*I. J. Computer Network and Information Security,* **2012, 2, 29-35**
Published Online March 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.02.05

# Error Detection & Correction in Wireless Sensor Networks By Using Residue Number Systems

M. Roshanzadeh
Department of Computer, Abadan Branch, Islamic Azad University, Abadan, Iran
Email: mohsen.mrz@gmail.com

S. Saqaeeyan
Department of Computer, Abadan Branch, Islamic Azad University, Abadan, Iran
Email: sasan_sagha@yahoo.com

*Abstract*— **Wireless Sensor Networks have potential of significantly enhancing our ability to monitor and interact with our physical environment. Realizing a fault tolerant operation is critical to the success of WSNs. The integrity of data has tremendous effects on performance of any data acquisition system. Noise and other disturbances can often degrade the information or data acquired from these systems. Devising a fault-tolerant mechanism in wireless sensor networks is very important due to the construction and deployment characteristics of these low powered sensing devices. Moreover, due to the low computation and communication capabilities of the sensor nodes, the fault-tolerant mechanism should have a very low computation overhead. In this paper we focus our work on low complexity error detection technique which can be implemented with low data redundancy and efficient energy consuming in wireless sensor node by using of Residue Number Systems.**

*Index Terms*—**Wireless Sensor Networks, Performance, QOS, Error Detection & Correction, Residue Number Systems (RNS).**

## I. Introduction

A Wireless Sensor Network (WSN) is a set of sensor nodes that can communicate wirelessly with each other across an extended environment [1]. Typically, a WSN is comprised of numerous tiny sensor nodes (or sensors for short) deployed in an environment for monitoring and tracking purposes. They are presented in various areas such as: life sciences, medical care and the vital signs, military affairs and development, and in general wherever it is needed to measure the physical quantity. Sensed data are aggregated and at times, stored "in-network" at sink nodes which may themselves be sensors or other nodes richer in capabilities and resources. Data are then communicated to the end users either periodically or on-demand through the sinks or a higher order node; the base station. Clearly, WSNs find numerous applications ranging from healthcare to crisis management and warfare. The problem of fault identification and isolation is generally a hard task in sensor networks due to the very nature of their construction and deployment.

In a fault-tolerant approach for sensor network is proposed by using back-up sensors for faulty ones [2]. Propose approach to reduce noise and uncertainty in sensor networks. This however assumes prior knowledge of true sensor reading. In [3], the author proposes an Evolvable Hardware (EHW) design to reprogram circuit in case of any faults occurring in the sensors. In order to detect faults in the sensors the paper proposes to use spatial correlation and Kalman Filter (to estimate actual output). Our proposed approach is similar to one proposed method [3], however we use Weighted function to reduce the "contribution" of faulty sensors instead of reprogramming the circuit. The advantage of our proposed fault tolerant mechanism is that, in general, it does not rely on the sensors to be geographically deployed close to each other. Also we use of Residue Number Systems (RNS) for reduce overhead and increase security in Wireless Sensor Networks (WSNs). A sensor network consists of hundreds or thousands of tiny sensor nodes which are randomly spread out over an area of interest. The objective is to measure values in the environment and propagate this information to data sinks of the system. I.F. Akyildiz gives a very comprehensive and detailed introduction on sensor networks in [1].

A sensor node typically consists of a battery, a microprocessor, a communication module, sensors and/or actuators. Due to the desired node's size of some millimeters, the dimensions of the communication module and the battery are critical. Consequently, the scarcest resource within a network is the available energy. Therefore, it is essential to use low power optimized algorithms beside power saving hardware components. Simple uncoordinated seeding of nodes yields a stochastic distribution of nodes after deployment phase. This impedes the assignment of a measured value to its location. Due to this fact, a position determination of all nodes is necessary which, however, consumes additional energy for calculations and data transmissions.

Types of bit error in wireless communication can be classified as either random errors or burst errors. The random bit error can appear at any location in a sequence of data transmission or radio packet. On the other hand, burst error occurs in a number of consecutive bits in a sequence of digital data transmission. A source of burst error could originate from long duration of disturbance that is larger than one bit duration or interference such as lightning or collision of communication packets over the radio channel. For wireless sensor network, the errordetection and correction services are usually provided by communication protocols at the data link and the transport layers in the OSI model. Generally, 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. For wireless sensor node that usually possesses limited resources in computational complexity and power budget, an efficient and low complexity error detection scheme is required. Unfortunately, some efficient error detection techniques are not suitable for wireless sensor networks because it may require large block of data and higher overhead. Simple error detection such as parity check bit is too weak for wireless communication in which quality of radio channel is often poor and burst errors often occurs. In this study we focus our work on low complexity error detection technique which can be implemented with low complexity data compression in wireless sensor node. In this study we focus our work on low complexity error detection technique which can be implemented with low complexity data compression in wireless sensor node.

