J. Basic. Appl. Sci. Res., 2(10)10150-10157, 2012

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

A Reliable & Energy-Efficient Scheme for Real Time Wireless Sensor Networks Applications

Ali Barati[1*], Ali Movaghar[2], Samira Modiri[3], Masoud Sabaei[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]Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran
[4]Computer and IT Department, Amir-Kabir University of Technology, Tehran, Iran

ABSTRACT

Reliability and energy efficiency are the main issues in real time wireless sensor networks applications. In this paper, a new real-time, error control, low energy consumption scheme using redundant residue number system is proposed to enhance the wireless sensor network's lifetime and increase reliability in data delivery. New moduli set $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1, 2^{3n+1}-1, 2^{4n}+1\}$ is proposed that $\{2^{3n+1}-1, 2^{4n}+1\}$ are redundant modulus. Efficient reverse converter for the main modulus $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1\}$ is presented using mixed radix conversion. Using simulation of error control algorithm for the proposed moduli set using C++ programming language by setting $n=2$, error control capability for 145'692 different error bits states is evaluated. Results show that the proposed scheme has considerable excellence in terms of reduction of end to end delay, error control and energy efficiency comparison with the other existing work.
KEYWORDS: Redundant Residue Number Systems, Reverse Converter, Mixed Radix Conversion, Wireless Sensor Networks

1. INTRODUCTION

Recent advancement in wireless communications, Micro Electro Mechanical System (MEMS), and also a tendency to use low cost, tiny, and autonomous high performance products have led to the emergence of wireless sensor networks (WSNs) [1]. The main task of wireless sensor networks is to collect the sensed data from environment and send them back to the sink node to be processed [2]. Because of the dynamic, lossy and low-power nature of sensor networks, important factors in all of these types are reducing energy consumption and reliability [3]. Moreover, some applications of wireless sensor networks need to real time operations such as forest fire detection. Thus end-to-end delay of operations in such as wireless networks is important too.

There are some works considered one or more critical issues in wireless sensor networks, such as delay, error control and energy efficiency. In [4, 5, 6, 7], energy and delay constraints were studied, without reliability consideration in data delivery. RAG [4] is a structure-free real time protocol for data aggregation that has advantages in terms of energy consumption, miss ratio, and aggregation gain. Energy-latency trade offs was explored in [5] using rate adaption techniques. A simple, distributed online protocol relay on the local information available at each sensor node proposed in this work. Authors in [6] presented an energy efficient algorithm for real time wireless sensor networks applications. Using this algorithm, a data aggregation tree under energy and latency constraints can construct. Dynamic time out for data aggregation in wireless sensor networks studied in [7]. In this work, a novel scheme proposed for time out control that can provide efficient trade off between energy consumption and latency in wireless sensor networks. As mentioned before, none of the aforesaid works has not considered the reliability problem in WSNs. In [8], error control for real time industrial wireless sensor networks considered, because in such as wireless networks, reliability is a very important issue. Different FEC codes were compared in terms of memory size requirement and processing time. Golay code, BCH code, and Reed Solomon code were evaluated and the results showed that Reed Solomon (15, 11) is the best. Energy consumption wasn't studied in this paper.

To improve reliability in data delivery, error control schemes such as Automatic Repeat reQuest (ARQ) and Forward Error Correction (FEC) are used. In ARQ-based schemes, the receiver must to detect lost packets and then request the sender to retransmit packets [9], thus it is a slow and energy consumer method. In FEC codes, sensor nodes encode the sensed data before sending them to the sink node, and at the receiver side, this encoded data are decoded, and if some of them were lost or damaged, receiver can reconstruct the original message, if enough number of encoded packets successfully received. In these schemes for transmit data from sensor to the sink, each aggregator must to decode the received data, aggregate them with new data and encrypt them again before sending to the sink. These operations cause to superabundant end-to-end delay and high

***Corresponding Author:** Ali Barati, Ph.D Student, Department of Computer Engineering and Information Technology, Qazvin Branch, Islamic Azad University, Qazvin, Iran, Tel: + 98 641 6262090, Email: abarati80@yahoo.com

energy consumption, thus cause to decrease the network lifetime. Thus these schemes are not suitable for real time applications. Thereupon, it is necessary to find a new solution with low power consumption that simultaneously provides proper reliability in real time wireless sensor networks applications. Redundant residue number systems (RRNSs) are appropriate for use in real time wireless sensor networks applications, because of obtaining enhancement in 4 factors: 1) real time operations, 2) strong error control capability, 3) energy saving, and 4) security. In this systems, by considering some modulus, instead of sending number X, the remainders of X is transmitted, so less packets are send and power consumption is reduced. In the receiver side using a reverse converter, the received packets are decoded and the original message is recovered.

