Robust CDMA Receiver Design under Disguised Jamming

Kai Zhou Tianlong Song Jian Ren Tongtong Li
Dept. of Electrical & Computer Engineering, Michigan State University
East Lansing, MI 48824, USA
Email: {zhoukai, songtia6}@msu.edu, {renjian, tongli}@egr.msu.edu

***Abstract*—This paper considers robust CDMA receiver design and jamming evaluation under disguised jamming, where the jammer generates a fake signal using the same spreading code, constellation and pulse shaping filter as that of the authorized signal. *First*, we analyze the performance of conventional CDMA systems under disguised jamming, and show that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. *Second*, by exploiting the small time difference between the authorized signal and the jamming interference, the conventional CDMA receiver can be re-designed to achieve robust performance under disguised jamming. More specifically, we propose to estimate the authorized signal, the phase and power level or range of the jamming interference by minimizing the MSE between the received signal and the jammed signal, which is the sum of the authorized signal and the disguised jamming. The effectiveness of the proposed approach is demonstrated through simulation examples. It is shown that with the proposed receiver design, the BER performance of CDMA can be improved significantly under disguised jamming, and an analytical evaluation about jamming can also be obtained.**

***Index Terms*—CDMA, disguised jamming, receiver design, MMSE.**

I. Introduction

Existing work on anti-jamming system design or jamming mitigation is mainly based on spread spectrum techniques [1], [2]. The spread spectrum systems, including code division multiple access (CDMA) and frequency hopping (FH), were originally developed for secure communications in military applications. Both CDMA and FH systems possess anti-jamming and anti-interception features by exploiting frequency diversity over large spectrum.

In CDMA, each user is assigned a specific pseudo-random code (also known as the signature) to spread its signal over a bandwidth N times larger. Due to the processing gain resulted from the spread spectrum technique, CDMA is especially robust under narrow band jamming and works very well under low SNR levels [3]. CDMA signals cannot be recovered unless the user signature is known at the receiver, and can be hidden within the noise floor, making it difficult to be detected. For these reasons, CDMA has been widely used in both civilian and military applications, such as 3GPP UMTS [4] and GPS [5].

The security of CDMA largely relies on the randomness in the PN sequence. For CDMA, the spreading code of each user is obtained through the modulo 2 sum of the Walsh code and the long code, and thus is varying in every symbol period. However, according to the Berlekamp-Massey algorithm [6], for a sequence generated from an n-stage linear feedback shift register, the characteristic polynomial and the entire sequence can be reconstructed if an eavesdropper can intercept a $2n$-bit sequence segment. Note that the characteristic polynomial is generally available to the public, then PN sequence can be recovered if an n-bit sequence segment is intercepted. That is, it is possible to break the PN sequence used in conventional CDMA systems in real time with today's high speed computing techniques [7]. In civilian GPS systems, the spreading code is actually made public to attract potential users and improve its global competitiveness. Once the PN sequence is recovered or broken, the jammer can generate a fake signal using the same spreading code, constellation and pulse shaping filter as that of the authorized signal. This is known as the *disguised jamming* for CDMA.

In this paper, we first analyze the performance of conventional CDMA systems under disguised jamming, and show that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. Second, we observe that while malicious user can get complete information about the spreading code and pulse shaping filter, they cannot capture the exact timing information of the authorized signal. By exploiting this small time difference between the authorized signal and the jamming interference, the conventional CDMA receiver can be re-designed to achieve robust performance under disguised jamming. More specifically, we propose to estimate the authorized signal, the phase and power level or range of the jamming interference by minimizing the MSE between the received signal and the jammed signal, which is the sum of the authorized signal and the disguised jamming. The effectiveness of the proposed approach is demonstrated through simulation examples. It is shown that with the proposed receiver design, the BER performance of CDMA can be improved significantly under disguised jamming. At the same time, we can get a good evaluation on how severe the jamming is.

