Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2008, Article ID 979813, 12 pages
doi:10.1155/2008/979813

Research Article

Design, Analysis, and Performance of a Noise Modulated Covert Communications System

Jack Chuang, Matthew W. DeMay, and Ram M. Narayanan

Department of Electrical Engineering, The Pennsylvania State University, University Park, PA 16802, USA

Correspondence should be addressed to Ram M. Narayanan, ram@engr.psu.edu

Received 10 March 2008; Revised 2 June 2008; Accepted 22 July 2008

Recommended by Ibrahim Develi

Ultrawideband (UWB) random noise signals provide secure communications because they cannot, in general, be detected using conventional receivers and are jam-resistant. We describe the theoretical underpinnings of a novel spread spectrum technique that can be used for covert communications using transmissions over orthogonal polarization channels. The noise key and the noise-like modulated signal are transmitted over orthogonal polarizations to mimic unpolarized noise. Since the transmitted signal is featureless and appears unpolarized and noise-like, linearly polarized receivers are unable to identify, detect, or otherwise extract useful information from the signal. The wide bandwidth of the transmitting signal provides significant immunity from interference. Dispersive effects caused by the atmosphere and other factors are significantly reduced since both polarization channels operate over the same frequency band. The received signals are mixed together to accomplish demodulation. Excellent bit error rate performance is achieved even under adverse propagation conditions.

1. INTRODUCTION

The primary objectives of today's wireless secure communications systems are to simultaneously and reliably provide communications that are robust to jamming and provide low probability of detection and low probability of intercept in hostile environments. Spread spectrum techniques, such as direct-sequence spread-spectrum systems and frequency-hopping spread-spectrum systems, have been widely used in wireless military applications for many years. Such systems have the ability to communicate in the presence of intentional interference and also permit transmission with a very low-power spectral density by spreading the signal energy over a large bandwidth to thwart detection [1, 2]. Thus, spread spectrum techniques offer both security and low probability of detection features. However, statistical processing techniques, such as triple correlation [3, 4], autocorrelation fluctuation estimators [5], and multihop maximum likelihood detection [6] have been developed which exploit the statistical properties of the pseudonoise sequences used in direct-sequence spread-spectrum systems and the pseudorandom frequency-hopping sequences used in frequency-hopping spread-spectrum systems, thereby permitting third parties to detect the hidden message signal. Further research has revealed that the chaotic and ultrawideband (UWB) noise waveforms are ideal solutions to combat detection and exploitation since the transmitted signals have unpredictable random-like behavior and do not possess repeatable features for signal identification purposes [7–9].

Digital communication systems utilizing wideband carriers require a coherent reference for optimal data processing. This reference may be either locally generated or transmitted simultaneously with the data. The transmitted reference (TR) technique was initially explored as a means for establishing communication when there are critical unknown properties of the transmitted signal or channel [10, 11]. This scheme completely avoids the synchronization problem of locally generated reference systems but performance will be worse than the locally generated reference systems at the same signal-to-noise ratios (SNRs) because the noise-cross-noise term will appear at the output of correlator [12].

The purpose of this new polarization diversity system is to be able to conceal a message from an adversary and to avoid jamming countermeasures while maintaining an acceptable performance level. A band-limited true Gaussian noise waveform is used to spread the signal's power into large bandwidth. Thus, an extremely large processing gain is achieved and the system can operate in a noisy and jammed channel. The primary reason of choosing the UWB noise waveform is because it provides covertness. In the time domain, the transmitted signal appears as unpolarized noise to the outside observer while the spectrum hides under the ambient noise in the frequency domain. However, the drawback of this noise modulated UWB TR system is the increased system complexity compared with the pulse-based UWB TR system introduced in [13, 14]. Since a continuous wave signal is used, the time separation structure introduced in [14] cannot be used because eight interference terms will be generated after the mixing process in our receiver. A solution is simultaneously transmitted the reference signal and message signal on orthogonal polarization channels and only three interference terms will be generated after mixing process. However, the system which may confront polarization mismatch will be discussed in Section 5, and the rotation angle between transmitter's and receiver's antenna needs to be estimates to compensate performance degrading causing by polarization mismatch. On the other hand, this noise modulated UWB TR system also requires adding extra circuit to alleviate BER degradation in multipath environment while the pulse-based UWB TR system can directly operate in multipath environment.

In our earlier publications, simulation results demonstrate that the noise modulated covert communication system maintains good performance in white Gaussian noise channels, and indoor experiments prove that the system can retrieve messages in interference-free channels [15, 16]. In this paper, a theoretical performance metric is derived and compared with simulations, for both single-user and multiuser environments, that demonstrate the system's ability to operate in a noisy channel. We also present preliminary field test results with the baseband processing implemented in a software defined radio architecture that clearly validates that the system concepts.

2. RF SYSTEM OVERVIEW

2.1. Transmitter

The block diagram of the transmitter section of our secure communications system is shown in Figure 1(a). A random noise generator generates a zero-mean band-limited Gaussian noise waveform. This Gaussian noise is passed through a bandpass filter. The bandpass filter ensures that the signal is confined within the 1-2-GHz operating frequency range with a 1.5-GHz center frequency. The output signal $n(t)$ can be expressed as [17]

$$n(t) = a(t)\cos\left(2\pi f_n t + \theta(t)\right), \tag{1}$$

where $a(t)$ is a Rayleigh distributed random variable, $\theta(t)$ is a uniformly distributed random variable in the range $[-\pi, \pi]$, and f_n is the center frequency (1.5-GHz in our case) of the band-limited noise. This filtered noise is then fed to a power divider. One output of the power divider connects to a delay line with a predetermined and controllable delay t_1. The delayed signal is amplified and transmitted through a horizontally polarized antenna working as the reference. The reference can be mathematically represented as

$$H(t) = a(t-t_1)\cos\left(2\pi f_n(t-t_1) + \theta(t-t_1)\right). \tag{2}$$

Without knowledge of this specific delay time, a third party cannot recover the data even if they know that the message and reference are being transmitted. Furthermore, assigning different delay times to different users will allow multiple users to share the same channel at the same time.

A binary bit sequence $m(t)$ is sent from the digital-to-analog converter of the field programmable gate array board to the mixer and is mixed with the 3-GHz ($= f_c$) carrier that is generated by a phase-locked oscillator. This narrow-band (3-GHz) modulated radio frequency (RF) message signal is used as the local oscillator of the single sideband up-converter and mixed with the filtered band-limited noise from the other output of the power divider. The single sideband up-converter can either select the upper sideband (centered at $f_c + f_n$) or the lower sideband (centered at $f_c - f_n$) of the mixing process. In our system, the lower sideband is selected. This noise-like signal is amplified and transmitted through a vertically polarized antenna which we denote as $V(t)$. The amplifier gains are adjusted to equalize the transmit power levels at the two antennas. Clearly, the noise-like signal $V(t)$ can be expressed as

$$V(t) = m(t)a(t)\cos\left(2\pi(f_c - f_n)t - \theta(t)\right). \tag{3}$$

By judiciously choosing $f_c = 2f_n$, we ensure that the lower sideband signal $V(t)$ is located over the same frequency range as $H(t)$. Thus, the dispersive effects caused by the atmosphere and other factors are significantly reduced since both polarization channels operate over the same frequency band. It is evident that the spread spectrum process is accomplished within the single sideband up-converter, and this noise-like signal contains the message that we wish to transmit covertly. Since $m(t)$ is either +1 or −1, the statistical properties of $V(t)$ should be the same as a zero-mean band-limited Gaussian random variable. From Figure 2, we confirm that the spectrum of $V(t)$ is indeed flat over the band and presents unpredictable behavior in the time domain.

