2006-01-24 **IEEE P802.16h™/~~D0~~, January 2006**

Draft IEEE Standard for
Local and metropolitan area networks

Part 16: Air Interface for Fixed Broadband Wireless Access Systems

Amendment for Improved Coexistence Mechanisms for License-Exempt Operation

~~Sponsor~~
~~**LAN MAN Standards Committee**~~
~~of the~~
~~**IEEE Computer Society**~~
~~and the~~
~~**IEEE Microwave Theory and Techniques Socie**~~‘··

Abstract:*Should be based on the scope and purpose of the standard as indicated on the PAR.*

Keywords: *Should highlight key terms and phrases from the abstract or text of the draft standard.*

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Print: ISBN 0-7381-xxxx-x SHxxxxx
PDF: ISBN 0-7381-xxxx-x SSxxxxx

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage,of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

This introduction is not part of IEEE P802.16h, Draft Amendment to IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment for Improved Coexistence Mechanisms for License-Exempt Operation.

Participants

This document was developed by the IEEE 802.16 Working Group on Broadband Wireless Access, which develops the WirelessMAN™ Standard for Wireless Metropolitan Area Networks.

IEEE 802.16 Working Group Officers
Roger B. Marks, *Chair*
Ken Stanwood, *Vice Chair*
Dean Chang, *Secretary*

Primary development was carried out by the Working Group's License-Exempt Task Group (TG le):

TG le Officers
Mariana Goldhamer, *Chair*
Barry Lewis, *Vice-chair*
Xuyong Wu, *Editor*
Paul Piggin, *Secretary*

The following members of the IEEE 802.16 Working Group on Broadband Wireless Access participated in the Working Group Letter Ballot in which the draft of this standard was prepared and finalized for IEEE Ballot:

[to be determined]

The following participated as non-members in the Working Group Letter Ballot:

[to be determined]

The following members of the IEEE Balloting Committee voted on this standard, whether voting for approval or disapproval, or abstaining.

[to be determined]

~~The following persons, who were not members of the IEEE Balloting Committee, participated (without voting) in the IEEE Sponsor Ballot in which the draft of this standard was approved:~~

~~***[to be determined]***~~

~~When the IEEE-SA Standards Board approved this standard on [date], it had the following membership:~~

~~***[to be determined]***~~

Contents

List of figures

List of Tables

Draft IEEE Standard for
Local and Metropolitan Area Networks

Part 16: Air Interface for Fixed Broadband Wireless Access Systems

Amendment for Improved Coexistence Mechanisms for License-Exempt Operation

NOTE-The editing instructions contained in this amendment/corrigendum define how to merge the material contained herein into the existing base standard IEEE Std 802.16-2004.

The editing instructions are shown ***bold italic***. Four editing instructions are used: ***change, delete, insert,*** and ***replace***. ***Change*** is used to make small corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using strike through (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make large changes in existing text, subclauses, tables, or figures by removing existing material and replacing it with new material. Editorial notes will not be carried over into future editions because the changes will be incorporated into the base standard.

1. Overview

scope: This amendment specifies improved mechanisms, as policies and medium access control enhancements, to enable coexistence among license-exempt systems based on IEEE Standard 802.16 and to facilitate the coexistence of such systems with primary users.

applicability: This amendment is applicable for un-coordinated frequency operation in all bands in which 802.16-2004 is applicable, including bands allowing shared services.

[insert a new subclause 1.5]

1.5 Co-existence for license-exempt and uncoordinated systems

Section 1.3.3 acknowledges that the equipment conformant to this standard may be used in license-exempt and uncoordinated bands. The WirelessHUMAN PHY (section 8.5) addresses the additional needs of systems operating in license-exempt bands; and section 6.3.15 provides suggested procedures and MAC support for addressing the needs of 'specific spectrum users'; users who are deemed to be protected from

interference by regulation. Further enhancements to facilitate co-existence for license-exempt and uncoordinated systems in utilizing improved co-existence mechanisms is embodied in policies, MAC enhancements, and recommended practice introduced in this section. This operation is designated WirelessMAN-CX. This designation, being PHY independent, provides specific features in additional to those supported for WirelessHUMAN and builds on new features and evolves those originally designed for licensed band operation.

License-exempt or uncoordinated bands may adopt RF profiling in terms of selecting a known set of RF parameters, such as a band plan. If such a convention is adopted the design, management and inter-working of uncoordinated systems is eased significantly. If no baseline assumptions about other systems sharing the band can be made then complexity is added to both system design and algorithms implemented. In adding license-exempt or uncoordinated operation to the WirelessMAN standard it is assumed that an amendment can draw heavily from the material embodied in the original air interface standard and provide a solution to a problem that is not significantly more complex than the base standard. To this end therefore assumptions about RF parameters, for example channel raster and channel bandwidths, are appropriate to the solution based on WirelessMAN. WirelessMAN-CX therefore provides enhancements to the MAC protocol to facilitate communication between infrastructure and subscriber devices for interference measurement, reporting and management; together with negotiation for spectrum sharing.

[Insert the following row into table-1:]

Designation	Applicability	PHY	Additional MAC requirements	Options	Duplexing alternative
WirelessMAN-CX	Below 11 GHz license-exempt and/or uncoordinated bands	Section 8	MAC enhancements for coexistence (6.4)	Those applicable to PHY implemented. Section 15.	TDD

2. References

3. Definitions

[Insert following sections after 3.85:]

3.86 WirelessMAN-CX: The designation used to describe the realization that adds co-existence procedures and recommended practice to systems implemented below 11GHz in license-exempt or uncoordinated bands. This designation is PHY independent and adds additional MAC functionality.

4. Abbreviations and acronyms

[Insert the following abbreviations at appropriate location:]

AH	Authentication Header
BSIS	Base Station Identification Server
CNTI	Cognitive Network Time Interval
CoNBR	Coexistence Neighbor
CR	Cognitive Radio
CR_NOC	Cognitive Radio Network Operations Centre.
CTS	Coexistence Time Slot
CX	Co-eXistence
DRRM	Distributed Radio Resource Management
DSM	Distribution System Medium
ESP	IP Encapsulating Security Payload
IANA	Internet Assigned Numbers Authority
IBS	Initializing Base Station
IETF	Internet Engineering Task Force
IPBC	IP address Broadcast
IPsec	Internet Protocol Security
NOC	Network operation center
OBS	Operating Base Station
PKM	Private Key Management
PLE	Path Loss Exponent
PSD	power spectrum density
RADIUS	Remote Authentication Dial-in User Service
SAP	Service Access Point
SSURF	Subscriber Station Uplink Radio Frequency
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTC	Universal Coordinated Time
WirelessMAN-CX	Wireless Metropolitan Access Network Co-eXistence

Notes: the IP broadcasting in the airlink is to be reconsidered and call for contribution for modification.

5. Service-specific CS

6. MAC common part sublayer

6.3 Data/Control plane

6.3.2 MAC PDU Format

6.3.2.3 MAC management messages

6.3.2.3.33 Channel measurement Report Request/Response (REP-REQ/RSP)

[change the section into the following text in 802.16 primary standard:]

If the BS, operating in bands below 11 GHz, requires RSSI and CINR channel measurement reports, or requires neighbor detection reports, it shall send the channel measurements Report Request message. The Report Request message shall additionally be used to request the results of the measurements the BS has previously scheduled. Table 62 shows the REP-REQ message.

The channel measurement Report Response message shall be used by the SS to respond to the channel measurements listed in the received Report Requests. Where regulation mandates detection of specific signals by the SS, the SS shall also send a REP-RSP in an unsolicited fashion upon detecting such signals on the channel it is operating in, if mandated by regulatory requirements. The SS may also send a REP-RSP containing channel measurement reports, in an unsolicited fashion, or when other interference is detected above a threshold value. In cases where specific signal detection by an SS is not mandated by regulation, the SS may indicate 'Unmeasured. Channel not measured.' (see 11.12) in the REP-RSP message when responding to the REP-REQ message from the BS. Especially for coexistence network, when SS have detected the IP broadcasting message from the coexistence neighbor BS, the SS need to use REP_RSP to report the information to its serving BS unsolicitedly. Table 63 shows the REP-RSP message.

[Insert a new section 6.4 :]

6.4 MAC enhancement for coexistence

This section describes MAC enhancements for WirelessMAN-CX in support of license-exempt and uncoordinated bands. Firstly concepts are described which are general to the MAC, after which PHY specific interactions are considered. PHY specific discussion is required since WirelessMAN-CX operation is dependant on the features supported for a given PHY.

[tbc for deriving the appropriate part from clause15 here]

6.4.1 General concepts

This section describes WirelessMAN-CX operation. These aspects are specific to the MAC and support of the PHY from the MAC..

6.4.1.1 Capability Negotiation

A mechanism is provided by which WirelessMAN-CX and non-WirelessMAN-CX devices are to interwork. This is an important mechanism for deployment scenarios where regulatory designation of WirelessMAN-CX operation is required. Some examples of how the capability negotiation can be used are given:

- A device with WirelessMAN-CX functionality will need to interact with infrastructure that knows nothing of WirelessMAN-CX.
- A non-WirelessMAN-CX device will need to interact with WirelessMAN-CX compliant infrastructure.
- A non-WirelessMAX-CX device shall have the ability to be barred from working in a WirelessMAX-CX network – this is deployment specific.
- A WirelessMAX-CX device shall work in a non- WirelessMAX-CX network as ‘normal’ non-WirelessMAX-CX device.

6.4.1.2 Extended channel numbering structure

License-exempt or uncoordinated bands may require or provide scope for the use of a defined channel raster or channel bandwidth. This section provides a means to achieve this, and therefore offer simplification to issues of interference managements. Extended channel numbering provide an enhancement to channelization and definition of channel number for WirelessHUMAN operation in section 8.5.1. This extension provides channelization references beyond the limits of 5-6GHz as defined. The channelization is defined accordingly.

- Extended Channel Number (ExChNr) – 1 byte specific channel number reference.
- Base Channel Reference (BaseChRef) – 1 byte base reference to frequency range or deployment band. This reference maps to an absolute frequency value
- Channel spacing (ChSp) - 2 byte channel spacing value (10kHz increments)

In summary the definition of the *Channel Centre Frequency* is:

*Channel Centre Frequency [MHz] = BaseFrequency(BaseChRef)[MHz] + (ExChNr*ChSp *0.01)[MHz] [xxx]*

This is shown in a graphical representation in Figure h 1.

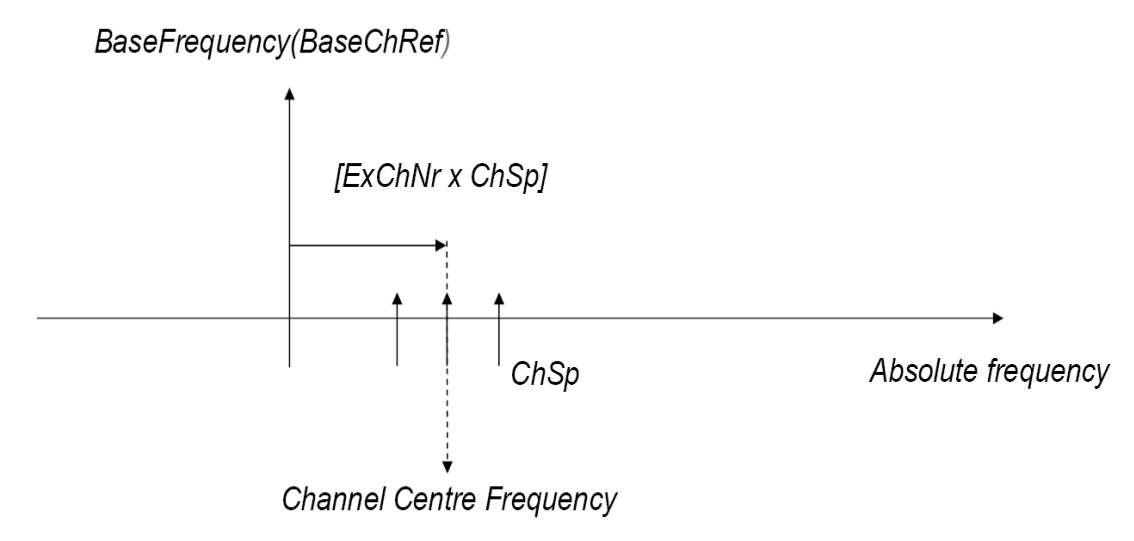

Figure h1—Representation of 'Channel Centre Frequency' calculation.

ExChNr is used in *REP-REQ/REP-RSP* messages while *BaseChRef*, and *ChSp* are communicated at a session setup or reconfiguration.

6.4.1.3 Measurement and Reporting

License-exempt or uncoordinated bands are likely to present an operating environment that has a significantly higher and more dynamic interference profile than licensed bands. Measurement and reporting of the prevailing environment is therefore an important consideration for system operation and stability. Measurement and reporting enhancements provide the ability to:

- Enhance details on environmental knowledge for license-exempt and uncoordinated band operation.
- Provide timely reports for fast link adaptation in an attempt to maintain BER performance.
- Provide bandwidth efficient reports maintain spectral efficiency but also to ensure interference reports are not out-of-date.
- Provide accurate measurements to retain WirelessMAN-CX integrity.

6.4.2 WirelessMAN-CX support for OFDMA PHY

This section provides a description of WirelessMAN-CX support for the WirelessMAN-OFDMA PHY.

6.4.2.1 Co-existence zone (CXZ) for downlink and uplink

The addition of a CXZ provides the means to include all co-existence enhancements in a defined region within the WirelessMAN-OFDMA PHY. It is expected that all co-existence operation will occur within this zone.

6.4.2.2 Measurement and Reporting

In order to meet strict requirement on measurement and reporting in license-exempt and uncoordinated bands enhanced reporting for WirelessMAN-CX is supported through the REP-REQ/REP-RSP MAC messages (see sections 11.11 and 11.12 respectively). Also the use of the WirelessMAN-OFDMA fast feedback channel is used to enhance reporting capabilities. Section 6.3.18.2 discusses periodic CINR report with fast-feedback (CQICH) channel. It is recommended that interference measurements are undertaken on the effective (feedback type=0b01) or physical (feedback type=0b00) CINR measurement for a CXZ permutation zone (Zone permutation=0b110 and report type=1) from pilot subcarriers (measurement type=0). Section 8.4.5.4.12 gives specific details of the CQICH allocation IE.

7. Privacy sublayer

8. PHY

8.4 WirelessMAN-OFDMA PHY

8.4.4 Frame structure

8.4.4.2 PMP frame structure

[change the last paragraph of section 8.4.4.2 into the following text in 802.16 primary standard:]

The OFDMA frame may include multiple zones (such as PUSC, FUSC, PUSC with all subchannels, optional FUSC, and AMC, CXZ, TUSC1, and TUSC2), the transition between zones is indicated in the DL-Map by the STC_DL_Zone IE (see 8.4.5.3.4), CXZ_DL_IE (see 8.4.5.3.11), or AAS_DL_IE (see 8.4.5.3.3). No DL-MAP or UL-MAP allocations can span over multiple zones. Figure 219 depicts the OFDMA frame with multiple zones.

[change figure 219 as following:]

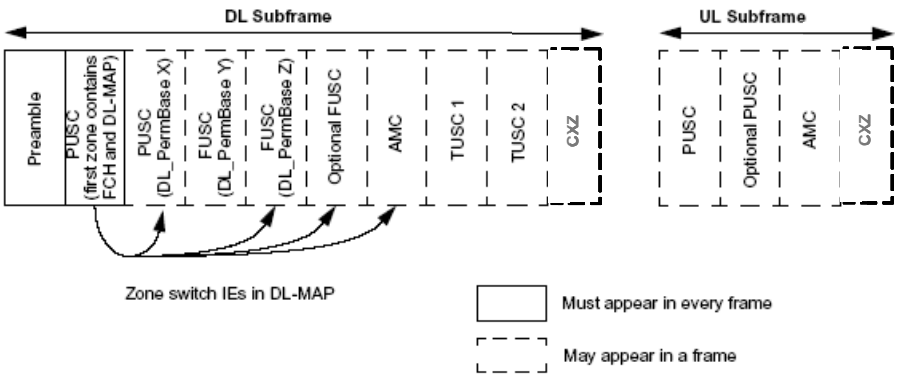

Figure 219—Illustration of OFDMA frame with multiple zones

[insert the following rows to table 277a, section 8.4.5.3.2.1.]

Extended DIUC (hexadecimal)	Usage
09	CXZ_DL_IE
~~09-~~0A	*reserved*

[Insert a new section 8.4.5.3.28:]

8.4.5.3.28 Co-existence zone (CXZ) downlink IE format

Within a frame, the switch to co-existence operation is marked by using the extended DIUC = 15 with the CXZ_DL_IE(). The CXZ_DL_IE defines a DL CX zone that spans continuous OFDMA symbols until terminated by another CXZ_DL_IE or the end of the DL frame. Multiple CXZ zones can exist within the same frame. When used, the CID in the DL_MAP_IE() shall be set to the broadcast CID.

Table 286aa—CXZ downlink IE

Syntax	Size	Notes
CXZ_DL_IE() {		
Extended DIUC	4 bits	CXZ = 0x09
Length	4 bits	Length = 0x01
OFDMA symbol offset	8 bits	Denotes the start of the zone (counting from the frame preamble and starting from 0).
}		

[insert following row into table-289a as indicate(section 8.4.5.4.4.1):]

Extended UIUC (hexadecimal)	Usage
0B	CXZ_UL_IE
~~0B~~0C … 0F	*reserved*

[change the row in table 300 as indicate (section 8.4.5.4.12)]

Syntax	Size	Notes
Zone permutation	3 bits	The type of zone for which to report 0b000 - PUSC with 'use all SC = 0' 0b001 - PUSC with 'use all SC = 1' 0b010 - FUSC 0b011 - Optional FUSC 0b100 - Safety Channel region 0b101 - AMC zone (only applicable to AAS mode) 0b110 - CXZ 0b~~110~~111 - Reserved

[Insert a new section 8.4.5.4.29]

8.4.5.4.29 Co-existence zone (CXZ) uplink IE format

Within a frame, the switch to co-existence operation is marked by using the extended UIUC = 15 with the CXZ_UL_IE(). The CXZ_UL_IE defines a DL CX zone that spans continuous OFDMA symbols until terminated by another CXZ_UL_IE or the end of the DL frame. Multiple CXZ zones can exist within the same frame. When used, the CID in the DL_MAP_IE() shall be set to the broadcast CID.

Table 302w—CXZ uplink IE

Syntax	Size	Notes
CXZ_UL_IE() {		
Extended DIUC	4 bits	CXZ = 0x09

Length	4 bits	Length = 0x01
CXZ zone length offset	8 bits	The length of the uplink CXZ zone.
}		

9. Configuration

10. Parameters and constants

11. TLV encodings

11.7 REG-REQ/RSP management message encodings

[Insert the following row into table 369a:]

Type	Parameter
45	WirelessMAX-CX capability
46	Base Channel Reference (BaseChRef)
47	Channel Spacing (ChSp)

11.7.8 SS capability encodings

[insert new subclause 11.7.8.14:]

11.7.8.14 WirelessMAX-CX capability

Name	Type (1 byte)	Length (1 byte)	Value	Scope
WirelessMAX-CX capability	45	1	Bit #0: No WirelessMAX-CX capability Bit #1: WirelessMAX-CX capability Bits #2 - #7: Reserved	REG-REQ
Base Channel Reference (BaseChRef)	46	1	Base Channel Reference in MHz providing base reference to frequency range or deployment band	REG-RSP
Channel Spacing (ChSp)	47	2	Channel Spacing in 10kHz increments.	REG-RSP

11.11 REP-REQ management message encodings

[insert the following entry in the second table of 11.11:]

Coexistence neighbor Interference Report	1.9	1	Bit #0: 1-include IP address received in IPBC Bit #1: 1-include RSSI of CTS symbols(only valid when bit#0 is set to one) Bit #2: 1-include frame number that start to receive IPBC Bit #3~7: reserved, shall be set to zero
ExChNr	1.10	2	Physical extended channel number (WirelessMAX-CX only)
Extended report type	1.11	1	Bit #0 = 1: Include extended report type A Bit #1 = 1: Include extended report type B Bits #2 - #7: Reserved

11.12 REP-REQ management message encodings

[insert the following entry in the first table of 11.12:]

Coexistence neighbor Report	7	variable	Compound
Extended report type	8	variable	Compound

[insert the following table into 11.12 as indicates:]

Coexistence neighbor Interference Report type	**Name**	**Type**	**Length**	**Value**
all	CoNBR count / New NDS	7.1	1	Bit #0:1-New CoNBR Discovered by IPBC received Bit #1-7:The number of CoNBR that interference to this SS
bit #0=1	CoNBR IP address	7.2	4	4bytes IP address of CoNBR interference to this SS, 255. 255. 255. 255 indicate the fail of CRC check.
bit #1=1	CoNBR IP address with RSSI	7.3	2	1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11) for details) 1byte standard deviation
Bit #2=1	Starting Frame Serial Number of IPBC	7.4	3	Bit# 0-24: frame number of IPBC starting frame

REP-REQ Extended report type	**Name**	**Type**	**Length**	**Value**
Bit #0 = 1 OR Bit #1 = 1	ExChNr	8.1	2	Extended physical channel number to be reported on.

Bit #0 = 1 OR Bit #1 = 1	WirelessMAX-CX interference indicator	8.2	1	Bit #0: Low interference indication Bit #1: Medium interference indication Bit #2: High interference indication Bit #3: Primary user detected on the channel Bit #4: Channel not measured.
Bit #1 = 1	Zone specific CINR report	8.3	2	1 byte: mean 1 byte: standard deviation
Bit #1 = 1	Zone specific RSSI report	8.4	2	1 byte: mean 1 byte: standard deviation

12. System profiles

13. 802.16 MIB structure for SNMP

14. Management Interfaces and Procedures

[insert new clause 15:]

15. Mechanism for improved coexistence

[Editor's notes: the figure number and table number is temporarily marked as Figure hxxx. And Table hxxx, these number should be corrected according to WG rules before the draft release]

15.1 General

15.2 Interference detection and prevention – general architecture

15.2.1 Operational Principles and Policies

15.2.1.1 General Principles

The approaches for interference resolution is based on separating the interference in the frequency and time domains. ***[call for suitable text here:]***

[call for high level description here of basic principles:]A possibility of 802.16h usage is in close relation with a data-base, including both deployment information and an IP identifier for allowing the operation of a technology-independent coexistence approach. It is assumed that:

1) *In some circumstances*,there is country/region data base, which includes, for every Base Station:
    - Operator ID
    - Base Station ID

- o Base Station GPS coordinates
- o IP identifier

The local Radio Administration may use, for light licensing procedure, its own database, generally not including the Base Station ID and IP identifier information.

There is a server that manage the write/reading of this Data Base, using the 802.16h standardized procedures; the server and the country/region data base can be hostedby one of the operators or a trusted entity, like the local Radio Administration.

Otherwise, if the region/country database is not available, the base stations should try to find its neighbor and the community topology in a coordinatively distributed fashion.

2) Every Base Station includes a data base, open for other Base Station in the same community; the BS data-base contains information necessary for spectrum sharing, and includes the information related to the Base station itself and the associated SSs; a Base Station and the associated SSs form a system. Other Base Stations can send queries related to the information in the database to the DRRM entity, located in a Base Station (see Figure h 18).The base station shall represent its system in the cooperation with other systems when communicating over the backbone. It's possible to use the subscriber station to relay the control messages in some situations. The base station locations may be registered by GPS or other positioning systems, however there is no need to register the subscriber locations;

3) All the Base Stations forming a community will have synchronized MAC frames and frame number.

4) A community will be limited to a reasonable size; the size limitations and interactions between different coexistence neighborhoods: t.b.d.

5) All Base Stations and their networks will as a first step seek the avoidance of co-channel utilization of the same spectrum, and will be equipped with a spectrum detection and monitoring capability which will allow this.

6) All base stations are synchronized to a GPS clock. The start of all MAC frame and other transaction are referenced to the rising edge of this clock.

7) All base stations and their networks, operating in the LE bands, will provide the opportunity to other non-IEEE 802.16h systems to communicate their coexistence requests to the IEEE 802.16h networks.

8) The IEEE 802.16h systems will recognize the use of radar and other systems having higher priority to LE spectrum.

9) Every network will have a guaranteed minimum access time for the interference free use of the radio resource, being able to receive with minimum interference and to transmit at the needed powers for allowing communication between its Base Station and the remote subscribers

Interference Neighborhood: Interference neighborhood is relative to a system (BS and its subscribers). A system (BS and its SSs) will perceive as interference neighbors, all other systems (BSs and their SSs) which create/receive interference to/from it.

Community: is composed of those systems (BSs and their SSs) which coordinate to resolve their interference.

Coexistence Community: is composed of those systems (BSs and their SSs) which have resolved their interference and coexist.

The figures below explain possible ways of implementing the guaranteed radio resource principle, using a example of three overlapping radio networks.

The overlapping radio networks create different interference zones, based on spatial distance between transmitters and receivers. As example of BS to SS interference,, the radio receivers in Zone A, in the figure below, suffer from the interference (noted with) between Network 1 and Network 2. Interference Zone B includes also the Base Station of the Network B.

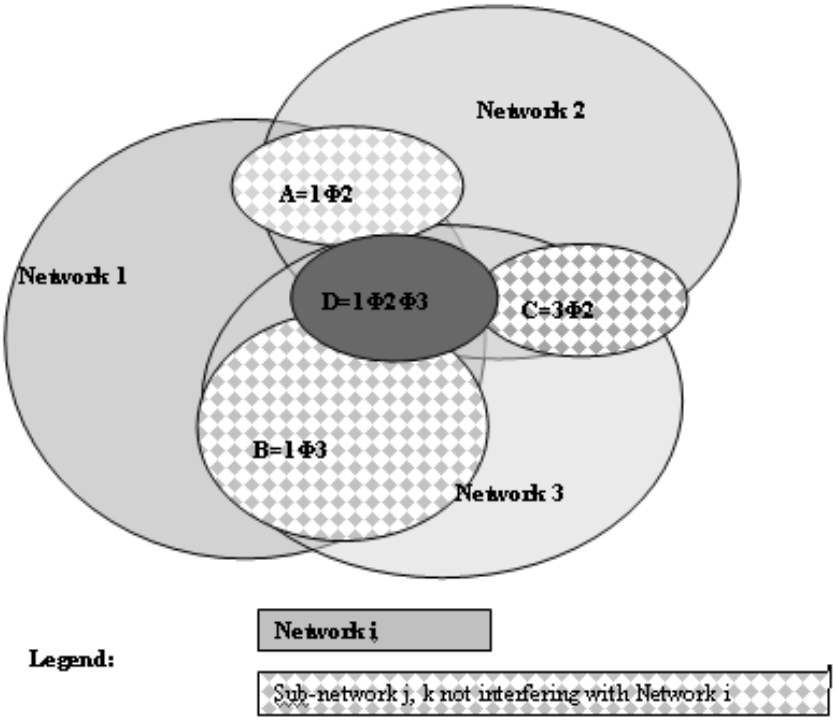

Figure h2—Interference due to overlapping networks

The operation of the 3 networks assume the following different situations:

Zones in which the networks 1,2,3 do not interfere;

- Zone A: Networks 1 and 2 interfere;
- Zone B: Networks 1 and 3 interfere;
- Zone C: Networks 3 and 2 interfere;
- Zone D: Networks 1 and 2 and 3 interfere.

Now lets suppose that we split a time frame in 3 sub-frames (being 3 different networks), and every network will receive an interference free interval for operation.

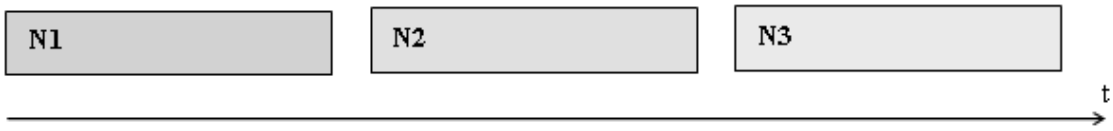

Figure h3—Equal splitting of radio resource between networks

Another possible approach will be to set an operating time for not interfering (noted Ø) situations, and split equally between the 3 networks the remaining resource, like shown below. It can be seen that non-interfering traffic may be scheduled in parallel, resulting a much better radio resource usage.

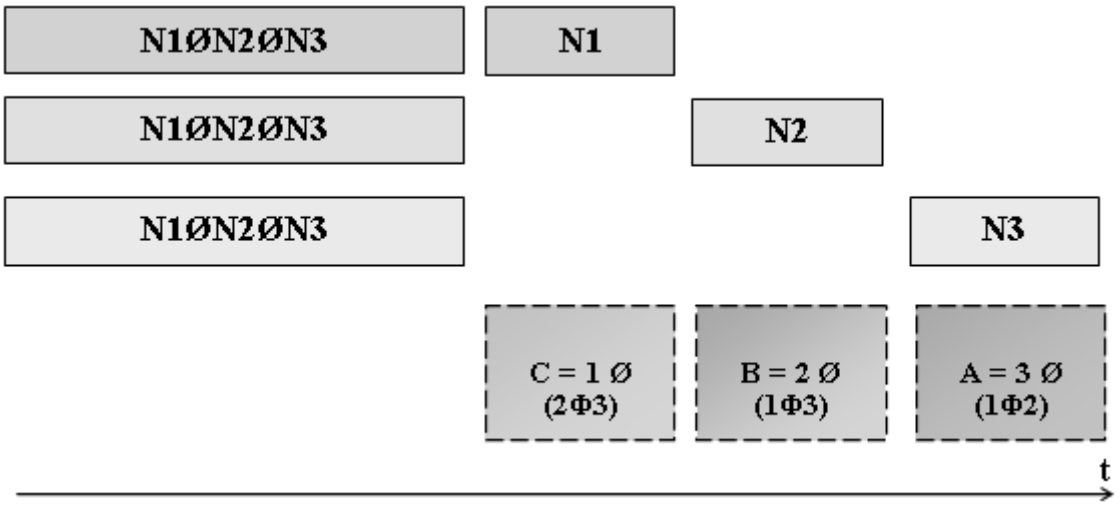

Figure h4—Usage of the spectrum by every system

Taking as example Network 1, it can be seen that this network operates in all the sub-frames, achieving in the same time interference-free operation and good spectral efficiency.

