Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	OCSI Collusion detection and resolution between systems
Date Submitted	**2006-11-11**
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)

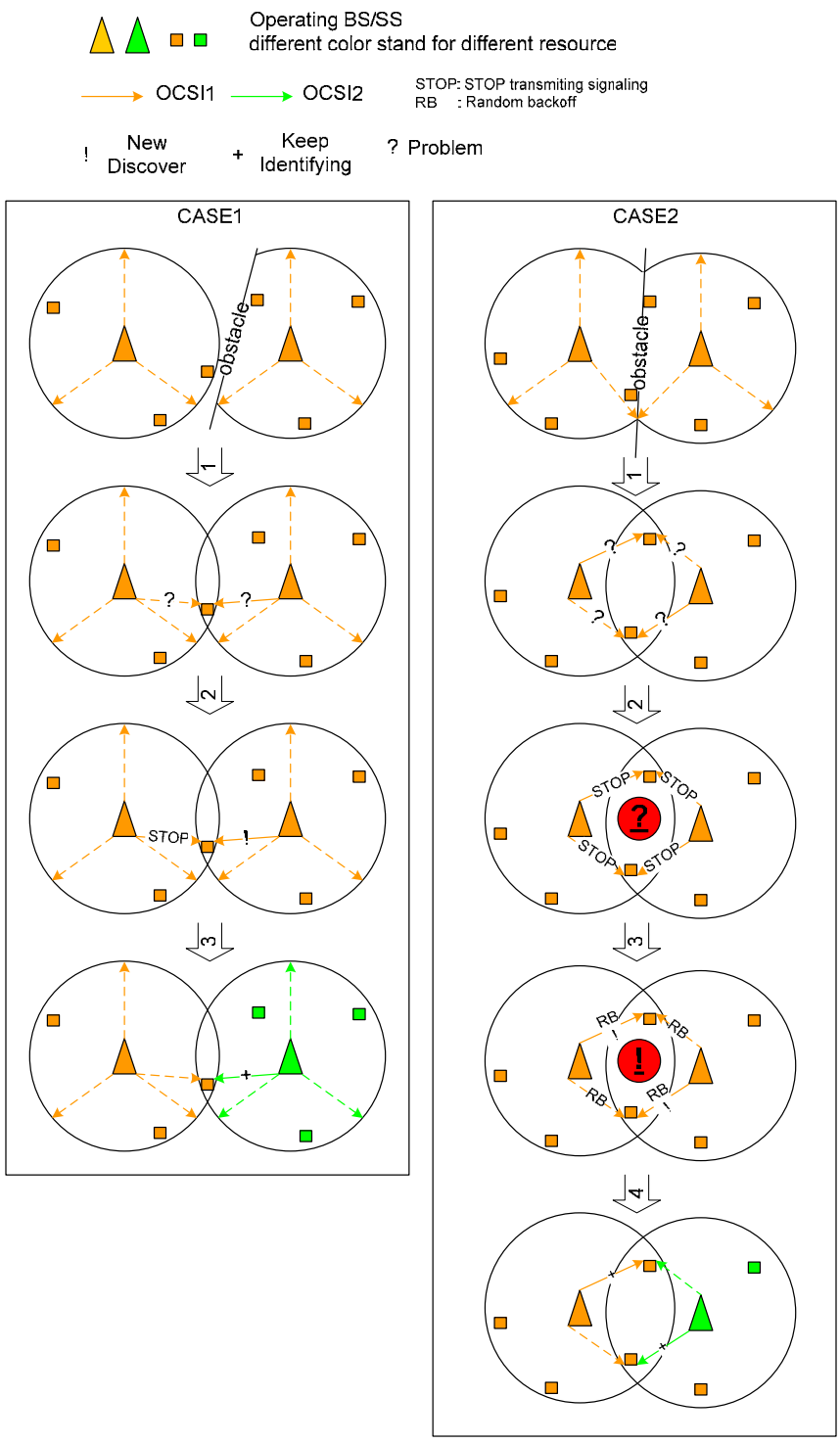
2) Else if this SS keep receiving harmful interference within this OCSI but can not identify the information inside, the system should consider to reallocated its resource else where.

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:

6.3.2.3.71 CSI monitoring request message (CSI_MNTR_REQ)

This message is broadcast from the operating BS to the SS within the system. The WirelessMAN-CX BS uses this message to request the SS to monitor on specific OCSI allocation, and configure the SS monitoring mode. (See 15.3.1.4) The timing for CSI is notified to SS by DCD.

