· 学术论文与技术报告 ·

Spreading Codes Combined Multiple Access and Encryption for A-CDMA System

Rao Nini

(Dept. of Automation, UEST of China Chengdu 610054)

Abstract In this paper, the requirements for the spreading codes combined multiple access and encryption for CDMA systems are presented using asynchronous direct sequence CDMA (A-CDMA) systems as a model. In order to investigate the effect of this sort spreading codes on operational performance of A-CDMA system, the probability distribution functions of the even cross-correlation functions of the purely random sequences and Gold codes is compared. Finally, some useful conclusions are obtained.

Key words multiple access; encryption; A-CDMA; spreading codes

DS-CDMA systems are often thought of as affording an inherently greater degree of "privacy" than other multiple access systems because an eavesdropper must determine the code used to spread the data and their phase in order to interpret the data intelligibly[1]. However, this assumption can be misleading and the properties of the spreading codes affect not only the operational performance (e.g. bit error rate) of the system, but also the level of confidentiality provided in the absence of any explicit encryption. Several families of codes have been proposed which may have application to combine multiple access and encryption using asynchronous DS-CDMA. These include GMW sequences, bent function sequences and chaotic sequences[2-4]. In this paper, the purely random codes and Gold codes are selected as spreading codes combined multiple access and encryption for A-CDMA system. The probability distribution functions of the even cross-correlation functions of both codes are compared in order to obtain some conclusions for the applications of spreading codes in A-CDMA system.

1 Requirements

In DS-CDMA, the data stream of an individual user is "spread" (at the transmitter) and "despread" (at the receiver) as illustrated in Fig.1. In the asynchronous case, with which we will be concerned, the transmission of the various users are not synchronized with each other at the bit or chip levels.

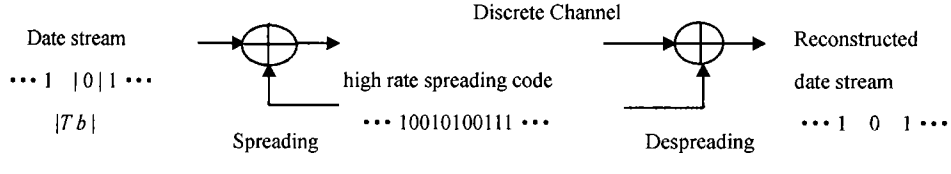

Fig.1 Spreading and despreading in DS-CDMA

A stream cipher system is shown in Fig.2[5]. The analogy with the spread spectrum operation is clear: a spreading code in DS-CDMA is employed in a similar manner to the key stream of a stream cipher. The essential difference is that several chips of the spreading code are added modulo-2 with each data bit in DS-CDMA; only one bit of the key stream is added modulo-2 with each data bit in a stream cipher.

Received September 6, 1999

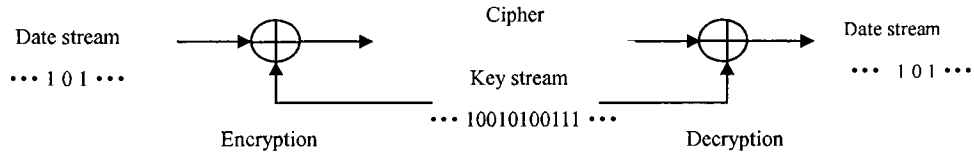

Fig.2 Stream cipher system

Hence, the requirements on codes employed for combined multiple access and encryption using asynchronous DS-CDMA are clearly the union of the operational requirements for spreading codes in DS-CDMA and the security requirements for key streams in stream ciphers. These can be summarized as:

1) Operational requirements[6]

O_1: low auto-correlation for all codes for all shifts not integer multiples of the code length. O_2: low cross-correlation for all code pairs for all shifts. O_3: a large number of codes belong to the family.

2) Security requirements[7]

S_1 extremely long. S_2 statistically indistinguishable from purely random sequences. S_3 generated non-linearly such as to have a very large linear complexity. S_4 possesses a high order of correlation immunity, generated in such a way that a cryptanalyst who knows the generic generation mechanism (but not the key) can obtain only a minimal amount of information.

2 Comparison

The purely random codes and Gold codes can satisfy the above operational and security requirements. In general, the performance of such codes in A-CDMA environment has been evaluated in terms of the even auto and cross-correlation functions. In particular, the bit error rate in an A-CDMA system is directly related to the probability that a given absolute cross-correlation threshold is exceeded (under the assumption of perfect synchronization between transmitter and receiver). In order to investigate this more fully, we compare the probability distribution functions of the even cross-correlation functions for purely random sequences and Gold codes of the same length. Purely random sequences naturally possess the maximum possible peak cross-correlation value, whereas Gold codes were designed specifically to possess a relatively low peak (even) cross-correlation value.

The distribution of cross-correlation values for Gold sequences can be found in Ref.[4]. The probability distribution function for the even cross-correlation function $\theta(\tau)$ of purely random codes is, under weak conditions, given by

$$\rho(\theta(\tau) < x) = \Phi(\frac{x}{\sqrt{n}}) \tag{1}$$

in which τ is a particular relative delay between two codes of length n and Φ is the probability distribution of a random variable distributed according to the standard normal distribution.

While purely random codes can have any arbitrary length, Gold codes are constrained to have a length n of the form $n=2^m-1$(m is a positive integer) and hence any comparison must be constrained to such a value of n. Two distinct comparisons will be made:1) one for $m=m_e$ even with m_e such that $m_e \neq 0 \bmod 4$; 2) one for $m=m_0$ odd with m_0 such that $m_0=m_e+1$.

