Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	OCSI Collusion detection and resolution between systems
Date Submitted	**2006-11-10**
Source(s)	Wu Xuyong, Huawei Huawei Industrial Base, Bantian, Longgang, Shenzhen 518129 P.R.C Voice: +86-755-28972327 Fax: wuxuyong@huawei.com
Re:	80216h-06_059：IEEE 802.16 Working Group Working Group Letter Ballot #24 (2006-10-11)
Abstract	By studying the case of the operating phase of CX systems, we find some case that not able to be solved in current draft. Here is point out some direction of effort which may work. Further discussion and remedy may be needed.
Purpose	To consolidate the working document.
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 <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of 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:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

OCSI Collusion detection and resolution between systems

Wu Xuyong
Huawei

Overview

The solution within the draft1 ensures that OCSI is not reused within one neighborhood. But the neighborhood is sometime is changed by the environment. Let's study on the following cases for the operating system, see the following figure:

Case1: Two systems operating in the same channel with the same OCSI, the two system does not interference with each other before, e.g. because of some obstacle between them. When obstacle between disappear, one of the system begin to interfere with another. (figure after arrow1)

Here we find the SS under interference can not receive the signaling information from the new interfere source, because its serving BS is occupying the same OCSI. But SS can still discover some new interference in the OCSI slot supposed to be silent within this OCSI. TBD: [configure message] [count for silent slot] [monitoring silent slot]

SS can report to the serving BS. The BS will temporary cease signaling broadcasting in order to let SS receiving the information sent by the neighbor. (figure after arrow2) TBD: [error report message] [ceasing to SS notify message 0/1] [ceasing to NB notify IP message 0/1]

When SS report the information it get or timer count down to zero, BS notify the ceasing phase ending, SS will then go the normal monitoring status. TBD: [ceasing timer] [modify RPT_RSP message]

1) If the BS get the contact information from the SS's report, it can than negotiate with the neighbor system to solve the interference. (figure after arrow3)

2) Else if this SS keep receiving harmful interference within this OCSI but can not identify the information inside, the system should consider to reallocated its resource else where.

3) Else, means the SS can not receive any harmful interference in this OCSI any more, after the timer expired, the system will go the normal operation and keep using the original resource.

Case2: The rest of situation is the same as case 1, except that SSs in both systems have discovered new interference within its OCSI.

Now, in order not prevent dead lock from everyone stop broadcasting within the period (figure after arrow2), we need to introduce a random back off method after the ceasing timer expired (figure after arrow2). Which means the BS will then randomly send a broadcasting message in a back off window (figure after arrow3). And try certain times with different window size, the systems follow the similar decision tree in case 1. TBD: [RB to SS notify message 0/1] [RB to NB notify IP message 0/1] [window timer[min step max]] [Maximum RB counter]

1) If the BS get the contact information from the SS's report, it can than negotiate with the neighbor system to solve the interference. (figure after arrow 4)

