BIT ERROR RATE MEASUREMENT FOR WIRELESS COMMUNICATION SYSTEM BY VLSI

Padma Priya. B., Bino Wesley, R and R.Hema

Dept. of Electronics and Communication Engineering

Madha Engineering College, Kundrathur, Chennai- 69, Tamil Nadu, India

ABSTRACT

This paper presents the Bit Error Rate (BER) performance of the wireless communication system. The complexity of modern wireless communication system are increasing at fast pace. It becomes challenging to design the hardware of wireless system. The proposed system consists of MIMO transmitter and MIMO receiver along with the along with a realistic fading channel. To make the data transmission more secure when the data are passed into channel Crypto-System with Embedded Error Control (CSEEC) is used. The system supports data security and reliability using forward error correction codes (FEC). Security is provided through the use of a new symmetric encryption algorithm, and reliability is provided by the use of FEC codes. The system aims at speeding up the encryption and encoding operations and reduces the hardware dedicated to each of these operations. The proposed system allows users to achieve more security and reliable communication. The proposed BER measurement communication system consumes low power compared to existing systems. Advantage of VLSI based BER measurement it that they can be used in the Real time applications and it provides single chip solution.

Keywords: Crypto-System, FEC codes, BER, CSEEC.

INTRODUCTION

Monte Carlo (MC) simulation techniques have been widely used to generate BER versus a range of expected signal-to- noise ratio (SNR) conditions. However, the execution times of software-based MC simulations of the baseband layer on workstations can be extremely long, especially for increasingly complex communication systems (1). Bit error rate (BER) characteristic is one of the basic measures of the performance of any digital communication system. Bit error rate (BER) is the ratio of the number of incorrect to the total number of received bits. The proposed BER measurement system consists of transmitter and receiver. The proposed wireless communication system consists of transmitter and receiver. The transmitter part consist of encoder, interleaver and modulator. The receiver part consists of ML detector, deinterleaver and decoder. There are two modes of operation in interleaver Read after write at the transmitter side and Write after read at the receiver side (2). LFSR is used to generate the PN sequence. To make the transmitted data more secure encryption and decryption process are followed.

ENCRYPTION

To encrypt, start by permuting the bits of the input block using the permutation array 1. Figure 3 illustrates how a permutation array is applied to a small input block of size3X3.Then the Permuted data are converted into Parallel to serial data because Manchester encoder accepts only the serial data. After encoding the serial data those data are converted into serial to parallel. The fig.1 illustrate how the encryption process is performed (3). Using a LFSR a random sequence are generated The objective of performing the XOR operation after encoding and before deletion is to increase the complexity of the PRNG cryptanalysis in this case, part of the generator output will be deleted and there is no way to recover what is deleted especially when is not protected by the

correction code. Thus, an attacker will not have a continuous output sequence from the PRNG. Therefore, he will not have reliable knowledge as a basis for his cryptanalysis. At the end of processing each block, a new set of permutation is generated. This new set allows different columns to be deleted as well as different bit permutations to be performed every time a block is encrypted. The new set is derived from the existing set using the encryption key. The encrypted data is given as the input forthe encoder in the wireless communication system.

Encoding and decoding*:* Fig 4 shows the block diagram of the BER measurement system. Here 8 bit of data is given as the input into the encoder along with the input the data the 14 bits of seed is added to provide security. A Linear Feedback Shift Register (LFSR) is a shift register whose input bit is a linear function of its previous state. LFSR is used to generate PN sequence. Generated PN sequence are interleaved with interleaver 16383 (4).

A. **Interleaver and Deinterleaver:** The basic function of an interleaver is to protect the transmitted data from burst errors. Due to the use of the speech coders, many important bits are produced together. The interleaver spreads these time bits out in time so that all these bits are not corrupted at the same time by the deep fade or noise burst. In the interleaver, a 14-bit counter is used to write the coded input bits into a 16 384×1 memory. This counter counts linearly from 1 to 16 383 and goes back to 1. At the output, a 14-bit LFSR is used to read out the coded bits randomly from the memory to decrease the correlation between the encoded samples. Notice that the counter does not generate 0 as zero is not among the values that are generated by an LFSR, hence the interleaver length is 16 384 − 1.

In the deinterleaver, the reverse operation is performed, where the received bits are written randomly into a memory using the same pseudorandom sequence and later read out using a circular counter that counts from 1 to 16 383 (5).