If $H(t_k)$ and $V(t_k)$ are the instantaneous magnitudes of the electromagnetic fields in the horizontal and vertical polarization channels at time t_k, respectively, then the instantaneous amplitude $E(t_k)$ and the instantaneous polarization angle $\phi(t_k)$ (with respect to the vertical) of the composite transmitted wave are, respectively, given by

$$\begin{aligned} E(t_k) &= \sqrt{H^2(t_k) + V^2(t_k)}, \\ \phi(t_k) &= \tan^{-1}\left(\frac{H(t_k)}{V(t_k)}\right). \end{aligned} \tag{4}$$

Clearly, the instantaneous amplitude and polarization angle of the transmitted composite electromagnetic wave are also random variables. Figure 3 shows the simulation results of the amplitude and phase plot for the composite electromagnetic wave. Since the polarization angle is random, the

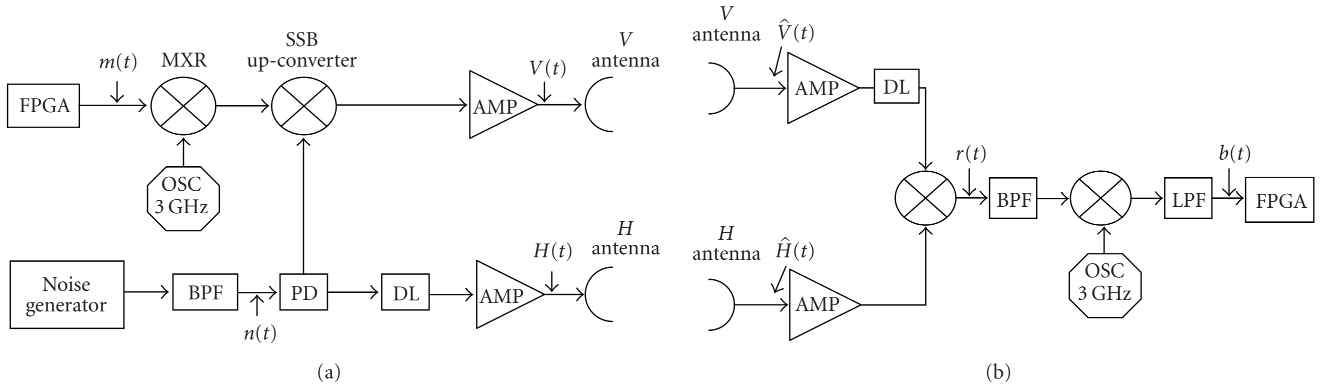


Figure 1: (a) Transmitter block diagram, (b) receiver block diagram. (AMP = amplifier, BPF = bandpass filter, DL = delay line, FPGA = field programmable gate array, H = horizontal, OSC = oscillator, PD = power divider, SSB = single sideband, V = vertical).

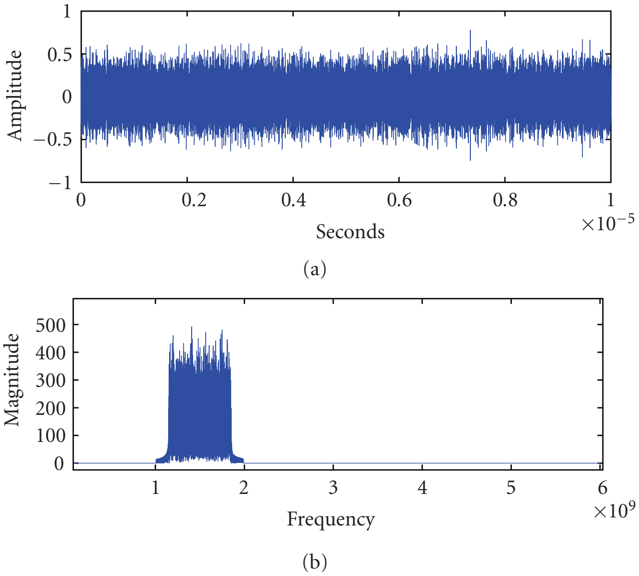


Figure 2: (a) Time domain and (b) frequency domain plot of vertically polarized transmitted signal.

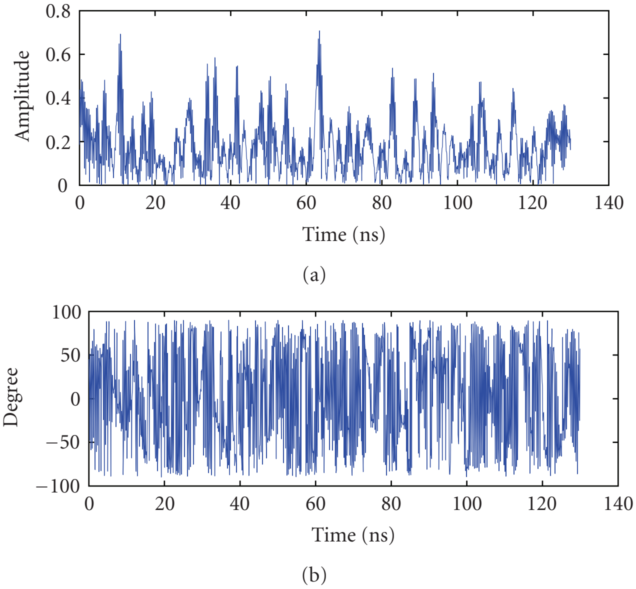


Figure 3: (a) Amplitude and (b) polarization angle plot of composite transmitted electromagnetic wave.

composite transmitted signal appears totally unpolarized to any outside observer. Unlike single carrier communication systems, the samples of our RF signals have aperiodic random behavior. It is therefore very difficult for a third party to recognize that there is a message propagating in the air since the waveform appears as unpolarized noise, thereby providing the covertness feature.

2.2. Receiver

The block diagram of the receiver section is shown in Figure 1(b). For short-range (less than 5 km) and low frequency (less than 20 GHz) applications, we can assume that the amplitude and phase factors are the same for both polarization channels, since they are specifically designed so as to operate over the same frequency band. The received signals $\hat{V}(t)$ and $\hat{H}(t)$ for the vertically and horizontally polarized channels, respectively, are given by

$$\hat{V}(t) = Am(t)a(t)\cos\left(2\pi(f_c - f_n + f_d)t - \theta(t)\right),$$
$$\hat{H}(t) = Aa(t-t_1)\cos\left(2\pi(f_n + f_d)(t-t_1) + \theta(t-t_1)\right), \tag{5}$$

where A is the attenuation factor ($0 \leq A \leq 1$) causing by propagation and f_d is Doppler shift due to moving transmitter or receiver. In general, A can be considered as constant when the distance between transmitter and receiver is small (a few km) under clear atmospheric conditions but will be a frequency-dependent when the distance becomes larger or unfavorable atmospheric conditions, such as heavy rain exists [18]. The performance will indeed degrade when the spectrum of received signal is not flat [15]. To overcome this problem, the communication link should ideally estimate attenuation information based on local climatology and compensate for it at the transmitter, especially when the system is used for operation over large distances. Without loss of generality, therefore, we assume that $A = 1$. We also assume perfect carrier synchronization at receiver side, and therefore f_d can be considered to be zero without affecting the following analysis.

The $\widehat{V}(t)$ signal is amplified and passed through a delay line with the exact same delay time t_1 as introduced in the transmitter (for the horizontal channel). It is then mixed with the $\widehat{H}(t)$ signal in the mixer, which acts as a correlator. This brings the two channels in synchronization. If this delay does not exactly match the corresponding transmit delay, no message can be extracted from the mixed signal. Only a friendly receiver knows the exact value of this delay, and thus an unfriendly receiver will not be able to perform the proper correlation to decode the hidden message.

The mixed output signal $r(t)$, caused by mixing (i.e., multiplying) $\widehat{V}(t-t_1)$ and $\widehat{H}(t)$, containing both the sum frequency signal $s(t)$ and the difference frequency signal $d(t)$ can be expressed as

$$\begin{aligned} r(t) &= 0.5a^2(t-t_1)m(t-t_1)\cos(2\pi f_c(t-t_1)) \\ &\quad + 0.5a^2(t-t_1)m(t-t_1)\cos(2\theta(t-t_1)) \\ &= s(t) + d(t). \end{aligned} \tag{6}$$

The difference frequency output containing the random phase term can be regarded primarily as low-frequency interference which can be eliminated by filtering. However, the sum frequency is always centered at $f_c = 2f_n$ and can be easily demodulated. The bandpass filter centered at f_c following the first mixer in the receiver will capture the desired sum frequency signal while discarding the low-frequency interference. The filtered RF signal is mixed with the output of an oscillator at f_c (3 GHz in our system) in order to strip off the carrier. The received baseband signal $b(t)$ at the output of the low-pass filter is expressed as

$$b(t) = 0.25a^2(t-t_1)m(t-t_1) \otimes h(t), \tag{7}$$

where $h(t)$ is filter impulse response. Since binary modulation is used and the $a^2(t-t_1)$ term is always positive, the transmitted bit sequence can be successfully retrieved from $b(t)$.

