t)+n(t) \tag{2}$$

where $J(t)$ and $n(t)$ represent the jamming term and AWGN term that have two-sided spectral densities $N_J/2$ and $N_0/2$,, respectively, and

$$r_k(t)=\gamma_k\int_{-\infty}^{\infty}\beta_k(\tau,t)\sqrt{2P}(t-\tau)a_k(t-\tau)d\tau+\sqrt{2P}(t)a_k(t) \tag{3}$$

where the nonnegative real parameter γ_k is the Rician channel coefficient for the kth node; $\beta_k(\tau,t)$ is a zero-mean complex Gaussian random process that represents the equivalent low-pass time-varying impulse response for the fading channel [10]. The covariance function for the fading process in a WSSUS channel is [22,23].

$$\Lambda_k(\tau,\sigma;t,s)=\frac{1}{2}E\left\{\beta_k(\tau,t)\beta_k^*(\tau,t)\right\}=\rho_k(\tau,t-s)\delta(\tau-\sigma) \tag{4}$$

In this paper, we focus on one class of WSSUS channels known as time-selective fading channels [22]; its covariance function is given by $\rho_k(\tau,t-s)=\rho_k(0,t-s)\delta(\tau)$ [23], where the covariance function $\rho_k(0,t-s)$ is defined as

$$\rho_k(0,t)=\begin{cases}1-\dfrac{\nu|t|}{T}, & |t|\le\lambda T_c\\ 0, & \text{otherwise}\end{cases} \tag{5}$$

where $\lambda=(n+\beta)<N$, n is a positive integer less than N, $0\le\beta<1$ and $\nu=(\lambda T_c)^{-1}T$ [10].

Similar to [24], the time delays and data symbols for the kth node are modeled as mutually independent random variables which are uniformly distributed on [0, T] and {−1, + 1}, respectively. We also assume $\tau_i=0$ when considering the output of the kth ($k\neq i$) correlation receiver.

3 Error probability analysis

In this section, we first investigate the average error probability for one hop, and then we employ a majority voting scheme to compute the overall error probability for one bit.

For each user k, the other K-1 users are considered as interference. Three different situations may occur in one hop: j out of K-1 users interfere with the same hopping channel of user k and (1) no jamming corrupts the channel, (2) jamming fully corrupts the channel, or (3) jamming partially corrupts the channel. Thus, the total average error probability P_ε^k of one hop for user k can be computed as:

$$\begin{aligned}P_\varepsilon^k&=\sum_{j=0}^{K-1}P_\varepsilon^k(j\,\text{users})\\&=\sum_{j=0}^{K-1}\{P_\varepsilon^k(j\,\text{users, no jam})\\&\quad+P_\varepsilon^k(j\,\text{users, full jam})\\&\quad+P_\varepsilon^k(j\,\text{users, partial jam})\}\end{aligned} \tag{6}$$

where $P_\varepsilon^k(j\,\text{users})$ is the average error probability of one hop due to j interfering users. Expression (6) is equivalent to

$$\begin{aligned}P_\varepsilon^k=\sum_{j=0}^{K-1}\{&P(j\,\text{users, no jam})P^k(\varepsilon|j\,\text{users, no jam})\\&+P(j\,\text{users, full jam})P^k(\varepsilon|j\,\text{users, full jam})\\&+P(j\,\text{users, partial jam})P^k(\varepsilon|j\,\text{users, partial jam})\}\end{aligned} \tag{7}$$

where $P(a,b)$ is the joint probability of events a and b, and $P^k(\varepsilon|a,b)$ is the conditional probability of error, given events a and b have occurred. From the problem formulation, we can obtain:

$$\begin{aligned}P(j\,\text{users, no jam})&=\binom{K-1}{j}\left(\frac{1}{M}\right)^j\left(1-\frac{1}{M}\right)^{K-1-j}\left(\frac{M-W-1}{M}\right)\\P(j\,\text{users, full jam})&=\binom{K-1}{j}\left(\frac{1}{M}\right)^j\left(1-\frac{1}{M}\right)^{K-1-j}\left(\frac{W}{M}\right)\\P(j\,\text{users, partial jam})&=\binom{K-1}{j}\left(\frac{1}{M}\right)^j\left(1-\frac{1}{M}\right)^{K-1-j}\left(\frac{1}{M}\right)\end{aligned} \tag{8}$$

The conditional error probabilities for each case of jamming over Rician fading channels are discussed next.

A. *Case 1: No Jamming*

When there is no jamming, the error probability for BPSK modulation is given as [25]:

$$P^k(\varepsilon|j\,\text{users, no jam})=Q\left(\frac{1}{\sqrt{NSR/2+I_j^k}}\right) \tag{9}$$

where I_j^k is the interference-to-signal ratio introduced by the other users hopping in user k's channel, $NSR=N_0/2PT$ is the noise-to-signal ratio, and $Q(\bullet)$ is the complementary error function. Following the arguments in [10] and [24], I_j^k is computed as:

$$I_{\mathrm{j}}^{\mathrm{k}}=\frac{2\gamma_{\mathrm{k}}^2\lambda}{N}\left[1-\frac{1}{2}(\nu+1)\frac{\lambda}{N}+\frac{\nu\lambda^2}{3N^2}\right]+\sum_{i=1,i\neq k}^{j+1}\left[\frac{2\gamma_{\mathrm{i}}^2}{N^4}\sum_{l=0}^{\mathrm{n}}\{\beta_{\mathrm{l}}R_{\mathrm{i}}(l)R_{\mathrm{k}}(l)\Gamma_{\mathrm{l}}(1/2)+\frac{\beta_l^2}{2}\left[\zeta_{\mathrm{i,k}}(l)+\zeta_{\mathrm{k,i}}(l)\right]\Gamma_{\mathrm{l}}(2/3)+\frac{\beta_{\mathrm{l}}^3}{3}\Delta_{\mathrm{i}}(l)\Delta_{\mathrm{k}}(l)\Gamma_{\mathrm{l}}(3/4)\}\right|+\sum_{i=1,i\neq k}^{j+1}\frac{1}{6N^3}m_{\mathrm{i,k}} \tag{10}$$

where $\beta_l = 1$ for $l < n$ and $\beta_n = \beta$, $\Delta_{\mathrm{i}}(l) = R_{\mathrm{i}}(l+1) - R_{\mathrm{i}}(l)$, $\zeta_{\mathrm{i,k}}(l) = \Delta_{\mathrm{i}}(l)R_{\mathrm{k}}(l)$, $\Gamma_{\mathrm{l}}(\mathrm{a}) = N - \nu(l + a\beta_l)$, $m_{\mathrm{i,k}} = 2\sum_{l=1-N}^{N-1}R_{\mathrm{i}}(l)R_{\mathrm{k}}(l) + \sum_{l=1-N}^{N-1}R_{\mathrm{i}}(l)R_{\mathrm{k}}(l+1)$, and $R_{\mathrm{i}}(l)$ is the usual aperiodic autocorrelation function for the PN-sequence.

Different PN-sequences correspond to different aperiodic autocorrelation functions which are functions of the length N of the sequence. In this work, we employ a maximal-length sequence (MLS) as the signature sequence. However, by using an MLS code, there does not exist a closed-form expression of the aperiodic autocorrelation function, $R_{\mathrm{i}}(l)$, for the general MLS code, which prevents us from finding a closed-form expression for $I_{\mathrm{j}}^{\mathrm{k}}$. However, we can compute a closed-form expression if we know exactly which MLS code is used. Actually, two different MLS codes with the same length will have different aperiodic autocorrelation functions. Therefore, we consider an upper bound on an MLS's aperiodic autocorrelation function derived in [26] to compute an upper bound on the error probability of the HSS system. From [26], we have $R_{\mathrm{i}}(0) = N$ and $R_{\mathrm{i}}(l) < R_{\mathrm{u}} = 1 + \frac{2}{\pi}(N+1)^{\frac{1}{2}}\mathrm{In}\left(\frac{4N}{\pi}\right)$, $l \neq 0$. Plugging them back into $I_{\mathrm{j}}^{\mathrm{k}}$ in (10) and assuming $\gamma_{\mathrm{k}} = \gamma$ as a constant for simplicity, we get an upper bound on $I_{\mathrm{j}}^{\mathrm{k}}$ as:

$$I_{\mathrm{j}}^{\mathrm{k}} < I_{\mathrm{j}}^{\mathrm{u}}=\frac{2\gamma^2\lambda}{N}\left[1-\frac{1}{2}(\nu+1)\frac{\lambda}{N}+\frac{\nu\lambda^2}{3N^2}\right]+\frac{2\gamma^2 j}{N^4}\left\{N^2R_{\mathrm{u}}-\frac{2}{3}NR_{\mathrm{u}}\nu-\frac{5}{6}N^2\nu+\frac{4}{3}N^3+\frac{13}{3}N(n-1)R_{\mathrm{u}}^2-\frac{17}{6}(n-1)R_{\mathrm{u}}^2\nu+\frac{13}{6}n(n-1)R_{\mathrm{u}}^2\nu+\beta R_{\mathrm{u}}^2(N-\nu n)\left(1+2\beta+\frac{4}{3}\beta^2\right)-\beta^2R_{\mathrm{u}}^2\nu\left(\frac{1}{2}+\frac{4}{3}\beta+\beta^2\right)\right\}+\frac{j\left(2N^2+4R_{\mathrm{u}}^2(N-1)\right)}{6N^3} \tag{11}$$

B. *Case 2: Full Jamming*

When jamming fully corrupts the user k's channel, the error probability for BPSK is given as:

$$P^{\mathrm{k}}(\varepsilon|j\,\mathrm{user},\,\mathrm{full\,jam})=Q\left(\frac{1}{\sqrt{NSR/2+JSR/2+I_{\mathrm{j}}^{\mathrm{k}}}}\right) \tag{12}$$

where $JSR = N_{\mathrm{J}}/2PT$ is the jamming-to-signal ratio.