The rest of the paper is organized as follows. In Section II, the system model is provided. The impact of disguised jamming on CDMA systems is analyzed in Section III. The proposed CDMA receiver design under disguised jamming is elaborated in Section IV. Numerical evaluation is conducted in Section V and we conclude in Section VI.

II. System Model

We consider an individual user in a typical CDMA system. Assuming the processing gain is N, namely, there are N chips per symbol. Let $\mathbf{c} = [c_0, c_1, ..., c_{N-1}]$ denote the spreading code, which is assumed to be public. In the isolated pulse case, the general baseband signal can be represented as

$$c(t) = \sum_{n=0}^{N-1} c_n g(t - nT_c), \tag{1}$$

where $g(t)$ is the pulse shaping filter, T_c the time duration of the spreading code chip, and we assume

$$\frac{1}{T}\int_0^T c^2(t)dt = 1, \tag{2}$$

where $T = NT_c$. Let Ω be the constellation, and $a \in \Omega$ the symbol to be transmitted. The transmitted signal would then be

$$s(t) = ac(t). \tag{3}$$

Note that $c(t)$ is real, while a can be complex depending on the constellation Ω.

The signal, $s(t)$, is transmitted through an additive white Gaussian noise (AWGN) channel, and simultaneously interfered by disguised jamming. The disguised jamming is typically launched to confuse the receiver by generating a signal which mimics the authorized signal [8]–[10]. With complete knowledge of the spreading code and the pulse shaping filter, the disguised jamming would likely have similar characteristics as the authorized signal, except that the fake symbol can only be randomly chosen out of Ω, and the small timing and amplitude differences between the authorized signal and disguised jamming due to the non-ideal estimation at the jammer side. Let $b \in \Omega$ denote the fake symbol, τ the small timing difference, and γ the amplitude ratio of the disguised jamming to the authorized signal. Then, the disguised jamming can be modeled as

$$j(t) = b\gamma c(t-\tau). \tag{4}$$

Taking both the noise and the disguised jamming into account, the received signal can be written as

$$r(t) = s(t) + j(t) + n(t) = ac(t) + b\gamma c(t-\tau) + n(t), \tag{5}$$

where $n(t)$ is the noise.

III. Performance of Conventional CDMA Receivers under Disguised Jamming

In this section, we will show that: under the worst case disguised jamming, due to the symmetricity between the authorized signal and the jamming interference, the symbol error probability of CDMA communication is lower bounded, and the resulted capacity is proved to be zero.

A. Error Probability

The conventional CDMA receiver estimates the transmitted symbol as

$$\hat{a} = \frac{1}{T}\int_0^T r(t)c(t)dt. \tag{6}$$

However, this receiver would fail under disguised jamming. In fact, substituting (5) into (6), and following (2), we have

$$\hat{a} = a + b\gamma\frac{1}{T}\int_0^T c(t-\tau)c(t)dt + \frac{1}{T}\int_0^T n(t)c(t)dt. \tag{7}$$

It is observed that the symbol estimation would be considerably influenced by the second term in the RHS of (7), which is introduced by the disguised jamming, especially when τ is small (e.g., $|\tau| < T_c$) and $\gamma \approx 1$. In the worst case, when $\tau = 0$ and $\gamma = 1$, (7) can be simplified as

$$\hat{a} = a + b + \frac{1}{T}\int_0^T n(t)c(t)dt. \tag{8}$$

Resulting from (8), the symbol error probability under the worst disguised jamming, $\mathcal{P}_s$, would be lower bounded by

$$\mathcal{P}_s \geq \frac{M-1}{2M}, \tag{9}$$

where M is the constellation size. An intuitive explanation is that: if the authorized symbol a and the fake one b are distinct, the receiver would have to guess between them as indicated in (8). Note that the error probability of a random guess between two symbols is $\frac{1}{2}$, and the two symbols randomly and independently selected out of Ω by the authorized transmitter and disguised jammer differ with a probability of $\frac{M-1}{M}$. The additional noise would make the error probability even larger.