Table hxx—OCSI_MNTR_REQ format

Syntax	Size	Notes
CSI_MNTR_REQ message format () {		
Management Message Type = 76	8 bits	
CSI_MNTR_ REQ TLVs	*variable*	
}		

6.3.2.3.72 CSI monitoring response message (OCSI_MNTR_RSP)

This message is the report message from the SS to the BS in response of the CSI monitoring require message, when the SS have detected the [harmful] interference or have received the information from a neighboring system. (See 15.3.1.4)

Table hxx—OCSI_MNTR_RSP format

Syntax	Size	Notes
CSI_MNTR_RSP message format () {		
Management Message Type = 77	8 bits	
CSI_MNTR_ RSP TLVs	*variable*	
}		

10.5.4 CSI timing parameters

System	Name	Time reference	Minimum Value	Default Value	Maximum Value
BS/SS	TCG	Transmition/CSI transition gap (15.1.4.1.1)	1PS/ 1 OFDM/OFDMA symbol		
BS/SS	CTG	CSI/receive transition gap (15.1.4.1.1)	1PS/ 1 OFDM/OFDMA symbol		
BS/SS	Tcsi_start	Starting point of the CSI in each frame (15.1.4.1.1)			
BS/SS	CSI duration	Time duration of each CSI interval (15.1.4.1.1)			50% DL duration
BS/SS	CSI cycle	CSI cycle in unit of frames (power of 2)		4	

		(15.3.1.1)			
BS/SS	Offset Frames	the frame number offset of CSI allocation		0	CSI cycle -1
BS/SS	ICSI cycle	ICSI cycle in unit of CSI cycle (power of 2) (15.3.1.1.1)		4	
BS/SS	OCSI cycle	OCSI cycle in unit of ICSI cycle (power of 2) (15.3.1.1.1)		4	
BS/SS	CSI Symbol Duration	The duration for each CSI symbol (15.3.1.1.3)	25us		1ms
BS	OCSI Backoff Start	Initial backoff window size for OCSI contention, expressed as a power of 2. (15.3.1.4)	1	2	6
BS	OCSI Backoff End	Final backoff window size for OCSI contention, expressed as a power of 2. (15.3.1.4)	2	4	6
BS	OCSI Backoff counter start	The initial value of the decreasing counter on the backoff window size change	1	3	10

11.21 CSI_MNTR_ REQ message encodings

CSI_MNTR_ REQ message encodings as below:

Name	Type	Length	Value
CSI_MNTR_ REQ	1	variable	compound
CSI_MNTR_ REQ Type	1.1	1	Bit#0: 0- no monitor on the ICSI 1- monitor on the ICSI, SS report on new discovered harmful interference/signaling in ICSI Bit#1: 0- stop monitoring on the specific OCSI allocation 1- to monitor the specific OCSI allocation Bit#2: (only useful when bit1=1) 0- collusion detect mode 1- collusion backoff mode Bit#3: 1-include information received in BS_NURBC Bit#4: 1-include RSSI of CSI symbols (only valid when bit#3 is set to one) Bit#5: 1-include frame number that start to receive BS_NURBC Bit#6-7: reserved
OCSN	1.2	1	The OCSI which configuration is to be modified
Known occupying BSID	1.3	6	Bits 47:0 - BSID

11.22 CSI_MNTR_ RSP message encodings

CSI_MNTR_ RSP message encodings as below:

CSI_MNTR_ REQ Type	Name	Type	Length	Value
Bit#0 =1	ICSI_MNTR_ RSP	1	variable	compound
Bit#1 =1 Bit#2 =0	OCSI_CD_RSP	2	variable	compound
Bit#1 =1 Bit#2 =1	OCSI_INFO_RSP	3	variable	compound