Fig. 3 compares probability distribution functions for the even cross-correlation functions of Gold and purely random codes for these values of m. In these comparisons, we assume that m and n are

relatively large. Then, the exact even cross-correlation levels for Gold code can be expressed approximately in terms of n as illustrated in Fig. 3[2].

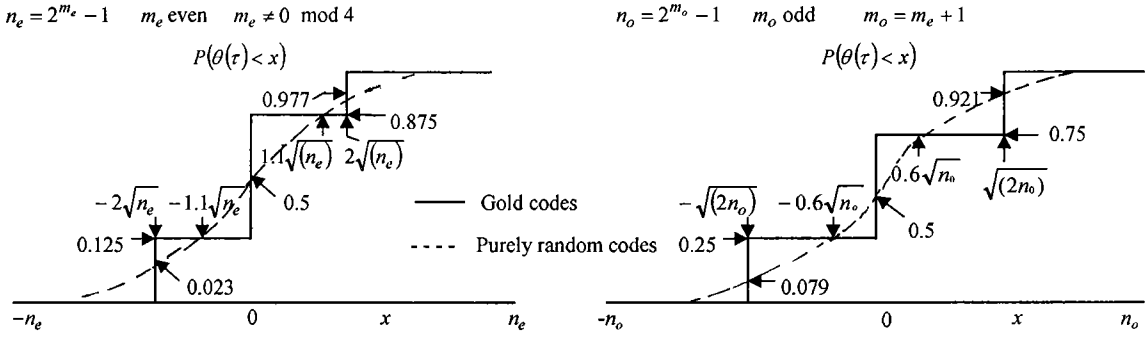

Fig.3　Probability distribution functions for the even cross – correlation functions of Gold and purely random codes

From Fig. 3, it is clear that for

1) $1.1\sqrt{n} < x < 2\sqrt{n}$ in the case of m even and $m \neq 0$ mod 4; 2) $0.6\sqrt{n} < x < \sqrt{2n}$ in the case of m odd.

Purely random codes perform better than Gold codes in which the quantity $\rho(|\theta(\tau)| > x)$ is lower for purely random codes. This is important because under the assumption of perfect synchronization between transmitter and receiver, the probability of error P_e for individual bits on any individual traffic channel in an A-CDMA system which is interference (rather than noise) limited and can be written conceptually as

$$P_e = P(|\theta(\tau)| > x_e(A)) \tag{2}$$

where A represents the instantaneous number of active users in the system. X_e is some strictly monotonically decreasing positive function of A.

In general, the form of the function X_e depends upon the code family employed. This implies that purely random codes will perform better on average than Gold codes for intermediate loading of an A-CDMA system, but worse for relatively low or high loading. However, in the case of relatively low loading, the system will probably be noise rather than interference limited. So Gold codes are only likely to perform better than purely random codes in the case of relatively high loading.

In Ref.[6], it is shown empirically that there is very little variation between calculated mean square cross-correlation values (whether even or odd) pertaining to different code families in spite of the fact that the maximum absolute cross-correlation values for the different families differ considerably. The above result is not unexpected.

3 Conclusion

Code sets specifically designed to facilitate combined multiple access and encryption using asynchronous DS-CDMA are likely to have lower peak (even) auto-correlation values but higher peak (even) cross-correlation values than typical spreading codes employed in conventional asynchronous DS-CDMA systems. The conventional A-CDMA is often thought advantageous from a performance perspective to equalize the peak auto and cross-correlation values as far as possible. However, these considerations do not necessarily imply that combining the multiple access and encryption functions leads to degraded performance. For the purely random sequences, only at high instantaneous loading is the instantaneous performance likely to be worse than system in which the multiple access and encryption

functions are distinct (or where no encryption exists), and the instantaneous performance may even be superior at intermediate instantaneous loading. The situation is just inverse for Gold sequences. Therefore, the different spreading codes have different effects on the bit error rate in an A-CDMA system. The average performance will of course depend upon the offered traffic distribution.

References

1 Dixon R C. Spread spectrum systems with commercial applications, 3rd edition. New York:John Wiley & Sons, 1994

2 Scholtz R , Welch L R . GMW sequences. IEEE Trans-IT, 1984, 30(5): 548~553

3 Olson J D, Scholtz R A, Welch L R. Bent function sequences. IEEE Trans -IT, 1982, 28(6): 858~864

4 Hu J D. CDMA & personal communication. Beijing: Press of People Telecommunication, 1996: 140~148

5 Lu T C. Information encryption technology. Chengdu: Press of Sichuan Science and Technology, 1989

6 Pursley M B, Sarwate D V. Cross-correlation properties of pseudo-random and related sequences. Proc IEEE, 1980, 68(5): 593~619

7 Karkkainen K H A. Mean - square cross-correlation as a performance measure for spreading code families. Proc IEEE Second International Symposium on Spread Spectrum Techniques and Applications, 1992 (ISSSTA '92): 147~150

A-CDMA 系统多址与保密结合的扩频码的研究*

饶妮妮**

(电子科技大学自动化系 成都 610054)

【摘要】 基于一个异步直接序列码分多址模型，给出了多址与保密结合的扩频码应具备的条件。为了研究这类扩频码对 A-CDMA 系统性能的影响，比较了纯随机序列和 Gold 伪随序列的偶互相关概率分布，得到一些有用结论。

关 键 词 多址； 保密； A - CDMA； 扩频码

中图分类号 TN919

1999 年 9 月 6 日收稿

* 国家留学基金管理委员会基金资助

** 女 36 岁 硕士 副教授