# Reliable Wireless Sensor Networks by Using Redundant Residue Number System

**Ali Barati[1], Ali Movaghar[2], Masoud Sabaei[3], Samira Modiri[4]**

[1]Ph.D Student, Department of Computer Engineering and Information Technology, Qazvin Branch, Islamic Azad University, Qazvin, Iran

[2]Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

[3]Computer and IT Department, Amir-Kabir University of Technology, Tehran, Iran

[4]Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran

abarati@iaud.ac.ir

**Abstract** - In this paper, a new scheme using redundant residue number system is proposed for decreasing the total consumption power and thus, increasing the lifetime, and also to reach error controllability to improve reliability of received data and therewith to obtain improvement in end-to-end delay in wireless sensor networks. The proposed scheme employs the new moduli set $\{2^{2n+2}, 2^{2n-1}-1, 2^{n}-1\}$. Moreover, to complete the new scheme, an efficient reverse converter in both terms of conversion delay and hardware saving is designed and implement based on mixed radix conversion algorithm.

Index Terms - Redundant Residue Number System, Reverse Converter, Mixed-Radix-Conversion, Wireless Sensor Networks

## I . Introduction

Wireless sensor networks technologies with a large number of multifunctional low-power sensor nodes have received tremendous attention because of wide applications in today's world[1]. In such as networks, two critical issues are energy conservation and reliability in data delivery[2]. In this paper, using redundant residue number system in wireless sensor network applications is proposed for solving the said problems.

Redundant residue number systems (RRNSs) are appropriate for use in wireless sensor network, because of 3 factors: 1) strong error controllability, 2) low energy consumption, 3) run-time operations.

In RRNS, by considering some modulus, instead of sending number $X$, the remainders of $X$ are transmitted, so fewer packets are sending and power consumption is reduced. Receiver using a reverse converter decodes the received packets and recovers the original message and then, detects and corrects error, if occurred.

The most important part of any RNS design is moduli set selection, because it has direct effect on system's speed, its dynamic range and area utilization of reverse converter. The reverse converter is responsible to convert back the received data from RNS to conventional representation and is the most complex of any residue to number system design.

In this paper, the new residue number system moduli set $\{2^{2n+2}, 2^{2n-1}-1, 2^{n}-1\}$ is proposed and an efficient reverse converter is designed and implement base on the new moduli set that is suitable for wireless sensor networks with low power resources.

## II. Advantages Of The Proposed Scheme

Because the absence of carry propagation between the arithmetic blocks results in high speed processing, RNS is high speed. This feature is beneficial for wireless sensor networks that need to run-time applications. RNS needs to reduce power. Because of smaller words are transmitted in RNS representation. Thus smaller arithmetic units are realized in the RNS processors that reduce the switching activities in each channel. This results in reduction in the dynamic power, since the dynamic power is directly proportional to switching activities. Therewith, RNS has parallel operations that reduce power consumption and delay simultaneously.

Moreover, noted that WSNs have wide applications and maybe deployed in a hostile environment, such as battlefield. In these conditions, error control and secure data aggregation is critical for WSNs. However data aggregation operation in WSNs improves the bandwidth and energy utilization, but on the other performance metrics such as delay, accuracy, fault-tolerance and security, it may have negative affect [3].

There is a strong conflict between security and data aggregation protocols[4]. An efficient aggregation scheme must implement data aggregation at every intermediate node and decrypt received data packets and encrypt them again after processing at every node, thus it sacrifice data confidentiality, energy and time of overall network.

Redundant RNS is a suitable solution to solve the mentioned problems, because no need to decrypt and encrypt data in every nodes, thus therewith RRNS is secure, it is an energy saving and real-time scheme too. Moreover, the data confidentiality is hold, because in this approach, moduli set acts as secret key, therefore we have secure channels among sensor nodes. Therewith, the most important benefit of using RRNS that it is an error control scheme. The RNS is a non-positional system with no dependence between its channels. Thus, an error in one channel does not propagate to other channels. Therefore, isolation of the faulty residues allows fault tolerance and facilitates error detection and correction.