The remainder of the paper is arranged as follows. In Section-II related works are presented. Section-III provides the background about Wireless Sensor Networks and also some of problems in WSN. The detail of the Residue Number Systems has been discussed in Section-IV. In Section-V, error detection & correction by RNS are shown. RRNS QC Encoder/Decoder is discussed in Section-VI and in section-VII improving performance in wireless sensor network such as: Reduce traffic and data transmission and energy efficiently is proposed. Finally, in the section-VIII conclusions are presented.

## II. Related Work

Although there have been several studies on error control techniques in wireless networks and especially in cellular networks, none of them are directly applicable to WSNs. Especially, the limited energy consumption requirements and the low complexity in the sensor hardware necessitate energy efficient error control and prevent high complexity codes to be deployed. Recently, there has been some work that considers the energy consumption analysis of error control techniques in WSNs. One of the goals of the wireless sensor networks is to enable reliable data collection to meet the goals of the applications. Providing reliability is an important issue to address because majority of the sensor networks are remotely operated with very little human intervention once deployed and the maintenance/repair is also infeasible at times. Additionally, the sensor network is inherently exposed to several sources of unreliability such as errors from hardware noise, communication errors, errors in sensors, etc., necessitating the need for reliability mechanisms. One of the important factors to be considered in providing reliability in large sensor networked systems is the overall deployment cost. The deployment cost can be reduced by using low-cost sensor nodes however that leads to constrained computational resources available on the sensor nodes. Another factor that affects the deployment of sensor networks is the lifetime of operation is primarily governed by the limited energy resources available. Hence, reliable sensor data collection should be provided using low-cost sensor nodes while consuming very low energy to enable proliferation of large-scale sensor networks. It has been observed that low-cost reliable sensor data collection can be provided by exploiting the properties of the process being sensed. In [4] introduced a technique which uses the temporal correlation of the data to correct transient errors in the received data by using data prediction model and a-posteriori information about future data. The suggested correction technique, however, assumes a perfect knowledge of the data properties and uses a pre characterized data model to assist the correction process. However, building a perfect model of data offline is practically infeasible at times because of the following reasons. In a real sensor network, the data properties are context dependent. For example, temperature variation in a sensor being deployed outside in the field is different than one deployed inside an apartment. Moreover, the data properties vary over the lifetime of the sensor application necessitating run time changes in the data model.

In [5], a cross-layer analysis of error control schemes is presented. More specifically the effects of multi-hop routing and the broadcast nature of the wireless communication are investigated to derive the equations governing the energy consumption, latency and packet error rate (PER) performance of error control schemes. As a result, a cross layer analysis framework which considers routing medium access control and physical layers is devised. It considered channel-aware geographical routing and contention-based MAC protocols. This analysis enables a comprehensive comparison of forward error correction (FEC) automatic repeat request (ARQ) as well as hybrid ARQ schemes in WSNs. Forward error correction (FEC) coding improves the error resiliency by sending redundant bits through the wireless channel. It is shown that this improvement can be exploited by transmit power control or hop length extension through channel-aware cross-layer geographical routing protocols in WSNs.

Recently, researchers in [6] proposed a simple lossless data compression algorithm which is suitable for available commercial wireless sensor nodes. The algorithm utilizes Huffman variable length code as a dictionary and computes difference data based on each new acquired data and previous data for data encoding. The compressed data is a result of concatenation between an appropriated dictionary which is a Huffman code and a difference data which is a portion of low-order bits from a 2’s complement representation. Thus, each compressed data have variable length or variable block size. Since the output compressed data are dependent with each other, errors in communication channel may cause error in either dictionary or difference data parts. This can occur more often in the harsh environment of radio channel of WSN. If there is an error in one of the data, the error might propagate through the succeeding data in the compressed sequence. To prevent such problem and reduce the probability of error, an error detection method is needed to initiate an error correction mechanism such as retransmission of data. Obviously, to protect simple data compression we also need a simple and efficient error detection technique for WSNs.

Similarly, errors in communication channels can be addressed by general error correction techniques used in data communication networks, such as various types of Forward Error Correction (FEC), Reed-Solomon, Turbo codes, along with retransmission techniques. However, unless it is accompanied by appropriate source coding, use of channel coding may lead to a significant overhead in terms of bits being transmitted, hence increases the energy consumption. The use of source coding schemes such as [7] is an alternate option to decrease the overhead cost by reducing the traffic volume generated from the node. However, we believe that the use of compression techniques will require higher computational resources at the sensor node, and will thus increase the cost of the nodes.

