© 2016 IJSRST | Volume 2 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

RRNS Based Error Detection and Correction in CDMA using Chinese Remainder Theorem

G. Karthik, R. Mohan Raj, B. Karthik

*[1] M.Tech Applied Electronic, ECE Department, Bharath University, Chennai, Tamil Nadu, India
[2]Assistant Professor, ECE Department, Bharath University, Chennai, Tamil Nadu, India

ABSTRACT

In communication systems corruption of data and hacking of data is unavoidable. These are the major problems we are facing in communication system. This paper presents an enhanced multiple error detection and correction scheme based on the Redundant Residue Number System (RRNS). RRNS is often used in parallel processing environments because of its ability to increase the robustness of information passing between the processors. The proposed multiple error correction scheme utilizes the Chinese Remainder Theorem (CRT) together with a novel algorithm that significantly simplifies the error correcting process for integers. This enhanced scheme is compared with the existing method and this enhanced scheme is used in the CDMA application.

Keywords: Redundant Residue Number System (RRNS)**,** Chinese Remainder Theorem (CRT) CDMA

I. INTRODUCTION

A Residue Number System (RNS) for integers describes methods of representing an integer as a set of its remainders or residues. Error control is achieved by addition of extra residues, hence the term RRNS. The RRNS code used in this work uses the Chinese Remainder Theorem (CRT) as a means of recovering the integer from a set of its residues. Error correcting codes based on the CRT are attractive because of their ability to perform carry-free arithmetic and lack of ordered significance among the residues. Some of the concepts related to this error correction technique such as the terms legitimate range and illegitimate range for consistency checking.

II. METHODS AND MATERIAL

A. RRNS (Resudue Redundency Number System)

A residue number system (RNS) represents a large integer using a set of smaller integers, so that computation is performed more efficiently. It relies on the Chinese remainder theorem of modular arithmetic for its operation, a mathematical idea from Sun Tsu Suan-Ching, when redundant residues are added to the information residues then it is called redundant residue number system. The receiver applies the same algorithm to the received data bits and compares its output to the received check bits; if the values do not match, an error has occurred at some point during the transmission. In a system that uses a "non-systematic" code, such as some raptor codes, data bits are transformed into at least as many code bits and the transmitter sends only the code bits.

B. Transmitter Model

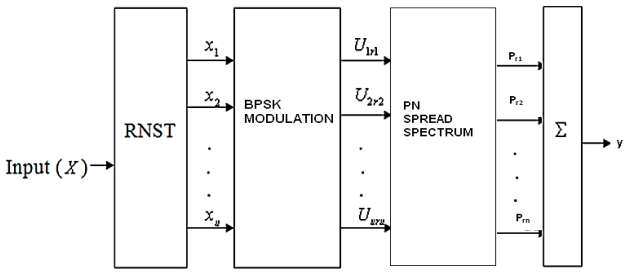

Figure 1. Transmitter Model

Algorithm for transmitter

1) Start the program
2) Get the inputs X, n, t, k

Where X - information

n - length of the prime number module

t - no of correctable errors($r-1$)

k - information range

3) Generate relatively pair wise prime number module (m_i)

4) Generate information range (M_K) and redundant range (M_R)

5) Calculate the residue vector to be transmitted

$$X \equiv x_i (\text{mod } m_i)$$

6) Generate orthogonal sequences,

$$\{U_{10}(t), U_{11}(t), \ldots, U_{1(m_1-1)}(t); U_{20}(t), U_{21}(t), \ldots, U_{2(m_2-1)}(t); \ldots; U_{n0}(t), U_{n1}(t), \ldots, U_{n(m_n-1)}(t)\}$$

7) Map the residues to the orthogonal sequences,

$$U_{1x_1}(t), U_{2x_2}(t), \ldots, U_{nx_n}(t)$$

8) Sum all the orthogonal sequences and multiply with the user specific scrambling code for spreading the signal.

9) Modulate the signal and transmit.

C. Receiver Model

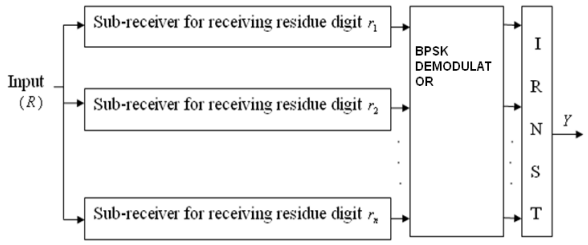

Figure 2. Receiver Model

Algorithm for receiver

1) Demodulate the signal R.

2) Divide the demodulated signal into six fingers $n = 6$.

3) Divide each finger into two paths because we assumed there are two paths in the channel.

4) Multiply the scrambling code to despread the signal in each path.

5) Multiply the conjugate of the corresponding channel impulse response in each path.

6) In the correlator bank, corresponding orthogonal sequences are multiplied with the signal each path.

