An Approach for Secure Communication by Chaos-Based Cryptosystem

Mr.V.Narsing Rao[1], Dr.K.Bhargavi[2], Dr.Ramachandra Reddy[3]

[1,2,3] *Department of Computer Science and Engineering, Sphoorthy Engineering College, Nadergul, Hyderabad*

Abstract- **There is a great interest in secure communications within industry and various sectors of society. It has been found that chaotic systems and cryptosystems share many similar properties. For instance, chaotic systems are sensitive to the initial conditions, which correspond to the diffusion property of good cryptosystems. In this paper we describe a technique for transmitting digital information using pseudo chaotic carrier. The pseudo chaotic sequences are used as spreading codes to encode each user's message. The user's message can again be separated by the orthogonal property of chaotic sequences at the receiver. Chaos-based communication systems offer higher security**

Index Terms- **chaos, pseudo chaotic carrier, chaotic function, NLFSR, PCS.**

1. INTRODUCTION

Cryptography is the science of protecting the privacy of information during communication under hostile conditions. In the present era of information technology and proliferating computer network communications, cryptography assumes special importance. Cryptography is now routinely used to protect data, which must be communicated and/or saved over long periods, to protect electronic fund transfers and classified communications .

Current cryptographic techniques are based on number theoretic or algebraic concepts. Chaos is another paradigm, which seems promising. Chaos is an offshoot from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems, both man-made and natural, are being investigated using this novel approach of nonlinear dynamics. The chaotic behavior is a subtle behavior of a nonlinear system, which apparently looks random. However, this randomness has no stochastic origin. It is purely resulting from the defining deterministic processes. The important characteristics of chaos are its extreme sensitivity to initial conditions of the system .

2 NEED OF CHAOS BASED COMMUNICATION

It was realised in the early 1990's that securing communications could be a potential application emerging out of studies on chaos theory. This was based on the discovery of chaotic synchronization principles, by Pecora & Carroll. These works motivated communication and signal processing engineers and scientists to look into this. The defining properties of chaotic dynamics, namely, ergodicity, sensitivity on initial conditions and system parameters, are in fact the key features contributing towards building up of secure communication schemes based on chaos. In this context, many hardware circuits were proposed and built [3],[4]. Interest in chaos based systems as an alternative to the existing schemes, such as RSA/ECC etc., in cryptography is increasing in the past few years. The subtle chaotic behavior can be simulated in the simplest of one or two dimensional systems represented by discrete maps or in higher dimensional physical systems described by three or more first order autonomous differential equations or two or more first order ordinary non-autonomous differential equations.

A large number of chaotic systems, both physical and mathematical, are now available which could potentially serve as both hardware and software equipments for realising encryption and decryption of messages.

In chaotic synchronization of analog devices, the stability and drifts are important practical hurdles, which are to be overcome before application of synchronization-based schemes for cryptography. In contrast, a software approach becomes more practical and in tune with present day advances in information processing. A synchronization based scheme involves the chaotic signal carrier which is prone to cryptographic attack, via a possible break of cipher using reconstruction dynamics approach.

Chaos based cryptography is an approach to enhance security of the scheme by providing larger key space, protection against reconstruction dynamics and resistance from statistical attack . Proving the security of encryption based on chaos is still an open topic because one cannot use the analytical methods of classical cryptography which are based on number theoretic concepts or hardness of discrete logarithmic problem, etc.

In this paper we had given an approach of design of cryptographic system for secured transmission of digital data using pseudo chaotic carrier sequence. Pseudo chaotic sequence is used as a key to encrypt a digital message. For decryption same pseudo-chaotic sequence is used. The pseudo-chaotic sequence generators are in the class of Non Linear Feedback Shift Registers (NLFSR). VHDL language was used for entire design. Simulation was carried out using active HDL and the design was targeted to targeted to Xilinx's Spartan3 device xc3s250e-4-tq144