C. *Case 3: Partial Jamming*

When jamming partially corrupts the user k's channel, the error probability includes two portions: one is the part of the channel corrupted and the other is the uncorrupted part. Let $q = W_{\mathrm{J}}^{\mathrm{p}}/(NW_{\mathrm{b}})$ denote the fraction of the channel jammed, where $W_{\mathrm{b}} = 1/T_{\mathrm{b}}$. Then the error probability for the BPSK case is given as:

$$P^{\mathrm{k}}(\varepsilon|j\,\mathrm{users},\,\mathrm{partial\,jam})=qP^{k}(\varepsilon|j\,\mathrm{users},\mathrm{full\,jam})+(1-q)P^{\mathrm{k}}(\varepsilon|j\,\mathrm{users},\mathrm{no\,jam}) \tag{13}$$

Based on the arguments above, the error probability per hop, $P_{\varepsilon}^{\mathrm{k}}$, is obtained. Without loss of generality, we assume the Rician channel coefficients for all users are identical, i.e., $\gamma_{\mathrm{k}} = \gamma$, then, for simplicity, $P_{\varepsilon}^{\mathrm{k}}$ can be represented as P_{ε}. To compute the error probability for *one bit*, denoted P_{E}, we employ a majority voting decision scheme given as:

$$P_{\mathrm{E}}=\sum_{d=\frac{L+1}{2}}^{L}\binom{L}{d}(P_{\varepsilon})^{\mathrm{d}}(1-P_{\varepsilon})^{L-d} \tag{14}$$

Due to the monotonicity of $Q(\bullet)$, using (11) provides an upper bound on $P_{\varepsilon}^{\mathrm{k}}$ and thus an upper bound on P_{E}. The problem of determining the HSS system parameters for an optimal performance is now discussed in the next section.

4 Optimization problem formulation

In realistic HSS systems, the overall system performance always suffers from practical parameter constraints. Thus, we formulate the problem of minimizing the bit-error performance subject to some representative parameter constraints.

The system design parameters of interest are the number of frequency-hopping channels M, the length of the PN-sequence N, the number of channels fully corrupted by jamming W, and the number of hops per bit L. Assume that these parameters satisfy the following constraints

$$MNW_{\mathrm{b}}-K_1\leq 0,\quad K_1>0 \tag{15}$$

$$W - K_2 M \geq 0,\ 0 \leq K_2 \leq 1 \tag{16}$$

$$K_3 - \frac{1}{LW_b} \leq 0, \quad K_3 > 0 \tag{17}$$

$$M, N, W, L > 0 \tag{18}$$

together with integer constraints on the parameters (i.e., M, N, W, L are positive integers).

The physical meaning of these constraints can be explained as follows: (15) represents that the total bandwidth of the system (MNW_b) is limited by K_1, where $K_1 > 0$; (16) means that the number of frequency channels fully corrupted by the jamming are a portion of the total number of channels, where $0 \leq K_2 \leq 1$; (17) provides a lower bound on the time duration of each hop $\left(\frac{1}{LW_b}\right)$ due to implementation limitations; and (18) restricts all the parameters to be positive.

The optimization problem is to minimize the system's bit- error rate (BER) in (14) with respect to the constraints described in (15) to (18). It can be written as:

$$\begin{aligned} &\min_{M,N,W,L} P_E \\ &\text{subject to } (15), (16), (17), (18) \end{aligned} \tag{19}$$

The integer constraints are removed in the problem statement and the following analysis because they can be imposed after the solutions of (19) are found. This will be discussed in more detail in the following section.

5 Necessary conditions of the optimization problem

By examining the structure of P_E, we can further relax the constraint (17). Note P_E is a monotonically decreasing function with respect to L, so constraint (17) can be written as:

$$L \leq \frac{1}{K_3 W_b} \tag{20}$$

which means that there is an upper bound on L. Moreover, as P_ε does not depend on L, the error probability P_E reaches its minimum when $L = \frac{1}{K_3 W_b}$ with the other parameters fixed.

Further, it is easy to see that P_E is a monotonically increasing function with respect to P_ε on the interval [0, 1], and M, N, W are all contained only in P_ε; thus, the optimization problem in (19) can be further simplified as:

$$\begin{aligned} &\min_{M,N,W} P_\varepsilon \\ &\text{subject to } (15), (16), (18) \end{aligned} \tag{21}$$

From Section 3, we have

$$P_\varepsilon = \sum_{j=0}^{K-1} \left\{ P_n P_{nj} + P_f P_{fj} + P_p P_{pj} \right\} \tag{22}$$

where $P_n = P(users,\ no\ jam)$, $P_f = P(users,\ full\ jam)$, $P_p = P(users,\ partial\ jam)$, $P_{nj} = P^k(\varepsilon | j \text{ users, no jam})$, $P_{fj} = P^k(\varepsilon | j \text{ user, full jam})$, $P_{pj} = P^k(\varepsilon | j \text{ users, partial jam})$. Expression (22) can be further simplified by representing P_{pj} in terms of P_{nj} and P_{fj} as follows:

$$P_\varepsilon = \sum_{j=0}^{K-1} \left\{ \left(P_n + P_p(1-q)\right) P_{nj} + \left(P_p q + P_f\right) P_{fj} \right\} \tag{23}$$

For convenience, let

$$P_{\varepsilon,j} = \left(P_n + P_p(1-q)\right) P_{nj} + \left(P_p q + P_f\right) P_{fj} \tag{24}$$

and also let $x = (M, N, W)$.

From Section 3, we observe that P_n and P_f are functions of both M and W, while P_p is only a function of M. Moreover, P_{nj} and P_{fj} are functions of N. We can also observe that the error probability to be minimized has a complex structure and is a non-convex function. Thus, to compute the optimal solution, we apply the Karush-Kuhn-Tucker (KKT) [20] conditions to problem (21).

Lemma 1: *(Karush-Kuhn-Tucker Conditions) Let y^* be a local minimum of the following problem*

$$\begin{aligned} &\min f(y) \\ &\text{subject to } g_1(y) \leq 0, \ldots, g_m(y) \leq 0 \end{aligned} \tag{25}$$

where f and g_i are continuously differentiable functions with appropriate dimensions. Then there exists an unique Lagrange multiplier vector $\mu = (\mu_1, \ldots, \mu_m)$, such that

$$\begin{aligned} &\nabla_y R(y^*, \mu) = 0, \\ &\mu_i \geq 0,\ i = 1, \ldots m, \text{ and } \mu_i = 0, \forall i \notin A(y^*) \end{aligned} \tag{26}$$

where $R(y, \mu) = f(y) + \sum_{i=1}^{m} \mu_i g_i(y)$ is the Lagrangian function and $A(y^*)$ is the set of active constraints at y^* defined as: For any feasible vector y (the vector that satisfies all constraints), the set of active inequality constraints is given as $A(y) = \{i | g_i(y) = 0\}$ and if $j \notin A(y)$, it is said that the jth constraint is inactive at y.

In addition, if f and g_i are twice continuously differentiable, then there holds $z^T \nabla^2_{yy} R(y^*, \mu) z \geq 0$, for all z in proper dimensions, such that $\nabla g_i (y^*)^T z = 0, \forall\, i \in A(y^*)$.

