Effectiveness of Hamming SEC/DED Code in Harsh Electromagnetic Environments

Jonas Van Waes, Jens Vankeirsbilck
and Jeroen Boydens
Department of Computer Science
KU Leuven, Bruges Campus
Belgium
{jonas.vanwaes,jens.vankeirsbilck,jeroen.boydens}@kuleuven.be

Jonas Lannoo
and Davy Pissoort
Department of Electrical Engineering
KU Leuven, Bruges Campus
Belgium
{jonas.lannoo,davy.pissoort}@kuleuven.be

***Abstract*—Error Correction Codes (ECCs) and Error Detection Codes (EDCs) are widely used in embedded systems and communication networks. Despite the use of an ECC or EDC, data corruption under the influence of electromagnetic interference, can still go unnoticed at the receiver. This phenomenon is commonly known as false negatives. This research analyzes the percentage of false negatives in different EDCs under harsh electromagnetic environments by simulating them with an in-house built simulation framework.**

I. Introduction

In our everyday lives, embedded devices are everywhere, ranging from smartphones and laptops to mission- and safety-critical applications. For an increasing number of them, reliable and robust communication is crucial. However, no communication medium is perfect due to noise and other disturbances, resulting in occasional corruption of transmitted data. This phenomenon is strengthened even further under the influence of harsh electromagnetic environments.

To improve communication reliability, several Error Detection Codes (EDCs) and Error Correction Codes (ECCs) have been proposed. However, in harsh environments, these codes can still report false negatives, i.e. corrupted data deemed valid.

II. Reverberation Room Simulation

By simulating a PBC trace with matched source and load impedances, the effectiveness of ECCs and EDCs is assessed. As depicted in Fig. 1, communication between a sender and a receiver is simulated. The sender sends a bit pattern to the receiver using a certain voltage encoding. The electromagnetic interference (EMI) is added to the sent voltages using superposition and the reciprocity theorem [1]. At receiver side, the received voltages are converted back into a bit pattern and possible errors are detected, corrected or neglected depending on the implemented EDC or ECC.

III. Preliminary Results

Currently, we performed preliminary experiments to assess the effectiveness of two ECCs and two EDCs. As ECCs, we selected Hamming Single Error Correction on the one hand, and data triplication on the other. While for EDC we selected the Hamming Double Error Detection mechanism and

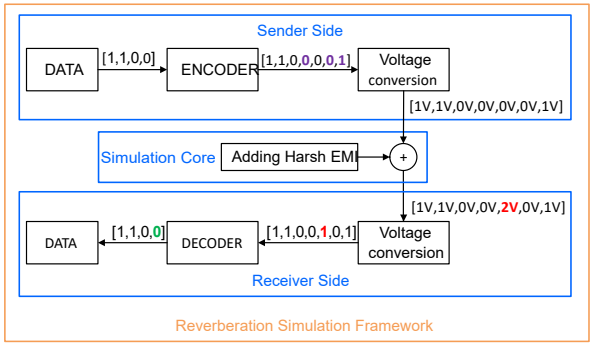

Fig. 1. Simulation Framework Outline

duplication. This paper focuses on the results obtained with the Hamming Codes. As data to be sent, we selected bit patterns of 4 and 11 bits long, based on the maximum data bits for a Hamming code with three and four parity bits, respectively. The bit pattern itself was randomly chosen.

A. ECC Effectiveness

To assess the effectiveness of the selected ECCs, we determined their *Word Error Rate* (WER) for several message lengths and bit frequencies on the PCB trace. In terms of EMI, we considered multiple distinct frequencies for the incoming incident fields. The WER indicates the percentage of mismatches between the data sent at the sender side and the data decoded at the receiver side. These mismatches occur either because the implemented ECC did not correct a received error, or it did *correct* it, but to the wrong bit pattern. These experiments showed that, when certain conditions arise, the implemented ECCs did not yield a better result than when sending unprotected data, which we call the baseline, as can be seen in Fig. 2. A first analysis revealed that these results are produced when the bit frequency and the EMI frequency are integer multiples of each other. Further information about these experiments can be found in [2], [3].

