International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Index Copernicus Value (2015): 62.86 | Impact Factor (2015): 3.791

FPGA Based Bert for Wireless Communication System: A Review

Muktai Surnar[1], S. S. Thorat[2]

[1]Student, Department of Electronics Engineering, Government College of Engineering, Amravati, India

[2]Assistant Professor, Department of Electronics Engineering, Government College of Engineering, Amravati, India

Abstract: ***The FPGA-based BERT increases speed of simulations in systems. These FPGA-based solutions are more cost effective than conventional performance measurements made using expensive test equipment. Basically the BERT Consists of PRBS (Pseudo Random Binary Sequence) Generator Module in the Transmitter Side and Pseudo Random Pulse signal is transmitted by the Serial link. The receivergenerate the same signal and compare with the transmitted signal, if any errors occurs like bit slip, bit error. Then Additive white Gaussian noise (AWGN) generator can detect the number of errors and these errors are evaluated by the BERT which estimate the error rate w.r.t number of bits .In wireless network communication systems exchange of information depends on networked Computers, mobile phones and other internet operated systems. Unsecured data that travels through different networks are get damaged by many types of attack, noises and interrupted by anyone who has access to that data. To prevent such interruptions, data must be encrypted and decrypts with effective techniques are employed.***

Keywords: BERT (bit error rate tester),CRC encoding, Cryptography, encryption, decryption

1. Introduction

BERT is Defined as the Bit Error Rate Tester analyse the error rate of the Data Information Bits. Transmitter sends the information bits and receiver receives the number of data information bits, and Bit Error Rate Tester analyse the error rate. Probability of a bit-error is identified at the output of the receiver compared with the input of the transmitter.

Basically Bit Error Rate Tester (BERT) consists of PRBS (Pseudo Random Binary Sequence) Generator for serial communication link. Error rate is estimated by comparing Transmitted PRBS Pattern Sequence with Received PRBS Pattern Sequence. The transmitter changes the raw information (sequences of binary digits) into a format that is matched to the characteristics of the channel. The recovery of transmitted binary digits happens when the receiver accepts the signal from the channel. The recovered digits are usually processed to permit interfacing with the final destination, such as a computer monitor. According to wireless communication when the data is in the route may hacked by unauthorized person in order to protect data there are two main techniques probably used i.e. Steganography and Cryptography. Steganography hides the messages inside harmless channel without altering it. Cryptography is the effective method of writing the secret message and introduces new techniques encryption and decryption information which hided. Cryptography is the science of hiding information from third party user for better accuracy. It provides the secrecy of transmitted data over an unsecure channel and prevent eavesdropping and data tampering.When data is transmitted there will be possibility of errors being introduced into the system, mostly where the medium is noisy, so that Networks must be able to transfer data from one device to another with complete accuracy.Integrity in which modifications of data only restricted to authorized users. However Non Repudiation is making the sender and receiver of the message not able to deny the communication. Access Control where the access to data limited for only that person who has access key.

2. Cryptography in Communication System

Wireless networks has been trying to replace the structure of the wired system, the system uses electromagnetic waves as medium which are mainly either radio frequency (RF) or infrared frequency (IR).Wireless system consist of two elements i.e. clients and Access Points (AP). Clients have featured with devices that allows user to use the RF medium to communicate with other wireless devices. AP's are used to represents a gateway between the wireless devices and a wired network.Fig.1shows simulation model of a wireless communication system In such a communication system, the text message is converted into integer and then encrypted by using RSA,DES,AES encryption algorithm. The encrypted data is converted into binary bits and channel encoded using CRC.