Now, the necessary conditions for a local minimum of problem (21) can be derived by applying the KKT conditions as follows:

Theorem 1: *Let $x^* = (M^*, N^*, W^*)$ be a local minimum of the problem* (21)*, then there exists unique $\mu_1 \geq 0$, $\mu_2 \geq 0$, such that*

$$\sum_{j=0}^{K-1} \frac{\partial P_{\varepsilon,\mathrm{j}}}{\partial M}\bigg|_{\mathrm{x}^*} + \mu_1 N^* W_{\mathrm{b}} - \mu_2 K_2 = 0 \tag{27}$$

$$\sum_{j=0}^{K-1} \frac{\partial P_{\varepsilon,\mathrm{j}}}{\partial N}\bigg|_{\mathrm{x}^*} + \mu_1 M^* W_{\mathrm{b}} = 0 \tag{28}$$

$$\sum_{j=0}^{K-1} \frac{\partial P_{\varepsilon,\mathrm{j}}}{\partial W}\bigg|_{\mathrm{x}^*} + \mu_2 = 0 \tag{29}$$

$$M^* N^* W_{\mathrm{b}} - K_1 = 0 \tag{30}$$

$$W^* - K_2 M^* = 0 \tag{31}$$

where

$$\frac{\partial P_{\varepsilon,\mathrm{j}}}{\partial M} = \frac{1}{NW_{\mathrm{b}}}\binom{K-1}{j}\left(\frac{1}{M}\right)^{j+1}\left(1-\frac{1}{M}\right)^{K-1-j} \times\left\{\frac{\left(NW_{\mathrm{b}}W + W_{\mathrm{j}}^{\mathrm{p}}\right)(jM+M-K)}{M^2-M}\left(P_{\mathrm{nj}}-P_{\mathrm{fj}}\right) - \frac{NW_b M(jM+1-K)}{M^2-M}P_{\mathrm{nj}}\right\} \tag{32}$$

$$\frac{\partial P_{\varepsilon,\mathrm{j}}}{\partial W} = \binom{K-1}{j}\left(\frac{1}{M}\right)^{j+1}\left(1-\frac{1}{M}\right)^{K-1-j}\left(-P_{\mathrm{nj}} + P_{\mathrm{fj}}\right) \tag{33}$$

$$\frac{\partial P_{\varepsilon,j}}{\partial N} = \left(P_n + P_p(1-q)\right)\frac{\partial P_{nj}}{\partial N} + \left(P_p q + P_f\right)\frac{\partial P_{fj}}{\partial N} + \frac{q}{N}P_p P_{nj} - \frac{q}{N}P_p P_{fj} \tag{34}$$

$$\frac{\partial P_{\mathrm{nj}}}{\partial N} = \frac{1}{\sqrt{\pi}}e^{-\frac{1}{NSR+2I_j^{\mathrm{k}}}}\left(NSR + 2I_{\mathrm{j}}^{\mathrm{k}}\right)^{-\frac{3}{2}}\frac{\partial I_{\mathrm{j}}^{\mathrm{k}}}{\partial N} \tag{35}$$

$$\frac{\partial P_{\mathrm{fj}}}{\partial N} = \frac{1}{\sqrt{\pi}}e^{-\frac{1}{NSR+JSR+2I_j^{\mathrm{k}}}}\left(NSR + JSR + 2I_{\mathrm{j}}^{\mathrm{k}}\right)^{-\frac{3}{2}}\frac{\partial I_{\mathrm{j}}^{\mathrm{k}}}{\partial N} \tag{36}$$

In addition, the following inequality holds:

$$\begin{bmatrix} \frac{1}{N^*} \\ \frac{M^*}{K_2} \end{bmatrix}^T \begin{bmatrix} \sum_{j=0}^{K-1}\frac{\partial^2 P_{\varepsilon,\mathrm{j}}}{\partial M^2} & \sum_{j=0}^{K-1}\frac{\partial^2 P_{\varepsilon,\mathrm{j}}}{\partial M\partial N} + \mu_1 W_{\mathrm{b}} & \sum_{j=0}^{K-1}\frac{\partial^2 P_{\varepsilon,\mathrm{j}}}{\partial M\partial W} \\ \sum_{j=0}^{K-1}\frac{\partial^2 P_{\varepsilon,\mathrm{j}}}{\partial M\partial N} + \mu_1 & \sum_{j=0}^{K-1}\frac{\partial^2 P_{\varepsilon,\mathrm{j}}}{\partial N^2} & \sum_{j=0}^{K-1}\frac{\partial^2 P_{\varepsilon,\mathrm{j}}}{\partial N\partial W} \\ \sum_{j=0}^{K-1}\frac{\partial^2 P_{\varepsilon,\mathrm{j}}}{\partial M\partial W} & \sum_{j=0}^{K-1}\frac{\partial^2 P_{\varepsilon,\mathrm{j}}}{\partial N\partial W} & 0 \end{bmatrix}_{x^*} \begin{bmatrix} \frac{1}{N^*} \\ \frac{M^*}{K_2} \end{bmatrix} \geq 0 \tag{37}$$

Proof:

In order to apply the KKT conditions, we first need to check the types of inequality constraints, to determine whether they are active or inactive inequality constraints.

It is obvious that (18) is inactive at x^*. To check for (15), first assume that (15) is also inactive at x^*, which infers $M^*N^*W_b - K_1 < 0$. However, it should be noted that P_ε is a monotonically decreasing function with respect to both M^* and N^*; thus, $M^*N^*W_{\mathrm{b}} - K_1 < 0$ means there is still an 'increasing space' for either M^* or N^*, such that P_ε can still be reduced by increasing M^* or N^* to $M^*N^*W_b = K_1$, which contradicts that x^* is the local minimum. Thus, (15) is an active constraint at x^*.

To check for (16), first assume that (16) is inactive at x^*, which means $W^* - K_2M^* > 0$, by applying the KKT necessary conditions (page 316, Proposition 3.3.1 in [20]), we have the unique Lagrange multiplier for (16) $\mu_2 = 0$ and $\sum_{j=0}^{K-1}\frac{\partial P_{\varepsilon,\mathrm{j}}}{\partial W}|_{\mathrm{x}^*} = 0$. However, we should also observe that by (33), $\sum_{j=0}^{K-1}\frac{\partial P_{\varepsilon,\mathrm{j}}}{\partial W}|_{\mathrm{x}^*} \neq 0$ as $P_{\mathrm{nj}} \neq P_{\mathrm{fj}}$, which leads to a contradiction. Thus, (16) is also an active constraint at x^*.

After specifying the type of each inequality constraint, we can obtain Theorem 1 by applying the KKT conditions in Lemma 1 to problem (21).

Remark 1 *We can similarly obtain second-order sufficiency conditions of the problem by applying the following KKT sufficient conditions (page 320, Proposition 3.3.2 in* [20]*): If (*27*) to (*37*) hold for some x and $\mu_i > 0$, $i = 1, \ldots m$, then x is a strict local minimum.*

Remark 2 *Once the solution is found, the integer constraints need to be imposed. For example, assume M, N, W, L are positive integers; first, round one parameter (*e.g., *N) to the nearest integer, then plug it back to the problem and re-compute the solution. After that, round the rest of the parameters in a similar fashion.*

Theorem 1 states the necessary conditions for the optimization problem by employing a general PN-sequence. Now, we will employ the MLS code as the PN-sequence in the HSS system and reformulate Theorem 1 explicitly.

Expression (11) describes that $I_{\mathrm{j}}^{\mathrm{k}}$ for an MLS code is upper-bounded by $I_{\mathrm{j}}^{\mathrm{u}}$. Note that the upper bound of the error probability reserves the same monotonicity with respect to the system parameters (e.g., *M*, *N*). Considering the upper bound $I_{\mathrm{j}}^{\mathrm{u}}$ in (11), Theorem 1 remains the same, with the exception that $\frac{\partial I_{\mathrm{j}}^{\mathrm{k}}}{\partial N}$ is replaced with $\frac{\partial I_{\mathrm{j}}^{\mathrm{u}}}{\partial N}$. After performing some derivations, we obtain:

$$\frac{\partial I_{\mathrm{j}}^{\mathrm{u}}}{\partial N} = I_1 + I_2 + I_3 + I_4 \tag{38}$$

where

$$I_1 = \frac{2\gamma^2\lambda}{N^2}\left(\frac{\lambda}{3N} - \frac{1}{2}\right)$$

$$
\begin{aligned}
I_2 = \frac{2\gamma^2 j}{N^4}\Bigg(& 2NR_u + N^2R_u' - \frac{4NR_u}{3\lambda} - \frac{2N^2R_u'}{3\lambda} - \frac{5N^2}{2\lambda} + 4N^2 \\
& + \left(\frac{(n-1)R_u^2}{6} + \frac{N(n-1)R_uR_u'}{3}\right)\left(26 - \frac{17}{\lambda}\right) \\
& + \frac{13Nn(n-1)R_uR_u'}{3\lambda} + \frac{13n(n-1)R_u^2}{6\lambda} \\
& + \beta\left(1 + 2\beta + \frac{4}{3}\beta^2\right)\left(1 - \frac{n}{\lambda}\right)R_u\left(2NR_u' + R_u\right) \\
& - \beta^2\left(\frac{1}{2} + \frac{4}{3}\beta + \beta^2\right)\frac{R_u}{\lambda}\left(2NR_u' + R_u\right)
\end{aligned}
$$

$$
\begin{aligned}
I_3 = -\frac{8\gamma^2 j}{N^5}\Bigg(& N^2R_u - \frac{2N^2}{3\lambda}R_u - \frac{5N^3}{6\lambda} + \frac{4}{3}N^3 \\
& + \frac{13}{3}N(n-1)R_u^2 - \frac{17N}{6\lambda}(n-1)R_u^2 + \frac{13N}{6\lambda}n(n-1)R_u^2 \\
& + \beta R_u^2 N\left(1 - \frac{n}{\lambda}\right) \times \left(1 + 2\beta + \frac{4}{3}\beta^2\right) \\
& - \beta^2 R_u^2 \frac{N}{\lambda}\left(\frac{1}{2} + \frac{4}{3}\beta + \beta^2\right)\Bigg)
\end{aligned}
$$

$$
I_4 = \frac{j}{6N^3}\left(4N + 8R_u(N-1)R_u' + 4R_u^2\right) - \frac{j}{2N^4}\left(2N^2 + 4R_u^2(N-1)\right) \tag{39}
$$

