CDMA in Signal Encryption and Information Security

Olanrewaju B. Wojuola, Stanley H. Mneney and Viranjay M. Srivastava
School of Engineering
University of KwaZulu-Natal
Durban - 4041, South Africa.
wojuolao@ukzn.ac.za, mneneys@ukzn.ac.za, viranjay@ieee.org

***Abstract*— Code-division multiple-access (CDMA) is a communication technique that was developed originally for the military because of its jam-resistant properties. It is one of the early forms of jam-resistant, signal encryption techniques used in military applications for the purpose of wireless signal transmission and information-hiding from adversaries. In recent years, CDMA has also played a key role in mobile telephony as a multiple-access technique because of certain properties that make it suitable for commercial and civilian applications. This paper gives a brief exposition on CDMA as a signal encryption technique, and the position that it occupies in future wireless technology. This paper also compares CDMA technology with a relatively recent technique, interleave-division multiple-access (IDMA) that has been attracting significant attention in wireless circles.**

Keywords— Code-division multiple-access, Interleave-division multiple-access, Signal encryption, Information security, Wireless communication.

I. INTRODUCTION

The advent of code-division multiple-access (CDMA) dates back to the 1940s. It was developed originally for the military as a means of establishing secure, jam-resistant communications [1-6]. During transmission, the existence of a CDMA signal can hardly be detected as it appears as noise spread out over a wideband channel, unlike amplitude or frequency modulated carriers that have concentrated energy over a narrowband. CDMA's large bandwidth makes it difficult to jam. In addition, CDMA signal energy is well below noise level, meaning that the signal is buried (hidden) in noise. It is for these reasons that CDMA can be used for covert transmissions.

CDMA relies on coding for user-separation. It involves the use of spreading codes (also known as spread-spectrum codes, pseudo-noise (PN) codes, or pseudo-random noise (PRN) codes or sequences) as user identification element. Examples of such codes include maximal linear code sequences, Gold codes, Walsh-Hadamard codes and Kasami codes [7-11]. In a CDMA system, each user is assigned a unique spreading code, and uses this code to encode (encrypt) the user's signal into a wideband signal. The receiver requires a knowledge of this unique code before the transmitted information can be detected and decoded. For good performance in multiple-access applications, spreading codes are required to have minimum cross-correlation between them.

CDMA can be classified into four protocol types: direct sequence CDMA (DS-CDMA), frequency-hopping CDMA (FH-CDMA), time-hopping CDMA (TH-CDMA) and hybrid CDMA [1, 12, 13]. The last group (hybrid CDMA) is obtained from any combination of the first three, or CDMA with any other technique.

This paper gives a brief exposition on the DS-CDMA from encryption point of view. This paper also briefly considers interleave-division multiple-access (IDMA) and the position that the techniques occupy in future wireless technologies. Other advanced forms of CDMA and IDMA systems exists (e.g. MIMO CDMA systems, space-time coded multicarrier CDMA systems, multicarrier IDMA systems, etc.) [14-16], but these are not the focus of this paper.

In literature, IDMA is usually presented as a better alternative to CDMA. As we shall see later in this paper, this common view does not represent the true picture, particularly from information security point of view.

The rest of this paper is organised as follows. Basic principles of operation of CDMA systems are presented in section II. By appealing to the basic theory, the use of CDMA (or spread spectrum) in signal encryption and information security has been explained in section III, followed by an illustrative example in section IV. The system performance curves are used in section V to further explain the principles behind the use of spread spectrum techniques, its application is in Section VI. In section VII, IDMA has been introduced. This is followed by a critical look at the position of IDMA and CDMA in information security and future wireless systems in Section VIII. Finally, the section IX concludes the work and recommend the future aspects.