BPSK MODULATION

The interleaved bit are modulated by the BPSK modulator. In a BPSK (binary phase-shift keying) modulation process, thephase of the sinusoidal carrier signal is changed according to the message level (“0” or “1”) while keeping the amplitude and frequency constant (3). Beginning of BPSK modulated signal’s period is positive values, if transmitting symbol is 1. But if transmitting signal is 0, beginning of BPSK modulated signal’s period is negative values.

B. ML DETECTOR

Maximum-Likelihood detection is fundamental problem for digital communication. The ML detector tries to achieve the best Bit Error Rate (BER) of the transmitted signal. In general ML detection problem is NP hard due to discrete nature of signal constellation. Large communication system often arise in scheme with efficient rate and diversity utilization .In a MIMO system, multiple antennas are used at the both transmitter side and receiver side. The function of the MIMO Ml detector is to estimate the symbol vector s from the received signal vector r (4). At the receiver end, by assuming that the channel matrix H is known, an ML detector computes an estimate ˆs for each transmitted ST symbol. For a 2 × 2 MIMO system with BPSK modulated symbols, there are 42 symbols in the search and four multiplications are required for calculating the cost of each of the tentative symbols. Because of the resource constraints in the chosen FPGA, we used only four multipliers for the calculation of the cost function and shared the pipelined datapath for calculating the 16 costs (6). The 16 clock cycle latency of the ML detector is the bottleneck that limits the symbol transmission rate of the MIMO communication system to Fclk/16 symbols per second, where Fclk denotes the clock frequency (7).The FIFO section in the ML datapath delays each of the tentative transmitted symbols according to the latency of the cost function datapath. It finds symbol with minimum cost, which is the output of the ML detector. Three comparators are used in the search section for finding the tentative

symbol with the minimum cost. Its due to the one clock cycle latency of the comparator. ML output is selected by comparing the cost of two final value of M1 and M2. The advantages of the ML detection is that it provides the best reliability, low power consumption and higher data rate that it provides the bestreliability, low power consumption and higher data rate.

FADING VARIANT GENERATOR

Consider two independent normally-distributed variants with zero means and equal variance. To implement a Rayleighfading variant generator, Without generating two Gaussian variables p and q we can compute the magnitude of thecomplex Gaussian-distributed variant. According to the BM algorithm, if there are two independent uniformly-distributed pseudorandom numbers (PNs) in the interval (0, 1) and, then and two independent variants from a zero-mean, u with Gaussian distribution N (0,1), it follows Rayleigh distribution (8). To implement a Rayleigh variant generator, using two independent Gaussian variables, and then computing the magnitude of the complex Gaussian-distributed variant where we use the BM algorithm. According to this algorithm, if and are two independent uniformly-distributed pseudorandom numbers (PNs) in the interval (0, 1) and, then and two independent variants from a zero-mean, unit-variance Gaussian distribution. Therefore the variant follows the Rayleigh distribution. Here we use the BM algorithm to generate Rayleigh distributed variants, but they use iterative CORDIC algorithm to implement the logarithm and square root operations. To obtain high throughput we use a hybrid segmentation scheme over the full domain. The subintervals (0, 0.5) and (0.5, 1) are segmented logarithmically into segments from 0.5 down to 0 and from 0.5 up to 1, respectively. Then each segment is subdivided uniformly into sub segments.

DECRYPTION

The first step of the decryption is to identify the exact positions of the deleted data for the decoding algorithm. It is not necessary to decrypt previous blocks successfully. However, it is necessary to be synchronized with the encryption process to maintain the right system state in terms of the permutation arrays and the PRNG state. The decryption process is described in Figure 6. To decrypt, start by reversing the post-permutation. Then, identify deleted columns and rearrange them into their proper order. This step will expand the block to include the deleted columns. This is an important step for successful decryption for a number of reasons (1) to ensure that the XORing with the random sequence is performed correctly and (2) because the order of symbols is as important as the value of symbols to decoding. Once the columns are put in order, the data can be extracted by adding Next, reconstruct the deleted columns using the decoding algorithm of Finally, recover the plaintext by reversing the bit permutation .The permutation update function in decryption must be identical to the one in the encryption if upcoming blocks are to be decrypted successfully. After decrypting the data the BER measurement is done.