B. EDC Effectiveness

Triggered by these results, we evaluated a Hamming Double Error Detection code and a duplication mechanism. For this

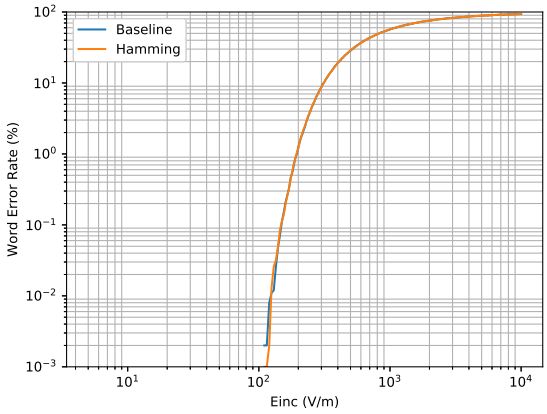

Fig. 2. Hamming SEC with Fbit = 200 MHz

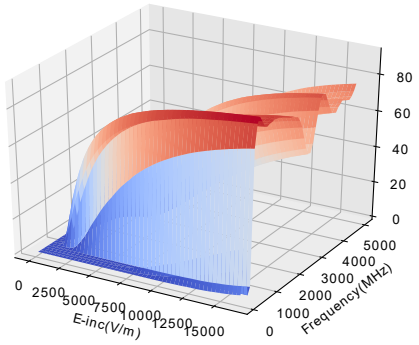

Fig. 3. Hamming EDC with Fbit = 200 MHz

EDC, we specifically focused on the occurrences of false negatives. A false negative denotes that the received data contains one or multiple errors and the implemented EDC has not detected it. Again, the results show a rise in false negatives when the bit frequency and the EMI frequency are integer multiples, as shown in Fig. 3. Therefore, we further analyzed the data. We noticed that for those conditions, the sent bit pattern is either received as an all one or an all zero bit pattern at receiver side. Because these bit patterns are valid bit patterns for the implemented EDC it does not indicate that corrupted data was received. The received data is, however, different from the sent data which is noted as a false negative.

The above conclusion for the rise in false negatives does not hold entirely. For some of the experiments at a bit frequency and an EMI frequency that are not integer multiples, we also saw a rise in false negatives. These results are shown in Fig. 4. Therefore, we suspect that the cause for false negatives might be data dependent. Further experiments with all possible bit patterns for 4 and 11 bits are necessary to find the root cause of this rise in false negatives for certain EMI conditions.

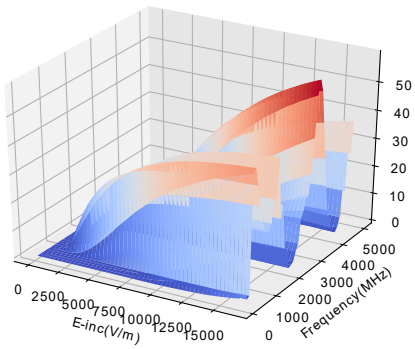

Fig. 4. Hamming EDC with Fbit = 197 MHz

IV. Future Work

The future work is specifically considering the expansion of the simulation framework. Multiple elements should be broadened in order to support the claims made for the currently used specific bit stream. Further expanding the considered bit and disturbance frequencies is needed, again in order to support the claims made in this work. Also, we want to consider ECCs and EDCs with larger Hamming distances, such as Reed-Solomon codes [4] and Bose-Chaudhuri-Hocquenghem codes [5].

V. Conclusions

There is no error detection mechanism identified to be free of false negatives under the influence of harsh EMI. Every mechanism is prone to false negatives when the bit-frequency or data length changes. Unidentified false data has a detriment effect on systems, especially for them residing in safety-critical applications. Therefore, the research continues to test and alter codes to solve this problem. By analyzing different codes, data lengths and bit and disturbance frequencies, it is the goal to develop harsh EMI-resilient codes to increase the reliability of communication channels.

References

[1] F. Vanhee, D. Pissoort, J. Catrysse, G. A. E. Vandenbosch, and G. G. E. Gielen, "Efficient reciprocity-based algorithm to predict worst case induced disturbances on multiconductor transmission lines due to incoming plane waves," *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, no. 1, pp. 208–216, Feb. 2013.

[2] J. Van Waes, J. Lannoo, J. Vankeirsbilck, A. Degraeve, J. Peuteman, D. Vanoost, D. Pissoort, and J. Boydens, "Effectiveness of hamming single error correction codes under harsh electromagnetic disturbances," accepted for EMC Europe 2018, Amsterdam, The Netherlands.

[3] J. Van Waes, J. Vankeirsbilck, J. Lannoo, D. Pissoort, and J. Boydens, "Effectiveness of data triplication in harsh electromagnetic environments," accepted for EMC Europe 2018, Amsterdam, The Netherlands.

[4] I. Reed, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, Jun. 1960.

[5] R. C. Bose and D. . Ray-Chaudhuri, "On a class of error-correcting binary group codes," *Information and Control*, vol. 3, no. 1, pp. 68–79, Mar. 1960.