Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**A fix for the DES encryption engine for OFDM.**
Date Submitted	**2004-07-08**
Source(s)	Raja Banerjea Proxim Corp. 935 Stewart Drive Sunnyvale, CA – 94085 350 rbanerjea@proxim.com Voice: 408-731-2870 Baraa Al-Dabagh Intel Corporation CHP3-105, East Plumeria Dr San Jose, CA 95134 baraa.al.dabagh@intel.com
Re:	Supporting document for recirculation ballot #14b.
Abstract	A fix for the DES encryption engine for OFDM.
Purpose	Discussion/Information
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:r.b.marks@ieee.org > as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

A fix for the DES encryption engine for OFDM

Introduction

This document describes a fix for the DES encryption engine for OFDM in the IEEE 802.16d/D5

Abstract

The addition of DLFP to the OFDM section in IEEE 802.16d/D4 and the removal of the parameters in the PHY synchronization field for OFDM made the DES encryption engine in OFDM unusable as defined. In this document we present a suggested change, which would fix the DES encryption engine for OFDM.

Background

The PHY Synchronization field parameters were removed going form IEEE 802.16d/D3 to IEEE 802.16d/D4. The OFDM PHY sync field is required by the DES encryption engine and therefore unless defined clearly could lead to the DES engine being unusable. The parameters of the PHY Synchronization field were removed in draft D4 and the information was moved to the DCD and the DLFP.
The information is therefore present in the latest draft, but wording needs to be added to redefine the DES encryption for OFDM.

Proposed Text

Modify page 297, line 26
The CBC IV for SCa and OFDMA shall be calculated as follows: in the downlink, the CBC shall be initialized with the exclusive-or (XOR) of (1) the IV parameter included in the TEK keying information, and (2) the content of the PHY Synchronization field (right justified) of the latest DL-MAP. In the uplink, the CBC shall be initialized with the XOR of (1) the IV parameter included in the TEK keying information, and (2) the content of the PHY Synchronization field of the DL-MAP that is in effect when the UL-MAP for the uplink transmission is created/received.

Add to page 297, line 33
The CBC IV for OFDM shall be calculated as follows: in the downlink, the CBC shall be initialized with the exclusive-or (XOR) of (1) the IV parameter included in the TEK keying information, and (2) the content of the OFDM PHY Synchronization word (right justified). In the uplink, the CBC shall be initialized with the XOR of (1) the IV parameter included in the TEK keying information, and (2) the content of the OFDM PHY Synchronization word that is in effect when the UL-MAP ~~for the uplink transmission is created/received~~ is transmitted. The OFDM PHY Synchronization word is formed by the 8-bit Frame Duration Code (Table 211) and the current frame number. The frame duration code is transmitted in the DCD message. The 20 msb of the frame number is obtained from the 20 msb of the frame number transmitted in the DCD message. The 4 lsb of the frame number is transmitted in the DLFP for non AAS SS and in the AAS_DLFP for the AAS enabled SS.

OFDM PHY Synchronization word