SIMULATION RESULTS

To encrypt, start by permuting the bits of the input block using the permutation array. The encoded block is randomizedby XORing it with the random sequence from PRNG.PRNG is generated by using the LFSR. This is followed by the delete step where out of the columns are selected and removed from the randomized block. After deletion post-permutation operation is performed. In the above fig.10 the encrypted input is given as the input to the transmitter.8 bit of encrypted data is given as the input to the encoder after encoding they are interleaved .To avoidthe data loss while the transmission is going they are loaded into the memory. The interleaved data are modulated using the BPSK modulator and the modulated is transmitted using the local oscillator. After when the data are passed into the channel it will be various like noise and Rayleigh fading.To decode the transmitted data which being transmitted data same set of PN sequences are generated at receiver side and the encrypted data are decrypted by following the same steps which are followed at receiver end to decode the data which are being transmitted. After performing the

decoding process Bit error rate is measured. After the HDL synthesis phase of the synthesis process, the RTL Viewer is used to view a schematic representation of the pre-optimized design in terms of generic symbols that are independent of the targeted Xilinx device. Fig.13 shows the Register Transfer Level of the entire communication system (9). Power analysis of the entire system is calculated using Xilinx 14.2 software. The above fig.14 shows the total power consumption of the wireless communication system. Environment in which the power is analyzed is 25C˚ temperature. Thermal properties of the system are Effective TJA(C/W) is 16.4, Max Ambient is 83.7C˚ and Junction temperature is 26.3C˚. Effective TJA(C/W) is minimum temperature which is required to operate the system. Max Ambient temperature is the maximum temperature to which it can operate, beyond it cannot operate. Clocks consume 0.001 W power. The total power consumed by the entire system is 0.081 W. Dynamic current is 0.001 (A) and Quiescent current is 0.081 (A).

CONCLUSION

In this paper Wireless communication system is designed using VDHL. To make the data transmission more secure when the data are passed into channel Crypto-System with Embedded Error Control (CSEEC) is used. Low power isconsumed 0.081 W due to switching activity.

REFERENCE

1. Alimohammad, A and Saeed Fouladi F-ard, "FPGA-Based Bit Error Rate Performance Measurement of Wireless Systems," *IEEE Trans. Very Large Scale Integration (VLSI) System* vol. 22, no. 7, pp 1-10 ,July 2014.
2. Fard, S. F and B. F. Cockburn, "Hardware implementation of Nakagami and Weibull variate generators," *IEEE Transaction in .Very Large Scale Integration. (VLSI) Syst.*, vol. 20, no. 7, pp. 1276–1284, Jul. 2012.
3. Alimohammad, A., Fard, S. F and B. F. Cockburn, "Reconfigurable performance measurement system-on-a-chip for baseband wireless algorithm design and verification," *IEEE Wireless Communication.*, vol. 19, no. 6, pp. 84–91, Dec. 2012.
4. Alimohammad, A., Fard, S. F and B. F. Cockburn, "An accurate MIMO fading channel simulator using a compact and high-throughput reconfigurable architecture," *IET Communication.*, vol. 5, no. 6, pp. 844–852, Apr. 2011.
5. Alimohammad, A., Fard, S. F and B. F. Cockburn, "Hardware implementation of Rayleigh and Ricean variate generators," *IEEE Trans. Very Large Scale Integration. (VLSI) Syst.*, vol. 99, no. 4, pp. 1– 5, Jan. 2010.
6. Fard, S. F., Alimohammad, A and B. F. Cockburn, "An FPGA-based simulator for high path count Rayleigh and Rician fading," *IEEE Transaction .Vehicular. Technology.*, vol. 59, no. 6, pp. 2725–2734, Jul. 2010.
7. Alimohammad, A., Fard, S. F and B. F. Cockburn, "FPGA-accelerated baseband design and verification of broadband MIMO wireless systems," *In Proc. IEEE 1st Int. Conf. Adv. Syst. Testing Validation*, pp. 135–140, Sep. 2009.
8. Lee, D.U., W. Luk, J. D. Villasenor, and P. Y. K. Cheung, "*A Gaussian noise generator for hardware-based simulations*," *IEEE Transactions. Computation.*,vol. 53, no. 12, pp. 1523–1534, Dec. 2009.
9. Alimohammad, S. F. Fard, and B. F. Cockburn, "A flexible layered architecture for accurate digital baseband algorithm development and verification," IEEE Trans *Proc. EURO Conference* , 2009, pp. 45–50.

