Redundant Residue Number System Based Fault Tolerant Architecture over Wireless Network

Olabanji Olatunde.T
Department Of Computer Science
Kwara State University,
Malete, Nigeria
toheeb.olabanji@kwasu.edu.ng

Kazeem .A. Gbolagade
Department Of Computer Science
Kwara State University,
Malete, Nigeria
kazeem.gbolagade@kwasu.edu.ng

Yunus Abolaji
Department Of Computer Science
Kwara State University,
Malete, Nigeria
yunus.isiaka@kwasu.edu.ng

ABSTRACT
Wireless communication has become an indispensable part of our lives by improving interaction demands relating within our environment. The result of interference of information passing through different systems often caused by noise reduces the completeness of the information or data received. A Fault-tolerant mechanism for wireless networks is of utmost importance to be devised due to the use of modular arithmetic over identical channels. Using the RRNS technique, we will be able to compute using modular arithmetic over identical channels. We can make this system fault tolerant by increasing the number of channels by adding more redundant residues which provides the error detection and error correction functions resulting from RRNS. This capability makes the redundancy in RNS a great indication to exhibit a faster arithmetic process in the field of digitizing computer information. From receivers end, RRNS codes are decoded using CRT. Alternatively, scheme called MRC is also used which results in low decoding complexity when compared to CRT. This research presents a fault-tolerant technique which is based on the RRNS for multiple error detection and correction. This algorithm doesn't require look-up table and detects multiple error which helps to save memory during implementation.

CCS Concepts
• **Networks → Network components → Wireless access points, base stations and infrastructure**

Keywords
Wireless Networks, Error Detection & Correction, Residue Number Systems (RNS), Redundant Residue Number Systems (RRNS), Chinese Remainder Theorem (CRT), Mixed Radix Conversion (MRC), Base Extension (BEX)

1. INTRODUCTION
Generally in wireless network, set of data are corrupted during transmission whenever bits flow from one point to another, they are subject to unpredictable changes of interference [3][4]. One of the major problems in wireless data transmission is caused by noise which can cause errors in the data when it is been transmitted through a channel [2]. Therefore respectively data should be decoded correctly accordingly at the receivers end. The ability of the communication system to withstand the channel impairment through signals will indicate the communication performance can be enhanced or improved by dealing with these transmission problems in implementing measures such as error detection and correction [3].

CoRI'16, Sept 7–9, 2016, Ibadan, Nigeria.

For wireless network, the error detection and correction services are usually provided by communication protocols at the data link and the transport layers in the OSI model.

The error detection scheme requires certain amount of overhead in term of additional bits which are added to the total transmitted data. These additional bits are used by the receiver to check for error on the sequence of data that might occur during the transmission. Some error detection scheme could be used to correct the error which is called error correction scheme. However, the number of bits in error that can be detected may be different depending on the scheme and required overhead [12]. Consequently, some efficient error detection techniques are not suitable for wireless networks because it may require larger block of data and higher overhead. Simple error detection such as parity check bit is be too weak for wireless communication in which quality of radio channel is often poor and burst errors often occurs[6]. Redundancy is achieved through various schemes. The ratio of the redundant bits to data/information bit is important to any scheme [12].

Residue number system helps to increase the speed of arithmetic operations when compared to other conventional number systems in digital communication systems. Residue number system (RNS) is a non-weighted, non- positional number system which can be represented by specifying its base. Thus, in RNS any given integer is represented by a set of residues which are obtained by modulo dividing the integer with moduli set[1][2][3][4][5].

Redundant residue number system (RRNS) is obtained by adding some redundancy to the RNS. RRNS can be used for self checking, error detection and error correction in digital computers [1] [2][3]. Thus, it helps in the design of general purpose systems which are capable of adding redundancy concept by sensing and rectifying their own transmission and processing errors [1][3]. Using RRNS for error detection and correction has more advantages over the conventional error codes. RRNS can be used for self consistency checking, error detection and error correction in digital computers.

The fundamental arithmetic operations are carry-free in RNS operations and does not propagate error from one residue digit to other. Another interesting advantage of RNS operation is the lack of ordered significance among residue digits. Therefore, an integer can be recovered from its residues even after discarding some of the redundant residues, provided that the retained residue digits should be correct. RNS offers great speed as a result of its underlying carry-free nature. As a result, these have increased the development of a number of error detection and error correction algorithms based on RNS [3][5].

