A Chaos based PN Sequence Generator for Direct-Sequence Spread Spectrum Communication System.

Deb Sunder Swami and Kandarpa Kumar Sarma.

Abstract—In this paper, a pseudo-random noise (PN) sequence generator is constructed exploiting the features of one-dimensional chaotic systems such as the logistic map. The use of logistic map is done in a novel manner to generate strong cryptographic sequence. The method, the logistic map scheme, is applicable for use on wireless networks because it requires simple devices to generate the sequence. The method is shown to achieve reliability from the perspective of communication agents, as well as unpredictability and randomness from the perspective of an eavesdropper. Lastly, the performance of the scheme is compared against that of existing techniques. Results from a 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.

Keywords—DSSS modulation, logistic map, PN sequence, Kasami sequence, AWGN channel, Rayleigh channel, BPSK modulation, QPSK modulation, DPSK modulation.

I. INTRODUCTION

In this era of modern communication 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, the security systems need to be deployed. Cryptographic techniques are used to provide necessary safety 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 proper statistical properties. Pseudo-random sequences, generated by encryption techniques of security systems, quality determine its strength from a cryptographic viewpoint. Apart from cryptography, PN sequences are equally applicable and significant in the areas of directsequence spread spectrum (DSSS), statistical sampling, computer simulation, etc. Linear feedback shift registers (LFSR) based PN sequence generators are very well suited for hardware realizations. LFSR-based generators are simpler in implementations, have high speed performance and satisfactory statistical properties. However, the disadvantage with LFSR based design is that the feedback tapings can be determined under Berlekamp Massey attack. The importance of careful design of PN Sequence generators cannot be underestimated as these generators can be particularly useful to ensure proper spreading of modulated data in directsequence spread spectrum modulation. Generating high quality randomness is a vital part of a PN sequence generator [1][2]. In the recent past, the behavior of chaotic systems has been much studied and analyzed. According to the chaos theory, chaotic systems are nonlinear dynamical systems whose state evolves with time [5]. 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 initial conditions, unstable periodic orbits with long period, ergodicity, etc. Due to these characteristics, chaotic systems are adopted as promising candidates for designing of PN sequence generators. Chaos based encryption methods provide cryptographically better protection than the conventional cryptographic techniques. Keeping these points under consideration, the characteristics of the chaotic systems are exploited to build a chaos based PN sequence generator, which can ascertain excellent statistical and randomness performance. The simple one-dimensional chaotic logistic maps are used to generate real valued chaotic sequences, which on pre-processing and quantization give a PN sequence that has noise-like characteristics [1].

To test the performance, the proposed chaos-based PN sequence is tested on a multipath environment using Rayleigh and AWGN channels with three different modulation schemes, viz. Binary Phase Shift Keying (BPSK) Quadrature Phase Shift Keying (QPSK), and Differential Phase Shift Keying (DPSK) modulation. Rest of the paper is organized as follows: the proposed chaos-based PN sequence generator is discussed in Section II. The Experimental details and the Results are given in Sections III, while the conclusions are drawn in Section IV.

II. PROPOSED LOGISTIC MAP BASED PN SEQUENCE GENERATOR

The one-dimensional logistic map is used to construct the proposed PN sequence generator. The one-dimensional logistic
map is used to produce real-valued chaotic sequences. The simple logistic map is defined by the equation (1).

\[ x(n + 1) = \lambda x(n) (1 - x(n)) \] (1)

Where \( x(0) \) is initial condition, \( \lambda \) is the system parameter and \( n \) is the number of iterations. Theresearch shows that the logistic map is chaotic for \( 3.57 < \lambda < 4 \) and \( 0 < x(n) < 1 \) for all \( n \geq 0 \). As is clear from their state equations, the value of state variable obtained on \( k \)th iteration will acts as seed for the next \( (k + 1) \)th iteration. The dynamical orbits of chaotic maps highly deviated from their normal trajectories, which impart randomness to the generated chaotic sequences. The diagram of the proposed PN sequence generator is shown in Figure 1.

