Chapter 8

A logistic-Map-Based PN Sequence for Stochastic Wireless Channels

Deb Sunder Swami
Gauhati University, India

Kandarpa Kumar Sarma
Gauhati University, India

ABSTRACT

The work in this chapter mainly focusses on a pseudo-noise (PN) sequence generator which is constructed exploiting the features of one-dimensional chaotic systems such as a logistic map. The use of logistic map to generate strong cryptographic sequences is novel in approach in terms of its use with a range of transmission techniques for wireless communication because it is easy to conceive and requires simple devices to generate the sequence. The generated sequence is used as a spreading sequence in a DS-SS modulation multipath environment with AWGN and Rayleigh fading channel, under various channel fading conditions. The BER curves and channel impulse responses are obtained and compared with the existing linear feedback shift register (LFSR) based PN sequence and Kasami sequence. Results from this comparative analysis indicate that the proposed method generally yields a greater number of reliable, unpredictable and random bits than existing techniques under the same conditions and can be practically implemented for DS-SS scheme as a spreading sequence.

INTRODUCTION

In the era of modern telecommunication technologies, people exchange information with each other via wired or wireless networks. To avoid unauthorized access and illegal usage of information being transferred over the insecure communication channel, securities system are needed to be build and deployed. Most of the security systems rely on the use of cryptographic techniques to provide necessary security to the user’s sensitive data against illegal usage. The challenging task in the design of cryptographic techniques is to generate sequences with high randomness and statistical properties. The quality of the
pseudo-random sequence generated by encryption technique determines its strength from a cryptographic viewpoint. Apart from cryptography, PN sequences are equally applicable and significant in the areas of DS-SS modulation, statistical sampling, computer simulation, (Cruselles, Soriano, and Melus, 1995) etc. The PN sequence generators may be realized in hardware and as well as in software. LFSR based PN sequence generators are well suited for hardware realizations. LFSR based generators are simpler in implementations, have high speed performance and good statistical properties. However, the disadvantage with LFSR based design is that the feedback tapings can be determined under Berlekamp Massey attack (Ahmad and Farooq, 2011). The importance of a careful design of cryptographic PN sequence generators cannot be underestimated as these generators are becoming particularly useful to ensure secure data transmission over an insecure communication channels. Generating high-quality randomness is a vital part of many cryptographic operations.

In the past decade, the behavior of chaotic systems has been much studied and analyzed. According to chaos theory, chaotic systems are nonlinear dynamical systems whose state evolves with time. The future dynamics of these systems are fully defined by their initial conditions. As a result, the behavior of these systems appears random. It has been determined that the chaotic systems have some interesting inherent characteristics such as high dependency on its initial conditions, unstable periodic orbits with long period, ergodicity etc. Due to these characteristics, the chaotic systems are adopted as promising candidates while designing the security systems for text, image, voice, video, etc. (Ahmad and Farooq, 2011). Chaos based encryption methods provides cryptographically better protection than the conventional cryptographic techniques. Keeping these points under consideration, the characteristics of the chaotic systems are exploited to build chaos based PN sequence generator, which can ascertain the excellent statistical and randomness performance. The simple one-dimensional chaotic ‘logistic map’ is integrated to generate the real-valued chaotic sequence, which on pre-processing and quantization gives a PN sequence that has noise-like characteristics. To justify the claim, the statistical, randomness and encryption performance of the proposed chaos-based PN sequence generator is compared with existing LFSR based PN sequence and Kasami sequence.

**BACKGROUND**

A PN sequence can be analyzed for quantitative performance measurements for wireless communication applications. The analysis of a PN sequence includes generation of the sequence, testing its inherent properties and verifying the sequence under some existing criteria. A lot of work has been done on chaos based systems and sequences.

In (Ahmad and Farooq, 2011), the features of one-dimensional chaotic systems are exploited to construct a PN sequence generator by the integration of chaotic logistic maps and cubic maps to generate a strong cryptographic sequence. The proposed system includes the preprocessing and quantization of the real-valued chaotic sequences. The statistical performance of the proposed generator is performed which ascertain that the generated PN sequence has noise-like characteristics. In addition, it is also examined that the proposed chaos-based generator has better statistical and encryption performance than the existing LFSR based generator. In (Cruselles, Soriano, and Melus, 1995) a nonlinear PN generator is proposed that can produce a great number of uncorrelated random sequences with good properties of auto and cross-correlation. Each of these shows good behavior to what is expected for this type of sequence, that is, high unpredictability and good statistical behavior. Moreover, it shows itself to be advantageous for