The uniqueness of the proposed schemes used in this paper over other related schemes is the high modularity level i.e. same hardware can encode and decode codes with different parameters therefore a generalized scheme will be achieved. The proposed scheme will eliminate multiple errors by using other schemes like the Mixed Radix MRC and BEX decoding schemes with lower complexity compared to the higher order of complexity of CRT by detecting by correcting using more consistent check. This proposed scheme in summary will be highly modular, detect and correct multiple errors, memory-less scheme (space complexity), more secured.

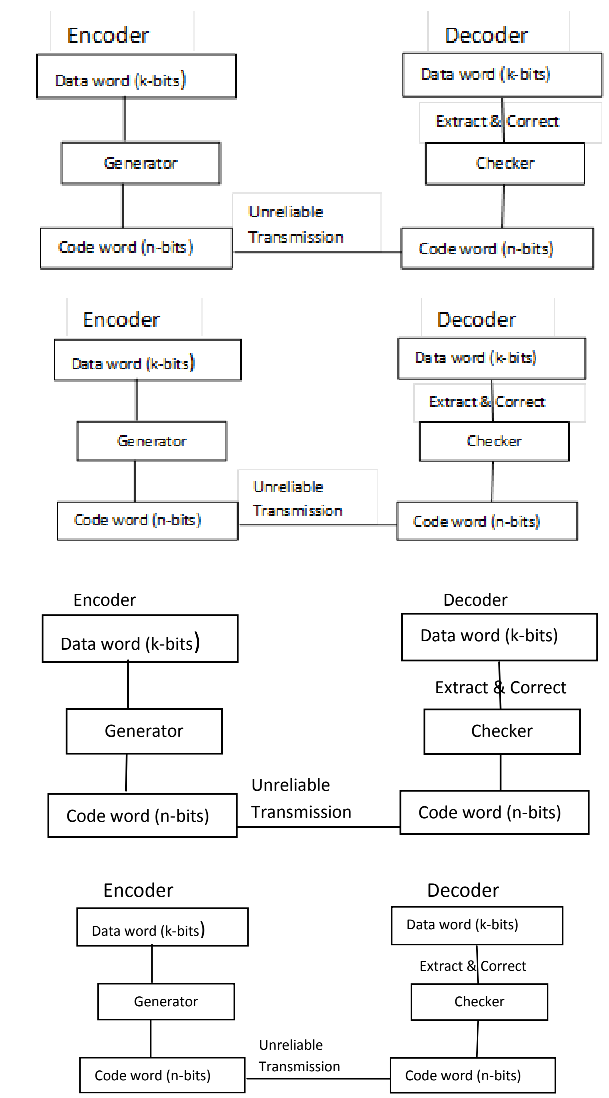

Figure.1. Structure of Encoder in Error Detection & Correction

The content of this paper is organized as follows: Section 2 reviews existing related works are presented, also introducing the fundamental mathematical model of RNS and RRNS. Section 3 describes the decoding alternative techniques of error correction and detection using RRNS and the description of the proposed algorithm is given in section 4. Section 5, Results, Discussions and comparison with representative examples showing the implementation of algorithm. Section.6 conclusion.

2. BACKGROUND AND EXISTING RELATED WORKS ON ERROR DETECTION & CORRECTION IN RRNS

[2] proposed scheme which introduced the concept of RRNS as a channel coding scheme by using an alternative scheme called MRC to compare the level of complexity when decoding. The resulting effect of this scheme when compared to CRT offers a low decoding complexity but could only correct single error.
Also introduced in [1] a multiple error correction concept on an Adaptive scheme, which utilizes the RRNS code structure to decrease the decoding complexity and increase the error performance of the system by applying MRC and syndrome check with the help of a look-up table. The resulting effect of this scheme when compared in terms of cost of implementation in terms of memory and delay is higher when compared to [1] scheme. To this effect, this proposed scheme will offer a bridge to provide a memory-less scheme which offers a great advantage in terms of area cost, delay and would be able to correct multiple errors with respect to any level of the modularity been introduced.

