Low Cost Error Recovery in Delay-Intolerant Wireless Sensor Networks

Rachit Agarwal†, Emanuel M. Popovici‡, Massimiliano Sala‡ and Brendan O’Flynn‡
†Department of Microelectronics Engineering, University College Cork, Cork, Ireland
‡Boole Centre for Research in Informatics, University College Cork, Cork, Ireland
‡Microelectronics Application Integration Group, Tyndall National Institute, Cork, Ireland
Email: rachit.agarwal@ue.ucc.ie, e.popovici@ucc.ie, msala@bcri.ucc.ie, brendan.oflynn@tyndall.ie

Abstract—Transmission efficiency of Wireless Sensor Networks (WSN) is lower than that of conventional networks due to frequent propagation errors. In light of specific features and diverse applications of WSN, common assumptions from communication systems may not hold true and efficient application-specific protocols can be formulated. In this paper, we demonstrate this based on an interesting observation related to shortened Reed-Solomon (RS) codes for packet reliability in WSN. We show that multiple instances (γ) of RS codes defined on a smaller alphabet combined with interleaving result in smaller resource usage while the performance exceeds the benefits of a shortened RS code defined over a larger alphabet. In particular, the proposed scheme can have an error correction capability of up to γ times larger that for the conventional RS scheme without changing the rate of the code with much lower power, timing and memory requirements. Implementation results on 25mm motes developed by Tyndall National Institute show that such a scheme is 43% more power efficient compared to RS scheme with same code rate. Besides, such an approach results in 44% faster computations and 53% reduction in memory required.

I. INTRODUCTION

The transmission efficiency of Wireless Sensor Networks (WSN) is lower than that of conventional wired and wireless networks due to high Bit Error Rate (BER). Their average BER is known to be in the range from $10^{-6}$ to $10^{-3}$, implying that many packets would be corrupted and thus dropped over wireless channels without some appropriate error prevention or recovery mechanisms. Some applications in WSN, like medical, security, monitoring and surveillance require high reliability in data transfer. Further, recovery protocols like Automatic Repeat Request (ARQ) can not be employed in Delay-Intolerant Wireless Multimedia Sensor Networks [1], high error introducing channels such as underwater sensor networks [2] due to associated retransmission costs, both in terms of energy consumption and delay [3]. In such scenarios, Error Control Coding (ECC) can be more energy efficient solution for recovering erroneous packets [1] [3].

Specific features of WSN, such as short data lengths and low data rates, demand application-specific protocols which consume low power and resources while obeying the performance requirements. Particularly, coding techniques from conventional communication systems (very long data lengths and communication ranges) may not be suitable for WSN and we have to look for viable alternatives, which are fast, resource efficient and low energy consuming [1].

Reed-Solomon (RS) codes are Maximum-Distance-Separable (MDS) codes, providing high error correcting capabilities [4]. Codes defined on larger symbol size are preferred in conventional coding theory, due to low performance of codes on smaller symbol size [4]. However, we show that this conventional approach has limitations in resource constrained WMSN where low data lengths favor the use of codes with smaller symbol size combined with interleaving. Since the comparisons are always made between regular and interleaved codes defined on same alphabet size, we avoid confusion by making as little a change as possible in terminology and call it a Multi-Codec Reed-Solomon (MCRS) scheme henceforth. MCRS is shown to be ultra-low power, reduced resource consuming and having much higher throughput when compared to conventional RS (cRS) scheme. The error correcting capabilities of MCRS can be up to γ times that of cRS scheme, where γ is the number of multiple instances of smaller codec.

II. PROBLEM FORMULATION

A $RS(n, k, 2t)$ code is characterized by a codeword length of $n$ symbols composed starting from a $k$ information symbols. Symbols composing the information and codeword are represented as elements of finite field $GF(2^m)$, i.e., each symbol is composed of $m$ bits. The error correcting capability of such a code is $t$ symbols ($t \times m$ bits). It is known that complexity of finite field arithmetic is exponential with respect to symbol size $m$ [4][5].

