MESSAGE PROTECTION BY SPREAD SPECTRUM MODULATION IN A PACKET VOICE RADIO LINK

M. Kowatsch, B.O. Eichinger, F.J. Seifert
Technische Universität Wien
A-1040 Vienna, Austria

1. Introduction

In spread spectrum communication systems the bandwidth of the transmitted signal is far in excess of the information bandwidth itself. The spectrum spreading is controlled by a pseudonoise (PN) code. Knowledge of this code allows authorized receivers to process the arriving signal with a significant gain in signal-to-noise ratio by correlating it with a locally generated reference waveform. The inherent interference suppression capability has been the primary motivation for the development of spread spectrum techniques /1/. The two most common forms of spread spectrum modulation are direct-sequence (DS) and frequency-hopping (FH), the first of which is considered in this paper. In DS systems the carrier is phase-modulated by a PN code with a code rate (chip rate) much higher than the data rate. The term 'chip' is used to distinguish between code and data stream. Although the codes most frequently used are not secure in a cryptographic sense, protection against unauthorized message access is associated with the low power spectral density of the wideband DS signals. This attribute applies even more to systems employing non-repeating spreading codes.

This paper describes a DS system for the transmission of packet voice. The next section presents a brief outline of the system concept. In section 3 the leading aspects for the selection of the PN codes are discussed.

2. The System Concept

A block diagram of the system to be considered is shown in Fig. 1. Continuously variable slope delta (CVSD) modulation is used to encode speech signals at 16 kbit/s. The encoder output data stream is split into blocks of 1024 bits. By adding a 14-bit header at the beginning

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 273-277, 1986.
© Springer-Verlag Berlin Heidelberg 1986

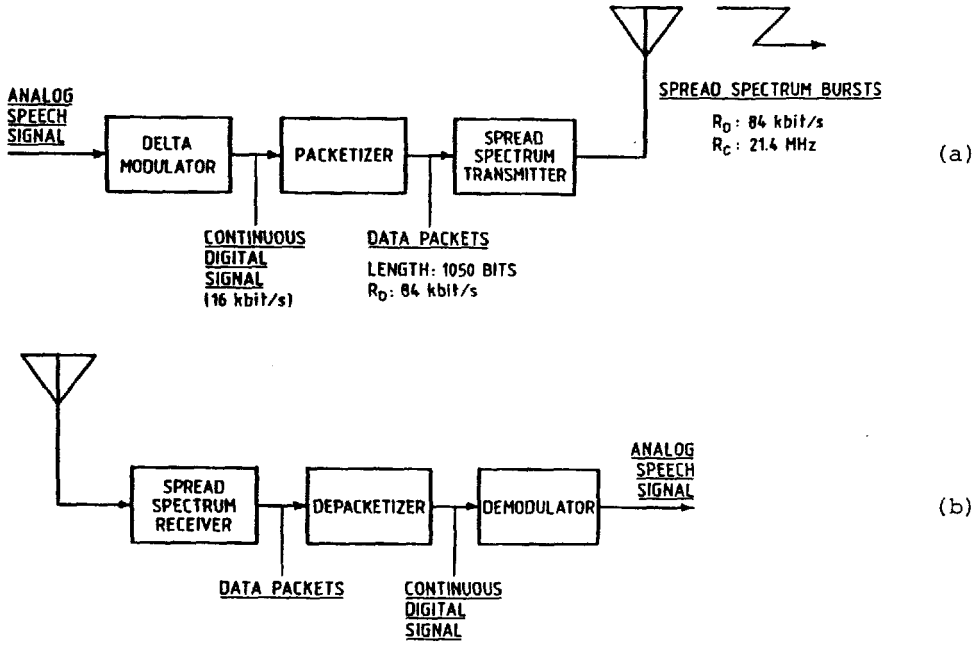

Fig.1: Block diagram of packet voice spread spectrum system
(a) Transmitter
(b) Receiver

and a 12-bit control sequence at the end of each block, data packets with a length of 1050 bits are obtained. These packets are routed to the spread spectrum section and transmitted in bursts at the data rate R_D = 84 kbit/s. For data signalling binary code shift keying (CSK) is employed. That is, ones and zeros of the message are represented by 255-chip PN codes with low crosscorrelation. The resulting chip rate R_C is 21.4 MHz. The spreading code is changed from bit to bit of the data packet. No code is used more than once in any particular burst.