Plugging the above equations back into Theorem 1, then we can obtain necessary conditions for the local minimum of the upper bound of the error probability for the MLS code. Sufficient conditions can also be obtained from Remark 1.

Remark 3 *Note that in an MLS code, N is an integer such that* $N = 2^n - 1$ *where n is a positive integer. Thus, after obtaining solutions of the local minimum of the problem, N in each solution should be rounded to the closest integers in the form of* $2^n - 1$ *(usually two integers correspond to N in one solution), and the rest of the parameters in the solution should be re-computed and rounded. Then, by comparing the error probabilities resulted from these two sets of parameters, we employ the parameter set with the lower error probability as the local minimum of the problem after re-applying the integer constraints.*

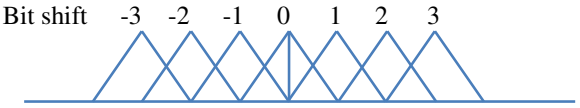

Figure 2 Code-Phase-Shift-Keying modulation for the DS signal.

In the next section, our specific design and implementation of a hybrid DS/FFH radio transceiver using a single FPGA are presented.

6 ORNL specific hybrid DS/FFH design and 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 to 928 MHz ISM band, although target applications such as the SG may ultimately use a dedicated frequency band. The system parameters for the prototype are selected based on the available ISM bandwidth and FPGA capabilities and using the analysis presented in the previous section. The selected parameters are considered to be nearly optimal for a typical smart grid environment.

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. This 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 Figure 1, the HSS unit splits the 902 to 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)

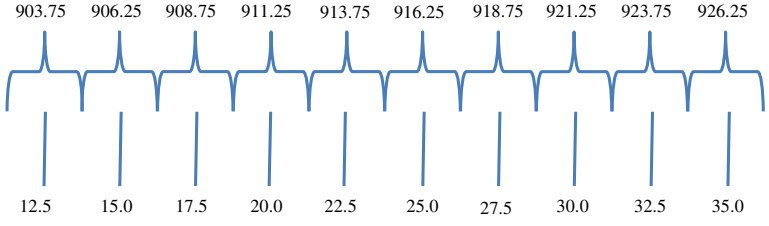

Figure 1 The prototype RF and FPGA frequencies in MHz.

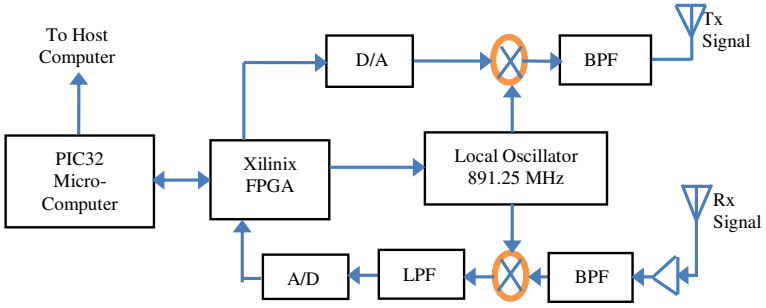

Figure 3 Hardware setup for the hybrid DS/FFH prototype.

converters. The SDR algorithms work over a designated 12.5 to 35.0 MHz frequency range. Each DS signal is a 63-bit length MLS code, although more advanced Gold or Kasami codes could also be used. Three hops per bit are used, and at the receiver a two-out-of-three majority voting decision scheme is employed.

Of particular, interest is the method used 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 [27] or similar mechanism to maintain this phase reference. With HSS in multipath channels, this phase reference is lost after each frequency hop; therefore, we decided to perform the 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 Figure 2.

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. 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. The work in [28] 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 smart grid applications and thus only requires 32 bytes, although the system has operated successfully with 256-byte packets.

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 Figure 3. The

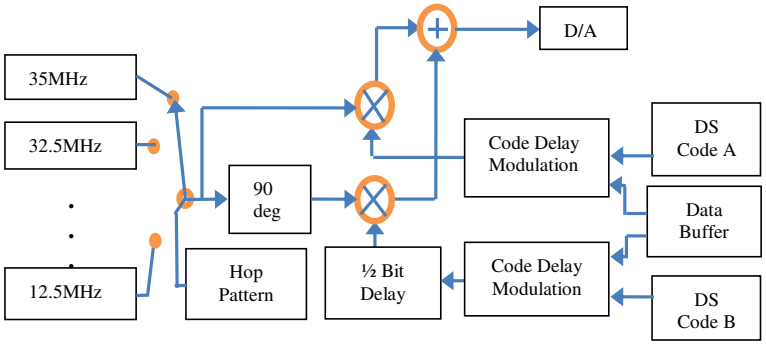

Figure 4 Transmitter portion of the FPGA code.

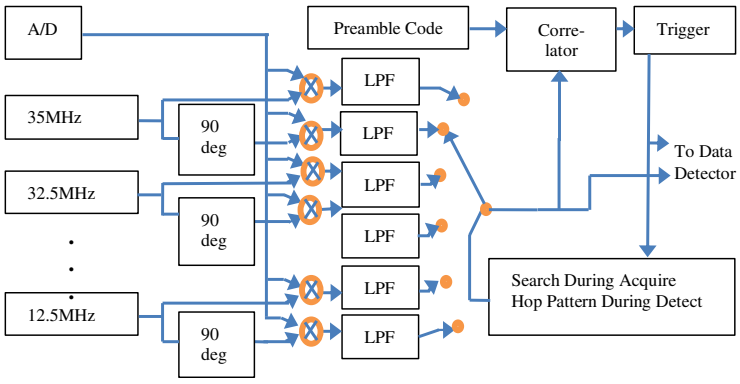

Figure 5 Preamble-detection section of the receiver.

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.

Figure 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 as illustrated in Figure 5.

To acquire the packet preamble, a spread-spectrum correlator continually looks for the preamble 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. To make the signal detection independent of the carrier phase, both phases of the carrier (I and Q) are correlated with the preamble's code. However, the phase relationship must remain consistent during the duration of the DS sequence.

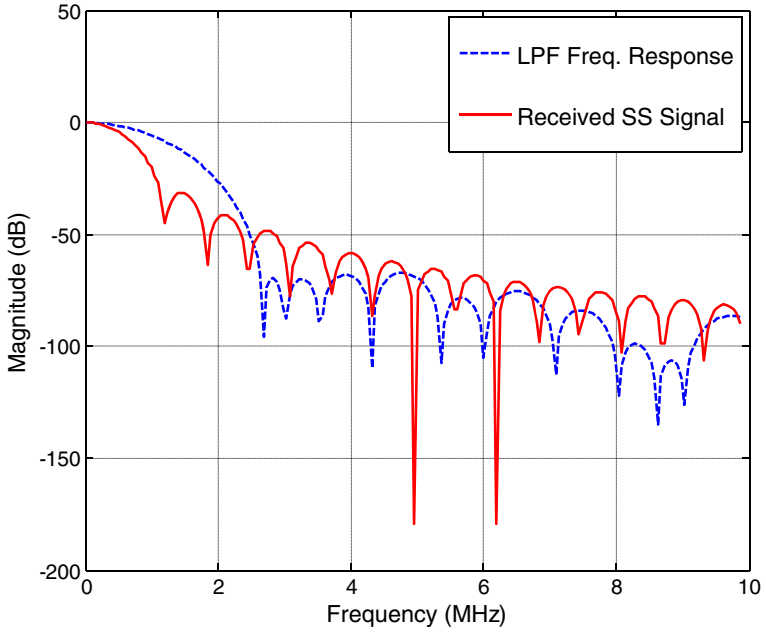

Figure 6 Analytically generated frequency response of the low-pass filter. The frequency response of the digital LPF implemented in the FPGA, superimposed on the frequency spectrum of the received SS signal.