While codes defined on smaller symbol size are less complex, they are prone to burst errors. For example, a 9 bit burst error can create maximum of 2 errors in codes defined over $GF(2^8)$ while the same burst can create 3 errors in codes defined over $GF(2^4)$. Another problem in using codes defined over smaller symbol size comes from the information theoretic aspects of coding theory. Given the error correction capability of a cRS codec $t$, a received word can have three scenarios: 1)More than $t$ Detectable Errors, Uncorrectable 2)More than $t$ Undetected Errors 3)Less than $t$ Errors, Detected and Corrected

Let us denote the probability of Detectable but Uncorrectable Errors as $P_{DUE}$, Detectable and Correctable Errors as $P_{DCe}$ and Undetectable Errors as $P_{UE}$. 

1-4244-1342-7/07/$25.00 ©2007 IEEE
The probabilities are given by following formulae [6]:

\[ P_{DUe} = \sum_{i=t+1}^{n} \binom{n}{i} P_b^i (1 - P_b)^{n-i} \]  
\[ P_{DCE} = \sum_{i=0}^{t} \binom{n}{i} P_b^i (1 - P_b)^{n-i} \]  
\[ P_{UE} = \sum_{i=1}^{n} A_i \left( \frac{P_b}{2^n - 1} \right)^i (1 - P_b)^{n-i} \]

where \( t \) is the error correcting capability of the code, \( n \) is the length of the code, \( m \) is the degree of finite field and \( A_i \) is the weight distribution of the code (number of codewords having exactly \( i \) non-zero symbols). \( P_b \) is the bit error probability which is dependent on channel being modeled. It is clear from Equation (1) - (3) that only Probability of Undetected Errors (PUE) depends on the code construction (degree of finite field). PUE for a \( RS(15, 11, 4) \) code defined over \( GF(2^8) \) and \( GF(2^4) \) is plotted in Figure 2 (A) as a function of bit error probability. It is clear that decrease in size of finite field results in an increase in PUE.

Discussions in Example 2 can be summarized as:
(a) Resource, timing and energy constraints favor choice of lower field dimension RS Codec.
(b) PUE and more importantly, burst error case scenario favor choice of higher field dimension RS Codec.
This is another trade-off which we try to overcome in this paper.

III. MCRS: AN INTRODUCTION

Consider that \( i(b), b = 1, 2, \ldots, k \) is a one-dimensional vector that denotes the \( k \) information symbols in \( GF(2^m) \) to be encoded and \( \phi_m \) and \( \varphi_m \) are cRS Encoder and Decoder for code in \( GF(2^m) \). We wish to design MCRS in \( GF(2^\gamma) \), where \( \gamma < m \). Given the information length \( k \), and coderate \( R_c \), the number of \( GF(2^m) \) code instances in MCRS will be:

\[ \gamma = \frac{k \times m}{R_c \times \tilde{m} \times \tilde{n}} \]  

where \( \tilde{m} \) is the code-length for multiple instances of MCRS (note that while keeping the code rate \( R_c \) unchanged, \( \tilde{m} = m/\gamma \)). The vector \( i(b) \) is then transformed into a two dimensional vector \( I(a, b) \) (denoted by \( I(X) \) in Figure 1) i.e. a matrix with dimensions \( \gamma \times k \) entries over \( GF(2^m) \). In such case, the dimensions of \( I(a, b) \) matrix will be given by \([\gamma \times \tilde{m}] \times (R_c \times (\tilde{m} \times \tilde{n})) \) bits. The data is input to the \( \gamma \) instances in a parallel fashion, i.e., in every iteration, \( \gamma \times \tilde{m} \) bits are input to multiple instances of encoders in MCRS, resulting in a MCRS codeword \( C(a, b) \) (denoted by \( C(X) \) in Figure 1).

This MCRS codeword matrix \( C(a, b) \) has dimensions \( \gamma \times \tilde{n} \). The MCRS codeword symbols in each column of \( C(a, b) \) are then concatenated to form a one-dimensional vector \( e(b) \). This vector \( e(b) \) is then transmitted over the wireless channel.

At the receiver end, \( R(a, b) = C(a, b) + e(a, b) \) is obtained by de-concatenating \( r(b) = c(b) + e(b) \). The \( \alpha \) columns of \( R(a, b) \) are then passed to the \( \gamma \) parallel decoders to eliminate the errors \( e(a, b) \) and receive the MCRS codeword \( C(a, b) \). The symbols in each column of \( C(a, b) \) are then concatenated to form the original information symbols. In this form, we consider a symbol in \( GF(2^m) \) as \( \gamma \) symbols in \( GF(2^m/\gamma) \) and a RS codec in \( GF(2^m/\gamma) \) as a two dimensional codec framed up of \( \gamma \) codec in \( GF(2^m/\gamma) \).