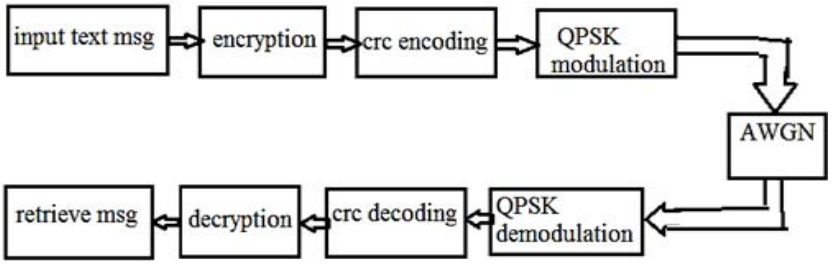

Figure 1: Wireless communication system using cryptography

Licensed Under Creative Commons Attribution CC BY

Basically Cryptography may be public key cryptography which is called asymmetric or it may be the private key cryptography also called symmetric. Encryption is a term element of cryptography in which information is hides by transforming it into an undecipherable code; Encryption creates a key to perform the data transformation.

1) Symmetric Encryption
In Symmetric encryption, single unique key is used for both encryption and decryption. This means the person who encrypts the input message should send the unique key to the recipient before they can decrypt it.

2) Asymmetric Encryption
Asymmetric encryption also known as Public-Key encryption, it consist two different keys one is a public key to encrypt the message else a private key to decrypt it. This allows a user to freely distribute public key to people who want to communicate.

3) Data Encryption Standard (DES)
Data Encryption Standard (DES) is a widely used method of data encryption using a private key.

4) Advanced Encryption Standard (AES)
AES is a new encryption standard recommended by NIST to replace DES. It is a symmetric cipher defined in Federal Information Processing (FIPS) Standard Number 197 in 2001.

Biterror Rate and Data Extraction

Bit error rate is important parameter while describing the performance of transmission in the digital link. It is usually defined as:

$$\text{BER} = \frac{nr}{N}$$

Where nr is the total number of received bits and N is the number of bits corrupted. The probability of errors occurring during data transmission in order of 10^9.so that equation becomes

$$\text{BER} = \frac{1}{b}\frac{nr}{\Delta t}$$

Where b is the bit rate and Δt is the measurement time. it is convenient to express Δt in seconds, and the bit rate is only a scaling factor.

Error Detection and Correction:
Cyclic Redundancy Check (CRC) codes are a subset of linear codes, which satisfy the cyclic shift property such as if C=[Cn-1,Cn-2 ……,C0] is a code word of a cyclic code. Cyclic Redundancy Check is error detection mechanism in which numbers of bits are appended to a block of data, because to detect if any changes introduced in transmission. The CRC is recalculated on retrieval and compared to the value originally transmitted, which can reveal certain types of error. Forward Error Correction When the receiver detects some error in the data received; it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

Additive White Gaussian Noise (AWGN):
Thenoise is additive in environment, the received signals are same as the transmit signals plus some noise, many times noise is statistically independent of the signal. The noise is white, in which the power spectral density is always flat in behaviour, so the autocorrelation of the noise in time domain is zero for any non-zero time offset. In signal separation the Additive White Gaussian Noise samples have a Gaussian distribution in characteristic.

3. Literature Review

The bit error rate tester designed for operation in 10 GB/s fiber optic to evaluate the degradation of the signal quality strength interrupted because of noises in environment. The architecture of the BERT described herein was specified abilities of Spartan3 FPGA. it was possible to overcome speed limits of Spartan3 FPGA[1].In addition, the capacity of the golay code generator (16 bits) proved to be too small and should be extended to 24 bits. According to Annie Xiang, Datao Gong, Suen Hou, Chonghan Liu et.al FPGA-based bit error rate tester has been developed to characterize a serial optical link removes problem over parallel link. The Stratix II GX kit operating at up to 5 GB/sIn addition to the PRBS generator, detector and transceiver blocks, the error logger and user interface were developed for better integrity of data acquisition. The tester was used in a serialized chip where two types of radiation produces errors they are recoded as per range and analyzed. A number of coding schemes and transmission protocols were used for better characterization. A single transceiver block supporting four duplex channels has been enabled on each of the Stratix II and IV platforms. It extends BER testing capability to high channel count and parallel systems.