B. Capacity

In this subsection, we will show that the capacity of CDMA communication under the worst case disguised jamming is actually zero, by applying the arbitrarily varying channel (AVC) model [8], [11]–[17]. An AVC channel model is generally characterized using a kernel $W : \mathcal{S} \times \mathcal{J} \to \mathcal{Y}$, where $\mathcal{S}$ is the transmitted signal space, $\mathcal{J}$ is the jamming space (i.e., the jamming is viewed as the arbitrarily varying channel states) and $\mathcal{Y}$ is the estimated signal space. For any $\mathbf{s} \in \mathcal{S}$, $\mathbf{j} \in \mathcal{J}$ and $\mathbf{y} \in \mathcal{Y}$, $W(\mathbf{y}|\mathbf{s},\mathbf{j})$ denotes the conditional probability that $\mathbf{y}$ is detected at the receiver, given that $\mathbf{s}$ is the transmitted signal and $\mathbf{j}$ is the jamming. If $\mathcal{S} = \mathcal{J}$ and $W(\mathbf{y}|\mathbf{s},\mathbf{j}) = W(\mathbf{y}|\mathbf{j},\mathbf{s})$ for any $\mathbf{s},\mathbf{j} \in \mathcal{S}, \mathbf{y} \in \mathcal{Y}$, the AVC is said to have a symmetric kernel [13]. The deterministic code capacity[1] of an AVC for the average probability of error is zero if the AVC is symmetric [13], [17].

In an isolated symbol period of CDMA communication, the worst case disguised jamming in its chip-rate representation can be written as

$$\mathbf{j} = [bc_0, bc_1, ..., bc_{N-1}], \tag{10}$$

where $[c_0, c_1, ..., c_{N-1}]$ is the spreading code, and $b \in \Omega$ the fake symbol. The authorized signal can similarly be represented as

$$\mathbf{s} = [ac_0, ac_1, ..., ac_{N-1}], \tag{11}$$

where $a \in \Omega$ is the authorized symbol. Taking both the noise and jamming into account, the received chip-rate signal can be written as

$$\mathbf{r} = \mathbf{s} + \mathbf{j} + \mathbf{n}, \tag{12}$$

in which $\mathbf{n} = [n_0, n_1, ..., n_{N-1}]$ and $\mathbf{r} = [r_0, r_1, ..., r_{N-1}]$ denote the AWGN noise vector and received signal vector, respectively.

Define the authorized signal space as $\mathcal{S} = \{a\mathbf{c}|a \in \Omega\}$, where $\mathbf{c} = [c_0, c_1, ..., c_{N-1}]$ is the spreading code. It follows immediately that the disguised jamming space

$$\mathcal{J} = \{b\mathbf{c}|b \in \Omega\} = \mathcal{S}. \tag{13}$$

Let $\hat{a} \in \Omega$ be the estimated version of the authorized symbol a at the receiver, and $W_0(\hat{a}|\mathbf{s},\mathbf{j})$ the conditional probability that $\hat{a}$ is estimated given that the authorized signal is $\mathbf{s} \in \mathcal{S}$, and the disguised jamming is $\mathbf{j} \in \mathcal{S}$. Thus, the CDMA system under disguised jamming can be modeled as an AVC channel characterized by the probability matrix

$$W_0 : \mathcal{S} \times \mathcal{S} \to \Omega, \tag{14}$$

where W_0 is the kernel of the AVC.

As indicated in (13), the jamming and the authorized signal are fully symmetric as they are generated from exactly the same space $\mathcal{S}$. Note that the recovery of the authorized symbol is fully based on $\mathbf{r}$ in (12), so we further have

$$W_0(\hat{a}|\mathbf{s},\mathbf{j}) = W_0(\hat{a}|\mathbf{j},\mathbf{s}). \tag{15}$$

Combining (13) and (15), we conclude that: *under the worst case disguised jamming, the kernel of the AVC corresponding to a CDMA system, W_0, is symmetric, and hence the resulted deterministic capacity of the CDMA system is zero*. The underlying physical meaning is that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the

[1] A deterministic capacity is defined by the capacity that can be achieved by a communication system, when it applies only one code pattern during the information transmission. In other words, the coding scheme is deterministic and can be readily repeated by other users [13].

authorized signal from jamming, leading to complete communication failure.