Figure 1 (A) shows the code construction overview block for MCRS scheme. The architecture for such a scheme consists of \( \gamma \) parallel RS encoders/decoders designed in \( GF(2^m/\gamma) \) as shown in Figure 1 (B).

Burst Errors: The most important solution offered by MCRS is to the problem of burst errors. In case of MCRS, the errors are distributed among various instances of the codec due to parallel data organization and only very long burst errors can result in uncorrectable error patterns.

Information Theoretic Aspects: Probability of Undetected Errors (PUE) for any code \( C \) is given by (3).

\[ P_{UE} = \sum_{i=1}^{n} A_i(C) \left( \frac{P_b}{2^m - 1} \right)^i (1 - P_b)^{n-i} \]  

Let \( C_\alpha \) be the \( \alpha^{th} \) codec instance in MCRS. PUE for each of the \( \gamma \) instances of the code in MCRS will be given by:

\[ P_{UE}(MC) = \sum_{i=1}^{n} A_i(C_\alpha) \left( \frac{P_b}{2^m/\gamma - 1} \right)^i (1 - P_b)^{n-i} \]  

and

\[ A_i(C_\alpha) = A_i(C_\beta) = A_i(C') \quad \forall \alpha, \beta \in 1, 2, \ldots, \gamma \]  

Notice that all the \( \gamma \) instances of the MCRS scheme are independent of each other. Hence, the PUE of the MCRS codec will be given by:

\[ P_{UE}(MCRS) = \left[ \sum_{i=1}^{n} A_i(C') \left( \frac{P_b}{2^m/\gamma - 1} \right)^i (1 - P_b)^{n-i} \right]^\gamma \]
Figure 2 shows the ratio of PUE for the proposed MCRS scheme and cRS codec for a RS(15,11,4) over $GF(2^8)$ codec and dual $GF(2^4)$. It is clear from the figure that the proposed scheme has a much lower PUE when compared to cRS codec.

IV. MCRS: ERROR CORRECTING CAPABILITIES

Error patterns in MCRS scheme will correspond to different error patterns in cRS scheme. To compare the error correcting capabilities of the two schemes, we wish to find a “mapping” for translating the number of errors in MCRS to cRS codec. Let $l_{\alpha,i}, l_{\beta,j}$ be error locations in $\alpha^{th}$ and $\beta^{th}$ codec instance of MCRS respectively. Let $k_\alpha$ and $I_{\alpha}$, $\alpha = 1,2,\ldots,\gamma$, denote the number of errors and the set containing error locations in $\alpha^{th}$ instance of MCRS codec respectively. To this end, let us define a function $\zeta(l_{\alpha,i}, l_{\beta,j})$ such that

$$\zeta(l_{\alpha,i}, l_{\beta,j}) = \begin{cases} 1 & \text{if } l_{\alpha,i} \neq l_{\beta,j} \\ 0 & \text{otherwise} \end{cases}$$

Without loss of generality, we can assume that $\alpha^{th}$ codec has the maximum number of errors ($k_\alpha$). The set $I_{\alpha}$ gives the values of $l_{\alpha,i}$ i.e. the error locations corresponding to $k_\alpha$ errors in $\alpha^{th}$ codec. For “mapping” of errors, we have the following Lemma:

**Lemma 1:** Given $k_\alpha$ and $I_{\alpha}$ for $\forall \alpha \in \{1,2,\ldots,\gamma\}$, the corresponding number of errors in conventional RS codec is given by:

$$\max(k_1,k_2,\ldots,k_\gamma) + \sum_{l_{\alpha,i} \in I_{\alpha}} \sum_{l_{\beta,j} \notin I_{\alpha}} \zeta(l_{\alpha,i}, l_{\beta,j})$$

**Proof:** The proof follows from the symbol structure in RS codes. Each error in multiple instances of MCRS will translate into an error in cRS codec if and only if there is no error in any other codec at the same location. The function $\zeta(l_{\alpha,i}, l_{\beta,j})$ gives an error count of 0 if two errors occur at the same location and 1 if different locations in $\alpha^{th}$ and $\beta^{th}$ instances of the codec. (9) “maps” the errors by adding the number of errors in the $\alpha^{th}$ codec instance to the additional error count because of varying error locations in multiple codec.