3. SYSTEM PERFORMANCE MODELING

In wireless communications, the bit error rate (BER) is an important metric which is used to gauge and compare the system performance. Since this noise modulated covert communications system is a new architecture, the theoretical BER performance in an additive white Gaussian noise channel is derived and compared with simulation results in this section. Unlike other single-channel spread spectrum systems, the low-pass equivalent model can directly be used to model the system behavior in the Gaussian channel. The spreading and dispreading process of our system is accomplished at the RF front-end. The noise floor at the antenna output is not the same as that at the output of the first mixer, and the noise terms within the system are generated by mixing of two zero mean independent Gaussian random variables. Thus, the system behavior needs to be modeled based upon the relationship between the SNR at the output of receiver antenna and the probability of bit error. In this section, we will demonstrate that the mixed noise can be approximated as Gaussian after passing through a narrow-band filter, and the BER equation can be expressed using the Q-function. The bandwidths of the signal, antenna, low-pass filter, and the SNR at the output of receiver's antenna are the parameters which dominate the BER when the bit rate is fixed.

To simplify the analysis, we assume that the delay term t_1 is set to zero in both the transmitter and the receiver. This simplification will not affect the BER analysis. In an additive white Gaussian noise channel, the actual received signal from the vertically polarized antenna $\widetilde{V}(t)$ and the horizontally polarized antenna $\widetilde{H}(t)$ can be written, respectively, as

$$\begin{aligned} \widetilde{V}(t) &= \widehat{V}(t) + n_V(t), \\ \widetilde{H}(t) &= \widehat{H}(t)|_{t_1=0} + n_H(t). \end{aligned} \tag{8}$$

The $n_V(t)$ and $n_H(t)$ terms are independent zero-mean band-limited Gaussian noise in the vertical and horizontal polarization channels, and these terms are also independent of $\widehat{V}(t)$ and $\widehat{H}(t)$. Their analytical forms are similar to $n(t)$ as shown in (1), that is,

$$\begin{aligned} n_V(t) &= a_V(t)\cos(2\pi f_n + \theta_V(t)), \\ n_H(t) &= a_H(t)\cos(2\pi f_n + \theta_H(t)), \end{aligned} \tag{9}$$

where $a_{V,H}$ and $\theta_{V,H}$ are the polarization dependent random Rayleigh-distributed amplitude and uniformly-distributed phase terms, respectively. The power of $n_V(t)$ and $n_H(t)$ is equal to their variance since they are zero-mean random variables and these are denoted as σ_V^2 and σ_H^2, respectively. We further assume that the powers of $\widehat{V}(t)$ and $\widehat{H}(t)$, both of which are zero-mean band-limited Gaussian processes, are the same, and each is denoted as σ_S^2. The corresponding SNR values at the output of vertical and horizontal polarized antennas are σ_S^2/σ_V^2 and σ_S^2/σ_H^2, respectively, and are denoted as SNR_V and SNR_H. In reality, the bandwidth of $V(t)$ is slightly greater than that of $H(t)$ due to the modulation $m(t)$ induced on it. However, the bandwidth of $m(t)$ is very small compared with $H(t)$. We assume that the signal bandwidth of $V(t)$ and $H(t)$ (hence the bandwidth of $\widehat{V}(t)$ and $\widehat{H}(t)$) is B_S, and that the bandwidth of $n_V(t)$ and $n_H(t)$ is B_n (equal to the receive antenna bandwidth). Usually, B_S is almost the same as B_n in order to avoid receiving additional interference.

Down the receiver chain, the noisy signals $\widetilde{V}(t-t_1) = \widetilde{V}(t)$ and $\widetilde{H}(t)$ are mixed together, and the mixed signal $S(t)$ contains the desired signal term $\widehat{V}(t)\widehat{H}(t)$ (first term below) and three interference cross-terms given by

$$S(t) = \widehat{V}(t)\widehat{H}(t) + n_V(t)\widehat{H}(t) + n_H(t)\widehat{V}(t) + n_V(t)n_H(t). \tag{10}$$

In the real system implementation, the bandpass filter is used to capture just the sum frequency signal centered at f_c (3 GHz) containing the information message, while discarding all difference frequency signals contained in $S(t)$ is discarded as noise. Let $\text{BPF}(x(t))$ denote the bandpass filtered output of the signal $x(t)$. The bandpass filtered noise signals are denoted as $n_1(t)$, $n_2(t)$, and $n_3(t)$, where $n_1(t) = \text{BPF}(n_V(t)\widehat{H}(t))$, $n_2(t) = \text{BPF}(n_H(t)\widehat{V}(t))$, and $n_3(t) = \text{BPF}(n_H(t)n_V(t))$. Generally, the probability density function of the noise needs to be found in order to calculate the BER. Since the probability density function of the product of two independent zero-mean normal distributions is approximated by a modified Bessel function of the second kind, the closed form probability density function for the sum $n_1(t) + n_2(t) + n_3(t)$ is extremely difficult to derive. Because the bandwidth of filtered noise is much smaller than before filtering, the noise spectrum following the filter is relatively flat compared to the sum frequency noise. Thus, we can approximate the filtered noise as a Gaussian variable. For convenience, we assume that the bandwidth of the bandpass filter is twice that of the low-pass filter following the second down-conversion, since the low-pass filter is the key component dominating the received noise spectrum before the decision circuit. Later in this section, we will compare the theoretical results with simulation results to show that our derivation by applying this assumption also works when the bandwidth of bandpass filter is much greater than bandwidth of low-pass filter.

Based on our simulation analysis, a cumulative distribution function comparison between $n_1(t)$ (a representative interference term) and a zero-mean band-limited Gaussian with the same power and frequency range is shown in Figure 4. In the simulation, the bandwidth of bandpass filter is 40 MHz ($B_L = 20$ MHz), the bandwidth of signal B_S is 970 MHz, and the bandwidth of the channel noise B_n is 980 MHz. We note that the two cumulative distribution function plots are very close. Thus, these results validate our assumption that the filtered sum frequency noise terms can be approximated as Gaussian.

After realizing that the filtered noise terms can be approximated as Gaussians, their means and variances need to be found for calculating the BER. The mean value of $n_1(t)$ is found as zero, as seen from

$$\begin{aligned} E[n_1(t)] &= E\left[\int_{-\infty}^{\infty} h(\tau)n_V(t-\tau)H(t-\tau)d\tau\right] \\ &= \int_{-\infty}^{\infty} h(\tau)E[n_V(t-\tau)]E[H(t-\tau)]d\tau \\ &= 0, \end{aligned} \tag{11}$$

where $h(\tau)$ is impulse response of bandpass filter [19]. Similarly, the mean values of $n_2(t)$ and $n_3(t)$ are both zero.

The next step is to calculate the variance of the filtered noise, which is equal to its power. Clearly, the power of $n_1(t)$, $n_2(t)$, and $n_3(t)$ can be calculated by integrating the power spectrum of the sum frequency noise of $n_V(t)\widehat{H}(t)$, $n_H(t)\widehat{V}(t)$, and $n_V(t)n_H(t)$ within the bandpass filter frequency range.

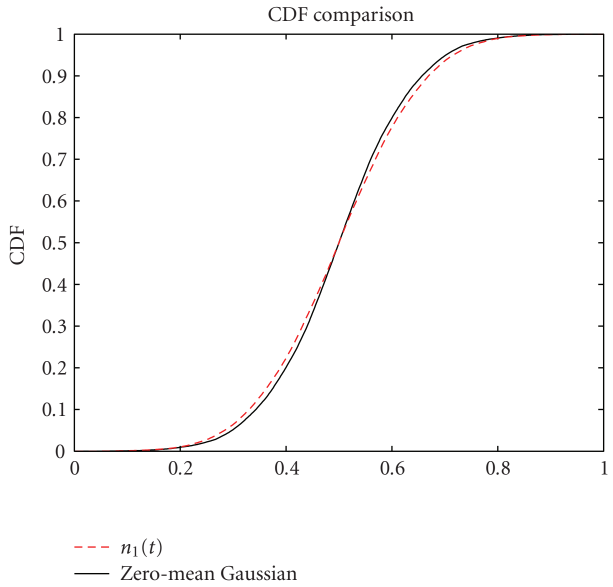


Figure 4: Cumulative distribution function comparison between zero-mean Gaussian and bandpass filtered noise term.