The receiver design is based on the application of surface acoustic wave (SAW) elastic convolvers to programmable matched filtering of the continuously changing PN patterns. The alignment of received signal and local reference is accomplished by means of an 11-bit synchronization preamble preceding each data packet /2/,/3/.

3. Spreading Code Selection

Several aspects have to be considered for the selection of the spreading codes. The first is to make it impossible for unintended parties to predict the PN sequences used to encode future data bits based on the

observation of past code segments. Furthermore, in the present case, each PN pattern used to encode one bit should be easily time-reversible, as the receiver code chips have to be in reversed order, because of the counterpropagation of the two waveforms in the convolver. Finally, for CSK applications, low crosscorrelation of the PN patterns representing ones and zeros, respectively, is of paramount importance. Thus, a large set of PN codes with bounded crosscorrelation is required. Moreover, a code-generation algorithm which allows direct generation of the time-reversed sequences is desirable.

A code set satisfying these conditions is the so-called large set of Kasami sequences /4/. These codes can be generated by modulo-2 addition of the output sequences of three properly selected linear feedback shift registers (LFSR). Two registers have length n, one has length n/2, the period of the resulting codes being 2^n-1 for any even n. The number of sequences in the set is given by

$$K = \begin{cases} 2^{n/2}(2^n+1), & n \equiv 2 \bmod 4 \\ 2^{n/2}(2^n+1)-1, & n \equiv 0 \bmod 4 \end{cases} \qquad (1)$$

In either case, the maximum value of the periodic crosscorrelation function θ is

$$\theta_{max} = 1 + 2^{(n+2)/2} \qquad (2)$$

Of course, (2) does not directly apply to the present case, where the PN pattern is changed from bit to bit of the data stream. However, it is a bound on the crosscorrelation for any two codes of the set in the zero code shift situation at the data decision instant, where periodic and aperiodic correlation values are equal. Thus, it yields an adequate estimate for CSK performance evaluations.

The principle of Kasami sequence generation is illustrated in Fig.2 for the 255-chip codes (n = 8) employed in the modem discussed in this paper. The three basic registers are represented by the polynomials 435E, 675C and 23F in the table of irreducible polynomials by Peterson and Weldon /5/. According to (1) a total number of 4111 different sequences satisfying (2) is available from all combinations of the relative phases of two or three of the fundamental sequences.

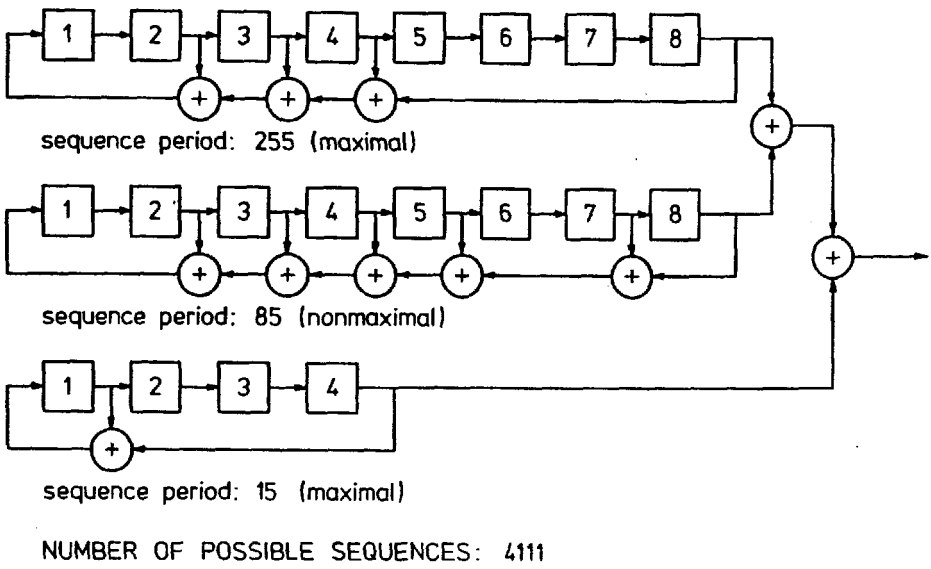

Fig.2: Generation of 255-chip Kasami sequences

The basic unit of the data code generator (Fig.3) is composed of two 8-bit LFSRs and two 4-bit LFSRs. On principle, three registers are required to implement the Kasami sequence generation algorithm, as in Fig.2. Using the two 4-bit registers data modulation is easily accomplished by assigning 7 of the 15 possible initial states for message