However, the networks working in the same time with the network having the control of the radio resource, shall use power control, sectorization or beam-forming in order to not create interference to that network.

15.2.1.1.1 Cooperation with other networks

A network may need more time resource for its BS communication with the SSs, than available for its operation in the assigned interference-free time interval. In this case, the specific network may request from one or more adjacent networks to reduce their interference free transmission intervals. The other networks will consider the request, and when possible will accept the request, by indicating the agreed new interference-free operating interval. The duration of each sub-frame may be negotiated through inter-network communication and using the common DRRM policy.

15.2.1.1.2 Scheduling of interference free intervals in the context of IEEE 802.16 MAC

A number of repetitive scheduling approaches are presented below, for Tx synchronized intervals. Same approach is valid for Rx intervals.

— *Type 1*: The MAC frame, for each Tx and Rx part, is split in N+1 sub-frames:

  - o One for non-interfering traffic
  - o Every other one to be used by a single BS or more non-interfering BSs which are assuming the Master role

— *Type 2*: The MAC frame, for each Tx and Rx part, is split in N sub-frames, every one to be used by a single BS or more non-interfering BSs which are assuming the Master role during a sub-frame

— *Type 3*: The MAC frame is split in two sub-frames: one for non-interfering traffic and one in which a single BS or more non-interfering BSs are assuming the Master role; each Base Station will assume the Master role after M frames

The duration of each sub-frame, in a given community, is calculated as follows:

for type 1:

— $T_{Tx\_sub\text{-}frame} = T_{TxMAC\ /\ (N+1)}$

— $T_{Tx\_sub\text{-}frame} = (T_{TxMAC} - T_{Txsh}) / N$

— $T_{Rx\_sub\text{-}frame} = T_{RxMAC} / (N+1)$

— $T_{Rx\_sub\text{-}frame} = (T_{RxMAC} - T_{Rxsh}) / N$

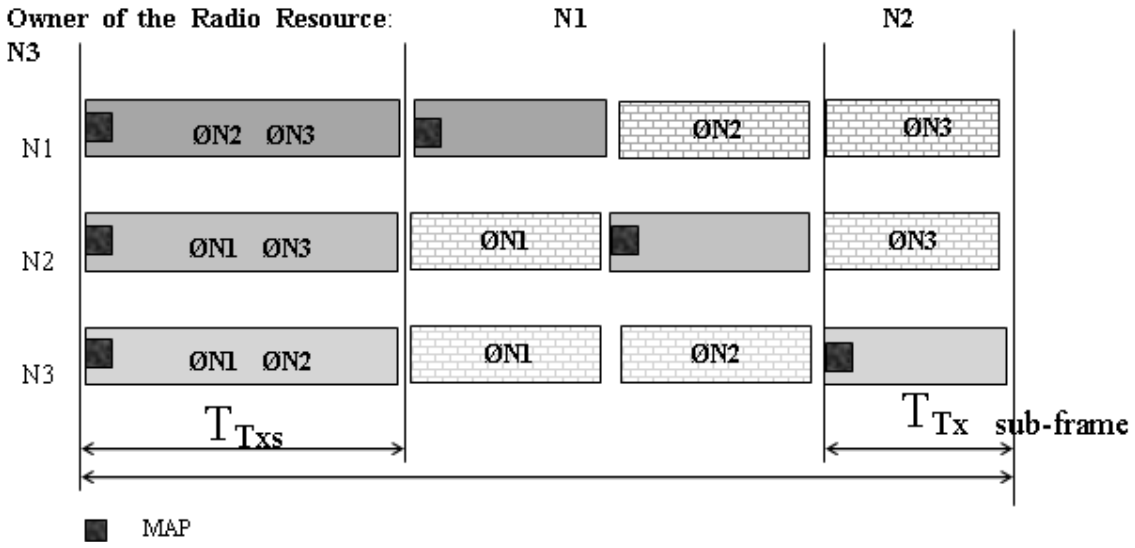

Figure h5—Sub-frame structure type1

for type 2:

— $T_{Tx\_sub\text{-}frame} = T_{TxMAC\ /\ N}$

— $T_{Rx\_sub\text{-}frame} = T_{RxMAC\ /\ N}$

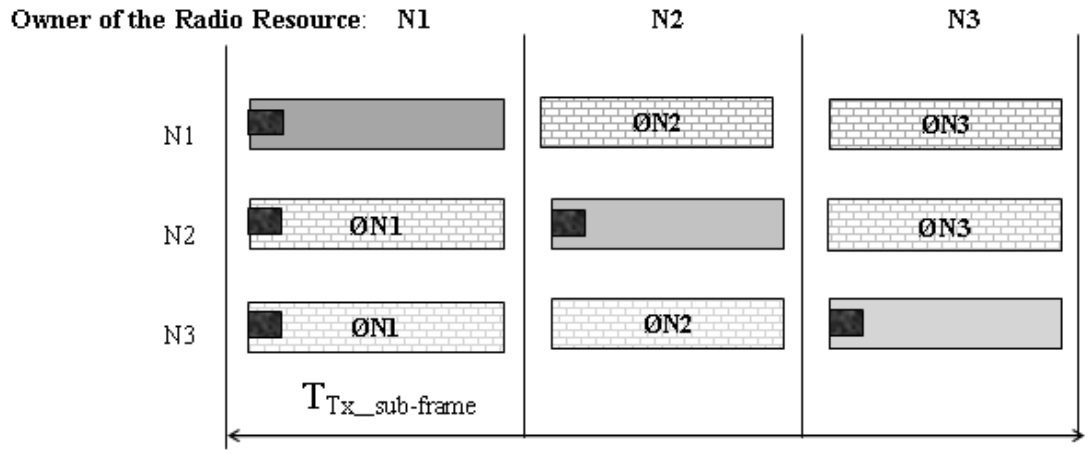

Figure h6—Sub-frame structure type 2

for type 3:

— $T_{Tx–sub\text{-}frame} = T_{TxMAC} / 2$

— $T_{Tx–sub\text{-}frame} = T_{TxMAC} - T_{Txsh}$

— $T_{Rx–sub\text{-}frame} = T_{RxMAC} / 2$

— $T_{Rx–sub\text{-}frame} = T_{RxMAC} - T_{Rxsh}$

repetition interval = $N*T_{MAC}$,

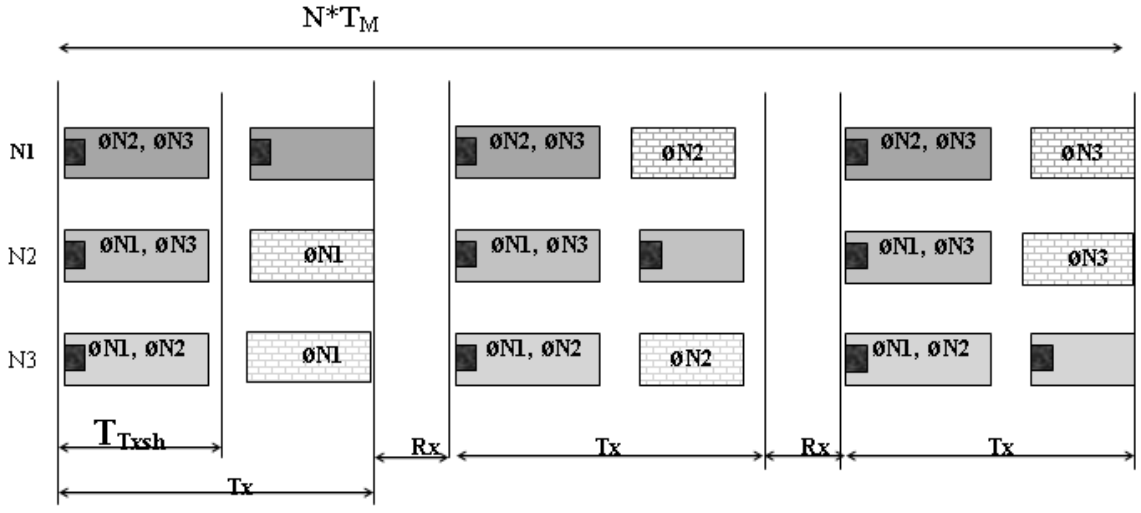

Figure h7—Sub-frame structure type 3

where T_{MAC}, T_{TxMAC}, T_{RxMAC}, T_{Txsh}, T_{Rxsh} are the durations of the respectively the MAC frame, Tx interval and Rx interval of the MAC frame or of the sub-frame used for shared used in the non-interfering sub-frame. In the above relations, the meaning of Tx or Rx is relative to the usage of the MAC Frame by a Base Station.

During the Master sub-frame the Base Stations assuming Master role may use their maximum power;

During every Master sub-frame, the Base Stations will create a slot, possibly not overlapping with another slot of a coexistence neighbor Base Station, during each every transmitter (BS or associated SS) will send a predefined signal; this signal, called “radio signature”, will be used to measure the interference created by that transmitter.

- The “radio signature slot” for a Base Station will be created during its Tx Master sub-frame, every B MAC-frames;
- The “radio signature slot” for a Subscriber Station will be created during the Rx Master sub-frame;
- UL MAP and suitable UIUC for scheduling the “radio signature” are t.b.d.
- During “radio signature” intervals, all the other BSs and SSs shall use a GAP interval;
- The Base Station shall take care to provide enough transmit opportunities for the active SSs.

The figure below shows the possible allocation of the “radio signature” transmission opportunity for a given system, using for example the Type 1 repetitive pattern, with a focus on Network 2.

The Network 2 will transmit its Base Station radio signatures from time to time (every N MAC intervals); different radio signatures will be sent for every used power/sub-channelization/OFDMA sub-channel/ spatial direction combination. During these intervals the other Base Stations will schedule a GAP interval, in order to identify solely one Base Station. Base Stations using the same MAC sub-frame as Master sub-frames shall schedule the transmission of their “radio-signatures” in such a way that will not interfere one with the other.

The transmission of “radio-signatures” used by the active SSs will take place during the Master sub-frame, from time to time (a timer shall be defined). The repetition period and the duration of the signature transmission shall be a parameter in the BS Data Base. The active SSs will provide a signature for every used power/ OFDMA/sub-channelization/ direction partition.

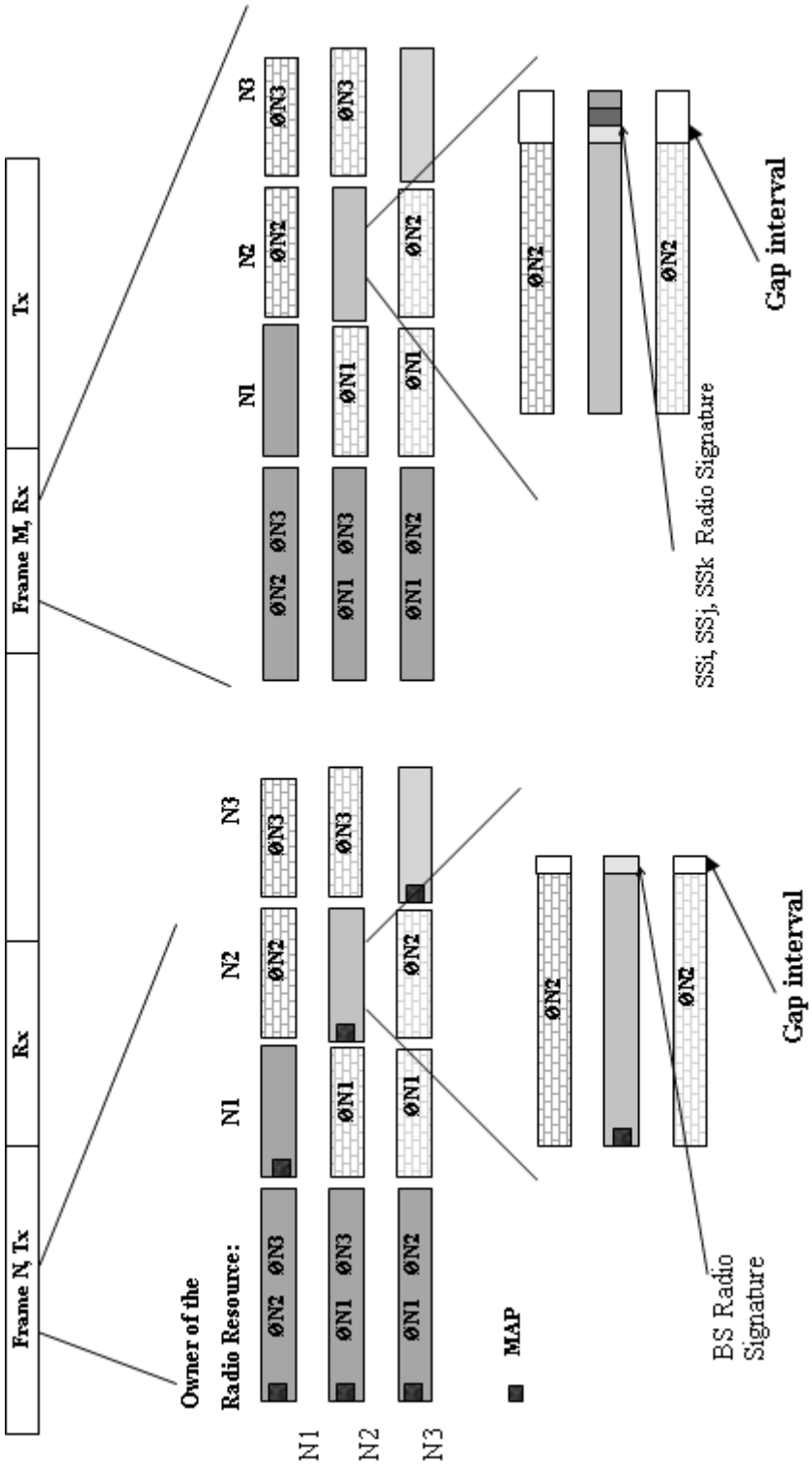

Figure h8—Allocation of slots for BS and SS radio signature

The BS data base will include:

- Operator ID
- Base Station ID
- MAC Frame duration (same for a community)
- Shared Tx and Rx sub-frame durations (same for a community)
- Type of sub-frame allocation (same for a community)
- MAC Frame number and sub-frame number chosen for the Master sub-frame (same for a community)
- Repetition period for Base Station radio-signature, measured in MAC-frames
- *Repetition interval between two Master sub-frames*, measured in MAC-frames
- *List of other used sub-frames*, in the interval between two Master sub-frames
- Time_shift from the Master sub-frame start, duration and the repetition information for the Base Station radio-signature transmission
- Time_shift from the Master sub-frame start, duration and the repetition information for the Subscriber Station radio-signature transmission
- *Time_shift from the Master sub-frame start and duration for network entry of a new Base Station*, which is evaluating the possibility of using the same Master slot.
- BS power relative to radio-signature, in the used sub-frames, in the interval between two Master subframes;
- For every active SS: SSID and its attenuation relative to radio-signature power, in the used sub-frames,in the interval between two Master sub-frames;
- For every coexistence neighbor BS: the BSID, the IP address of the coexistence neighbor and other profile information, and the SSs it interfered to, (and the SSs belong to it that interfered by the database owner BS.tbd.)
- For every BS in the same community: the contact IP address and the interference situation between this BS and other BS, including the interference situation with the DB owner.
- For every SS registered: the interference situation, the number of interference source, the IP address and RSSI of each source detected by the SS.

15.2.1.1.3 Coexistence Time Slot

CTS (Coexistence Time Slot): a predefined time slot for the coexistence protocol signaling purpose, especially for the BS to contact its coexistence neighbor BS through one or more coexistence neighbor SSs in the common coverage area.

ICTS(Initialization Coexistence Time Slot): the periodical appointed CTS specially used by IBS to contact its neighbor OBS. When the IBS get the OCTS allocation and start the operating stage, it will ceased to use the ICTS.

OCTS(Operation Coexistence Time Slot): the rest CTS other than ICTS, periodically reallocated to OBSs.

CTSN(Coexistence Time Slot Number): the periodical number of CTS according to the time order.

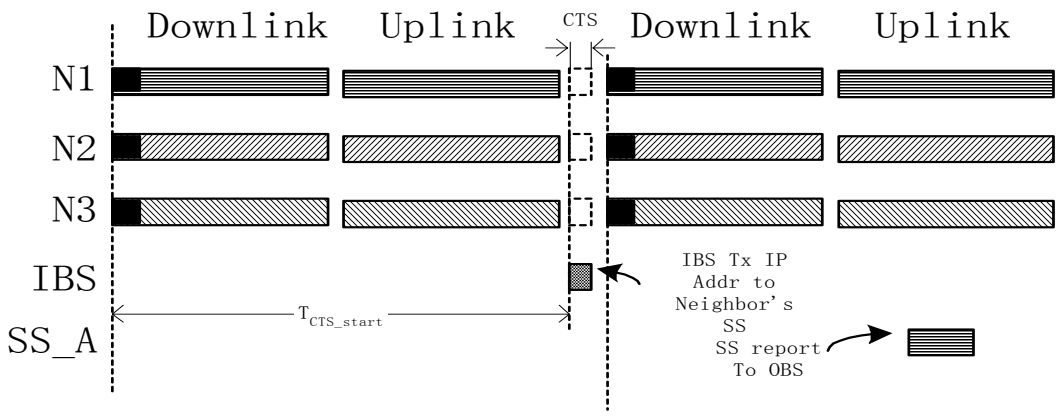

Figure h9—Timing of Coexistence Time Slot

ICTS must not be used for other purpose by all the BSs, so that it will be an interference free slot for the coexistence neighbor discovery purpose. Initializing BS (IBS) shall use this slot to broadcast its IP identifier, by sending a message and/or by cognitive radio signaling, so that the coexistence neighbor operating BS (OBS) could find the new coexistence neighbor in IP network after the SS report the message. Then the IBS and OBS begin further negotiation for coexistence protocol. After coordination with the neighbors in the community, IBS will get periodical interference free OCTSs, and become OBS, after that, it will cease to use the ICTS.

Not to break the downlink PDU, and to prevent overhead of more preamble and gaps. CTS slots shall be located before RTG/TTG in TTD frame structure or before the preamble of downlink frame in FDD frame structure .To unify the location in these two kind of duplexing frame , CTS slots in FDD frame shall be put into the downlink structure right before the preamble, and shall be located right before RTG in TDD frame.

The IBS_IPBC broadcasting procedure is unidirectional, only from the IBS to the SSs in IBS/OBS's common coverage, and the SSs shall report all the useful information to their OBSs they registered to. The SSs that succeed in receiving the message should report the IP address of IBS and the frame number of the starting frame of IBS_IPBC, the SSs failed to received the broadcasting message but got IBS_IPBC like interference in the ICTS should report the error status and the starting frame number of receiving the ICTS interference. By the IBS IP address reported from the SSs, the OBSs will then find the IBS in the IP network, and go further signaling using IP network. And by checking the frame number in the report, OBS need to find out if the SSs that report the error status in IBS_IPBC receiving have got the same interference source, then OBS will update the database and reply to the SSs which send the error report.

The CTS/ICTS parameters need to be unified in a particular region, and to be well known by the BSs. So that each BS could know the exact time to transmit the broadcasting message in its initialization. The parameters include:

— $T_{CTSstart}$ *: CTS starting time from the beginning of the frame (ms)*

— ***$T_{CTSdurat}$:*** CTS duration time (ms)

— ***$N_{CTSstart}$*** : CTS starting frame number frames

— $N_{CTSintv}$ *:* number of frames in CTS interval

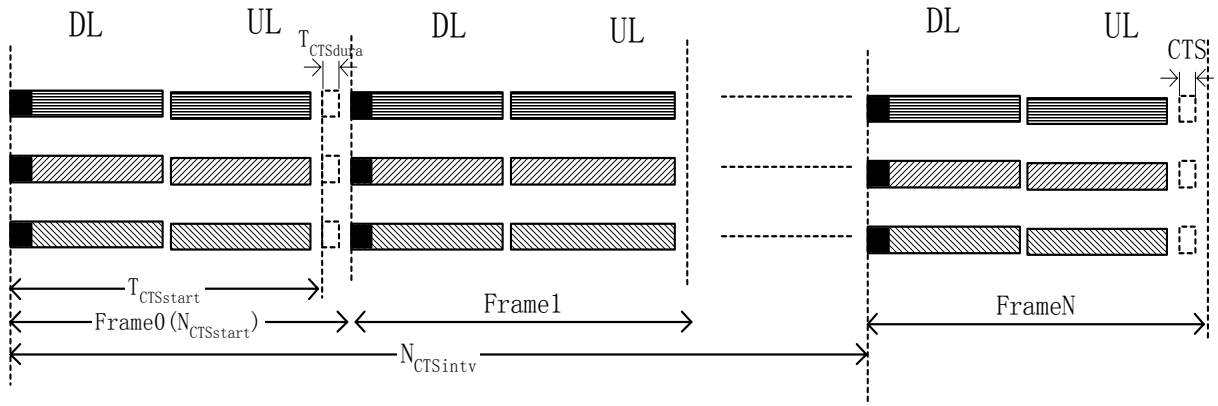

Figure h10—CTS parameters

— N_{ICTS_Cycle}: ICTS cycle counted in CTS cycles

— N_{OCTS_Cycle}: OCTS cycle counted in ICTS cycles

Assuming NCTSintv =4, NICTS_Cycle =4, NOCTS_Cycle =2, here is the example of the timing indication:

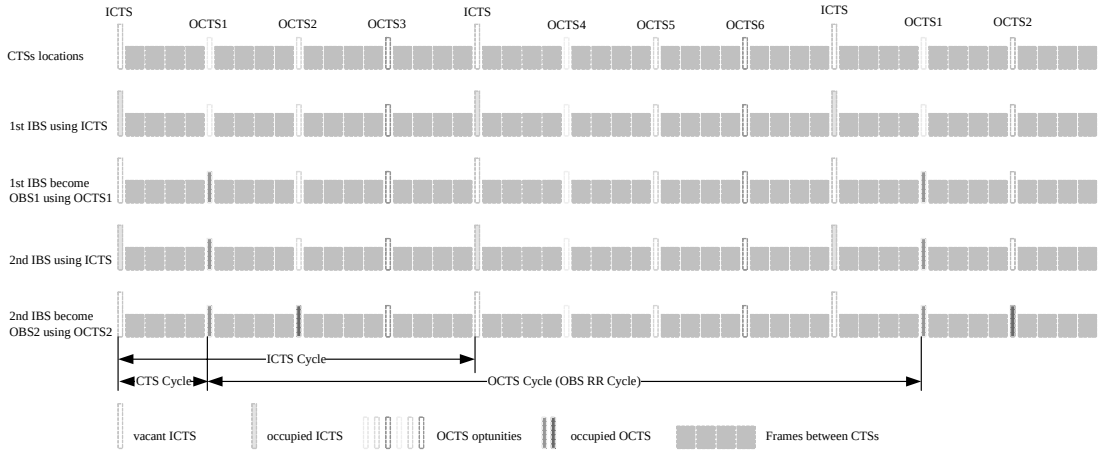

Figure h11—ICTS/OCTS occupation and timing example

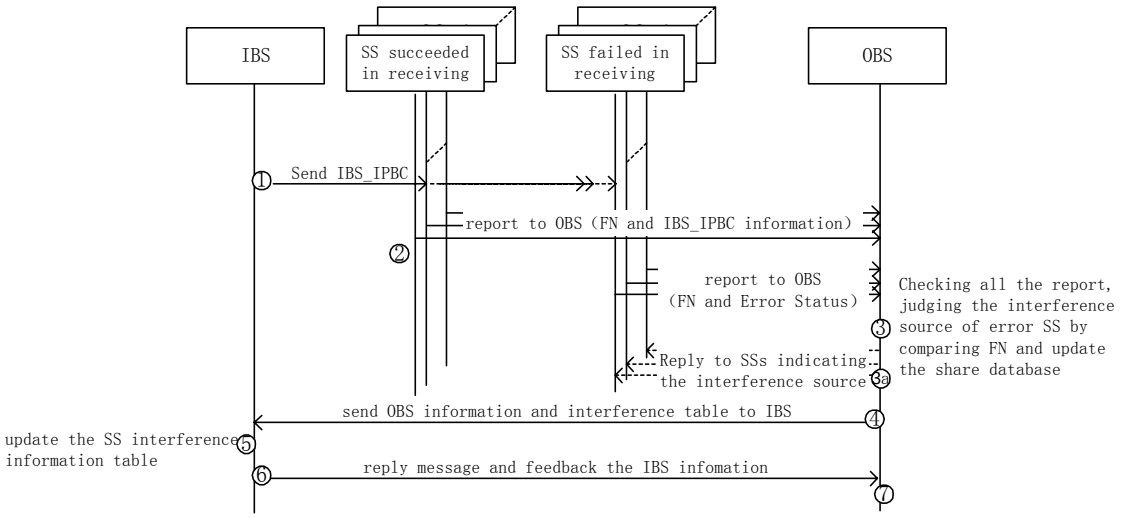

Figure h12—CTS usage example- IBS broadcast IP address to CoNBR's SS

A coexistence time slot (CTS) is a reserved physical frame used for the coexistence protocol signaling purposes. For example, the beginning of the first CTS is at HH:MM:00 UTC, the second CTS is at HH:MM:06 UTC, etc. The beginning of every CTS slot is specified by a UTC message (time stamp). (Figure h 13).

The CTS could be used by ad hoc wireless LE systems (BSs and their SSs) to mediate their co -channel coexistence. The CTS will be an opportunity for systems (BSs and their SSs) to indicate to other systems (BSs and their SSs) the extent of the interference they can cause; newly arriving interfering base stations (IBS) will use the CTS to make themselves known to established communities of operating base stations (OBS). Newly entering SS will make their presence known when they are detected by base stations to which they are not associated (see Section[tbd.]). Sporadic interference from BS or SS will also be detected by the same process.

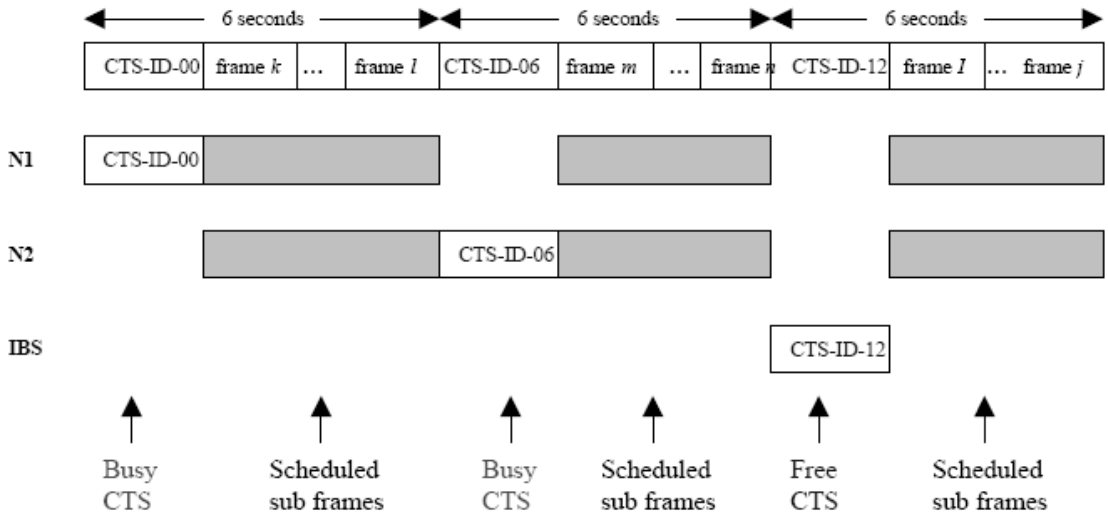

Figure h13—Alternative Timing of Coexistence Time Slot

[Notes: 15.2.1.1.4 & 15.2.1.1.5 is provisional, taken from C80216h-05_029 and call for comments and futher contribution]

15.2.1.1.4 Energy Symbols Used in the CTS

The symbols used in the CTS slots is used to broadcast by the BS and received by the SS in coexistence neighbor network. The modulation technology on both side should be one of the3 following: SCa, OFDM or OFDMA, and could be different on two side. The band of the two side shall have overlapped part, and the bandwidth of two side could be different.

The symbol is defined only in the power and time aspect, and could use any one of the modulation technology and any band that have been used in the equipment. The length of the energy symbol shall be 1/N of the CTS length, here N is a natural number and to be consolidated in region/country regulator.

There is 4 kinds of symbols:<SOF>,0/null,1,<EOF>, to be used to form any frame in CTS.

- <SOF>: Start Of Frame, indicating the data part will start at the following symbol.
- 0/null: Binary code 0 used to compose the data part, same with null symbol.
- 1: Binary code 1 used to compose the data part.
- <EOF>End Of Frame, indicating the data part ended at the last symbol

Each symbol is divided into two equal length parts. And for each part, there is 2 kinds of power keying level defined, H (high) and L (low). High power level part need the BS to use the maximum power to transmit and the SS will detect higher RSSI at that part, and the low power level part need BS to be silent and SS will detect lower RSSI at that time.

The format of each kind of symbols is shown in the table below:

Table h1—CTS symbol Format

format		signification
Part1	Part2	
L	H	<SOF>
H	L	<EOF>
L	L	0
H	H	1

The receiving SS shall follow up the CTS timing and detect each symbol continuously in every symbol space. The SSs shall verdict the symbol by this aspect of RSSI and time. One CTS consists of several symbols with the same length, the number of symbols in each CTS slot is standardized in region/country.