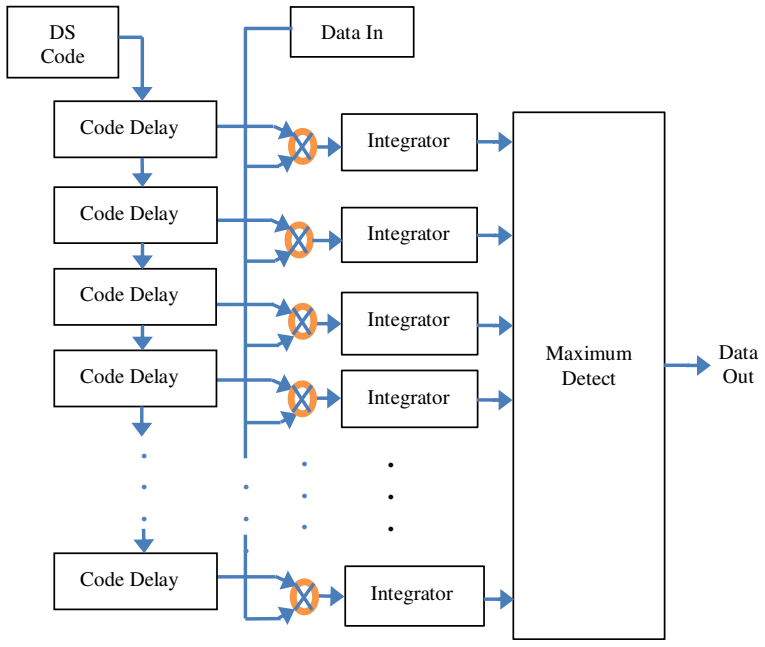

Figure 7 Data-detection section of the receiver.

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. Figure 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.

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

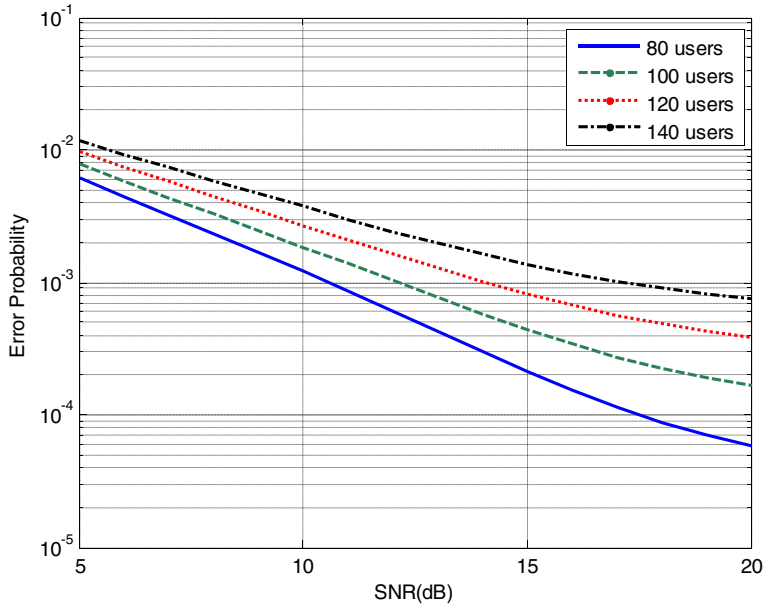

Figure 8 Performance of a hybrid DS/FFH system. Effect of different number of users (multi-user interference).

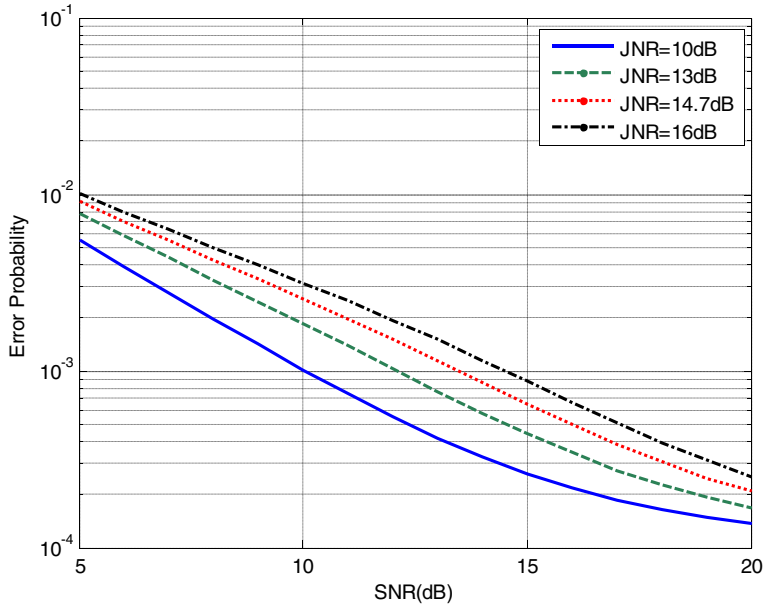

Figure 9 Performance of a hybrid DS/FFH system. Effect of different jamming-to-noise ratios (JNRs).

for signal detection as illustrated in Figure 7. In the next section, we present experimental results to demonstrate the performance of the hybrid DS/FFH prototype.

7 Numerical and experimental results

7.1 Hybrid DS/FFT system performance

We first demonstrate the performance of a hybrid DS/FFH system over Rician time-selective fading channels, progressively including the effects from wide- and partial-band jamming, multi-user interference, and varying degrees of Rician fading. The performance measure is the upper bound of BER described in (14) by employing (11). The parameters of the reference system model considered in this numerical example are total number of users is $K = 100$; number of hops per bit is $L = 5$; number of frequency-hopping channels is $M = 30$; period of PN-sequence in DSSS is $N = 127$; jamming-to-noise ratio (JNR) is 13 dB; number of channels fully jammed is 5; the Rician channel coefficient $\gamma = 0.1$ (represents the channel fading part); channel covariance function scaling factor $\lambda = 10.8$; and the

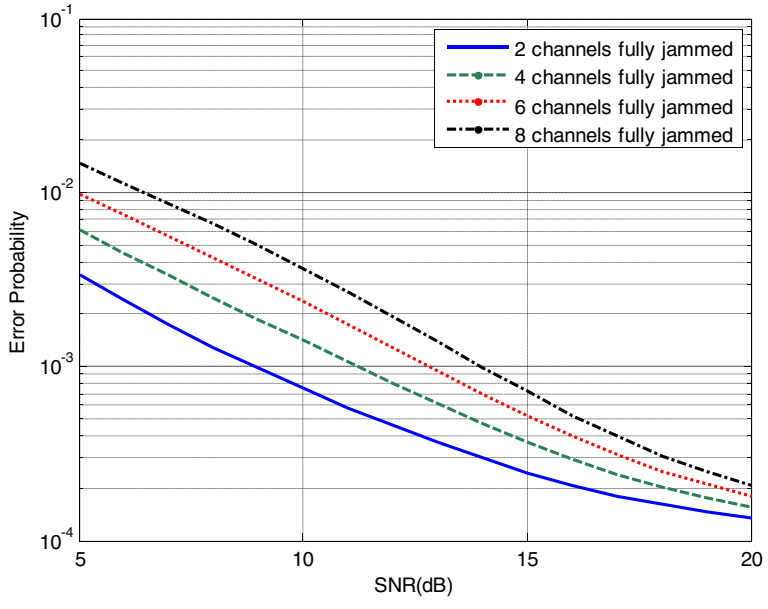

Figure 10 Performance of a hybrid DS/FFH system. Effect of different number of fully jammed channels.

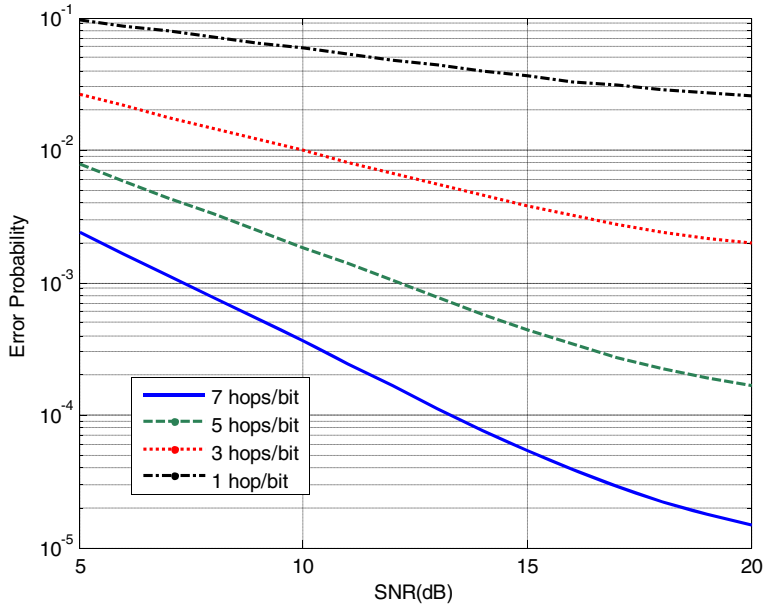

Figure 11 Performance of a hybrid DS/FFH system. Effect of different number of hops per bit.

portion of the channel partially corrupted is 0.4. The parameter space of the HSS system is explored to demonstrate its effectiveness under different conditions and scenarios. In the following analysis, we successively vary one parameter in the reference system model while fixing the other parameters.