II. BASIC THEORY OF CDMA SYSTEMS

Consider a DS-CDMA system. Let $b_n(t)$ (with a bit time T) be the data for the n^{th} user and $C_n(t) = \sum_{i=1}^{N} c_n(t - iT_c)$ be the unique code for theuser. If we assume that there are M users, then$0 \leq n \leq M$, and there are M unique codes. The coded output for each user is given by

$$y_n(t) = b_n(t).C_n(t) = b_n(t)\sum_{i=1}^{N} c_n(t - iT_c), \qquad (1)$$

where T_c the chip time, is much less than the bit time T. This multiplication has the implication that the spectrum of the bit which is proportional to $1/T$ is now much larger and is proportional to $1/T_c$. Thus the encoding in (1) spreads (enlarges) the spectrum of the signal and it is for this reason that CDMA is sometimes referred as spread-spectrum multiple access (SSMA). The spread factor is given by the ratio T_c/T.

Assume the presence of other users in the communication channel. At the receiving side, the signals from all users reach the receiver simultaneously. For a Gaussian channel, received signal *r*(t) is:

$$r(t) = \sum_{n=1}^{M} b_n(t)\sum_{i=1}^{N} c_n(t - iT_c) + n(t), \qquad (2)$$

where *n*(t) is additive white Gaussian noise with a double-sided power spectral density $N_o/2$. The signals from other users constitute interference. In order to recover the data from a specific user (selecting user 1), the composite signal is multiplied by the specific user code as in equation (3):

$$r_{n=1}(t) = b_1(t)\sum_{i=1}^{N}[c_1(t - iT_c)]^2 + \sum_{n=2}^{M} b_n(t)\sum_{i=1}^{N}[c_1(t - iT_c)]\ \ c_n(t - iT_c) + n(t)\sum_{i=1}^{N}[c_1(t - iT_c)], \qquad (3)$$

Since $[c_1(t - iT_c)] \in \mp 1$, $[c_1(t - iT_c)]^2 = 1$, equation (3) thus reduces to:

$$r_1(t) = b_1(t) + \sum_{n=2}^{M} b_n(t)\sum_{i=1}^{N}[c_1(t - iT_c)]c_n(t - iT_c) + n(t)\sum_{i=1}^{N}[c_1(t - iT_c)]. \qquad (4)$$

In equation (4), $b_1(t)$ is the recovered data for user 1; the second term represents multiple-access interference (MAI) from other users and the third term is noise which is spread out further.

In digital DS-CDMA represented by equation (1) to (4), the message signal is, in principle, multiplied directly by the code signal and the resulting signal modulates a carrier for onward transmission through a communication channel. The receiver correlates the received signal with the code of the user. Because each user's unique code has low cross-correlation with the other codes, the receiver is able to distinguish between users. Correlating the received signal with a code for a certain user de-spreads (decodes) the signal for the user.

III. CDMA AND INFORMATION SECURITY

The possibility of using CDMA in information-hiding centres around signal spreading as in fig. 1. In this figure, the message signal is multiplied by the spreading code to give the spread spectrum (SS) signal, spreading out the signal energy over a wideband. By spreading the spectrum of the signal, its energy or power density can be reduced to a level much lower than that of channel noise. Furthermore, the spreading process makes the signal itself to look like noise. Thus the signal is hidden inside the channel noise. An adversary cannot perceive the existence of the communication because the signal is buried in noise. A receiver can detect and decode the signal if and only if the receiver knows the spreading code with which the signal was encoded originally. Thus the code serves as the key for recovering the original information.