15.2.1.1.5 CTS Frame Structure

CTS frame is broadcasted from the base station to coexistence neighbor's subscriber station. They are loaded into serialized CTS slots. It consists of power keying energy symbols as basic element and carry the information from BS to the coexistence neighbor's SS. The CTS frame has the <SOF> symbols and <EOF> symbols as the boundary of slots, and two consecutive <SOF> and <EOF> indicate the message boundary, it shall be filled with symbol one in the rest part of last slots which have not enough payload and checking appendant.CTS frame should be continuously carried in the serialized CTS slots during the whole CTS frame structure. Each CTS frame shall have 8 bits cyclic redundancy check (Polynomial "X8+X2+X+1") appendant to check the validity of the information carried in the CTS frame. The basic structure is shown below:

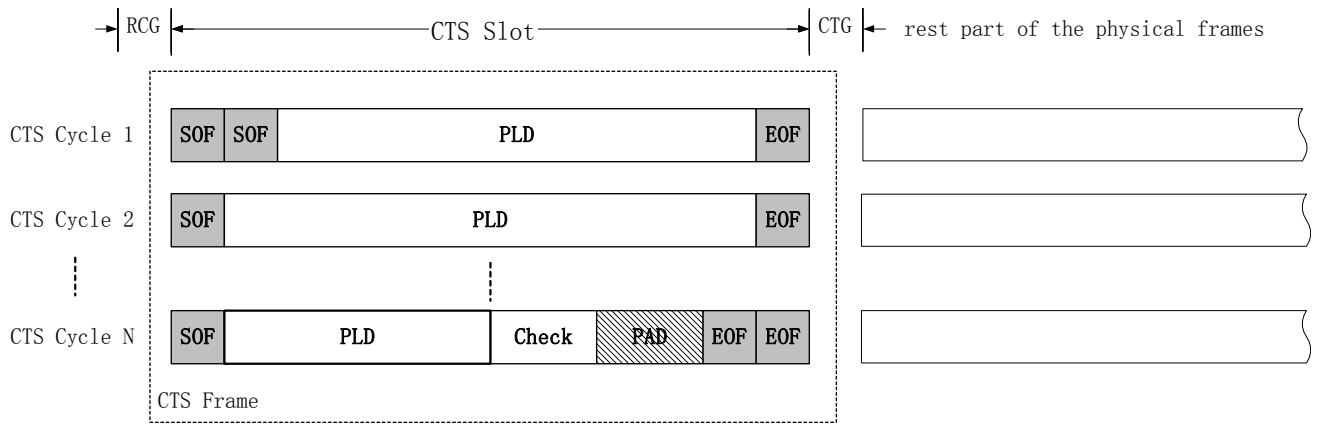

Figure h14—CTS frame construction

The PLD (payload) part of the CTS frame should be divided into TLV aspect. TYPE indicate the type of the payload, LENGTH correspond to the number of symbols/bits contained in the VALUE portion. (TYPE and LENGTH is 1 octet each.)

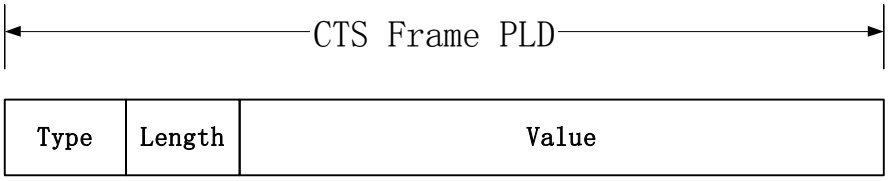

Figure h15—CTS frame PLD

15.2.1.2 Interference Control

Interferer identification using the radio signature

— A receiver will listen to the media during the radio signature slot and will find out which are the strongest interferes; by scanning the BS data bases will be possible to identify, due to the knowledge of the frame number, sub-frame number and offset, to which BS is the interferer associated; based on time-shift information, the Base Station will be able to identify the Subscriber Station ID. During the allocated radio-signature transmit opportunity no other radio transmitters will operate.

Interference reduction

— A BS has the right to *request an interferer to reduce its power by P dB*, for transmissions during the time in which a Base Station is a Master; if the requested transmitter cannot execute the request, it has to cease the operation during the Master sub-frame of the requesting Base Station; this applies also for systems using the sub-frame as a Master

Sharing the Master time

— A Base Station will indicate in the data base *what portion of the sub-frame time, separately for Tx and Rx, is actually used*

— Other systems, which do not interfere one with each other, may use that time interval

Target acceptable interference levels during Master sub-frames:

For the Base Station and its SS, using the Master sub-frame: min. 14dB above the noise + interference level (16QAM 1/2 ***[note: we should define the interference criteria; the existing one may be too stringent and not necessary for short links]***

15.2.1.3 Community Entry of new BS

Figure h 16 explains how one new entry BS discovers its coexistence neighbor BSs. The new entry BS-5 uses its GPS coordinates (x5, y5) and its maximum coverage radius in LOS, Rm, at allowed maximum transmission power. A BS is *potential* coexistence neighbor BS of another BS if:

— In co-channel operation the LOS maximum coverage area resulting for the allowed maximum transmission power overlaps one with each other. As depicted in Figure h 16,the regional LE DB will return BS-1, BS-2 and BS-3 as the *potential* coexistence neighbor BSs of the new entry BS.

— In first or alternate adjacent channels operation, the BS should consider the attenuation of the transmitted power, corresponding to the actual operation channels of different Base Stations

Once a LE BS has learnt its *potential* coexistence neighbor topology from the regional LE DB, it evaluates the coexisting LE BSs and identifies which BSs might create interferences. The Adaptive Channel selection will select the actual operating frequency, such that the probability of interference will be minimized. Each LE BS tries to form its own community. By including the coexistence neighbor BSs that create interferences to the associated SSs The members of community will change when the working frequency of any BSs changes or new interfering coexistence neighbor BS comes in.

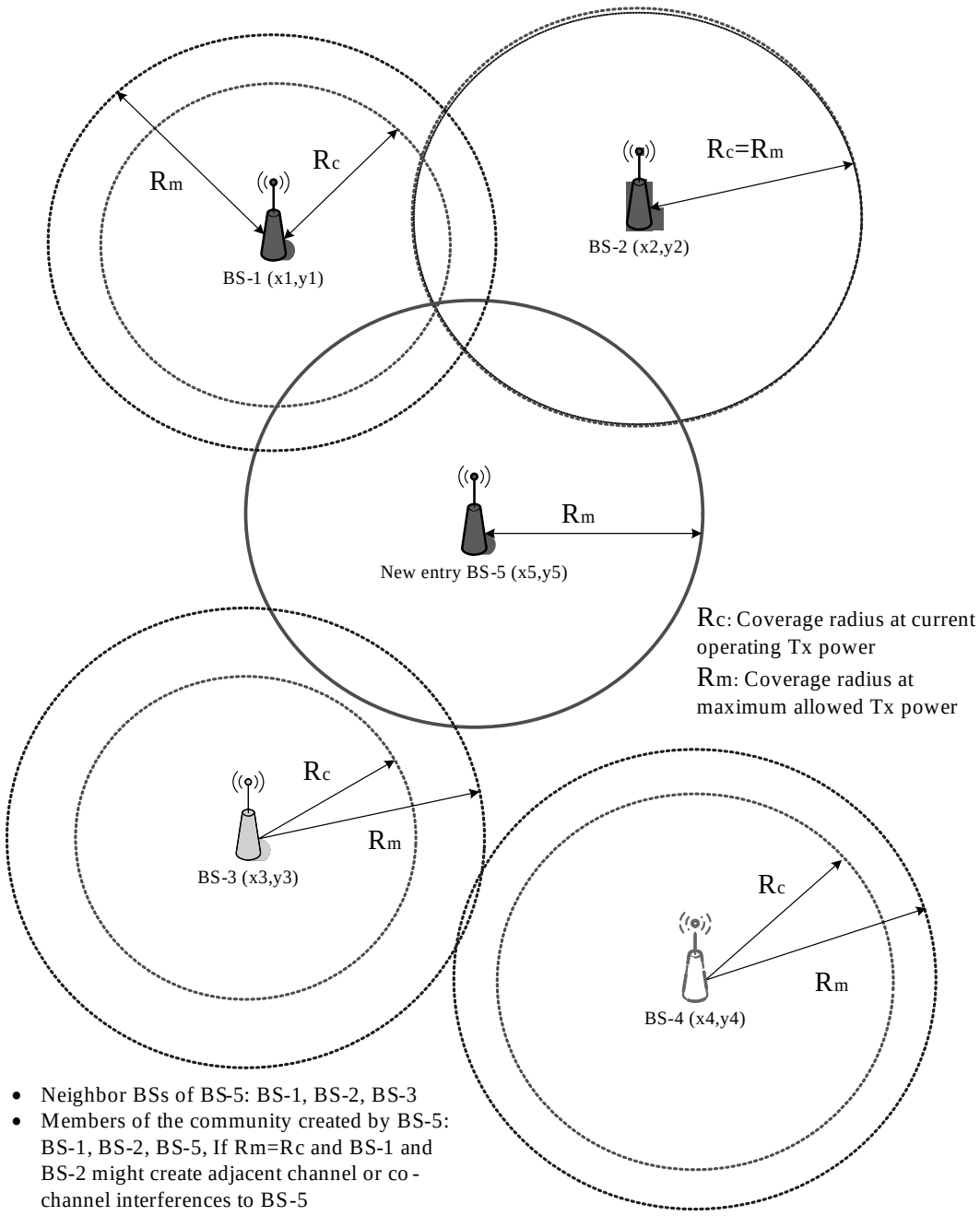

Figure h16—802.16 LE Coexistence neighbor BSs discovery and definition of coexistence neighbor and community

With the regional LE DB a LE BS can construct its coexistence neighbor topology and acquire the IP addresses of its coexistence neighbor securely.

In any case that the new coming BS could not find the region LE DB, it should start a ad-hoc method to find the neighbor topology. The new coming BS use the coexistence time slot to broadcast its IP address to the reachable SSs in the neighbor network. Once the SSs received this message, they will report to their serving BS one by one unsolicitedly, the information of the new BS and the interference status that they record during the receiving will be reported to there serving BS.

The serving BS will get all the information from the related SSs and saved the useful content to their database. After that, the serving BS will contact new BS using the IP address reported by the SS and transfer the parameter of its own to the new coming one with authorization and negotiation, thereafter the serving BS will also get the parameter and other corresponding information from the new coming BS.

In general, the coexistence detection, avoidance and resolution are performed in two stages, initialization stage and operating stage.

(1) *Initialization stage*

In initialization stage the LE BSs may avoid the co-channel or adjacent channel interference by scanning the available frequencies. But this method cannot avoid the *hidden* LE BS problem, i.e. the BS that cannot be heard directly but may have overlapping service coverage. Thus, with the knowledge of coexistence neighbor topology the LE BSs can detect the *hidden* LE BSs and can, therefore, avoid the possible interferences from coexisting coexistence neighbors. Alternatively, if the country/region database is not valid in this phase, the initializing BS will use the coexistence time slot to broadcast its IP address to its coverage using its maximum power. In this way, the SSs in the reachable zone of the new BS's interference will receive the message and forward the address to its serving BS. And after the neighbor BSs get the address via the SSs' reports, they will contact with their new coming neighbor via IP network and updating the database on both side. Thus, in ad-hoc fashion, it will avoid the hidden neighbor BS issue by the SSs in the neighbor network. If the LE BS finds that there is no "free" channel, the coexistence neighbor topology in the share database provides the information of with whom it should negotiate. LE BS may decide whether a "free" frequency can be allocated for itself by channel reallocation within community, If IBS can figure out optimized channel distribution in the community, which made every member in the community could occupy a exclusive channel, IBS should contact the BSs in the community which need to reallocate the channel in the new distribution and negotiate, after admitted by each BS, IBS should send a message to the candidate BS to indicate the switch time and the target channel, all the candidate BS should then follow the indication and switch to the target channel synchronously. Otherwise, if IBS can't get a "free" frequency whatever reallocation executed, that means IBS should have to share a frequency with one or some of its neighbors. The procedures are described in Figure12.

(2) *Operating stage*

In operating stage the LE BS has SS associated with it, however, even the operating system parameters has decided, the co-channel or adjacent channel interference from LE BSs of different network may still have a chance to happen due to the detection of interference from primary user, channel switching of coexistence neighbor BS or the entry of new coexistence neighbor BS makes the community so crowded that there is no enough channels. If the LE BS finds that there is no "free" channel at that moment, synchronous channel switching maybe executed, or the coexistence neighbor topology provides the guidelines of with whom it should negotiate to share the channel. ***[detailed procedures are to be defined]***

Figure h 17 shows the initialization procedures for the 802.16 LE BSs. Note that the procedures that BS tries to create a Master slot or channel switching are also applicable for operating stage. The detailed negotiation and update procedures are described in section 15.6.1and 15.7.1.4.

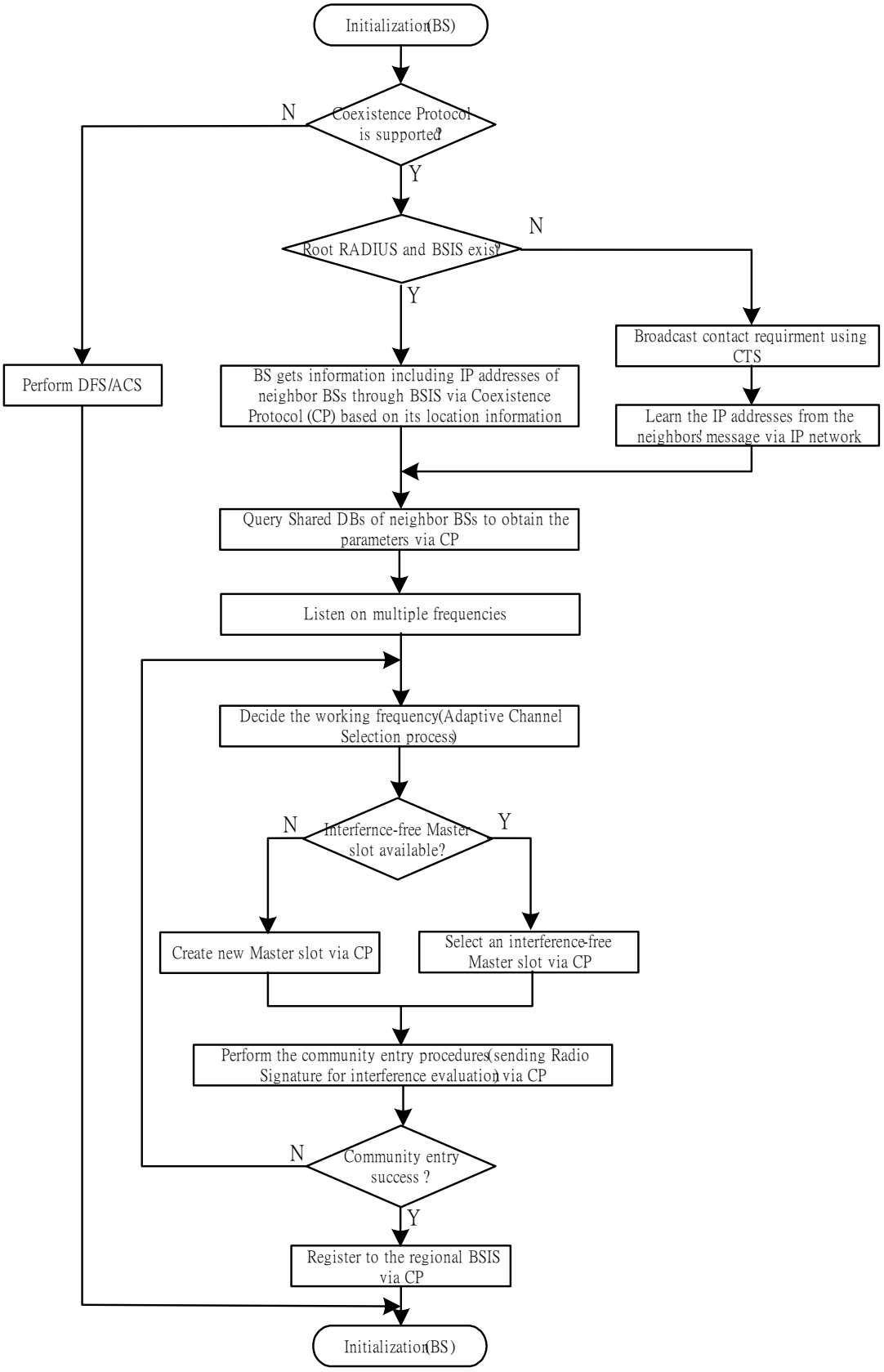

Figure h17—Initialization procedures — BS

[Note: the following text needs further consideration]

— *The first phase of* the Community Entry is to judge the validity of country/region data base. If the country/region Root RADIUS serveris valid(t.b.c: what means valid?),, the processfurther queries Root RADIUS server::

- o Get the BSISs from the country/region Root RADIUS server;
- o *Read the data base maintained by BSIS via Coexistence Protocol;*
- o Identify which Base Stations might create interference, based on the location information;
- o The IBS learn the IP identifier for those Base Stations;

Otherwise:

- o New BS uses the interference free slot to broadcast the message containing the contact request and/or the cognitive radio signal transmitting the IP address
- o *The SS in the common coverage will forward the information to its operating base station. using REP_RSP message*
- o The operating BS update its database and send feedback informationto the IBS, using the IP network
- o *learn the IP identifier of the coexistence neighbor BS from the message sent by the coexistence neighbor BS via IP network*

— Build the local image of the relevant information in the community BS's, *by copying the info in those BSs*

— Listen on multiple frequencies

- o Identify the level of interference on each frequency channel;

— Decide the working frequency (ACS – Adaptive Channel Selection process);

- o If no interference detected on some channels, select one randomly as working channel;
- o If interference detected by IBS or OBS network on all channels, then IBS should decide whether an optimized channel distribution can allocate an exclusive channel for each BSs including IBS in community.
- o If every BS in community can be allocated an exclusive channel without interfering with others, that means default interference-free Master slot is available for this initializing BS.

— If available, select an interference-free Master sub-frame; if not, use the procedure for creating new Master sub-frames;

— Search the Base Station data base for finding the BSs using the selected Master sub-frame;

— *Request those Base Stations, by sending IP unicast messages, to listen during the BS_entry slot* in order to evaluate the interference from the new Base Station;

— Use the allocated slots for transmitting the "radio signature" at maximum power, maximum power density and in all the used directions;

— *Ask for permission of the Base Stations*, using the sub-frame as Masters, *to operate in parallel and use the same sub-frames;*

— If all of them acknowledge, the Base Station acquires a “temporary community entry”status; the final status will be achieved after admission of the SSs;

— If no free Master slot sub-frame is found, use the procedure for creating new Master slotssub-frames.

15.2.1.4 Network and Community Entry for SS

— Start listening;

— Determine interference intervals;

— Assume that the interference is reciprocal;

— Build database for possible working slots and sub-frames;

— Wait for the Base Station community entry and start of operation;

— At BS request, s*end a list of the above identified time intervals;*

— If an old Base Station will perceive interference from the new SSs, it will *ask the new Base Station to find another sub-frame for that SS operation;*

— If the SS will sense interference, will request their Base Station to *find another sub-frame for operation as Master.*

15.2.1.5 BS regular operation

— Schedule SS traffic:The traffic of each served SS should be schedule into corresponding sub-frame/ resource based on the SSs’ interference situation. Traffic of SSs in the interference free zone could be scheduled into any available sub-frame/resource of the serving BS, and traffic of SSs in the interference zone should take only corresponding master subframe/resource of the serving BS.

— Set Tx power levels, such to use minimum power levels for both BS and SSs;

— Maintain it own database when other BSs join the network.

— The BS need to keep updating the information of all the BS in the community including the coexistence neighbor BS, and the information of the served SSs in the own network. The information include the profile and the interference situation of the stations. The interference situation information include the interference status, the interference source and corresponding RSSI, the interference victims founded. Etc.

15.2.1.6 Operational dynamic changes

15.2.1.7 Creation of a new sub-frame

If none sub-frame can be used, a *new Base Station may request the addition of another sub-frame.* The effect of such a request will be the reduction of operating time for those Base Stations that interfere with the new Base Station. However, all the others, that do not interfere one with each other and with the new one, may work in parallel and use the same operating time.

A Base Station will request the creation of a new sub-frame by:

— Sending IP messages to all BS members of the community, and indicating:

  - The interfering operator ID and BS ID
  - The MAC frame-number in which the addition of a new sub-frame will take place.

— All the requested *BSs will acknowledge the request*, by
  - o Sending back a message having as parameters:
  - o Frame-number for the change (must be the same as the requested one
  - o Master sub-frame number for the new BS (SF = Sfold+1).
  - o If are missing acknowledges, those BS will be asked again, for another M attempts, after that will be considered that they are not working;
  - o At the above specified MAC frame number, a new sub-frame partition will take place, by inserting in the sub-frame calculation relation N=N+1
  - o The BSs will up-date the own SSs about the change
— Start to use the created Master sub-frame.

15.2.1.8 Controlling interference during master sub-frame

15.2.1.8.1 Interferer identification

The interferers will be identified by their radio signature, for example a short preamble for OFDM/OFDMA cases. The radio signature consist of:

— Peak power

— Relative spectral density

— Direction of arrival.

Every transmitter will send the radio signature during an interference-free slot. The *time position of this slot (frame_number, sub-frame, time-shift)* will be used for identification.

In IBS's coexistence neighbor discovery phase, the IBS's IP address shall be broadcast using the IPBC frame with pulse energy keying. And this shall be detected by coexistence neighbor's SS in the IBS's reach-able range and reported to its serving BS.

The IP address is used to identify the coexistence neighbor BS by the receiver SS in the IBS's coexistence neighbor discovery phase. And also be the identifier of the IBS for the coexistence neighbor BS before the coexistence neighbor got in touch with the IBS in the IP network.

15.2.1.8.2 Interference to BS

— Identify the interferers;

— Send messages to interfering BSs, *asking to drop the power of the specified transmitter by P dB;*

— Alternatively, send messages to related BSs, *asking to stop operating during the BS master slot*

— The requested Base Station has the alternative of looking for another Master slot.

15.2.1.8.3 Interference to SS

— *Report* to BS about experienced interference

— List of frame_number, sub-frame, offset, IP address of source BS (if detected)

— BS start process for interference reduction with *feedback from the SS.*

15.2.1.9 Controlling interference during not-interfering traffic sub-frames

The Base Station data base shall keep the following information regarding the usage of " non-interfering sub-frame" or Master sub-frames belonging to other systems:

— BS power, relative to the radio signature ***power***, when using each of the sub-frames;

— List of SSs and their power, relative to the radio signature ***power***, when using each of the sub-frames.

The received power during other sub-frames can be obtained by using the radio signature measurement and suitable calculations, according to data-base information on used powers. Messages as Stop_Operating_Request and Reduce_Power_Request can be used for controlling the interference levels.

15.2.1.10 Power Control

Every network will strive to reduce its transmit powers to the minimum, such that the C/I+N will be sufficient to allow the operation at the minimum common rate, considered as QPSK1/2 for all the 802.16 systems; an exception from this rule is possible only when a network is operating during its interference-free period. The power control mandatory algorithm will be defined in chap. ***[t.b.c.]***

15.2.1.11 Coexistence with non-802.16 wireless access systems

The above principles are also applicable to non-802.16 systems, like 802.11. During every 802.16 MAC frame, a 802.11 system may find that a sub-frame may be used, due to the low created interference levels. In the case that no operation in parallel is possible, the new system will ask for the creation of a new Master sub-frame. The Coexistence Protocol, working at IP level, will allow the communication between systems using different PHY/MAC standards.

The scheduled use of the MAC frame is possible by using the 802.11 PCF mode.

15.2.2 Shared distributed system architecture

15.2.2.1 Architecture

The architecture for Radio Resource Management in the context of IEEE 802.16h it is a distributed one and allows communication and exchange of parameters between different networks. A network consists from a Base Station and its associated Subscriber Stations.

Every Base Station includes a Distributed Radio Resource Management entity, to apply the 802.16h spectrum sharing policies, and a Data Base to store the shared information regarding the actual usage and the intended usage of the Radio Resource.

A subscriber Station may include an instance of DRRM, adapted to SS functionality in 802.16h context.The following figure shows the functional diagram of the IEEE 802.16h network architecture:

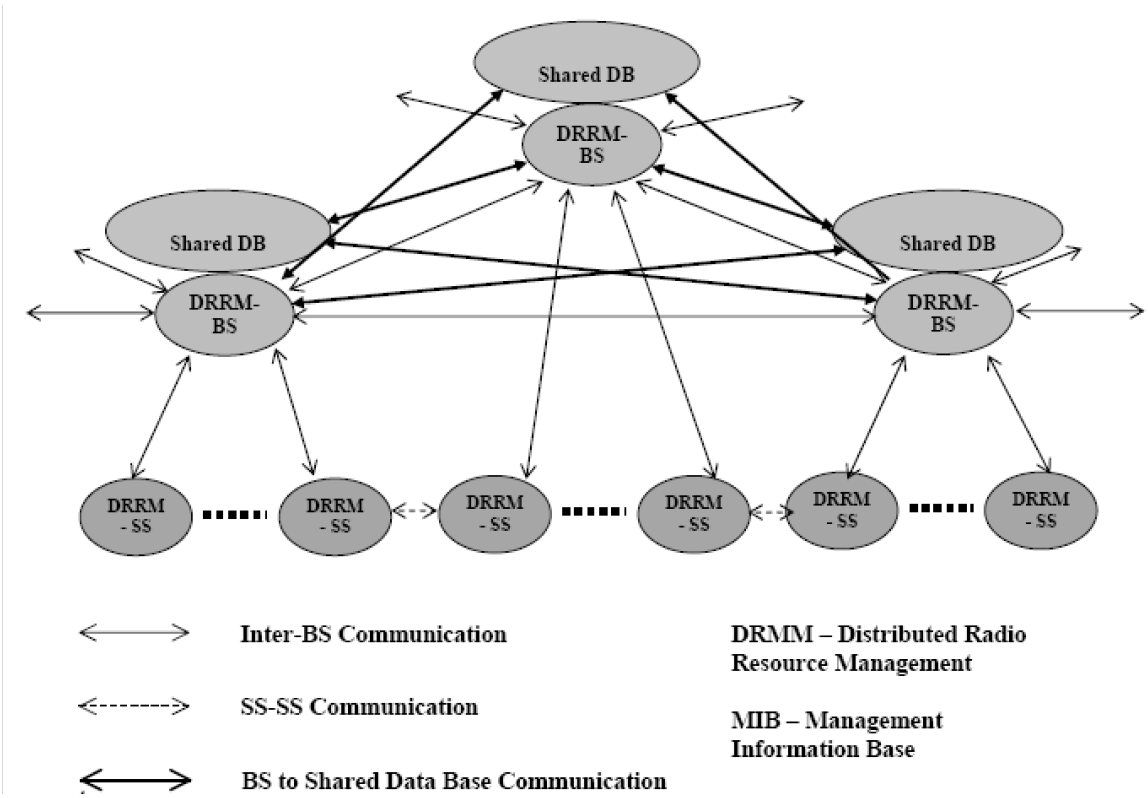

Figure h18—System Architecture

[Note: the security part is a temporary text adopted from contribution C802.16h-05/11r1 and 802.16h is calling for comments]

Figure h 18 shows the IEEE 802.16 LE inter-network communication architecture:

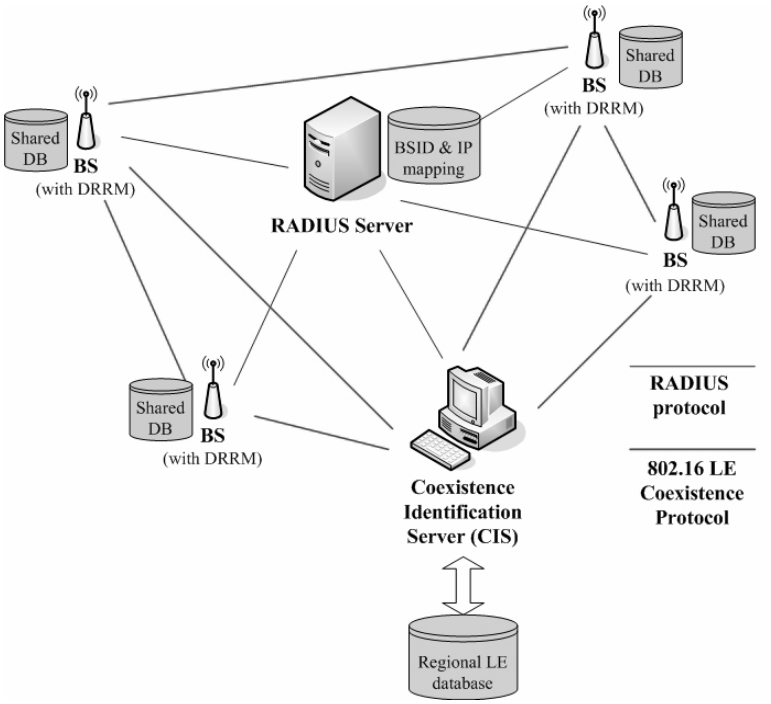

Figure h19—Network Architecture

General architecture includes the components operating over IP-based network:

- The RADIUS Server- The Base Station Identification Server (BSIS), described in detail in section xxx - The BSs cooperating with the Distributed Radio Resource Management (DRRM) procedure RADIUS server to maintain the address mapping of wireless medium addresses of BSs (their BSID) and medium addresses of BSIS to their IP addresses.

15.2.2.2 Inter-network communication

The inter-network communication consists in:

— Inter-netwo*rk messages*

  - o Base Station to/from Base Station
  - o Base Station to/from Subscriber Station to/from foreign Base Station; the subscriber Station is used as relay, if the two Base Stations are hidden one from the other

— Open access to DRRM Data Base:

  - o To read the parameters of the hosting Base Station
  - o *To request c*hange of the hosting Base Station operating parameters.

15.2.2.3 Coexistence Protocol

[Note: the security part is a temporary text adopted from contribution C802.16h-05/11r1 and is subject to further discussion.]