Under the worst case disguised jamming (i.e., $\tau = 0$ and $\gamma = 1$), the lower bound in (9) sets up a limit for the error probability performance of CDMA, and zero capacity implies a complete failure in information transmission. However, in practical systems, the worst case disguised jamming is difficult to launch, since the disguised jammer cannot really capture the exact timing and amplitude information of the authorized signal. That is, practical disguised jamming is usually not fully symmetric with the authorized signal. As will be shown in Section V-A, nearly worst disguised jamming (i.e., $|\tau| \approx 0$ and $\gamma \approx 1$) can also be very harmful if left unattended. In this paper, by taking the timing difference τ and amplitude ratio γ into account, we find that the error probability of CDMA systems under practical disguised jamming can be reduced significantly.

IV. Proposed CDMA Receiver Design under Disguised Jamming

In this section, we estimate the jamming parameters as well as the authorized symbol using the minimum mean square error (MMSE) criterion. Unlike traditional MSE between the received signal and transmitted signal, the MSE here is calculated between the received signal and jammed signal, which is the sum of the authorized signal and the disguised jamming.

Following (3)-(5), the aforementioned MSE can be calculated as

$$\begin{aligned} &J(a,b,\tau,\gamma) \\ =&\frac{1}{T}\int_0^T |r(t)-s(t)-j(t)|^2 dt \\ =&\frac{1}{T}\int_0^T |r(t)-ac(t)-b\gamma c(t-\tau)|^2 dt \\ =&\frac{1}{T}\int_0^T |r(t)-ac(t)|^2 dt - \frac{\gamma b^*}{T}\int_0^T [r(t)-ac(t)]c(t-\tau)dt \\ &-\frac{\gamma b}{T}\int_0^T [r(t)-ac(t)]^* c(t-\tau)dt + \frac{\gamma^2|b|^2}{T}\int_0^T c^2(t-\tau)dt, \end{aligned} \tag{16}$$

where $(\cdot)^*$ denotes the complex conjugate. Since $c(t)$ is T-periodic, following (2), we have $\frac{1}{T}\int_0^T c^2(t-\tau)dt = \frac{1}{T}\int_0^T c^2(t)dt = 1$. If we further denote

$$A(a,\tau) = \frac{1}{T}\int_0^T [r(t)-ac(t)]c(t-\tau)dt, \tag{17}$$

the MSE can be rewritten as

$$\begin{aligned} J(a,b,\tau,\gamma) =&\frac{1}{T}\int_0^T |r(t)-ac(t)|^2 dt \\ &-\gamma b^* A(a,\tau) - \gamma b A^*(a,\tau) + \gamma^2|b|^2. \end{aligned} \tag{18}$$

Thus, the problem can be formulated as minimizing (18) by finding the optimal a, b, τ and γ, i.e.,

$$\{\hat{a},\hat{b},\hat{\tau},\hat{\gamma}\} = \arg\min_{a,b,\tau,\gamma} J(a,b,\tau,\gamma). \tag{19}$$

To minimize (18), one necessary condition is that its partial derivatives regarding b and γ are zero. Note that when z is a complex variable, we have $\frac{\partial z}{\partial z} = 0$, $\frac{\partial z^*}{\partial z} = 2$ and $\frac{\partial |z|^2}{\partial z} = 2z$. Hence,

$$\begin{cases} \frac{\partial J}{\partial b} = -2\gamma A(a,\tau) + 2\gamma^2 b = 0, \\ \frac{\partial J}{\partial \gamma} = -b^* A(a,\tau) - bA^*(a,\tau) + 2\gamma|b|^2 = 0, \end{cases} \tag{20}$$

from which we can get

$$\gamma = \frac{A(a,\tau)}{b} = \frac{A^*(a,\tau)}{b^*}. \tag{21}$$

Substituting (21) into (18), the MSE can be reduced to

$$J = \frac{1}{T}\int_0^T |r(t)-ac(t)|^2 dt - |A(a,\tau)|^2, \tag{22}$$

which is a function depending only on a and τ.

