ERROR CORRECTION IN HIGH FREQUENCY AUTOMATIC LINK ESTABLISHMENT RADIOS WITH AND WITHOUT LINK PROTECTION

Richard Lay
Naval Command, Control and Ocean Surveillance Center
Research, Development, Test and Evaluation Division
Electronic Countermeasures Branch

ABSTRACT

Error correcting techniques used by High Frequency Automatic Link Establishment (HF ALE) radios, including those with link protection, transform a basic 24-bit ALE word into 147 bits to be transmitted and received. This paper examines the effect random errors in the 147 received bits have on the received 24-bit ALE word.

ALE ERROR CORRECTION

High Frequency Automatic Link Establishment (HF ALE) radios conforming to MIL-STD-188-141A [1] utilize error correcting code, interleaving, and redundancy to reduce errors in the received data. In these radios, a 24-bit ALE word to be transmitted is divided into two 12-bit subwords. Each of these subwords is encoded using the Golay (24,12) error correction code, resulting in a total of 48 bits after the encoding. These 48 bits are interleaved, and a 49th stuff bit is added. This 49-bit block is repeated 3 times, for a total of 147 bits to be transmitted. These bits are 8-ary FSK modulated and transmitted. The receiver demodulates the signal, and a 2/3 majority vote is performed on the 147 received bits, resulting in a 49-bit block. Ignoring the 49th stuff bit, the 48 bits are deinterleaved and Golay (24,12) decoded. The result is a received 24-bit ALE word. See Figure 1.

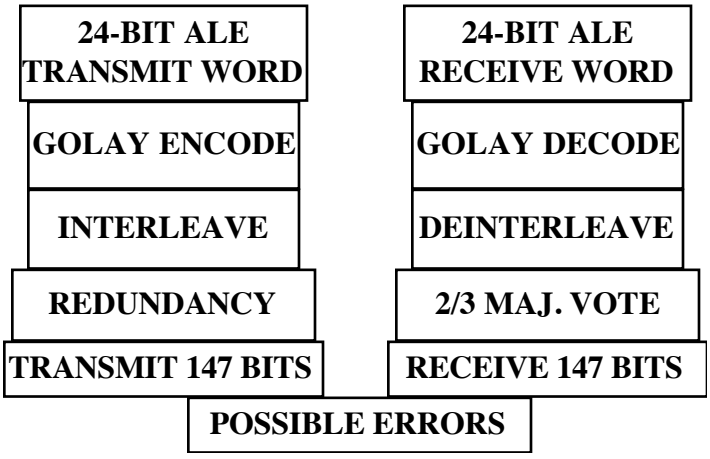

Figure 1. Error correcting scheme used in HF ALE radios.

In HF ALE radios with linking protection (LP) provided, the 24-bit ALE word is first encrypted before the Golay encoder, and decrypted after the Golay decoder. See Figure 2. For some LP applications, an encryption algorithm [2] is specified [1].

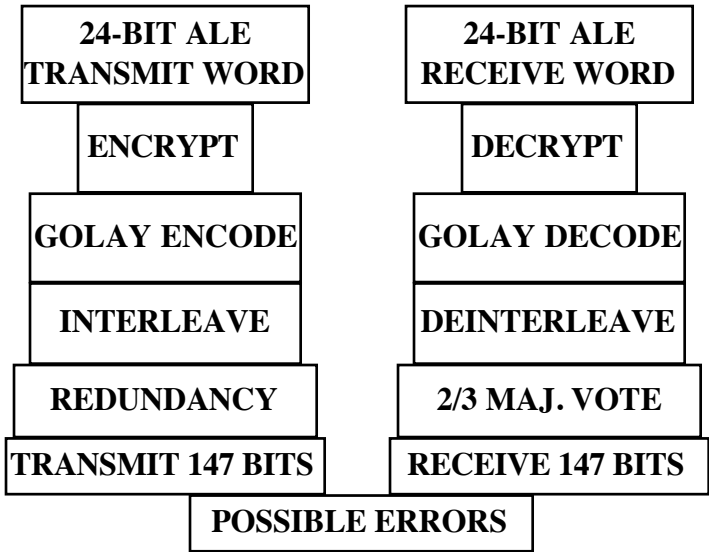

Figure 2. Error correcting scheme utilized in HF ALE radios with Link Protection.

Although ALE radios use adaptive frequency techniques to avoid interference [1] a smart jammer may be able to follow the frequency changes. Thus this paper will be more applicable in cases of intentional interference, where the possibility of frequency following exists.

EFFECT OF ERRORS

The effect receive-bit errors have on the received ALE word was investigated using code developed to simulate HF ALE radios [3]. The code was modified to allow specific errors to be added to the 147 received bits.

The investigation proceeded as follows. A 24-bit ALE transmit word was encrypted (if LP utilized), Golay encoded, interleaved, and repeated. Of the 147 bits, a number selected at random were inverted. These bits proceeded to the 2/3 majority voting, deinterleaving, Golay decoding, and decrypting (if LP utilized). The resulting received 24-bit ALE word was compared to the transmit ALE word, and the number of bit errors totaled.