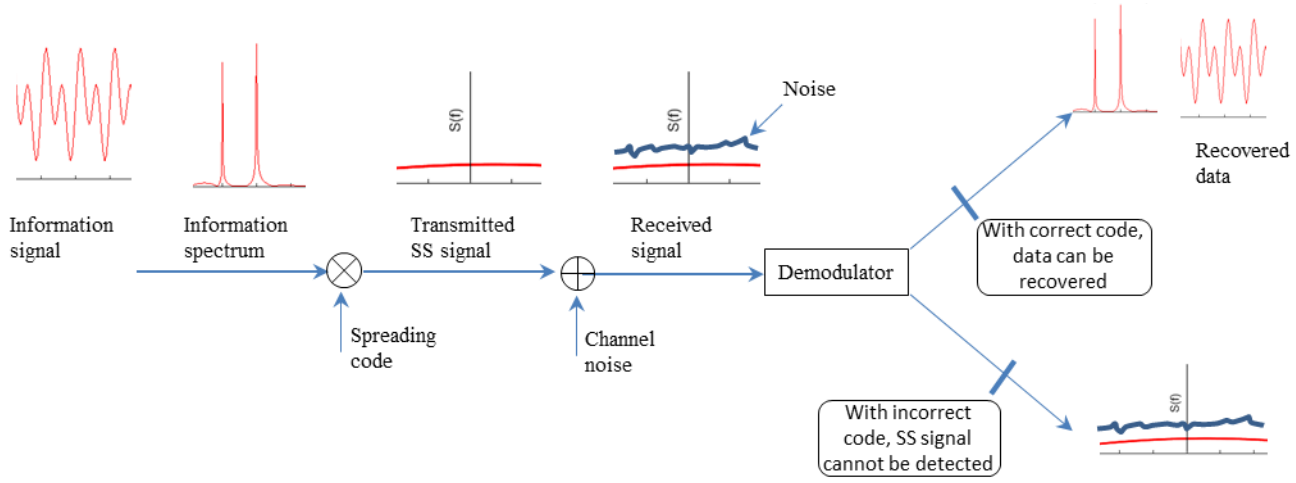

Fig. 1. The use of spread-spectrum techniques in information-hiding. (An adversary cannot perceive the existence of the communication because the signal is buried in noise).

IV. AN ILLUSTRATIVE EXAMPLE

An illustrative example shall now be used to further exemplify the principles behind the use of spread-spectrum techniques in information security. We shall first consider plain, *uncoded* signal transmission. By this we mean transmission not involving the use of spreading codes. Let the information signal $x(t) = 0.7 \sin(2\pi(50)t) + \sin(2\pi(100)t)$. Fig 2(a) shows the signal both in time and frequency domain. Its frequency spectrum clearly shows the signal's component frequencies (50 and 100 Hz), in agreement with the analytic expression $x(t)$ for the signal . Now consider a Gaussian noise having a mean of zero and unit variance. Fig. 2(b) shows the noise and its spectrum. Fig. 2(c) shows the results of superimposing the signal on the noise. Clearly, the signal power is much stronger than the noise, so that the signal can be picked up easily by an observer, making the signal vulnerable to attack. Fig 2(d) is a sum of the signal and the noise. The frequency spectrum of this figure shows that the presence of the signal is still visible even when mixed with noise. This shows the vulnerability of uncoded signal transmission.

Now consider the use of spreading codes. Let the signal energy be spread out over a wide bandwidth, to give a spread-spectrum (SS) signal. Fig 3(a) shows the SS signal, superimposed on the channel noise (the SS signal and the noise are superimposed in one plot both in time and frequency domain).