In digital implementation, limited by the time resolution, τ becomes discrete and thus has only a few possible values with $|\tau| < T_c$. In this way, an exhaustive search[2] on τ and a would be feasible and also an effective approach to minimize (22). The required computation mainly lies in a finite number of MSE calculation, and the number of possible (a,τ) pairs is $M \times Q$, where M is the constellation size and Q is the number of possible values for τ. Ultimately, the recovered symbol $\hat{a}$ and the estimated timing difference $\hat{\tau}$ would be the ones minimizing (22) which we obtained from the exhaustive search above.

Following (21), the amplitude ratio can be estimated as

$$\hat{\gamma} = \frac{|A(\hat{a},\hat{\tau})|}{|b|}, \tag{23}$$

for a constant-modulus constellation (e.g., PSK), where $|b|$ is readily available since it holds constant for all $b \in \Omega$. For non-constant-modulus constellation, the amplitude ratio cannot be exactly drawn. This is because that from (21), we can only determine $\hat{b}\hat{\gamma} = A(\hat{a},\hat{\tau})$, which cannot yield a specific $\hat{\gamma}$ when the amplitude of the jamming symbol is not specifically available. However, in this case, we can obtain a range for $\hat{\gamma}$. More specifically, if $B_1 \le |b| \le B_2$ for $b \in \Omega$, then we have

$$\frac{|A(\hat{a},\hat{\tau})|}{B_2} \le \hat{\gamma} \le \frac{|A(\hat{a},\hat{\tau})|}{B_1}. \tag{24}$$

Discussions: 1) The major differences between the estimation of disguised jamming and that of multipath signals [18], [19] lie in: i) Multipath signals always contain the same symbol as the primary signal (which is the signal going through the line-of-sight path), while the symbol carried by disguised jamming is chosen independently from the authorized signal; ii) Multipath signals are generally much weaker than the primary signal, while disguised jamming maintains a similar power level as the authorized signal; iii) Multipath signals always arrive at the receiver after the primary signal, while disguised jamming can have either a leading or lagging phase compared with the authorized signal.

2) Although we primarily focus on recovering the authorized symbols under disguised jamming here; however, the information obtained from the MMSE receiver can be used for jamming detection and evaluation. The estimated amplitude ratio can be used as a metric to determine whether a disguised jammer is present or not by comparing it with an appropriate threshold. Through cooperation of multiple receivers, it is also possible to locate the disguised jammer by exploiting the estimated timing differences between the jamming interference and the authorized signal. These potential topics are left for future work.

[2]Generally it would be sufficient to perform an exhaustive search for regular time resolution with a practical sampling rate; however, for high time resolution, we suggest the usage of state-of-the-art iterative optimization methods, e.g., Newton's method.

V. Numerical Results

In this section, we first evaluate the performance degradation of CDMA systems under disguised jamming, and then demonstrate the effectiveness of the proposed receiver in jamming estimation and BER performance improvement. We assume AWGN channels and apply BPSK modulation, which is generally used in GPS, and the spreading code is a Gold sequence with a processing gain N = 1023. In the simulation, we set the oversampling factor to 32, which means that there are 32 samples in each chip with a T_c duration. Note that the oversampling factor determines the resolution of the timing difference estimation, i.e., $\frac{1}{32}T_c$, for the current setting.

