

Self-Encoded Spread Spectrum Communications

Lim Nguyen

Computer and Electronics Engineering
University of Nebraska-Lincoln
Omaha, Nebraska 68182-0572

ABSTRACT

We present a novel spread spectrum communication system for the secured transmission of digital information. The approach is based on the unconventional self-encoding principles that we have developed at the University of Nebraska for the modulation and detection of spread spectrum signals. The proposed system does not use pseudo-random codes, and is unique in that traditional transmit and receive code generators based on maximal-length sequences or chaotic signals are not needed. In fact, the enhanced transmission security arises not only due to the spread-spectrum nature of the signal, but also from the stochastic nature of the unique spectrum spreading and de-spreading processes. This paper describes the proposed system and presents the theoretical and simulation results of the system performance in an additive-white Gaussian noise channel.

INTRODUCTION

Wireless transmission of digital information is an active research area of considerable military and economic interest. Military operations require secure communication systems that are anti-jamming (AJ) and have a low probability of detection (LPD) by enemies. Spread spectrum communication systems have been developed since the 1950's to provide such a capability. Its distinct AJ and LPD advantages have found applications in tactical communication systems ranging from point-to-point communications to satellite links and multiple access networks. This technique has recently become the technology for mobile telephony and Global Positioning Systems. Spread spectrum is the basis for code-division multiple-access (CDMA) communications, an industry standard (IS-95) for cellular telephones and personal communications services.

A principal problem facing the design of a secure military communication system is to protect the transmission from the threat of interruption and detection by enemies. In a tactical communication environment, intentional jamming can critically impair radio receptions while unintended detection can seriously threaten the message privacy. This problem represents a continued challenge due to the ever increasing sophistication of electronic counter-measures and complex signal processing capability.

Unlike cryptography that relies on data encryption for privacy protection, spread spectrum can simultaneously accomplish both AJ and LPD objectives by means of signal

waveform encoding [1]. Figure 1 illustrates the conventional direct spread spectrum scheme that employs pseudo-noise (PN) code generators. Digital information is sent from a transmitter to a receiver by varying the transmission signal at a rate much faster than the information rate. This results in the spreading of the signal energy over a bandwidth much larger than that of the digital information, making effective jamming difficult. The PN spreading signal, or code, is deterministic but carefully chosen so that it appears "random", or noise-like, to an unintended receiver, preventing it from detecting the data [2]. This code is known to the intended receiver, allowing it to recover the digital information.

PN code generators are typically linear feedback shift register circuits that generate maximal-length or related sequences. These deterministic sequences have random-like properties with low crosscorrelations critical for achieving good system performance [3]. A fundamental problem with the deterministic PN codes is that they can be duplicated, potentially compromising the transmission security. Although random codes have sometimes been employed for analysis purposes [4], they present a practical implementation problem because data recovery by the intended receiver requires prior knowledge of the codes for signal de-spreading. As a result, the random codes in these studies would remain fixed once they have been generated. It was generally believed that spread spectrum systems with time-varying random codes are not possible in practice.

In this paper, we describe a novel spread spectrum system that does not use PN codes. The new techniques are unique in that traditional transmit and receive code generators based on m-sequences or chaotic signals are not needed. The enhanced transmission security arises not only due to the spread-spectrum nature of the signal, but also from the stochastic nature of the unique spectrum spreading and de-spreading processes. As a result, detection of the digital data by an unintended receiver is practically impossible, resulting in ideally secure transmissions. The proposed techniques in fact provide a feasible implementation of random-coded spread spectrum systems that previously have been thought to be impractical.