Nowadays, RSA generally uses cryptographic method generally uses in PKC applications. However, recently ECC cryptography system has a trend which substitutes for RSA to hardware realizations. ECC provides security with shorter bit sizes than in RSA. Shorter key length saves bandwidth and power. SHA-1 is a hashing algorithm recommended by ANSI. The code is written in four secure phases, which are generating the signature, verification, encryption and decryption [2].

Encryption and decryption technique in wireless sensor networks was described by author S. Kannadhasan et.al. the energy efficiency of symmetric key in cryptography algorithms to be used in wireless sensor networks (WSNs) and in this paper block ciphers term was explained with benefiter factors that have transferred through the network are secured. Wireless sensor networks [3] operated on encryption and decryption.

In this paper the asymmetric RSA cryptographic encryption/decryption algorithm precedes wireless communication system with the help of QPSK modulation over AWGN channel. The deployment of RSA cryptographic algorithm in CRC encoding wireless communication system is more efficient and highly secured [4]. Amirhossein Alimohammad et,al explained the efficient BERT for a MIMO channel of digital baseband communication system based on single FPGA. According to it the intensive signal

Licensed Under Creative Commons Attribution CC BY

processing algorithms for fast simulation chain dedicated to hardware, the simulation time was reduced by over four orders of magnitude in GNG behavior[5][6]. Simulation of bit error rate test bench using Altera transceiver development kit however the test bench implements PRBS generator and detector to produce patterns and error introducing test bench and FIFO to record both bit error data and link operation events. FPGAs have widely used dedicated communication interfaces. Bit error rate (BER) characteristic is one of the basic important testing factors of any digital communication system. Traditionally, BER is evaluated using Monte-Carlo simulation algorithms which are very time-consuming.so fast simulation processing fpga has AGNG which increases capability of BER.

4. Conclusion

VHDL Implementation of various modules gives an easy and less expensive way to implement Encoding and decoding system. First the different components that constitute the coder have been designed with required inputs, outputs & control signals. The interface between the designed components and hardware make it faster. This is then realized in VHDL language using Xilinx Software. The cryptographic implementation provides various techniques of encryption and decryption.However all techniques implements secure data transmission over authorised user and hide data from third party.

References

[1] Łukasz ´Sliwczy´nski and Przemysław Krehlik "Bit Error Rate Tester for 10 Gb/s Fibre Optic Link"*Advances in electronics and telecommunications, vol. 1, no. 2, november 2010*

[2] Annie Xiang, Datao Gong, Suen Hou, Chonghan Liu, Futian Liang, Tiankuan Liu, Da-Shung Su,Ping-Kun Teng, Jingbo Ye"Design and verification of an FPGA-based bit error rate tester" *Technology and Instrumentation in Particle Physics 2011*

[3] H. Modares, M. T. Shahgoli, H. Keshavarz, A. Moravejosharieh, R. Salleh "Make a secure connection using elliptic curve digital signature" *International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012 1 ISSN 2229-5518*

[4] S.Kannadhasan, P.Suresh, M.Rajesh Baba "Encryption and Decryption Technique in Wireless Sensor Networks"International Journal of Advanced Research in Computer Science Volume 4, No. 4, March-April 2013 ISSN No. 0976-5697

[5] Md. Ashraful Islam, A. Z. M. Touhidul Islam "Secure Wireless Text Message Transmission with theImplementation of RSA Cryptographic Algorithm" *International Journal of Computer Networks and Communications Security VOL. 2, NO. 5, MAY 2014, 146–151 Available online at: www.ijcncs.or ISSN 2308-9830*

[6] Amirhossein Alimohammad and Saeed Fouladi Fard "FPGA-Based Bit Error Rate Performance Measurement of Wireless Systems" *IEEE transactions on very large scale integration (vlsi) systems, vol. 22, no. 7, july 2014*

[7] Viha Pataskar, Vishal Puranik "FPGA-Based Bit Error Rate Performance measuring of Wireless Systems" *International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 5, May 2015*

Licensed Under Creative Commons Attribution CC BY