![Figure 1: Proposed PN Sequence Generator](image)

As shown in the Figure 1 above, \( x(0) \) and \( \lambda \) are fed to the system as initial seeds. On each iteration, the real valued state variable \( x_i(n) \) of chaotic map is captured and preprocessed/quantized into a 3-bit value. So, for each real-valued chaotic sequence \( x_i(n) \), we get a binary random sequence \( Z_i(n) \). After the quantization step, the sequence of a predefined length is used for spreading of modulated data.

### A. Direct-Sequence Spread-Spectrum

Direct Sequence Spread Spectrum (DSSS) is a spread spectrum technique whereby the original data signal is multiplied with a pseudo random noise spreading code. This spreading code has a higher chip rate which results in a wideband time-continuous scrambled signal. DSSS significantly improves protection against interfering (or jamming) signals, especially narrowband and makes the signal less noticeable. It also provides security of transmission if the code is not known to the public. The effect is to diffuse the information in a larger bandwidth. Conversely, we can remove the spread-spectrum code (called a despreading operation) at a point in the receive chain before data retrieval. A despreading operation reconstitutes the information into its original bandwidth.

Obviously, the same code must be known in advance at both ends of the transmission channel.

Figure 2 shown below shows a setup of DSSS modulation. Here the logistic map based PN sequence is used for spreading the transmitted data. At the receiver end the same PN sequence is used to despread the data before demodulating it.

![Figure 2: DSSS Modulation Scheme](image)

### B. Validation of Proposed Sequence in DSSS Scheme

To check the performance of the logistic map PN sequence generated, the spreaded data is tested in a multipath environment with Rayleigh and AWGN channel and three different modulation schemes. The comparison is made with Kasami sequence and existing LFSR based PN sequence. In the first simulation, the logistic map based PN sequence is used to spread BPSK modulated data in a multipath AWGN channel. BPSK is a method for modulating a binary signal onto a complex waveform by shifting the phase of the complex signal. In digital baseband BPSK, the symbols 0 and 1 are modulated to the complex numbers \( \exp(j\theta) \) and \( -\exp(j\theta) \), respectively, where \( \theta \) is a fixed angle or the phase offset. The output from the BPSK modulator is multiplied with the logistic map based PN sequence generated to spread the data. Next, the spreaded data is passed through a multipath AWGN channel. The AWGN channel adds white Gaussian noise to a real or complex signal. Then the signal is despreaded and the individual paths are combined in terms of power or gain. The despreaded data is then demodulated using BPSK demodulator. Finally the BER of the signal is calculated. The same procedure is done with the LFSR based PN sequence and Kasami sequence. The BER curves plotted for the three sequences in a SNR range of -10dB to +10dB. The PN sequence generator, generates a sequence of pseudorandom binary numbers using a linear-feedback shift register (LFSR). The LFSR is implemented using a simple shift register generator (SSRG, or Fibonacci) configuration. Kasami sequence is also an PN sequence generated by a polynomial method with good correlation properties.

The above mentioned steps are repeated with QPSK and DPSK modulations. In case of QPSK for input m, the output symbol is \( \exp(j\theta + j\pi m/2) \), where \( \theta \) is the phase offset parameter for input m. The M-DPSK modulates using the M-ary differential phase shift keying method. The M-ary number parameter, M, is the number of possible output symbols that
can immediately follow a given output symbol. The three spreading sequences are used in both modulation schemes and the results compared. In the following section, the experimental setup is provided and the results shown. As will be shown later the logistic map scheme gives better error performance compared to both PN sequence and Kasami sequence. For a Rayleigh channel also the above steps have been carried out. Rayleigh fading models assume that the magnitude of a signal that has passed through such a communications channel will vary randomly, or fade, according to a Rayleigh distribution (the radial component of the sum of two uncorrelated Gaussian random variables.) Here too the logistic map based spreading channel performed on expected lines and better compared to both PN sequence and Kasami sequence.

Next, the characteristics of the generated sequence is tested under different fading channels, viz. slow fading channel, fast fading channel and frequency selective fading channel. The BER curves are generated and their respective channel impulse responses are shown for three different modulation schemes.