## III. The Some Problems In WSN

### *A. Energy efficiency*

Every sensor node has very limited computing and communication capability, especially very limited energy resource. Sensor nodes are normally powered by batteries and can only last for a short period of time operating at high transmitting level. Hence, the energy efficient design is required for prolonging network lifetime. The lifetime of sensor nodes increases in proportioned to limited battery capacity in wireless sensor networks. Conserving the energy of nodes for extending network lifetime is very important, because once deployed node in wireless sensor networks is almost impossible to be recharged battery [8], [9]. Therefore, all nodes must reduce energy consumption to maximize network lifetime. The dominant energy consumption in the wireless sensor networks occurs in the radio transceiver. The energy consumption of the other components in the sensor node is very small. For this reason, many researches advanced to reduce the wireless transmission.

### *B. Fault-tolerance*

The integrity of data has tremendous effects on the performance of any data acquisition system. Noise and other disturbances can often degrade the information or data acquired from these systems. Devising a fault-tolerant mechanism in wireless sensor networks is very important due to the construction and deployment characteristics of these low powered sensing devices. Moreover, due to the low computation and communication capabilities of the sensor nodes, the fault-tolerant mechanism should have very low computation overhead sensor nodes are very vulnerable to failures. They may lose functionalities at any time because of energy depletion by harsh environment factors or malicious attack from enemies. So it is important I/O consider survivability in sensor network.

## IV. The Residue Number Systems (RNS)

We begin with a short summary of the RNS system, and introduce our terminology:

In the 1950s, RNS were rediscovered by computer scientists, who sought to put them to use in the implementation of fast arithmetic and fault-tolerant computing. Three properties of RNS make them well suited for these. The first is absence of carry-propagation in addition and multiplication, carry-propagation being the most significant speed-limiting factor in these operations. The second is that because the residue representations carry no weight-information, an error in any digit-position in a given representation does not affect other digit-positions. And the third is that there is no significance-ordering of digits in an RNS representation, which means that faulty digit-positions may be discarded with no effect other than a reduction in dynamic range. The new interest in RNS was not long-lived, for three main reasons:

One, a complete arithmetic unit should be capable of at least addition, multiplication, division, square-root, and comparisons, but implementing the last three in RNS is not easy; two, computer technology became more reliable; and three, converting from RNS notation to conventional notation, for “human consumption”, is difficult. Nevertheless, in recent years there has been renewed interest in RNS. There are several reasons for this new interest, including the following. A great deal of computing now takes place in embedded processors, such as those found in mobile devices and for these high speed and low-power consumption are critical; the absence of carry-propagation facilitates the realization of high-speed, low-power arithmetic. Also, computer chips are now getting to be so dense that full testing will no longer be possible; so fault-tolerance and the general area of computational integrity have again become more important. Lastly, there has been progress in the implementation of the difficult arithmetic operations. True, that progress has not been of an order that would justify a deluge of letters home; but progress is progress, and the proper attitude should be gratitude for whatever we can get. In any case, RNS is extremely good for many applications such as digital signal processing, communications engineering, computer security (cryptography), image processing, speech processing, and transforms in which the critical arithmetic operations are addition and multiplication. The residue number system (RNS) [10] is an integer system capable of supporting parallel, carry-free, high-speed arithmetic. The system also offers some useful properties for error detection, error correction and fault tolerance in digital systems. Important areas of application of the RNS include:

Digital signal processing (DSP) intensive computations such as digital filtering, convolutions, correlations discrete Fourier transform (DFT) and fast Fourier transform (FFT) computations [11], [12], [13], [14] direct digital frequency synthesis [15]. A residue number system is defined by a set of relative prime numbers, $\{m_1, m_2, \ldots, m_r\}$ called the "moduli". In such a system, an integer X is represented by an ordered set of r residues, $\{X_1, X_2, \ldots, X_r\}$ , where xi = (X mod mi). If only positive numbers are permitted, then any integer in the range [0, M) where, $M= m_1 \cdot m_2 \cdot \ldots \cdot m_r$, can be uniquely represented. If negative numbers are also allowed, then it is usual to let the dynamic range be [-M/2, M/2). The choice of moduli is crucial to the representational efficiency and to the complexity and delay of the arithmetic unit.