SYSTEM DESCRIPTION

Our approach to improving the LPD performance is to completely abandon the use of PN codes. We have developed a practical method to generate self-encoded spread spectrum

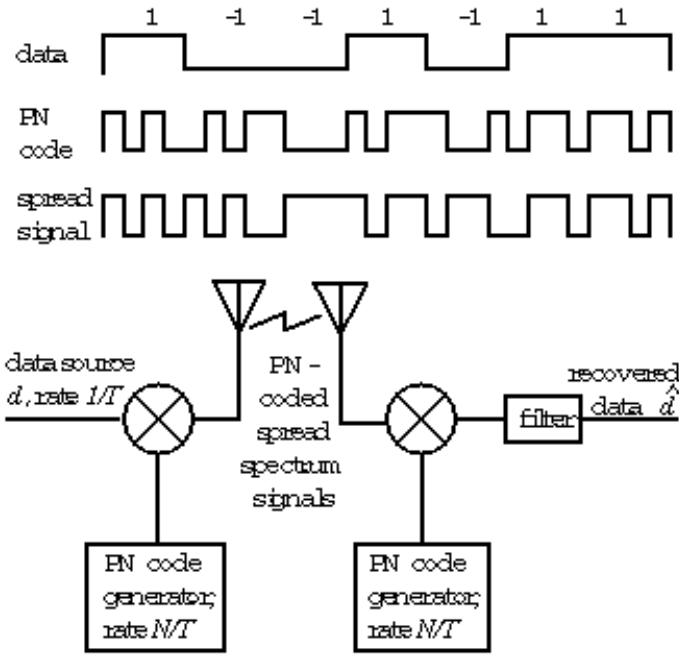


Figure 1: Conventional direct-sequence spread spectrum scheme.

sequences in the transmitter, and to regenerate them in the intended receiver. A realization of the self-encoding principles is illustrated by the simplified schematic in Figure 2 for a direct-sequence spread spectrum system. As the term implies, the spreading code is instead obtained from the random digital information source itself. At the transmitter, the delay registers are constantly updated from an N -tap delay of the data, where N is the code length. The delay registers generate the code chips that switch at N times the data rate for signal spreading. The random nature of the digital information source is assured by applying appropriate data compression methods to remove any redundancy in the data stream, thereby maximizing its entropy. The binary data symbols can therefore be modeled as independent and identically distributed Bernoulli random variables. Symbol values of $+1$ and -1 occur equally likely with a probability of $1/2$. As a result, the spreading sequence is not only randomly generated and independent of the current symbol, but also dynamically changing from one symbol to the next.

The self-encoding operation at the transmitter is reversed at the receiver. The recovered data are fed back to the N -tap delay registers that provide an estimate of the transmitter's spreading codes required for signal de-spreading. Data recovery is by means of a correlation detector. Notice that the contents of the delay registers in the transmitter and receiver should be identical at the start of the transmission. This is accomplished as part of the initial synchronization procedure. Unless *initially* synchronized *and* having a complete knowledge of the tap register structure (intended receiver),

data recovery will be extremely unreliable since the spreading codes as constructed are time-varying, random and uncorrelated. As a result, self-encoding makes unwanted detection of the data by an unintended receiver practically impossible. The security of the transmission system can greatly be enhanced with this LPD communication system.

ANALYSIS

The bit-error rate (BER) performance of the proposed system is analyzed assuming an additive, white Gaussian noise (AWGN) channel. We assume that synchronization between the transmitter and receiver has been achieved. Notice that self-encoded systems present a unique synchronization problem: the spreading code is needed for data recovery, but the data itself determines the code information.

Intuitively, we want $N < 1/BER$ so that the receiver's estimate of the spreading codes is reliable. This reduces the effect of bursty chip errors while increasing the probability of recovery from the chip errors. N also has to be sufficiently large so that the signal degradation from chip errors is negligible. In fact, we can model the effect of chip errors as self-interference introduced by self-encoding. The reduction in signal strength or signal-to-noise ratio is given by:

$$A = 20 \log \left(1 - \frac{2n}{N} \right) \text{ dB}, \quad (1)$$

where n is the number of chip errors in the receiver's delay registers. The average signal-to-noise ratio degradation due to BER can be expressed as:

$$A = 20 \log(1 - 2BER) \text{ dB}. \quad (2)$$

Now the BER of the unspread transmission is given as $BER = \frac{1}{2} \text{erfc}(\sqrt{SNR})$ for binary phase-shift keying, where SNR is the symbol signal-to-noise power ratio and erfc is the complementary error function [5]. This allows us to obtain an estimate of the average BER degradation due to self-encoding for AWGN channels, according to:

$$BER = \frac{1}{2} \text{erfc} \left(\sqrt{SNR(1 - 2BER)^2} \right). \quad (3)$$