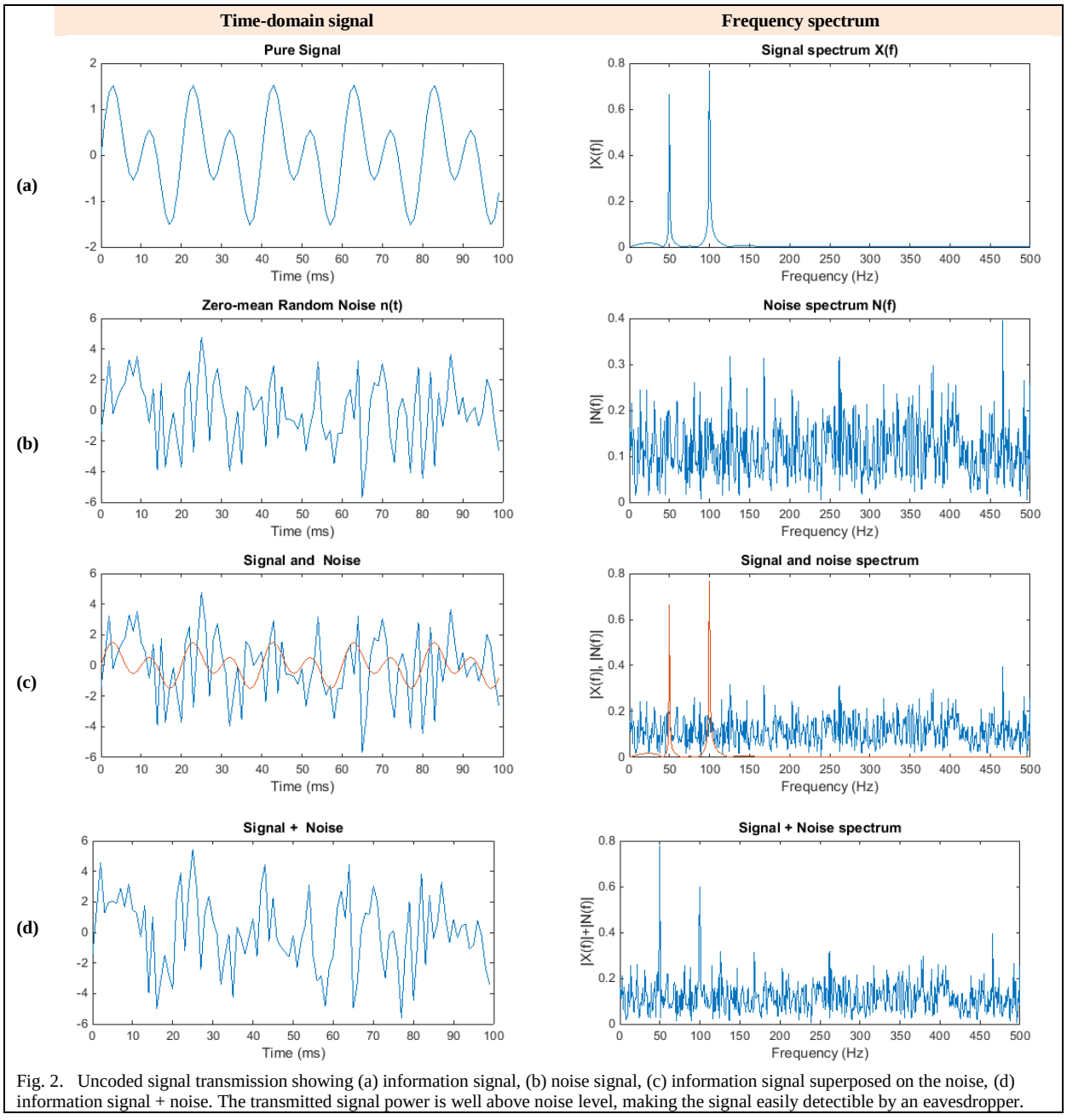

Fig. 2. Uncoded signal transmission showing (a) information signal, (b) noise signal, (c) information signal superposed on the noise, (d) information signal + noise. The transmitted signal power is well above noise level, making the signal easily detectible by an eavesdropper.