In order to get the coexistence neighbor topology, perform registration to the database and registration to peer, negotiation for Shared RRM etc. will be used a Coexistence Protocol (CP). Figure h 20 describes the 802.16h protocol architecture. The protocol architecture indicates that DRRM, Coexistence Protocol and Shared DB belong to LE Management Part located in management plane and the messages will be exchanged over IP network. Thus, DRRM in LE Management Part uses the Coexistence protocol to communicate with other BSs and with Regional LE DB and interact with MAC or PHY. Figure h 20 is LE BS architecture with Coexistence Protocol. The gray area indicates area where there is an absence of connection between blocks. DSM is Distribution System Medium which is another interface to the backbone network. Note that is architecture is only for reference. Similarly, Figure h 20 is the BSIS architecture with co-located regional LE database. Other architectures are not being illustrated. The Coexistence Protocol services are accessed by the LE Management Entity through CP SAP. The service primitives are described in t.b.d A BS uses the Coexistence Protocol, which is similar to PKM protocol, to perform the coexistence resolution and negotiation procedures. There are two types of messages to support Coexistence Protocol:

(1) LE_CP-REQ: BS->BS or BS->BSIS

(2) LE_CP-RSP: BS->BS or BSIS->BS

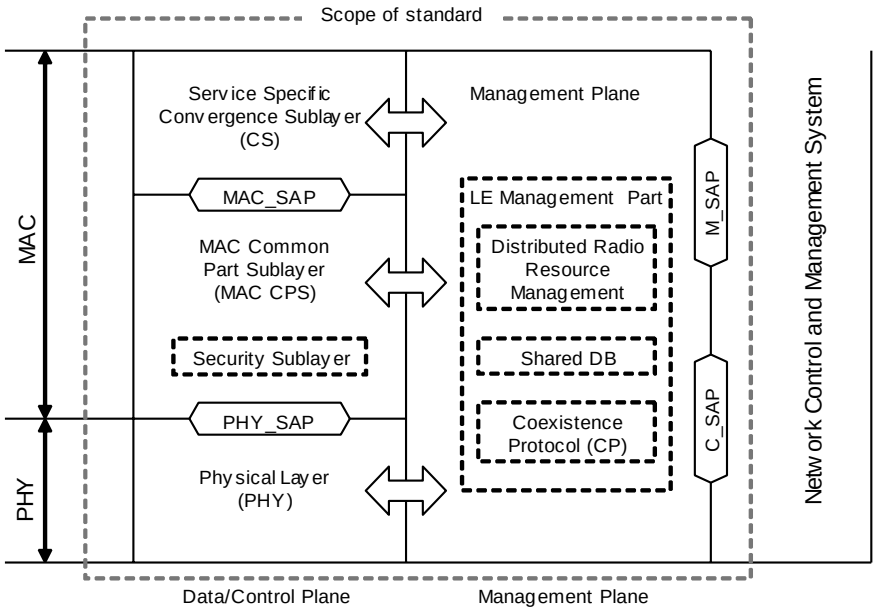

Figure h20—802.16h BS Protocol architecture Model

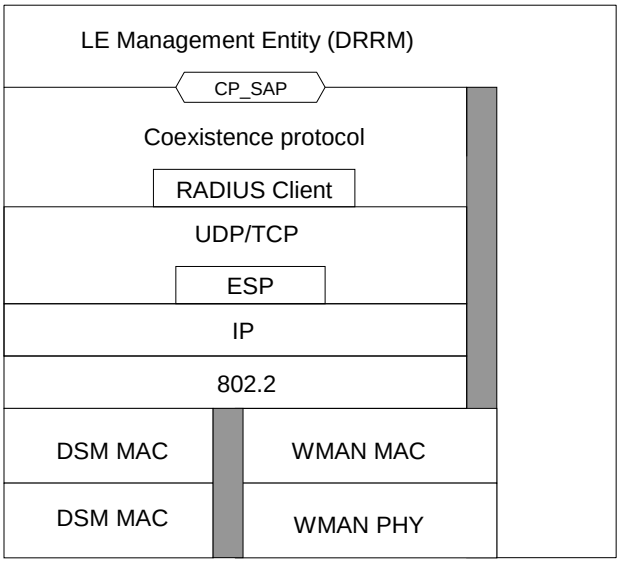

Figure h21—LE BS architecture with Coexistence Protocol

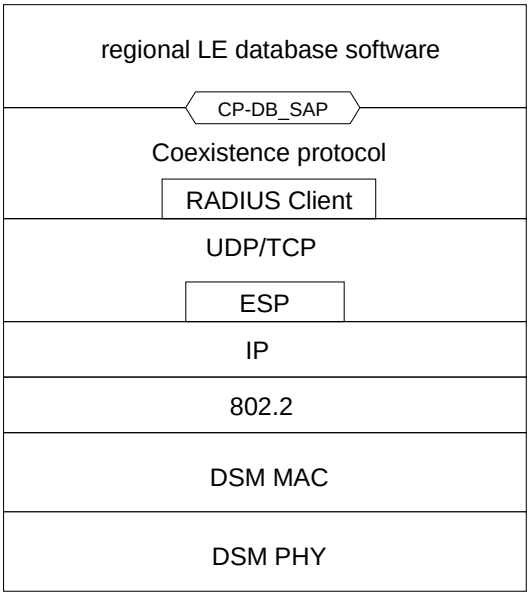

Figure h22—BSIS architecture with co-located regional LE database

15.2.2.3.1 Same PHY Profile

For networks using the same 802.16 PHY Profile, including elements as:

- Mandatory channel spacing for LE system in[tbd.] MHz will be[tbd.] MHz*;*
- PHY mode:
  - WirelessMAN-OFDM (256 FFT points)
    Mandatory profiles for operation in the LE 5725-5850 MHz band will be:
    - profM3_pmp,profP3_10,profC3_23,TDD,profR13
  - WirelessMAN OFDMA 2k (in future 128, 512, 1k) FFT points
  - *WirelessMAN* SCa,

the inter-network communication may be done using 802.16 messages over the air, including messages defined by 802.16h amendment. The procedures for sending these messages are described in ***t.b.d.***

[The text below is taken from C80216h-06_003, and call for comment]

The CTS is the duration of a frame (20 msec) , and consists of an uplink and downlink intervals of equal size (10 msec). Downlink messages carry information (Radio Signatures/BSD messages [tbd.]) unique to the identity of the base station controlling the network for which the particular CTS is associated. Uplink messages carry information (Radio Signatures/SSURF messages[tbd.]) unique to the subscriber stations associated with the network and base station associated with the same CTS. During a CTS all other networks, not associated with the particular CTS, remain silent and receive only.

A base station descriptor (BSD) messages are broadcast within the downlink portion of the CTS every minute by a base station. This is always done in the same CTS frame, ie the frame claimed by the base station. In broadcasting in this manner the base station announces its (and its network's) existence. The BSD serves two purposes. First, it contains pertinent information related to the base station, allowing other base stations to identify it (via their SS). Secondly, it allows the differentiation of a CTS frame from a non-CTS frame. When it is received, SS associated with the BS will recognize the frame containing the BSD message as a CTS frame, and will transmit SSURF (uplink Radio Signature) messages (section 15.6.6.2.3) in response to it. Note that SSURF will use the uplink bandwidth granted only in the CTS frame, and is not transmitted in the data link.

Every BSD sent downlink has a BS_ID associated with it, it is always included in the DL_MAP message as specified in IEEE 802.16-2004. This is thus a de facto tag to the downlink frame, and can be used as an interference identification tag as well. The message contains the UL-MAP, which addresses specific SS to send their SSURF messages. The duration of the BSD message is typically 1 msec [tbd.].

There is only one downlink BSD PDU in the CTS frame and it is transmitted at random starting point within the downlink time interval of the CTS. The rationale for the random placement of the BSD within the downlink subframe is shown below:

There is the possibility that two or more potentially interfering base stations choose the same CTS slot. Such base stations and the respective networks they control may coexist peacefully without interference to each other because of hidden SS or no SS in the common coverage area. Essentially, such networks do not form a community because they do not interfere with each other. However, when the hidden SS or new SS enters into the common coverage area, co-channel interference will be detected at the new SS resulting in a situation that impacts the neighboring base stations having a common CTS.

CTS slot collision occurs in this situation. Two co-channel base stations, inadvertently and independently, have chosen the same CTS prior to interference being detected by the networks. To resolve this situation the start times of downlink sub frame PDU and uplink SSURF messages in the CTS slots are randomized. This reduces the possibility that two networks, sharing the same CTS, will overlap in their downlink and uplink transmissions. Realize that the downlink slot will be 10 msec wide and that the downlink sub frame PDU itself is only < 1 msec. For the worst CTS slot collision case, there are n base stations in the common coverage area, the successful (non-overlapping) CTS slot transmission probability is

$$' = 1 - \frac{1}{m} \bullet \frac{1}{m} \bullet C_n^2 = 1 - \frac{1}{m} \bullet \frac{1}{m} \bullet \frac{n!}{(n-2)! \bullet 2} \quad \textit{(h1)}$$

Where $m = \frac{t}{td}$. Assume the CTS downlink duration time length is t which is the uplink portion of a physical frame (physical frame duration is varying from 2, 2.5, 4, 5, 8, 10, 12.5, to 20ms), the CTS downlink PDU time duration is d t , which is typically < 1 msec.

15.2.2.3.2 Mixed-PHY Profile communication

In the case of different PHY Profiles the communication will be done at IP Level. Every Base Station should know the IP address of the DRRM of the Base Stations around, by provisioning or/and by using a regional data base approach or/and by using cognitive radio signaling.

15.2.2.4 Information table in share database

Table h2—This BS information table

Syntax	Size	Notes
This BS information table(){		
BSID	48bits	
Operator ID	?bits	
IP address	32bits	IPv4 address
Master resource ID	8bits	Sub-frame number
Negotiation status	8bits	Bit0: get communication in the IP network Bit1: be registered in Bit2: registered to Bit3: done for resource sharing(if neighboring) Bit4-7: tbc.
CTS parameter(){		Regulated by region/country
Tcts_start	16bits	In microseconds
Tcts_duration	8bits	In microseconds
Period of frames	8bits	frames
Starting frames offset	16bits	frame serial number of the first frame that CTS presented
Length of Symbols	8bits	In microseconds, need to be 1/n of Tcts_duration
}		
Number of CoNBRs	8bits	m:The number of coexistence neighbors of this BS
for (i= 1; i <= m; i++) {		
BSID	48bits	
(Tbc.)	(Tbc.)	(Tbc.)
}		
Profile(){		

Band		
PHY mode(){		
Modulation		
(Tbc.)		
}		
Maximum power	8 bits	dbm
Number of registered SS	12bits	n
for (i = 1; i <= n; i++) {		
SSID	48bits	
(tbc.)	(tbc.)	(tbc.)
}		
(tbc.)	(tbc.)	(tbc.)
}		
}		

Table h3—BS information table

Syntax	Size	Notes
BS information table(){		
Index	16bits	
BSID	48bits	
Operator ID	?bits	
IP address	32bits	IPv4 address
Sector ID	8bits	
Master resource ID	8bits	Sub-frame number
Negotiation status	8bits	Bit0: get communication in the IP network Bit1: be registered in Bit2: registered to Bit3: done for resource sharing(if coexistence neighboring) Bit4-7: tbc.
Coexistence neighboring	1bit	Coexistence neighbor with this BS? 1-yes 0-no
If (Coexistence neighbor){		
Number of victim SSs	16bits	n:The number of victim SSs of this coexistence neighbor, in this network
for (i = i; i <= n; i++) {		
SSID	48bits	
RSSI	16bits	1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11) for details) 1byte standard deviation
}		
(Tbc.)	(Tbc.)	(Tbc.)
}		
Number of Coexistence neighbors	8bits	m:The number of coexistence neighbors of this BS
for (i= 1; i <= m; i++) {		
BSID	48bits	
(Tbc.)	(Tbc.)	(Tbc.)
}		
Profile(){		
Band		
PHY mode(){		

Modulation		
(Tbc.)		
}		
Maximum power	8 bits	dbm
Number of registered SS	12bits	
(tbc.)	(tbc.)	(tbc.)
}		
(tbc.)	(tbc.)	(tbc.)
}		

Table h4—SS information table

Syntax	Size	Notes
SS information table(){		
Index	16bits	
SSID	48bits	
Interference status	1bit	Interfered by coexistence neighbor? 1-yes 0-no
If (Interfered){		
Number of source BSs	8bits	n:The number of interference source of coexistence neighbor
for (i = 1; i<= n; i++) {		
BSID	48bits	
IBS_IPBC detected	1bits	1-yes 0-no
If (IBS_IPBC detected){		
IP address	32bits	If the IBS_IPBC message detected, the IP address report by the SS will add here, and updating the bit above
Sector ID	?bits	Reported by SS
Frame number	24bits	Reported by SS
Error Status	?bits	0 -no error 1 - not capable to decode the energe pulse symbol.; 2 - not able to find the eligible <SOF>; 3 - not able to find the eligible <EOF>; 4 - not able to pass the CRC check for message;
(tbc.)	(tbc.)	(tbc.)
}		
RSSI	16bits	1byte RSSI mean (see also 8.2.2, 8.3.9, 8.4.11 for details) 1byte standard deviation
(tbc.)	(tbc.)	(tbc.)
}		
(tbc.)	(tbc.)	(tbc.)
}		
(tbc.)	(tbc.)	(tbc.)
}		

15.3 Interference victims and sources

15.3.1 Identification of the interference situations

15.3.1.1 Interferer identification

The interferers will be identified by their radio signature, for example a short preamble for OFDM/OFDMA cases. The radio signature consist of:

— Peak power

— Relative spectral density

— Direction of arrival.

Every transmitter will send the radio signature during an interference-free slot. The *time position of this slot (frame_number, sub-frame, time-shift)* will be used for identification.

The transmitted power of non-interfering radio transmitters using a Master sub-frame will be known from the BS data base, indicating their power attenuation relative to the radio signature, for every used sub-frame.

15.3.1.1.1 Interference Identification & Resolution via CTS Detection

15.3.1.1.2 Interference from 802.16 networks

15.3.1.1.3 Interference from Non-IEEE 802.16 systems.

15.3.1.1.3.1 Non-IEEE 802.16 Systems (BSs and their SSs) capable of GPS/UTC Timing Recovery

Non-IEEE 802.16 LE systems (BSs and their SSs) that are capable of GPS/UTC timing recovery can monitor the CTS intervals to determine the existence of co -channel IEEE 802.16 users. Monitoring the intervals and undertaking CCI measurements over CTS cycles will allow a non -IEEE 802.16 system(BS and its SSs) to determine the occupancy on a channel and avoid settling on it.

Additionally, [CTS_ID54] [tbd.] will be left unoccupied by IEEE 802.16 systems (BSs and their SSs). Non -IEEE 802.16 systems(BSs and their SSs) occupying LE spectrum can insert downlink and uplink power bursts [tbd.] into this interval. Such energy can be detected by IEEE 802.16systems(BSs and their SSs) which will consequently avoid use of the given channel.

15.3.1.1.3.2 Non-IEEE 802.16 Systems(BSs and their SSs) not capable of GPS/UTC Timing Recovery

The majority of co-channel interferers will be systems (BSs and their SSs) and devices that cannot perform rudimentary of signaling required for IEEE 802.16 coexistence and channel detection. To deal with such interferers the IEEE 802.16 networks will have to opt for avoidance of such users. To facilitate this IEEE 802.16 BS and SS will have the ability to undertake [Power Spectral Density mappings] of selected bandwidth and disseminate such information as part of their [tbd.] inter-network messaging.

Sections 15.6.1.34. and 15.6.1.36 describe the instructions and formatting that will be used by the IEEE 802.16 systems(BSs and their SSs)to undertake [PSD] measurements of contented spectrum. These mea-

surements should be undertaken by a BS prior to occupancy of spectrum space and they can be undertaken throughout the operational period of a network to determine encroachments and to identify other spectrum that may have to be used in the event of uncontrolled interference arising in the occupied spectrum. The [PSD] measurements will be undertaken by the SS as well and this sensor information will be sent to the BS. [PSD] measurement information forms part of the data base that is exchanged between networks as part of their mutual spectrum management tasks. SSURF messages [tbd.] could be used to transport spectrum information.

15.3.1.2 Grouping of interfering/not-interfering units

15.3.2 Identification of spectrum sharers

15.3.2.1 Regulations

15.3.2.2 Messages to disseminate the information

15.3.2.3 Avoid false-identification situations

15.3.2.4 Using centralized server

[Note: overlapping chapter]

15.3.2.4.1 Base Station Identification Server

[Note: The following part from 3.2.4.1 is a temporary text adopted from contribution C802.16h-05/11r1 and is subject to further discussion. A call for comment from security experts is open to comment on this text.]

The *Base Station Identification Server* (BSIS) acts as an interface between 802.16 LE BSs and the regional LE DB which stores the geographic and important operational information, e.g. latitude, longitude, BSID etc., of the LE BSs belonging to the same region. It converts the actions carried in PDUs received from the 802.16 LE BSs to the proper formats, e.g. SQL (Structured Query Language) string, and forwards the strings to the regional LE DB, which can be any available database software. BSIS converts the query results from the regional LE DB to the proper format, e.g. TLV encodings, and replies to the requested BSs. Figure h 19 shows the general architecture of inter-network communication across 802.16 LE systems. BSIS acts as a peer of 802.16 LE BSs in this architecture. The BSID of regional BSIS is well known among the 802.16 LE systems within certain domain. The messages exchanged between the LE BSs and the BSIS will be revealed in the next section.

[Note that the interface between BSIS and regional LE DB is out of scope.]

15.4 Interference prevention

15.4.1 Adaptive Channel Selection – ACS

15.4.1.1 Between 802.16 systems

15.4.2 Dynamic Frequency Selection – DFS

15.4.2.1 Frequency selection for regulatory compliance

15.5 Pro-active cognitive approach

15.5.1 Signaling to other systems

[Note: the cognitive signaling may have effect on the power amplifier and on the PAPR. Call for contribution to investigate if there are any such effects.]

15.5.1.1 Ad-hoc systems - operating principles using Cognitive Radio signaling

In order to reduce the interference situations, in deployments in which may exist a combination of 802.16 systems using a Coexistence Protocol and 802.16 ad-hoc systems, the 802.16 ad-hoc systems will apply the Adaptive Channel Selection procedures and use cognitive radio signaling procedures to interact with systems using a Coexistence Protocol. The ad-hoc systems obtain a temporary Community registration status, that has to be renewed from time to time.

15.5.1.2 Registration

The 802.16h pro-active cognitive radio approach defines signals and procedures for the reservation of the activity intervals and registration of ad-hoc systems. The operational procedures are described below:

- 802.16h Community registered systems, using a Coexistence Protocol, will reserve the MAC frame Tx/Rx intervals by using, during the MAC Frame N, cognitive signals to indicate the MAC Tx_start, MAC Tx_end, MAC Rx_start, MAC Rx_end. These signals are transmitted by Base Stations and Repeaters. The specific MAC frame N is indicated in the BS data-base and these procedures will repeat after N_{cogn} MAC frames;
- During the MAC frame N+1, cognitive signals will indicate the beginning and the end of Master sub-frames, by transmitting signals indicating by their transmission start the Tx_start, Tx_end, Rx_start, Rx_end for the specific sub-frame; these signals are transmitted by Base Stations, Repeaters and those SSs which experiences interference, at intervals equal with N_{cog} MAC Frames;
- During the MAC frame N+2, will be indicated the position of the time-slots, in each Master sub-frame, to be used starting with the MAC Frame N+3 for registration using cognitive signaling. The start of the "Rx_slot" signal will indicate the start of the slot.
- The start of the MAC frame N+4 is the start of a registration interval using the cognitive signaling; the registration interval has the duration of Tcr_reg seconds; The ad-hoc transmitters shall use during the MAC frame N+4, the marked slot for sending their radio signature. The radio signature will be used for the evaluation of the potential interference during the Master slot, to systems which use the sub-frame as Master systems.
    - An ad-hoc radio unit (BS, Repeater or SS) will send this signal using a random access mode for Tcr_reg1 seconds, using the sub-frame intended for their regular transmission (BSs and SSs use different sub-frames for transmission).

- The ad-hoc transmitters will have to use the registration procedures every Tad_reg seconds.

— Registration replay

- The radio units using the Master sub-frame will send a NACK signal, to be sent in a random mode during the next Tcr_reg_ack seconds, if they appreciate that the ad-hoc transmitter will cause interference. Typically, to a registration signal sent during a DL sub-frame, the NAK will be sent by one or more SSs, while to a registration signal sent during UL sub-frame, the NACK signal will be sent by a Base Station. The radio units using the Master sub-frame will send their response in random mode.
- The NACK signal indicates that the requesting ad-hoc device cannot use the specific sub-frame, while using the requesting radio signature
- Same device may try again, if using a different radio signature (for example, lower power).
- Lack of response, for Tcr_reg_ack seconds, indicates that the registration is accepted for transmission during the specific sub-frame.

15.5.1.3 Selection of suitable reception sub-frames

An ad-hoc unit will find his suitable reception sub-frames, by using the ACS and Registration process in a repetitive way, searching for a suitable operation frequency. The practical interference situations, with synchronized MAC Frames are BS-SS and SS-BS interference. Assuming similar transmit powers, the above mentioned process will have as result finding Master sub-frames in which the path attenuation between interfering units is maximal.

15.5.1.4 Signaling procedures for Cognitive Radio applications

The signaling and message exchange between an ad-hoc system and systems using a Coexistence Protocol is done as detailed below:

— Split the narrowest channel to be used (as defined in 802.16 Profiles) into 32 energy bins, as follows:

- For 256FFT, to 8 sub-carriers/bin
- For 512 FFT, to 16 sub-carriers/bin
- For 1024FFT, to 32 sub-carriers/bin
- For 2048FFT, to 64 sub-carriers/bin.

— Send an 802.16h MAC message, at a suitable rate, such that the MAC header will use 1 symbol and the MAC PDU will use another symbol; the MAC header and the data field will be built in such a way that the power distribution for different bins will be with at least 5dB higher for a bin marked in Tablex with “H” than for bin marked with “L”.

The data field for both transmit and receive operations, taking into account possible FFT sizes, channel widths and the defined PHY modes, is defined in chap. t.b.d.

The following figures show the desired spectral density for cognitive signaling and the possible outcome of the MAC PDU approach, introducing some distortions in time or frequency domain, but still detectable by non-802.16 systems.

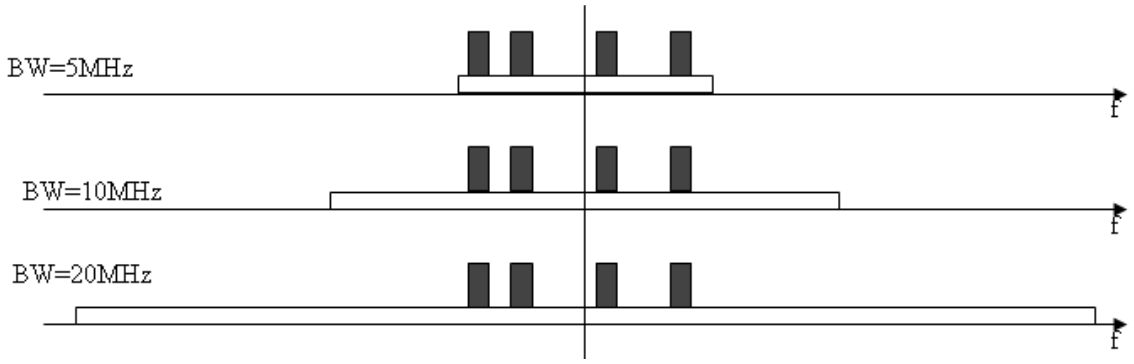

Figure h23—Desired spectral densities for different channel BWs

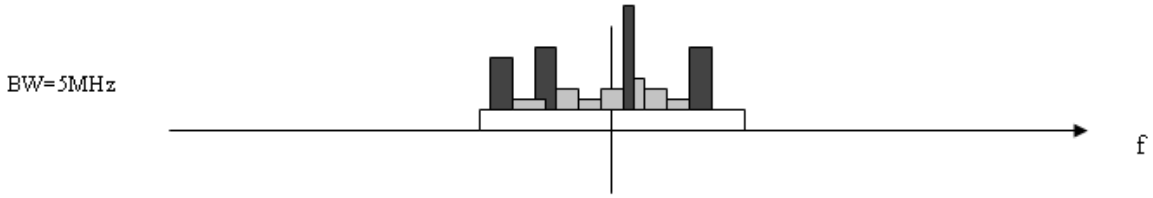

Figure h24—Obtainable spectral densities with MAC PDU approach

Due to the FFT guard sub-carriers, not all the bins are usable; we will use in continuation, from the bins numbered 0…31, where the bin#0 corresponds to the lowest frequency, only the bins 6…26. The MAC PDUs, having the spectral characteristics defined in the Table x, are defined in Chap. t.b.d for each of the 3 802.16 PHY modes.

In Table h 5 were defined a number of cognitive signals, having low inter-correlation properties. The energy on the not-used bins can take any value, but not more than the energy on a bin marked with "H". This tolerance will allow finding adequate data mapping for each PHY mode. Obviously, if the energy on not-used bins will be minimal, the detection process will be easier.

Table h5—Cognitive signal definition

Bin number /Signal number	6	8	10	12	14	18	20	22	24	26
1 (802.16h Cognitive MAC Header)	H	L	L	H	H	L	L	L	H	L
2 (Tx_start)	L	H	L	L	H	H	L	L	L	H
3 (Rx_start or Rx_slot)	H	L	H	L	L	H	H	L	L	L
4 (Tx_end)	L	H	L	H	L	L	H	H	L	L
5 (Rx_end)	L	L	H	L	H	L	L	H	H	L
6 (NACK)	L	L	L	H	L	H	L	L	H	H
7 (CTS_Start)	H	L	L	L	H	L	H	L	L	H
8 (CTS_Continuation)	L	H	H	L	L	H	L	H	L	L
9	L	L	H	H	L	L	H	L	H	L

[Note: 15.5.1.5 is provisional, taken from C80216h-05_032r1 and call for comments and further contribution]

15.5.1.5 Using the coexistence slot for transmitting the BS IP identifier

The cognitive radio signaling described above may be also used for the transmission of the BS IP identifier, when there is no installed Base Station Identification Server.

The transmission is done in consecutive coexistence time slots, every NIptx MAC frames. The first CTS in the series starts with CTS start signal, the last CTS contains the Tx_end signal, the continuation in sequential MAC frames starts with the CTS_Continuation, as defined in Table x. Between these signals is transmitted the IP identifier of the BS and a 8bit CRC, the L.S.B (least significant bit) for each field being transmitted first. The transmission of the above information uses only the bins 6,8,10,12,14,18,20,22,24,26 (10bits / symbol), the L.S.B. corresponding to the lowest frequency.

The transmission of a IPV4 address will request 1+ (32+8)/10 + 1 = 6 symbols and the transmission of a IPv6 address will request 1+ceil((128+8)/10) +1 = 16 symbols.

15.5.2 Recognition of other systems

15.6 Transmission of information

15.6.1 Coexistence Protocol (CP) messages (LE_CP-REQ/ LE_CP-RSP)

Coexistence Protocol employs two MAC message types: LE CP Request (LE_CP-REQ) and LE CP Response (LE_CP-RSP), as described in Table x.

Table h6—LE_CP MAC messages

Type Value	Message name	Message description
0	LE_CP-REQ	LE Coexistence Resolution and Negotiation Request
1	LE_CP-RSP	LE Coexistence Resolution and Negotiation Response

These MAC management messages are exchanged between peers, e.g. BS and BSIS or BS and BS or BS and SS., and distinguish between CP requests (BS -> BS/BSIS/SS or SS-> BS) and CP responses (BS/BSIS/ SS -> BS or SS->BS). Each message encapsulates one CP message in the Management Message Payload. Coexistence Protocol messages exchanged between the BS and BS or between BS and BSIS or between BS and SS shall use the form shown in Table h 7.

Table h7—LE_CP message format

Syntax	Size	Notes
CP _Message_Format() {		
Version of protocol in use	*4* bits	1 for current version
Code	8 bits	See Table h 8
Management Message Type	16bits	0-LE_CP-REQ 1-LE_CP-RSP
Length of Payload	*16*bits	

Confirmation Code	8 bits	0-OK/success 1-Reject-other 2-Reject-unrecognized-configuration-set-ting 3-Reject-unknow-action 4-Reject-authentication-failure 5-255 Reserved
Alignment	4 bits	
AssociationID	*??*bits	
CP Message Seq_ID	8 bits	
TLV Encoded Attributes	variable	TLV specific
}		

The parameters shall be as follows:

Version of protocol in use

This specification of the protocol is version 1.

Code

The Code is one byte and identifies the type of CP packet. When a packet is received with an invalid Code, it shall be silently discarded. The code values are defined in Table x.

Length of payload

The length of payload descript the length of payload in bytes .

CP Message Sequence Identifier (CP Message Seq_ID)

The CP Message Sequence Identifier field is one byte. A BS/BSIS uses the identifier to match a BS/BSIS response to the BS's requests. The BS shall increment (modulo 256) the Identifier field whenever it issues a new CP message. The retransmission mechanism relies on TCP. The Identifier field in a BS/BSIS's CP-RSP message shall match the Identifier field of the CP-REQ message the BS/BSIS is responding to.

Association identifier(Association ID)

For uniquely identifying an CP connection between a initiator and responder

An Association ID is a parameter used to uniquely assign or relate a response to a request. The association identifier used on the responder and initiator MUST be a random number greater than zero to protect against blind attacks and delayed packets.

When the initiator sends subsequent messages, it uses the responder's association identifier in the Association ID field; when the responder sends a message it uses the initiator's association identifier in the Association ID field.

Confirmation Code

The appropriate CC for the entire corresponding LE_CP-RSP.

Attributes

CP attributes carry the specific authentication, coexistence resolution, and coexistence negotiation data exchanged between peers. Each CP packet type has its own set of required and optional attributes. Unless explicitly stated, there are no requirements on the ordering of attributes within a CP message. The end of the list of attributes is indicated by the LEN field of the MAC PDU header.