The average BER performance versus the symbol SNR can be obtained numerically from this non-linear expression. As an example, for a processing gain of 30 dB or $N = 1000$, the average performance degradation in an AWGN channel is negligible at $BER = 10^{-5}$ or less (9.5 dB SNR). The results of the BER analysis according to (3) are shown in Figure 3, demonstrating excellent agreement with the simulation results. The Monte Carlo simulations were averaged over code lengths that varied from 16 to 1028. There is little degradation in the BER performance for SNR greater than 4 dB. As expected, self-interference effects become severe only at low SNR . The plots show that for normal operations with a BER performance better than 10^{-3} , the proposed LPD

communication system will be just as reliable as the conventional, PN-coded spread spectrum system.

Notice that portions of the N -tap delay registers may be loaded with known, fixed code elements should we wish to limit the maximum SNR degradation. This suggests that a combination of PN and self-encoded spread spectrum techniques will enable design trade-offs in system performance. A feasible but undesirable solution to (3) corresponds to $BER = 1/2$, independent of the SNR . This motivates theoretically why unwanted detection by an unintended receiver is practically impossible. The analytical result illustrates the importance for the receiver to have an accurate estimate of the transmitter's delay registers. Excessive errors due to signal fading or bursty channel conditions could result in gross self interference that may not be recoverable, even under high SNR . Appropriate synchronization measures must be taken to prevent this potential instability that is unique to the self-encoding designs.

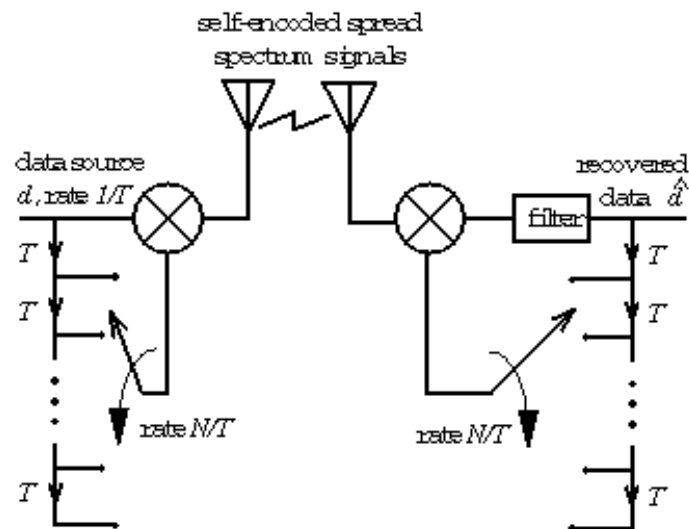


Figure 2: Proposed self-encoded, direct-sequence spread spectrum scheme.

DISCUSSION

The scheme illustrated in Figure 2 can be thought of as a feasible implementation of spread spectrum systems with random codes that have been thought to be impractical. In previous study of CDMA systems with random signature sequences [4], [6], [7], the analysis would assume that the receiver has a clairvoyant knowledge of the spreading code that has been randomly generated at the transmitter. Conceptually, the random codes in practice must be transmitted by means of spread spectrum to the non-clairvoyant receiver that in turn uses the received codes for both data and code recovery. This is a catch-22 problem similar to the unique synchronization problem mentioned earlier. Self-encoding makes the connection that the random data themselves could

be a source of spreading sequences. As we have observed, this also means that any redundancy in the information source should be minimized by means of data compression. Thus, self-encoding requires the sensible design objective that the information content of the transmission be maximized.