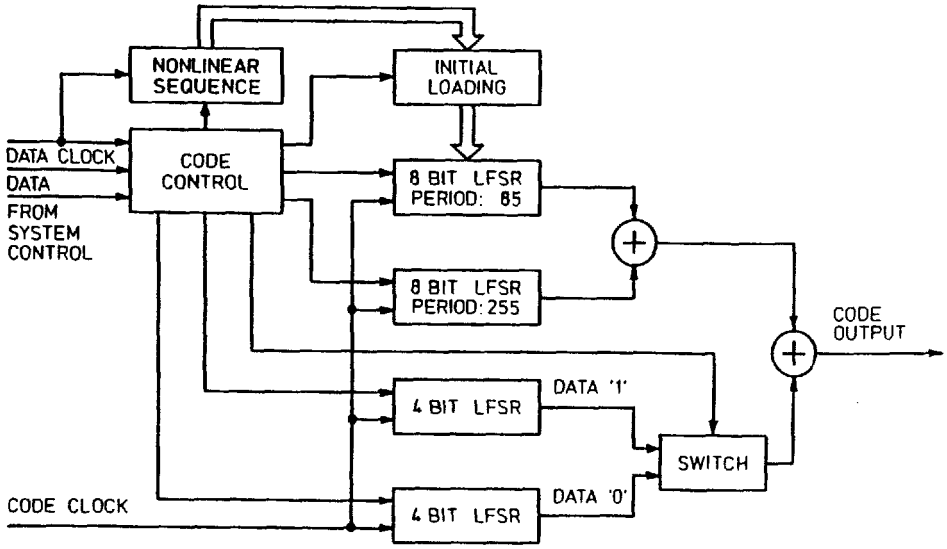

Fig.3: Implementation of code generation and CSK modulation

ones, and 7 for zeros. In order to obtain the large sequence set, the initial state of the 8-bit nonmaximal LFSR with period 85 has to be varied too. This is done under control of a nonlinear code. The applied strategy allows to generate two code sets, each containing 1764 different sequences, for the representation of ones and zeros in the message.

4. Results and Conclusion

A breadboard packet voice spread spectrum modem was built and tested on a simulated additive white Gaussian noise channel, measures of performance being the probability of packet loss and the bit error probability within a packet. The experiments indicated that the system can maintain reliable speech communication at receiver input signal-to-noise ratios down to - 10 dB. This is in good agreement with theoretical predictions /6/.

In conclusion, spread spectrum modulation can be used to reduce the power spectral density of radio signals. This facilitates covert communication with low probability of intercept by unintended parties, provided that the transmission bandwidth is sufficiently wider than the information bandwidth. However, with restricted spreading ratios effective protection against unauthorized information access is still feasible. In the case of CSK signalling with continuously changing codes, as discussed in this paper, the eavesdropper has no realistic chance to determine whether a particular received PN pattern represents a message one or a zero.

References

/1/ R.C.DIXON, Spread Spectrum Systems, 2nd ed., New York: Wiley, 1984.

/2/ M.KOWATSCH, "Synchronization in a Spread Spectrum Communication Modem Based on SAW Convolvers," Proc. 1984 IEEE Military Communications Conference, pp.125-130.

/3/ M.KOWATSCH, "Application of Surface-Acoustic-Wave Technology to Burst-Format Spread-Spectrum Communications," IEE Proc., Vol.131, Pt.F, pp.734-741, Dec.1984.

/4/ D.V.SARWATE and M.B.PURSLEY, "Crosscorrelation Properties of Pseudorandom and Related Sequences," Proc.IEEE, vol.68, pp.593-619, May 1980.

/5/ W.W.PETERSON and E.J.WELDON, Jr., "Error-Correcting Codes," 2nd ed., Cambridge, MA: M.I.T. Press, 1972.

/6/ M.KOWATSCH, "Design of a Convolver-Based Packet Voice Spread Spectrum System," Proc. IEEE 1984 Ultrasonics Symposium, pp.127-131.