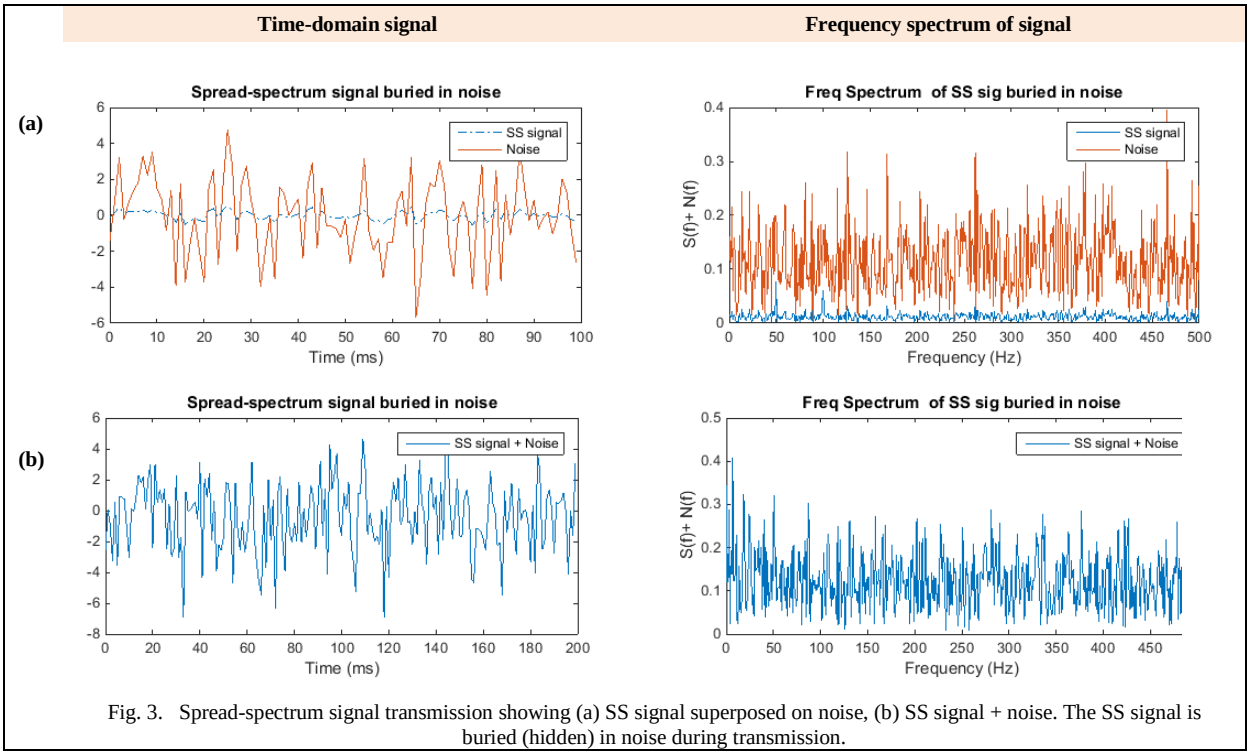

Fig. 3. Spread-spectrum signal transmission showing (a) SS signal superposed on noise, (b) SS signal + noise. The SS signal is buried (hidden) in noise during transmission.

Clearly, the SS signal power is much less than that of the noise. Frequency spectrum (right graph of Fig. 3(a)) shows that the SS power spectral density is much below that of noise

Fig. 3(b) shows a plot of the sum of the signal and the noise. Clearly, this resulting sum-signal looks entirely like noise, and it is difficult to recognise the presence of the actual signal. That is to say, the spread spectrum signal is buried (hidden) in the noise. Therefore during transmission, it is difficult to detect the presence of the actual signal, making it hidden from eavesdroppers.

V. CDMA Performance Curves

Performance curves [17, 18] for a CDMA system gives another way of viewing the information-hiding capability of a CDMA system. Fig. 4 shows the system performance for Gold codes of different lengths N in terms of bit-error-rate (BER) as a function of signal-to-noise ratio (SNR). Here, zero decibel (0 dB) represents the point where signal strength is the same as that of noise. In order words, 0 dB represents the noise level.

Communication systems are normally operated at low BER. Therefore as we look at this performance curves, we shall be focussing on the behaviour at low BER. The right-most curve on the figure is that of uncoded signal transmission. By *uncoded* we mean transmission not involving the use of power is much above noise level. Therefore the signal is easily detectable by eavesdroppers spreading codes. At a BER of 10^{-5}, the uncoded system has an SNR of about 12 dB, which is equivalent to 15.85. That is, the signal power is 15.85 times bigger than the noise power. This implies that for the uncoded signal transmission, the signal power is much above noise level.

Now in Fig. 4, consider the performance curve for the shortest code length (N = 31). For this curve, at a BER of 10^{-5} the system SNR is about -2 dB, which is equivalent to about 0.63. That is, the signal power is about 0.63 times the value of the noise power. This implies that the 31-chip spreading code transmits the signal slightly below noise level. That is to say, the signal is slightly buried in noise.

Extending this treatment to the other code lengths gives a SNR of -8 dB, -14 dB and -21 dB for code length N = 127, 511 and 2047 respectively when BER is 10^{-5}. This implies that for the code length N = 127, 511 and 2047 respectively, the spread spectrum signal is 0.158, 0.040 and 0.008 times the value of