In one experiment, the ALE word 'THIS IS SAM' (55160315 octal) was used as the transmit ALE word. The number of random errors added to the transmit bits ranged from 0 to 147. Figures 3 and 4 show the minimum, maximum, and average number of errors in the received ALE word, taken over 1000 runs.

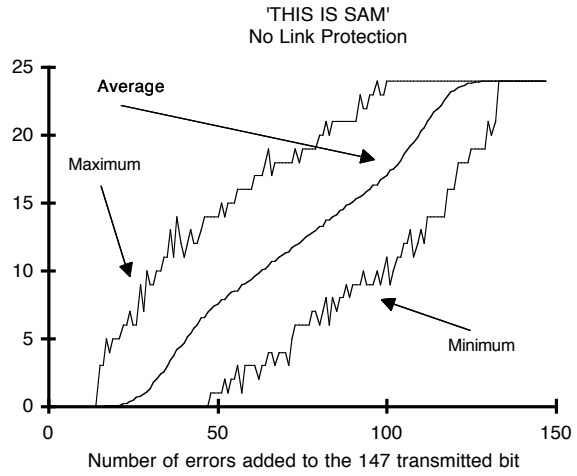

Figure 3. Minimum, maximum, and average number of errors in the received ALE word, taken over 1000 runs. The input ALE word was 'THIS IS SAM'. No Link Protection.

A 1-bit error in the encrypted ALE word makes a considerable number of errors in the decrypted ALE word [2]. This effect manifests itself in Figure 4 as a sharp increase at around 35 added errors. Note in Figure 3 that at 35 added errors the average number of received word errors is about 1.

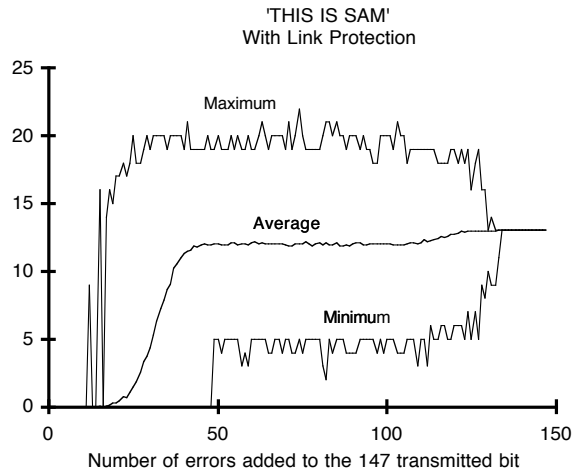

Figure 4. Experiment results for ALE word 'THIS IS SAM', with Link Protection.

One would expect the average number of errors in the LP case to be about 50 percent, after a rapid rise from 0. Figure 4 shows that the average number of errors increases from 12 to 13 as the number of added errors approaches 147. This is an effect of the LP algorithm. For 147 received bit errors (all bits inverted) the output of the Golay decoder is an inverted version of the input to the Golay encoder, as in the non-LP case. Once these bits pass through the decryption algorithm the difference between the resulting received ALE word and the transmitted ALE word can be anything from 0 to 24 bits. This is equivalent to encrypting the ALE word, inverting the bits, and decrypting it. The actual number of errors will depend on the ALE word, and on variables used in the LP algorithm. So as the number of added errors approaches 147, the number of received word errors will approach some pseudorandom constant, not necessarily 24. In Figure 4, this constant is 13.

Figures 5 and 6 show results obtained using 'TO BOB' (24123702 octal) as the ALE transmit word. Note the number of word errors in Figure 6 approaches 9 as the number of added errors approaches 147.

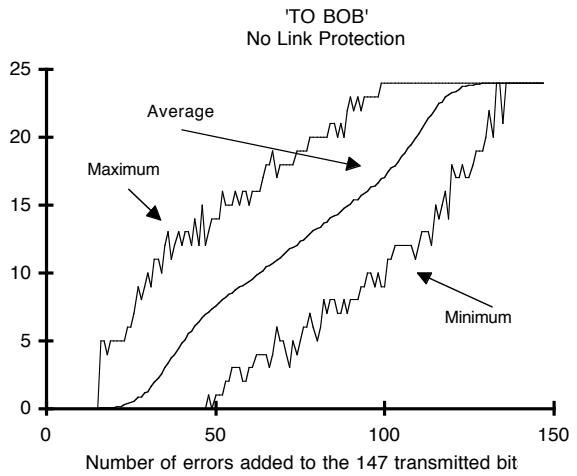

Figure 5. Minimum, maximum, and average number of errors in the received ALE word, taken over 1000 runs. The input ALE word was 'TO BOB'. No Link Protection.