Let the power spectral density of the sum frequency noise of $n_V(t)\widehat{H}(t)$ be denoted as $S_{n_V\widehat{H}}(f)$. The average power of the sum frequency noise needs to be found first in order to find the mathematical expression for $S_{n_V\widehat{H}}(f)$. We know that for a given ergodic random process $x(t)$, its autocorrelation function $R_{xx}(\tau)$ and its power spectral density $S_x(f)$ form a Fourier transform pair, that is, $R_{xx}(\tau) \leftrightarrow S_x(f)$. Furthermore, the average power of such a random process is the value of the autocorrelation function at zero lag, that is, equal to $R_{xx}(0)$.

The sum frequency noise of $n_V(t)\widehat{H}(t)$, noting that $t_1 = 0$, can be expressed as

$$N_1(t) = 0.5a(t)a_V(t)\cos\left(2\pi f_c + \theta_V(t) + \theta(t)\right). \tag{12}$$

The average power of $N_1(t)$ can be determined from its autocorrelation function with the lag τ set equal to zero and can be expressed as

$$\begin{aligned} P_S &= E\left[\left(0.5a(t)a_V(t)\cos(2\pi f_c t + \theta(t) + \theta_V(t))\right)^2\right] \\ &= 0.125E\left[a^2(t)a_V^2(t)\cos\left(4\pi f_c t + 2\theta(t) + 2\theta_V(t)\right)\right] \\ &\quad + 0.125E\left[a^2(t)a_V^2(t)\right] \\ &= 0.125E\left[a^2(t)\right]E\left[a_V^2(t)\right]. \end{aligned} \tag{13}$$

Recognizing that $a(t)$ and $a_V(t)$ are independent Rayleigh distributed random variables. Furthermore, the kth moment of a Rayleigh distributed random variable x is noted as [19]

$$E[x^k] = \begin{cases} 1\cdot 3\cdots k\sigma^k\sqrt{\dfrac{\pi}{2}}, & k = 2n+1, \\ 2^n n!\sigma^{2n}, & k = 2n, \end{cases} \tag{14}$$

where $\sqrt{\pi\sigma^2/2}$ is the mean. For $k = 2$, that is, $n = 1$, we have $E[a^2(t)] = 2\sigma_S^2$ and $E[a_V^2(t)] = 2\sigma_V^2$. We therefore have

$$P_S = 0.5\sigma_S^2\sigma_V^2. \tag{15}$$

Thus, the value of the corresponding power spectral density of the sum frequency noise $S_{n_V\hat{H}}(f)$ integrated over frequency is $0.5\sigma_S^2\sigma_V^2$. Since the sum frequency noise $n_V(t)\hat{H}(t)$ is the product of two band-limited rectangular spectra centered at $f_n = f_c/2$ with bandwidths B_n and B_S ($B_S \approx B_n$), respectively, $S_{n_V,\hat{H}}(f)$ has an isosceles triangle shape centered also at f_c with an overall bandwidth equal to $B_n + B_S$. Therefore, $S_{n_V,\hat{H}}(f)$ can be expressed as

$$S_{n_V,\hat{H}}(f) = \begin{cases} \dfrac{-2\sigma_V^2\sigma_S^2\,|f - f_c|}{(B_n + B_S)^2} + \dfrac{\sigma_V^2\sigma_S^2}{B_n + B_S}, & f_c - 0.5(B_n + B_S) \leq f \\ & \leq f_c + 0.5(B_n + B_S), \\ 0, & \text{otherwise.} \end{cases} \tag{16}$$

The power of $n_1(t)$ contained within the low-pass filter bandwidth B_L can be finally found from

$$P_{n1} = \int_{f_c-B_L}^{f_c+B_L} S_{n_V,\hat{H}}(f)df = 0.5G_1\sigma_S^2\sigma_V^2, \tag{17}$$

where G_1 is given by

$$G_1 = \left(1 - \left(1 - \frac{2B_L}{B_n + B_S}\right)^2\right). \tag{18}$$

In a similar manner, $n_2(t)$ and $n_3(t)$ can be derived as $0.5G_1\sigma_S^2\sigma_H^2$ and $0.5G_2\sigma_V^2\sigma_H^2$, respectively, where G_2 is given by

$$G_2 = \left(1 - \left(1 - \frac{B_L}{B_n}\right)^2\right). \tag{19}$$

The summation of $n_1(t)$, $n_2(t)$, and $n_3(t)$, representing the total interference component, is also a zero-mean band-limited Gaussian random variable and we denote it as $n(t)$. The variance of $n(t)$ is equal to its average power and is given by

$$\begin{aligned} \operatorname{var}(n) = {} & \operatorname{var}(n_1) + \operatorname{var}(n_2) + \operatorname{var}(n_3) + \operatorname{cov}(n_1, n_2) \\ & + \operatorname{cov}(n_1, n_3) + \operatorname{cov}(n_2, n_3). \end{aligned} \tag{20}$$

Since $n_1(t)$, $n_2(t)$, and $n_3(t)$ are uncorrelated zero-mean Gaussian distributions, the covariance terms are zero, and therefore, the interference power is obtained as

$$\operatorname{var}(n) = 0.5(G_1\sigma_S^2\sigma_V^2 + G_1\sigma_S^2\sigma_H^2 + G_2\sigma_V^2\sigma_H^2). \tag{21}$$

The $n(t)$ term is mixed with the 3-GHz carrier and down to the baseband with a power that is equal to $0.125(G_1\sigma_S^2\sigma_V^2 + G_1\sigma_S^2\sigma_H^2 + G_2\sigma_V^2\sigma_H^2)$. Since the baseband noise is zero-mean Gaussian and binary modulation is used, the BER equation for the optimal receiver can be expressed by the Q-function with two parameters: the spectrum magnitude of the noise (N_0) and the bit energy (E_b) [20, 21].

From (7), when there is no low-pass filter truncating the signal spectrum, the average power of received baseband signal can be found using the fourth moment of $a(t)$ and is shown to be

$$P_b \approx E\{(0.25a^2(t))^2\} = 0.5\sigma_S^4. \tag{22}$$

Since the $a^2(t)$ term in (7) will spread out the baseband signal power over a frequency range wider than the low-pass filter bandwidth, the low-pass filter at the receiver will truncate the signal spectrum, and the received power will be lower than the value obtained in (22). Therefore, the bit energy at the output of low-pass filter can be expressed as $0.5\rho\sigma_S^4T_b$ when bit duration time is T_b. The ρ is the power loss factor due to the filtering, defined as the ratio between the truncated baseband signal power after the low-pass filter to the untruncated baseband signal. Clearly, the loss factor satisfies $0 \leq \rho \leq 1$. From above discussion, the BER of the noise modulated covert communication system with a two-sided spectrum can be mathematically expressed as

$$P_e = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) = Q\left(\sqrt{\frac{8\rho\sigma_S^4T_bB_L}{G_1\sigma_S^2\sigma_V^2 + G_1\sigma_S^2\sigma_H^2 + G_2\sigma_V^2\sigma_H^2}}\right). \tag{23}$$

The well-known $Q(x)$ function is shown below for reference as

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-y^2/2}dy. \tag{24}$$

Equation (23) can be also expressed using SNR_V and SNR_H as follows:

$$P_e = Q\left(\sqrt{\frac{8\rho T_bB_L}{G_1\mathrm{SNR}_V^{-1} + G_1\mathrm{SNR}_H^{-1} + G_2\mathrm{SNR}_V^{-1}\mathrm{SNR}_H^{-1}}}\right). \tag{25}$$