In this paper, a new high speed, reliable and low energy consumer using redundant residue number system is proposed and for create it, a new three moduli set $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1\}$ is presented and an efficient reverse converter in terms of area utilization and speed of operations is designed. Moreover by adding two redundant modulus $\{2^{3n+1}-1, 2^{4n}+1\}$ to the new three main moduli set, a new five-moduli set is created that enables error control capability in the proposed scheme. Finally, error detection and correction capability of the proposed scheme will be evaluated.

The rest of this paper is organized as follows: In section 2 the preferences of the proposed scheme comparison with the other existent works are presented. An efficient reverse converter for the new proposed 3-main moduli set $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1\}$ is designed in section 3. In section 4, error control performance of the proposed moduli set, $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1, 2^{3n+1}-1, 2^{4n}+1\}$ is evaluated using simulation of redundant residue number system algorithm's functionality for the proposed moduli set using C++ language programming. Finally, the paper is concluded in section 5.

2. PREFERENCES OF THE PROPOSED SCHEME

Residue number system is an unconventional, high speed, and fault tolerance number system. By using redundant residue number systems in wireless sensor networks, below excellences will be acquired:

1. High speed operations: In residue number systems, the calculations are performed paralleled, that cause to increase the speed of the operations. Moreover, in often schemes that using data aggregation, in each aggregator node must accomplish 3 phases: decryption the received data, aggregation, and encryption the aggregated data again. But using the proposed scheme, in each aggregator node, no need to decrypt the received data, and encrypt them again after aggregation operation. Only aggregation process is accomplished, and no need to consume energy and time for the other 2 phases. If the numbers of nodes be very large, these decreases will be very salient.

2. Energy efficiency: Hardware requirement and complexity for data aggregation is reduced and small arithmetic units are used using the proposed scheme, because the remainders of the sensed data are sent by sensors, instead of data itself. Therefore, energy consumption is very low and speed of operations increased.

3. Error detection and correction capability: by adding some redundant modulus to the residue number system, redundant residue number system is created that has error control capability. Moreover in such as systems, if error occurs in one modulo, it is not propagates between the other residues.

4. Security: Because the remainders of sensed data are sent instead of data itself, the received packet is encrypted and for decrypt the message, need to have the moduli set. Thus the moduli set act as secret key. In the proposed scheme, the sink node using the modulus, decrypt the received packets and recover the original message. If an adversary can acquire the transmitted message, while he doesn't know the moduli set, he can not decrypt this message.

5. Confidentiality: As mentioned above, in often proposed scheme for data aggregation in wireless sensor networks, in each aggregator, the received message will be decrypt, and encrypt again after accomplishment of aggregation operations. These two phases cause to the encrypted data lie in danger, and maybe an adversary can achieve the transmitted massage easily. But using the proposed scheme, the confidentiality of data will be preserved.

3. DESIGN AND IMPLEMENTATION OF THE PROPOSED REVERSE CONVERTER

A residue number system is defined in terms of relatively prime moduli set $\{P_1, P_2, \ldots, P_n\}$ that is $\gcd(P_i, P_j) = 1$ for $(i \neq j)$. A weighted number X can be represented as $X = (x_1, x_2 \ldots x_n)$ 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 $M = P_1 P_2 \ldots P_n$ is the dynamic range of the moduli set $\{P_1 P_2 \ldots P_n\}$. [10]. The residue to binary conversion can be performed using the MRC as follows:

$$X = V_n \prod_{i=1}^{n} P_i + \cdots + V_3 P_2 P_1 + V_2 P_1 + V_1 \quad (2)$$

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

$$V_1 = x_1 \tag{3}$$

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

$$V_3 = |((x_3 - x_1)|P_1^{-1}|_{P_3} - V_2)\,|P_2^{-1}|_{P_3}|_{P_3} \tag{5}$$

In the general case, we have:

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

Where $|P_i^{-1}|_{P_j}$ is multiplicative inverse of of P_i modulo P_j. The modular multiplicative inverse of a moduli m can be found using the extended Euclidean algorithm.