Let the error correcting capability of the cRS code being used is $t_0$. For the error correcting capability of MCRS, we have the following Lemma:

**Lemma 2:** The error correcting capabilities of MCRS scheme $t_{MC}$ is bounded by the error correcting capability of the original scheme $t_0$ and the number of codec instances $\gamma$ as:

$$t_0 \leq t_{MC} \leq \gamma t_0$$

**Proof:** Recall that the error correcting capability of each codec in MCRS is $t_0$. Let

$$k_\alpha \leq t_0 \quad \forall \alpha \in \{1,2,\ldots,\gamma\}$$

From (9), the minimum and maximum number of mapped errors for this case is given by:

$$\max(k_1,k_2,\ldots,k_\gamma) \leq k_{map} \leq \gamma \times \max(k_1,k_2,\ldots,k_\gamma)$$

The lower limit case is given by the condition

$$l_{\alpha,i} = l_{\beta,j} \quad \forall \alpha, \beta \in \{1,2,\ldots,\gamma\}$$

and the upper limit case is given by the condition

$$l_{\alpha,i} \neq l_{\beta,j} \quad \forall \alpha, \beta \in \{1,2,\ldots,\gamma\}$$

Given the condition (11), MCRS can correct all the errors $k_{map}$ and so the claim is proved.

**Worst Case Analysis:** From (12) the worst case scenario will be the one in which errors occur at the same location in both the instances of dual-codec. Notice that if more than $t_0$ errors (say, $t_0 + 1$ for example) occur in any of the instances of the code, it will be equivalent to the same number of errors i.e. $t_0 + 1$, in the cRS codec, which is beyond the error correcting capability of cRS codec. Since both the codec have error correcting capability of $t_0$ errors, this scheme will have as good performance as the original scheme in worst case. Similarly, a $GF(2^4)$ quad codec will have as good performance as cRS and dual codec in worst case. Such a situation is shown in Figure 3 (A).

**Best Case Analysis:** Following (13), the case when $t_0$ errors occur at mutually different locations, corresponds to $\gamma \times t_0$ errors in cRS scheme, which is far beyond its error correcting capability. However, in the proposed scheme, this corresponds to $t_0$ errors in both the instances, which is within the error correcting capability of MCRS. Hence a dual codec has an
error correction capability of $\gamma = 2$ times that of cRS codec in best case. Following the discussion, a quad codec would have an error correcting capability of $\gamma = 4$ times that of cRS codec. Such a situation is shown in Figure 3 (B).

V. MCRS Implementation Results

We present some remarks and implementation results of MCRS and cRS schemes on Tyndall National Institute 25mm wireless motes [7]. Implementation results for memory, time and energy consumption are shown in Table I. It is clear that MCRS reduces the overall power consumption by 43%, memory requirements by 53%. Also, MCRS requires 44% lesser decoding time when compared to cRS scheme. A trade-off in finite field computations is the power consumption due to computational and look-up table models [8]. MCRS reduces the memory requirements for look-up table model from $2^{17}$ bytes for a codec in $GF(2^{16})$ to $2^8$ bytes for corresponding dual codec in $GF(2^8)$ and further to $2^2$ for quad-codec in $GF(2^2)$. These savings further reduce the encoding and decoding power consumption for MCRS.

VI. Conclusion and Future Work

In this paper, we have shown that assumptions from conventional coding theory may not be applicable in resource constrained WMSN. We show that using multiple instances of RS codec in lower finite fields by replacing the conventional RS codec, the performance can be enhanced not only by having possibilities of higher error correcting capability but also by much lower timing, energy and resource requirements. The work has several dimensions in terms of its applicability.

The structure of such a scheme suggests that the scheme can be successfully employed as a solution to an open problem discussed in [9] With a much higher throughput performance, MCRS promises to be a preferable scheme for Delay-intolerant systems. MCRS may also be seen as a collaborative error control coding scheme due to the fact that all the codec instances in MCRS are completely independent of information processing in other codec instances.

ACKNOWLEDGMENT

The authors would also like to acknowledge the financial support of Enterprise Ireland (ATRP-02/227A) and Science Foundation Ireland (Tyndall National Institute National Access Program). The third author has been partially supported by STMicroelectronics.

REFERENCES