A full system simulation in an additive white Gaussian noise channel was done to validate the theoretical results in (25), and the results are shown in Figures 5 and 6. In the simulation, both the SNR_V and the SNR_H terms are equal, and the bandwidth of the antenna is 10 MHz wider than the bandwidth of the transmitted signal in order to avoid truncation of the wider spectrum caused by the modulation. The bandpass filter has a bandwidth of 100 MHz and is centered at 3 GHz. In Figure 5, a low-pass filter bandwidth of 10 MHz is used for the simulation. The value of ρ depends on the bit rate and the low-pass filter bandwidth. From our independent simulation result, for a bit rate of 5 Mbps, the value of ρ was determined to be approximately 0.487 when the transmitted signal bandwidth is 970 MHz and approximately 0.5 when the transmitted signal bandwidth is 500 MHz. In Figure 6, the low-pass filter bandwidth is 20 MHz, and the signal bandwidth is 970 MHz bandwidth in the simulation. The value of ρ was determined to be 0.49, 0.5, and 0.518 when the bit rate is 10 Mbps, 5 Mbps, and 2 Mbps, respectively. From Figures 5 and 6, we note that the maximum deviation between the simulation results and theoretical results is 0.5 dB. Thus, the system behavior of this ultrawideband communication system is properly modeled. As the bandwidth of $V(t)$ and $H(t)$ is increased, the noise power will be dispersed into larger frequency ranges after the mixing process, and the system performance will improve because the processing gain will increase.

4. MULTIUSER MODELING

In a multiuser environment, each user uses the same channel but is assigned a different delay. The receiver contains a switchable delay bank between the vertical polarization antenna and the first mixer to select a particular user. If σ_i^2 is the signal power of $\hat{V}_i(t)$ and $\hat{H}_i(t)$ corresponding to the ith user, the received signals in the vertically and horizontally polarized antennas in an additive white Gaussian noise channel are given by

$$\widetilde{V}_N(t) = \sum_{i=1}^{N} \hat{V}_i(t) + n_V(t), \tag{26}$$

$$\widetilde{H}_N(t) = \sum_{i=1}^{N} \hat{H}_i(t - t_i) + n_H(t), \tag{27}$$

when there are N users in the channel. The t_i term in (27) is the specific delay time assigned to the ith user, and the receiver already knows this information. Since the output signals of different noise generators are independent of each other, the $\hat{V}_i(t)$ terms are independent to each other and so are the $\hat{H}_i(t)$ terms.

For any user who wants to receive the message from the ith user, the delay line with the delay t_i between vertical polarization antenna and the first mixer in the receiver is activated. Then, the signal at the output of the first mixer can be written as

$$\begin{aligned} S_N(t) = {} & \hat{V}_i(t-t_i)\hat{H}_i(t-t_i) + \sum_{n=1}^{N}\sum_{m=1}^{N} \hat{V}_m(t-t_i)\hat{H}_n(t-t_n) \\ & + \sum_{m=1}^{N} \left(\hat{V}_m(t-t_i)n_H(t) + \hat{H}_m(t-t_m)n_V(t-t_i)\right) \\ & + n_V(t-t_i)n_H(t), \quad (m,n) \neq (i,i). \end{aligned} \tag{28}$$

The second term in (28) can be considered as interference and its characteristics are similar to the third and fourth terms when the difference between each t_i term is large enough. Thus, the sum frequency signal in (28) contains $N^2 - 1$ interference terms with bandwidth $2B_S$, $2N$ interference terms with bandwidth $B_S + B_n$, and one interference term with bandwidth $2B_n$. All the interference terms are centered at f_c. Using the same method that was used to derive the BER for the single-user environment, the BER equation for N users in the additive white Gaussian noise channel can be mathematically expressed as

$$P_e = Q\left(\sqrt{\frac{8\rho\sigma_i^4 T_b B_L}{\mathcal{H}}}\right), \quad (m,n) \neq (i,i), \tag{29}$$

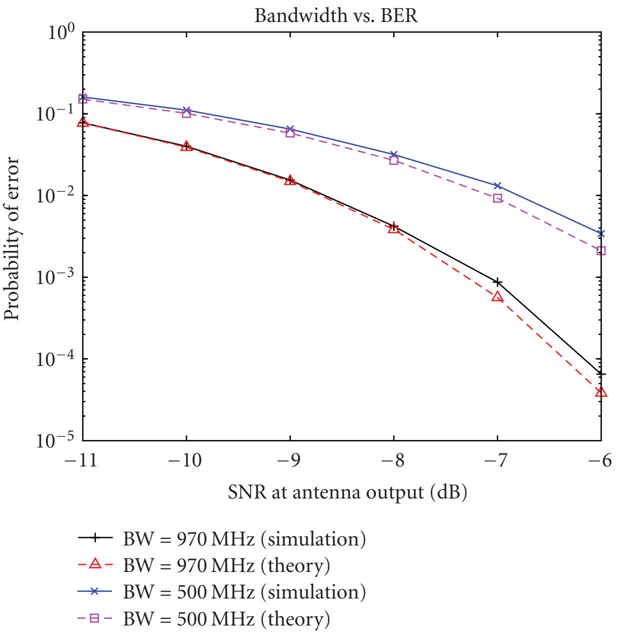


FIGURE 5: Comparison of SNR and BER characteristics between simulation and theory in a single user environment at different signal bandwidths.

where

$$\mathcal{H} = G_3 \sum_{n=1}^{N}\sum_{m=1}^{N} \sigma_n^2\sigma_m^2 + G_1 \sum_{m=1}^{N} \left(\sigma_m^2\sigma_H^2 + \sigma_m^2\sigma_V^2\right) + G_2\sigma_V^2\sigma_H^2. \tag{30}$$

The G_1 and G_2 terms are shown in (18) and (19), respectively, and G_3 is given by

$$G_3 = \left(1 - \left(1 - \frac{B_L}{B_S}\right)^2\right). \tag{31}$$

In our simulation, we assume that each user has the same power, in which case, (29) reduces to

$$P_e = Q\left(\sqrt{\mathcal{Z}}\right), \tag{32}$$

where

$$\mathcal{Z} = \frac{8\rho\sigma_S^4 T_b B_L}{\left((N^2-1)G_3\sigma_S^4 + G_1 N\left(\sigma_S^2\sigma_H^2 + \sigma_S^2\sigma_V^2\right) + G_2\sigma_V^2\sigma_H^2\right)}. \tag{33}$$

The bit rate is 5 Mbps, and the bandwidth of antenna and the signal is 980 MHz and 970 MHz, respectively. The simulation results are shown in Figure 7 from which we note that the deviation between the simulation results and theoretical results is less than 0.5 dB. As the number of users increases, the noise floor also increases and the BER degrades.

5. COMPREHENSIVE EXPERIMENTAL RESULTS

As a test of the noise modulated covert communication system functionality, comprehensive tests were performed.

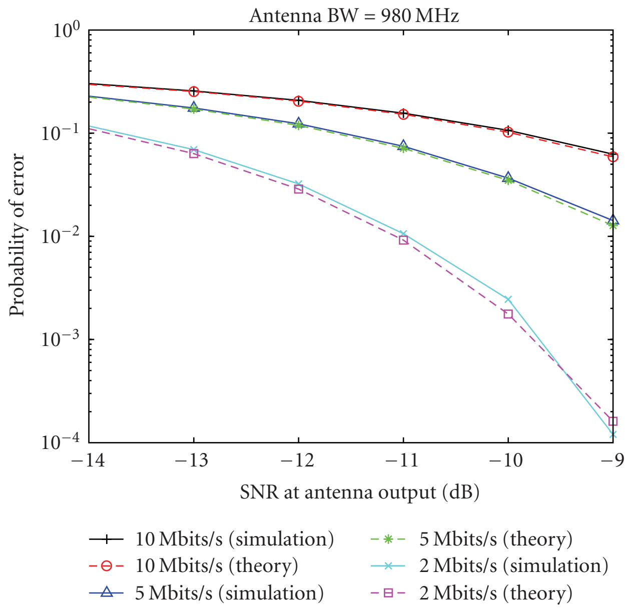


Figure 6: Comparison of SNR and BER characteristics between simulation and theory in a single user environment at different bit rates.