According to the above equations, the proposed reverse converter for the new 3-moduli set can be designed as follows: Consider the three-moduli set with three corresponding residues (x_1, x_2, x_3). For design of a residue to binary converter, firstly need to prove that the modulus of proposed moduli set are in fact pair wise relatively prime for the validity of the RNS. Next, should to find the multiplicative inverses, and then the values of the multiplicative inverses and moduli set must be substituted in the conversion algorithm formulas. Then, the resulted equations should be simplified using arithmetic properties. Finally, simplified equations would be realized using hardware components such as full adders and logic gates. Based on Euclid's Theorem, we have:

$$\gcd(a, b) = \gcd(b, a \bmod b),\ a > b \tag{7}$$

Hence,

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

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

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

Since the greatest common divisors are 1s in $(8-10)$, thus the numbers $< 2^{2n+1} + 2^n - 1, 2^{2n+1}, 2^n - 1 >$ are relatively prime together. In what follows, using three propositions $(1-3)$, the closed form expressions for the multiplicative inverses under the MRC algorithm are derived that form the basis of our algorithm for the proposed reverse converter.

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

$$|-2^{2n+1} - 2^n + 1|_{2^{2n+1}} = 1 \tag{11}$$

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

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

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

$$|2^{n-1} \times 2^{2n+1}|_{2^n-1} = |2^{3n}|_{2^n-1} = 1 \tag{13}$$

Therefore, let the values $< k_1 = -1, k_2 = 2^{n-1}, k_3 = 2^{n-1}, P_1 = 2^{2n+1} + 2^n - 1, P_2 = 2^{2n+1}, P_3 = 2^n - 1 >$ in $(2-5)$and we have:

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

$$V_1 = x_1 \tag{15}$$

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

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

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

Property 1: The residue of a negative residue number $(-v)$ in modulo $(2^n - 1)$ is the one's complement of v, where $0 \le v < (2^n\text{-}1)$ [11].

Property 2: 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 [11].

For designing an efficient reverse converter, firstly we must to design V_2 based on (16), then designing V_3 is performed based on (17), because for designing V_3, we need to have the value V_2. Finally, X is designed based on (14). For (15), no need to design anything, and input x_1 is connected straightly to the port V_1. Using FAs, carry save adders ($CSAs$) with end around carry (EAC) and carry propagation adder (CPA) with EAC, the proposed reverse converter is implemented. For designing V_2, simplify (16) as follows:

$$V_2 = \left|(x_2 - x_1)|P_1^{-1}|_{P_2}\right|_{P_2} = |x_1 - x_2|_{2^{2n+1}} = |x_1|_{2^{2n+1}} + |-x_2|_{2^{2n+1}} = V_{21} + V_{22} \tag{18}$$

$$V_{21} = |x_1|_{2^{2n+1}} = \underbrace{x_{1,2n}\, x_{1,2n-1} \dots x_{1,0}}_{(2n+1)bits} \tag{19}$$

$$V_{22} = |-x_2|_{2^{n+1}} = \underbrace{\bar{x}_{2,2n}\, \bar{x}_{2,2n-1} \dots \bar{x}_{2,0}}_{(2n+1)\text{bits}} \tag{20}$$

For implementation of V_2 based on (19, 20), we need to a $(2n+1) - bits\ CPA\ with\ EAC$, because we have two $(n+1) - bits$ inputs, one input in (19) and another in (20). Figure 1 shows the realization of V_2. Note that there are $(2n+1)$ one complements in (20) that are prepared using $(2n+1) NOT\ gates$ by OPU 1.

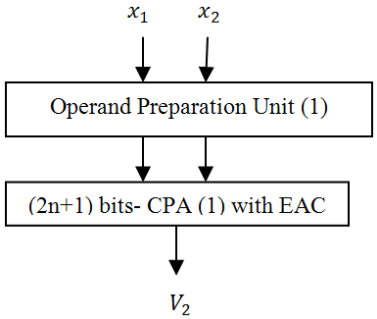

Figure 1: Implementation of V_2 based on (19, 20)

Now, for realize V_3 based on (17), we have:

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

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

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

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

For implementation of V_3 based on $(22 - 24)$, we need to five $(n) - bits\ CSAs\ with\ EAC$, because there are seven $(n) - bits$ inputs and each $CSA\ with\ EAC$ has three inputs and two outputs. Thus, a tree of seven $CSAs\ with\ EAC$ will be created, and for realization of $(2^n - 1)$modulo adder, need to use a $(n) - bits\ CPA\ with\ EAC$. Realization of V_3 is shown in Figure 2. Note that in (23) and (24), we have $(n-2)$ and $(n-1)$ consecutive 1s, respectively. Thus $(n-2)\ and\ (n-1) FAs$ can be substituted by $(n-2)\ and\ (n-1) pairs\ of\ OR/XNOR\ gates$ in $CSA\ 2\ and\ CSA\ 5\ with\ EAC$, respectively. Moreover, for implementation of

(23) and (24), we need to $(2n+2)$ and $(2n+1)$ $NOT\ gates$, respectively, that are prepared using $OPU\ 1\ and\ OPU\ 2$, respectively.