From this point of view, there is also a degree of similarity with the transmitted-reference (TR) spread spectrum scheme [2], [8]. This counterpart to the PN-coded method has enjoyed much less popularity, primarily because it requires a separate channel to transmit the spreading codes to the receiver. In principle, random codes could be implemented with such a TR scheme. Self-encoding in effect provides a reasonable and obvious modification to the TR scheme: the same channel shall be used to send both spreading codes and data (further generalizations can be obtained from this observation.) The random codes can then be obtained from the data, provided that the data have been compressed to remove any redundancy prior to self-encoding.

Self-encoding techniques are also applicable to other spread spectrum systems, such as time hopping, frequency hopping or hybrid systems. The self-encoded sequences can be obtained in a similar manner to provide hopping patterns that are completely random. Obviously, the N -tap delay register structure shown in Figure 2 is but one possible realization of spreading sequences from the data. More sophisticated realizations, possibly combined with encryption, can provide further LPD performance and implementation advantages.

In terms of the classic “cock-tail party” analogy for CDMA [9], self-encoded spread spectrum amounts to the party goers conversing in continuously changing languages that are constructed anew depending on the words that have been spoken. Since the messages being conveyed by the words are unpredictable (otherwise there is no need for conveying them in the first place), the conversing languages are also unpredictable. There is a number of implications associated with such a self-encoded multiple access (SEMA) scenario. First, in principle code initializations are only required at the starts of the conversations. For security and privacy, this can be accomplished with encryption keys. Second, the interference is uncorrelated even among the speakers that began the conversations with the same language. This should mitigate the correlation problems that exist in asynchronous operations with PN codes. Third, it is imperative that some form of error correction mechanism be employed to correct the missed words that are expected to occur due to noise and interference, so that the conversations remain intelligible. We expect that iterative and soft decoding methods such as turbo coding will significantly improve the system performance in this respect. This is especially critical during propagation fades that could result in burst errors. Incorporating random or periodic reset of the initialization, as part of the transmitter/receiver synchronization scheme, along with interleaving, will improve the robustness of self-encoded systems to the

channel conditions.

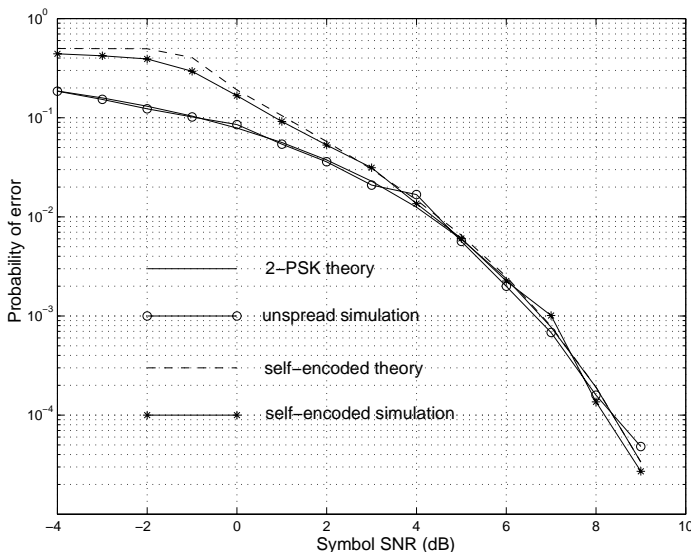


Figure 3: BER performance comparisons of a self-encoded, direct-sequence spread spectrum system in an AWGN channel.

In conventional CDMA communications, the number of available PN codes depends on the code length and puts a limit on the number of subscribers. The constant code length makes it difficult to accommodate transmissions that have variable data rates. In a SEMA system, the signals from simultaneous users are uncorrelated because their data should be random and independent from one another. Thus, unlike the conventional approach, self-encoding does not put a limit on the number of subscribers: the system is strictly interference-limited by the multiple access interference (MAI) from the simultaneous users. Likewise, the problems associated with variable data rates are greatly mitigated because the spreading waveforms from different users are uncorrelated. The random nature of self-encoding allows the users to transmit asynchronously at their own symbol rates and chip lengths N . In this respect, we expect that there are strong interplays between source and channel codings, and self-encoding.