Figure 8 shows the effect of different number of continuously transmitting users (multi-user interference) on the performance of a hybrid DS/FFH system. You can observe the high multiple access capability of such a technique, especially at high SNRs. Figure 9 demonstrates the performance for different jamming to noise ratios (JNRs), and Figure 10 demonstrates the performance for varying number of fully jammed channels. You can observe from Figures 9 and 10 the high anti-jamming capability of such a technique, especially at high SNRs. Also, it can be observed that under high SNRs the performance gap reduces for different JNRs and different numbers of fully jammed channels. Figure 11 demonstrates the performance for different numbers of hops per bit. Notice that the

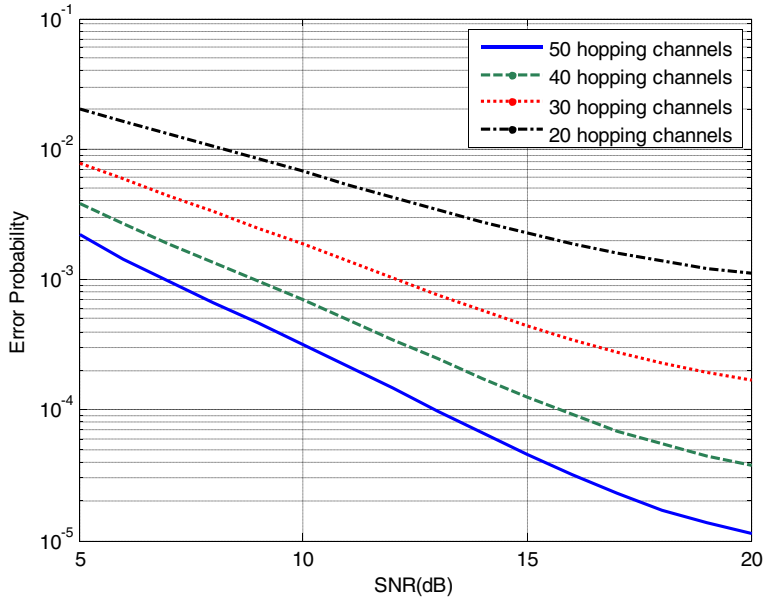

Figure 12 Performance of a hybrid DS/FFH system. Effect of different number of available hopping channels.

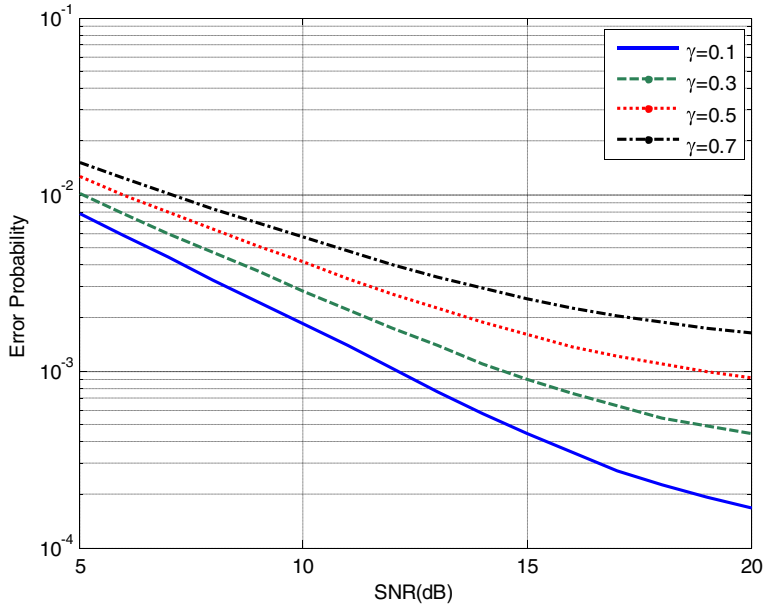

Figure 13 Performance of a hybrid DS/FFH system. Effect of different Rician fading channel parameters.

performance of the DS/FFH system is superior to that of the DS/SFH system (represented by the 1 hop/bit case). Also, notice the high improvement in performance at higher SNRs when increasing the number of hops per bit. This reveals the effectiveness of the proposed technique at high SNRs.

Figure 12 demonstrates the DS/FFH performance for different numbers of available hopping channels. Increasing the number of hopping channels reduces the likelihood of hits from other users using the same spreading PN-code and, therefore, enhances the performance. Figure 13 demonstrates the DS/FFH performance over varying degrees of Rician fading in the channels. You can observe how the performance deteriorates with increasing the fading component in the Rician channel represented by the parameter γ.

Figure 14 demonstrates the DS/FFH performance compared with the other SS systems that include DS, SFH, FFH, DS/SFH, and DS/FFH. It can be observed that the hybrid

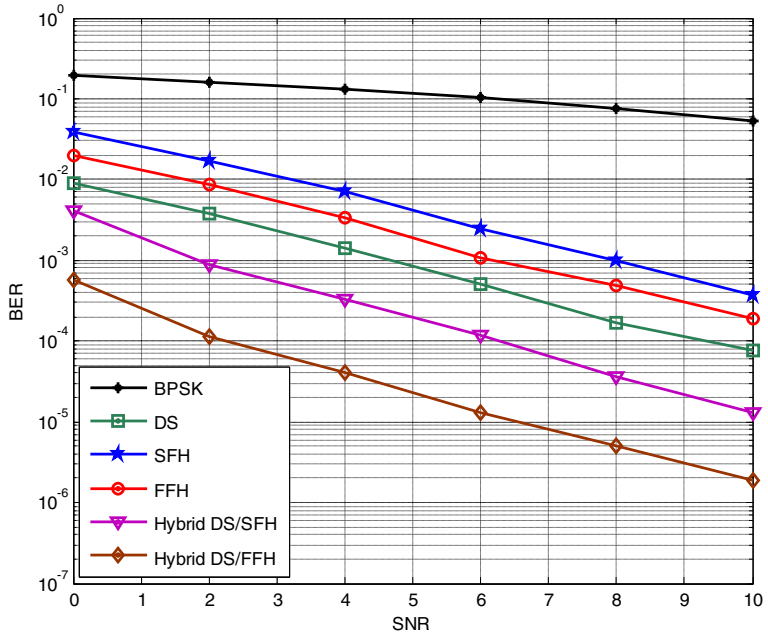

Figure 14 Performance of a two-path Rayleigh hybrid DS/FFH system. Performance comparison.

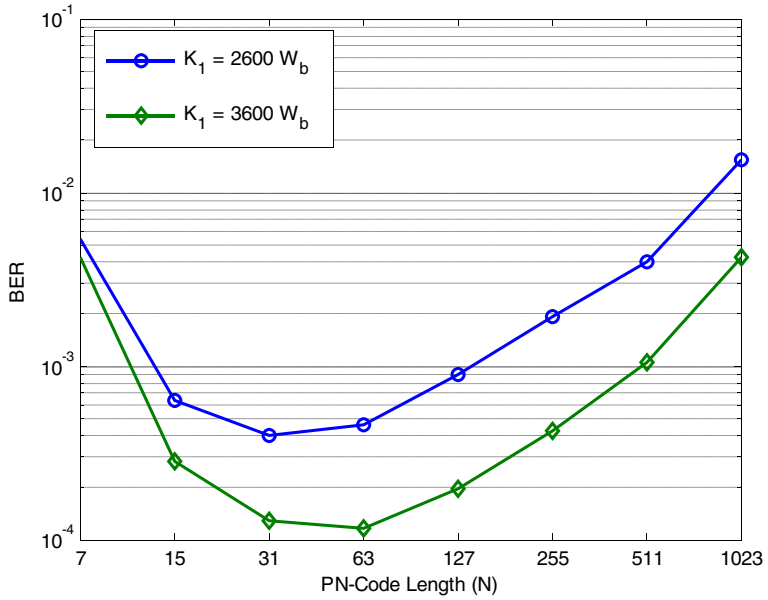

Figure 15 BER versus DS PN-code length *N*.