Finally, to find X based on (14), we have:

$$X = x_1 + P_1\,(V_2 + V_3\,P_2) = x_1 + (2^{2n+1} + 2^n - 1)\underbrace{(V_2 + (2^{2n+1})V_3)}_{C} = x_1 + (2^{2n+1} + 2^n - 1)C \tag{25}$$

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

$$C = Concatenation\ (V_2, V_3) \tag{27}$$

$$X = x_1 + (2^{2n+1} + 2^n - 1)C$$

$$= \left\{ \begin{array}{c} \overbrace{\bar{C}_{3n}\,\bar{C}_{3n-1} \dots \bar{C}_{2n}}^{(n+1)bits}\ \overbrace{\bar{C}_{2n-1} \dots \bar{C}_{n}}^{n\ bits}\ \overbrace{\bar{C}_{n-1} \dots \bar{C}_{0}}^{n\ bits}\ \overbrace{\bar{C}_{n}\bar{C}_{n-1} \dots \bar{C}_{0}}^{(n+1)bits}\ \overbrace{\bar{C}_{n} \dots \bar{C}_{0}}^{n\ bits} \\ \overbrace{0\ 0 \dots .0 \dots .0}^{(n+1)bits}\ \overbrace{\bar{C}_{3n} \dots \bar{C}_{2n+1}}^{n\ bits}\ \overbrace{\bar{C}_{2n} \dots \bar{C}_{n+1}}^{n\ bits}\ \overbrace{\bar{C}_{2n}\bar{C}_{2n-1} \dots \bar{C}_{n}}^{(n+1)bits}\ \overbrace{x_{1,n-1} \dots x_{1,0}}^{n\ bits} + \\ \underbrace{1\ 1 \dots .1 \dots 1 \dots .1}_{(n+1)bits}\ \underbrace{\bar{C}_{3n} \dots \bar{C}_{2n+1}}_{n\ bits}\ \underbrace{x_{1,2n}x_{1,2n-1} \dots x_{1,n}}_{(n+1)bits}\ \underbrace{0 \dots .0 \dots .0 \dots .0}_{n\ bits} \\ \underbrace{0\ 0 \dots .0. \dots 0 \dots .0 \dots .0 \dots 0 \dots .0 \dots .0 \dots .0}_{(3n)bits}\ \underbrace{x_{1,2n+1}}_{1\ bit}\ \underbrace{0 \dots 0 \dots 0 \dots .0 \dots 0}_{(2n+1)bits} \end{array} \right\} \tag{28}$$

As shown in (27), realizing of C no need to hardware requirement, and is based on a simple concatenation. For implementation of (28), we need to two $(5n+2) - bits\ CSAs\ with\ EAC$ and a $(5n+2) - bits\ Regular\ CPA$. Implementation of X is shown in Figure 3.