3. CHAOS-BASED SECURE COMMUNICATION ARCHITECTURE

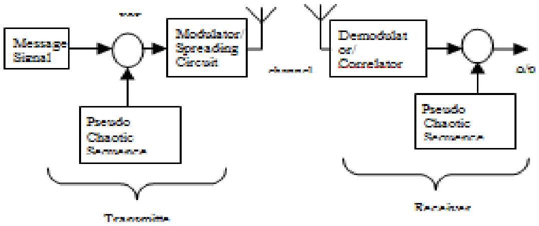

Fig 1: Chaos-based Secure Communication Architecture

Spread spectrum techniques for digital communication were originally developed for military applications because of their high security and their susceptibility to interference from other parties . Now a day spread spectrum techniques are being used in variety of commercial applications such as mobile and wireless communication. In order to spread the bandwidth of the transmitting signals, the binary Pseudo Noise (PN) sequences have been used extensively in Spread Spectrum (SS) communication systems. One of the most commonly used PN sequence in DSSS is maximal length sequences (m-sequences). The length of m-sequences depends on the number of shift registers. Good correlation properties can be achieved with m-sequences. The ability to predict future sequence is nevertheless possible though difficult. Therefore transmission is not completely secured [9]. The use of chaotic sequences (chaos-based) as spreading sequences has been proposed in the literature because of its sensitivity to initial conditions and has characteristics similar to random noise.

4 DESIGN DETAILS

Pseudo Chaotic Sequence Generator

Pseudo noise is defined as a coded sequence of 1's and 0's with certain auto-correlation properties . The class of sequences used in spread spectrum communication is usually periodic in that a sequence of 1's and 0's repeats itself exactly with a known period.

The highlight of this paper is the PCS Generator, which generates a pseudo-chaotic sequence with good cross-correlation and auto-correlation properties that is well suited for this system. Because of long periodicity, it provides very high security and is capable of handling many users. It consists of a cascade of four basic cells with two 8-bit programmable registers each. The output of the last cell i.e. each bit of the last cell output are XORed together to obtain pseudo-chaotic sequence and also this bit is fed back to the system to maintain nonlinearity. By increasing number of cells and size of the registers, one can further increase the number of users and period of the sequence. Since the number of implementation possibilities are very high due to initial condition programmability, this new class of sequence is inherently more difficult to intercept .

Non linear feed back shift register cell is basic building block of pseudo-chaotic sequence generator. The pseudo-chaotic sequence generator consists of such four non linear feed back shift register cells cascaded with each other.

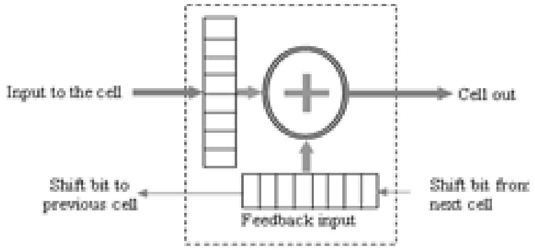

Fig 2: Basic NLFSR Cell Structure

Fig 2 shows a basic NLFSR cell, each cell consists of two 8-bit registers and a XOR function block. Initial conditions are set to both the registers. The contents of the two registers are XORed to obtain 8-bit output Cell out, which is used as input to the upper register of the next cell. The contents of the two registers are altered for the next iterations by shifting the contents of the lower register towards left. The most significant bit that shifts out of the register is loaded into the least significant bit place of the feedback register of the previous cell. Similarly, the shifted bit from the next cell is moved into most significant bit place of the lower (feedback) register. The contents of the upper register are replaced by the 8-bit output of the previous cell. The PCS generator used in this paper consists of four such cells connected in series as shown in fig 3.

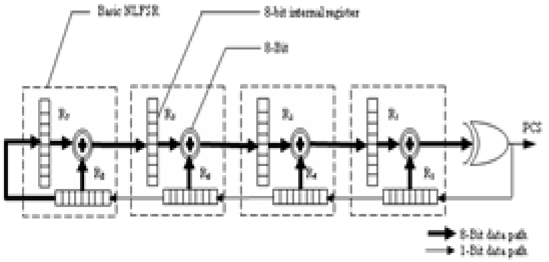

Fig 3: Pseudo Chaotic Sequence Generator

Several chaotic trajectory pairs were generated. The two trajectories with very close initial condition have been observed to diverge quickly and remain that way for large number of iterations, indicating the sensitive dependence on initial conditions. Next, to assess the performance of the PCS generator, the output sequences have been characterized with respect to their auto-correlation, cross-correlation and balance properties.