III. EXPERIMENTAL SETUP AND RESULTS

The logistic map based PN sequence has been generated using MATLAB and the simulation has been done on Simulink tool. The following initial conditions have been taken for the logistic map: x(0) = 0.1 and \( \lambda = 4 \). The auto-correlation function is one of statistical parameters used to assess the random nature of sequences, it has delta-function form for a perfectly pseudo random noise sequence. The auto-correlation function of PN sequence generated is shown in Figure 3. It is clear from the figure that sequence generated by the proposed generator has moderate autocorrelation function form.

Figure 3: Autocorrelation Function of PN Sequence Generated

Using Simulink, the blocks have been arranged using standard communication criteria and all the three spreading sequences (logistic map PN sequence, LFSR based PN sequence and Kasami sequence) have been tested in same conditions. The BER values for a SNR range of -10dB to +10dB have been obtained. The obtained BER values are then plotted using MATLAB.

For calculating BER 2400 samples have been compared. The BER curve for BPSK modulation in AWGN channel with comparison between three spreading sequences is provided in Figure 4. It is obvious from the figure that the logistic map PN sequence has better error performance compared to the LFSR PN sequence and Kasami Sequence.

In the next setup the modulation scheme that is used is QPSK. Here also the same conditions have been used for the three spreading sequences.

Figure 4: BER curve for BPSK Modulation.

Similarly, in the third setup, DPSK modulation scheme has been used using the same conditions. Figure 6 shows the BER curve obtained from the setup. Again the logistic map PN sequence provides comparatively better error performance than the Kasami and LFSR PN sequence. However, here the
overall system performance is slightly degraded due to the differential modulation scheme used.

Figure 6: BER curve for DPSK Modulation.

As is obvious from the curves shown above, the logistic map PN sequence provides better error performance in a multipath environment.

In the next setup a Rayleigh fading channel has been added to the model. The Rayleigh channel adds fading noise to the signal, and it accepts only complex inputs. For simulation simplicity the complex phase gains have been removed to maintain uniformity and multipath have been added externally. Rest of the criteria has been kept same as the previous model. The simulations were done for BPSK, QPSK and DPSK modulation schemes. The error performance for logistic map PN Sequence, LFSR PN sequence and Kasami sequence has been compared. Their respective BER has been plotted.

Figure 7 shows the BER curve for BPSK modulation in Rayleigh channel. It can be seen that the logistic map PN sequence clearly gives better error performance than the other two spreading sequences. But due to the presence of Rayleigh channel the fading is flat and the overall system performance degrades to some extent.

In the next simulation, QPSK modulation scheme has been used. Here also the same conditions have been used for the three spreading sequences. Figure 8 shows the BER curve obtained. Here also it is clear that logistic map PN sequence provides comparatively better error performance and the overall performance remains same. The LFSR PN sequence and the Kasami sequence have similar error performance.

Figure 7: BER curve for BPSK Modulation in Rayleigh Channel.

Figure 8: BER curve for QPSK Modulation in Rayleigh Channel.

Figure 9: BER curve for DPSK Modulation in Rayleigh Channel.
In the final simulation DPSK modulation scheme has been used using the same conditions. Figure 9 shows the BER curve obtained from the setup. Again the logistic map PN sequence provides better error performance than the Kasami and LFSR PN sequence.

From the above simulations it is clear that the proposed logistic map based PN sequence gives better error performance than both LFSR based PN sequence and Kasami sequence. A comparison was also made with Hadamard code and BER performance obtained for the logistic map PN sequence was much better than the Hadamard code.

In the next setup the fading characteristics of a wireless communication channel is verified using the logistic map based spreading sequence. The different fading characteristics tested are as described below.

A. Fading Channels
The type of fading experienced by a signal propagating through a mobile radio channel depends on the nature of the transmitted signal with respect to the characteristics of the channel. Depending on the relation between the signal parameters (such as bandwidth, symbol period, etc) and the channel parameter (such as RMS delay spread and Doppler spread), different transmitted signals will undergo different types of fading. The time dispersion and frequency dispersion mechanisms in a mobile radio channel lead to four possible distinct effects, which are manifested depending on the nature of the transmitted signal, the channel, and the velocity [6].