## III. Design of The Reverse Converter for Proposed Moduli Set

A residue number system is defined in terms of relatively

prime moduli set $\{P_1, P_2 \dots P_n\}$ that is $\gcd(P_i, P_j) = 1$ for $(i \neq j)$. A weighted number $X$ can be represented as $X = (x_1, x_2 \dots x_n)$, where:

$$x_i = X \bmod P_i = |X|_{P_i}, 0 \leq x_i < P_i \quad (1)$$

Such a representation is unique for any integer $X$ in the range $[0, M)$, where $M = (P_1 \times P_2 \times \dots \times P_n)$ is the dynamic range of the moduli set $\{P_1, P_2, \dots, P_n\}$[5]. The residue to binary conversion can be performed using the MRC as follows:

$$X = V_n P_n \dots P_1 + V_3 P_2 P_1 + V_2 P_1 + V_1 \quad (2)$$

The coefficients $V_i P$ can be obtained from residues by:

$$V_1 = x_1 \quad (3)$$

$$V_2 = |(x_2 - x_1)\,|P_1^{-1}|_{P_2}|_{P_2} \quad (4)$$

$$X = V_n P_n \dots P_1 + V_3 P_2 P_1 + V_2 P_1 + V_1 \quad (5)$$

In the general case, we have:

$$V_n = (((x_n - V_1)\,|P_1^{-1}|_{P_n} - V_2)\,|P_2^{-1}|_{P_n} - \dots - V_{n-1})\,|P_{n-1}^{-1}|P_n\,|_{P_n} \quad (6)$$

Where $|P_i^{-1}|\,P_j$ denotes the multiplicative inverse of $P_i$ modulo $P_i$.

Consider the three new modulus in the moduli set $\{2^{2n+2}, 2^{2n-1}-1, 2^n-1\}$ with three corresponding residues $(x_1, x_2, x_3)$. For design a residue to binary converter, firstly need to prove the modulus of proposed moduli set $\{2^{2n+2}, 2^{2n-1}-1, 2^n-1\}$ are in fact pair wise relatively prime for the validity of the RNS. Next, we should to find the multiplicative inverses, and then the values of the multiplicative inverses and modulus must substitute in conversion algorithm formulas. Then, the resulted equations should be simplified by using arithmetic properties. Finally, simplified equations would realize using hardware components such as full adders and logic gates.

Based on Euclid's Theorem:

$$gcd\,(a,b) = gcd\,(b, a \bmod b), \quad a > b \quad (7)$$

Hence:

$$gcd\,(2^{2n+2}, 2^{2n-1}-1) = gcd\,(2^{2n-1}-1, 8) = 1 \quad (8)$$

$$gcd\,(2^{2n+2}, 2^n-1) = gcd\,(2^n-1, 4) = 1 \quad (9)$$

$$gcd\,(2^{2n-1}-1, 2^n-1) = gcd\,(2^n-1, 2^{n-1}-1) = gcd\,(2^{n-1}-1, 1) = 1 \quad (10)$$

Since the greatest common divisors are one, thus the numbers $2^{2n+2}, 2^{2n-1}-1, 2^n-1$ are relatively prime together. In what follows, by use of three propositions, the closed form expressions for the multiplicative inverses under the MRC are derived that form the basis of our algorithm for the reverse converter.