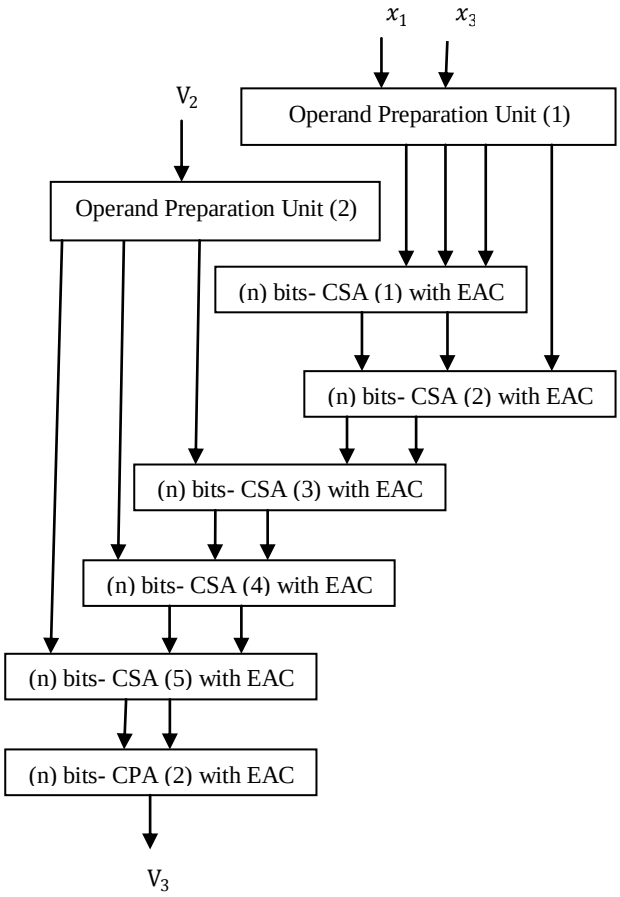

Figure 2: Implementation of V_3 based on $(22-24)$

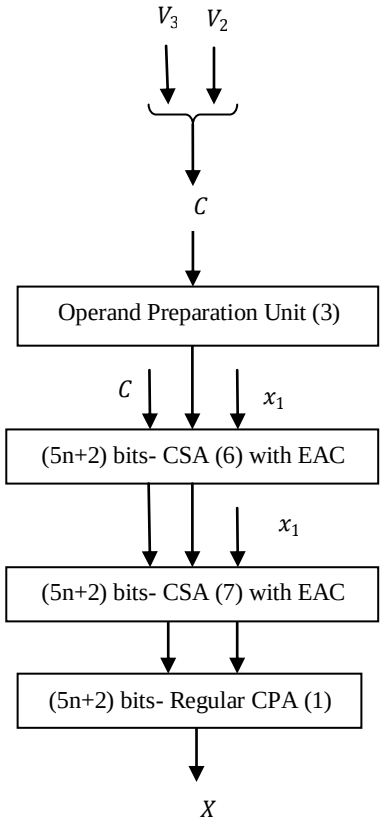

Figure 3: Implementation of X based on $(27, 28)$

Note that in the third row in (28), we have $(2n+1)$ and (n)consecutive 1s and 0s, respectively. Thus in $CSA\ 6$, $(2n+1)and\ (n)FAs$ can be substituted by $(2n+1)and\ (n)pairs\ of\ OR/XNOR$ and

$AND/XOR\ gates$, respectively. Moreover, in (28), we need to $(3n+1)NOT\ gates$ that are prepared by OPU 3. Addition to these, in the forth row of (28), $(5n+1)FAs$can be substituted by $(5n+1)pairs\ of\ AND/XOR\ gates$. Area and delay specifications of each requirement part for implementation of the proposed reverse converter are shown in Table 1. Using Table 1, total hardware requirement (hardware complexity) and delay of retrieving the original data can be calculated. These values are shown in (29) and (30).

Then, specification comparison of the proposed reverse converter for new moduli set $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1\}$ with the reverse converters with the same or less dynimc range is shown in Table 2.

Finally, performance evaluation of the proposed scheme is shown in the next section.

Table 1: Hardware requirements for implementation of the proposed reverse converter based on the new three moduli set $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1\}$

$Parts$	FA	NOT	AND/XOR	$OR/XNOR$	$Delay$
$OPU\ 1$	$-$	$(4n+3)$	$-$	$-$	t_{NOT}
$CPA\ 1$	$(2n+1)$	$-$	$-$	$-$	$(4n+2)t_{FA}$
$CSA\ 1$	n	$-$	$-$	$-$	t_{FA}
$CSA\ 2$	2	$-$	$-$	$(n-2)$	t_{FA}
$OPU\ 2$	$-$	$(2n+1)$	$-$	$-$	t_{NOT}
$CSA\ 3$	n	$-$	$-$	$-$	t_{FA}
$CSA\ 4$	n	$-$	$-$	$-$	t_{FA}
$CSA\ 5$	1	$-$	$-$	$(n-1)$	t_{FA}
$CPA\ 2$	n	$-$	$-$	$-$	$(2n)t_{FA}$
$OPU\ 3$	$-$	$(3n+1)$	$-$	$-$	t_{NOT}
$CSA\ 6$	$(2n+1)$	$-$	n	$(2n+1)$	t_{FA}
$CSA\ 7$	1	$-$	$(5n+1)$	$-$	t_{FA}
$R-CPA$	$(5n+2)$	$-$	$-$	$-$	$(5n+2)t_{FA}$