The moduli set: $\{2^n-1, 2^n, 2^n+1\}$ is used throughout this paper. This is a popular moduli-set, as the restriction to powers of two (±1) in the set makes it relatively easy to implement efficient arithmetic units and to produce generalized designs that are parameterized by operand word length. Fig. 1, shown general structure of an RNS processor:

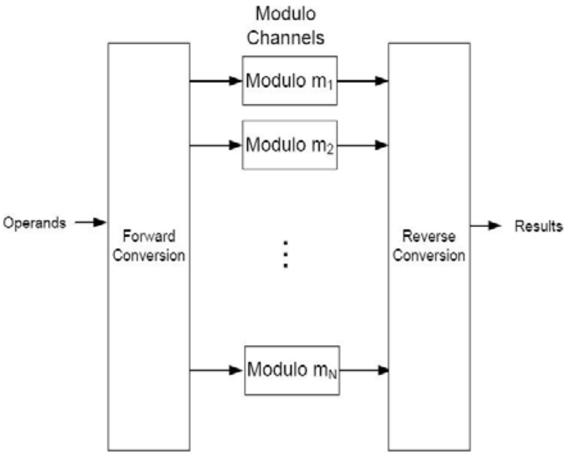

Figure 1. The general structure of an RNS processor.

## V. Error Detection & Correction In Wireless Sensor Networks By Residue number systems

Residue number systems are also useful in error detection and correction. This is apparent, given the independence of digits in a residue number representation: an error in one digit does not corrupt any other digits. In general, the use of redundant moduli, i.e. extra moduli that play no role in determining the dynamic range, facilitates both error detection and correction. But even without redundant moduli, fault-tolerance is possible, since computation can still continue after the isolation of faulty digit-positions, provided that a smaller dynamic range is acceptable. RNS have techniques to error detection and correction that this ability can be used in wireless sensor network to decrease renewed data sending via occur error in data packets. It is also of very low complexity, thus good for energy constrained sensors. Fig. 2, shows the structure of an circuit error detection.

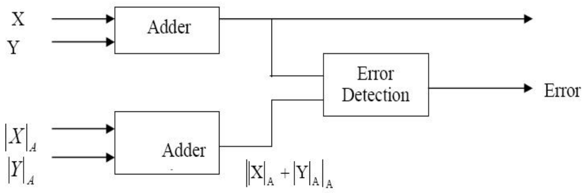

Figure 2. Show Circuit Error Detection.

An RRNS is defined as a chosen RNS with additional redundant moduli. Each redundant modulus is generally greater than any of the moduli of the chosen moduli set. Assuming the standard RNS consists of the moduli set of $\{P_1, P_2, \ldots, P_m\}$, the corresponding RRNS consists of a moduli set of $\{P_1, P_2, \ldots, P_m, \ldots, P_{m+2r}\}$ (r ≥ 1). Assuming MAX $(P_1, P_2, \ldots, P_m)$ is a function to get the largest modulus in this set, we get $P_{m+j} > \text{MAX}(P_1, P_2, \ldots, P_m)$, for j=1,2,…,2r. A typical RRNS system consists of (m+2r) B/R converters, (m+2r) subsystems and an R/B converter. The RRNS has capability of error detection and correction; by using 2r (r ≥ 1) redundant moduli r errors can be detected and corrected. We need the following definition to describe the error detection and correction capability of the RRNS. Definition 1: the $U_i$ projection is denoted by the representation of an arbitrary number U in the RRNS with the residue digit $u_i$ deleted. Thus, based on the RRNS $\{P_1, P_2, \ldots, P_m, \ldots, P_{m+2r}\}$, we have $U_i = (U_1, U_2, \ldots, U_{i-1}, U_{i+2}, \ldots, U_{m+2r})$ where i=1,2,...,m,..., m+2r. If it is found that one projection Ui is within the correct dynamic range, and none of the other projections $U_j$ with j≠i are within the correct dynamic range, then, the residue Ui is determined to be erroneous [16]. The RRNS with the (m+2r) moduli set can detect r erroneous residues associated with r moduli and can use the remaining (m+r) moduli to compute the correct result U. This provides a technique for checking and correcting the errors. In other words, the RRNS is a method of detecting and correcting errors for some subsystems inside the RNS by using the extra moduli. Generally, the function of the error detection and correction is performed at the R/B converter.