A. Performance Degradation of Conventional CDMA Systems under Disguised Jamming

In this subsection, we evaluate the impact of disguised jamming with different timing differences on BER performance of the conventional CDMA system. The amplitude ratio γ is set to 1, and we apply the conventional receiver in (6) without jamming estimation. It is observed in Fig. 1 that compared with jamming-free case, the BER performance is severely degraded by disguised jamming, especially when the timing difference τ is small. In the worst case with τ = 0, the BER maintains at approximately $\frac{1}{4}$ no matter how high the SNR is, which agrees with the lower bound in (9).

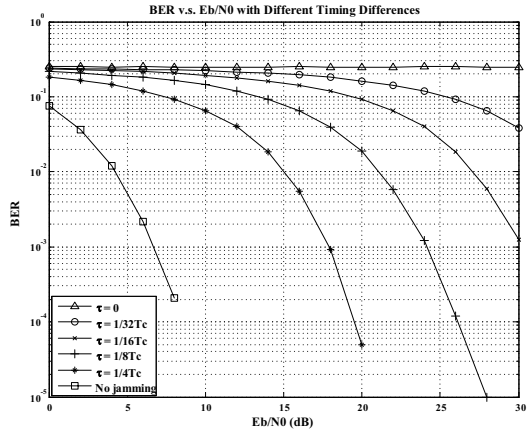

Fig. 1. BER v.s. Eb/N0 for the conventional CDMA receiver under various disguised jamming.

B. Timing Difference and Amplitude Ratio Estimation

In this subsection, we provide the estimation results of the timing difference τ and amplitude ratio γ by applying the proposed CDMA receiver. Here we set $\tau = \frac{1}{4}T_c$ and $\gamma = 1.2$. In Fig. 2, we can observe that both the timing difference and amplitude ratio can be accurately estimated with reasonable SNRs, and the accuracy improves as the SNR increases.

C. BER Performance Improvement with Jamming Estimation

In this subsection, we compare the BER performance of the proposed CDMA receiver with that of the conventional receiver. To explore a time-varying jamming scenario, the timing difference τ is set to be uniformly distributed on $[-\frac{1}{4}T_c, 0) \cup (0, \frac{1}{4}T_c]$, and the amplitude ratio γ follows a normal distribution $\mathcal{N}(1, \sigma^2)$, where $\sigma = \frac{1}{6}$. Note that we do not take into account τ = 0, in which case the BER cannot be decreased because of the lower bound in (9). In Fig. 3, it is observed that the BER is decreased significantly

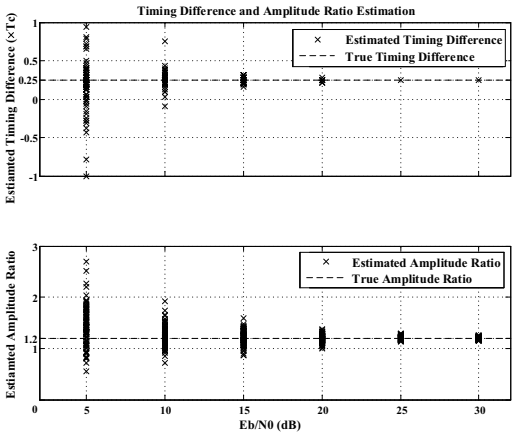

Fig. 2. Timing difference and amplitude ratio estimation.

by the proposed CDMA receiver with reasonable SNRs. With low SNRs, the BER cannot be decreased due to the inaccurate jamming estimation, which demonstrates that it is more difficult to combat disguised jamming under poor channel conditions.

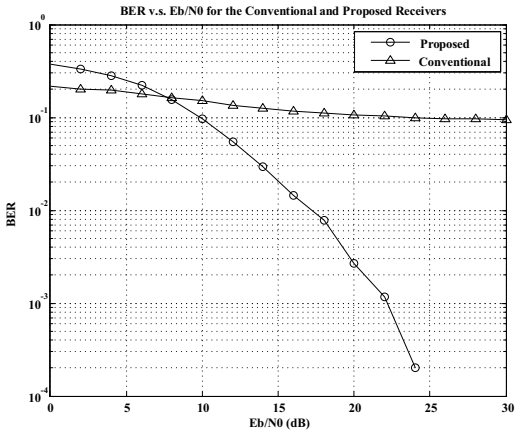

Fig. 3. Performance comparison of the conventional receiver and the proposed receiver under disguised jamming.