The PCS generator contains eight 8-bit registers. These registers provide a total of 64 binary memory elements. Therefore, the PCS generator can be viewed as a sequential state machine with at most 264 possible states. The initial values to these registers can be initialized individually.

Transmitter

The structure of the transmitter mainly consists of CPSK modulator, multiplier and PCS generator. In this system, the data bits are spread using PCS sequence which are generated using PCS generator. To generate PCS sequence, one need to initialize the 8 bit registers R1 to R8 of PCS generator. After receiving one bit input the PCS generator is enabled and it starts generating PCS sequence. One bit of the input is transferred to multiplier where it is multiplied by the first 32-bits of generated PCS sequence resulting in 32-bits of spread sequence and the same is transmitted. After the first data bit is spread by 32-bits of PCS sequence, the second data bit is received in the multiplier and is multiplied by the next 32-bits of the PCS sequence.

The output of a multiplier is a scrambled output. The scrambled output is nothing but the encrypted message

Receiver

The receiver consist detector, control circuit, PCS generator and demodulator. The receiver works in 3 phases: the training phase, the detection phase, and the despreading phase. Before the training phase, the 8 bit registers R1 to R8 are again initialized with the same initial values used in the transmitter.

During the training phase the Detector/correlator is initialized with a training sequence i.e., the first 32 bits of the PCS are loaded into the lower registers. A prototype of eight bit correlator is as shown in fig 4.

In the detection phase, the received data of 32 bits are loaded into the upper register of detector. This register is compared with lower register of detector. Upon reaching a certain threshold value, the detector sends a signal. The occurrence of this signal marks the end of the detection phase and start of the dispreading phase.

In de-spreading phase the detector output is shifted to the de-spreader where the incoming wideband data stream is multiplied by the sequence from the local PCS generator.

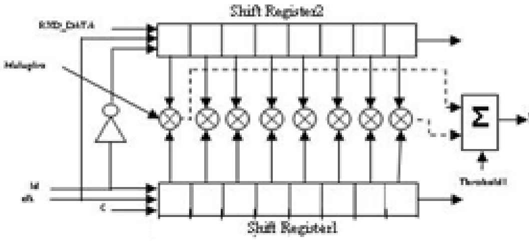

Figure 4: Eight bit Correlator

Detector/ Correlator

This system uses a technique called correlation for detection and synchronization of the system. The device used is called correlator or detector. The detector at the receiver detects the signal from the transmitter and to achieve synchronization between the transmitter and receiver during the communication system that uses chaotic sequence.

A prototype of eight bit correlator is as shown in figure 4. The detection of signal from the intended transmitter at receiver and to achieve the synchronization between them is very important in this system especially when the system uses pseudo-chaotic sequence.

The 32-bits of the PCS generator are loaded in to the Shift Register1. The 32-bits of received output from transmitter are loaded in Shift Register2. Each bit of shift register1 with the corresponding bits of shift register2 and the summer sums up the output of the bit wise multiplier. If the sum exceeds the threshold value, it decides that the received bit is 1 else 0.

5 SIMULATION RESULT

The Fig. 5 shows the simulation result of Pseudo-Chaotic Sequences (PCS) Generator

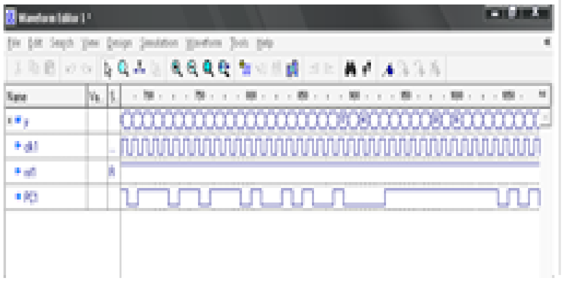

Fig. 5: Pseudo-Chaotic Sequences

A pseudo-Chaotic sequence shown above is generated by initially loading 01110001 in all the eight registers of PCS generator.