The structure of a RRNS QC encoder/decoder [17] is shown in Fig. 3, it consists of (m+2r) B/R converters, (m+2r) pairs of modulo QC encoder/decoders, and an R/B converter. Like the standard RNS, the RRNS also offers carry-free, high-speed and concurrent arithmetic operations, which are useful from the point of view of implementation. Further, this RRNS QC encoder/decoder adds error-correcting capability inside the transmission channel. Inside the channel, several checking circuits are added to perform the function of error detection and correction. Another importance aspect of the RRNS QC encoder/decoder is that it can achieve more security than the binary QC encoder/decoder. In the binary QC encoder/decoder, the secret keys are the delay values $D_i$'s and the coefficients $a_i$'s (i=1, 2, .., P). In the RRNS QC encoder/decoder, besides $a_i$'s and Di's, the moduli set $\{P_1, P_2, \ldots, P_m, \ldots, P_{m+2r}\}$ is also part of the secret keys.The unauthorized listener needs more information to decrypt the system. Thus, the RRNS QC encoder/decoder increases the degree of security.

## VI. RRNS QC Encoder/Decoder

In this section, we explain an efficient structure for the RRNS QC encoder/decoder as shown in "Fig. 3". It consists of (m+2r) B/R converters, (m+2r) binary sub encoders, (m+2r) binary sub decoders and an R/B converter with error-correcting capability [18].

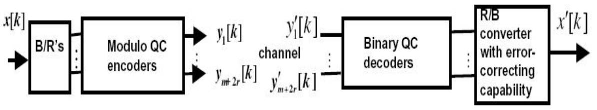

Figure 3. The Encoder/Decoder Diagram.

Based on the redundant moduli$\{P_1,P_2,\ldots,P_m, \ldots,P_{m+2r}\}$, the B/R converters convert the binary message signal X[k] into its residue format, ($X_1$[k], $X_2$[k], … ,$X_m$[k],…,$X_{m+2r}$[k]), where $X_i$[k]= ∣X[k]∣and Pi, i=1, ..., m, ..., m+2r. Then, for each $X_i$[k], one binary encoder is used to generate the corresponding encoded output $Y_i$[k]. The (m+2r) encoded signals $Y_i$[k] are transmitted through the transmission channel. At the receiver, the binary decoders, which are the inverse of the corresponding encoders, recover each residue message $X'_i$[k]. Finally, the R/B converter with error-correcting capability will detect and correct the r errors and generate the final output message signal X'[k]. The proposed architecture has the following features:

- Binary encoders and decoders are used. Thus, a number of modulo operations required by the design in [18], [19] are removed.
- The proposed architecture produces a security in the transmission (QC properties), and has an error-correcting capability at the back end of the receiver. Thus, the message received from the final stage is error-corrected.
- If the word length of the input message is *L* bits, the word length of each binary encoder or decoder is approximately log (*L*) bits. Thus, the speed of the encoding and decoding can be very high.

In the proposed structure, the word length of each Sub channel is approximately log (*L*)-bits. Thus, each B/R converter consists of a log (*L*)-bit modulo adder and each encoder or decoder is an IIR or FIR filter with a simple log (*L*)-bit truncation. Therefore is very easy design of B/R converters and binary encoders/decoders. However, the choice of the moduli set needs to be considered. Furthermore, the design of the R/B converter with error-correcting capability is rather complex and is the most crucial part of the system. In this section, we briery summarize some properties of the associated error detection and correction procedures in the context of the RRNS. Error detection/correction decoding of RRNS (U;V) codes has been discussed in depth in [16]. Let us invoke two simple examples, in order to gain insight into the error-detection and error-correction mechanism of the RRNS.

### A. Example 1

Let us consider the moduli 3, 4, 5, 7, where 3, 4 and 5 are the information moduli and 7 is the redundant modulus. The information dynamic range is [0, M=3×4×5) = [0, 60). Upon considering an integer decimal message of X=21, the corresponding residue values are X = (0, 1, 1, 0). If there is an error in the RNS representation due to transmission or processing, for example $r_3$ is changed from 1 to 3, and then the received RNS representation becomes (0, 1, 3, 0). Upon following the general approach of the CRT and using the first three residue digits and their moduli, we obtain:

$M_1 = 4\times5 = 20$ , $T_1 = 2$
$M_2 = 3\times5 = 15$ , $T_2 = 3$
$M_3 = 3\times4 = 12$ , $T_3 = 3$
$X = [0 \times 2 \times 20 + 1 \times 3 \times 15 + 3 \times 3 \times 12] \bmod 60 = 33.$

However, where X = 33 (mod 7) = 5 ≠ $r_4$ = 0, and we can conclude that there were errors in the RNS representation. Therefore, upon designing the RNS using one redundant modulus, the residue digit error of $r_3$ can be detected.

### B. Example 2

Let us now invoke an additional redundant modulus, namely 11 in the above example, which results in a total of two redundant moduli, namely 7 and 11 in the RRNS.

