Harris Semiconductor

APPNOTE

No. AN9701 February 1997

Harris Wireless Products

CRC-16 Algorithm for Packetized WLAN Protocols on the HSP3824

Authors: Al Petrick, John Fakatselis

Introduction

In packetize RF data transmissions systems, transmitted messages are susceptible to various types of bit errors due to noise, interference, data collisions, and multipath in a given RF channel. The main purpose of error detection algorithms is to enable an RF receiver of a transmitted message to determine if the message is corrupted. There are various types of error detection algorithms to chose from. The most common method for detecting bits errors in messages is through the use of CRCs (Cyclic Redundancy Codes). CRCs are very useful in detecting single bit errors, multiple bit errors, and burst errors in packetized messages. In theory CRCs could be thought of as simply taking a binary message and dividing it by a fixed binary number, with the remainder being the checksum, or more commonly the CRC. The fixed binary number is the divisor commonly called the polynomial. The CRC-16 algorithm is specified by the IEEE802.11 for use in the direct sequence physical layer PLCP (Physical Layer Convergence Protocol). The CCITT CRC-16 is a standardized algorithm with origins to the CCITT standards body. The polynomial for the CRC calculation is a 16-bit function and is given as $Gx = X^{16} + X^{12} + X^5 +1$. The mathematics performed on in calculating the CRC is binary modulo 2 arithmetic, and typically implemented with an XOR function.

CRC16 Algorithm Implementation

The HSP3824 implements the specified IEEE802.11 CRC function. The CRC can be programmed to protect the PLCP header fields. Any error detected by the CRC on the header will flag the MAC and the package will be dropped. The HSP3824 can be programmed to process the packet independent of the CRC indication. This mode may be applicable for non - IEEE802.11 applications.

In this mode the HSP3824 can is configured to pass the data to the MAC even when a CRC error has occurred. In this case the MAC can decide on how the packet data can be used.

There are various ways to implement a CRC algorithm in software and hardware. Processing the IEEE802.11 PLCP DS-PHY header is a time critical function, which favors a hardware approach. A typical implementation is illustrated in Figure 1. The CRC calculator illustrated uses a 16-bit D-Flip-flop shift register an three XOR gates to perform the modulo 2 arithmetic. Only the coefficient taps in the polynomial are used with the XOR gates for modulo 2 arithmetic. The message is shifted in serially MSB first. The resultant 16-bit parallel output is the remainder, inverted and appended as the checksum of the message. The CRC checker at the receive end needs to be initialized with an all “1's” value. The CRC check engine will calculate the proper sum assuming that an all 1's value has been used as the initialization seed. The CRC generator will lock if it is initially seeded with a value of all zeros. This initial condition needs to be avoided.

CRC16 Protected Fields in the PLCP Header

The CCITT CRC-16 is calculated bit serially in the HSP3824 protecting the Signal, Service and Length fields of the PLCP header. Figure 2 illustrates the Preamble and PLCP header used for IEEE802.11 data transmission. This feature is enabled in the HSP3824 by asserting bits 3 and 4 of control register CR# 0 to a logic “1”. Before the PLCP header is transmitted a CRC-16 checksum calculated and appended to the length field. The Signal, Service and Length fields of the PLCP header are clocked bit serially (MSB) first through a shift register, and multiplied by tapped branches corresponding to the polynomial $Gx = X^{16} + X^{12} + X^5 +1$. Typically CRC algorithms initialize their shift registers to some known value. For the IEEE802.11 algorithm a value of all ones has been chosen. The initialization value has no impact on the performance of the CRC calculation. Initialization only provides a starting point for processing the checksum. In some cases, it is possible for the data in the signal and service fields to be zero values.

After the 32 bits of the PLCP header are shifted into the CRC calculator, the remainder a 16-bit value is configured into a 16-bit word, logically inverted and appended to the length field as its own field. At the receiving DS-PHY, the incoming message, is processed through the same algorithm after the detection of a valid SFD (start-of-frame delimiter). The CRC-16 is recalculated on the PLCP header and compared against the transmitted value for bit error discrepancies. If the calculated checksum of the received message differs for the transmitted appended value, then the message is declared corrupt and discarded.

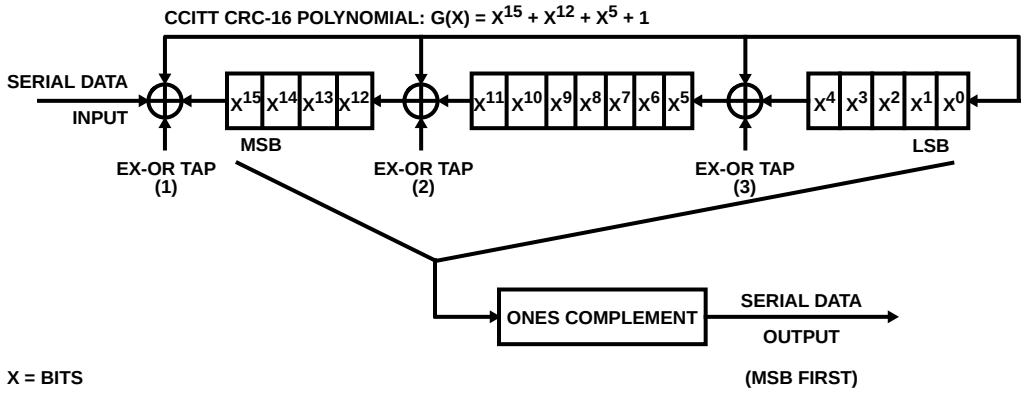

FIGURE 1. CCITT CRC-16 IMPLEMENTATION

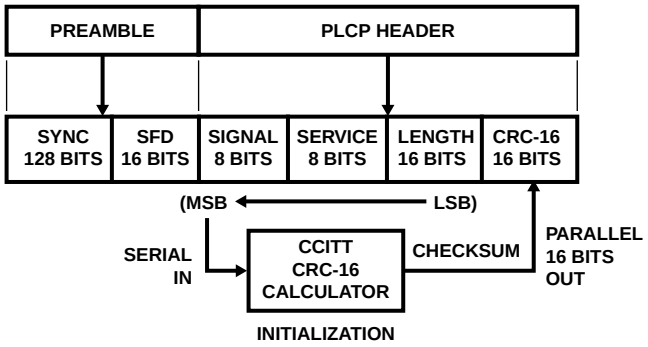

FIGURE 2.

All Harris Semiconductor products are manufactured, assembled and tested under **ISO9000** quality systems certification.

Sales Office Headquarters

For general information regarding Harris Semiconductor and its products, call **1-800-4-HARRIS**

NORTH AMERICA
Harris Semiconductor
P. O. Box 883, Mail Stop 53-210
Melbourne, FL 32902
TEL: 1-800-442-7747
(407) 729-4984
FAX: (407) 729-5321

EUROPE
Harris Semiconductor
Mercure Center
100, Rue de la Fusee
1130 Brussels, Belgium
TEL: (32) 2.724.2111
FAX: (32) 2.724.22.05

ASIA
Harris Semiconductor PTE Ltd.
No. 1 Tannery Road
Cencon 1, #09-01
Singapore 1334
TEL: (65) 748-4200
FAX: (65) 748-0400

HARRIS SEMICONDUCTOR