Fundamentals of Residue Number System

Residue Number System: Residue number system is a technique in which an integer is represented by a set of remainders that are obtained after the modulo division by a set of relatively prime moduli. The process of converting a weighted number system to residue format is called RNS encoding [5]. Consider an arbitrary integer X and a set of v relatively prime integers (m_l, m_2, ..., m_v) called moduli with M as the product of all moduli[7]. i.e.

$$M = \prod_{i=1}^{w} mi \qquad (1)$$

Then integer X can be represented as a set of w remainders (r_1, r_2... r_w) where ri = X (mod m_i) (2)
The dynamic range of the RNS is given by M and the set [0,M - 1] gives the legitimate range such that all integers in this range can be represented as residues by this set of moduli[3]. The dynamic range R for negative numbers is given as

$$R = \begin{cases} (-\frac{M-1}{2}, \frac{M-1}{2} & \text{if M is odd} \\ (-\frac{M-1}{2}, \frac{M}{2} - 1 & \text{,if M is even} \end{cases}$$

Arithmetic operations using RNS has the merit of carry free property. Therefore, in RNS the arithmetic operations performed are mutually independent between residue digits [5]. Let X_1 and X_2 be two integers
$X1 \bullet X2 \Leftrightarrow (r_{1i} \bullet r_{2i})$ mod mi, i = 1, 2,... w (3)
Where • denotes arithmetic addition, subtraction or multiplication and r_{li} and r_{2i} are residues of X_1 and X_2 with respect to moduli mi.

Fundamentals of Redundant Residue Number System

Redundant Residue Number System: Redundant Residue Number System is achieved by adding some redundancy to the Residue Number System. RRNS helps in both correction and error detection. By adding (u - w) redundant moduli (m_{w+l}, m_{w+2}... m_w) to the v information moduli (m_l, m_2... m_w), a RRNS (u,w) code can be generated. This process is called RRNS encoding. Thus an integer X is represented in the RRNS form as

$$X = \{r_1, r_2 \ldots r_w, r_{w+1} \ldots r_u\} \quad (4)$$

Where (m_1' m_2, ..., mw) are called information moduli and ($m_{w+l'}$ m_{w+2}, ..., mw) are called redundant moduli. Similarly (r_1, r_2, ..., rw) are called information residues and ($r_{w+l'}$ r_{w+2}, ..., r_w) are called redundant residues. M_r denotes the product of redundant moduli. In RRNS, the legitimate range is defined as [0, M] and illegitimate range indicating overflow, where residues are obtained using redundant moduli, is [M, M M_r].

For RRNS, even if we remove some of the redundant residues, an integer can be recovered if the retained residue digits are correct.

Theorem 1: RRNS (u - w, v) code has a detection capability of (u - w - v) errors and an error correction capability of (u - w - v) /2 [1]. The code rate of a redundant residue number system can be defined as

$$Rc = \frac{Kb}{\sum_{j=1}^{u} Kb} \quad (5)$$

where kb = $\lfloor \log_2 Mr \rfloor$ and $k_{bj} = \lceil \log_2 m_j \rceil$l, where m_j, (j = 1,2 ... u) are the moduli. By varying the number of redundant bits that are transmitted, the code rate and error correction capability are varied. Redundancy is added to the information/data, therefore the code rate decreases and error correction property is improved. In RNS, the number of non-zero elements in a vector is defined as its hamming weight. Let X_i and X_j are two code vectors, then hamming distance d (Xi, X_j) is defined as the number of bits in which two code vectors Xi and X_j differ. Minimum distance, d is the minimum of hamming distances

$$d = \min (d (x_i, x_j); x_i \neq Xj). \quad (6)$$

Theorem 2: The minimum hamming distance d of an RRNS (u,w)-code is defined as d = u - w + 1, provided ($m_l < m_2 < \ldots < m_w < m_{w+l} < \ldots < m_u$).

Theorem 3: For a redundant residue number system, the error detecting capability, c = d - 1 and the error correcting capability [1],

t = $\lfloor$ (d -1) / 2$\rfloor$ where $\lfloor a \rfloor$ is the largest integer smaller than a. Thus RRNS (u,w) code can detect up to u - w residue digits and can correct up to t = $\lfloor$ (u - w) /2$\rfloor$ residue digits. This means that single error and multiple error correction algorithms can be developed by suitably selecting u and w. In this paper, we based our focus on the multiple error correction with u - w = 2.