**Proposition 1:** The multiplicative inverse of $(2^{2n+2})$ modulo $(2^{2n-1}-1)$ is $k_1 = 2^{2n-4}$.

Proof:

$$|2^{2n-4} \times 2^{2n+2}|_{2^{2n-1}-1} = 1 \quad (11)$$

**Proposition 2:** The multiplicative inverse of $(2^{2n+2})$ modulo $(2^n-1)$ is $k_2 = 2^{n-2}$.

Proof:

$$|2^{n-2} \times 2^{2n+2}|_{2^n-1} = |2^{3n}|_{2^n-1} = 1 \quad (12)$$

**Proposition 3:** The multiplicative inverse of $(2^{2n-1}-1)$ modulo $(2^n-1)$ is $k_3 = -2$.

Proof:

$$|-2 \times 2^{2n-1} - 1|_{2^n-1} = 1 \quad (13)$$

Therefore, let the values $k_1 = 2^{(2n-4)}$, $k_2 = 2^{(n-2)}$, $k_3 = -2$, $P_1 = 2^{(2n+2)}$, $P_2 = 2^{(2n-1)} - 1$, $P_3 = 2^{n-1}$

In (2-5) and we have:

$$X = x_1 + P_1(V_2 + V_3 P_2) = x_1 + (2^{2n+2})(V_2 + (2^{2n-1}-1)V_3) \quad (14)$$

$$V_1 = x_1 \quad (15)$$

$$V_2 = |(x_2 - x_1)\,|P_1^{-1}|_{P_2}|_{P_2} = |2^{2n-4} \times (x_2 - x_1)|_{2^{2n-1}-1} \quad (16)$$

$$V_3 = |((x_3 - x_1)|P_1^{-1}|_{P_3} - V_2)\,|P_2^{-1}|_{P_3}|_{P_3} = |2^{n-2} \times (x_3 - x_1) + 2 \times V_2|_{2^n-1} \quad (17)$$

According to the following two properties, (14-17) can be simplified to decrease the hardware complexity.

**Property 1[6]:** The residue of a negative residue number ($-v$) in modulo ($2^n$-1) is the one's complement of $v$, where $0 \leq v < (2^n-1)$.

**Property 2[6]:** The multiplication of a residue number $v$ by $2^p$ in modulo ($2^n$-1) is carried out by $P$ bit circular left shift, where $P$ is a natural number.

For designing an efficient reverse converter, simplify (14,16,17) as follow:

$$V_2 = |(x_2 - x_1)\,|P_1^{-1}|_{P_2}|_{P_2} = |2^{2n-4} \times (x_2 - x_1)|_{2^{2n-1}-1} = |2^{2n-4} \times x_2|_{2^{2n-1}-1} + |-2^{2n-4} \times x_1|_{2^{2n-1}-1} = V_{21} + V_{22} \quad (18)$$

Where,

$$V_{21} = |2^{2n-4} \times x_2|_{2^{2n-1}-1} = \underbrace{x_{2,2}x_{2,1}x_{2,0}}_{3\ bits}\underbrace{x_{2,2n-2} \cdots x_{2,3}}_{(2n-4)bits} \quad (19)$$

$$V_{22} = |-2^{2n-4} \times x_1|_{2^{2n-1}-1} = \left\{ \begin{matrix} \overbrace{\bar{x}_{1,2}\bar{x}_{1,1}\bar{x}_{1,0}}^{3\ bits}\overbrace{\bar{x}_{1,2n-2} \cdots \bar{x}_{1,3}}^{(2n-4)bits} + \\ \underbrace{\bar{x}_{1,2n+1}\bar{x}_{1,2n}\bar{x}_{1,2n-1}}_{3\ bits}\underbrace{1 \ldots 1}_{(2n-4)bits} \end{matrix} \right\} \quad (20)$$

For realize $V_3$ based on (17) , we have:

$$\begin{aligned} V_3 &= |((x_3 - x_1)|P_1^{-1}|_{P_3} - V_2)\ |P_2^{-1}|_{P_2}|_{P_3} \\ &= |2^{n-2} \times (x_3 - x_1) + 2 \times V_2|_{2^n-1} \\ &= |2^{n-2} \times x_3|_{2^n-1} + |-2^{n-2} \times x_1|_{2^n-1} + |2 \times V_2|_{2^n-1} \\ &= V_{31} + V_{32} + V_{33} \end{aligned} \quad (21)$$