7) Sum the outputs of the correlator bank of all the paths.

8) Find the maximum of all the values.

9) The index is taken as the output of first finger and this process from step 5 is done for all the fingers.

10) Two residues are assumed to be known residues and all these values are put in a vector y .

11) Compute Y from the received vector y using

$$Y = \sum_{i=1}^{n} y_i M_i a_i \bmod M$$

where,

$$M = \frac{M}{m_i}, a_i = M_i^{-1} \bmod m_i$$

&

$$M = \prod_{i=1}^{n} m_i = M_K . M_R$$

12) If Y is in the legitimate range, stop and output else proceed to step (13).

13a) List all possible, k positions combination

$$a = {}^nC_k$$

13b) Compute $Z_a = \prod_{a=a_1}^{a_2} m_a$

14) Compute for all values of $X = Y \bmod Z_a$ for all values of a .

15) Assign all legitimate values of X into another set V_i .

16) Calculate the residue vectors $v_i = V_i \bmod m_i$ and the Hamming distance for all elements of set V_i .

17) Assign the values of V_i to S for which the hamming distance is minimum.

18) Calculate the bit error rate for minimum hamming distance value.

D. Chinese Remainder Theorem

The Chinese remainder theorem is a result about congruences in number theory and its generalizations in abstract algebra.

The Chinese remainder theorem can also be used in Secret sharing, which consists of distributing a set of shares among a group of people who, all together (but no one alone), can recover a certain secret from the given set of shares. Each of the shares is represented in congruence, and the solution of the system of congruence using the Chinese remainder theorem is the secret to be recovered.

E. Channel Result

During transmission, errors propagate into the residue vector *x* at positions u1= 1, u2=3, u3=5. Therefore, let the received vector be *y*= {2, 2, 2, 7, 3, 7}

x = {1, 2, 0, 7, 7, 7}

$y = \{2, 2, 2, 7, 3, 7\}$

Three errors are introduced because $t = r - 1 = 3$

F. Receiver Results

- From y, the computed integer Y using,

$$Y = \sum_{i=1}^{n} y_i M_i a_i \bmod M$$

$$= 88832$$

- The corresponding values of Mi and the multiplicative inverse are
- Mi = {85085,51051,36465,23205, 19635, 15015};
- ai = {2, 1, 4, 2, 8, 13};
- The minimum Hamming distance is 3. Hence the set = { 2, 7}.
- The moduli set for the integer 2 (elements in S) is {2, 3, 5, 7, 11, 13}.
- The moduli set for the integer 7 (elements in S) is {3, 5, 7, 11, 13, 17}.
- S = {11, 13, 17, 19, 23, 29, 31}
  Since the moduli set for integer 7 and are same, the transmitted integer is 7.

G. Comparison Between Existing and Proposed Method

Without doing the mapping function in the transmitter, only the residues x_i are transmitted. In the channel $t = r - 1$ errors are introduced in the transmitted vector. In the receiver side, the vector $y = x + e$ is received; in the receiver algorithm from steps 11 to 17 are performed. The 18th step is verification step

- Compute the relative pair wise prime number set for each value of S and compare it with transmitted m_i.
- The transmitted integer is the value of S for which, the moduli of m_i and the transmitted m_i is same.
- Compare the existing method and the proposed method.