Table h8—LE_CP message codes

Code	CP Message type	MAC Message Type	Protocol type	Direction
0	Reserved	—	—	—
1	Identify Coexistence Request	LE_CP-REQ	TCP	BSIS->BSIS
2	Identify Coexistence Response	LE_CP-RSP	TCP	BSIS->BSIS
3	CoNBR Topology Request	LE_CP-REQ	TCP	BS-> BSIS
4	CoNBR Topology Reply	LE_CP-RSP	TCP	BSIS->BS
5	Registration Request	LE_CP-REQ	TCP	BS-> BSIS
6	Registration Reply	LE_CP-RSP	TCP	BSIS->BS
7	Registration Update Request	LE_CP-REQ	TCP	BS-> BSIS
8	Registration Update Reply	LE_CP-RSP	TCP	BSIS->BS
9	De-registration Request	LE_CP-REQ	TCP	BS-> BSIS
10	De-registration Reply	LE_CP-RSP	TCP	BSIS->BS
11	Add Coexistence Neighbor Request	LE_CP-REQ	TCP	BS->BS
12	Add Coexistence Neighbor Reply	LE_CP-RSP	TCP	BS->BS
13	Update Coexistence Neighbor Request	LE_CP-REQ	TCP	BS->BS
14	Update Coexistence Neighbor Reply	LE_CP-RSP	TCP	BS->BS
15	Delete Coexistence Neighbor Request	LE_CP-REQ	TCP	BS->BS
16	Delete Coexistence Neighbor Reply	LE_CP-RSP	TCP	BS->BS
17	Get_Param_Request	LE_CP-REQ	UDP	BS->BS
18	Get_Param_Reply	LE_CP-RSP	UDP	BS->BS
19	Evaluate_Interference_Request	LE_CP-REQ	UDP	BS->BS
20	Evaluate_Interference_Reply	LE_CP-RSP	UDP	BS->BS
21	Work_In_Parallel_Request	LE_CP-REQ	UDP	BS->BS
22	Work_In_Parallel_Reply	LE_CP-RSP	UDP	BS->BS
23	Quit_Sub_Frame_Request	LE_CP-REQ	UDP	BS->BS
24	Quit_Sub_Frame_Reply	LE_CP-RSP	UDP	BS->BS
25	Create_New_Sub_Frame_Request	LE_CP-REQ	UDP	BS->BS(MC?)
26	Create_New_Sub_Frame_Reply	LE_CP-RSP	UDP	BS->BS
27	Reduce_Power_Request	LE_CP-REQ	UDP	BS->BS
28	Reduce_Power_Reply	LE_CP-RSP	UDP	BS->BS

29	Stop_Operating_Request	LE_CP-REQ	UDP	BS->BS
30	Stop_Operating_Reply	LE_CP-RSP	UDP	BS->BS
31	BS_CCID_IND	LE_CP-REQ	UDP	BS->BS
32	BS_CCID_RSP	LE_CP-RSP	UDP	BS->BS
33	SS_CCID_IND	LE_CP-REQ	UDP	BS->BS
34	SS_CCID_RSP	LE_CP-RSP	UDP	BS->BS
35	PSD_REQ	LE_CP-REQ	UDP	BS->BS
36	PSD_RSP	LE_CP-RSP	UDP	BS->BS
37	Channel Switch Negotiation Request	LE_CP-REQ	TCP	BS->BS
38	Channel Switch Negotiation Reply	LE_CP-RSP	TCP	BS->BS
39	Channel Switch Request	LE_CP-REQ	TCP	BS->BS
40	Channel Switch Reply	LE_CP-RSP	TCP	BS->BS
41-255	reserved			

Formats for each of the CP messages are described in the following subclauses. The descriptions list the CP attributes contained within each CP message type. The attributes themselves are described in *x.xx*. Unknown attributes shall be ignored on receipt and skipped over while scanning for recognized attributes. The BS/ BSIS shall silently discard all requests that do not contain ALL required attributes. The BS shall silently discard all responses that do not contain ALL required attributes.

[Note: The following security part is a temporary text adopted from contribution C802.16h-05/11r1 and is subject to further discussion. A call for comment from security experts is open to comment on this text.]

The following Type-Length-Value (TLV) types may be present in the CP payload depending on the Message_Type:

Table h9—TLV types for CP payload

Type	Parameter Description
tbc	Operator ID
tbc	BS-ID
tbc	BS GPS coordinates
tbc	BS IP Address
tbc	MAC Frame duration
tbc	Type of sub-frame allocation
tbc	MAC Frame number chosen for the Master sub-frame
tbc	Sub-frame number chosen for the Master sub-frame
tbc	Repetition interval between two Master sub-frames, measured in MAC-frames
tbc	Time shift from the Master sub-frame start of the Base Station radio-signature transmission
tbc	Duration information for the Base Station radio-signature transmission
tbc	Repetition information for the Base Station radio-signature transmission
tbc	Time shift from the Master sub-frame start of the Subscriber Station radio-signature transmission
tbc	Duration information for the Subscriber Station radio-signature transmission
tbc	Repetition information for the Subscriber Station radio-signature transmission
tbc	List of other used sub-frames, in the interval between two Master sub-frames
tbc	Slot position
Tbc	Country Code
Tbc	Operator contact - phone
Tbc	Operator contact – E-mail
Tbc	PHY mode
Tbc	Maximum coverage at Max. power

Tbc	Current Tx power

15.6.1.1 Identify Coexistence Request message

The BSIS requests to the foreign BSIS with geographical information of the requesting LE BS.

Code: 1

Attributes are show in Table x

Table h10—Identify Coexistence Request message attribute

Attribute	Contents
Operator identifier	The operator ID of the BSIS.
Country code	The country code of the BSIS
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Maximum coverage at Max. power	The maximum radius at maximum allowed/designed power that the BS intends to detect its coexistence neighbors.

15.6.1.2 Identify Coexistence Reply message

The BSIS responds to the foreign BSIS to Identify Coexistence Request with a Identify Coexistence Reply message.

Code: 2

The query results is in the format of Coexistence Neighbor Topology Parameter Set, each result will contain the attributes shown in Table x. Each BSID TLV indicates start of new result.

Table h11—Coexistence neighbor Topology Parameter Set

Attribute	Contents
BSID	The BSID of the requested BS.
Operator identifier	The operator ID.
Operator contact - phone	The phone number in ASCII string of the operator.
Operator contact – E-mail	The E-mail address in ASCII string of the operator.
Country code	The country code of the BS
PHY mode	The PHY modes of the requested BS.
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Maximum coverage at Max. power	The maximum radius at maximum allowed/designed power that the BS intends to detect its coexistence neighbors.

15.6.1.3 Coexistence Neighbor Topology Request message

This message is sent by the BS to the BSIS to request its coexistence neighbor topology with its geometric information.

Code: 3

Attributes are shown in Table x.

Table h12—Coexistence Neighbor Topology Request message attribute

Attribute	Contents
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Maximum Coverage at Max. power	The maximum radius at maximum power that the BS intends to detect its coexistence neighbors.

15.6.1.4 Coexistence neighbor Topology Reply message

The BSIS responds to the BS' to Coexistence neighbor Topology Request with a Coexistence neighbor Topology Reply message.

Code: 4

Specification of the query results of coexistence neighbor topology from BSIS specific parameters.

The query results is in the format of Coexistence Neighbor Topology Parameter Set, each result will contain the attributes shown in Table x. Each BSID TLV indicates start of new result.

Table h13—Coexistence neighbor Topology Parameter Set

Attribute	Contents
BSID	The BSID of the requested BS.
Operator identifier	The operator ID.
Operator contact - phone	The phone number in ASCII string of the operator.
Operator contact – E-mail	The E-mail address in ASCII string of the operator.
Country code	The country code of the BS
PHY mode	The PHY modes of the requested BS.
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Maximum coverage at Max. power	The maximum radius at maximum allowed/designed power that the BS intends to detect its coexistence neighbors.

15.6.1.5 Registration Request message

This message is sent by the BS to the regional LE DB to perform the registration.

Code: 5

Attributes are shown in Table h 14.

Table h14—Registration Request message attributes

Attribute	Contents
BSID	The BSID of the requested BS.
BS IP	The IP address of BS.
Operator identifier	The operator ID.
Operator contact - phone	The phone number in ASCII string of the operator.
Operator contact – E-mail	The E-mail address in ASCII string of the operator.
Country code	The country code of the BS
PHY mode	The PHY modes of the requested BS.
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Operational Range at Max. Power	The maximum operational radius of the BS at Max. power.

15.6.1.6 Registration Reply message

The BSIS responds to the BS' to Registration Request with a Registration Reply message.

Code: 6

No Attributes.

15.6.1.7 Registration Update Request message

This message is sent by the BS to the regional LE DB to update the registration.

Code:7

Attributes are shown in Table h 14.

15.6.1.8 Registration Update Reply message

The BSIS responds to the BS' to Registration update Request with a Registration update Reply message.

Code: 8

No Attributes.

15.6.1.9 De-registration Request message

This message is sent by the BS to the BSIS to perform de-registration.

Code: 9

Attributes are shown in Table h 15.

Table h15—De-registration Request message attributes

Attribute	Contents
BSID	The BSID of the request BS.

15.6.1.10 De-registration Reply message

The BSIS responds to the BS' to De-registration Request with a De-registration Reply message.

Code: 10

No Attributes.

15.6.1.11 Add Coexistence Neighbor Request message

This message is sent by the BS to the coexistence neighbor BS to request to add it to coexistence neighbor list.

Code: 11

Attributes are shown in Table h 16.

Table h16—Add Coexistence Neighbor Request message attributes

Attribute	Contents
BSID	The BSID of the requested BS.
BS IP	The IP address of requested BS.
Operator identifier	The operator ID.
Country code	The country code of the requested BS.
PHY mode	The PHY modes of the requested BS.
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.
Altitude	The altitude information of the BS.
Current Tx power	Current Tx power of the BS.
Operational Range	The operational radius of the BS.
PHY specific parameters	The PHY specific encodings.

15.6.1.12 Add Coexistence Neighbor Reply message

The BSIS responds to the BS' to Add Coexistence Neighbor Request with an Add Coexistence Neighbor Reply message.

Code: 12

No Attributes.

15.6.1.13 Update Coexistence Neighbor Request message

This message is sent by the BS to the coexistence neighbor BS to request to update its neighbor list.

Code: 13

Attributes are shown in Table h 17.

Table h17—Update Coexistence Neighbor Request message attributes

Attribute	Contents
BSID	The BSID of the requested BS.
PHY mode	The PHY modes of the requested BS.
Latitude	The latitude information of the BS.
Longitude	The longitude information of the BS.

Altitude	The altitude information of the BS.
Operational Range	The operational radius of the BS.
PHY specific parameters	The PHY specific parameters.

15.6.1.14 Update Coexistence Neighbor Reply message

The BSIS responds to the BS' to Update Coexistence Neighbor Request with an Update Coexistence Coexistence neighbor Reply message.

Code: 14

No Attributes.

15.6.1.15 Delete Coexistence Neighbor Request message

This message is sent by the BS to the coexistence neighbor BS to request to delete form its coexistence neighbor list.

Code: 15

Attributes are shown in Table h 18.

Table h18—Delete Coexistence Neighbor Request message attrubutes

Attribute	Contents
BSID	The BSID of the requested BS.

15.6.1.16 Delete Coexistence Neighbor Reply message

The BSIS responds to the BS' to Delete Coexistence Neighbor Request with a Delete Coexistence Neighbor Reply message.

Code: 16

No Attributes.

15.6.1.17 Get_Param_Request message

Messages between BSs, used to request the list of parameters

Code:17

Parameters: list of the BS parameters

15.6.1.18 Get_Param_Reply message

Messages between BSs, reply to the Get_Param_Request

Code:18

Parameters: list of the BS parameters

15.6.1.19 Evaluate_Interference_Request message

A message sent by a new BS wishing to use an existing Master sub-frame, to the BSs already acting as Masters, requesting them to evaluate its interference

Code:19

Parameters: tbc.

15.6.1.20 Evaluate_Interference_Reply message

A message sent by the existing Master BSs, reply to the Evaluate_Interference_Request.

Code:20

Parameters: tbc.

15.6.1.21 Work_In_Parallel_Request message

A message sent by a new BS to request the use an existing Master sub-frame

Code: 21

Parameters: tbc.

15.6.1.22 Work_In_Parallel_Reply message

A message sent by a existing Master BS in response to the Work_In_Paraller_Request message.

Code: 22

Parameters: tbc.

15.6.1.23 Quit_Sub_Frame_Request message

A message sent by an old Base Station, in order to request the new Base Station to cease the operation as Master in the current sub-frame

Code:23

Parameters: tbc.

15.6.1.24 Quit_Sub_Frame_Reply message

A message sent by an new Base Station, in response to the old Base Station's Quit_Sub_Frame_Request message.

Code:24

Parameters: tbc.

15.6.1.25 Create_New_Sub_Frame_Request message

A message sent by a BSs to all the community BSs, to request the creation of a new Master sub-frame; the message will include: interfering BSIDs and the frame-number in which the change will take place

Code:25

Parameters: tbc.

15.6.1.26 Create_New_Sub_Frame_Request message

A message sent in response to the Create_New_Sub_Frame_Request message.

Code:26

Parameters: tbc.

15.6.1.27 Reduce_Power_Request message

A message between a BS and an interfering BS requesting to reduce the power of the specified transmitter (identified by frame_number, sub-frame, time-shift) by P dB

Code: 27

Parameters: tbc.

15.6.1.28 Reduce_Power_Reply message

A message by an interfering BS in response to the Reduce_Power_Reply message.

Code: 28

Parameters: tbc.

15.6.1.29 Stop_Operating_Request message

A message sent by a Master BS to the BSs operating in its Master sub-frame, but not being Masters for this sub-frame, requesting to cease using this sub-frame in parallel

Code: 29

Parameters: tbc.

15.6.1.30 Stop_Operating_Reply message

A message sent by the BSs operating in its Master sub-frame,in response to the Stop_Operating_Request message.

Code: 30

Parameters: tbc.

15.6.1.31 BS_CCID_IND message

A message sent by BSs to indicate co-channel interference detected.

Code: 31

This is a message sent by a SS to CR_NMS when co-channel interference is detected at SS. This message shall contain the following minimum information to help determine the source and victim of co-channel interference:

- BS_NUM: total number of base stations from which CCI interference is detected.
- BS_ID: the base station IDs causing CCI
- Sector_ID: the sector IDs of the base stations causing CCI
- SS_ID: the SS that sent this message.

Essentially, this message will contain a table of co-channel interference sources for this SS.

Table h19—table of co-channel interference source for SS

Base station ID	Sector ID
123456	2
234534	4
…	…

15.6.1.32 BS_CCID_RSP message

A “set” message to BS.

Code: 32

This is a “set” message; it is to set the emission or reception qualities of the specified SS. Upon receiving co-channel interference notification, the algorithm in CR-NMS will determine an appropriate CCI mitigation decision and forward

This message to the victim SS.

SS_CCID_RSP can contain the following information for example:

SS_ID: the ID of subscriber station that causes/receives co-channel interference. It is the receiver of this message.

- EIRP for the specified SS. This is a reduced/increased EIRP value for this SS based on algorithm.
- Downlink/uplink frequency change.
- Reregistration request to a new BS
- Specification of allowable uplink timing slots.
- Adaptive antenna configuration parameters for reception/transmission.

15.6.1.33 SS_CCID_IND message

A message sent by SSs to indicate co-channel interference detected.

Code: 33

This is a message sent by a BS to CR_NMS when co-channel interference is detected at BS. This message shall contain the following information to help determine the source and victim of co-channel interference:

- SS_NUM: total number of subscriber stations that interference events were noted.
- SS_ID: the subscriber stations ID that causes the co-channel interference
- Sector_ID: the sector ID of the subscriber stations that cause interference
- Source basestation ID: the BS that sent this message.
- Source sector_ID: the antenna sector that detects the co-channel interference.

Essentially, this message will contain a table of co-channel interference sources for this BS.

15.6.1.34 SS_CCID_RSP message

A “set” message to SS.

Code: 34

This is a “set” message; it is to set the configuration of the BS. Upon receiving co-channel interference notification, the algorithm in CR-NMS will use this message to set the emission or reception qualities of the specified BS. It shall have the following information:

- BS_ID: Base station ID of Base Station receiving/causing interference. It is the receiver of this message.
- EIRP for the specified BS
- Downlink/Uplink frequency change.
- Adaptive antenna configuration parameters for reception/transmission.

15.6.1.35 PSD_REQ message

A”set” message to start PSD (power spectrum density) sampling

Code: 35

All co-channel interference that is created cannot necessarily be demodulated or decoded correctly, allowing the extraction of Tagged information from interference frames. Additionally, some users of license-exempt spectrum may not comply with any of the IEEE standards and be impossible to identify. In this event it is useful for a to be able to monitor the LE spectrum to determine available spectrum “white space” and determine sub-detection interference. “Snapshots” of spectrum space are useful to CR systems, especially when new base stations or terminals are installed and are searching for unoccupied spectrum.

This is a “set” message, it is requests a BS or SS to sample PSD (power spectrum density) data for next “get” message. Since sampling PSD data will take some time, depending on environment, nature of bursty users, the following “get” message shall wait long enough for BS/SS to complete the PSD data sampling.

There shall be only one scalar MIB object defined for this operation.

15.6.1.36 PSD_RSP message

A “get” message to get PSD (power spectrum density) data table.

Code: 36

This is a “get” response message, MIB objects shall be defined accordingly; it shall contain the following values for a complete PSD:

- Antenna Parameter List containing attributes of antenna undertaking PSD
- X-min, the lower bound of channel frequency (in kilohertz)
- X-max, the upper bound of channel frequency (in kilohertz)
- Resolution bandwidth
- Power spectrum density measurement

Resolution bandwidth is scalar, it is used together with X-max and X-min to determine how many PSD values are collected and contained in the STRUF_REP message (i.e.).

$$(X_{max} - X_{min}) / (resolutionBandwidth) + 1 \qquad (h2)$$

Upon reception of this message, CR_NMS will stamp the message based on the arrival time and translate the information into internal format and store it into database.

Here is an example of PSD display:

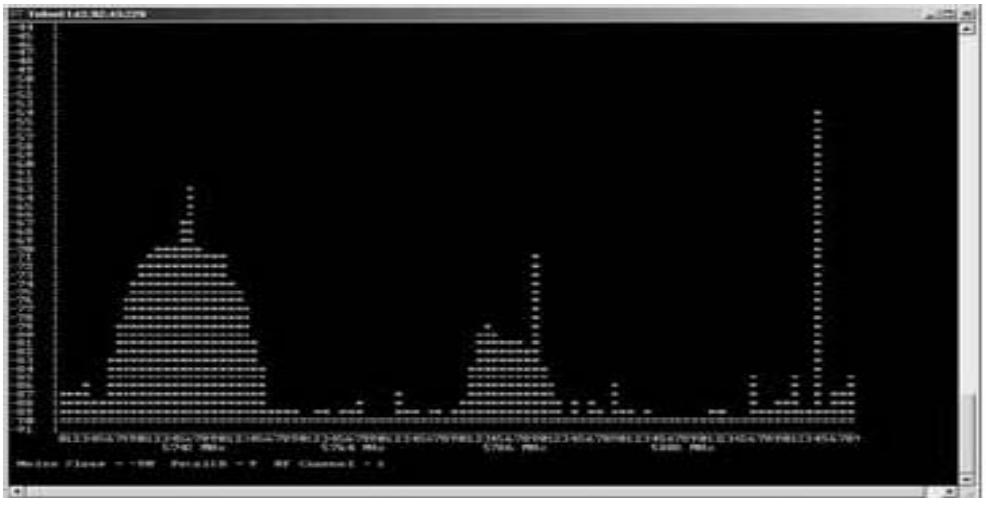

Figure h25—Example of PSD Display

15.6.1.37 Channel Switch Negotiation Request message

This message is send by BS to another coexistence BS in the community to negotiate to switch to a certain target channel.

Code: 37

Parameters: tbc.

15.6.1.38 Channel Switch Negotiation Reply message

A message sent by BS, reply to Channel Switch Negotiation Request message about whether it agree or refuse to switch.

Code: 38

Parameters: tbc.

15.6.1.39 Channel Switch Request message

This message is send by BS to another coexistence BS in the community to request to switch to a certain target channel.

Code: 39

Parameters: tbc.

15.6.1.40 Channel Switch reply message

A message sent by BS, reply to Channel Switch Request message.

Code: 40

Parameters: tbc.

[Note: the following part "RADIUS Protocol Messages" is from contribution C802.16-05/012r1, calling for comments, as all the security issues]

15.6.2 Sequencing and Retransmission

CP is a request-response protocol. In any particular message exchange, one party acts as the initiator (sends a request) and the other party acts as the responder (sends a response message).

The initiator sets the Message ID in the header to any value in the first message of the CP association, and increases the Message ID by one for each new request using serial number arithmetic. Retransmissions do not increment the Message ID. The responder sets the message ID in the response to the value of the message ID in the request.

The initiator is always responsible for retransmissions. The responder only retransmits a response on seeing a retransmitted request; it does not otherwise process the retransmitted request.

The retransmitted requests/responses are exact duplicates of previous requests/responses. The initiator must not send a new request until it receives a response to the previous one. Packets with out-of-sequence Message IDs are considered invalid packets and are discarded.

The initiator must retransmit after a configurable interval until either it gets a valid response, or decides after a configurable number of attempts that the CP association has failed. (Since the retransmission algorithm is implementation-dependent, it is not defined here.)

15.6.3 Message Validity Check

A message is only accepted if all the following holds true:

- Message version *field = 1*.
- Association ID must match a current association
- All messages received by peer have R bit in flag set to zero
- All responses received by authenticator have R bit in flag set to one.
- Message opCode is valid
- Message length equals size of payload
- Message ID must match the expected sequence number
- The payload contains only those TLVs expected given the value of the opCode
- *All TLVs within the payload are well-form*ed, TLVs marked as mandatory are recognized.

15.6.4 Fragmentation

CP does not provide support for fragmentation.

15.6.5 Transport Protocol

CP uses UDP as the transport protocol with port number[tbd.]. All messages are unicast.

15.6.6 Using dedicated messages

15.6.6.1 Common PHY

15.6.6.2 Between BS and SS

[Note: following 15.6.8.2.1 is provisional, taken from C80216h-05_029 and call for comments and further contribution]

15.6.6.2.1 IBS_IPBC

IBS_IPBC message is the message broadcasted by the initializing base station to the SS in the coexistence neighbor network. It use the CTS frame to carry the IP address information from the IBS to the SS, and the IP information shall be reported by the SS to the serving coexistence neighbor BS. And the serving coexistence neighbor BS will find the initializing BS in the IP network, and then start the further coexistence negotiation.

Table h20—IBS_IPBC message TLV encoding

Name	Type(1byte)	Length	Value (Variable length)
IPBC_V4	0	4	BS IP address(IPv4)
IPBC_V6	1	16	BS IP address(IPv6)

[Notes: The following paragraph need to be move into the SS_MEM and SSURF section:]

Two MAC messages are defined for use between the BS and SS. These messages are called “tags” since the tag the radio packet communication bursts which create co-channel interference

15.6.6.2.2 SS_MEM

The subscriber station membership (SS_MEM) message can be a new (or modified) MAC message for IEEE 802.16h FDD. The BS broadcasts a SS_MEM message in each RF sector at a periodic intervals, inserted within the DL MAC PDU. It defines the radio emission characteristics of the downlink of the sector, and provides information on uplink FDD channels utilized by the sector and could include channel width information as well. The message is encoded in the following format:

BS_ID	SECTOR_ID	DL EIRP	UPLINK RF	FRSEQ#	BS IP ADDRESS

Parameters:

— BS_ID: The base station ID. This information will help SS to determine which BS this message is received from. If it is not received from the home base station (it registered with), then it is co-channel interference caused by another BS downlink. In this case, a BS_CCID_IND message shall be send to Network Management System (CR_NMS) to indicate co-channel interference source and victim. Upon receiving this message, CR_NMS will initiate a response, which could access the CIS or be determined by the CR-NMS by itself, based on the SS_Mem contents.

— Sector_ID: Identifies the Sector antenna broadcasting this SS_MEM message. This information will help SS to determine which BS sector this message is received from. This could contain the GPS location, height of sector antenna, beamwidth of sector and direction of sector antenna, etc.

— DL EIRP: Down link EIRP of sector

— Uplink RF: Uplink RF frequency channels used by this sector

— FrSeq#: Frame sequence number

— BS IP address: IP address of the base station that broadcasts this message.

15.6.6.2.3 SSURF

— The subscriber station uplink radio frequency (SSURF) message shall be a modified (or new) MAC message for IEEE 802.16h. This message is periodically sent by SS as uplink tags, but could also contain interference and other event information experienced by the SS.

BS_ID	SECTOR_ID	FRSEQ#	APL	EIRP	GEOPL	CH_STATE

SSURF message fields are:

— BS_ID: The base station ID to identify which base station this message is sent to. This information will help receiving BS to determine if received packet is CCI. If BS_ID it is different from the receiving base station ID, co-channel interference has occurred with another SS uplink. In this case, a SS_CCID_IND message shall be send to Network Management System (CR_NMS) to indicate co-channel interference source and victim. Upon receiving this message, CR_NMS will, initiate a CR response, which could access the CIS or be determined by the CR-NMS by itself. A response could be based on the SSURF contents.

— Sector_ID: Identifies the destination sector antenna of this message. In essence, it is the same field as used in the SS_MEM message. Contains information, that if this packet is received as CCI, can to transported to a CR_NMS within the SS_CCID_IND message.

— FrSeq#: Frame sequence number.

— APL: Antenna parameter list giving information on antenna type (adaptive w/parameters; beam width, polarization, diversity, etc) of SS

— EIRP: EIRP of transmitted SSURF

— GeoPl: Geographical placement of SS, Range from associated BS, GPS coordinates, etc.)

— Ch_State: mean fade duration, mean fade depth, variance of DL signal strength, Bit Error Rate mean, Bit Error Rate Variance, RSSI mean, RSSI variance, etc.

Upon reception of this message, BS will stamp the message based on the arrival time and translate the information into internal format for construction of a SS_CCID_IND message.

15.6.6.3 BS to BS

15.6.6.4 Connection sponsorship

15.6.6.5 Using a common management system

15.6.6.6 Higher layers communication

15.6.6.7 Decentralized control

15.6.6.8 Information sharing

15.6.6.9 IP / MAC address dissemination

15.7 Common policies

15.7.1 How to select a “free” channel (for ACS and DFS)

BS should listen on multiple frequencies during the selection of working frequency. If the interference’s level is greater than the detection threshold, which is the required strength level of a received signal within the channel bandwidth, the channel is considered as a interfered channel. If IBS can’t find a “free” channel by scanning, it should figure out whether an indirect “free” channel can be found by optimized channel distribution, as described in 15.7.1.4.

Process of ACS is shown in Figure h35. ACS results two kinds of resolution, a “free” channel found with or without channel switching, or no “free” channel found.

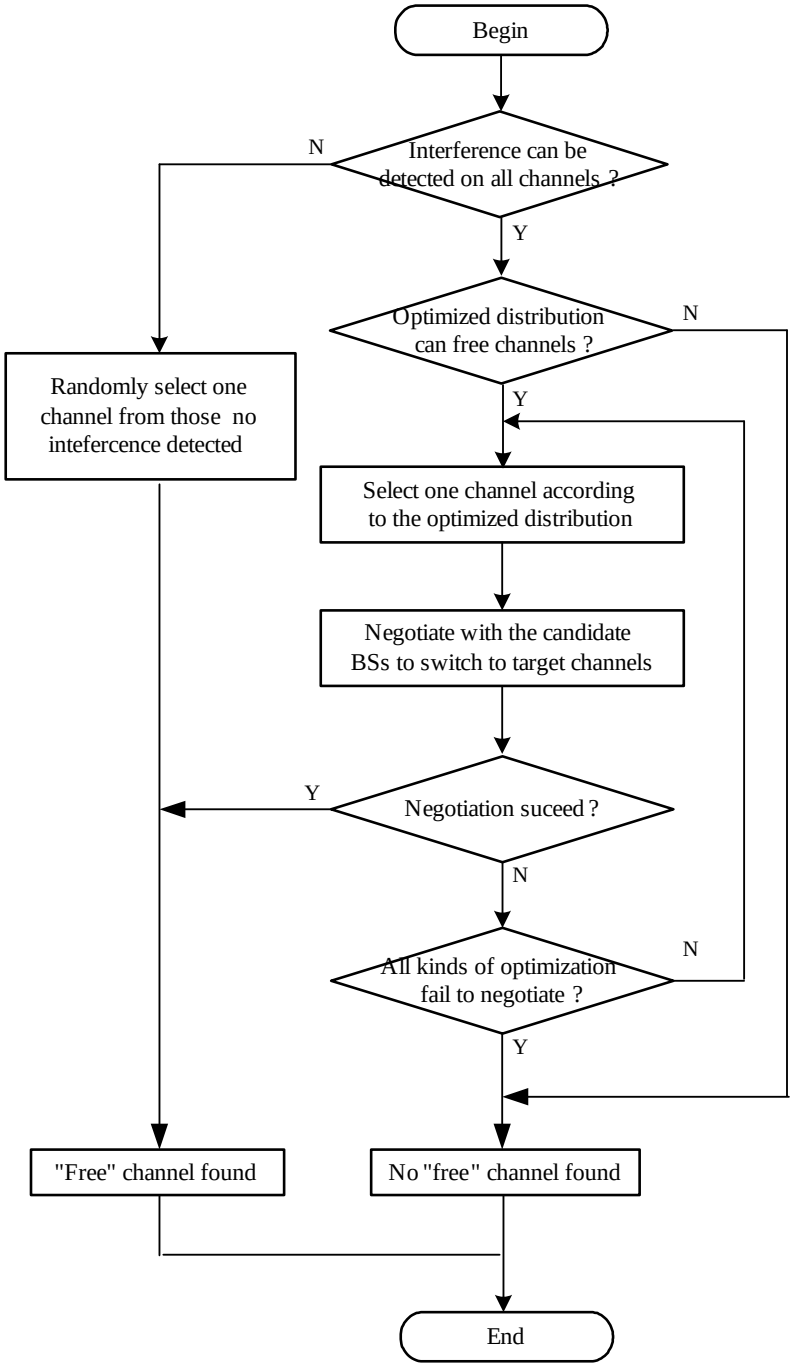

Figure h26—Process of ACS

If a “free” channel found, means default interference-free Master slot is available, otherwise, IBS need to share the channel with coexistence neighbors, as described in 15.2.1.7.