Where,

$$V_{31} = |2^{n-2} \times x_3|_{2^n-1} = \underbrace{x_{3,1}x_{3,0}}_{2\ bits}\underbrace{x_{3,n-1} \cdots x_{3,2}}_{(n-2)bits} \quad (22)$$

$$V_{32} = |-2^{n-2} \times x_1|_{2^n-1} = \left\{ \begin{matrix} \overbrace{\bar{x}_{1,1}\bar{x}_{1,0}}^{2\ bits}\overbrace{\bar{x}_{1,n-1} \cdots \bar{x}_{1,2}}^{(n-2)bits} + \\ \overbrace{\bar{x}_{1,n+1}\bar{x}_{1,n}}^{2\ bits}\overbrace{\bar{x}_{1,2n-1} \cdots \bar{x}_{1,n+2}}^{(n-2)bits} + \\ \overbrace{\bar{x}_{1,2n+1}\bar{x}_{1,2n}}^{2\ bits}\overbrace{1 \ldots 1 \ldots 1}^{(n-2)bits} \end{matrix} \right\} \quad (23)$$

$$V_{33} = |2 \times V_2|_{2^n-1} = \left\{ \begin{matrix} \overbrace{V_{2,n-2} \cdots V_{2,0}}^{(n-1)bits}\overbrace{V_{2,n-1}}^{1\ bit} + \\ \underbrace{V_{2,2n-2} \cdots V_{2,n}}_{(n-1)bits}\underbrace{0}_{1\ bit} \end{matrix} \right\} \quad (24)$$

Finally, for finding *X* based on (14), we have:

$$X = x_1 + P_1(V_2 + V_3P_2) = x_1(2^{2n+2})(V_2 + (2^{2n-1} - 1)V_3) = x_1 + (2^{2n+2})C \quad (25)$$

$$C = V_2 + (2^{2n-1} - 1)V_3 \quad (26)$$

$$C = \left\{ \begin{matrix} \overbrace{\bar{V}_{3,n-1} \cdots \bar{V}_{3,0}}^{n\ bits}\overbrace{V_{2,2n-2} \cdots V_{2,n}}^{(n-1)bits}\overbrace{\bar{V}_{3,n-1} \cdots \bar{V}_{3,0}}^{n\ bits} + \\ \underbrace{1 \ldots 1 \ldots 1 \ldots 1 \ldots 1}_{(2n-1)bits}\underbrace{V_{2,n-1} \cdots V_{2,0}}_{n\ bits} \end{matrix} \right\} \quad (27)$$

$$X = x_1 + (2^{2n+2})C = Concatenation\ of\ (x_1, C) \quad (28)$$

## IV. Hardware Implementation of The Proposed Reverse Converter

Hardware architecture of the proposed reverse converter for the 3-moduli set $\{2^{(2n+2)}, 2^{(2n-1)}\text{-}1, 2^n\text{-}1\}$ is shown in figure 1. Implementation is based on (18,21,26,28).