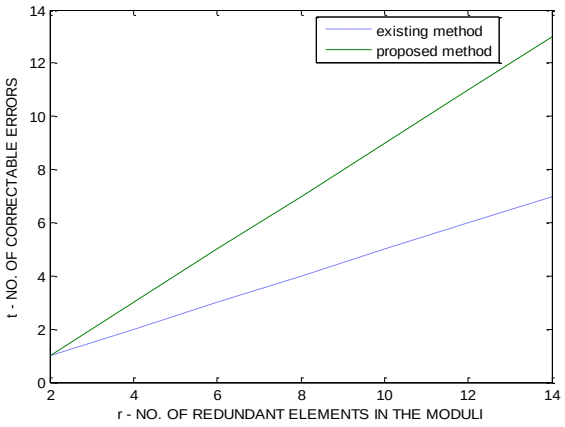

Figure 3. Comparison between Existing and Proposed Method

III. RESULT AND DISCUSSION

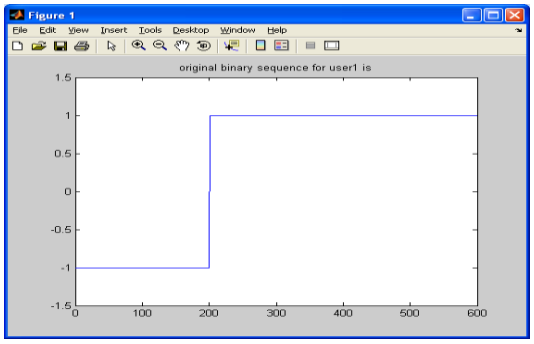

Figure 4. original binary sequence for user1

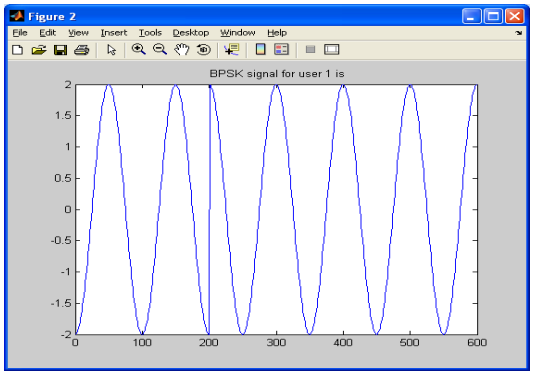

Figure 5. BPSK signal for user 1

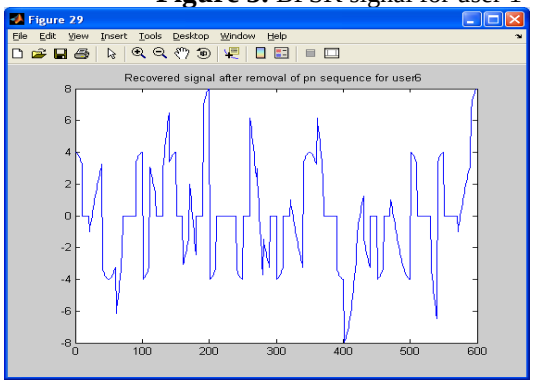

Figure 6. Recovered signal after removal of pn sequence for user6

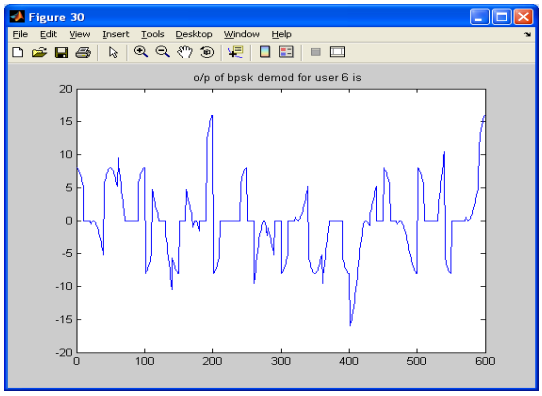

Figure 7. O/P of BPSK demod for user 6

IV. CONCLUSION

In this paper, a modified algorithm is proposed for correcting multiple errors. This is different from existing multiple error correction schemes. This algorithm is quite simple and easy to implement. The proposed algorithm can correct more errors than the other existing schemes at the expense of marginal increase in computation and it is compared with the existing method without implementing in the CDMA application but when it is implemented in the CDMA application the BER is calculated for several SNR values. The future work is to reduce the number of orthogonal codes and computation.

V. REFERENCES

[1] Barsi and P. Maestrini, "Error correcting properties of redundant residue number systems," IEEE Trans. Comput., vol. 81, pp. 307-315, Mar. 1973.

[2] P. E. Beckmann and B. R. Musicus, "Fast fault-tolerant digital convolution using a polynomial residue number system," IEEE Trans. Signal Processing, vol. 41, pp. 2300- 2313, July 1993.

[3] O. Goldreich, D. Ron, and M. Sudan, "Chinese remaindering with errors," IEEE Trans. Inform. Theory, vol. 46, pp. 1330-1338, July 2000.

[4] Krishna, K. Y. Lin, and J. D. Sun, "A coding theory approach to error control in redundant residue number systems. Part I: Theory and single error correction," IEEE Trans. Circuits Syst., vol. 39, pp. 8-17, Jan. 1992.

[5] D. M. Mandelbaum, "Error correction in residue arithmetic," IEEE Trans. Comput., vol. 21, pp. 538-545, June 1972.

[6] D. M. Mandelbaum, "On a class of arithmetic codes and a decoding algorithm," IEEE Trans. Inform. Theory, vol. 22, pp. 85-88, Jan. 1976.

[7] D. Sun and H. Krishna, "A coding theory approach to error control in redundant residue number systems. Part II: Multiple error detection and correction," IEEE Trans. Circuits Syst., vol. 39, pp. 18-34, Jan. 1992.

[8] Vik Tor Goh and Mohammed Umar Siddiqi "Mutiple Error detection and Correction Based on Redundant Residue Number Systems" IEEE Transaction on Communication Vol.56, No.3, March 2008.

[9] K. Yen, L.L. Yang, and L. Hanzo, "Residue Number System Assisted CDMA: A New System Concept" Department Of Electronics And Computer Science, University Of Southampton, UK.

[10] L. L. Yang and L. Hanzo, "Redundant residue number system based error correction codes," in Proc. 54th Veh. Technol. Conf., 2001, pp. 1472-1476.