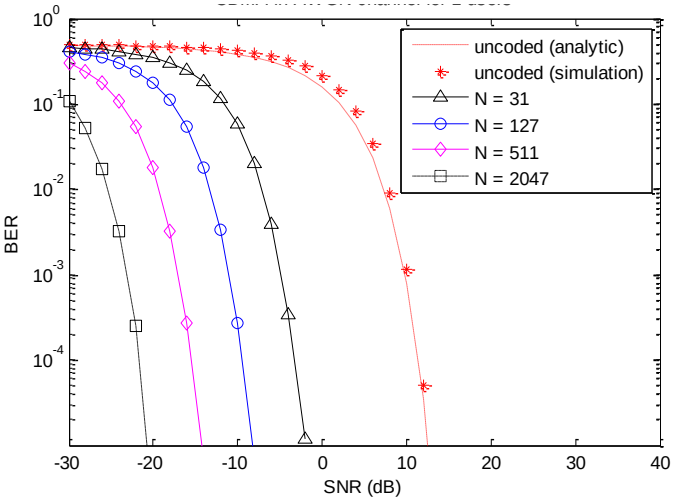

Fig. 4. CDMA performance curves showing the technique's information-hiding capability.

noise power. This clearly shows that the longer the code, the deeper the signal is buried inside noise. For the longest code (N = 2047), the spread spectrum signal is about 0.8% the noise power, meaning that the signal is very much below noise level, thus implying that the signal is deeply buried in noise. Therefore an eavesdropper will not perceive the communication because it is deeply buried in noise. Furthermore, whereas the original information is a narrowband signal, the encrypted version is a wideband signal having a bandwidth much larger than that of the original signal. These make it difficult for a casual observer to detect or jam the signal.

VI. CDMA IN MULTIPLE-ACCESS APPLICATIONS

Though developed originally for the military, CDMA has become an important worldwide technique in wireless communication because of certain properties that makes it attractive for commercial and civilian applications, These properties include: multiple-access capability, enhanced spectral efficiency, frequency diversity, unity cluster size and simplified frequency planning [1, 2, 12, 13, 19, 20]. Statistics [21] show that the number of CDMA subscribers grew from about 7.8 millions in 1997, to about 577 millions in 2010. Viterbi [4] indicates that as at 2002, over one hundred million consumers use devices that employ CDMA technology to provide wireless personal communication or position-location or both. CDMA is the mode of communication in the global positioning system (GPS) [22].

The use of CDMA in mobile telephony and other multiple-access applications is based on properties of spreading sequences. Among other things, orthogonality of spreading sequences is central to the system performance. Members of a set of functions f(x) on a closed interval [a, b] are said to be orthogonal if;

$$\langle f_i, f_j \rangle = \int_a^b f_i(x) f_j(x) dx = \delta_{ij}, \qquad (5)$$

where $\delta_{ij} = \begin{cases} 1 & if\ i = j, \\ 0 & if\ i \neq j. \end{cases}$

Therefore for an othorgonal set of spreading codes C(t) over a period [0,T],

$$\langle C_i, C_j \rangle = \int_0^T C_i(t) C_j(t) dt = \delta_{ij} \qquad (6)$$

Using this relationship reduces equation (4) to:

$$r_1(t) = b_1(t) + n(t) \sum_{i=1}^{N} [c_1(t - iT_c)] \qquad (7)$$

This equation shows for an orthogonal set of codes, multiplying a received signal with the spreading code for a particular user isolates the user's signal from all others. All other signals are suppressed. This equation also shows at the receiving end, the noise term becomes spread out by the user spreading code. By implication, the average noise power density becomes reduced by a factor of the process gain. For example, if the process gain is 1000, the average noise power density becomes reduced by this factor. Thus the noise power is suppressed. That is, the same signal spreading that enhances the desired signal simultaneously suppresses multi-user interference and channel noise.

VII. INTERLEAVE-DIVISION MULTIPLE-ACCESS

We shall now be considering interleave division multiple access (IDMA). IDMA is a relatively recent technique that was first proposed around the turn of the 21st century [23-26] as an alternative to CDMA. As the name implies, IDMA involves the use of interleavers as user-separating element. In IDMA, users are distinguished by user-specific interleavers instead of spreading codes used in CDMA.

In IDMA, signal spreading is avoided. This results in certain benefits which include avoidance of computationally intensive matrix multiplications and matrix inversion, and low-cost iterative multi-user detection [26-30]. However, these attractive features of IDMA are not without a price.