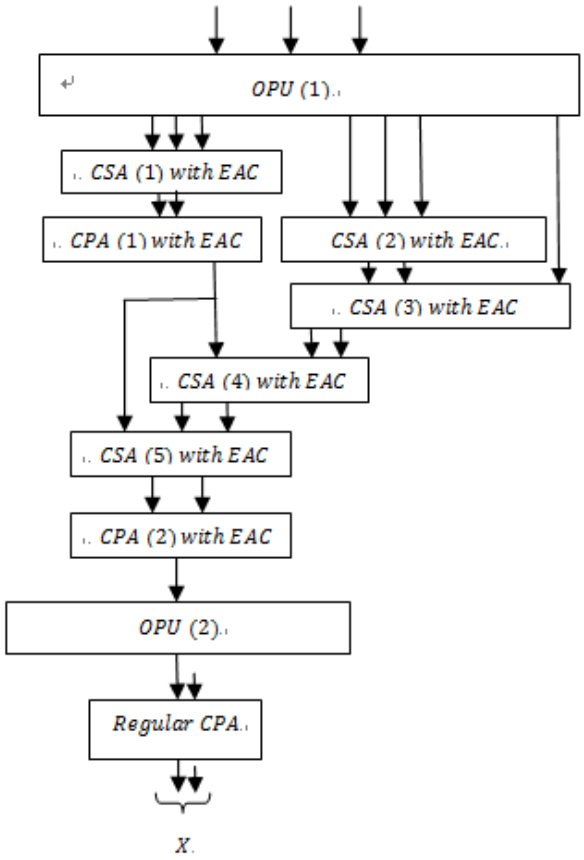


Fig.1. Hardware Implementation of Residue to Binary Converter for the Moduli Set $\{2^{2n+2}, 2^{2n-1} - 1, 2^n - 1\}$

Firstly, the operand preparation unit (1) (OPU (1)) prepares the required operands $(19, 20, 22, 23)$ and these preparation rely on simply manipulating the routing of the bits of the residues. Realization of $(19, 20)$ rely on a $(2n-1)$ –bits carry save adder with end around carry (CSA (1) with EAC) and a $(2n-1)$ –bits carry propagate adder (CPA (1)). $(n - bits)$ – CSA (2) and CSA (3) with EAC are used to implementation of equations $(22, 23)$. In these equations, a FA with a constant input "1" can be reduced to a pair of two-input XNOR and OR gates and a FA with a constant input "0" can be reduced to a pair of two-input XOR and AND gates[7]. Moreover, OPU (2) prepare the required operands for equation $(26)$. Realization of(24) relies on 3-operand $(n - bits)$ – CSA (4, 5) with EAC and a modulo $(2^n - 1)$ adder for implementation of $V_3$ . Finally, implementation of (27) requires a $(3n - 1) - bits$ regular CPA. It should be noted realization of (28) rely on simple concatenation without the use of any computational hardware[8]. Area and delay specifications of each part of the proposed converter are shown in table 1. Then, performance of the proposed reverse converter for new 3-moduli set $\{2^{2n+2}, 2^{2n-1} - 1, 2^n - 1\}$ is compared with the reverse converters that designed for the other moduli sets with the same dynimc range or less in table 2, in terms of area

utilization and delay of operations. Dynamic range is defined as products of modulus in the moduli set and shows the number of integers than we can show uniqely based on this moduli set.

Table.1.Characterization of Each Part of the Proposed Converter.

| *Parts* | *FA* | *Not* | *And/ Xor* | *Or/Xnor* | *Delay* |
|---|---|---|---|---|---|
| $OPU(1)$ | – | $(2n+2)$ | – | – | $t_{NOT}$ |
| $CSA(1)$ | 3 | – | $(2n-4)$ | – | $t_{FA}$ |
| $CPA(1)$ | $(2n-1)$ | – | – | – | $(4n-2)t_{FA}$ |
| $CSA(2)$ | $n$ | – | – | – | $t_{FA}$ |
| $CSA(3)$ | 2 | – | – | $(n-2)$ | $t_{FA}$ |
| $CSA(4)$ | $n$ | – | – | – | $t_{FA}$ |
| $CSA(5)$ | $(n-1)$ | – | 1 | – | $t_{FA}$ |
| $CPA(2)$ | $n$ | – | – | – | $(2n)t_{FA}$ |
| $OPU(2)$ | – | $n$ | – | – | $t_{NOT}$ |
| $CPA(1)$ | $n$ | – | – | $(2n-1)$ | $(3n-1)t_{FA}$ |

$$(7n+3)A_{FA}+(3n+2)A_{NOT}+$$
$$(2n-3)A_{AND}+(2n-3)A_{XOR}+$$
$$(3n-3)A_{OR}+(3n-3)A_{XNOR} \quad (29)$$

$$Total\ Delay: (9n+2)t_{FA}+2t_{NOT} \quad (30)$$

## V . Conclusions

This paper proposes a new scheme for wireless sensor networks applications. The presented scheme is based on redundant residue number system and employs a new 3-moduli set and a reverse converter. An efficient reverse converter based on mixed radix conversion algorithm designs and implements completely. Comparison with the other reverse converters for the moduli sets with the same and even less dynamic range demonstrates the proposed reverse converter has preference in terms of area utilization and speed of operations. Thus the proposed scheme based on the new moduli set and the presented reverse converter is suitable for wireless sensor networks applications that need to reliability, and low-power consumer and fast operations parts.