- Flat Fading: If the mobile radio channel has a constant gain and linear phase response over a bandwidth which is greater than the bandwidth of the transmitted signal, then the received signal will undergo flat fading. In flat fading, the multipath structure of the channel is such that the spectral characteristics of the transmitted signal are preserved at the receiver. However, the strength of the received signal changes with time, due to fluctuations in the gain of the channel caused by multipath. Flat fading channels are also known as amplitude varying channels and are sometimes referred to as narrowband channels, since the bandwidth of the applied signal is narrow as compared to the channel flat fading bandwidth.

- Frequency Selective Fading: If the channel possesses a constant gain and linear phase response over a bandwidth that is smaller than the bandwidth of the transmitted signal, the channel creates frequency selective fading on the received signal. Under such conditions the channel impulse response has a multipath delay spread which is greater than the reciprocal bandwidth of the transmitted message waveform. Whenit occurs, the received signal includes multiple versions of the transmitted waveform that are attenuated and delayed, and hence the received signal is distorted. For instance, the fading type in a GSM system is frequency selective.

- Fast Fading: In a fast fading channel, the channel impulse response changes rapidly within the symbol duration. That is, the coherence time of the channel is smaller than the symbol period of the transmitted signal. Viewed in the frequency domain, signal distortion due to this increases with increasing Doppler spread relative to the bandwidth of the transmitted signal.

- Slow Fading: In a slow fading channel, the channel impulse response changes at a rate much slower than the transmitted baseband signal S(t). In the frequency domain, this implies that the Doppler spread of the channel is much less than the bandwidth of the baseband signals.

The above mentioned characteristics of a wireless communication channel were tried using the logistic map based PN sequence in a Rayleigh fading channel. The BER curves and the channel impulse responses shown below justify the characteristics for the above mentioned channels. For modeling slow fading and fast fading channels, Doppler frequencies of 10 Hz and 110 Hz have been used respectively. For modeling a frequency selective fading channel, a delay vector with different delays and path gains has been used.

The BER performance of slow fading channel is marginally better because of the dependence on the lower Doppler frequency value, shown in Figure 10.

Figure 10: BER curve showing flat fading versus slow fading for BPSK.

The channel impulse response of both the cases is shown in Figure 11 and Figure 12 below which showed that in a fast fading channel, the channel impulse response changed at a much faster rate compared to a slow fading channel.

The BER curves shown in Figure 13 show that frequency selective fading is the worst case scenario and as such a
equalization technique has been used to compensate for the performance.

Figure 11: Channel Impulse response for slow fading channel.

Figure 12: Channel Impulse response for fast fading channel.

Figure 13: BER curve showing frequency selective fading.

For a frequency selective fading case the channel impulse response is shown in Figure 14. The impulse response has a multipath delay spread which is greater than the reciprocal bandwidth of the transmitted message waveform. When it occurs, the received signal includes multiple versions of the transmitted waveform that are attenuated and delayed, and hence the received signal is distorted.

The same procedures were carried for QPSK and DPSK modulation schemes as well. For QPSK modulation, Figure 15 shows slow fading and fast fading channel BER curves. Here as well, the slow fading channel has significantly better error performance compared to a fast fading channel because signal distortion due to fast fading increases with increasing Doppler spread relative to the bandwidth of the transmitted signal.

Figure 14: Channel Impulse response for frequency selective fading channel.

Figure 15: BER curve showing flat fading versus slow fading for QPSK.

Their respective channel impulse responses are shown in Figure 16 and Figure 17 where it was observed that in a fast fading channel the channel impulse response changed at much faster rate compared to slow fading channel. Similarly for QPSK, the BER curve for frequency selective fading channel
is shown in Figure 18 which presents the worst casescenario. As such equalization is used to improve the BER performance. The channel impulse response is shown in Figure 19, under this condition the channel impulse response had multipath delayspread.

Figure 16: Channel Impulse response for slow fading channel.