VI. Conclusions

In this paper, we analyzed the impact of disguised jamming on conventional CDMA systems, and developed an effective approach to recover the authorized symbols with CDMA transmission under disguised jamming. The proposed approach exploited the small timing difference between the authorized signal and the jamming interference. We estimated the authorized symbols as well as the jamming parameters by finding the minimum mean square error (MMSE) between the received signal and jammed signal, which is the sum of the authorized signal and the disguised jamming. The numerical results demonstrated that with reasonable SNRs, the proposed receiver significantly improves the BER performance of CDMA systems under disguised jamming, and also provides a good evaluation about jamming.

Acknowledgment

This research is partially supported by National Science Foundation under awards: CNS 1217206 and ECCS 1232109.

REFERENCES

[1] S. Barbarossa and A. Scaglione, "Adaptive time-varying cancellation of wideband interferences in spread-spectrum communications based on time-frequency distributions," *IEEE Trans. Signal Processing*, vol. 47, no. 4, pp. 957–965, Apr 1999.

[2] S. Aromaa, P. Henttu, and M. Juntti, "Transform-selective interference suppression algorithm for spread-spectrum communications," *IEEE Signal Processing Lett.*, vol. 12, no. 1, pp. 49–51, Jan 2005.

[3] C.-L. Wang and K.-M. Wu, "A new narrowband interference suppression scheme for spread-spectrum CDMA communications," *IEEE Trans. Signal Processing*, vol. 49, no. 11, pp. 2832–2838, Nov 2001.

[4] H. Holma and A. Toskala, *WCDMA for UMTS: HSPA Evolution and LTE*. New York, NY, USA: John Wiley & Sons, Inc., 2007.

[5] E. Kaplan, *Understanding GPS - Principles and applications*, 2nd ed. Artech House, December 2005.

[6] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. 15, no. 1, pp. 122–127, Jan 1969.

[7] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, no. 1, p. 083589, 2007.

[8] T. Ericson, "The noncooperative binary adder channel," *IEEE Trans. Inform. Theory*, vol. 32, no. 3, pp. 365–374, 1986.

[9] M. Medard, "Capacity of correlated jamming channels," in *Allerton Conference on Communications, Computing and Control*, 1997.

[10] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping-part i: System design," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 70 –79, Jan. 2013.

[11] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *The Annals of Mathematical Statistics*, vol. 31, no. 3, pp. pp. 558–567, 1960.

[12] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 44, no. 2, pp. 159–175, 1978.

[13] T. Ericson, "Exponential error bounds for random codes in the arbitrarily varying channel," *IEEE Trans. Inform. Theory*, vol. 31, no. 1, pp. 42–48, 1985.

[14] I. Csiszar and P. Narayan, "Arbitrarily varying channels with constrained inputs and states," *IEEE Trans. Inform. Theory*, vol. 34, no. 1, pp. 27–34, 1988.

[15] ——, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Trans. Inform. Theory*, vol. 34, no. 2, pp. 181–193, 1988.

[16] ——, "Capacity of the Gaussian arbitrarily varying channel," *IEEE Trans. Inform. Theory*, vol. 37, no. 1, pp. 18–26, 1991.

[17] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2148–2177, 1998.

[18] M. Sahmoudi and M. Amin, "Fast iterative maximum-likelihood algorithm (FIMLA) for multipath mitigation in the next generation of GNSS receivers," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4362–4374, November 2008.

[19] Z. Xu and P. Liu, "Code-constrained blind detection of CDMA signals in multipath channels," *IEEE Signal Processing Lett.*, vol. 9, no. 12, pp. 389–392, Dec 2002.