IEEE 802.11
Wireless Access Method and Physical Layer Specifications

Title: Using Data Scrambling for the IEEE802.11

Date: May 5, 1995

Authors:

John Fakatselis, Al Petrick, Carl Andren
Harris Semiconductor
P.O. Box 883
Melbourne, Florida 32901-0883
Telephone: 407-729-4733
Fax: 407-724-7094
E-mail: jfakat01@ccmail.mis.semi.harris.com
E-mail: apetrick@ccmail.mis.semi.harris.com

Abstract

This submission was requested by the DS-PHY sub-group to review the need for data scrambling. This paper describes a fundemental understanding and the advantages for data scrambling in the DS-PHY and FH-PHY layers as derived from the current IEEE802.1 working draft document.

General Overview

The proposed IEEE802.11 scrambler for Direct Sequence (DS) utilizes a maximal length pseudorandom (PN) sequence of 127 bits to randomize the data bits. Some basic reasons for scrambling the signal are summarized below:

Scrambling for Direct Sequence

A. The DS signal is spread with a very short sequence. Since the Barker sequence used is 11 bits long at a rate of 11MCPS , it causes the spectrum to have 11 discrete spectral lines (or 22 null to null) spaced at the reciprocal of the spreading sequence length rate. The rate that the 11 bit spreading sequence repeats itself is 1 microsecond (i.e. 1 MBPS BPSK data), so the lines are spaced in 1 MHz frequency intervals. The scrambling will effectively provide additional spreading to each of the spectral lines of this minimally spread DS signal. The additional spreading due to the scrambling will have a null to null bandwidth of up to 2 MHz reflecting the maximum bit rate which is presently defined at 2MBPS. Since the spectral lines due to the DS spreading alone are 1 MHz apart, scrambling will fill in reasonably well between these lines. The scrambling line spectrum will have a spacing of 1/127 MHz or about 8 KHz. This is derived from the recommended scrambling sequence which is 127 (2^7-1) bits long. Thus the overall spectrum between the DS code and the data scrambling code will have 22*127 or 2794 lines. Each of these spectral lines will have 21 dB (10 log 127) lower amplitude than the case where no scrambling is used. This results to reduced interference caused by the transmitted DS waveform against any other signals that coexist over the same bandwidth.

In the absence of scrambling, the data patterns could contain long strings of ones or zeros. This is definitely the case with the proposed DS preamble which has a stream of 128 continuos ones. The continuos ones would cause the spectrum to be concentrated at the discrete lines defined by the spreading code and potentially cause interference with other narrow band users at these frequencies. Additionally, the DS system itself would be moderately more susceptible to interference at these frequencies. With scrambling, the spectrum is more uniform and these negative effects are reduced, in proportion with the scrambling code length.

B.The second reason to scramble is to gain a small measure of privacy. The DS nature of the signal is easily demodulated with a correlating receiver. Indeed, the data modulation can be recovered from one of the discrete spectral lines with a narrow band receiver (with a 10 dB loss in sensitivity). This means that the signal gets little security from the DS spreading code alone. Scrambling adds a privacy feature to the waveform that would require the listener to know the scrambling parameters in order to listen in. When the data is scrambled it cannot be defeated by listening to one of the scrambling spectral lines since the unintentional receiver in this case is too narrow band to recover the data modulation. This assumes though that each user can set up different scrambling patterns achieving privacy from casual snoopers (presently there is a single scrambling code defined). There are 9 maximal length codes that can be utilized with a generator of length 7. The different codes can be used to implement a basic privacy scheme. It needs to be clear though that this small scrambling code length and the actual properties of such codes are not a major challenge for a sophisticated intentional interceptor to be listening in. This is why we refer to this scrambling advantage as a communications privacy feature as opposed to a secure communications feature .

Scrambling for Frequency Hop

In addition to the DS case, scrambling can be applied on the Frequency Hop (FH) version of IEEE802.11. There is an additional benefit to be mentioned for the FH case. Some FSK receivers that are using Automatic Frequency Control (AFC) have a problem with long runs of ones or zeros. These continuous runs tend to bias the frequency measurement and cause data degradation. Scrambling breaks up such continuos streams in the data and prevents this problem. For users without AFDC, the scrambling still might provide some benefit. If interference is on the mark or space frequency, the data decisions will be biased accordingly towards ones or zeros. With scrambling, the demodulation errors are still the same, but the error statistics are evenly spread between one and zero decisions. For some cases this might be a desirable statistical relationship.

As far as the spectral benefits of scrambling on FH, they are similar to those for DS. Continuos data streams of either ones or zeros will tend to concentrate the spectral energy at the mark or space frequency and cause additional interference to other users of the same channel. Scrambling breaks up these streams and it more evenly spreads the spectral energy. Binary FSK has a two line spectrum which is smeared with a sinx/x waveform when the data is randomized. With narrow deviation, the waveform peaks are not discernible. With a stream of ones, the spectrum would collapse to a single line, which can cause increased interfere to other coexisting signals.

The privacy benefits for FH are the same as for the DS case. FH gains a small additional measure of privacy by hopping, but the proposed hop rates are relatively low and can be easily overcome by a fast scanner.