Residual Channel Coding in Low-Power WSNs Using Minimum Hamming Distance Decoder

Bafrin Zarei, Vallipuram Muthukkumarasamy, and Xin-Wen Wu

Abstract—Forward Error Correction is an essential requirement for wireless communication systems with high bit error rates. Redundant Residue Number System codes are normally superior in parallel communication environments, such as sensor networks due to their weightless structure. Underlying error correction capability of redundant residue representation has led to the development of a new set of coding schemes. In this research, a novel error control technique, based on the residue number system is proposed and implemented using MATLAB. With the design of a new minimum-Hamming distance decoder, the proposed system achieved a more efficient error correction ability compared to the Reed Solomon code, particularly in lower signal to noise ratios.

Keywords—bit error rate; signal to noise ratio; additive white Gaussian noise; channel coding; wireless sensor networks

I. Introduction

A wide range of application areas, including health, environment, industry, and military, use Wireless Sensor Networks (WSN) as a low-cost, easily deployable, self-organized network [1]. Energy constraint is one of the most crucial challenges in WSN due to limited resources in each sensor. On the other hand, random noise, interference, channel fading or physical defects may cause errors during data transmission in the wireless medium. Two basic methods to recover erroneous data are Automatic Repeat reQuest (ARQ) and Forward Error Correction (FEC). In this study, an efficient FEC scheme for WSN is developed to avoid retransmissions. The scheme is simulated using MATLAB and the performance of the proposed method is analysed. This new method named Residual Channel Coding with Minimum Distance Decoding (RCCMDD), efficiently exploits the advantages in the Residue Number Systems (RNS). Applying the residual error control scheme with the proposed decoder not only saves retransmission energy but also extends link functionality and enables the network to handle burst errors.

The main aim is to decrease redundancy in error correction codes without reducing its throughput. The next section briefly describes the research relating to FEC methods in WSN. The residue number system components and error control in this system are defined in Sections III. The proposed RCCMDD is presented in Section IV. Section V illustrates the simulation results and compares the error correction ability with a number of FEC codes and analyses the energy consumption of the proposed method. Section VI concludes the paper.

II. Forward Error Correction in WSNs

The link failure corruption can be reduced by applying an appropriate error control scheme. There is a vital demand for an energy efficient control scheme in WSN due to stringent energy constraints. The effects of Hamming codes in WSN were studied in [2, 3] to control errors and maximize network life time. Where codes are designed to correct random channel errors, wireless channels are often subjected to burst errors [4]. The limitation of the Hamming code is the number of bits which can be restored.

The efficiency of BCH and Reed-Solomon (RS) codes has been previously demonstrated [5, 6]. They are very powerful codes, provided that the block length is not excessively long. These codes can be adapted to the error nature of the channel, where RS codes are particularly appropriate to handle burst errors and BCH codes are applicable to random single errors.

LDPC codes in [7, 8] have been investigated for WSN. Although LDPC codes are strong block codes, they are not appropriate in WSN due to their inflexibility and the need for high memory usage and a high number of operations during the encoding and decoding process. Another drawback of LDPC codes is their efficiency only with very long length block codes, which are not suitable for applications in the WSNs, where only short data blocks are transmitted. Several non-block codes such as Turbo codes were studied in [9, 10]. In these codes, the average energy consumption per useful bit grows exponentially with the constraint length of the code. In addition to very complex implementation of decoders, the interleaver, which consumes a large part of silicon area in their architecture, is a key component of Turbo codes. Increased latency is another noticeable disadvantage of interleaving. Chase proposed an algorithm for block codes, which utilizes the channel measurement information and algebraic properties of the code [11].

FEC is not generally applicable in WSN, because of computational and redundant data transmission power overhead that is introduced by error control techniques. This provides motivation for using residual error control energy efficient errors.
In [13], the energy efficiency of WSN was increased using a Redundant Residue Number System (RNS) packet-forwarding solution. However, RRNS as a broadcast authentication scheme is applicable [14]. The efficiency of the RRNS code for fault-tolerant hybrid memories was studied and compared to RS codes [15]. Both RRNS and RS codes are block codes which reach minimum-maximum distance and perform error control in the frame level. In the Improved RRNS (IRRNS), an extra error detection mechanism (parity check), which is able to detect an odd number of errors in each remainder, is added to increase the error correction capability of RRNS [12]. In RRNS, each remainder is distinct from every other remainder. In this paper, this exclusivity of received remainders has been used in minimum Hamming distance RCCMDD decoder to reach almost the same error correction capability without adding extra redundancy. In other words, RCCMDD has two distinct contributions compared to IRRNS. Firstly, it is applicable to every type of error, and secondly the error correction capability of RCCMDD is doubled without adding any error detection code. In order to illustrate its efficiency, it is compared with RS codes.