15.7.1.1 Acceptable S/(N+I)

15.7.1.2 Acceptable time occupancy

15.7.1.3 Capability of sharing the spectrum

15.7.1.4 Optimization of Channel Distribution

15.7.2 Interference reduction policies

15.7.2.1 BS synchronization

15.7.2.1.1 Synchronization of the IEEE 802.16h Networks

All base stations forming a community of users sharing common radio spectrum will use a common clock to synchronize their MAC frames. The common clock will be available to all outdoor IEEE 802.16h networks. Such a clock can be provided by global navigational systems such as GPS (Annex 2) or can be distributed by other mean . Every BS upon activation, will as a first step ensure the derivation of the common system clock.

15.7.2.1.1.1 Network Time Interval

All synchronized IEEE 802.16h base stations will either synthesize or derive a 1 pps clock broadcast by a global navigational system or other means. The 1 sec duration is called the Network Time Interval (NTI). The rising edge of the 1 pps synchronization pulse will be considered as the start of the NTI. The 1pps pulse will have a stability of +/- 100 XX microseconds, as measured from rising edge to rising edge.

15.7.2.1.1.2 Granularity of the NTI

The NTI will be comprised of 1000 1 Millisecond slotsNTI_S unit that will be used by both TDD and FDD networks to negotiate times and durations of co-channel occupancy. Negotiation for access time to common spectrum will be specified in terms of the NTI_S unit 1 millisecond units. Occupancy times will be specified in terms of time from the beginning of the NTI and in terms of negotiated number of NTI_S unit1 millisecond intervals.

15.7.2.1.1.3 UTC Standard Time

The common clock specified in 15.7.2.1.1 will provide a Universal Coordinated Time (UTC) signal to all IEEE802.16h networks, making all networks synchronized to this referenced time stamp. IEEE 802.16h base stations will use the UTC time standard for coordinating and identifying specific NTI intervals.

15.7.2.1.2 Ad-hoc

15.7.2.2 Shared Radio Resource Management

15.7.2.2.1 Fairness criteria

15.7.2.2.1.1 Power control

15.7.2.2.1.2 Mutual tolerance

15.7.2.2.2 Distributed scheduling

15.7.2.2.2.1 Assignments

15.7.2.2.3 Distributed power control

15.7.2.2.4 Distributed bandwidth control

15.7.2.2.5 Beam-forming

15.7.2.2.6 Credit token based coexistence protocol

Spectrum sharing between several networks (NW) can be achieved through the sharing of a common MAC frame between the different NWs as exampled by Figure h 27. In such a MAC frame structure, dedicated portions (denoted as “master NW sub-frames”) of the frame are periodically and exclusively allocated to a NW (denoted as the “master NW”) respectively in the forward and reverse link. The terminology used here-after defines a slave NW as a NW that may operate during the other master NWs sub-frames. With respect to this definition, the slave NW sub-frames are the time intervals operating in parallel of the master NWs sub-frames.

Additional flexibility can be provided by such a frame structure if The length of each master sub-frame(interference free sub-frame) can be dynamically adjusted as a function of the spatial and temporal traffic load variations of each NWas stated in section 15.2.1.1.1.

To achieve this, this section proposes the dynamic coordination of the frame structure sharing between BSs when several master NWs compete to share this common shared MAC frame.

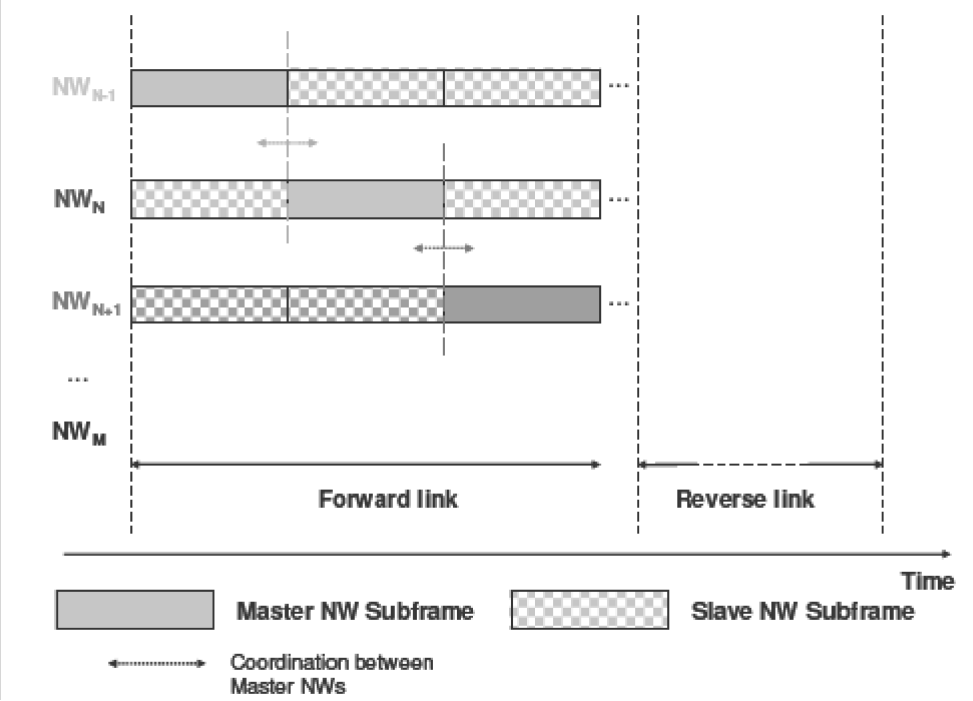

Figure h27—Example of TDD based MAC frame sharing structure between M NWs

15.7.2.2.6.1 General principle

In order to solve contention access channel and resources scheduling issues between NWs, the first step consists in defining credit tokens and designing appropriate reserve price auctioning and bidding mechanisms. Then, on the basis of the credit tokens based mechanisms usage, the second step consists in managing dynamically(temporally) the bandwidthrequests and grants mechanisms for the sharing of the master sub frames within the common MAC frame.

Based on the credit tokens transactions (selling, purchase and awarding), these two steps provide the mechanisms to enable spectrum efficiency and a fair spectrum usage in a real time fashion, while ensuring both the master and slave NWs QoS. These two steps enable to manage spectrum sharing between master NWs themselves. The result is the dynamic shaping of the MAC frame structure sharing as a function of the space time traffic intensity variations, and the dynamic credit tokens portfolio account of the master NWs. The transaction mechanisms are detailed in the following sections.

15.7.2.2.6.2 Credit tokens assignment and usage principles

— Each NW is initially allocated with a given credit tokens account.

— Negotiation for spectrum sharing between NWs is based on credit tokens transactions.

— Credit tokens transactions occur dynamically between a seller (master NW owner of the radio resources during the active master sub-frame) and one or several bidders (the other master NWs).

— The negotiation occurs dynamically between master NWs to agree the length of each master sub-frame as a function of the spatial and temporal traffic load variations need of each master NW.

15.7.2.2.6.3 Negotiation between master NWs

15.7.2.2.6.3.1 Definition and notation

— BSN denotes the BS belonging to the master NWN.

— BSk denotes the BS belonging to the slave NWk.

— Each BSk can dynamically make a bid BS_CT(n)k at the nth iteration. This bid corresponds to the amount of credit tokens per time unit corresponding to the BSk during the nth iteration of the auctioning/bidding phase.

— Resource scheduling is carried out by an auction like mechanism. The auction type used for the scheduling is dynamic in time. Starting from the reserved price auction RPA, the price of auction is successfully raised (at each iteration n) until the winning bidders remain.

15.7.2.2.6.3.2 Dynamic credit tokens based scheduling cycle

The contribution proposes a dynamic scheduling cycle between one BSN of master NWN and several BSk of different slave NWk. For the sake of simplicity, the cycle is illustrated (Figure 1 and Figure 2) for one BSN and one BSk of a given slave NWk. The cycle is composed of different phases, and each phase can be composed of several sequences as follows.

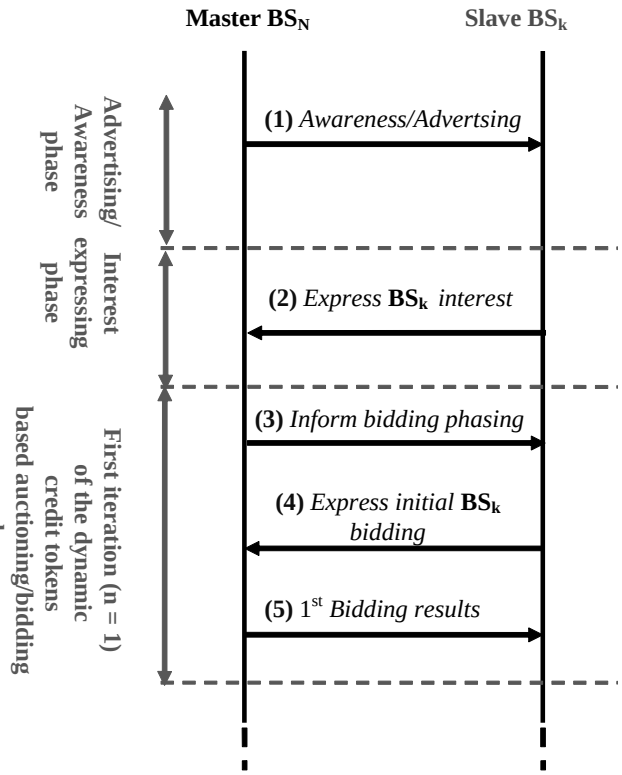

Figure h28—Dynamic (iterative) credit tokens based scheduling cycle – (sequences (1) to (5))

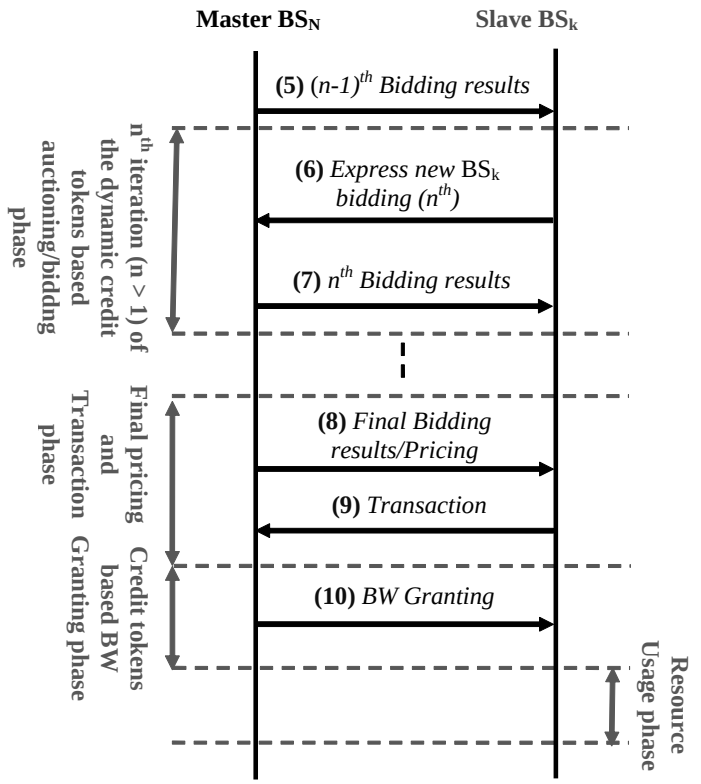

Figure h29—Dynamic (iterative) credit tokens based scheduling cycle – (sequences (5) to (10))

15.7.2.2.6.3.3 Negotiation mechanisms between master NWs

For each of the phase of the credit tokens based scheduling cycle presented in section 15.7.2.2.6.3.2, this section 15.7.2.2.6.3.3 describes the details of the enhanced mechanisms.

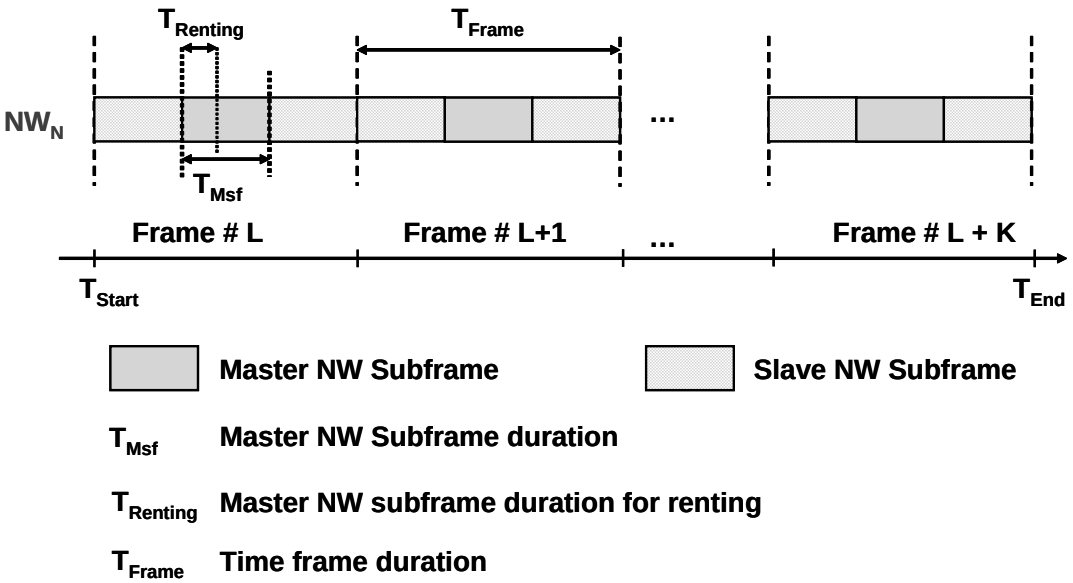

Figure h30—Simplified MAC frame structure illustrating master NW sub-frame renting principle and associated notations

Advertising/Awareness phase

This phase is composed of the single sequence (1) as follows:

— The master NW_N (seller) advertises that its periodic assigned master sub-frame is open for renting (Figure h34) from starting time $\mathbf{T_{Start}}$ to ending time $\mathbf{T_{End}}$ for a fraction ($\mathbf{T_{Renting}}/\mathbf{T_{Msf}}$) of its master sub-frame duration $\mathbf{T_{Msf}}$. $\mathbf{T_{Renting}} = \mathbf{T_{End\ Renting}} - \mathbf{T_{Start\ Renting}}$.

— The master NW_N proposes a reserve price auction **RPA** for this renting. The **RPA** is expressed as a number of credit tokens per time unit.

Interest expressing phase

This phase is composed of the single sequence (2) as follows: each BSk informs the master BSN about its willingness (or not) to participate to the bidding. If the BSk is interested, it communicates its idk to the master BSN.

First iteration (n = 1) of the credit tokens based auctioning/bidding phase

This phase is divided into 3 sequences as follows:

— In sequence (3), the master BS_N provides the following information to the slave BS_ks that have expressed the interest to participate to the bidding:

  o $\mathbf{T_{Start\ Bidding}}$: time from which the bidding phase will start,

  o $\mathbf{T_{End\ Bidding}}$: time at which the bidding phase will end ($\mathbf{T_{End\ Bidding}} < \mathbf{T_{Start}}$),

  o Note: For this first iteration (n = 1), the initial $\{\mathbf{id_k}\}$ is noted $\{\mathbf{id^{(1)}_k}\}$.

— In sequence (4), each BS_k provides the following information to BS_N: $\mathbf{BID^{(1)}_k} = \{\mathbf{BS\_CT^{(1)}_k}, \mathbf{x_k}, \mathbf{T_{Start\ k}}, \mathbf{T_{End\ k}}\}$ where:

  - $\mathbf{BS\_CT^{(1)}_k}$ is the amount of bided credit tokens per time unit proposed by BS_k for the first iteration,
  - x_k is the fraction of $T_{Renting}$ for which bid $\mathbf{BS\_CT^{(1)}_k}$ applies for,
  - $[T_{Start\ k}, T_{End\ k}]$ is the time interval for which bid $\mathbf{BS\_CT^{(1)}_k}$ applies for. $[\mathbf{T_{Start\ k}}, \mathbf{T_{End\ k}}] \subset [\mathbf{T_{Start}}, \mathbf{T_{End}}]$.

— In sequence (5), BS_N performs the following action:

  - Given the set of intervals $\{[\mathbf{T_{Start\ k}}, \mathbf{T_{End\ k}}]\}$ received from different bidders $\{\mathbf{id^{(1)}_k}\}$, BS_N partitions $\{[\mathbf{T_{Start}}, \mathbf{T_{End}}]\}$ into contiguous time segments $\{\mathbf{TS_m}\}$. Each $\mathbf{TS_m}$ corresponds to a time window (integer number of $\mathbf{T_{Frame}}$) in which a subset of intervals of $\{[\mathbf{T_{Start\ k}}, \mathbf{T_{End\ k}}]\}$ overlap.
  - The different bidders $\{\mathbf{id^{(1)}_k}\}$ assigned to a given $\mathbf{TS_m}$ are identified by $\{\mathbf{id^{(1)}_{k,m}}\}$. $\{\mathbf{id^{(1)}_{k,m}}\}$ compete for each $\mathbf{TS_m}$. Each involved bidder $\mathbf{id^{(1)}_{k,m}}$ competes with his respective $\mathbf{BID^{(1)}_k}$.
  - Then, for each $\mathbf{TS_m}$, the master BS_N calculates the payoff $\mathbf{P^{(1)}_k} = \mathbf{BS\_CT^{(1)}_k} * \mathbf{x_k} * \mathbf{T_{Renting}} * \mathbf{N_{Frame\ m}}$ for each bidder k, and searches the subset $(\{\mathbf{id^{(1)}_{k,m}}\}_{selected})$ of $\{\mathbf{id^{(1)}_{k,m}}\}$ such as $sum(\mathbf{x_k}) = \mathbf{1}$ and $sum(\mathbf{P^{(1)}_k})$ is maximal. $\mathbf{N_{Frame\ m}}$ is the number of frames within $\mathbf{TS_m}$ ($\mathbf{N_{Frame\ m}} = \mathbf{TS_m}/\mathbf{T_{Frame}}$).
  - For each $\mathbf{TS_m}$, BS_N informs all $\{\mathbf{id^{(1)}_{k,m}}\}$ about $\mathbf{P^{min,\ (1)}_m}$ and $\mathbf{P^{max,\ (1)}_m}$ where $\mathbf{P^{min,\ (1)}_m}$ is the minimal payoff from $\{\mathbf{id^{(1)}_{k,m}}\}_{selected}$ and $\mathbf{P^{max,\ (1)}_m}$ is the maximal payoff from $\{\mathbf{id^{(1)}_{k,m}}\}_{selected}$ during the first iteration. With this approach, each BS_k is directly informed whether it has been selected or not, and has some information on how far it is from $\mathbf{P^{min,\ (1)}_m}$ while still having some information on $\mathbf{P^{max,\ (1)}_m}$. This approach enables to keep the privacy of competing $\{\mathbf{id^{(1)}_{k,m}}\}$ on $\mathbf{TS_m}$.

n^{th} iteration of the credit tokens based auctioning/bidding phase

This phase is composed of 2 sequences as follows:

— In sequence (6):

  - If $\mathbf{P^{(1)}_k} < \mathbf{P^{min,\ (1)}_m}$, this means that BS_k has not been selected for being granted the resources he has bided for during the first iteration n = 1. More generally speaking, for n>1, if $\mathbf{P^{(n-1)}_k} < \mathbf{P^{min,\ (n-1)}_m}$, this means that BS_k has not been selected for being granted the resources he has bided for during the $(n-1)^{th}$ iteration.
  - If $\mathbf{P^{(n-1)}_k} < \mathbf{P^{min,\ (n-1)}_m}$ and if BS_k is still interest to be allocated with the additional resources he initially requested for, it can propose a new $\mathbf{BS\_CT^{(n)}_k}$ for the n^{th} iteration. Then, BS_k computes the new $\mathbf{P^{(n)}_k} = \mathbf{BS\_CT^{(n)}_k} * \mathbf{x_k} * \mathbf{T_{Renting}} * \mathbf{N_{Frame\ m}}$ where $\mathbf{x_k}$,$\mathbf{T_{Renting}}$ and $\mathbf{N_{Frame\ m}}$ are fixed for all n on $\mathbf{TS_m}$.
  - If $\mathbf{P^{(n)}_k} > \mathbf{P^{(n-1)}_k}$ and $\mathbf{P^{(n)}_k} > \mathbf{P^{min,\ (n-1)}_m}$, BS_k expresses its interest to keep on participating in the bidding with the new bid $\mathbf{P^{(n)}_k}$. In that case, it informs BS_N with its new (update) value of $\mathbf{BS\_CT^{(n)}_k}$. In case $\mathbf{P^{(n)}_k} = \mathbf{P^{(n-1)}_k}$ or $\mathbf{P^{(n)}_k} < \mathbf{P^{min,\ (n-1)}_m}$, BS_k leaves the bidding phase and will not be granted with the additional resources he asked for.

— In sequence (7), BS_N updates $\{\mathbf{id^{(n-1)}_{k,m}}\}$ into $\{\mathbf{id^{(n)}_{k,m}}\}$. Based on the new received biddings $\{\mathbf{BS\_CT^{(n)}_k}\}$ for each $\mathbf{TS_m}$, the master BS_N calculates the new payoff $\mathbf{P^{(n)}_k} = \mathbf{BS\_CT^{(n)}_k} * \mathbf{x_k} * \mathbf{T_{Renting}} * \mathbf{N_{Frame\ m}}$ for each bidder k who still participates to the bidding. Then, for each $\mathbf{TS_m}$,

BS_N searches the subset ($\{\mathbf{id^{(n)}_{k,m}}\}_{selected}$) of $\{\mathbf{id^{(n)}_{k,m}}\}$ such as sum($\mathbf{x_k}$) = **1** and sum($\mathbf{P^{(n)}_k}$) is maximal. Next, BS_N performs the same actions as in sequence (5): for each $\mathbf{TS_m}$, BS_N informs all $\{\mathbf{id^{(n)}_{k,m}}\}$ about $\mathbf{P^{min,\ (n)}_{\ m}}$ and $\mathbf{P^{max,\ (n)}_{\ m}}$ where $\mathbf{P^{min,\ (n)}_{\ m}}$ is the minimal payoff from $\{\mathbf{id^{(n)}_{k,m}}\}_{selected}$ and $\mathbf{P^{max,\ (n)}_{\ m}}$ is the maximal payoff from $\{\mathbf{id^{(n)}_{k,m}}\}_{selected}$ during the n^{th} iteration.

Final pricing and credit tokens transaction phase

This phase is composed of two sequences as follows:

— In sequence (8):

  o As long as $\mathbf{T_{End\ Bidding} - T_{Start\ Bidding}} > 0$ (i.e. the bidding phase duration has not yet elapsed), n is increased and the credit tokens based bidding phase mechanisms of the previous paragraph "***n^{th} iteration of the credit tokens based auctioning/bidding phase***" are applied.

  o When $\mathbf{T_{End\ Bidding} - T_{Start\ Bidding}} = 0$, bidding phase is over. None BS_k can propose a new bid. $\{\mathbf{id^{(n\ final)}_{k,m}}\}_{selected}$ is derived. At this point, BS_N derives the clearing price auction $\mathbf{BS\_CPA_k}$ (expressed as a number of credit tokens per time unit) for each $\mathbf{TS_m}$ and each k from $\{\mathbf{id^{(n\ final)}_{k,m}}\}$. For each k and m, $\mathbf{BS\_CPA_k}$ can correspond to the $\mathbf{BS\_CT^{(final)}_k}$, or for example can follow another price auction method.

— In sequence (9), eack BS_k is requested to pay $\mathbf{Pr_k} = \mathbf{BS\_CPA_k} * \mathbf{x_k} * \mathbf{T_{Renting}} * \mathbf{N_{Frame\ m}}$ to be allowed to use the resources it won on its corresponding $\mathbf{TS_m}$. Provided that $\mathbf{Pr_k}$ does not exceed the credit tokens account of BS_k, the token transaction between BS_N and each BS_k is performed.

Credit tokens based bandwidth granting phase

This phase is composed of the single sequence (10). During this phase, BS_N grants the resource to each BS_k who has successfully performed the credit transaction operation in sequence (9).

Resource usage phase

After BS_k has been granted with the resources, BS_k can use them during during $\boldsymbol{x_k * T_{Renting}}$ time unit of NW_N and for $\mathbf{N_{Frame\ m}}$ frames from the beginning on its corresponding $\mathbf{TS_m}$.

15.7.2.2.6.4 Inter BSs communication

The above mechanisms require inter BSs communication between different NWs. This inter BS communications is necessary to exchange the parameters related to the *Advertising phase,* the *Admissible co-channel interference control phase* and the *Auctioning/bidding phase.* It is assumed that these parameters are stored into the regional LE DB and into the local database of each LE BS. The information exchange between these databases and the RADIUS/BSIS servers can be either supported by secured over the air signalling, or by IP communication between the networks.

15.7.2.2.7 Legitimate Request for Bandwidth and Transmission Time

An IEEE 802.16h network that is a member of a community of networks granted access to shared spectrum resources only if it forms an actual network comprised of at least one base station and one subscriber station and supports a bi-directional link.

15.7.2.2.8 Coverage Area

15.7.2.2.9 Direction of Coverage Area

15.7.2.2.10 Bandwidth Utilization

Annexes

Annex A

(informative)

Machanism of security in coexistence –reference

A.1 General Principal

The access to Data Bases is secured by authentication and possibly encryption

[Note: the security part is a temporary text adopted from contribution C802.16h-05/11r1 and 802.16h is calling for comments]

Figure h A1 shows the IEEE 802.16 LE inter-network communication architecture:

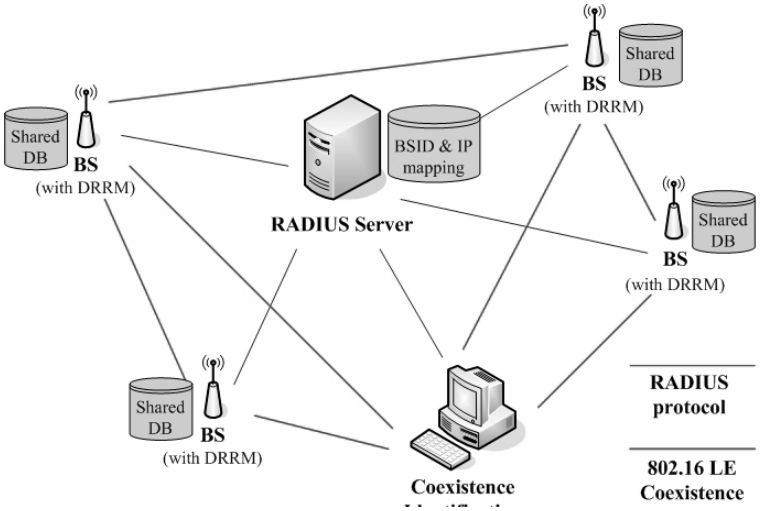

Figure h-A1—Network Architecture

General architecture includes the components operating over IP-based network:

- The RADIUS Server- The Base Station Identification Server (BSIS), described in detail in section xxx - The BSs cooperating with the Distributed Radio Resource Management (DRRM) procedureRADIUS server performs two primary functions. The first one is to authenticate 802.16 LE BSs and BSIS. Keyed-Hashing for Message Authentication (HMAC) with Message Digest 5 (MD5) (RFC2869:2000) is adopted for authentication. The second one is to maintain the address mapping of wireless medium addresses of BSs (their BSID) and medium addresses of BSIS to their IP addresses. This mapping is to distribute the keys for ESP used by BSs belonging to different networks.

BSIS maintains the geographic and operational information such as latitude, longitude and the BSID of LE BSs within certain management domain. BSs operating under LE system shall first query the foreign BSISs which are geographically close to the local BSIS and find the coexistence neighbor BSs while starting up, following the Coexistenceprotocol (detailed description in section 15.2.2.3). After the successful query procedure, the BS can obtain the BSIDs of the coexistence neighbor BSs. Intercommunication between BSs belonging to different networks is permitted after the BS acquires coexisting neighbor's Pairwise Masterkey. and PMK-index for ESP.

Considering the IP network firewalls and different filtering rules, we should find a common security solution to make BSs/BSISs data connection transparent under almost common network management cases. IPSec is used to IPv4 and also included in IPv6 for the IP-Layer security solution. And all BSs/BSISs don't just reside in the same network environment. The data connections should go through some routers/firewalls and need to follow a common security rules.

Figureh15 shows the BSs/BSISs connections encrypted in IPSec. Based on IPSec, all data connections between BSs/BSISs could pass through firewalls and routers unless some firewalls block IPSec connections.

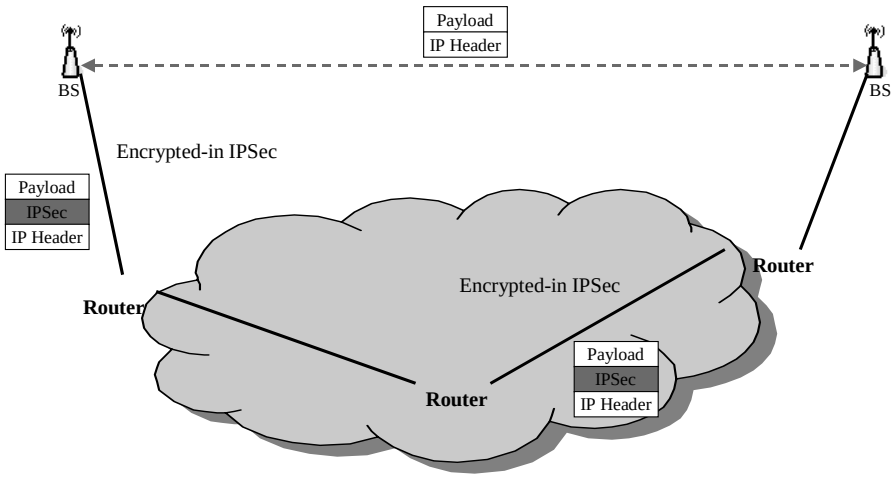

Figure h-A2—BSs/BSISs connection encrypted in IPSec

Figure h15 demonstrates the IEEE 802.16 LE inter-network communication architecture under multi-Operators with multi-RADIUS Servers.