Our simulation of interference-limited CDMA systems has indicated that both PN and self-encoded methods have similar BER performance using the correlation detector. This can be reasonably expected, because PN codes seek to approximate random sequences that are in fact implemented by self-encoding. In fact, the standard deviation of the crosscorrelations of purely random sequences is equal to \sqrt{N} which is similar to the Welch's lower bound on the crosscorrelation between any two binary sequences. However, while the Kassami codes achieve this bound, the random MAI associated with self-encoding is quite a contrast to the predictable MAI from using the Kassami codes. Indeed, we have found that the multi-user BER for SEMA is well described by the

AWGN approximation for MAI when N is large (about 1028 or more typically). Thus, while SEMA does not guarantee code isolation (as in PN systems), the BER performance does degrade gracefully as the number of users increases, with the probability of worst-case code collisions between any two users being 2^{-N} .

An interesting and important issue in CDMA is that of multi-user detection [10], [11], [12]. Obviously, multi-user detection schemes that have been developed for conventional CDMA systems are not feasible with SEMA systems. However, we know that with PN codes the theoretical single-user bound can be approached using multi-user detectors. This suggests the intriguing possibility that there may exist source/channel coding schemes and modulation/detection methods that would achieve the single-user bound for SEMA systems.

APPLICATION

A principal advantage of spread spectrum is LPD in military applications, and security and privacy in commercial applications. Self-encoding further enhances the spread spectrum advantage to reduce the risk of detection, and contributes to privacy. In an application using transponder – bent pipe satellites including DSCS and ACTS, concurrent narrow band communications will cause little interference but provide no LPD or protection against passive geo-location listeners. Incorporation of self-encoded spread spectrum would provide enhanced LPD protection when using either satellite or ground-based transponders.

The self-encoding techniques presented in this paper represent a continually changing key in the TRANSEC portion of current spread spectrum systems. This dynamic key can be used as a continually changing crypto key for ciphertext. (Self-encoding therefore can be considered a variant of the cyphertext autokey.) The purpose of such an implementation would be to reduce the cost associated with maintaining symmetric cryptographic keys. A protocol implementation of self-encoding techniques with an asymmetric public-key system would proceed as follows:

- The sender and listener synchronize to a mutual public-key cryptosystem.
- The listener sends the public-key that the sender uses to encrypt the ciphertext message.
- The listener decrypts the message text using the private-key.
- The message text is then used as a session key to initiate the self-encoded spread spectrum process that provides the security and privacy.
- The crypto sequence could then be terminated to reduce the overhead on the message traffic.

An intercept listener would only get the public-keys and the ciphertext, but without the private-keys could not determine the upcoming spreading sequences. The lifetime of the session keys would be very short, lasting only until the self-encoded dynamic key has been established.

CONCLUSION

We have presented a spread spectrum communication system based on self-encoding principles that could improve LPD performance over the PN approach due to the random and dynamically changing, coded waveform. The proposed techniques chart a completely different approach to spread spectrum communications. Conventional spread spectrum attempts to realize an insight obtained from Shannon's theory [13]. In essence, it suggests that the information bearing signals should appear as noise over as wide a bandwidth as possible. The deterministic PN codes are somewhat contradictory in this respect. The random nature of self-encoding methods is in accord with this theoretical insight. Thus, information theoretic spread spectrum communication has come full circle with self-encoding. The simplicity in the code generation and regeneration at the transmitter and the receiver is somewhat surprising. This should be regarded as a natural consequence of the completely random characteristics of self-encoding.

The military and economic interest in spread spectrum technology warrants further research of self-encoded spread spectrum communications. We are investigating optical communication applications with optical SEMA networks, including self-encoded wavelength multiplexing. Optical CDMA can provide secure transmission and support simultaneous network access for many users [14], [15]. Studies are also under way for applications of self-encoding to frequency hopping, and time hopping systems such as ultra-wide bandwidth radios [16]. The performance analysis includes channel disturbances such as fading/multi-paths, interference/jamming, and impulsive noise. Incorporating both PN and self-encoding schemes, or iterative and soft decoding methods such as turbo codes, should also be of significant importance. Sampling methods are being developed for efficient simulation study of self-encoded systems due to its unique stochastic models.