$$Total\ area = (13n+8)A_{FA} + (9n+5)A_{NOT} + (6n+1)A_{AND} + (6n+1)A_{XOR} + (4n-2)A_{OR} + (4n-2)A_{XNOR} \quad (29)$$

$$Total\ delay = (11n+11)t_{FA} + 3t_{NOT} \quad (30)$$

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

	$Moduli\ set$	DR	$Area\ (A_{FA})$	t_{FA}
[12]	$\{2^n-1, 2^n, 2^n+1, 2^{2n+1}-1\}$	$5n+1$	$8n+2$	$12n+5$
[13]	$\{2^n-1, 2^n, 2^n+1, 2^{n-1}-1, 2^{n+1}-1\}$	$5n$	$(5n^2+43n)/6+16n-1$	$18n+7$
[14]	$\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$	$5n-1$	$10n+5$	$13n+1$
[15]	$\{2^n, 2^{2n+1}-1, 2^{n/2}-1, 2^{n/2}+1, 2^n+1\}$	$5n+1$	$12.5n+6$	$12n+6$
[16]	$\{2^n, 2^{n/2}-1, 2^{n/2}+1, 2^n+1, 2^{2n-1}-1\}$	$5n-1$	$10n+5$	$12n+1$
[17] − 1	$\{2^n, 2^n-1, 2^n+1, 2^{n+1}-1\}$	$4n+1$	$9n+5$	$11.5n+6$
[17] − 2	$\{2^n, 2^n-1, 2^n+1, 2^{n+1}+1\}$	$4n+1$	$n^2+12n+12$	$16n+22$
[17] − 3	$\{2^n, 2^n-1, 2^n+1, 2^{n+1}+1\}$	$4n+1$	$9n+10$	$11n+14$
[18]	$\{2^n, 2^n-1, 2^n+1, 2^{n+1}-1\}$	$4n+1$	$n^2/2+11n+4$	$11n+8$
[19] − 1	$\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$	$4n$	$2.5n^2+25.5n+12$	$18n+23$
[19] − 2	$\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$	$4n$	$2.5n^2+37.5n+28$	$12n+15$
[19] − 3	$\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$	$4n$	$20n+17$	$13n+22$
[19] − 4	$\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$	$4n$	$23n+11$	$16n+14$
$Proposed$	$\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1\}$	$5n+3$	$13n+8$	$11n+11$

4. PERFORMANCE EVALUATION

As mentioned before, in section 2, the proposed scheme is reliable, real time and energy efficient. In this section, the performance of the proposed moduli set $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1, 2^{3n+1}-1, 2^{4n}+1\}$ is evaluated in terms of error detection and error correction capability. Firstly we must to explain that why these two redundant modulus were selected for the proposed main modulus. Note that the redundant modulus must be greater than the main modulus, and all of the modulus including the main and redundant modulus must be primed together. In the proposed moduli set,$\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1, 2^{3n+1}-1, 2^{4n}+1\}$ it is obvious that the redundant moduli are bigger than the main modulus. For indicate that the modulus in the proposed

moduli set are pair wise prime, only need to show each redundant modulo is prime respect to each main modulo, and the redundant modulus are prime together. Because before, in the previous section, we demonstrate that the main modulus are prime together. Based on Euclid's theorem (equation (7)), we have:

$$\gcd(2^{3n+1}-1, 2^{2n+1}+2^n-1) = 1 \tag{31}$$

$$\gcd(2^{3n+1}-1, 2^{2n+1}) = \gcd(2^{2n+1}, -1) = 1 \tag{32}$$

$$\gcd(2^{3n+1}-1, 2^n-1) = \gcd(2^n-1, 1) = 1 \tag{33}$$

$$\gcd(2^{4n}+1, 2^{2n+1}+2^n-1) = 1 \tag{34}$$

$$\gcd(2^{4n}+1, 2^{2n+1}) = \gcd(2^{2n+1}, 1) = 1 \tag{35}$$

$$\gcd(2^{4n}+1, 2^n-1) = \gcd(2^n-1, 2) = 1 \tag{36}$$

$$\gcd(2^{4n}+1, 2^{3n+1}-1) = \gcd(2^{3n+1}-1, 2^{n-1}+1) = \gcd(2^{n-1}+1, -2) = 1 \tag{37}$$

It is obvious from $(31-37)$ that the redundant modulus are prime together and are prime against the main modulus, thus these redundant modulus are suitable for these three main modulus.