VIII. CDMA VERSUS IDMA IN INFORMATION SECURITY

IDMA is generally believed to be a promising candidate for future wireless technology. In literature, IDMA is usually presented as a better alternative to CDMA. However, it is useful to note that although IDMA has important benefits, it has its drawbacks. The limitations of IDMA are usually ignored in literature.

As stated earlier, CDMA involves signal spreading. The signal spreading requires matrix multiplication and inversion, and these are computationally intensive processes. In IDMA, signal spreading and hence matrix multiplication and inversion are avoided. This has important advantages because it minimises transmission bandwidth and computational requirements [26-30]. Because of these important benefits, IDMA is usually presented in literature as a better alternative to CDMA. For the same reasons, CDMA is also sometimes considered as being outdated and irrelevant to future wireless communication. A careful consideration shows that this is not the case. This is briefly explained as follows.

Signal spreading in CDMA has important advantages, some of which has been highlighted previously in this paper. Signal spreading produces low-level signals, spread out over a wideband. This makes it possible for CDMA systems to co-exist over the same bandwidth alongside with other transmission technologies like the frequency-division multiple-access (FDMA) whose energy is concentrated over a narrowband. This is important because it is a potential means of maximizing the use of the scarce electromagnetic spectrum. In contrast, IDMA does not possess this important benefit simply because of the absence of signal spreading in IDMA.

Apart from this, signal spreading is the secret behind CDMA's capability for covert transmission. This is important from information security's point of view. Signal spreading

results in very weak, low-level, noise-like signals which are difficult to detect. These characteristics can be used for keeping a spread-spectrum signal protected to maintain privacy of transmitted information. Furthermore, because CDMA signals are spread out over a wide frequency band, they are difficult to jam: jamming them requires excessive signal energy. IDMA systems lack these important benefits due to the avoidance of signal spreading in IDMA. Although IDMA has important potential benefits, the benefits are not without a price.

IX. CONCLUSION

Starting from basic principles, this work highlighted the inherent properties of CDMA that enables its use in signal encryption and information security.

This research work also considered the relevance of CDMA and IDMA techniques to information security and future wireless systems. While IDMA have certain desirable properties, it lacks the security features that are inherent in CDMA. Although IDMA has some potential benefits, it is not likely to replace CDMA in future communication systems.

REFERENCES

[1] D. L. Nicholson, *Spread spectrum signal design. LPE and AJ systems*. Rockville, MD, USA: Computer Science Press, 1988.

[2] A. J. Viterbi, *CDMA: principles of spread spectrum communication*: Addison-Wesley Pub. Co., 1995.

[3] A. Viterbi, "Spread spectrum communications--Myths and realities," *IEEE Communications Magazine*, vol. 17, pp. 11-18, 1979.

[4] A. J. Viterbi, "Spread spectrum communications: myths and realities," *IEEE Communications Magazine*, vol. 40, pp. 34-41, 2002.

[5] R. C. Dixon, *Spread Spectrum Techniques*. Canada: John Wiley & Sons Ltd, 1976.

[6] S. H. Mneney, "Wireless CDMA for rural application," in *AFRICON*, Stellenbosch, South Africa, 1996, pp. 408-13.

[7] M. B. Mollah and M. R. Islam, "Comparative analysis of Gold Codes with PN codes using correlation property in CDMA technology," in *International Conference on Computer Communication and Informatics (ICCCI)*, Coinbatore, India, 2012, pp. 1-6.

[8] P. Samundiswary and P. Viswa Kalyan, "Performance Analysis of WCDMA using Different Spreading Codes," *International Journal of Computer Applications*, vol. 38, pp. 8-11, 2012.

[9] G. Suchitra and M. L. Valarmathi, "Performance of Concatenated Complete Complementary code in CDMA systems," in *First UK-India International Workshop on Cognitive Wireless Systems (UKIWCWS)*, 2009, pp. 1-5.

[10] A. Ziani and A. Medouri, "Analysis of different Pseudo-Random and orthogonal spreading sequences in DS-CDMA," in *Multimedia Computing and Systems (ICMCS)*, Tangier, 2012, pp. 558-564.

[11] D. Muirhead and M. A. Imran, "Alamouti Transmit Diversity for Energy Efficient Femtocells," in *73rd IEEE Vehicular Technology Conference (VTC Spring)*, Piscataway, NJ, USA, 2011, p. 5.