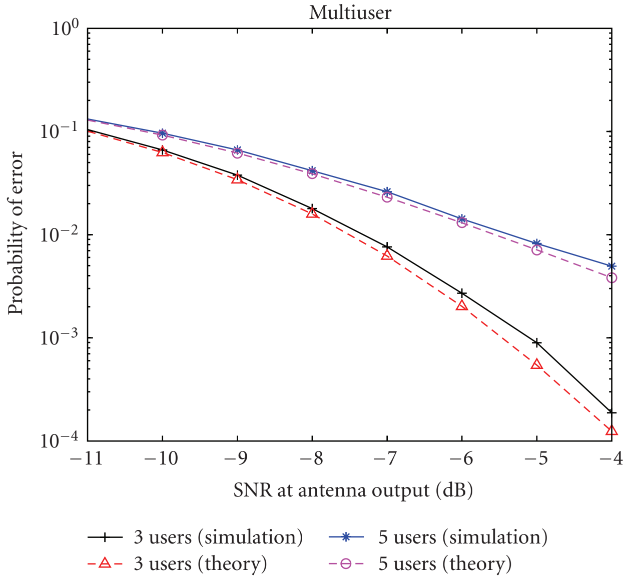


Figure 7: Comparison of SNR and BER characteristics between theory and simulation in a multiuser environment.

A Lyrtech field programmable gate array board samples the audio wave and translates it into binary bit stream. This bit stream is interpreted as +/– voltage by the digital to analog converter and is mixed with a 3-GHz carrier as radio frequency modulated signal. At the transmitter, a 1-2-GHz noise source is used. The noise source is connected to a 1.2–1.8-GHz bandpass filter and then to a power divider. The RF modulated signal and filtered noise are sent to a single sideband up-converter, and then the lower sideband is chosen as the transmitted signal in the vertical channel. The antennas used at the transmitter and receiver are dual linear horn antennas. At the receiver side, the 40-dB gain limiting-amplifiers are connected after the antennas in order to drive the mixer in the square-low region. A 2.9–3.1-GHz bandpass filter and two 14-dB gain amplifiers are connected after the mixer at the receiver. The output of the amplifier is connected to the second mixer, and then to a 1.9-MHz bandwidth low-pass filter. The low-pass filter is connected to another Lyrtech board, and the audio is recovered. In the experiment, the system is placed in the open field with grass terrain and the distance between the transmitter and receiver is 30 meters. An additional 10-dB attenuator is added to imitate a distance of 94 meters. Since the carrier synchronization loop is not built in the receiver, an Agilent E4438C vector signal generator is used as a common frequency source. The experimental setup and system implementation are shown in Figure 8.

All the baseband signal processing is implemented on Lyrtech SignalWAVe DSP/FPGA development boards. Using Xilinx ISE 7.0 and the Xilinx and Lyrtech blocksets, the baseband signal processing was designed in the Simulink environment and then loaded into the Lyrtech board. The transmitter design is shown in Figure 9(a). An audio signal is sampled by the audio codec with sample frequency approximately equal to 3.85 kHz and then quantized into a 14-bit frame. The 14-bit header [1,0,1,1,1,0,1,0,1,0,0,0,0] is inserted between every 7000 data frames and then the bit stream with the header is sent to the digital-to-analog converter where bit-1 and bit-0 are represented as +/– voltages. The receiver baseband signal processing design is shown in Figure 9(b). At the output of the low-pass filter, hard decisions are made by taking the sign (output 1 or −1) of the incoming samples. The resulting sequence is passed through the framing and timing synchronization circuits to ensure that the serial to parallel block is activated at the proper times and then the received data frame is transformed back into the original sample values and the audio can be recovered.

At the receiver side, the received signals at the output of vertical polarization antenna and horizontal polarization antenna are at power levels of −56 dBm and −57 dBm, respectively. The Agilent DSO-80804B oscilloscope is used to record the received $V(t)$, a plot of which is shown in Figure 10. Our signal does show random behavior in the time domain and flat spectrum in the frequency domain. The spectrum is not perfectly flat because the conversion loss of the single sideband up-converter is not entirely constant over the 1.2–1.8-GHz band. The peaks around 900 MHz and 1900 MHz are caused by the cell phone signals, and the one around 1900 MHz is considered as interference because it will generate extra interference terms after the mixing process.

In the field test, the audio could be heard with good quality. Due to the unknown and uncertain delay caused by wiring and the propagation channel, it is difficult to directly compare the input and the output audio waveforms. By properly modifying the baseband signal processing design, the system will send a header continuously with a bit rate of

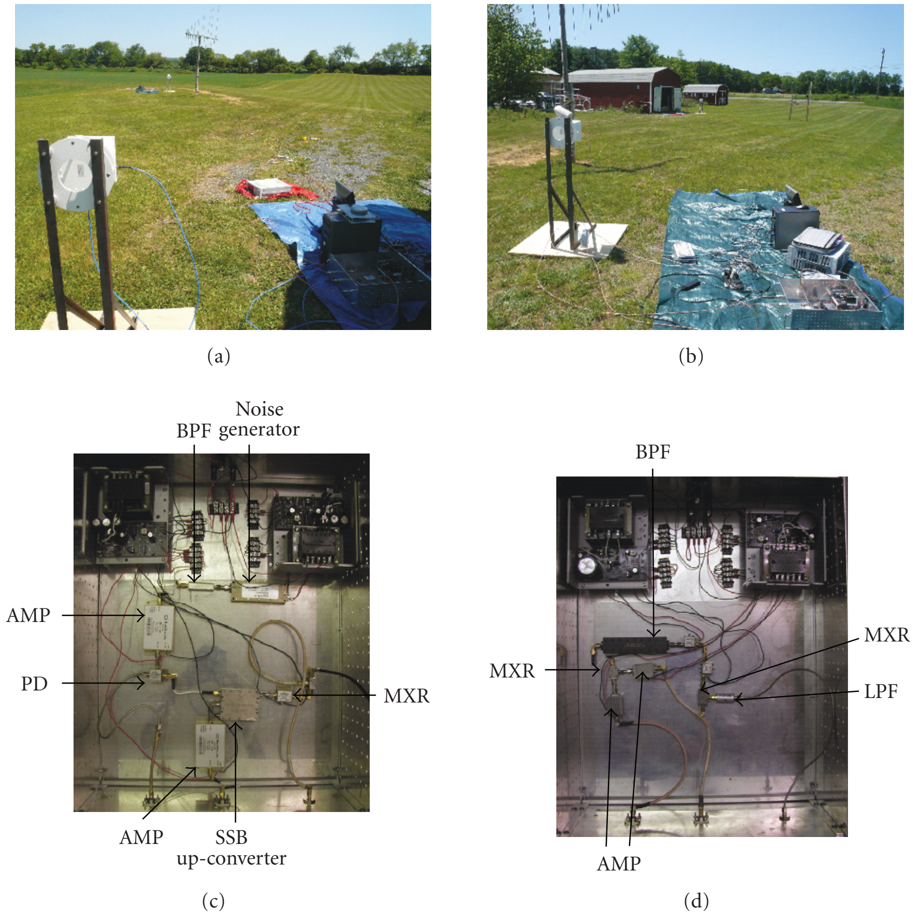


Figure 8: (a) Transmitter view, (b) receiver view, (c) transmitter and (d) receiver layout.

approximately 110 Kbps. Thus, we can compare the sent and received bit streams in an ideal channel and a noisy channel. Figure 11 shows the transmitted bit stream (a) and the received bit stream (b) in the ideal channel. The waveform is recorded by the Agilent DSO-80804B oscilloscope at the output of the low-pass filter. We note that the ideal channel amplitude fluctuations, caused by the random $a^2(t)$ term, will not affect the decision for binary modulation. Figure 11 also shows the same bit stream being received in an additive white Gaussian noise channel (c) and a channel containing tone interference (d).