The proposed moduli set $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1, 2^{3n+1}-1, 2^{4n}+1\}$ can correct up to $(2n+2$adjacent error bits, while the error bits sat in the first modulo of the received remainders. For study the error detection capability, we consider a special case of the proposed moduli set by setting $n=2$. As result, the proposed moduli set is equal to $\{35, 32, 3, 127, 257\}$ that $\{35, 32, 3\}$ are the main modulus and $\{127, 257\}$ are redundant modulus. Error detection capability in this special case is up to 6 bits, because by setting $n=2$ in $(2n+2)$, the number 6 is acquired. For study the error detection capability, we study 18 different sent numbers that have error bits in more than one moduli. Thus error correction is impossible. These numbers are in $X \in [0, 3360)$ that is equal to dynamic range of the moduli set $\{35, 32, 3\}$, because $35 \times 32 \times 3 = 3'360$. The selected numbers are {0, 200, 400, 600, 800, 1'000, 1'200, 1'400, 1'600, 1'800, 2'000, 2'200, 2'400, 2'600, 2'800, 3'000, 3'200, 3'359}. Overall, $150'000$ error bits are considered. The results are shown in Figure 4.

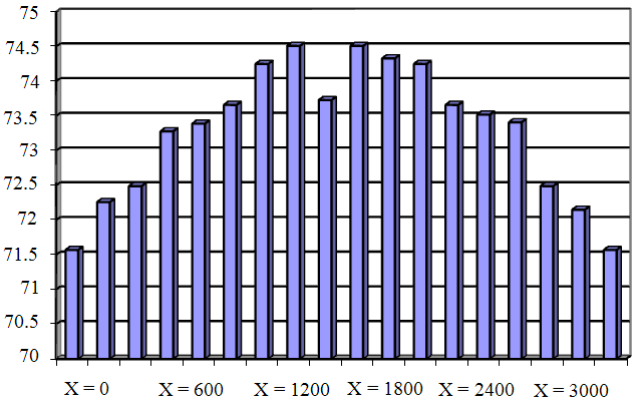

Figure 4: Percent of error detection capability of the proposed scheme by setting $n=2$ for 18 different sent data by considering $150'000$ different error bits states

It is obvious from Figure 1 that the percent of error detection is always more than 71%. The best percent of error detection capability is 74.51% and in the worst case, it is 71.57%, as shown in the Figure 1, and the average percent of the error detection for 150'000 under consideration error bits states is equal to 73.28%.

5. CONCLUSION

This paper presents a new high speed, reliable and energy efficient scheme for real time wireless sensor networks applications. For create the proposed scheme, a new moduli set $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1, 2^{3n+1}-1, 2^{4n}+1\}$ presents that the modulus $\{2^{2n+1}+2^n-1, 2^{2n+1}, 2^n-1\}$ are the main modulus and the modulus $\{2^{3n+1}-1, 2^{4n}+1\}$ are redundant modulus. Moreover, an efficient reverse converter based on mixed radix conversion designs for the main proposed moduus that has supremacy in terms of hardware requirement and speed of operations comparison with the other reverse converters for the moduli sets with the same or less

dynamic ranges. Addition to these, error control capability of the proposed moduli set for the proposed scheme evaluates using simulation of error detection and correction algorithm by C++ programming language by setting $n = 2$ in the proposed moduli set $\{2^{2n+1} + 2^n - 1, 2^{2n+1}, 2^n - 1, 2^{3n+1} - 1, 2^{4n} + 1\}$, and for 18 different sensed sent data under consideration of $150'000$ error bit states, error detection capability studies. The results show that the proposed scheme can detect error bits with the probability of 73.28% on average. Moreover, in the special case (n=2), the error detection and correction algorithm can correct up to 6 error bits. As totality results, the proposed scheme has excellent preference in terms of real time operations, reliability in data delivery and energy efficiency comparison with the other schemes in wireless sensor networks.