DS/FFH system outperforms the other SS systems. The hybrid DS/FFH system is preferred over the other systems because of its unique advantages, including the better spreading properties gained by frequency hopping and better multipath rejection via the direct-sequence modulation component.

The presented results demonstrate the effectiveness of the proposed hybrid DS/FFH scheme under severe channel conditions and, therefore, indicate that there is a high potential for employing it in complex smart grid communications.

7.2 *Optimizing hybrid DS/FFT system performance*

We now provide numerical examples to illustrate the results derived in Section 5. For convenience, we only test the necessary conditions that apply to the MLS code. We compute the solutions of the first-order necessary conditions (27) to (31) and impose the integer constraints. Then, the upper bound of the BER, P_E, is plotted for different MLS code lengths N using (14) and (11) to verify the results computed from the derived first-order necessary conditions.

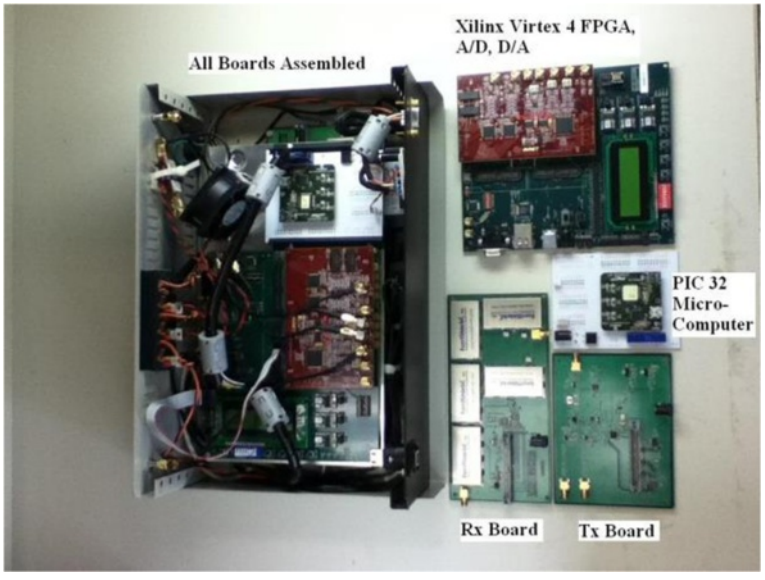

Figure 16 The implemented hybrid DS/FFH prototype.

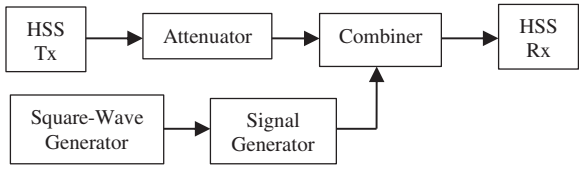

Figure 17 Experimental setup for testing hybrid DS/FFH jamming resistance.

The parameters of the reference hybrid DS/FFH system model considered is the same as described in the previous section ($K = 100$; JNR = 13 dB; $\gamma = 0.1$; *and* $\lambda = 10.8$), in addition to a signal-to-noise ratio (SNR) of 20 dB; finally, the portion of the channel partially corrupted is $q = W_J^p/(NW_b) = 30/N$. Note that the parameters M, N, W, L need to be computed for assessing the optimal performance. From the previous analysis, the number of hops per bit is chosen as $L = (1/K_3W_b) = 5$.

First, we choose $K_1 = 2600$ W_b and $K_2 = 0.2$. Then, by applying (27) to (31), we obtain $N = 42$. Because of the integer power-of-two constraint of N ($N = 2^n - 1$), it is rounded to the nearest two integers, 31 and 63. Then by applying (30) and (31) for each integer of N and comparing the corresponding BER of both integers, we see that $N = 31$, $M = 83$, and $W = 17$ results in a smaller BER. The upper bound of the BER in (14) for different PN-code lengths, N, is demonstrated in Figure 15, in which we can now observe that at $N = 31$, the BER reaches its minimum. This coincides with the result from the first-order necessary conditions.

Now, we consider $K_1 = 3600$ W_b, with K_2 unaltered. Through a similar procedure, we obtain $N = 48.3$. After rounding N to 31 and 63, it can found that $N = 63$, $M = 57$, and $W = 11$ results in smaller BER values. Figure 15 demonstrates the upper bound of the BER for different PN-code lengths, N, for this scenario. It can now be observed that the BER reaches its minimum at $N = 63$, which also coincides with the result from our analysis.

7.3 Experimental evaluations

Four bi-directional hybrid DS/FFH radio transceivers have been built in our lab and have performed well. The hardware prototype is shown in Figure 16. 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. Also, the radios demonstrated a bit error rate of less than 10^{-6}.

The jamming performance of the system was measured directly with laboratory equipment. The testing method used for the HSS evaluation is shown in Figure 17. 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

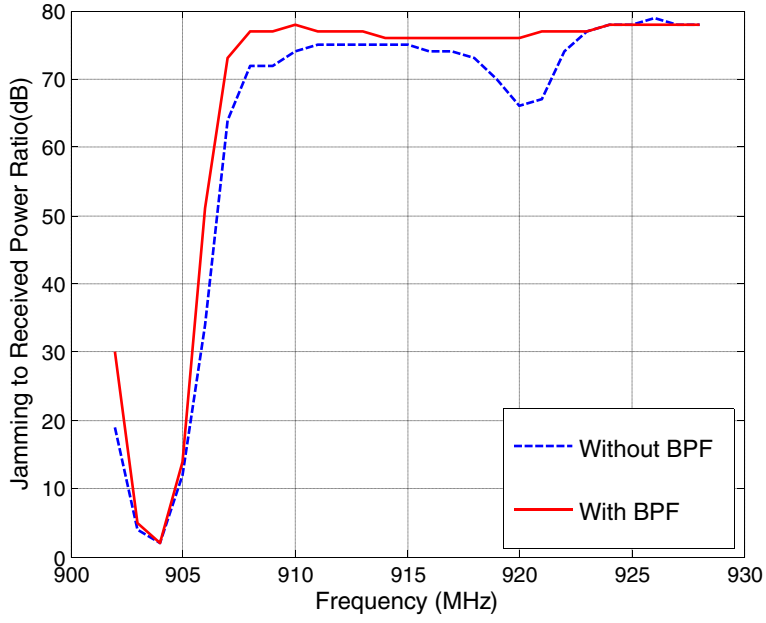

Figure 18 The hybrid DS/FFH prototype performance while the frequency-hopping feature is disabled and with no jamming.

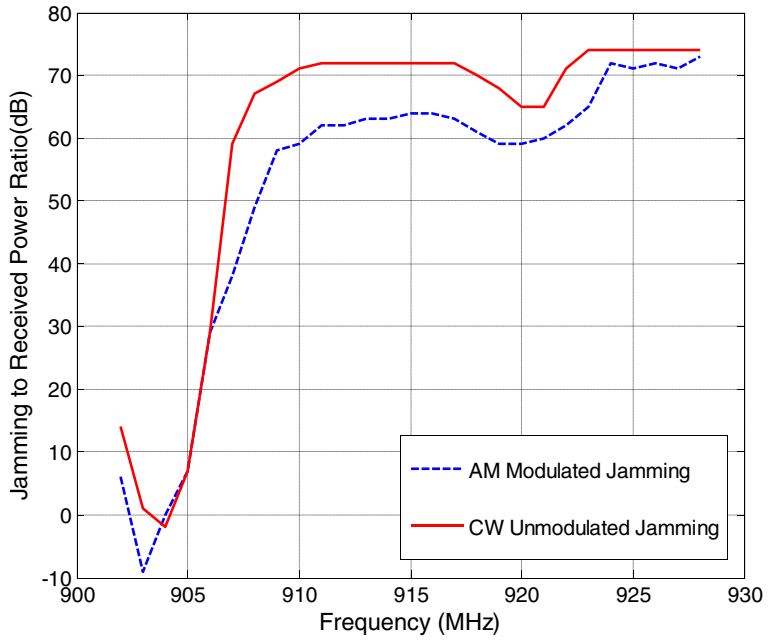

Figure 19 The hybrid DS/FFH prototype performance while the frequency hopping feature is disabled and in the presence of jamming.

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 nonlinear effects that are expected in the A/D converter, SDR arithmetic, and analog front-end components.