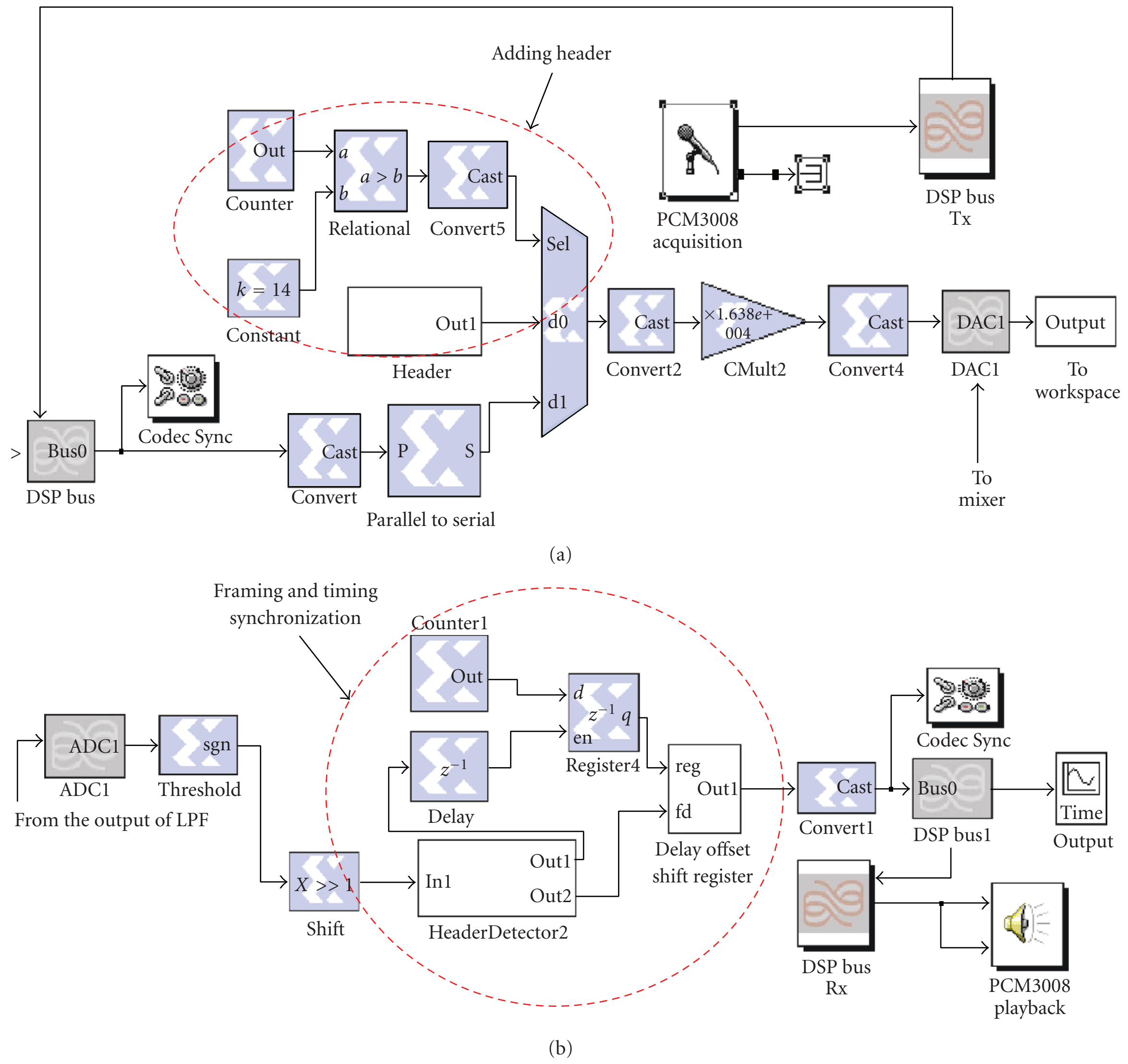
The zero crossings show up when the channel is not clean but the message can still be retrieved. Although not shown, when both tone interferences are located within the narrow frequency range ($0.5f_c - B_L < f < 0.5f_c + B_L$) in the low-SIR channel, the bit stream is ruined because of high-power tone interference at the output of low-pass filter generated by the sum frequency signal of the tone interference in the V-channel mixed with the tone interference in H-channel. Usually, this problem can be solved by adding a digital filter in the baseband signal processing design.

In practice, polarization mismatch may occur between transmitter and receiver antennas and this is an important factor that will affect system performance. When the antennas at either end are not perfectly aligned, there will exist a rotation angle between the antenna axes at either end. Thus, each polarization channel at the receiver side not only receives the desired received signal but also the leakage from the orthogonal polarization component. The signals that send from V-channel and H-channel to the first mixer at the receiver side can then be expressed as

$$\begin{aligned}\widetilde{V}(t) &= \alpha\widehat{V}(t-t_1) + \beta\widehat{H}(t-2t_1) + n_V(t-t_1),\\ \widetilde{H}(t) &= \alpha\widehat{H}(t-t_1) + \beta\widehat{V}(t) + n_H(t),\end{aligned} \tag{34}$$

where t_1 is the delay time of the delay line ($t_1 \gg B_S^{-1}$ in the system implementation), $\beta\widehat{H}(t-2t_1)$ is the received leakage from the transmit H-channel into the receive V-channel, and $\beta\widehat{V}(t)$ is the received leakage from the transmit V-channel into the received H-channel. The terms α and β are the square root of polarization loss factor with value depending on the rotation angle. They are within the range $[0, 1]$ and $\alpha^2 + \beta^2 = 1$ [22]. For perfect antenna alignment, $\alpha = 1$ and $\beta = 0$, and there is no polarization leakage.

As the rotation angle increases, the value of β increases while the value of α decreases. When the rotation angle is 45 degrees, $\alpha = \beta = \sqrt{0.5}$. The worst case occurs at a rotation angle of 90 degrees because the power of desired received signal is zero and no message can be extracted from the



(a)

(b)

Figure 9: (a) Transmitter baseband signal processing design, (b) receiver baseband signal processing design.

received signal ($\alpha = 0$, $\beta = 1$). The BER equation upon considering nonperfect alignment in a Gaussian channel can be expressed as

$$P_e = Q\left(\sqrt{\frac{8\rho\alpha^4\sigma_S^4 T_b B_L}{G_3\left(2\alpha^2\beta^2+\beta^4\right)\sigma_S^4 + \mathcal{Y} + G_2\sigma_V^2\sigma_H^2}}\right), \qquad (35)$$

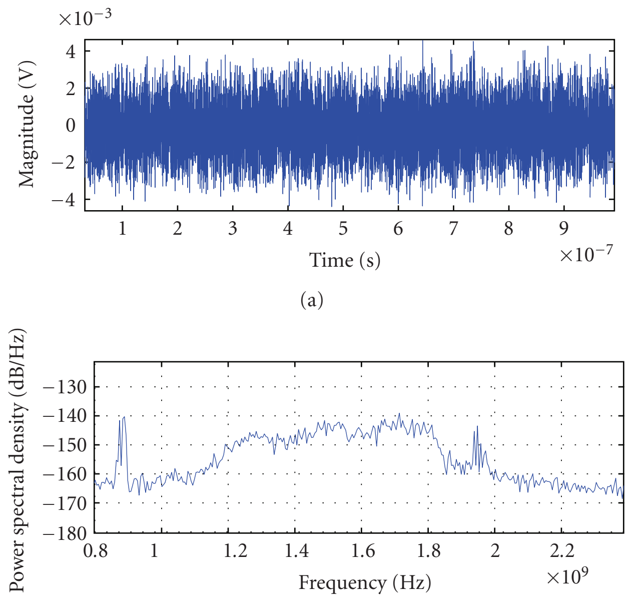
where

$$\mathcal{Y} = G_1\left(\alpha^2+\beta^2\right)\left(\sigma_S^2\sigma_H^2+\sigma_S^2\sigma_V^2\right), \qquad (36)$$

and G_1, G_2, G_3 are as shown in (18), (19), and (31). Comparing (35) with (23), nonperfect antenna alignment will degrade system performance because it generates extra interference terms and decreases the power of desired received signal. A method for measuring the rotation angle is to send a pilot tone from one of the dual-polarization channels and use the power ratio between received V-channel signal and received H-channel signal to determine the rotation angle. To simplify the structure, better estimation technique should be developed for measuring rotation angle without using a pilot.