The Fig. 6 shows the simulation result of transceiver. From fig 6 it can be seen that final output is same as massage in.

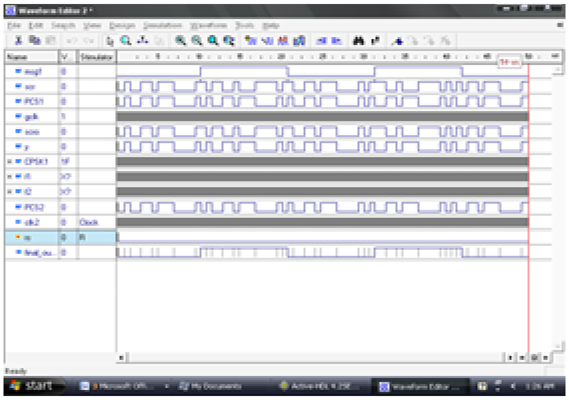

Fig. 6: Transceiver Output

The complexity of PCS based digital data communication system is more as compared to PN based digital data communication system because the generation of PCS sequence is complex. Also the synchronization of transmitter and receiver to get back the transmitted signal in case of PCS based digital data communication system is not so easy as compared to PN based digital data communication system. The security of PCS based digital data communication system is better than the PN based digital data communication system.

6 CONCLUSIONS

The initial conditions of the sequence generators used in this paper can be randomly selected to produce pseudo-chaotic sequence with good correlation properties. The family of pseudo-chaotic PN sequences proved better correlation properties than conventional m-sequences. Pseudo-chaotic sequence generation with its robust digital implementation avoids many difficulties associated with analog chaotic circuits. The large set of system parameters (initial conditions and internal configuration of cells and generators) and the non-linear nature of the feedback generation circuitry lead to potential applications for programmable secure communication systems. Results have shown that, using random selections of initial conditions can provide pseudo-chaotic sequences that are relatively long with good correlation properties. Since the number of implementation possibilities is very high due to initial condition which can be made software controlled and this new class of sequences is more difficult to detect.

REFERENCES

[1] Q.V. Lawande, Theoretical Physics Division and B. R. Ivan and S. D. Dhodapkar, Reactor Control Division, "CHAOS BASED CRYPTOGRAPHY : A NEW APPROACH TO SECURE COMMUNICATIONS", BARK Newsletter, No:258, July 2005

[2] L.M.Pecora and T.L.Carroll, "Synchronization in Chaotic Systems", Phys. Rev Lett, Vol. 64, (1990) 821.

[3] L. J. Kocarev, K. S. Halle, K. Eckert, U. Parlitz, and L.O. Chua, "Experimental demonstration of secure communications via chaotic

synchronization", Int. J. Bifur. Chaos 2(1992) 709-713.

[4] "Chua's Circuit : A Paradigm for Chaos"; Madan R.N.(Ed.); World Scientific, Singapore, 1993

[5] P. G. Vaidya, "A new method to embed time series data and for parameter identification", J. Indian Inst. Science, Vol78, (1998) 257.

[6] Bernard Sklar, "Digital communication. Fundamentals and Applications". Prentice Hall. (2001)

[7] G.Heidari-Bateni, C.D.McGillem, "Chaotic sequences for spread spectrum: An alternative to PN-sequences", Proc. IEEE ICWC-92 437C440(1992)

[8] G.Heidari-Bateni, C.D.McGillem "A chaotic direct sequence spread spectrum communication Systems", IEEE Trans.Commun.42(3):1524-1527(1994)

[9] Y. Soobul, K.Chady, Harry C.S Rughoopath, "Digital chaotic coding and modulation in CDMA", Proc. of IEEE Africon 841-846 (2002)

[10] D. Leon, S.Balkir,M.W.Hoffman, l. C. Perez, "Pseudo-chaotic PN sequence generators circuits for SS communication", Proc. of IEE-Circuits Dev. Syst.151(6):543-550(2004)