3. DECODING SCHEMES IN RESIDUE NUMBER SYSTEM

In the course of converting back the received residues into the integers the decoding algorithms are used. Two decoding algorithms, CRT and MRC can be used. For CRT, we have

$$X = (\sum_{i=1}^{k} ri\ Ti\ Mi) Mod\ M \quad (7)$$

where Mi = M/m_i and Ti is the multiplicative inverse of Mi which can be calculated as

$$T_i M_i = 1 \bmod m_i \quad (8)$$

This can be simplified as Ti Mi _

$$\frac{TiMi}{mi} - \lfloor \frac{TiMi}{mi} \rfloor \frac{1}{Mi} = 0 \quad (9)$$

This study will be limited to the MRC because the real time implementation of CRT is not possible because it involves a modular operation with large integer M which results in a complexity of O (n^3). To avoid the computations with such larger M, the CRT satisfies the real-time signal processing due to its parallel means of computation and there is a constant limit to this approach[1][2][7][8]. However, an alternative decoding technique called Mixed Radix Conversion (MRC) is used in this study. The BEX based on MRC will be used to generate additional residues. BEX offers a reduction in the latency and hardware resources. For Mixed radix conversion MRC we have, a number in RNS can be converted to mixed radix system using:

$$x = a_N \prod_{i=1}^{N-1} m_i + a_3 m_1 m_2 + a_2 m_1 + a_1 \ldots \ldots \ldots \ldots (10)$$

Where a_i are the mixed radix system coefficients and are determined sequentially in the following manner. Locating the residue digit error is more time- consuming than correcting the residue digit error. This process dictates the overall delay of an error detection and correction algorithm.

RRNS codes can be used for error detection and correction in both information residues and redundant residues.

Theorem 4: The redundant residue number system can correct any single residue error if it satisfies the following two conditions[l]:

1) R > $m_w m_{w-1}$

2) min (R/m_{w+i}) ≠ m_w 1 ≤ j≤ r where R = $m_{w+1} m_{w+2}$ ...m $_{w+r}$ and r ≥ 2.

Consider that a set of residues $|X|'_{mi}$, are transmitted and received sequence are $|X|'_{mi}$, where i = 1, 2,… u. With the help of W received information residues, redundant residues ($|X|''m_{w+l}$,$|X|''m_{w+2}$,⋯,$|X|''m_u$) can be computed using base extension method.

Define this procedure is called as consistency checking which forms the basis of error correction algorithm described in this paper.

BEX is given as enlargement of the original base

$$x = a_{N+1} \prod_{i=1}^{N} m_i + a_N \prod_{i=1}^{N-1} m_i + a_3 m_1 m_2 + a_2 m_1 + a_{1 \ldots .(11)}$$

Theorem 5: If any one of the residue is in error, then one of the following cases can occur[2]

Case 1: If all the elements in the set ($|\Delta|m_{w+r}$, ... ,$|\Delta|m_{w+l}$) are zero, then all the residues are correct.

Case 2: If only one of the element in this set ($|\Delta|m_{w+r'}$ ...,$|\Delta|m_{w+1}$) is non-zero, then $|X|'m_z$ is wrong and this can be corrected by replacing with $|X|''m_z$.

Case 3: If more than one element in this set ($|\Delta|m_{w+r}$, ... , $|\Delta|m_{w+l}$) is non-zero, then any one of the information residue is in error and all the redundant residues are correct. The above theorem helps in the detection of a single residue error and helps to identify whether the detected error is in information residue or in redundant residue.

Theorem 6: If one of the residues in the set ($|X|'m_1$, $|X|'m_2$, ... , $|X|m_{w\_2j}$) is in error, then one of the following cases can occur[I].

Case 1: If the residue $|X|'m_z$, 1≤ z ≤ w -2j -2, is in error, then $|\Delta|m_{w-2j}$ and $|\Delta|m_{w-2j-l}$ are non-zero.

Case 2: If $|X|'m_{w-2j-1}$ is in error, then $|\Delta|m_{w-2j-l}$ is non-zero and $|\Delta|m_{w-2j}$ is zero. Error can be corrected by replacing it with |X|" .. m_{w-2j-l}

Case 3: If $|X|'m_{w-2j}$ is in error, then $|\Delta|m_{w-2j}$ is non-zero and $|\Delta|m_{w-2j-l}$ is zero.

Error can be corrected by replacing it with $|X|''m_{w-2j}$. This theorem helps in finding the location of multiple residue error. This paper describes a multiple error correction algorithm which is based on the above theorem proposed by [1].