In terms of implementations, modified commercially available cellular mobile phone equipment would allow further exploitation of the new technology. The warfighters presently only have access to highly secure and robust communications in the battlefield through MILSTAR using the SCAMP terminals. Current cellular systems are not secure, however spread spectrum capability could be readily added to these systems using the self-encoding techniques. Self-encoding not only improves the communication security, but also provide additional payoff in direct cost savings from the reduction of crypto logistics.

ACKNOWLEDGEMENT

We would like to thank Frank Fisk (formerly with AFRL) for his valuable comments and suggestions, and Paul Schleck for portions of the simulation. Thanks are also due to Robert Fladby and Robert Frankland of the Computer and Electronics Engineering department. This work was partly supported by the Mobile Communications Research Project of the Nebraska Research Initiatives and a Research Council fellowship from the University of Nebraska-Lincoln.

References

- [1] R. L. Peterson, R. E. Ziemer, and D. E. Borth, *Introduction to Spread Spectrum Communications*. Englewood Cliffs, NJ: Prentice Hall, 1995.
- [2] R. C. Dixon, *Spread Spectrum System*. New York, NY: John Wiley & Sons, 1984.
- [3] D. V. Sarwate and M. B. Pursley, "Crosscorrelation Properties of Pseudorandom and Related Sequences," *Proceedings of the IEEE*, vol. 68, pp. 593-619, May 1980.
- [4] T. M. Lok and J. S. Lehnert, "Error Probabilities for Generalized Quadrphase DS/SSMA Communication Systems with Random Signature Sequences," *IEEE Trans. Commun.*, vol. 44, pp. 876-885, Apr. 1996.
- [5] J. G. Proakis, *Digital Communications*. New York, N.Y.: McGraw-Hill, 1989.
- [6] J. S. Lehnert and M. B. Pursley, "Error Probabilities for Binary Direct Sequence Spread-Spectrum Communications with Random Signature Sequences," *IEEE Trans. Commun.*, vol. 35, pp. 87-98, Jan. 1987.
- [7] E. Geraniotis and B. Ghaffari, "Performance of Binary and Quaternary Direct-Sequence Spread-Spectrum Multiple-Access Systems with Random Signature Sequences," *IEEE Trans. Commun.*, vol. COM-39, pp. 713-724, May 1991.
- [8] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. I, II and III. Rockville, MD: Computer Science Press, 1985.
- [9] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*. Reading, MA: Addison-Wesley, 1995.
- [10] N. Abramson, ed., *Multiple Access Communications, Foundation for Emerging Technologies*. New York, NY: IEEE Press, 1993.
- [11] S. Verdú, "Minimum Probability of Error for Asynchronous Gaussian Multiple-Access Channels," *IEEE Trans. Info. Theory*, vol. IT-32, pp. 85-96, Jan. 1986.
- [12] R. Lupas and S. Verdú, "Linear Multiuser Detectors for Synchronous Code Division Multiple-Access Systems," *IEEE Trans. Info. Theory*, vol. IT-35, pp. 123-136, Jan. 1989.
- [13] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 31, pp. 379-423 and 623-656, 1948.
- [14] L. Nguyen, B. Aazhang, and J. F. Young, "All-optical CDMA with Bipolar Codes," *Electron. Lett.*, vol. 31, pp. 469-470, Mar. 1995.
- [15] M. J. Parham, C. Smythe, and B. L. Weiss, "Code Division Multiple-access Techniques for use in Optical-fibre Local-area Networks," *Electron. Commun. Eng. Journal*, pp. 206-212, Aug. 1992.
- [16] M. Z. Win and R. A. Scholtz, "Impulse Radio: How It Works," *IEEE Commun. Lett.*, vol. 2, pp. 36-38, Feb. 1998.