Table.2.Area and Delay comparison between the proposed reverse converter and related works.

| Converter | Area ($A_{FA}$) | Delay ($t_{FA}$) |
|---|---|---|
| [8] | $8n+2$ | $12n+5$ |
| [9] | $(5n^2+43n)/6+16n-1$ | $18n+7$ |
| [10] | $10n+5$ | $13n+1$ |
| [11] | $12.5n+6$ | $12n+6$ |
| [12] | $10n+5$ | $12n+1$ |
| [13]-1 | $9n+5$ | $11.5n+6$ |
| [13]-2 | $8n+4$ | $9n+6$ |
| [13]-3 | $n^2+12n+12$ | $16n+22$ |
| [13]-4 | $9n+10$ | $11n+14$ |
| [14]-1 | $n^2/2+11n+4$ | $11n+8$ |
| [14]-2 | $n^2+10n+3$ | $9n+6$ |
| [15]-CICE | $2.5n^2+25.5n+12$ | $18n+23$ |
| [15]-CIHS | $2.5n^2+37.5n+28$ | $12n+15$ |
| [15]-C2CE | $20n+17$ | $13n+22$ |
| [15]-C3CE | $23n+11$ | $16n+14$ |
| Proposed | $7n+3$ | $9n+2$ |

## References


[1] J. Yick, B. Mukherjee and D. Ghosal, Elsevier/Computer Networks. 52, 2330 (2008).
[2] S. Naziri, M. Haghparast and S. Hasanpoor, Australian journal of basic and applied sciences. 5 (9) 1105 (2011).
[3] K. Akkaya, M. Demirbas and R.S. Aygun, Wiley wireless communications on mobile computation (WCMC). 8, 171 (2008).
[4] S. Ozdemir and Y. Xiao, Elsevier/computer networks. 53, 2022 (2009).
[5] F. J. Taylor, Computer. 17, 50 (1986).
[6] S. J. Piestrak, IEEE Transactions on circuits and systems. II, Analogue and digital Signal Processing. 42 (10), 661 (1995).
[7] B. Cao, C.H. Chang and T.H. Srikanthan, IEEE Transactions on circuits and systems-I: Fundamental theory and applications. 50 (10), 1296 (2003).
[8] A.S. Molahossenin, K. Navi, C.H. Dadkhah and S. Timarchi, IEEE Transactions on circuits and systems-I: Regular papers. 57 (4), 1 (2010).
[9] B. Cao, C.H. Chang and T.H. Srikanthan, IEEE Transactions on circuits and systems – I: regular papers. 54 (5), 1041 (2007).
[10] A.S. Molahosseini, C.H. Dadkhah and K. Navi, IEICE Electronics Express. 6 (14), 1006 (2009).
[11] M. Esmaeildoust, K. Navi and R. Taheri, IEICE Electronics Express. 7 (3), 118 (2011).
[12] A.S. Molahosseini and M.K. Rafsanjani, World applied sciences. 11 (2), 132 (2010).
[13] P.V.A. Mohan, IEEE Transactions on Circuits and Systems- I: Regular papers. 24 (6), 1245 (2007).
[14] B. Cao, T. Srikanthan and C.H. Chang, IEE Procceeding on computer digital technology. 152 (5), 687 (2005).
[15] P. V. A Mohan, Elsevier/ International journal of electronic communication (AEU). 62 (9), 643 (2008).