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. In this test, the intermediate frequency

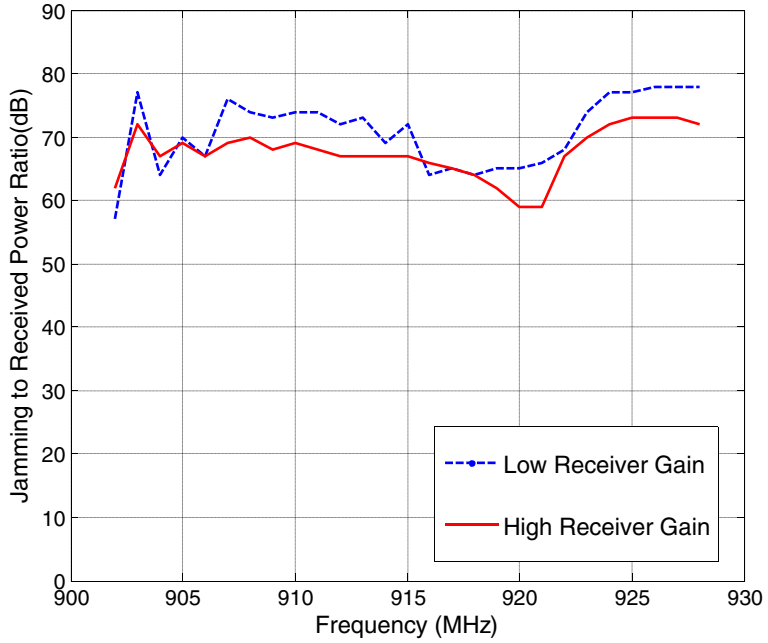

Figure 20 The hybrid DS/FFH prototype performance in the presence of jamming.

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 Figure 18. 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 19 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 feature 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. Figure 20 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 Figure 20 that the smaller signal has less distortion and is able to better reject the undesired jamming signal at almost all frequencies.

8 Conclusion

In this paper, the performance of a hybrid DS/FFH system over Rician fading channels was considered. We derived the average BER for a hybrid DS/FFH system that includes the effects from wide- and partial-band jamming, multi-user interference, and/or varying degrees of Rician fading. Numerical results exploring the parameter space of the HSS system have also been presented to demonstrate its effectiveness under different conditions and scenarios. We have also demonstrated a novel non-convex optimization technique that minimizes the bit-error probability of a hybrid DS/FFH communication system under multiple constraints. By employing the Karush-Kuhn-Tucker conditions, the process solves for the optimal system design parameters. In addition, 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 and interference 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 use of hybrid DS/FFH waveform in wireless networks as employed in the smart grid is recommended, as it offers superior resistance to jamming attacks and improves the reliability of transmission compared to existing SS techniques like DS, FH, and hybrid DS/SFH systems.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

MO carried out the hybrid DS/FFH system performance evaluation studies, conducted the computer simulations that provided numerical results, participated in deriving the analytical expressions and conducting experimental evaluations, and drafted the manuscript. XM derived the analytical expressions for evaluating and optimizing the performance and helped in drafting the manuscript. SK implemented the hybrid DS/FFH radio transceiver and evaluated its performance experimentally. TK shaped the main idea of the study and participated in its design, development, and coordination. SS conceived of the study and participated in investigating and enhancing its security performance. SD guided the analytical derivations and analysis. All authors read and approved the final manuscript.

Acknowledgment

This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. 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. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan. In addition, this work has been partially supported by NSF grant CMMI-1334094.

Author details

[1]Computational Sciences and Engineering Division, Oak Ridge National Laboratory, P.O. Box 2008, MS 6085, Oak Ridge, TN 37831, USA. [2]Department of Electrical Engineering and Computer Science, University of Tennessee, 1520 Middle Drive, Knoxville, TN 37996, USA. [3]Department of Electrical Engineering and Computer Science, Masdar Institute of Science and Technology, Masdar City, Abu Dhabi, UAE.

Received: 30 October 2014 Accepted: 17 February 2015
Published online: 12 March 2015

References

1. MP Pursley, Direct sequence spread spectrum communications for multipath channels. IEEE Trans Microwave Theory Tech **50**(3), 653–661 (2002)
2. EA Geraniotis, Noncoherent hybrid DS-SFH spread-spectrum multiple-access communications. IEEE Trans Commun **34**(9), 862–872 (1986)
3. J Zhang, KC Teh, KH Li, Error probability analysis of FFH/MFSK receivers over frequency-selective Rician-fading channels with partial band noise jamming. IEEE Trans Commun **57**(10), 2880–2885 (2009)
4. JH Lee, BS Yu, SC Lee, Probability of error for a hybrid spread spectrum system under tone jamming, in *Proc. of the IEEE Military Communications Conference (MILCOM'90)*, 1990, pp. 410–414
5. MM Olama, X Ma, PT Kuruganti, SF Smith, SM Djouadi, Hybrid DS/FFH spread-spectrum: a robust, secure transmission technique for communication in harsh environments, in *Proc. of the IEEE Military Communications Conference (MILCOM'11)*, 2011, pp. 2136–2141

6. Y Fu, H Leung, Narrow-band interference cancellation in spread-spectrum communication systems using chaos. IEEE Trans Circuit Syst I **48**(7), 847–858 (2001)
7. Security Profile for Advanced Metering Infrastructure (AMI), The Advanced Security Acceleration Project (ASAP-SG), Version 2.0, Jun. 2010. Available at: http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20Profile%20-%20v2_0.pdf
8. Analog Devices, A Technical Tutorial on Digital Signal Synthesis, Technical Report, 1999. Available at: http://www.analog.com/media/cn/training-seminars/tutorials/450968421DDS_Tutorial_rev12-2-99.pdf
9. PA Bello, Characterization of randomly time-variant linear channels. IEEE Trans Commun Syst **11**, 360–393 (1963)
10. DE Borth, MB Pursley, Analysis of direct-sequence spread-spectrum multiple access communication over Rician fading channels. IEEE Trans Commun **27** (10), 1566–1577 (1979)
11. EA Geraniotis, MB Pursley, Error probabilities for slow-frequency-hopped spread-spectrum multiple-access communications over fading channels. IEEE Trans Commun **30**(5), 996–1010 (1982)
12. EA Geraniotis, Coherent hybrid DS-SFH spread-spectrum multiple-access communications. IEEE Trans Commun **3**(5), 695–705 (1985)
13. B Solaiman, A Glavieux, A Hillion, Error probability of fast frequency hopping spread spectrum with BFSK modulation in selective Rayleigh and selective Rician fading channels. IEEE Trans Commun **38**(2), 233–240 (1990)
14. C Park, JH Lee, Probability of error for a hybrid DS/SFH spread spectrum system over a Rician fading channel in the presence of multiple-tone jamming, in *Proc. of the IEEE Second International Symposium on Spread Spectrum Techniques and Applications (ISSSTA'92)*, 1992, pp. 123–126
15. CC Chen, K Yao, K Umeno, E Biglieri, Design of spread-spectrum sequences using chaotic dynamical systems and ergodic theory. IEEE Trans Circuit Syst I **48**(9), 1110–1114 (2001)
16. MM Olama, SF Smith, PT Kuruganti, X Ma, Performance study of hybrid DS/FFH spread-spectrum systems in the presence of frequency-selective fading and multiple-access interference, in *Proc. of the IEEE International Communications Quality and Reliability (CQR) Conference*, 2012
17. X Ma, MM Olama, T Kuruganti, SF Smith, SM Djouadi, Determining system parameters for optimal performance of hybrid DS/FFH spread-spectrum, in *Proc. of the IEEE Military Communication Conference (MILCOM'12)*, 2012, pp. 1888–1893
18. M Killough, MM Olama, T Kuruganti, SF Smith, FPGA-based implementation of a hybrid DS/FFH spread-spectrum transceiver, in *Proc. of the World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'13)*, 2013
19. MM Olama, SM Killough, T Kuruganti, TE Carroll, Design, implementation, and evaluation of a hybrid DS/FFH spread-spectrum radio transceiver, in *Proc. of the IEEE Military Communication Conference (MILCOM'14)*, 2014
20. DP Bertsekas, *Nonlinear Programming*, 3rd edn. (Athena Scientific, Belmont, Massachusetts, 1999)
21. M Schwartz, WR Bennett, S Stein, *Communication Systems and Techniques* (McGraw-Hill, New York, 1966)
22. HL Van Trees, *Detection, Estimation, and Modulation Theory, Part 111* (Wiley, New York, 1971)
23. RS Kennedy, *Fading Dispersive Communication Channels* (Wiley, New York, 1969)
24. MB Pursley, Performance evaluation for phase coded spread spectrum multiple-access communication-Part I: system analysis. IEEE Trans Comm **25**, 759–799 (1977)
25. TS Rappaport, *Wireless Communications: Principles and Practice* (Prentice Hall, New Jersey, 1996)
26. DV Sarwate, An upper bound on the aperiodic autocorrelation function for a maximal-length sequence. IEEE Trans Inf Theory **30**(4), 685–687 (1984)
27. D Taylor, Introduction to synchronous communications, a classic paper by. J Costas Proc IEEE **90**(8), 1459–1460 (2002)
28. Y-R Tsai, M-ary Spreading-Code-Phase-Shift-Keying modulation for DSSS multiple access systems. IEEE Trans Comm **57**(11), 3220–3224 (2009)