Let us also consider the integer message X=21, now having corresponding residue digits of X = (0, 1, 1, 0, 10) and that $r_3$ is in error and it was changed from 1 to 3, i.e. the received RNS representation becomes (0, 1, 3, 0, 10). According to the CRT's approach, the integer X in the range [0, 60) can be recovered by invoking any three moduli and their corresponding residue digits if no errors occurred in the received RNS representation. Let us now consider all possible cases and attempt to recover the integer X represented by (0, 1, 3, 0, 10), upon retaining all possible combinations of three out of five residue digits, which results in:

$(r_1; r_2; r_3) = (0; 1; 3) \leftrightarrow X_{123} = 33 \pmod{60};$
$(r_1; r_2; r_4) = (0; 1; 0) \leftrightarrow X_{124} = 21 \pmod{84};$
$(r_1; r_2; r_5) = (0; 1; 10) \leftrightarrow X_{125} = 21 \pmod{132};$
$(r_1; r_3; r_4) = (0; 3; 0) \leftrightarrow X_{134} = 63 \pmod{105};$
$(r_1; r_3; r_5) = (0; 3; 10) \leftrightarrow X_{135} = 153 \pmod{165};$
$(r_1; r_4; r_5) = (0; 0; 10) \leftrightarrow X_{145} = 21 \pmod{231};$
$(r_2; r_3; r_4) = (1; 3; 0) \leftrightarrow X_{234} = 133 \pmod{140};$
$(r_2; r_3; r_5) = (1; 3; 10) \leftrightarrow X_{235} = 153 \pmod{220};$
$(r_2; r_4; r_5) = (1; 0; 10) \leftrightarrow X_{245} = 21 \pmod{308};$
$(r_3; r_4; r_5) = (3; 0; 10) \leftrightarrow X_{345} = 98 \pmod{385};$

Where $X_{ijk}$ represents the recovered result by using moduli mi, mj and mk as well as their corresponding residue digits ri, rj and rk. From these results we observe that $X_{134}$, $X_{135}$, $X_{234}$, $X_{235}$ and $X_{345}$ are all illegitimate numbers, since their values are out of the legitimate range[0, 60). In the remaining five cases, except for $X_{123}$, all the results are the same and equal to 21. Moreover, all these results were recovered from three moduli without including $m_3$, i.e. from $X_{124}$; $X_{125}$; $X_{145}$ and $X_{245}$, which are equal to 21. Hence, we might conclude that the correct result is 21 and that there was an error in $r_3$, which can be corrected by computing: $r_3 = 21 \pmod 5) = 1$.

In Table 1 shown RRNS code words of some typical decimal integer messages X in the RRNS with moduli $m_1 = 4$; $m_2 = 5$; $m_3 = 7$; $m_4 = 9$; $m_5 = 11$; $m_6 = 13$ and $m_7 = 17$; where $r_i = X \pmod{mi}$ and $M = 4 \times 5 \times 7 = 140$.

TABLE I. SHOWN RRNS CODE WORDS OF SOME TYPICAL DECIMAL INTEGER MESSAGES

| **Decimal Message X** | **No redundant Residue digits** | | | **Redundant Residue digits** | | | |
|---|---|---|---|---|---|---|---|
| | $r_1$ | $r_2$ | $r_3$ | $r_4$ | $r_5$ | $r_6$ | $r_7$ |
| $X_0 = 0$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $X_1 = 1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $X_2 = 2$ | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| $X_3 = 5$ | 1 | 0 | 5 | 5 | 5 | 5 | 5 |
| $X_4 = 10$ | 2 | 0 | 3 | 1 | 10 | 10 | 10 |
| $X_5 = 20$ | 0 | 0 | 6 | 2 | 9 | 7 | 3 |
| $X_6 = 50$ | 2 | 0 | 1 | 5 | 6 | 11 | 16 |
| $X_7 = 100$ | 0 | 0 | 2 | 1 | 1 | 9 | 15 |

In Table 2 shown RRNS code words of some typical binary messages X in the RRNS with moduli $m_1$=4; $m_2$=5; $m_3$=7; $m_4$=9; $m_5$=11; $m_6$=13 and $m_7$=17; where $r_i = X \pmod{mi}$ and $M = 4 \times 5 \times 7 = 140$.