### III. Residue Number System

Residue Number System (RNS) is an unconventional numerical system, which is defined by a set of $k$ positive integers $(m_1, m_2, ..., m_k)$ referred to as moduli [16-18]. Any integer $X$ in the dynamic operating range $0 \leq X < M_{op}$ can be uniquely represented by the residue sequence $(x_1, x_2, ..., x_k)$, where $x_i = [X]_{m_i}, i = 1, 2, ..., k$. A pair of any two moduli such as $m_a$ and $m_b$ with $a \neq b$, must be relatively prime positive integers such that their greatest common divisor, $gcd (a, b) = 1$. Then $M_{op}$ is obtained by $M_{op} = \prod_{i=1}^{k} m_i$.

According to the Chinese Remainder Theorem (CRT), for any given $k$-tuple $(x_1, x_2, ..., x_k)$, where $0 \leq x_i < m_i$, one and only one integer $X$ exists such that:

$$X = \sum_{i=1}^{k} x_iM_i^{-1}M \pmod{M_{op}}$$

where $0 \leq X < M_{op}$ and $x_i = [X]_{m_i}, i = 1, 2, ..., k$. The integers $M_i = M_{op}/m_i$ and the integers $M_i^{-1}$, which create the multiplicative inverses of $M_i$, are computed by solving $M_i^{-1} M_i = [1]_{m_i}$. In RRNS, $l$-bit values, $X$ will be encoded into $n$-residue digits [16, 18]. These residues are divided into two sets; $k$ number of $x_i$ non-redundant residues and $r = (n-k)$ number of $x_j$ redundant residues, where $1 \leq i \leq k$ and $k+1 \leq j \leq n$. To prevent decoding of residues to result in more than one output, the succeeding residues must be greater than the preceding modulus, such that $m_1 < m_2 < \ldots < m_n$. 

![Figure 1: Transmission System Model](image1)

and the product of moduli $M_{op} = \prod_{i=1}^{k} m_i$, is sufficient to represent all numbers in the operating range of input data $[0, 2^l - 1]$ for $l$-bit input data. A RNS $(n,k)$ achieves the maximum – minimum Hamming distance of $d = (n-k + 1)$, where $n$ is the number of total moduli (redundant and non-redundant), and $k$ is the number of non-redundant moduli.

### IV. Proposed Method

#### A. System Model

The current research considers the transmission of block codes with binary phase-shift keying (BPSK) modulation over additive white Gaussian noise (AWGN) channel. The system block diagram of the proposed RNS based communication system using BPSK signalling known as RCCMDD is shown in Fig. 1.

The sensed binary data $X$ to be transmitted is coded into the residues $c = (x_1, x_2, ..., x_n)$, which are then mapped into $-1, +1$ sequences to produce the channel input signal $s$ using $s = 2 \times c - 1$. The channel output signal $y$ is produced by applying zero-mean AWGN with $0 \text{ dB}$ variance to the input signal $s$. With the use of the resource rich Base Station (BS) playing the decoder role on the demodulated signal $\hat{c} = (\hat{x}_1, \hat{x}_2, ..., \hat{x}_n)$, the estimated data $\hat{X}$ is reconstructed. The current research investigates the encoding complexity, transmission energy consumption and error correction ability of the proposed method.

![Figure 2: RCCMDD Block Diagram](image2)
B. Residual Channel Coding with Minimum Hamming Distance Decoding

The Fig. 2.A illustrates an example RNS block diagram which encodes [12] the sensed binary data X, which is to be transmitted into the residues $c = (x_1, x_2, x_3)$, using moduli set $(m_1, m_2, m_3)$, where $x_i = |X|_{m_i}$ and $1 \leq i \leq 3$. The proposed decoder based on minimum hamming distance is represented in Fig. 2.B. The flow chart in Fig. 3 shows the flow diagram of the proposed RCCMDD decoder on the decoder side. While data is not recoverable using CRT, and error is detected, the proposed RCCMDD $(n,k)$ starts its operation drawing from the $k$-combination of a received remainder set $\tilde{c}$, where $n$ and $k$ are the number of total residues and non-redundant residues, respectively. Therefore, CRT is run $\binom{n}{k}$ times and produces $\binom{k}{n}$ potential output.

In the next step, the Hamming distances between the encoded forms of the potential output and the received signal $\tilde{c} = (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n)$ are calculated and the one which has the minimum distance is selected as the final output of the RCCMDD decoder. The key idea in this work is that the data are recoverable having a $k$ error free remainder. There are $n = r + k$ received remainders at the receiver side. In other words, when the $k$ number of error-free residues is applied for decoding, the original data are obtained. The challenge is that it is not clear which received remainder has errors and which one is error-free. Therefore, the $k$ different combination of the $n$ received remainder set is used in the decoder in the RCCMDD.

