Mitigating the Effects of Pulsed Interference on Data Communications

Robert H. Boling[(1)], Ira Kohlberg[(2)]

[(1)] ***Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, VA, USA 22311, rboling@org***

[(2)] ***As (1) above, but email: ikohlber@ida.org***

ABSTRACT

Recent studies have focused upon data networks and systems disrupted by bit errors caused by pulsed intentional electromagnetic interference (IEMI). In general, pulsed IEMI is most effective against data systems designed for very low noise environments, in which minimum provisions have been made to mitigate errors. Acknowledging that effective IEMI can cause errors in the transmitted data bit stream, this paper addresses the mitigation of such errors by the application of information coding methods. Specific cases are explored, and the tradeoffs examined between the acceptable error rate and the signal bandwidth and data transmission rate, for a generalized IEMI waveform.

INTRODUCTION AND BACKGROUND

Recent attention and research efforts have focused upon data networks and systems interrupted or even disabled by bit errors caused by pulsed intentional electromagnetic interference (IEMI), as addressed in Cohen, et al [1]. This observation is based upon a combination of recent theoretical studies and experiments employing various electromagnetic sources and environments, such as the paper by Kohlberg and Gardner [2]. Further, the potential vulnerability of data systems to external influences is likely to increase due to lowered voltage planes in integrated circuits under current development.

In general, pulsed IEMI is most effective upon data communication systems that have been designed to function in operational conditions of very high signal to noise (S/N) ratios, in which minimum provisions have been made to mitigate errors (other than requests to retransmit). Such systems usually have a very high information communication rate — reaching one bit of information for each bit transmitted. In particular, most "local" data networks, including those used to communicate and control devices integral to autonomous platforms such as aircraft, operate under such design assumptions. Even systems designed for low S/N are usually based upon expectations of a wideband Gaussian noise environment, rather than an intense pulsed interfering signal, and may be similarly vulnerable to pulsed IEMI.

This paper is an extension of earlier work by the authors addressing the interference of bit communications by pulsed IEMI. In previous papers, we looked at the calculation of probabilities of bit error due to pulse interference [3], and the use of message coding to lessen, or even eliminate, the impact of bit errors on message signaling in certain situations [4].

INFORMATION CODING

Digital data communication is almost always executed in blocks of data, ranging from the familiar 4-bit representation of a numeric digit, to the 8-bit ASCII code for alphanumeric characters. For generality, however, we

consider that a continuous stream of information bits is translated into a series of symbols (blocks) for transmission. Coding for error mitigation may be considered to be an algorithmic method to add redundant bits to a block to aid in detecting and correcting errors in digital communication [4].

It is clear that, if every block code in a chosen set differs in three or more bits from every other coded block in the set, a single-bit error will not cause an incorrect block decision at the detector, because the disrupted block is still most like the "correct" block than any other. Formally, the measure of the bit-wise difference between two coded blocks is known as the Hamming distance, d_H. It can be shown [5] that a coding scheme that produces blocks with a minimum difference, or distance, of $d_{H,min}$ can correct up to t errors, where

$$t = \lceil (d_{H,min} - 1)/2 \rceil,$$

and the half-brackets mean the largest integer less than or equal to the argument.

Further, it is known [6] that, for any positive integers m and t (where $m = n - k$, and n is the block size in bits, and k is the number of information bits in the block), a code exists that can correct t errors with

$$n = 2^m - 1 \quad \text{and} \quad k \geq n - mt,$$

and, of course, $d_{H,min} \geq 2t + 1$.

As an example, if $t = 1$ and $m = 3$, then $n = 8 - 1 = 7$ and $k \geq 7 - 4 = 3$. That is, a block code exists where each 4-bit input "word" is encoded to become a 7-bit block that is effectively immune to a single bit error in *any* of its seven bits.

There is, of course, a cost to error correction or prevention via encoding, which is exhibited in increased transmission bandwidth or time, and in transceiver complexity. Also, if the bandwidth is expanded to accommodate the increased bit rate, the noise bandwidth expands accordingly.

PULSED INTENTIONAL ELECTROMAGNETIC INTERFERENCE

For the purposes of this paper, the interfering signal will be considered to be a single pulse of duration δ and repetition interval T. We will not address the probabilities of causing bit errors(s) due to the IEMI pulse – we readily concede such error(s). The amplitude and phase of the IEMI pulse is considered to be adequate to cause a detection error of all signal bits during the period δ. Although the actual transmitted pulse waveform may, in fact, be much shorter in duration, but the complex pulse shaping effects of excited cavities, scattering [2], and other pulse-extending phenomena are assumed in this paper to be expressed effectively by the considered pulse width δ.

For discussion, consider blocks of n-bits to be transmitted over the network at B blocks per second. The resultant bit rate is therefore nB /second. Note that the period of each transmitted bit is $1/nB$ seconds, and the number of bits corrupted by a single IEMI pulse will be δnB. As an obvious example, if the signal transmission rate is such that the interfering pulse corrupts only a single bit, and the pulse repetition interval T is greater than 7δ, then the encoded system could use the seven-bit code described above and communicate *without error* continuously!

CONCLUSIONS

If the coding and transmission rates are known for the encoded system, the waveform of the IEMI can be optimized. On the other hand, the selection of an effective coding protocol, transmission rate, and detection scheme can also be optimized if the form of the IEMI transmission is known. At this time, it appears that the IEMI signal offers far less flexibility than the coding protocol. In fact, an adaptive data communication scheme is easily devised to thwart a disruptive attack if the IEMI inter-pulse interval $T >> \delta$, the pulse duration. It has been noted that this is usually the case, for conventional high power RF pulse generators.

This approach to mitigating pulsed IEMI will have its greatest impact when applied to just the type of environments discussed earlier as primary 'targets': local area networks or control links configured for a low-noise environment. Such systems usually have a surplus of unused bandwidth, and may easily accommodate the higher bit rate required to maintain the same (unencoded) information rate.

REFERENCES

[1] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, "Breakdown of the Internet under intentional attack," Phys. Rev. Lett. 86, pp 3682-3685, April 2001

[2] I. Kohlberg and R. L. Gardner, "Systems Topology for Electromagnetic Effects on Local Area Networks and Information Systems," Proceedings of the International Conference on Electromagnetics in Advanced Applications (ICEAA 01), Torino, Italy, pp 83-86, September 10-14, 2001

[3] I. Kohlberg and R. Carter, "Some Theoretical Considerations Regarding the Susceptibility of Information Systems to Unwanted Electromagnetic Signals," Proceedings of the 14th International Zurich Symposium on Electromagnetic Compatibility, Zurich, Switzerland, paper #883 (in press), February 20-22, 2001.

[4] R. Boling and I. Kohlberg, "Effects of Unwanted Electromagnetic Signals on Message Signaling," presented at USNC-URSI National Radio Science Meeting, Boulder, Colorado, January 8-12, 2002.

[5] Don J. Torrieri, *Principles of Secure Communication Systems*, Norwood, MA: Artech, p36, 1985

[6] Edward Lee and David Messerschmitt, *Digital Communication*, Boston: Kluwer Academic Publishers, pp 478, 1988