CSI_MNTR _ REQ Type	Name	Type	Length	Value

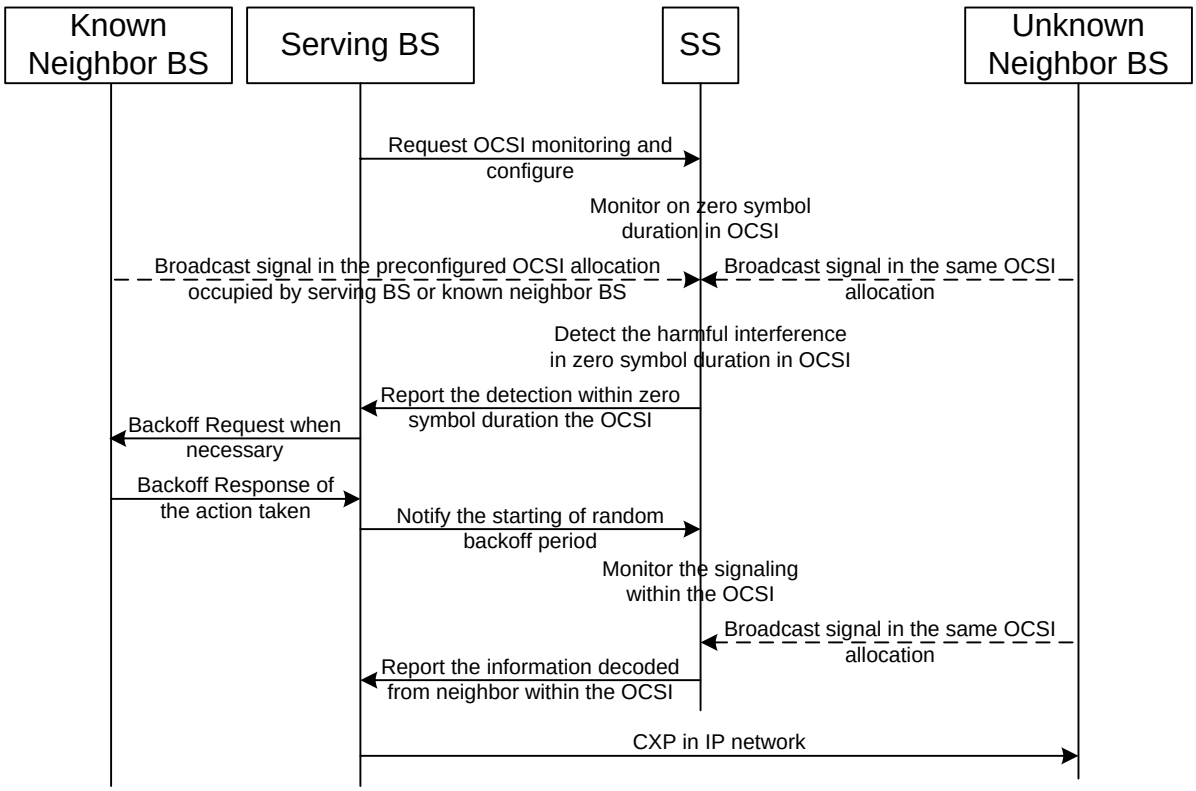
bit#3-5				
All	Report result	1.1	1	Bit0: 0-Fail 1-success in receiving and checking Bit1-7: reserved error code
Bit#3=1	Neighborhood update request report IPv4	1.2	12	Bits 15:0 - RTK Bits 63:16 - BSID Bits 95:64 - BS IP address(IPv4) 4bytes IPv4 address of CoNBR interference to this SS, 255. 255. 255. 255 indicate the fail of CRC check.
Bit #3=1	Neighborhood update request report IPv6	1.3	24	Bits 15:0-RTK Bits 63:16-BSID Bits 191:64-BS IP address(IPv4) 16bytes IPv6 address of CoNBR interference to this SS, all ones indicate the fail of CRC check.
Bit #4=1	BS_NURBC RSSI	1.4	2	1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11) for details) 1byte standard deviation
Bit #5=1	Starting Frame Serial Number of BS_NURBC	1.5	3	Bit# 0-24: frame number of BS_NURBC starting frame
Bit #3=1	CRC error indication			

CSI_MNTR _ REQ Type bit#3-5	Name	Type	Length	Value
all	Report result	2.1	1	Bit0: 0- interference detected again in OCSI 1- interference detected in new OCSI allocation Bit1:3 reserved Bit 4-7: OCSN
Bit #4=1	Detected [I+N]to[N] ratio	2.2	1	In unit of 0.5 dB
Bit #5=1	Frame Number of interference occur	2.3	2	Bit# 0-15: Frame Number of interference detection in OCSI

CSI_MNTR _ REQ Type bit#3-5	Name	Type	Length	Value
all	Report result	3.1	1	Bit0: 0-Fail 1-success in receiving and checking Bit1:3 reserved error code Bit 4-7: OCSN
Bit#3=1	Neighborhood update request report IPv4	3.2	12	Bits 15:0 - RTK Bits 63:16 - BSID Bits 95:64 - BS IP address(IPv4) 4bytes IPv4 address of CoNBR interference to this SS, 255. 255. 255. 255 indicate the fail of CRC check.
Bit #3=1	Neighborhood update request report IPv6	3.3	24	Bits 15:0-RTK Bits 63:16-BSID Bits 191:64-BS IP address(IPv4) 16bytes IPv6 address of CoNBR interference to this SS, all ones indicate the fail of CRC check.
Bit #4=1	BS_NURBC RSSI	3.4	2	1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11) for details) 1byte standard deviation
Bit #5=1	Starting Frame Serial Number of BS_NURBC	3.5	3	Bit# 0-24: frame number of BS_NURBC starting frame