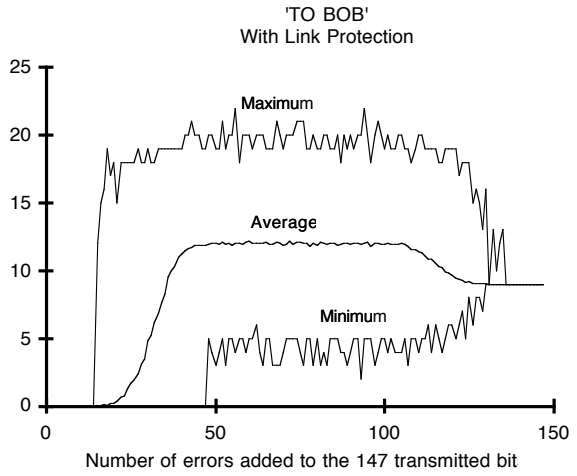

Figure 6. Minimum, maximum, and average number of errors in the received ALE word, taken over 1000 runs. The input ALE word was 'TO BOB'. With Link Protection.

Without LP, 29 errors must occur in the received bits to cause 1 bit error, on average, in the received ALE word. With LP, 24 added errors are required. The number of added errors required to cause 4 bit errors is 38 (no LP) and 30 (with LP).

INTERFERENCE

To show what level of interference might be necessary to achieve the corresponding added bit errors discussed in the previous section, assume the interference is white Gaussian noise. This assumption leads to a probability of symbol error given a specific signal to noise level, as derived by Torrieri [4]. Also assume that whenever the receiver is in error for an 8-ary symbol, the output is equally likely to be any of the 7 other 3-bit symbols. This assumption leads to a probability of bit error given a probability of symbol error, as derived by Stremler [5]. Given these results, one may plot the probability of a bit error given a signal to noise ratio. See Figure 7. Figure 8 shows the probability of a bit error vs. the noise to signal ratio.

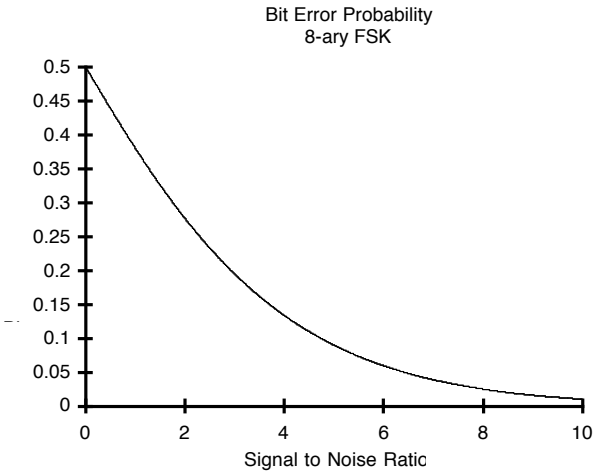

Figure 7. Probability of bit error for 8-ary FSK vs. signal to noise ratio.

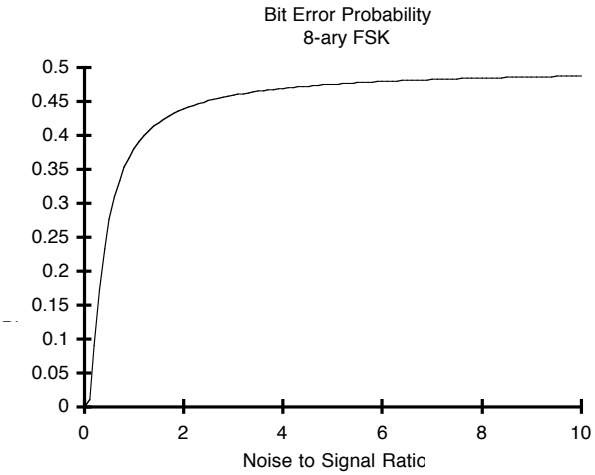

Figure 8. Probability of bit error for 8-ary FSK vs. noise to signal ratio.

To illustrate the use of these plots, assume a 1 bit error in the received ALE word is desired. Assume the link is not protected (no LP). From Figure 3, this requires 29 errors on average, or a 29/147 20 percent error rate. From Figure 7 the signal to noise ratio required to achieve a 20 percent error rate is about 3.

CONCLUSION

Link protection makes ALE radios more susceptible to errors. If these errors are caused by interference from a frequency following jammer, the adaptive frequency capabilities of ALE radios may not be able to compensate. However, ALE radios without link protection are more susceptible to other types of jamming, such as playback jamming and malicious linking attempts.

ACKNOWLEDGEMENT

This work has been supported by the Office of Naval Research. The author would like to thank Dr. Eric E. Johnson for the use of his ALE simulation code.

REFERENCES

[1] MIL-STD-188-141A, "Interoperability and Performance Standards for Medium and High Frequency Radio Equipment," U.S. Army Information Systems Engineering Command, Fort Huachuca, Arizona, 1992.

[2] Technical Report ASQB-OSI-S-TR-92-04, "A 24-Bit Encryption Algorithm for Linking Protection," U.S. Army Information Systems Engineering Command, Fort Huachuca, Arizona, 1992.

[3] ALE/LP simulator code written by Dr. Eric E. Johnson, New Mexico State University, 1992.

[4] D. J. Torrieri. *Principles of Secure Communication Systems*. Norwood, M.A.: Artech House Inc., 1985.

[5] F.G. Stremler. *Communication Systems*. Reading, M.A.: Addison-Wesley, 1990.