If BS-1 wants to communicate with BS-2, it must get BS-2's Country's Code, Operator ID and BSID from local BSIS first. And then work as the following steps

(1) BS-1 send RADIUS-Access-Request frame with BS-2's Country's Code, Operator ID and BSID to local RADIUS-Server

(2) Local RADIUS-Server will act as RADIUS-Proxy and transfer this RADIUS-Access-Request to the target RADIUS-Server

(3) Target RADIUS-Server will response RADIUS-Access-Accept with Pairwise-Master-Key and PMK-index for BS-1 and Security-Block for BS-2

(4) Local RADIUS-Server will generate Security-Block including Pairwise-Master-Key and PMK-index from target Raidus-Server

(5) BS-1 will receive RADIUS-Access-Accept from its local RADIUS-Server and get the Pairwise-Master-Key PMK-index and ESP Authentication/Transform IDs in Security-Block for BS-1

(6) BS-1 will act as a PKM-initiator to send Session-Key-Start to BS-2 with Security-Block for BS-2

(7) BS-2 will calculate the ESP-Key-Stuffs with Pairwise-Master-Key, choose the ESP Authentication/ Transform IDs supported by BS-2 and response Session-Key-Request to BS-1

(8) BS-1 will also calculate the ESP-Key-Stuffs with Pairwise-Master-Key to verify Key-Signature, compare ESP Authentication/Transform IDs support by BS-2 with current settings supported by BS-1 and response Session-Key-Response to BS-2

(9) BS-2 will verify Key-Signature and response Session-Key-Accept to BS-1

(10) After the above procedures, BS-1 and BS-2 could communicate in IPSec with the ESP-Key-Stuffs generated dynamically

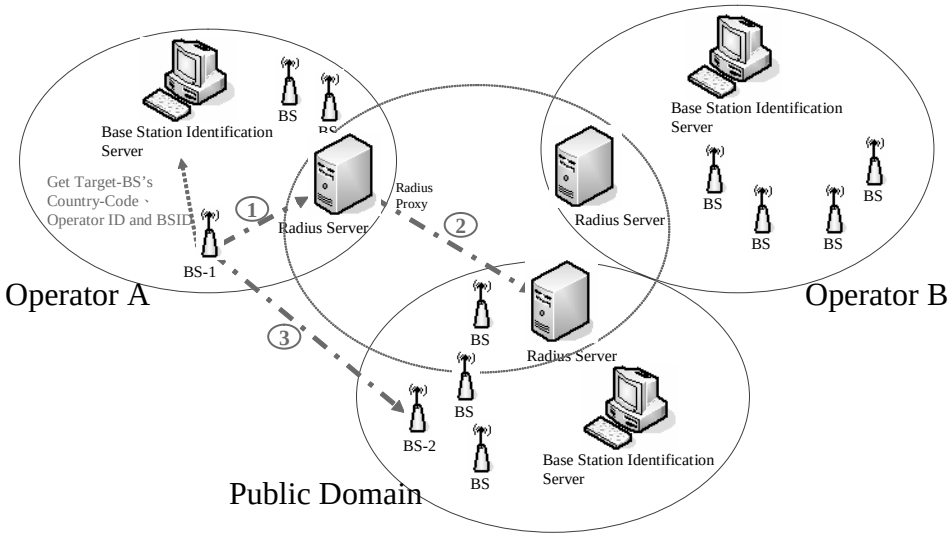

Figure h-A3—Network Architecture under multi-Operators with multi-RADIUS Servers

The following figure shows the each connection of BSs/BSISs will be encrypted in individual Session-Key in IPsec

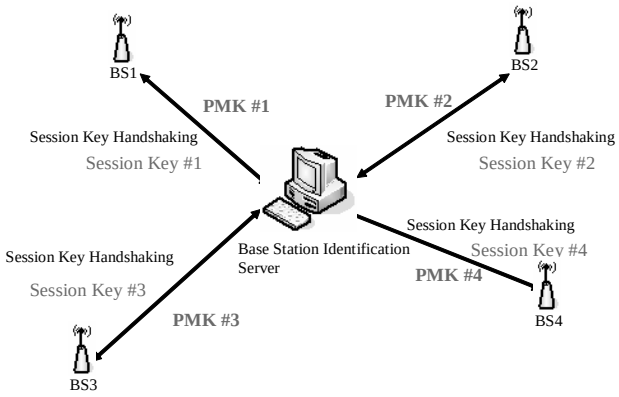

Figure h-A4—Individual Session-Key

For the BSs/BSISs, each connection with different BSs/BSISs will use individual Session-Key in IPsec. Those Session Keys would be generated from PKM-Handshaking with Pairwise-Master-Keys between each pair BSs/BSISs. The re-key procedures also don't need RADIUS-Servers and just use Pairwise-Master-Keys.

A.2 Coexistence Protocol

[Note: the security part is a temporary text adopted from contribution C802.16h-05/11r1 and is subject to further discussion.]

In order to get the coexistence neighbor topology, perform registration to the database and registration to peer, negotiation for Shared RRM etc. will be used a Coexistence Protocol (CP). Figure h A5 describes the 802.16h protocol architecture. The protocol architecture indicates that DRRM, Coexistence Protocol and Shared DB belong to LE Management Part located in management plane and the messages will be exchanged over IP network. Thus, DRRM in LE Management Part uses the Coexistence protocol to communicate with other BSs and with Regional LE DB and interact with MAC or PHY. Figure h A5 is LE BS architecture with Coexistence Protocol. The gray area indicates area where there is an absence of connection between blocks. DSM is Distribution System Medium which is another interface to the backbone network. Note that is architecture is only for reference. Similarly, Figure h A5 is the BSIS architecture with co-located regional LE database. Other architectures are not being illustrated. The Coexistence Protocol services are accessed by the LE Management Entity through CP SAP. The service primitives are described in t.b.d A BS uses the Coexistence Protocol, which is similar to PKM protocol, to perform the coexistence resolution and negotiation procedures. There are two types of messages to support Coexistence Protocol:

(1) LE_CP-REQ: BS->BS or BS->BSIS

(2) LE_CP-RSP: BS->BS or BSIS->BS

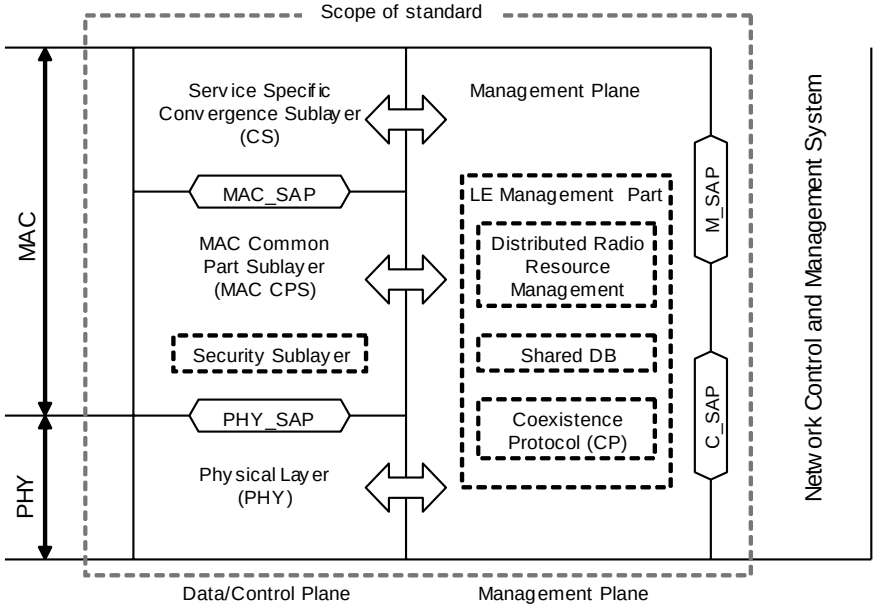

Figure h-A5—802.16h BS Protocol architecture Model

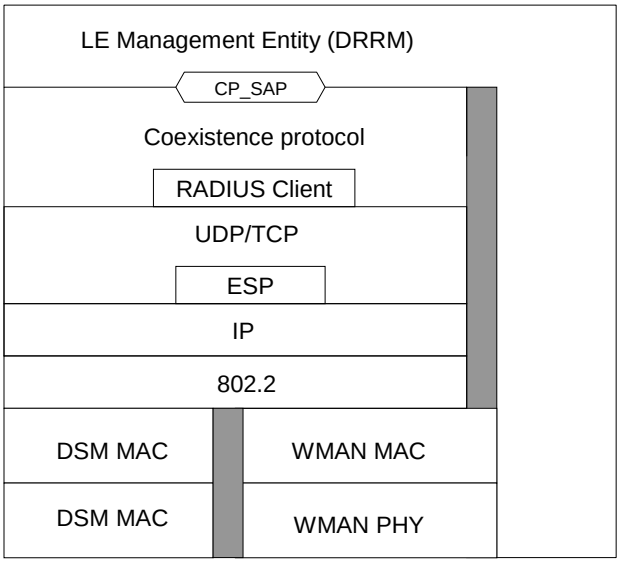

Figure h-A6—LE BS architecture with Coexistence Protocol

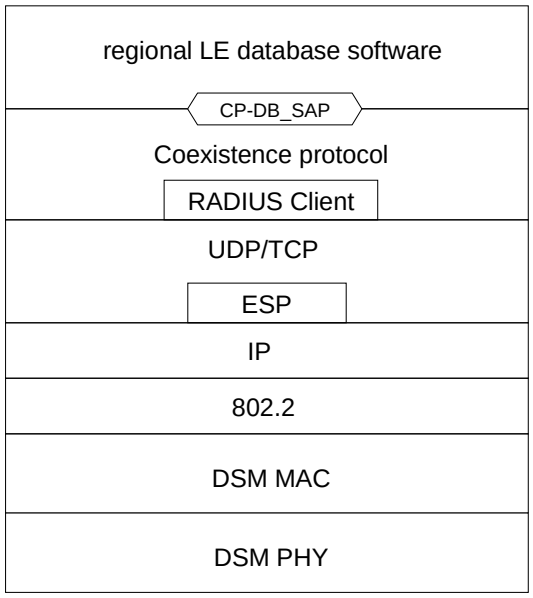

Figure h-A7—BSIS architecture with co-located regional LE database

To use the Coexistence Protocol, which is similar to PKM protocol, to perform the coexistence resolution and negotiation procedures a BS sends a LE_CP-REQ to another BS or BSIS and waits for the LE_CP-RSP.

Before any data can be exchanged between BS and BS/BSIS, security association must be setup first. IEEE 802.16 LE security associations between peers are established through RADIUS server. Any BS wants to communicate with another BS or BSIS shall first send a *RADIUS Access-Request* to request the establishment of the security association between originated BS and terminated BS/BSIS. RADIUS server replies a *RADIUS Access-Accept*, which includes security information for ESP operation, to the BS. At this point, only *virtual* security association is established between the peers. The BS sends the Security Block for the peer, which it received from the RADIUS Server, as a LE_CP-REQ packet with message type *Send-Security-Block*. This is the first message in the Coexistence Protocol TCP exchange between the BS and BS or BS and BSIS. The peer returns LE_CP-RSP packet with message type *Send-Security-Block*. At this point both sides have the information to encrypt all further packets for this exchange between the BS and BS or BS and BSIS.

The UDP port number assigned by IANA to be opened for the CP for transmission and reception of CP packets is *xxxx*.

The TCP port number assigned by IANA to be opened for the CP for transmission and reception of CP packets is xxxx.

A.3 Base Station Identification Server

[Note: The following part from 3.2.4.1 is a temporary text adopted from contribution C802.16h-05/11r1 and is subject to further discussion. A call for comment from security experts is open to comment on this text.]

The *Base Station Identification Server* (BSIS) acts as an interface between 802.16 LE BSs and the regional LE DB which stores the geographic and important operational information, e.g. latitude, longitude, BSID etc., of the LE BSs belonging to the same region. It converts the actions carried in PDUs received from the 802.16 LE BSs to the proper formats, e.g. SQL (Structured Query Language) string, and forwards the strings to the regional LE DB, which can be any available database software. BSIS converts the query results from the regional LE DB to the proper format, e.g. TLV encodings, and replies to the requested BSs. Figure h A7 shows the general architecture of inter-network communication across 802.16 LE systems. In this architecture, the 802.16 LE systems (BSs and BSIS) from different networks set up security association (including BS and BS, BSIS and BSIS) with each other by utilizing the services provided by the RADIUS server. BSIS acts as a peer of 802.16 LE BSs in this architecture. The BSID of regional BSIS is well known among the 802.16 LE systems within certain domain.In summary, ESP with RADIUS can discover a Rogue BS or BSIS. The messages exchanged between the LE BSs and the BSIS will be revealed in the next section. Note that the interface between BSIS and regional LE DB is out of scope.

A.4 RADIUS Protocol Usage

For future interoperability consideration, similar mechanisms are maintained. Secure exchange of 802.16 LE signaling information can be achieved after successful procedures of the RADIUS protocol. To include RADIUS support, the RADIUS server and the BS/BSIS RADIUS client must be configured with the shared secret key and with each other's IP address. Each BS/BSIS acts as a RADIUS client and has its own shared secret key with the RADIUS server. The shared secret key may be different from that of any other BS/BSIS.

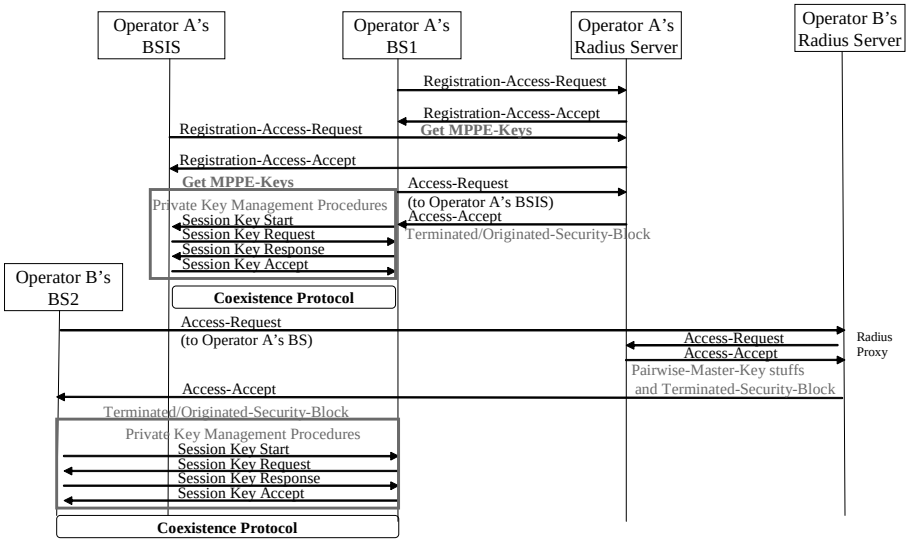

Figure h-A8—RADIUS protocol example

Figure 4 shows the RADIUS protocol message exchange sequence. At starting up, each BS or BSIS must send a RADIUS-BS/BSIS-Registration-Access-Request (shown in table x) to the RADIUS server for authentication purpose and leave the address mapping (BSID to IP) information in the server. At this time, the RADIUS server will retain the following information of registered BS or BSIS:

a) Wireless medium address of BS (BSID) or medium address of BSIS,

b) MPPE-Keys in RADIUS-BS/BSIS-Registration-Access-Request/Accept Procedures

c) IP address or DNS name,

d) Cipher suites supported by the BS or BSIS for the protection of Coexistence Protocol communications,

e) and Pairwise-Master-Key for BS or BSIS to establish Session-Key-Handshaking procedures

Same as [2], Microsoft Point-to-Point Encryption (MPPE) (RFC 2548:1999) key is introduced. The MS-MPPE-Send-Key, which could be got in the RADIUS-BS/BSIS-Registration-Access-Accept message (shown in table x) and RADIUS-BS/BSIS-Access-Accept message (shown in table x), is used for encrypting the security blocks in the RADIUS-BS/BSIS-Access-accept message for PKM-target and PKM-initiator. A registration access reject message may be issued due to a BS not supporting the ESP Transform or ESP Authentication algorithm selected for use in securing the following intercommunication, or for other RADIUS configuration reasons not discussed here.

Once a BS wants to get the knowledge of coexistence neighbor topology, it must first send RADIUS-BS/BSIS-Access-Request message (shown in table x) to the RADIUS server in order to acquire the regional BSIS's IP address. The wireless medium addresses of regional BSIS, similar to BSID, well known by all BSs supporting LE operation, is sent in the RADIUS-BS/BSIS-Access-Request message to the RADIUS server for looking up IP address of the BSIS. Upon receiving the request message, the RADIUS server will respond with a RADIUS-BS/BSIS-Access-Accept message (shown in table x) if the BS is a valid member which is allowed to perform inter-communication. The RADIUS-BS/BSIS-Access-Accept message would contain Originated-BS-Security-Block(for BS encrypted in MPPE-Send-Key from current RADIUS-BS/BSIS-Access-Request/Accept message) and Terminated-BS/BSIS-Security-Block(for BSIS encrypted in MPPE-Send-Key from BSIS's RADIUS-BS/BSIS-Registration-Access-Request/Accept message). Security-Block (shown in table x) contains Pairwise Master Key IndexPairwise-Master-KEYKey Lifetimethe list of ESP Authentication/Transform IDs for initiator-send/receive for establishing a secure connection with the BSIS .

After querying process between the BS and the regional BSIS in Coexistence Protocol, the BSIS will respond to the BS with possible coexistence neighbor BSs candidates and their BSIDs. The BS, then, tries to establish secure connections with the coexistence neighbor BSs after evaluating the coexistence relationships with these candidates. The BS sends RADIUS-BS/BSIS-Access-Request message to local RADIUS server for Originated/Terminated-BS/BSIS-Security-Blocks. After getting Security-Blocks from RADIUS-BS/BSIS-Access-Accept messages, the BS establishes secure connections with each evaluated coexistence neighbor BS.

An access reject message may be issued due to a BS or the regional BSIS not supporting the ESP Transform or ESP Authentication algorithm selected for the following intercommunication, or for other RADIUS configuration reasons not discussed here.

Table h-A1—Security Block Format

Element ID	Length	Information
1	1	Pairwise Master Key Index for BS/BSIS (0-255)
2	32	Pairwise-Master-KEY
3	4 * number	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-send

4	4 * number	The list of ESP Transform IDs corresponding to the ESP transforms for initiator-send
5	4 * number	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-receive
6	4 * number	The list of ESP Transform IDs corresponding to the ESP transforms for initiator-receive
7	4	Pairwise-Master-KEY Lifetime

The Security-Block would be encrypted in 32-bytes MPPE-Send-Key with the following manner ('+' indicates concatenation):

b(1) = MD5(MPPE-Send-Key+BSID) c(1) = p(1) xor b(1) C = c(1)

b(2) = MD5(MPPE-Send-Key+BSID + c(1)) c(2) = p(2) xor b(2) C = C + c(2)

. .

. .

. .

b(i) = MD5(MPPE-Send-Key+BSID + c(i-1)) c(i) = p(i) xor b(i) C = C + c(i)

Break plain text into 16 octet chunks p(1), p(2)...p(i), where i = len(P)/16. Call the ciphertext blocks c(1), c(2)...c(i) and the final ciphertext C. Intermediate values b(1), b(2)...c(i) are required. The resulting encrypted String field will contain c(1)+c(2)+...+c(i).

For Originated Security Block, the encrypted MPPE-Send-Key is from “RADIUS-Access-Request/Accept”.For Terminated Security Block, the encrypted MPPE-Send-Key is from “RADIUS-Registration-Access-Request/Accept”.

A.5 Privacy Key Management protocol usage

The PKM protocol would provide a flexible and easy-to-maintain key exchange mechanism. The PKM is based on the Pairwise-Master-Key to provide a symmetric key for the PKM-Initiator and PKM-Target side.

The following figure shows the PKM Session-Key-Handshaking procedures

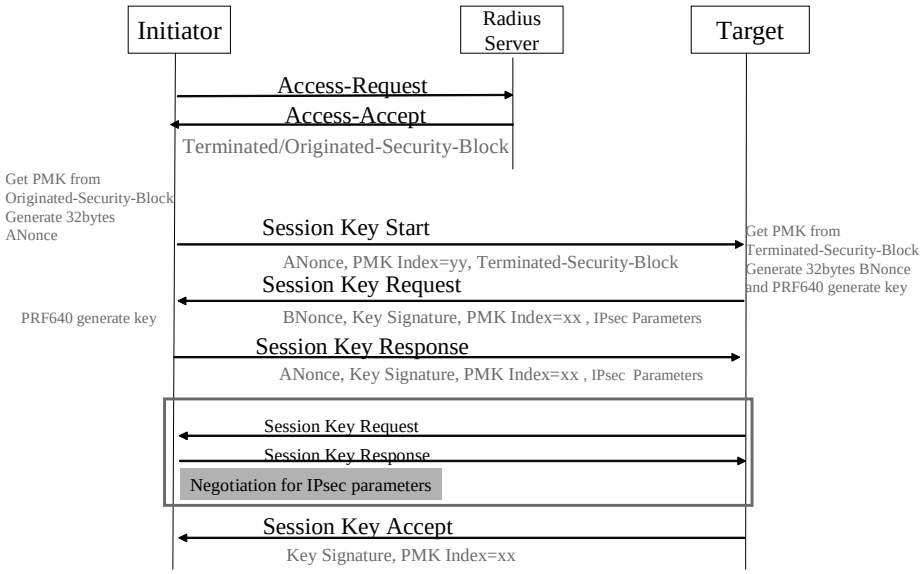

Figure h-A9—Figure 5 PKM Session-Key-Handshaking procedures

The PKM-Initiator will need to get the Pairwise-Master Key in Originated-BS-Security-Block from RADIUS-Server. And then perform the following steps

1) PKM-Initiator would get Pairwise-Master-Key-IndexPairwise -Master-KeyESP Authentication/Transform IDs and Key-Lifetime in originated Security-Block in RADIUS-BS/BSIS-Access-Accept message and then generate a random 32-bytes ANonce.
2) PKM-Initiator would will send Session-Key-Start message to PKM-Target with "ANonce""Pairwise-Master-Key-Index" and "Terminated Security-Block".
3) After receiving Session-Key-Start message, PKM-Target would generate a random 32-bytes BNonce. And perform the PRF640 algorithm to generate the 640-bits Key. Keep the first 512-bits ESP-Transform/Authentication Keys and use the last 128-bits M-Key as the HMAC-MD5 key to generate 16-bytes Key-Signature.
4) PKM-Target would will send Session-Key-Request message to PKM-Initiator with "BNonce""Pairwise-Master-Key-Index" and " ESP Authentication/Transform IDs"(PKM-Target chosen).
5) After receiving Session-Key-Request message, PKM-Initiator would perform the PRF640 algorithm to generate the 640-bits Key. Keep the first 512-bits ESP-Transform/Authentication Keys and use the last 128-bits M-Key as the HMAC-MD5 key to generate 16-bytes Key-Signature to verify the Key-Signature field on the Session-Key-Request message. If it is wrong, PKM-Initiator would perform silent-drop and doesn't response any message. If it is correct, PKM-Initiator would prepare the Session-Key-Response message and use HMAC-MD5 generate Key-Signature filed.
6) PKM-Initiator would will send Session-Key-Response message to PKM-Target with "ANonce""Pairwise-Master-Key-Index" and " ESP Authentication/Transform IDs"(PKM-Initiator chosen) .
7) After receiving Session-Key- Response message, PKM-Target would check the ANonce value if equal to the previous ANonce value in Session-Key-Start message and use HMAC-MD5

generate Key-Signature filed to verify the Key-Signature field. Compare the values of ”ESP Authentication/Transform IDs” to make sure the security parameters.

8) After the above, PKM-Target will send Session-Key-Accept with Key-Signature filed to PKM-Initiator to verify.

9) The following IPsec connection will use the first 512-bits ESP-Transform/Authentication Keys from PRF640 as keys and perform the ESP-Transform/Authentication algorithms from chosen ESP Authentication/Transform IDs.

The following figure shows the PKM Session-Key Re-Key procedures

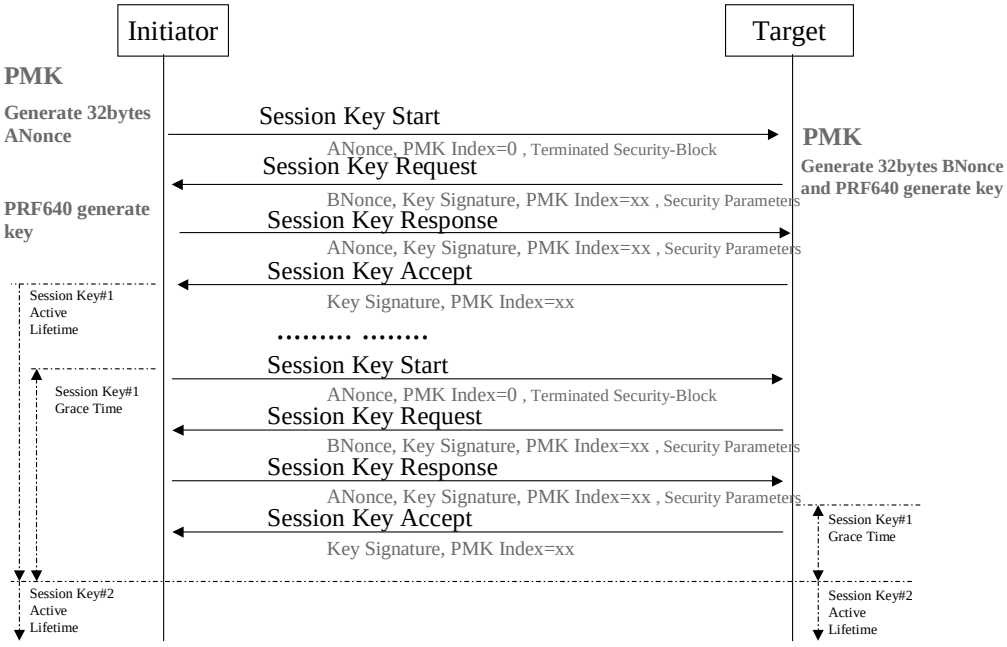

Figure h-A10—Figure 6 PKM Session-Key Re-Key procedures

Each Session-Key would set a Key-Lifetime, and PKM-Initiator could set a Session-Key grace time to perform Session-Key-Handshaking for the next new Session-Key#2 to be generated until the end of the key lifetime. The Session-Key#1 could use up its lifetime and then activate the Session-Key#2. If each side use the Session-Key#2 first in IPsec connection, it could also activate the Session-Key#2. If the lifetime of Session-Key#1 use up, the PKM-Initiator doesn’t perform the Session-Key Re-Key procedures. PKM-Target would disconnect the IP connection until the Session-Key#2 generated.

The following figure shows the PKM Session-Key Re-Key procedures with the PMK update

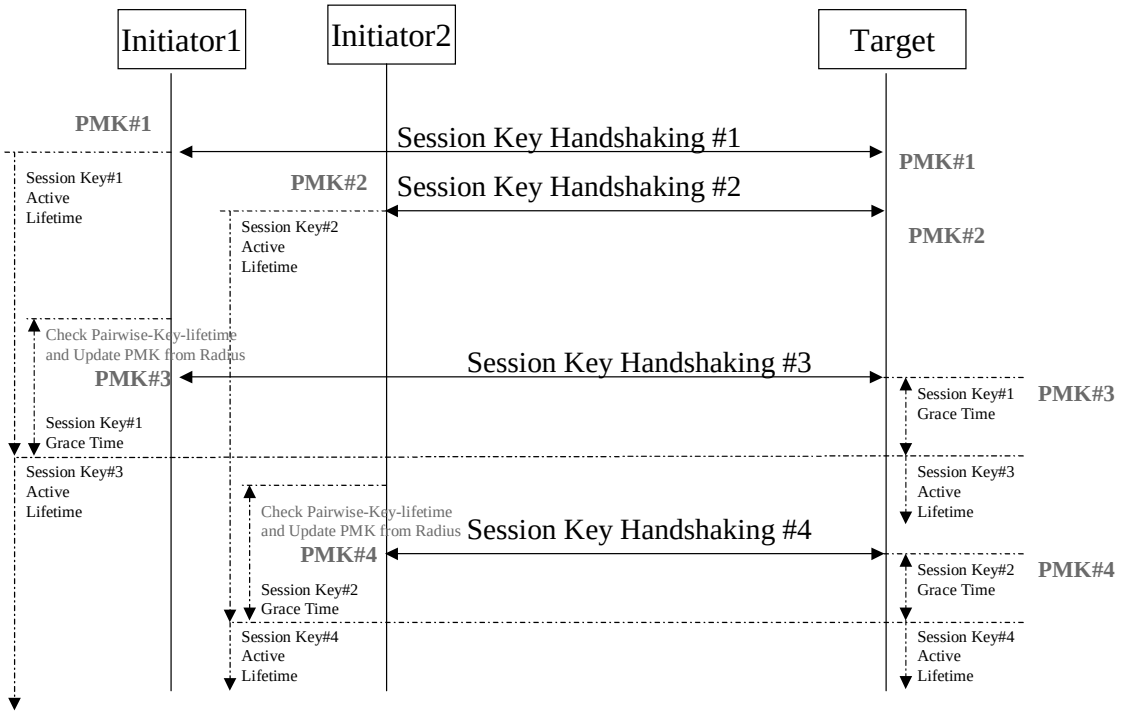

Figure h-A11—PKM Session-Key Re-Key procedures with the MK update of PKM-Target

The PKM-Initiator will check the current Pairwise-Key-Lifetime if still valid. If the PKM-Initiator detects the Pairwise-Key-Lifetime used up, it would perform RADIUS-BS/BSIS- Access-Request/Accept procedures to get the latest Pairwise-Master-Key in Security-Blocks from RADIUS-Server.