4. PROPOSED ALGORITHM

1. Decode information into the information residue digits and redundant residue digits using both information and redundant moduli sets.
2. Compute the mixed radix digit for the information residue digit with respect to information moduli set.
3. Compute the consistent check respectively to detect erroneous digit & location. If $d_1=d_2=d_3=0$, there is no error, goto stop Else
4. Correct the error by substituting two error free residues from the information moduli and from the redundant residue.
5. Perform consistent check ,IF=Ai(s) = Ai(r)=0 goto Stop Else repeat step 2

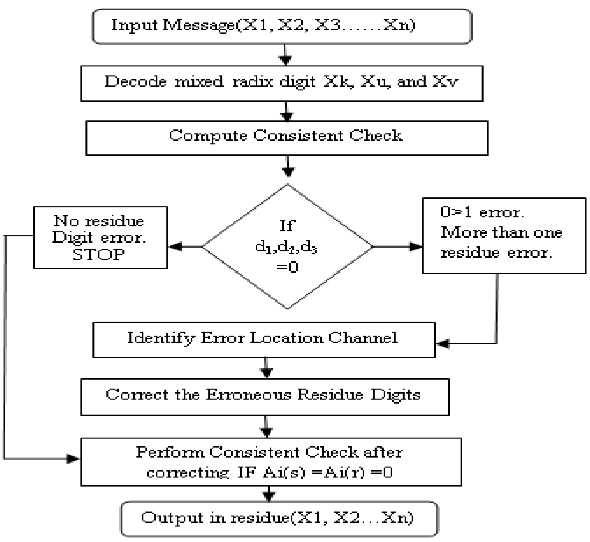

Figure. 2. Flow chart of the proposed Multiple Residue error detection and correction procedure

5. RESULT AND DISCUSSION

Illustrative Example: Suppose given the moduli set {7, 9, 11, 13, 17, 19, 23, 25, 29} where {7, 9, 11} are the information moduli and {13, 17, 19, 23, 25, 29} are the redundant moduli. Therefore, M_u = 693, M_w= 4,199 and M_V=16,675. Since the number of redundant moduli is 6, this RRNS is capable of correcting three residue digit errors. Let the error free residue representation be X = 246 (1, 3, 4, 12, 8, 18, 16, 21, 14). Consider if due to error three residue digit errors were introduced into the received codeword which changed to {1,5,4,12,8,5,0,21,14} Here we consider the first three codeword for decoding.

Step 1: Using MRC The received codeword is decoded as $X_U(154)=554$, $X_w(12,8,5)=2456$ and $X_v=(0,21,14)=10396$.

Step 2: Perform Consistent check to respectively to detect erroneous digit & location. If $d_1=d_2=d_3=0$, there is no error, goto stop
$|554|_7=1$ =1 yes $|554|_9=5=3$=no $|554|_{11}=4=4$=yes $|2456|_{13}=12=12$=yes $|2456|_{17}=8=8$=yes,$|2456|_{19}=18=5$=no $|10396|_{23}=16=0$=no, $|10396|_{25}=21=21$=yes, $|10396|_{29}=14=14$ yes.

Step 3: Since non-zeros occurred, error has occurred in both the information residue and redundant residue. Using base extension method, we can now find redundant residue since in the information moduli m_2, m6 for redundant moduli and m_7 are the error channel. Now we take m_1, m_3, m_4, m_5, m_2 using base extension, to decode the residue for m_2 in the information moduli to replace corrected residue with the error residue respectively for each channel. We then have $|X|''_9=3$ $|X|''_{19}=18$ and $|X|''_{23}=16$. So therefore we can conclude that the received codeword has been corrected for each channel.
Step 4: Perform consistent check, IF=Ai(s) = Ai(r) =0 goto Stop Else repeat step 2 So for $|\Delta|_9 =|3-3|_9 = 0$, $|\Delta|_{19}= |18-18|_{19}= 0$ $|\Delta|_{19}= |16-16|_{23}= 0$ since all $|\Delta|_{9,19,23}$ equals zero respectively then error is corrected

5.1 Discussion Notes and Comparison

The numbers of detectable and correctable residue digit errors are governed by the number of redundant moduli. i.e. with r redundant moduli , RRNS is capable of detecting r and correcting| r/2|.Eliminating look-up table by performing more consistent check. Decoding using CRT requires large compute intensive modulo operation. Legitimate range represents useful computational range while illegitimate range is useful for error and overflow detection. Our algorithm uses MRC which are smaller and needs to be performed sequentially therefore from the first decoding. Comparison of Multiple Residue Digit Error Detection and correction Algorithms can easily identify if error is in a channel.

The algorithm applies base extension and MRC to detect, locate and correct error by eliminating table- look up, therefore the scheme provides a memory less based scheme. Locating error is usually time consuming in most algorithm, but in our algorithm, it uses a pipelining approach to breakdown the problem with a level of complexity O(n) after decoding and performing consistent checks on all the residue, these can be achieved for hardware design we can tell which channel the error has occurred. So therefore we believe the overall delay will be lesser.