TABLE II. SHOWN RRNS CODE WORDS OF SOME TYPICAL BINARY INTEGER MESSAGES

| **Binary Message X** | **No redundant Residue digits** | | | **Redundant Residue digits** | | | |
|---|---|---|---|---|---|---|---|
| | $r_1$ | $r_2$ | $r_3$ | $r_4$ | $r_5$ | $r_6$ | $r_7$ |
| $X_0 = 0000000$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $X_1 = 0000001$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $X_2 = 0000010$ | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| $X_3 = 0000100$ | 0 | 4 | 4 | 4 | 4 | 4 | 4 |
| $X_4 = 0001000$ | 0 | 3 | 1 | 8 | 8 | 8 | 8 |
| $X_5 = 0010000$ | 0 | 1 | 2 | 7 | 5 | 3 | 16 |
| $X_6 = 0100000$ | 0 | 2 | 3 | 5 | 10 | 6 | 15 |
| $X_7 = 1000000$ | 0 | 4 | 1 | 1 | 9 | 12 | 13 |

## VII. Improving Performance In WSN By Residue Number Systems

By usage of Residue Number Systems (RNS), we increase performance of wireless sensor networks. This is thus that we do first for all nodes and states which define Module, then whenever data got of methods Built-In Test (BIT) [20] would like transmission to other nodes or states beneficial of method Residue Number Systems. RNS have some capabilities that improve QoS in WSN. Moreover, RNS have techniques to error detection and correction that this ability can be used in wireless sensor network to decrease renewed sending data via occur error in data packets. It is also of very low complexity, thus good for energy constrained sensors. It has a very high degree of flexibility and scalability because no knowledge about the current network information is needed and new nodes can be added without a need to change the algorithm for existing nodes. Localization is then possible even in environments that are out of reach of GPS signal.

### *A. Reduce Traffic and Data Transmission in Network*

In most traditional methods of error detection and correction, to detect errors occurring in the data, in addition sending original data large volume of additional bits for error detection or correction of data should be sent to the destination. Additional data will cause some problems such as: increase data transmission rates and network traffic in wireless sensor networks. By using of Residue Number Systems we can reduce amount of data transmission in Wireless Sensor Network, whenever a sensor wants send a data, instead of whole transmission data, it can only send partial of data that includes residue and toward the primary data has less bit. Therefore whatever amount of transmission data becomes less therewith decreases traffic in network.

### *B. Energy-Efficient by Residue Number Systems*

The lifetime of sensor nodes increases mainly in proportion to limited battery capacity in wireless sensor networks. All sensor nodes must reduce energy consumption for maximizing network lifetime [21], [22]. The part of the most energy consumption in the wireless sensor networks is wireless transmission part. Many researches that minimize energy consumption of wireless transmission part progress to maximize lifetime of sensors. As was described in the previous section, RNS reduces the bit rate of data; this will reduce the energy consumption of sensor nodes. Also, considering that RNS for error detection are not requirement high computing power. Hence, by reducing the processing power lower computing energy is consumed for error detection in network. In this section, we demonstrate that energy efficiency can be improved by Residue Number Systems. Use of RNS reduce calculation and also reduce rate of data transmission, as for the two topics, decrease amount of power consumption in wireless sensor networks.

## VIII. Conclution

In this paper, first, we consider some of problems in wireless sensor networks such as: errors in transmitted data and consumed energy of nodes. Then were studied some of existing capabilities in the RNS. These capabilities can be used to improve the existing problems in wireless sensor networks. The advantages described in this paper are, reduce traffic rate in wireless sensor network with decrease amount of data transmission and this reduces the power consumption of sensor nodes. Additionally, RNS has the ability to detect and correct errors in data transmitted with the using minimum redundancy. Also, by reducing the processing power lower computing energy is consumed for error detection in network. In this paper, we use of these advantages to error detection and correction in wireless sensor networks.

## References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 38, Issue 4, 2002.

[2] Elnahrawy, E., Nath, B., "Cleaning and querying noisy sensors", Workshop on wireless sensor networks and applications, 2003, pp. 78– 87.

[3] Hereford, J, "Fault-Tolerant Sensor Systems Using Evolvable Hardware", IEEE Transactions on Instrumentation and Measurement".

[4] S. Mukhopadhyay, D. Panigrahi, and S. Dey, “Data aware, low cost error correction for wireless sensor networks,” in Proc. IEEE Wireless Communications and Networking Conference (WCNC), pp. 2492–7, Mar. 2004.

[5] M. C. Vuran and I. F. Akyildiz, “Error Control in Wireless Sensor Networks: A Cross Layer Analysis,” in IEEE/ACM Transactions On Networking, Vol. 17, No. 4, August 2009.