Each Pairwise-Master-Key would set a Pairwise-Master-Key-Lifetime, and BSs/BSISs could set a Pairwise-Master-Key grace time to perform Access-Request/Accept procedures for the new Pairwise-Master-Key until the end of the Pairwise-Master-Key lifetime. If the lifetime of Pairwise-Master-Key use up, the originated BSs/BSISs don't perform the Access-Request/Accept procedures, the terminated BSs/BSISs should discard the connections.

The following figure shows the 640-bits Key generated by PRF640

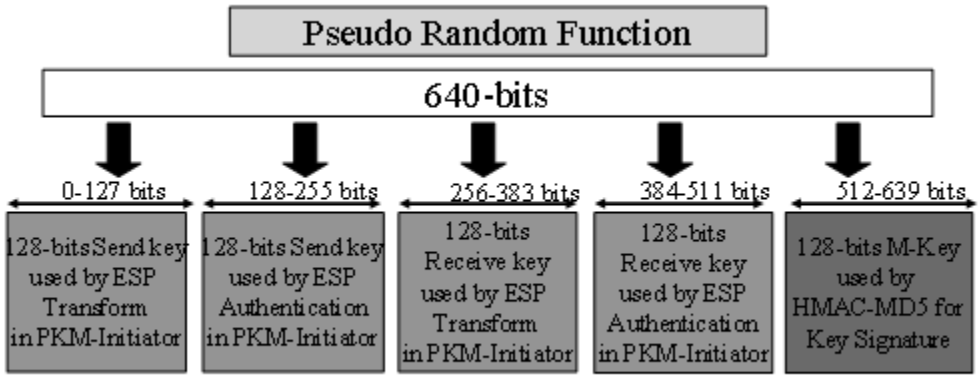

Figure h-A12—the 640-bits Key generated by PRF640

The BSs/BSISs get Pairwise-Master-Key from RADIUS-Servers and generate 32-bytes Nonce value to derive 640-bits key as follows

PRF-640(PMK, "BS-BSIS key expansion", Min(BS1ID,BS2ID) || Max (BS1ID,BS2ID)|| Min(ANonce,BNonce) || Max(ANonce,BNonce))

Where

PRF-640 (K,A,B) =
for i=0 to 4 do
R=R|HMAC-SHA-1(K, A|0|B|I)

return LeastSignificant-640-bits(R)
and "|" denotes bitstring concatenation

A.6 Security consideration

In this model, data traffic is protected by using IPsec.

The IP Security Protocol provides cryptographically based security for IPv4. The protection offered by IPsec is achieved by using one or both of the data protection protocols (AH and ESP). Data protection requirements are defined in the Security Policy Database (SPD). IPsec assumes use of version 2 of the Internet Key Exchange protocol , but a key and security association (SA) management system with comparable features can be used instead.

A.7 RADIUS Protocol Messages

The following messages are listed to support RADIUS protocol:

Note that[tbd.] means To Be Defined.

— *RADIUS-*BS*/BSIS-Registration-Request (BS/BSIS* RADIUS *server): A startup BS/BSIS sends this message for authentication purpose.*

Table h-A2—RADIUS-BS/BSIS-Registration-Access-Request

Attribute number	Attribute name	Value
1	User-Name	BSID. The BSID should be represented in ASCII format, with octet values separated by a "-". Example: "00-10-A4-23-19-C0".
4	NAS-IP-Address	BS's IP Address
6	Service-Type	Coexistence-Protocol-Register (value =[tbd.], ex. IAPP-Register, value = 15)
26 26-TBD	Vendor-Specific-Attribute (VSA) Supported-ESP-Authentica-tion-Algorithms	 The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms supported by this BS (See Table h A7)
26-TBD	Supported-ESP-Transforms	The list of ESP Transform IDs corresponding to the ESP transforms supported by this BS (See Table h A6
32	NAS-Identifier	BS's NAS Identifier
80	Message-Authenticator	The RADIUS message's authenticator

According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/BSIS-Registration-Access-Request packet in addition to the ones listed in Table x.

— RADIUS-*BS/BSIS-Registration-Accept (RADIUS server BS/BSIS): After RADIUS server verifies the valid membership, it will respond with this accept message.*

Table h-A3—RADIUS-BS/BSIS-Registration-Access-Accept

Attribute number	Attribute name	Value
1	User-Name	BSID.
6	Service-Type	Coexistence-Protocol -Register (value =[tbd.], ex. IAPP-Register, value = 15)
26 26-TBD	Vendor-Specific-Attribute (VSA) Supported-ESP-Authenti-cation-Algorithms	 The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms approved by Radius Server
26-TBD	Supported-ESP-Trans-forms	The list of ESP Transform IDs corresponding to the ESP transforms approved by Radius Server
27	Session-Timeout	Number of seconds until the BS should re-issue the registration Access-Request to the RADIUS server to obtain new key information.
80	Message-Authenticator	The RADIUS message's authenticator

According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/BSIS-Registration-Access-Accept packet in addition to the ones listed in Table x.

— RADIUS-BS/BSIS-Access-Request (BS/BSIS RADIUS server): The BS sends this message to request for inter-communication with another coexistence neighbor BS or a regional BSIS.F:Figure <n+>\m

Table h-A4—RADIUS-BS/BSIS- Access-Request

Attribute number	Attribute name	Value
1	User-Name	User-Name must include Country-CodeOperator ID and Regional BSIS's WM address or coexistence neighbor BS's BSID
4	NAS-IP-Address	Original BS's IP Address (the BS sending this request message)
6	Service-Type	CS/CIS-Check (value =[tbd.], ex. IAPP-AP-Check, value = 16)
61	NAS-Port-Type	Wireless – Other (value = 18)
80	Message-Authenticator	The RADIUS message's authenticator

According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/BSIS-Access-Request packet in addition to the ones listed in Table x.

RADIUS-BS/BSIS-Access-Accept (RADIUS server BS/BSIS): After verifying that the coexistence neighbor BS is valid member, RADIUS server will respond with the security blocks necessary for establishing a secure connection between the coexistence neighbor BS and requesting BS or between BSIS and requesting BS.

Table h-A5—RADIUS-BS/BSIS- Access-Accept

Attribute number	Attribute name	Value
1	User-Name	User-Name must include Country-CodeOperator ID and Regional BSIS's WM address or coexistence neighbor BS's BSID
8	Framed-IP-Address	IP Address of Regional BSIS or coexistence neighbor BS.
26 26-TBD 26-TBD	Vendor-Specific-Attribute (VSA) Originated-BS-Security-Block Terminated-BS/BSIS-Security-Block	 Security Block encrypted using originated BS's MPPE-SEND-KEY, to be decrypted and used by the original BS Security Block encrypted using coexistence neighbor BS's MPPE-SEND-KEY (or BSIS's), to be decrypted and used by the coexistence neighbor BS (or BSIS)
80	Message-Authenticator	The RADIUS message's authenticator

According to RFC 2865:2000, other RADIUS attributes may be included in the RADIUS-BS/BSIS-Access-Accept packet in addition to the ones listed in Table x.

Table h-A6—ESP Transform identifiers

Transform identifier	Value	Reference
RESERVED	0	[RFC2407]
ESP_DES_IV64	1	[RFC2407]
ESP_DES	2	[RFC2407]
ESP_3DES	3	[RFC2407]
ESP_RC5	4	[RFC2407]
ESP_IDEA	5	[RFC2407]
ESP_CAST	6	[RFC2407]
ESP_BLOWFISH	7	[RFC2407]
ESP_3IDEA	8	[RFC2407]

ESP_DES_IV32	9	[RFC2407]
ESP_RC4	10	[RFC2407]
ESP_NULL	11	[RFC2407]
ESP_AES-CBC	12	[RFC3602]
Reserved for privacy use	249-255	[RFC2407]

Table h-A7—ESP Authentication algorithm identifiers

Transform identifier	Value	Reference
RESERVED	0	[RFC2407]
HMAC-MD5	1	[RFC2407]
HMAC-SHA	2	[RFC2407]
DES-MAC	3	[RFC2407]
KPDK	4	[RFC2407]
HMAC-SHA2-256	5	[Leech]
HMAC-SHA2-384	6	[Leech]
HMAC-SHA2-512	7	[Leech]
HMAC-RIPEMD	8	[RFC2857]
RESERVED	9-61439	
Reserved for privacy use	61440-65535	

A.8 Privacy Key Management protocol messages

The PKM protocol procedures contain 4 message actions, and each-side could check the code value of the begin of PKM message to recognize which *action need to perform this moment. The meaning of codes for PKM message as follows*

— *0* = Session Key Start

— 1 = Session Key Request

— 2 = Session Key Response

— 3 = Session Key Acce*pt*

The PKM message uses TLV format *to add the following attributes*

Table h-A8—Session Key frame TLV

Type	Length	Value Information
1	32	Nonce
2	8	Replay Counter
3	8	Key lifetime in seconds
4	16	Key Signature
5	4	Security Parameter Index
6	4 * number	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-send supported by this BS
7	4 * number	The list of ESP Transform IDs corresponding to the ESP transforms for initiator-send supported by this BS
8	4 * number	The list of ESP Authentication IDs corresponding to the ESP Authentication algorithms for initiator-receive supported by this BS

9	4 * number	The list of ESP Transform IDs corresponding to the ESP transforms for initiator-receive supported by this BS
10	33 + 4*n	Security Block

The Length field contains a 16-bits value to record the whole frames size starting from Code field, with the ESP-Transforms-and-Authentication-Algorithms-Codes field filled in if present.

The PMK-Index field contains a 8-bits value to record the current Pairwise-Master-Key-Index each PKM-side used. If the PKM-Target detects the PMK-Index different of PKM-Initiator, it must update the latest Pairwise-Master-Key.

The Replay-Counter field contains a 64-bits random number (such as 64-bit NTP timestamp) and does not repeat within the life of the Master-Key material.

The Key-Lifetime field contains a 64-bits value to record the Session-Key lifetime in seconds.

The Key-Signature field contains an HMAC-MD5 message integrity check computed over the Session-Key-Frame starting from Code field, with the ESP-Transforms-and-Authentication-Algorithms-Codes field filled in if present, but with the Key Signature field set to zero. The M-Key is used as the HMAC-MD5 key.

The Security-Parameters-Index field contains a 32-bits value to assign to the IPsec Security Association (including the encryption and authentication keys, the authentication algorithm for AH and ESP, the encryption algorithm for ESP, the lifetime of encryption keys…etc in this session). PKM-Initiator/Target could check the SPI value in ESP-Header to detect to use which SA for this IPsec connection.

The following figure shows the Session-Key-Start message format

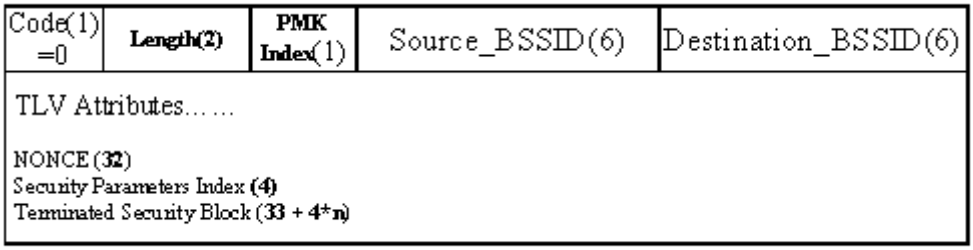

Figure h-A13—Session-Key-Start message format

The following figure shows the Session-Key-Request message format

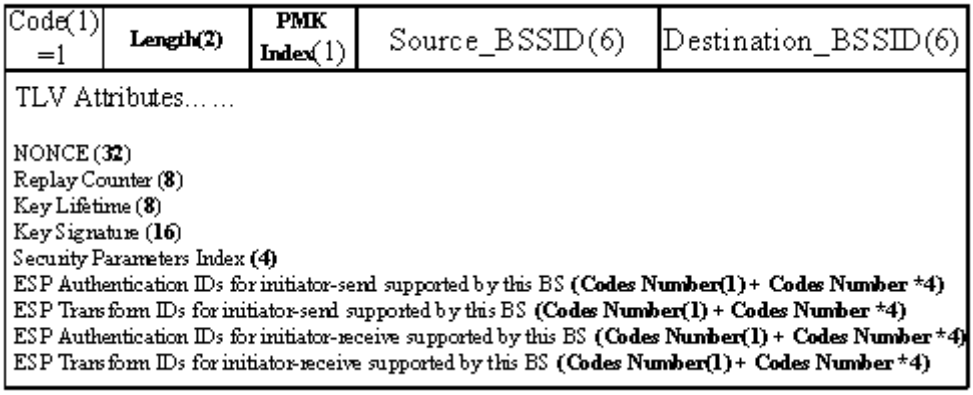

Figure h-A14—Session-Key-Request message format

The following figure shows the Session-Key-Response message format

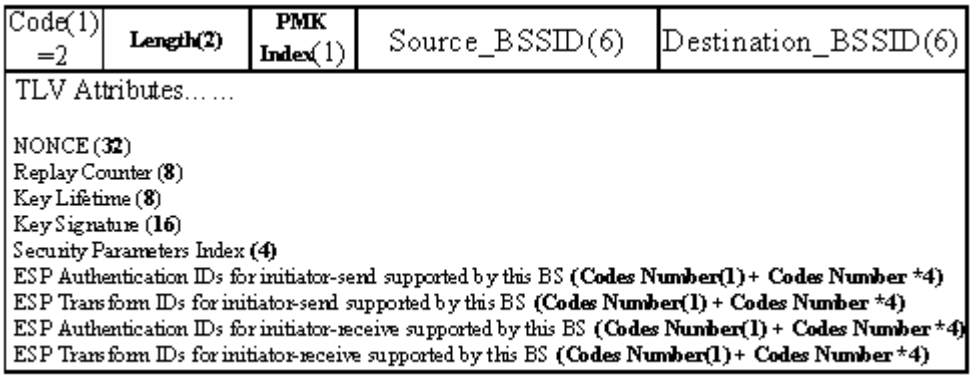

Figure h-A15—Session-Key-Response message format

The following figure shows the Session-Key-Accept message format

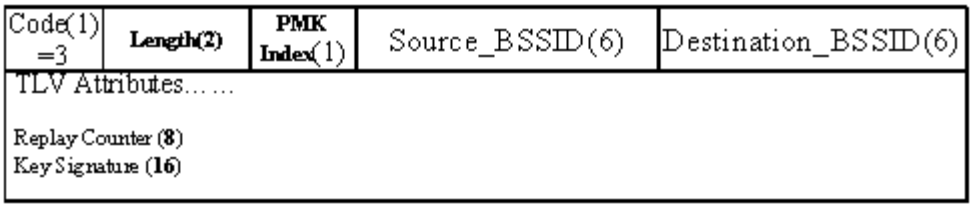

Figure h-A16—Session-Key-Accept message format

Annex B

(informative)

GPS Timing and Base Station Synchronization

Every IEEE 802.16h network will be synchronized to a globally distributed reference timing system that is capable of allowing the network Base Stations to synthesize a 1 pps NTI and a UTC time stamp. The Global Positioning System (GPS) is capable of providing such a temporal references to the Base Stations providing they are equipped with GPS receivers.

Every base station equipped with a GPS receiver would be capable of receiving a UTC synchronized 1 pps timing signal. The accuracy of the clock pulses derived from using GPS are accurate to +/- 100 usec and the pulses that are derived typically have rise times within +/- 2.5 nsec. Fig 1 shows a typical GPS 1 sec pulse and its duration (Trimble Inc. Palisade output).

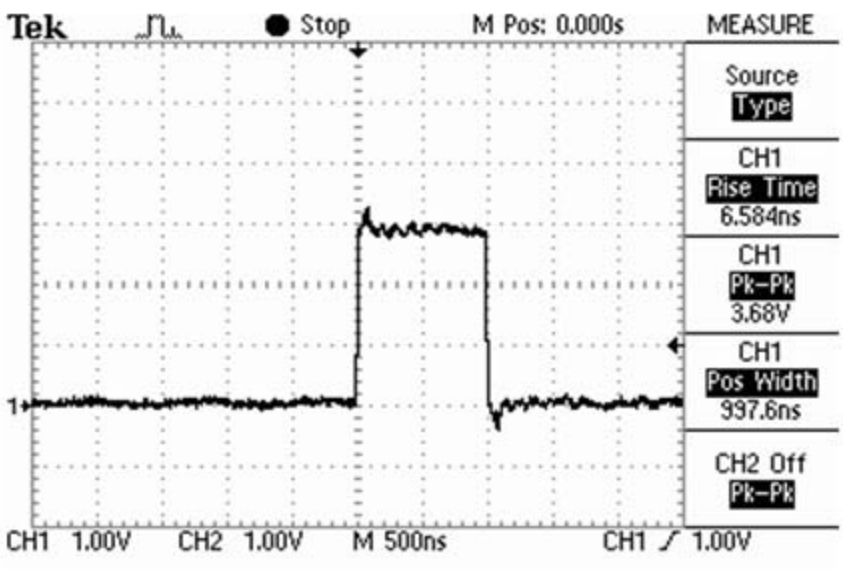

Figure h-B1—GPS 1pps Pulse

The availability of a globally distributed clock will result in a common temporal unit that can be used in negotiating access times to spectrum shared by a community of ad-hoc users. Non-IEEE 802.16h networks having different architectures and messaging signals could also use a common 1 sec interval for synchronization of their networks. This would conceivably allow communication between them and IEEE 802.16h networks in a synchronized manner, to facilitating the exchange of information related to coexistence and spectrum sharing.

The one second unit is considered ideal because it is distributed by the GPS as such and the length of the unit is seemingly appropriate. IEEE 802.16h networks typically have frames in the order of several to tens of milliseconds, which is of a granularity that could allow several to several tens of networks to negotiate coexistence subintervals within the 1 second span. Additionally, for IP networks, the 1 second interval is of a

length sufficient to accommodate inter-router TCP/IP latency, especially over networks that are likely to be close to each other, such as ad-hoc LE networks.

Annex C

(informative)

interference scenario case study

C.1 Base Station initialization scenario case study

See to the figure below:

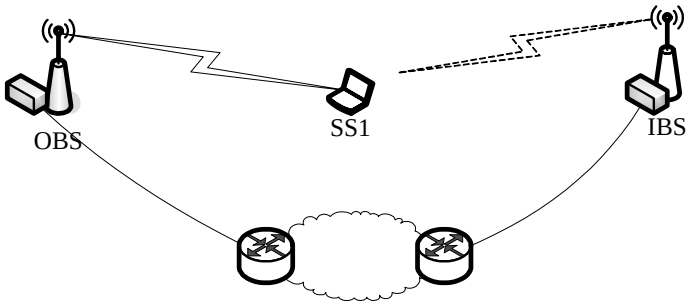

Figure h-C1—Enviorment of initializing basestation

Suppose OBS and SS1 is part of a operation network, SS1 have a stable air link with it's BS before IBS start, OBS have a wired link Now the IBS comes into this area with wire link to the core network, IBS could contact OBS if he knows the address, unfortunately it does not know the IP address and probably there may be no regulatory server to ask for help. Notice here, the IBS will not have any SS attached before IBS itself has finished initialization. Based on list of assumptions referred to the working document, we can study on cases IBS is in and what kind of problems it may meet.

There is three kind of situation may exist in both SS2BS and BS2SS interference/signaling,

— not able to be detected

— interference detected but signaling not able to be decoded

— interference detected and the signaling is decodable

We will use three kind of line with arrow to indicate these situation in the following figure during discussion.

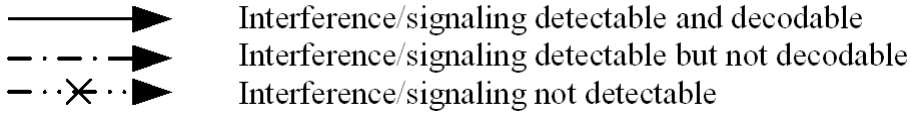

Figure h-C2—Legend of arrow indicating interference direction

[note: based on the synchronization assumption, the BS/BS and SS/SS interference could be ignored.]

We can easily list out the possible cases by logical thinking as below:

- Case1x: IBS interference/signaling can not detected by SS1
  - Case1a: the IBS can not detect the signal from the operating network
  - Case1b: the IBS can detect the signal from the operating network, but not decodable
  - Case1c: the IBS can detect and decode the signaling from the operating network
- Case2x: IBS interference/signaling can detected by SS1 but not decodable
  - Case2a: the IBS can not detect the signal from the operating network
  - Case2b: he IBS can detect the signal from the operating network, but not decodable
  - Case2c: the IBS can detect and decode the signaling from the operating network
- Case3x: IBS interference/signaling can detected and decoded by SS1
  - Case3a: the IBS can not detect the signal from the operating network
  - Case3b: the IBS can detect the signal from the operating network, but not decodable
  - Case3c: the IBS can detect and decode the signaling from the operating network

We can discuss these cases one by one in the following:

Note:

1)The red tick here means one of the BS may know the IP address of another BS by receiving the signaling from the air; The red cross here stands for that the BS can not know the IP address of another BS by the signaling from the air.

2)The red dot line in one side means that from this side, the station can decode the signaling from the transmitter; The red dash line means from this side, the station can detect but can not decode; and the read solid line means the station can not sense the existence of the transmitter.

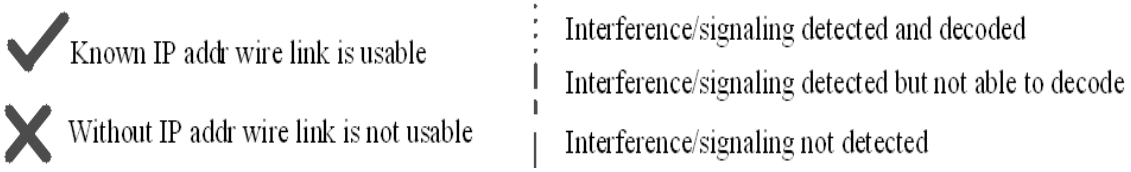

Figure h-C3—Legend of line indicating interference situation and symbols indicating wire-link usability

Case 1x:

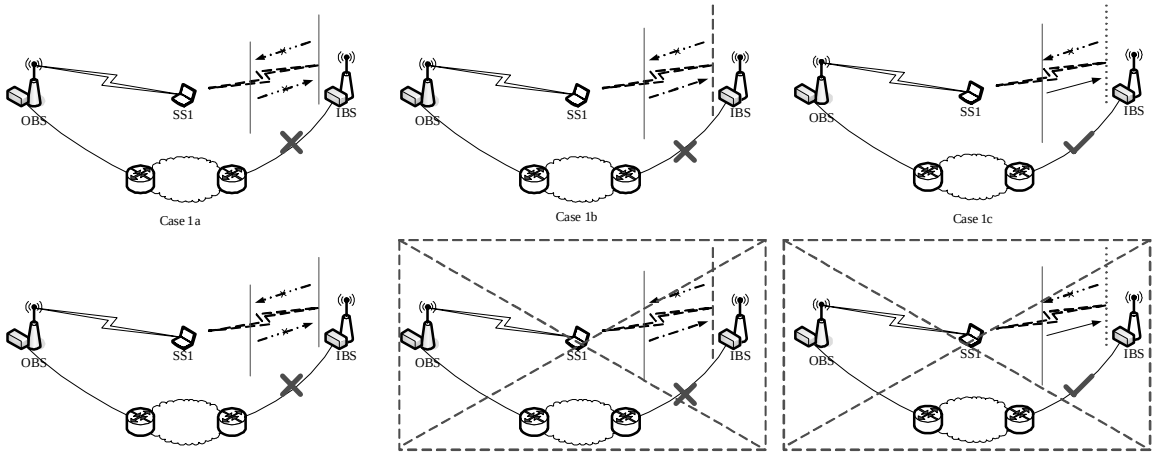

Figure h-C4—case 1x study

[Note: although logically case 1b and 1c could happen, these cases are not normally exist, because the channel propagation are symmetric in both direction, but the BSs' transmition power are normally higher than the SSs'. So when the IBS couldn't been detected by SS1, the IBS will not detect SS1's signal also.]

In these cases IBS doesn't interference with SS1, which means the OBS's network is not necessary to contact IBS. So case 1x(1a/1b/1c) are not the target initialization scenarios in 16h.

Case 2x:

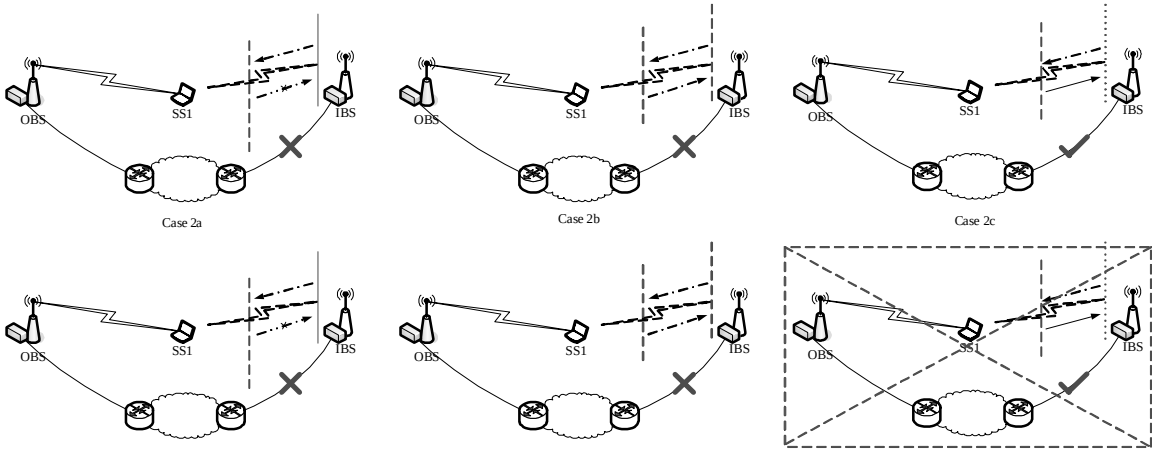

Figure h-C5—case 2x study

[Note: case 2c normally doesn't happen for the same reason with case 1b & 1c.]

In these cases, IBS's signaling could be detected by SS1, but SS1 could not decode the signaling. The problem here is, IBS may interfere to SS1, but SS1 can't know who is the interferer, so it can not tell the OBS who is the interferer, so the OBS could not contact IBS for cooperation. These cases is the worst cases that 16h should deal with.

The reason for this problem is the difference of condition between decodable signaling and troubling interference. The condition could be measured in SNR requirement, the lower SNR required for the signaling, the lower probability to have this problem; another approach may help was introduced to the working document 15.2.1.1.3 in the meetings before is shown in IEEE C802.16h-05/041,and we could easily understand it in the following figure.

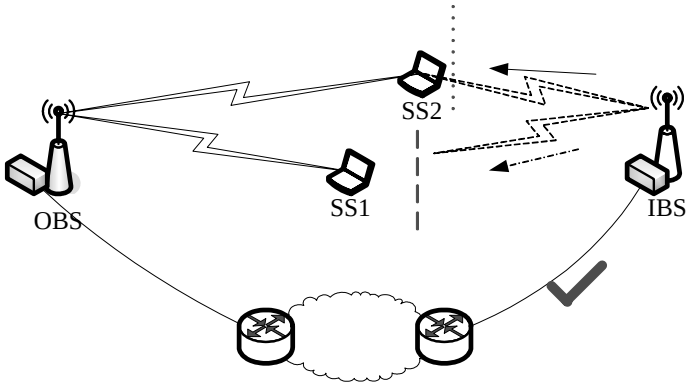

Figure h-C6—Enhanced mechanism dealing with case 2x

No matter how hard we try, we could not absolutely get rid of the difference, so we can not totally get rid of this problems, all we could do is to make the probability as low as possible. Once in operating network all the interfered SSs could not decode the signaling, we have no chance to tell who is coming to interfere the network, and this operating network may need to switch/escape to another channel.

Case 3x:

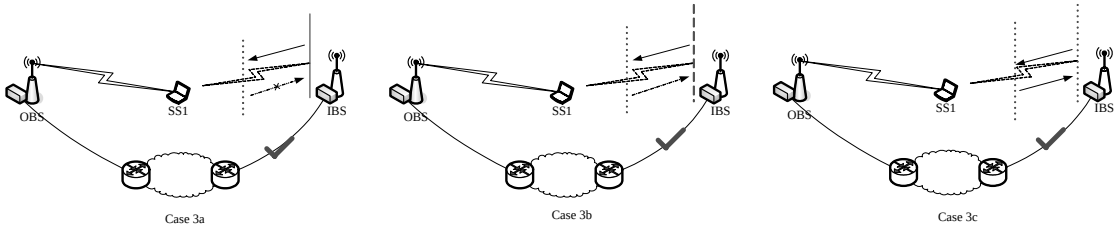

Figure h-C7—case 3x study

These cases are most interesting cases that 16h need to make out the solution. We can see each one of the 3 cases here is a normal case, and we need to deal with them all. In order to find the common solution, we need to take the advantage of the common condition. That is, SS can decode the IBS signaling. It's understood that if we don't depends on the IBS signaling transmition, in case 3a and 3b, operation network will not be able to find IBS in the core network. And the only way we may enable the operating network to do this is using the SS to relay the signaling which is managed to contain the IP address information.

The security issue may be mitigated by checking the instant random key and frame numbering in the contact requirement message sent by the OBS. That may prevent the IBS being cheated by someone faraway or by someone which is not able to control or access the 16h air link. We may need to think about this approach if we have no other choice to meet the cooperation contact requirement in case 3a and 3b.

For the sake of Case 2a and 3a, it's not logical to randomly choose the periodically silent CTS to occupy by the IBS, otherwise in the CTS which the IBS choose will cause collusion and make the initializing procedure

not effective. Instead, it's needed to have a predefined periodical ICTS among all the CTS, and every IBS know the timing of ICTS as well. And the rest CTS will be used as OCTS and reallocated periodically to carry the signaling such as radio signature by the OBSs.