REFERENCES

1. Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. A survey on sensor networks. IEEE Communications Magazine, 40:102-114.
2. Naziri, S., M. Haghparast and S., Hasanpoor, 2011. Improving lifetime and reliability in routing real-time wireless sensor networks based on hybrid algorithms. Australian Journal of Basic and Applied Sciences, 5 (9): 1105-1109.
3. Khodadoustan, S., F. Jalali and A. Ejlali, 2011. Reliability/energy trade-off in Bluetooth error control schemes. Elsevier/Microelectronics Reliability, 51: 1398-1412.
4. Yousefi, H., M.H. Yeganeh, N. Alinaghipour and A. Movaghar, 2012. Structure-free real-time data aggregation in wireless sensor networks. Elsevier/ Computer Communications, 35 (9): 1132-1140.
5. Yu, Y., V.K. Prasanna and B. Krishnamachari, 2006. Energy minimization for real-time data gathering in wireless sensor networks. IEEE Transactions on Wireless Communications, 5 (11): 1-11.
6. Du, H., X. Hu and X. Jia, 2006. Energy efficient routing and scheduling for real time data aggregation in WSNs. Elsevier/ScienceDirect. 29 (17): 3527-3535.
7. Kwon, S., J.H. Ko, J. Kim and C. Kim, 2011. Dynamic timeout for data aggregation in wireless sensor networks. Elsevier/computer networks, Computer Networks, Elsevier, 55 (3): 650-664.
8. Yu, K., M. Gidlund, J. Åkerberg and M. Björkman., 2011. Reliable and low latency transmission in industrial wireless sensor networks. Elsevier/ScienceDirect, 5: 866-873.
9. Guo, Z., B. Wang, P. Xie, W. Zeng and J.H. Cui, 2009. Efficient error recovery with network coding in underwater sensor networks. Elsevier/ Ad Hoc Networks, 7: 791-802.
10. Taylor, F.J, 1986. Residue arithmetic: A tutorial with examples. IEEE Computer Magazine, 17 (5): 50-62.
11. Piestrak, S.J., 1995. A high speed realization of a residue to binary converter. IEEE Transactions on circuits and systems. II, Analogue and Digital Signal Processing, 42 (10): 661-663.
12. Molahossenin, A. S., K. Navi, C. Dadkhah, O. Kavehei, S. Timarchi, 2010. Efficient reverse converter designs for the new 4-moduli sets $\{2^n\text{-}1, 2^n, 2^n\text{+}1, 2^{2n+1}\text{-}1\}$ and $\{2^n\text{-}1, 2^n\text{+}1, 2^{2n}, 2^{2n}\text{+}1\}$ based on new CRTs. IEEE Transactions on Circuits and Systems-I: Regular papers, 57 (4): 1-13.
13. Cao, B., C.H. Chang and T.H. Srikanthan, 2007. A residue to binary converter for a new five moduli set. IEEE Transactions on Circuits and Systems – I: regular papers, 54 (5): 1041-1049.
14. Molahosseini, A.S., C.H. Dadkhah and K. Navi, 2009. A new five moduli set for efficient hardware implementation of the reverse converter. IEICE Electronics Express, 6 (14): 1006-1012.
15. Esmaeildoust, M., K. Navi and R. Taheri, 2011. High speed reverse converter for new five-moduli set $\{2^n, 2^{2n+1}\text{-}1, 2^{n/2}\text{-}1, 2^{n/2}\text{+}1, 2^n\text{+}1\}$. IEICE Electronics Express, 7 (3): 118-125.
16. Molahosseini, A.S. and M.K. Rafsanjani, 2010. An improved five-modulus reverse converter. World Applied Sciences, 11 (2): 132-135.
17. Mohan, P.V.A. and A.B. Premkumar, 2007. RNS to binary converters for two four moduli set $\{2^n\text{-}1, 2^n, 2^n\text{+}1, 2^{n+1}\text{-}1\}$ and $\{2^n\text{-}1, 2^n, 2^n\text{+}1, 2^{n+1}\text{+}1\}$. IEEE Transactions on Circuits and Systems- I: Regular papers, 24 (6): 1245-1254.
18. Cao, B., T. Srikanthan and C.H. Chang, 2005. Efficient reverse converters for four moduli sets $\{2^n\text{-}1, 2^n, 2^n\text{+}1, 2^{n+1}\text{-}1\}$ and $\{2^n\text{-}1, 2^n, 2^n\text{+}1, 2^{n-1}\text{-}1\}$. IEE Proceedings on Computer Digital Technology, 152 (5): 687-696.
19. Mohan, P.V.A, 2008. New reverse converters for the moduli set $\{2^n\text{-}3, 2^n\text{-}1, 2^n\text{+}1, 2^n\text{+}3\}$. Elsevier/ International Journal of Electronics and Communications (AEU), 62 (9): 643- 658.