[12] R. C. Dixon, *Spread spectrum systems*, 2nd ed. Chichester, Sussex, UK: Wiley, 1984.

[13] R. Prasad, *CDMA for Wireless Personal Communications* Artech House, 1996.

[14] K. Jyostna, F. Fadhil, N. M. Gouri, and B. N. Bhandari, "Performance analysis of SC MIMO-CDMA system using STBC codes," in *11th International Conference on Wireless and Optical Communications Networks (WOCN)*, 2014, pp. 1-5.

[15] V. N. Mohammed, A. Kabra, P. S. Mallick, and L. Nithyanandan, "Multi access interference reduction in STBC MC-CDMA using binary orthogonal complementary sequence," in *International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Ngercoil, India, 2015, pp. 1-4.

[16] C. Bui Quang, Q. Zhang Tian, and J. Wu Wang, "A simplified advantage ACE and PSO algorithm for PAR reduction in STBC MC-CDMA systems," in *12th International Conference on Signal Processing (ICSP)*, 2014, pp. 1637-1642.

[17] O. B. Wojuola and S. H. Mneney, "Multiple-access interference of Gold codes in a DS-CDMA system," *SAIEE African Research Journal*, vol. 106, pp. 4-10, 2015.

[18] O. B. Wojuola and S. H. Mneney, "Performance of even- and odd-degree Gold codes in a multi-user spread-spectrum system," in *4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, Alborg, Denmark, 2014, pp. 1-5.

[19] N. Yee and J. P. Linnartz, "BER of multi-carrier CDMA in an indoor Rician fading channel," in *Proceedings of the 27th Asilomar Conference on Signals, Systems & Computers*, Pacific Grove, CA, USA, 1993, pp. 426-430.

[20] N. Yee, J. P. Linnartz, and G. Fettweis, "Multi-carrier CDMA in indoor wireless radio networks," *IEICE Transactions on Communications*, vol. E77-B, pp. 900-904, 1994.

[21] The CDMA Development Group, "4Q 2010 CDMA Subscribers," Report Dec 2010.

[22] Los Angeles Air Force Base (2011, 27 October). *Fact Sheet: Pseudorandom Noise (PRN) Code Assignments*, Available on http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=8618

[23] W. K. Leung, L. Lihai, and P. Li, "Interleaving-based multiple access and iterative chip-by-chip multiuser detection," *IEICE transactions on communications*, vol. 86, pp. 3634-3637, 2003.

[24] L. Ping, "Interleave-division multiple access and chip-by-chip iterative multi-user detection," *IEEE Communications Magazine*, vol. 43, pp. S19-S23, 2005.

[25] P. A. Hoeher and H. Schoeneich, "Interleave-division multiple access from a multiuser theory point of view," in *4th International Symposium on Turbo Codes & Related Topics; 6th International ITG-Conference on Source and Channel Coding (TURBO-CODING)*, Munich, Germany, 2006, pp. 1-5.

[26] P. Li, L. Lihai, W. Keying, and W. K. Leung, "Interleave division multiple-access," *IEEE Transactions on Wireless Communications*, vol. 5, pp. 938-947, 2006.

[27] M. K. Shukla, A. Gupta, and R. Bhatia, "A Survey on Various Interleavers in Iterative IDMA Communication System," in *International Conference on Special Functions and their Applications in Science and Engineering*, 2011.

[28] P. Li, G. Qinghua, and T. Jun, "The OFDM-IDMA approach to wireless communication systems," *IEEE Wireless Communications*, vol. 14, pp. 18-24, 2007.

[29] R. Gupta, B. Kanaujia, R. Chauhan, and M. Shukla, "Prime number based interleaver for multiuser iterative IDMA systems," in *International Conference on Computational Intelligence and Communication Networks (CICN)*, Bhopal, India, 2010, pp. 603-607.

[30] K. Kusume, G. Bauch, and W. Utschick, "IDMA vs. CDMA: Analysis and Comparison of Two Multiple Access Schemes," *IEEE Transactions on Wireless Communications*, vol. 11, pp. 78-87, 2012.