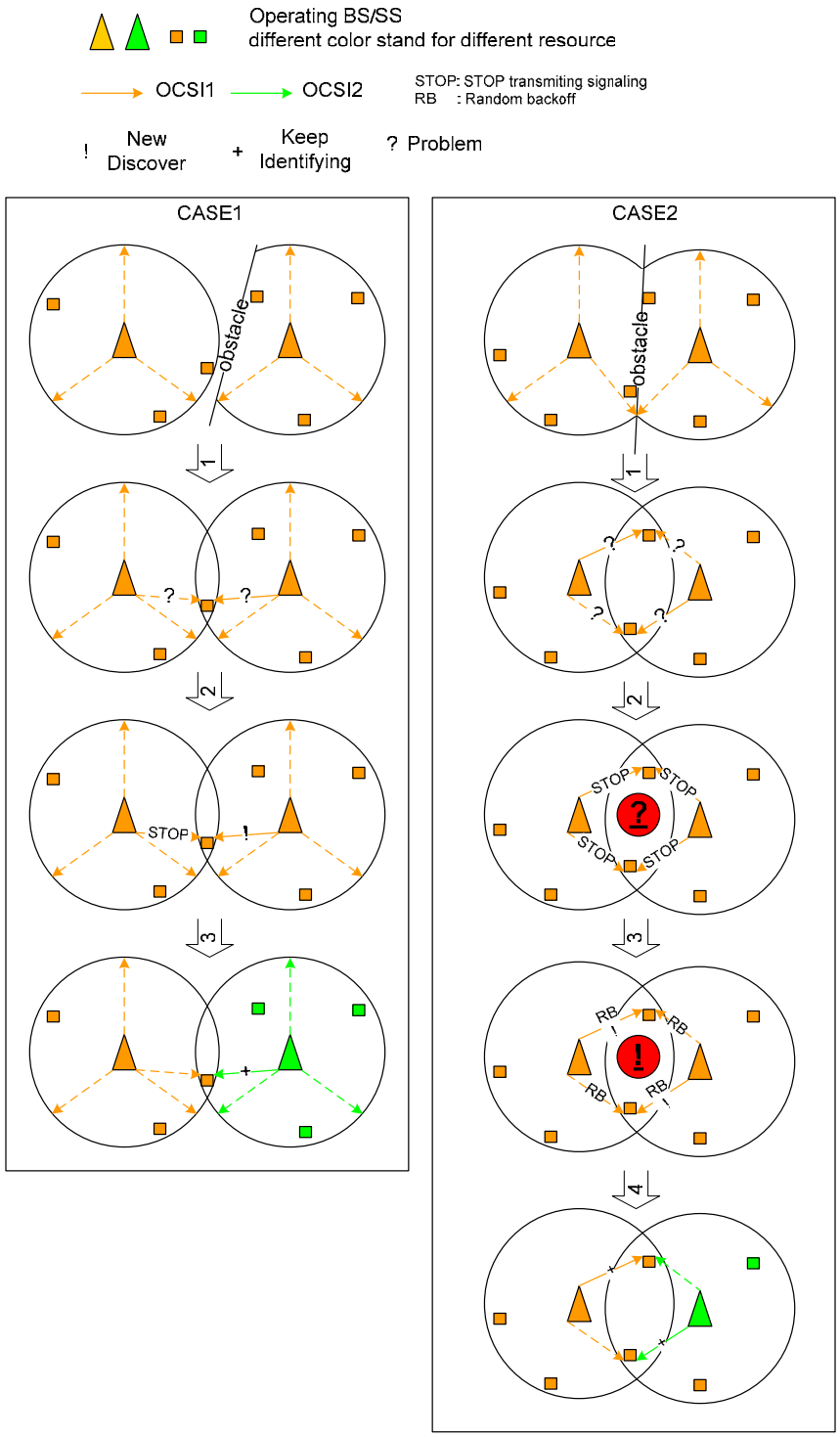
2) Else if this SS keep receiving harmful interference within this OCSI but can not identify the information inside, the system should consider to reallocated its resource else where.

3) Else, means the SS can not receive any harmful interference in this OCSI any more, after the ceasing timer expired, the BS will run a random back off procedure. With the parameter min/max window size and the maximum backoff counter.

a) Within each back off window, BS will send out one broadcasting message with random offset. In the mean while, SS keep monitoring the interference, once successful to receive the message from neighbor, the system can than negotiate with the neighbor system to solve the interference. The whole procedure will end up.

b) When back off window expired, and maximum backoff counter does not reach, BS will start another backoff window with updated size.

c) If the counter reaches, the system will go the normal operation and keep using the original resource.



Reference:

[1] *IEEE P802.16h/D1: Working Document for P802.16h (2006-08-01)*

[2] *80216h-06_059：IEEE 802.16 Working Group Working Group Letter Ballot #24 (2006-10-11)*

[3] *IEEE 802.16-2004: IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems (2004-10-01)*

[4] *IEEE 802.16e-2005: IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1 (2006-02-28)*

[5] *IEEE C802.16h-06/054 Discussion on implementing the energy pulse (2006-07-10)*

Proposed Changes:

BS2SS message

[Configure message]

Tbc.

[Ceasing to SS notify message 0/1]

Tbc.

[RB to SS notify message 0/1]

Tbc.

SS2BS message

[Error report message]

Tbc.

[Modified RPT_RSP message]

Tbc.

[RB to NB notify IP message 0/1]

Tbc.

BS2BS IP message

[Ceasing to NB notify IP message 0/1]

Tbc.

Description

[Count for silent slot]

Tbc.

[Monitoring silent slot]

Tbc.

Parameter

[Interference Criteria]

Tbc.

[Ceasing timer]

Tbc.

[Window timer [min step max]]

Tbc.

[Maximum RB counters]

Tbc.