[6] Neal R. Wagner and Paul S. Putter, "Error detecting decimal digits. " Communications of the ACM, Vol. 32, Issue 1, pp. 106 110, Jan. 1989.

[7] S. S. Pradhan and K. Ramachandran, “Distributed source coding: Symmetric rates and applications to sensor networks,” in Proc. IEEE Data Compression Conference (DCC), Mar. 2000.

[8] S. R. Madden et al., “TAG: a Tiny AGgregation Service for Ad-Hoc Sensor Networks,” in Proceedings of OSDI, Dec. 2002.

[9] R. Min et al., “Energy-centric enabling technologies for wireless sensor networks,” in Proceedings of IEEE Wireless Communications, Aug. 2002, pp. 28-39.

[10] W. K. Jenkins and B. J. Leon, “The use of residue number systems in the design of finite impulse response digital filters,” IEEE Trans. Circuits Syst., vol. CAS-24, no. 4, pp. 191–201, Apr. 1977.

[11] M. A. Soderstrand, “A high-speed low-cost recursive digital filter using residue number arithmetic,” Proc. IEEE, vol. 65, pp. 1065–1067, Jul.1977.

[12] H. K. Nagpal, G. A. Jullien, and W. C. Miller, “Processor architectures for two-dimensional convolvers using a single multiplexed computational element with finite field arithmetic,” IEEE Trans. Comp., vol.C-32, no. 11, pp. 989–1000, Nov. 1983.

[13] F. J. Taylor, G. Papadourakis, A. Skavantzos, and A. Stouraitis, “A radix-4 FFT using complex RNS arithmetic,” IEEE Trans. Comp., vol. C-34, no. 6, pp. 573–576, Jun. 1985.

[14] W. A. Chren, “RNS-based enhancements for direct digital frequency Synthesis,” IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.I, Anlaog Digit. Signal Process., Anlaog Digit. Signal Process., vol. 42, no. 8, pp.516–524, Aug. 1995.

[15] M. A. Soderstrand, W. K. Jenkins, G. A. Jullien, and F. J. Taylor, Eds., Residue Number System Arithmetic: Modern Applications in Digital Signal Processing. New York: IEEE Press, 1986.

[16] Heinzelman,W.,Chandrakasan,A., and Balakrishnan, H., "Energy Efficient Communication Protocol for Wireless Micro sensor Networks", Proc. of the 33rd Hawaii International Conference on System Sciences (HICSS '00), 2000, pp. 3005-3014.

[17] Bandyopadhyay, S., Colye, E., "An energy efficient hierarchical clustering algorithm for wireless sensor networks", IEEE Inforcom, 2003, pp. 1713-1723.

[18] Wei Wang, Xiaolin Zhang, Chenyang Yang, M. N. S. Swamy and M. O. Ahmad "RRNS QUASI-CHAOTIC CODING AND ITS FPGA IMPLEMENTATION " 0-7695-2294-7/05 $20.00 © 2005 IEEE.

[19] Lie-Liang Yang and Lajos Hanzo " Redundant Residue Number System Based Error Correction" 0-7803-7005-8/01/$10.00 (c) 2001 IEEE.

[20] Asad M. Madni, Prasanna Sridhar, Mo Jamshidi,"Fault-Tolerant Data Acquisition in Sensor Networks" 1-4244-1160-2/07/ 2007 IEEE.

[21] Sangsik Kim, Sangha Kim "A Energy Conservation Scheme to Maintain Data Aggregation Tree in Sensor Networks" Asia-Pacific Conference on Communications, Perth, Western Australia, 3-5 October 2005.

[22] Yongxuan Lai1,2, Hong Chen1,2 "Energy-Efficient Fault-Tolerant Mechanism for Clustered Wireless Sensor Networks" This work is supported by the National Natural Science Foundation of China under Grant No.60673138. 1-4244-1251-X/07/$25.00 ©2007 IEEE.

**Mohsen Roshanzadeh** received the B.Sc. degree in computer hardware engineering from Islamic Azad University, Dezful, Iran, in 2007. He received the M.S. degree in Computer Systems Architecture engineering from the Islamic Azad University, Tabriz Branch, Iran, in January 2011. From February 2009 he has worked as a Lecturer in the Islamic Azad University. His research focuses on wireless sensor network, especially on the routing algorithms in wireless sensor networks.

**Sasan Saqaeeyan** received the B.Sc. degree in computer software engineering in 2008 from the University of Isfahan and M.S. degree in computer software engineering in January 2010, from the Islamic Azad University Khoozestan Science and Research Branch, Iran. From January 2011 he has worked in the Islamic Azad University Abadan Branch as a Faculty Member.