6. CONCLUSIONS

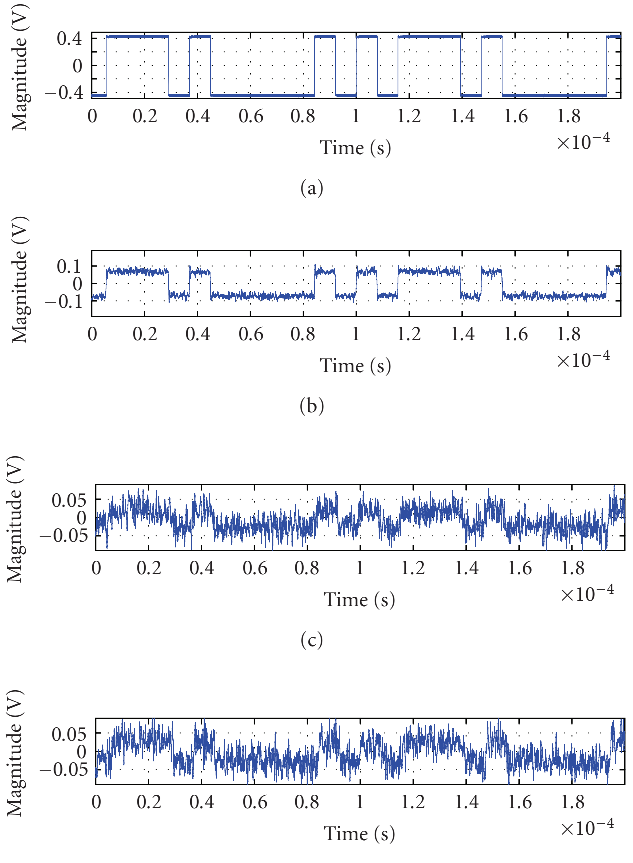
A spread spectrum technique using noise-modulated waveforms is proposed for covert communications. The featureless characteristics of the transmitted waveform in the noise modulated covert communication system ensure the security of communications. By using a band-limited true Gaussian noise waveform to spread the signal's power into a large bandwidth, an extremely large processing gain is achieved and the system can operate very well in a low SNR or SIR channel. Based on our current research, the “cross-multiplication” method could alleviate performance degradation caused by multipath. The underlying concept



(a)

(b)

Figure 10: (a) Recorded time domain of received $V(t)$, (b) recorded frequency domain of received $V(t)$.



(a)

(b)

(c)

(d)

Figure 11: (a) Original transmitted bit stream, (b) bit stream received in ideal channel, (c) bit stream received in additive white Gaussian noise channel, (d) bit stream received in single-tone interference channel.

of this method is to synchronize the nth path in the V-channel with the mth path in the H-channel instead of directly synchronizing the received V-channel and H-channel signals. Without considering system complexity, combining a pseudonoise sequence with our method can show better performance than a RAKE receiver since more diversity can be used. For example, if each channel contains N multipath terms, there are N diversity that can be used by the RAKE receiver but N^2 diversity can be used by our method.

The performance of this noise modulated covert communication system in a single and multiuser environment is properly modeled and compared with simulations. The bandwidth of the transmitted signal and antenna controls the BER performance when the SNR at the output of antenna and bit rate is fixed. The field tests demonstrate that the concept can be realized, and the system can operate in an additive white Gaussian noise channel with negative SNR.

ACKNOWLEDGMENTS

This work is supported by the Office of Naval Research (ONR) under Contract no. N00014-04-1-0640. The authors appreciate fruitful discussions with Mr. John Moniz and Mr. Timothy Wasilition of ONR. They thank Dr. Sven Bilen of The Pennsylvania State University for supplying the two-field programmable gate array boards for the experiments. Moreover, they also thank Star-H Corporation, Pa, USA , for providing the location for the field tests and Arhan Gunel, Keith Newlander, and Paul Bucci for their help in the field testing.

REFERENCES

[1] C. E. Cook and H. S. Marsh, "An introduction to spread spectrum," *IEEE Communications Magazine*, vol. 21, no. 2, pp. 8–16, 1983.

[2] R. A. Scholtz, "The origins of spread-spectrum communications," *IEEE Transactions on Communications*, vol. 30, no. 5, part 2, pp. 822–854, 1982.

[3] P. C. J. Hill, V. E. Comley, and E. R. Adams, "Techniques for detecting and characterizing covert communication signals," in *Proceedings of the IEEE Military Communications Conference (MILCOM '97)*, vol. 3, pp. 1361–1365, Monterey, Calif, USA, November 1997.

[4] M. Gouda, E. R. Adams, and P. C. J. Hill, "Detection & discrimination of covert DS/SS signals using triple correlation," in *Proceedings of the 15th National Radio Science Conference (NRSC '98)*, pp. C35/1–C35/6, Cairo, Egypt, February 1998.

[5] G. Burel, "Detection of spread spectrum transmissions using fluctuations of correlation estimators," in *Proceedings of the IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS '00)*, pp. 1–6, Honolulu, Hawaii, USA, November 2000.

[6] N. C. Beaulieu, W. L. Hopkins, and P. J. McLane, "Interception of frequency-hopped spread-spectrum signals," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 5, pp. 853–870, 1990.

[7] G. R. Cooper and L. H. Cooper, "Covert communication with a purely random spreading function," in *Proceedings of the IEEE Military Communications Conference (MILCOM '82)*, pp. 2.4-1–2.4-2, Boston, Mass, USA, October 1982.

[8] L. Turner, "The evolution of featureless waveforms for LPI communications," in *Proceedings of the IEEE National Aerospace and Electronics Conference (NAECON '91)*, vol. 3, pp. 1325–1331, Dayton, Ohio, USA, May 1991.

[9] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Transactions on Circuits and Systems II*, vol. 40, no. 10, pp. 626–633, 1993.

[10] C. K. Rushforth, "Transmitted-reference techniques for random or unknown channels," *IEEE Transactions on Information Theory*, vol. 10, no. 1, pp. 39–42, 1964.

[11] R. M. Gagliardi, "A geometrical study of transmitted reference communication systems," *IEEE Transactions on Communication Technology*, vol. 12, no. 4, pp. 118–123, 1964.

[12] M.-H. Chung and R. A. Scholtz, "Comparison of transmitted- and stored-reference systems for ultrawideband communications," in *Proceedings of the IEEE Military Communications Conference (MILCOM '04)*, vol. 1, pp. 521–527, Monterey, Calif, USA, October-November 2004.

[13] T. Q. S. Quek and M. Z. Win, "Analysis of UWB transmitted-reference communication systems in dense multipath channels," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 9, pp. 1863–1874, 2005.

[14] T. Q. S. Quek, M. Z. Win, and D. Dardari, "Unified analysis of UWB transmitted-reference schemes in the presence of narrowband interference," *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2126–2139, 2007.

[15] R. M. Narayanan and J. Chuang, "Covert communications using heterodyne correlation random noise signals," *Electronics Letters*, vol. 43, no. 22, pp. 1211–1212, 2007.

[16] J. Chuang, M. W. DeMay, and R. M. Narayanan, "Secure spread spectrum communication using ultrawideband random noise signals," in *Proceedings of the IEEE Military Communications Conference (MILCOM '07)*, pp. 1–7, Washington, DC, USA, October 2007.

[17] M. Dawood and R. M. Narayanan, "Receiver operating characteristics for the coherent UWB random noise radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 37, no. 2, pp. 586–594, 2001.

[18] K. M. Mohan, *Covert communication system using random noise signals: propagation and multipath effects*, M.S. thesis, The Pennsylvania State University, University Park, Pa, USA, December 2005.

[19] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*, McGraw-Hill, New York, NY, USA, 4th edition, 2002.

[20] R. L. Peterson, R. E. Ziemer, and D. E. Borth, *Introduction to Spread Spectrum Communications*, Prentice-Hall, Upper Saddle River, NJ, USA, 1995.

[21] G. K. Kaleh, "Frequency-diversity spread spectrum communication system to counter bandlimited Gaussian interference," *IEEE Transactions on Communications*, vol. 44, no. 7, pp. 886–893, 1996.

[22] C. A. Balanis, *Antenna Theory: Analysis and Design*, John Wiley & Sons, New York, NY, USA, 3rd edition, 2005.