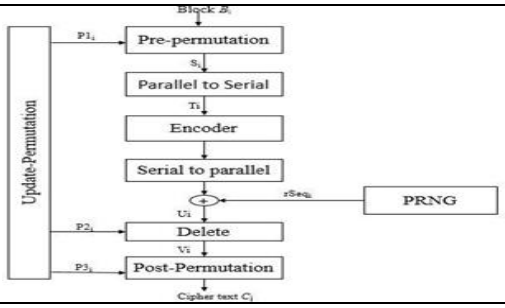

Fig.1 Encryption

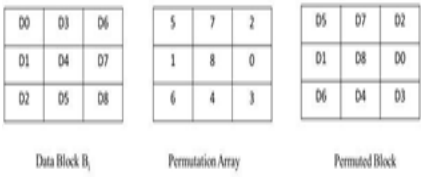

Fig. 2. Permutation Example

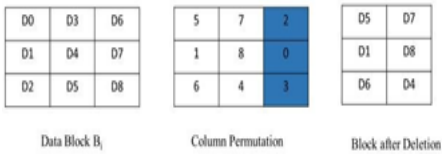

Fig.3 Delete Step Illustration.

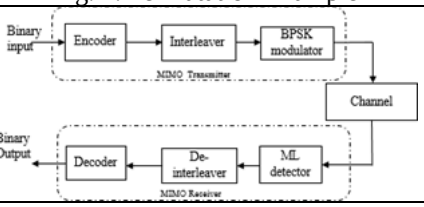

Fig.4 Block diagram of wireless communication system

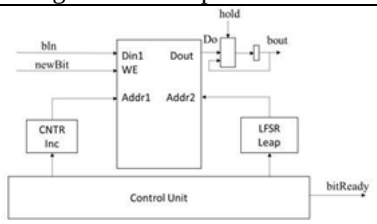

Fig.5 Data path for implemented interleaver

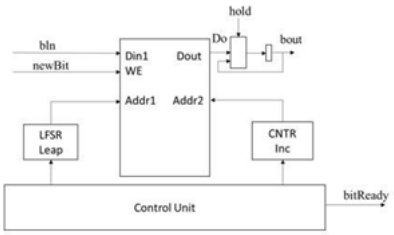

Fig.6 Data path for implemented Deinterleaver

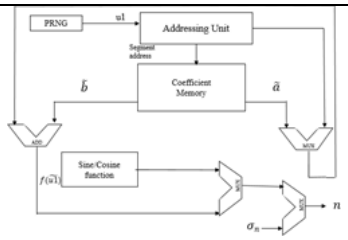

Fig .7. Data flow diagram for Rayleigh variants

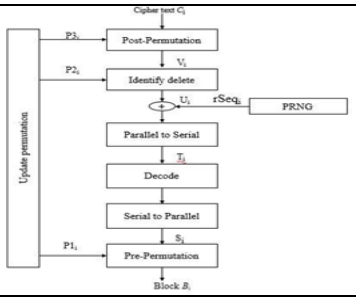

Fig. 8. Decryption

Fig.9 Encryption output

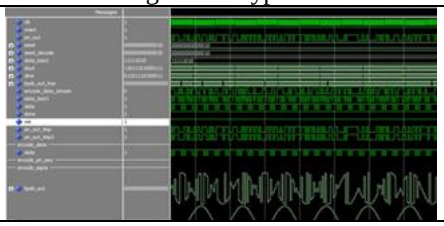

Fig. 10. Transmitter output

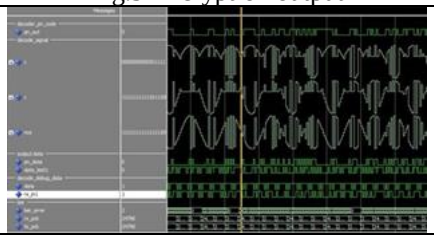

Fig.11 Receiver output

Fig.12 Decryption output

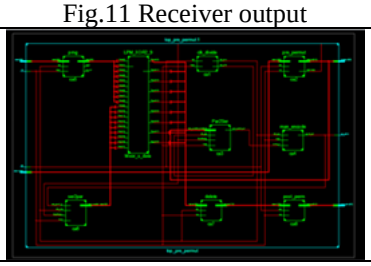

Fig. 13. RTL view

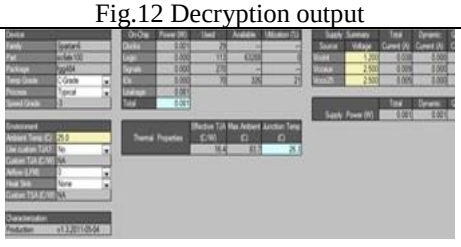

Fig. 14. Power analysis