Figure 17: Channel Impulse response for fast fading channel.

Figure 18: BER curve showing frequency selective fading.

The above procedures were carried for DPSK modulation schemes too. For DPSK modulation, Figure 20 shows slow fading and fast fading channel BER curves. Here as well, the slow fading channel has better error performance compared to a fast fading channel because signal distortion due to fast fading increases with increasing Dopplerspread relative to the bandwidth of the transmitted signal.

Figure 19: Channel Impulse response for frequency selective fading channel.

Figure 20: BER curve showing flat fading versus slow fading for DPSK.

Their respective channel impulse responses are shown in Figure 21 and Figure 22 where it was observed that in a fast fading channel the channel impulse response changed at a faster rate compared to slow fading channel. It is clear that the velocity of the mobile (or velocity of objects in the channel) and the basebandsignaling determines whether a signal undergoes fast fading or slow fading.
Similarly for DPSK, the BER curve for frequency selective fading channel is shown in Figure 23 which presents the worst case scenario, as such equalization is used to improve the BER performance. The channel impulse response is shown in Figure 24, under this condition the channel impulse response had multipath delay spread.

From the above simulations we can say that when a channel is specified as a fast fading or slow fading channel, it does not specify whether the channel is flat fading or frequency selective fading in nature. Fast fading channel only deals with the rate of change of the channel due to motion. Hence a flat fading, fast fading channel is a channel in which the channel impulse response is approximated to be a delta function (no time delay). In case of frequency selective channel, the amplitudes, phases, and time delays of any one of the multipath components vary faster than the rate of change of the transmitted signal [6].

In the final simulation a comparative study has been done between logistic map based spreading sequence, LFSR based PN sequence and Kasami sequence under slow and fast fading channels conditions. The BER curves for slow and fast fading channels are shown Figures 26 and 27. It is clear from the Figures shown below that the logistic map based spreading sequence performs better than both the LFSR based PN sequence and Kasami sequence.
A logistic map based PN sequence generator is proposed in this paper. The generator employed one-dimensional chaotic logistic map to generate a PN sequence. The generated sequence was used as a spreading sequence in a direct sequence spread spectrum modulation multipath environment with AWGN and Rayleigh fading channels. The BER curves were obtained and compared with the existing LFSR-based PN sequence generator and Kasami sequence. The comparative study reveals that proposed generator performs better than both. The generated sequence was then tested under various channel fading conditions. Their respective BER curves and channel impulse responses were generated and upon comparison with theoretical standards, the sequence was found to perform under expected lines. Also, a comparative study was done between logistic map based PN sequence, LFSR based PN sequence and Kasami sequence under slow and fast fading conditions. The BER curves obtained showed that the logistic map based PN sequence performed better than both the other sequences. Hence, we can say that the PN sequence generated is cryptographically strong and can be applied for Direct Sequence Spread Spectrum (DSSS) Modulation.

REFERENCES


Deb Sunder Swami is presently working has Assistant Professor, Department of Electronics and Telecommunication Engineering, Royal School of Engineering And Technology, Guwahati, Assam, India. He has two international conference publications and several other publications.

Kandarpa Kumar Sarma is currently with the Department of Electronics and Communication Technology, Gauhati University, Guwahati, Assam, India serving as Associate Professor. He obtained MTech from Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, Assam, India in 2005 and later PhD from the same institute. His areas of interest include MIMO system, mobile and wireless communication, soft computing, speech processing, antenna design and document image analysis. He is a senior member of IEEE (USA) and fellow of IETE (India). He is an author of seven books, several research papers published in peer reviewed international journals and conference proceedings. He serves as reviewer to over thirty international journals, and has been TPC member/reviewer of over hundred international conferences.

V. VI REMARKS

This paper is an extended version of the conference paper published in the proceedings of 1st WSEAS International Conference on Wireless and Mobile Communication (WMCS), Paris, October, 2013, Paper Id: 70801-112 (8209).

VI. APPENDIX

Figure 27: System model for AWGN Channel.

Figure 28: System model for Rayleigh Channel.