The proposed algorithm corrected multiple errors, performs double consistent check because distortion can occur either from the information residue or a redundant residue. Consequently with this property any residue can be restored belonging to the legitimate range of either the information residue or redundant residue, but we believe the decoding time can be improved upon but will eliminate total error, therefore $O \leq X < M$ is satisfied. The proposed algorithm will be more efficient for hardware implementation due to the less complexity in using MRC O(n) and size of modulo operation.

Algorithm	No. of correctable errors	Method		Fixed latency	Memory	Output domain
		Detect Error	Locate Error			
Thian Fatt Tay	Multiple	Syndrome	Syndrome Check	Yes	Yes	Residue
Amusa	Multiple	MRC	Modulus Projection	No	Yes	Integer
Jilu james	Single	MRC	Consistent Check	No	No	Residue
Proposed Algorithm	Multiple	MRC	Double Consistent Check	Yes	No	Residue

6. CONCLUSION

A new multiple residue digit error detection and correction algorithm in RRNS is presented. It requires a small and fixed number of computations with no table look-up compared to other existing algorithm. The hardware implementation of an RNS based application is greatly dependent on the chosen moduli set. The theoretical implementation of the proposed algorithm in this study is explained only with illustrative examples. The advantages of RNS encoding is fast computational blocks , carry free and parallel operations are possible which helps in developing fast digital signal processing(DSP) processors which is the aim of parallel computation. The outcome of this research, which will provide the following expected contributions amongst others:

1. Capability to understand and reason about error detection and correction, and the ability to withstand faults as communication circuits are stochastic in nature and may fail. The ability to cope up with fault will be driven from the parallelisms property of RNS, as a error that occur in one channel will not affect the other channels.
2. The speed of the communication channel will tremendously be increased due to the carry-free property of RNS.
3. Congestion in the communication channel will be reduced as partial representation of actual data will be transmitted, therefore reducing the data traffic in the communication channel. This will increase the general throughput of the communication system.
4. There will be a reduction in energy and memory consumption.
5. Generally the quality of service is expected to improve.

7. REFERENCES

[1] Thian Fatt Tay, Chip-Hong Chang Feb.2016 "A Non-Iterative Multiple Residue Digit Error Detection and Correction Algorithm in RRNS" IEEE transactions on computers, vol. 65, no. 2,

[2] Jilu James , Ameenudeen Pe, Dec.2015,"A Novel Method for Error Correction using Redundant Residue Number System in Digital Communication Systems" International Conference on Advances in Computing, Communications and Informatics (ICACCI)

[3] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393 – 422, 2002. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128601003024

[4] C.-Y. Chong and S. Kumar, "Sensor networks: evolution, opportunities, and chal-lenges," Proceedings of the IEEE, vol. 91, no. 8, pp. 1247 – 1256, aug. 2003.

[5] D. Bagri, J. Statman, and M. Gatti, "Proposed array-based deep space network for nasa," Proceedings of the IEEE, vol. 95, no. 10, pp. 1916 –1922, oct. 2007.

[6] M. Roshanzadeh, A. Ghaffari and S. Saqaeeyan, 2011 "Using Residue Number Systems for Improving QoS and Error Detection & Correction in Wireless Sensor Networks"

[7] Kazeem Alagbe Gbolagade, 2010 "Effective Reverse Conversions in Residue Number Systems Processors" 2010

[8] Amir Sabbagh Molahosseini and Keivan Navi, 2007 "New Arithmetic Residue to Binary Converters "

[9] V. T. Goh and M. Siddiqi, "Multiple error detection and correction based on redundant residue number systems," Communications, IEEE Transactions on, vol. 56, no. 3, pp. 325 – 330, march 2008.

[10] T. Keller, T. Liew, and L. Hanzo, "Adaptive rate RRNS coded OFDM transmission for mobile communication channels," in Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st, vol. 1, 2000, pp. 230 –234 vol.1.

[11] B. Edem and K. Gbolagade. New Efficient FPGA Design of Residue to Binary Converter. International Journal of VLSI design & Communication Systems (VLSICS) Vol. 4, No. 6, Dec, 2013.

[12] Behrouz A.Forouzan, Data Communications and Networking Fourth Edition." Error Detection and Correction " Computer, Vol.23, No.7, pp.267-306,2008