After decoding by the RCCMDD, a list of valid code-words is produced. Based on the binary Hamming distance of the encoded valid code-words and received remainders, the minimum distance output is selected. Consequently, the complexity increases with the number of $k$ and $n$, since there are $\binom{n}{k}$ combinations of $k$ that can be drawn from the $n$-member set. This means that there are $\binom{n}{k}$ different candidate inputs for the RCCMDD decoder and maximum $\binom{k}{n}$ different potential outputs for the RCCMDD decoder. The decoded vector, having the minimum distance from the received vector, is not necessarily the correct one, but it is shown in the simulation results that it is more reliable that RS codes for lower SNRs. As it can be seen in Fig. 3, if the message cannot be recovered with the RRNS decoder at the receiver side, the RCCMDD tries to use the maximum $r$ remainder correction ability. This means that after demodulating the received signal, the received remainders go to the RRNS $(n,k)$ decoder. If the output decoded value is not valid, the number of $\binom{n}{k}$ with $k$-

<table>
<thead>
<tr>
<th>Remainders</th>
<th>Moduli Set</th>
<th>Mop</th>
<th>M$_1$</th>
<th>M$_1^{-1}$</th>
<th>CRT Output</th>
<th>Hamming Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\tilde{x}_1=6, \tilde{x}_2=5$</td>
<td>$m_1 = 7, m_2 = 8$</td>
<td>56</td>
<td>$M_1^{-1} = 1, M_1^{-1} = 7$</td>
<td>13</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$\tilde{x}_1=6, \tilde{x}_3=1$</td>
<td>$m_1 = 7, m_2 = 9$</td>
<td>63</td>
<td>$M_1^{-1} = 4, M_1^{-1} = 4$</td>
<td>55</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$\tilde{x}_2=5, \tilde{x}_3=1$</td>
<td>$m_2 = 8, m_3 = 9$</td>
<td>72</td>
<td>$M_2^{-1} = 1, M_2^{-1} = 8$</td>
<td>37</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3 Empowered RRNS Decoder Architecture
v. Experimental Evaluation and Analysis

In this section, the performance of RCCMDD is compared in terms of energy consumption and error correction capability to RS codes, by means of simulations. Moreover, some results are provided comparing the proposed solution with Reed Solomon (RS) codes. The RS code is selected in a way to keep the transmission energy consumption almost the same as the RCCMDD code to study the capability of the codes to correct transmission errors. The sensor nodes are assumed to be static as is usual in most applications [1]. By injecting redundancy into the data to be sent, even in the presence of noise, the received signal can be successfully decoded. In other words, the channel encoder creates a larger number of bits in order to achieve successful transmission.

The redundancy allows the receiver to detect and correct a limited number of errors without retransmitting additional data. The redundancy overhead imposed by FEC costs channel bandwidth and transmission power. Therefore, decreasing redundancy is one of the main goals of the code designers.

The code rate, $R$, is a quantitative measure for redundancy as the ratio of the message length $k$ to the codeword length $n$. The maximum value for coding rate is 1 when there is no redundancy in an uncoded message. Coding performance is the opposing factor to coding rate.

In Fig. 4, the error correction capability of RS (15,13) RS (15,11), RCCMDD (4,3), and RCCMDD (5,3) is illustrated. We use a new representation of RCCMDD($m_1, m_2, ..., m_k, m_{k+1}, m_{k+2}, ..., m_n$) to add more detail about the moduli set on the graphs, where $m_k, m_{k+1}, m_{k+2}, ..., m_n$ are redundant moduli. The code rates of these codes are 0.86, 0.73, 0.75, and 0.6 respectively. A code rate closer to 1 is desirable which means that the redundant data to be transmitted is lower. For signal to noise ratios lower than about 6 dB, RCCMDD(4,3) outperform other codes, which have a considerably high code rate.

The RCCMDD(4,3) coding gain is calculated a Frame Error Rate (FER) 0.7 and it is more than 1 dB compared to the other codes. It is worth mentioning that in conventional RRNS, in order to have one modulus error correction capability, at least two redundant moduli are needed. In other word RRNS(4,3) is unable to correct errors. By adding more redundancy, the error correction capability of FEC is generally strengthened. RCCMDD does not follow this pattern (see Fig. 5). The higher the redundant moduli, the more adverse effects there are on RCCMDD performance in terms of FER, as well as coding complexity and transmission power overhead. Because of the greater number of redundant moduli, there is higher chance to receive remainders that are more erroneous.

The functionality of the RCCMDD decoder is based on the number of redundant remainders, which make it more complex and may lead to ambiguous output. This means that the RCCMDD decoder may find an erroneous output, which has minimum, Hamming distance, whereas the correct data set is still in the potential output list.
energy overhead as compared to the RS codes. To achieve optimal energy consumption, the parallel processing property of the RNS can be further exploited this will be explored in future work.

References