Insert a new section 15.3.1.4 as follow:

15.3.1.4 OCSI Collusion detection and resolution in operation phase



The monitoring on ICSI is for SS to discover the initializing BS by decoding the signaling within ICSI broadcast from the initializing neighbor BS. (See 15.3.1.3) By recognizing the OCSI allocation map (See 15.3.1.1.1), the BS can set on each OCSI allocation to be monitored or not, using ***CSI monitoring request*** message (See 6.3.2.3.71).

While one OCSI allocation is monitored, the monitoring has two modes based on the status of the OCSI collusion detection, collusion detection mode and backoff mode:

In OCSI collusion detection mode, the SS keep monitoring the interference level on the zero symbol duration (see 15.3.1.1.3) which is supposed to have only noise without other neighbor's occupancy. When the SS discovers that the interference level there is above the interference criteria, it will report to its serving BS, using ***CSI monitoring response*** message (See 6.3.2.3.72). So that the serving BS or the known occupier can request OCSI monitoring into backoff mode. The BS broadcast the CSI_MNTR_REQ to the SSs containing the BSID of the known occupier, so that the SS can easily find the zero symbol duration according to the predefined the signaling message structure (see 15.3.1.1.2, 15.5.6.2.1).

In OCSI collusion backoff mode, original occupying BS will broadcast the signaling message in the backoff window only one time, so that most of time the OCSI will not be occupied by the original occupier. Therefore, the SS is able to receive the signaling from its new neighbor system, and decodes the information other than the original OCSI payload. After that, new neighbor will be discovered and identified to be negotiated with.

When the collusion is solved or the backoff timer expired, the BS should reconfigure the CSI monitoring mode using ***CSI monitoring request*** message (See 6.3.2.3.71). The OCSI backoff resolution shall be based on a truncated binary exponential backoff, with the initial backoff window and the maximum backoff window selected by the BS. The known occupier BS shall internally count backoff window timer only and requests the SS to switch monitoring mode accordingly. In case the known occupier BS of the OCSN is a known neighbor BS, the serving BS shall contact that neighbor BS using CXP message (see **15.5.2.59)** to request its backoff in broadcasting, and the known neighbor BS shall response according to its action using CXP as well (see **15.5.2.60)**.

The backoff window was initialized as a selected power-of-two value (See 10.5.4), unit in the durations of broadcasting a whole signaling message. For example, if one signaling message takes 100 OCSI cycles, the value 2 stands for 4 times the duration which means 400 OCSI cycles. The BS will random choose a valid starting point (1-301st OCSI in the example) from the whole duration and broadcast one signaling message. Therefore at most time in the backoff window, no signal from its serving BS will disturb the signaling from its neighbor BS using the same OCSI allocation. The reason not to stop all the signaling broadcasting in the duration is, to avoid dead lock in case that 2 neighbor systems detect the collusion at the same time and both stop the signaling broadcasting, The backoff window will be increasingly updated for

predefined times. Within these updates, the backoff window will stop increasing if the upper limit (see 10.5.4) reaches.

15.5.2.59 OCSI backoff request message

A message sent by BS to its neighbor BS, when the sender BS is reported by its SS that collusion has been detected in the OCSI which is occupying by this neighbor. See 15.3.1.4
Code: 59
Parameters:

Table hxx— OCSI backoff request message attributes

Attribute Contents	Contents
Operator ID	The Operator identifier of requesting BS
BSID	The requesting BS identifier
Requested BSID	identifier of the requested BS
OCSN	OCSN of the occupying OCSI
Backoff request	1- start backoff request 0- end of backoff request

15.5.2.60 OCSI backoff response message

A message sent by BS to its neighbor BS, in response according to its action. See 15.3.1.4
Code: 60
Parameters:

Table hxx— OCSI backoff response message attributes

Attribute Contents	Contents
Operator ID	The Operator identifier of requesting BS
BSID	The requesting BS identifier
Requested BSID	identifier of the requested BS
OCSN	OCSN of the occupying OCSI
Response indication	01- refuse to backoff 00- refuse to end the backoff 11- notification of acceptance and backoff begin 10- notification of acceptance and backoff end because of timer and counter having run out