IEEE P802.22
Wireless RANs

|  |
| --- |
| Security Recommendations for TGb |
| Date: 2014-07-09 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Ranga Reddy | Self |  |  | Ranga.reddy@me.com |
|  |  |  |  |  |

Abstract

This document outlines recommendations for amending the security sublayer and handling of security concepts with regards to new functionality being developed during TGb balloting.

R0: Initial version of this document

**Notice:** This document has been prepared to assist IEEE 802.22. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

**Release:** The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.22.

**Patent Policy and Procedures:** The contributor is familiar with the IEEE 802 Patent Policy and Procedures

<[**http://standards.ieee.org/guides/bylaws/sb-bylaws.pdf**](http://standards.ieee.org/guides/bylaws/sb-bylaws.pdf)>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair Apurva Mody <apurva.mody@ieee.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.22 Working Group. **If you have questions, contact the IEEE Patent Committee Administrator at <****patcom@ieee.org****>**.

# Introduction

TGb is developing a several different capabilities that will increase the coverage and data transmission capabilities of the WRAN. In this document a basic review of some of these new capabilities will be provided. For each new capability presented, the implications on the security sublayer and recommendations for modification/additional text required to address these issues will be presented as well.

In each section recommendations for new modifications will be numbered, as well as ***highlighted in bold and italics***. The organization of the rest of this document is as follows:

1. Relay CPE Operation Considerations
2. Extensions of Existing Cryptographic Methods
3. Multi-channel Operation Considerations
4. CBP Protection considerations

In this contribution some of the recommendation go beyond the security sublayer development. Some of these recommendations are made to address issues that are not clearly defined in the LB2 draft, as well has having some interdependcies with how the security sublayer is defined but are dependent on how the security sublayer operation is defined.

# 1. Relay CPE Operation Considerations

Relay CPEs or R-CPEs are a new class of CPE that are being added to the WRAN. R-CPEs extended coverage and can increase capacity by relaying traffic between the MR-BS and other CPEs (those belonging to customers of a network operator). R-CPEs can be centralized scheduling or distributed scheduling to the subscribers attaching through them. With centralized scheduling, the attached subscriber CPEs do not know they are having their traffic relayed in the DS/US through the CPE. For this case, the MR-BS handles all scheduling decisions. With distributed scheduling relaying, the attached subscriber CPEs (S-CPE) see transmissions from the R-CPE (e.g. preambles/MAPs) distinct of those from MR-BS. The R-CPE has local authority to grant bandwidth to subscriber CPEs.

With the addition of both types of R-CPEs several concepts from the base standard are being modified, and some are new concepts being considered for addition to the IEEE Std. 802.22-2011. The most important concepts related to relaying that need consideration are the following:

1. New frame structure options are required to support either type of R-CPE
2. New MAC management messages, and additional IEs to configure/monitor R-CPE operation
3. Security Setup (authentication/keying) for R-CPEs and subscriber CPEs.
4. Security Considerations specific to distributed R-CPEs
5. Security Considerations specifc to centralized R-CPEs
6. Allocation of resources based on shared common characteristics (location, bw requirements, etc)
7. A two-link ARQ mechanism
8. Container Message/Local Cell Update operational usage clarification

## 1.A New Frame Structure Options

The new frame structure options and MAC PDU generation allow packaging of MAC PDUs and the exchanging of said PDUs in the US and DS between the subscriber CPE and the MR-BS. This basic functionality hasn’t really deviated from the base standard, so with regard to the frame structure.

***1.A.1: No new security implicaitons have to be considered when dealing with new frame structure options***.

## 1.B MAC management messages

Several new MAC management messages are being added with regard to R-CPE operation configuration and monitoring. All of these new messages/IEs are described in modifications to section 7.7 of the current TGb draft.

***1.B.1: The handling of the extension of basic messages and IEs (e.g. new FCH, MAPs, DCD/UCDs) has not previously fallen under the purview of the security sublayer, and does not need to do so for the foreseeable future.***

The list of new MAC management messages are listed in modifications to Table 19, pg 62, line 9 of the current TGb draft. Each of these new messages in limited to being transmitted on the Primary Management FID assigned to R-CPE.

***1.B.2: If authentication of R-CPEs and S-CPEs is supported, mechanisms to authenticate those CPEs and setup keying to protect MAC amangement messages sent to/from R-CPEs and S-CPEs has already be developed.***

Implications on authentication and keying are to be discussing in 1.C of this document.

## 1.C Security Setup (Authentication/Keying) for R-CPE/S-CPE

Authenticating a CPE is a process by which the identity of a CPE is verified by exchanging credentials between the CPE and a server the network operator maintains. This operation is desireable, but not mandatory, as it provides verification that a CPE (R- or S-) is a valid CPE that is authorized to operate on the network.

***1.C.1: Having said that, the basic procedures as outlined in Section 8.2.1/8.2.2/8.2.4-8.2.8/8.5 in IEEE Std. 802.22-2011 does not need to change for R-CPE and S-CPEs.***

Once a CPE has been authenticated, keying can be setup so the CPE and BS can authenticate and/or encrypt MAC PDUs related to the exchange of MAC management or user data messages between it and the CPE. This operation is desireable because it provides the means of protecting user data and MAC management messages, thereby preventing malicious users from exploiting the network. The setup of keying to protect MAC management messages is accomplished immediately upon completion of authentication. The setup of keying to protect user data is only executed if the CPE is configured to do so, and if the CPE will be used to transmit higher-layer user application data.

***1.C.2: R-CPEs SHALL not start TEK/GTEK state machines as described in Section 8.2.3. The reasoning for this is simple, R-CPEs are not intended to originate higher layer SDUs to be transmitted in the network.***

***1.C.3: R-CPEs shall not be able be provided with keying material used to derive S-CPEs keys used to protect MAC management and user data exchanged between the MR-BS and S-CPE through the R-CPE. This is suggested to avoid adding complexity at the R-CPE to maintain keying material for all S-CPEs attached through it, as well as avoiding introduction of another point of vulnerability in the network.***

***1.C.4: S-CPEs, if configured to do so, MAY start TEK/GTEK state machines as described in 8.2.3, in order to facilitate the generation of keying to proctect higher-layer SDUs encapsulated in MAC PDUs that are transmitted in the network.***

## 1.D Security Considerations specific to distributed R-CPEs

With centralized R-CPE, the R-CPE only transits data between the MR-BS and the S-CPE. Processing of subheaders, fragmentation/packing, ARQ (for more on ARQ see section 1.F); is dealt with on an end-to-end basis. This behaviour is no different that how things are handled in the base standard. For distributed R-CPE, some of these behaviors are handled differently

Subheaders that carry pertinent information have to be visible and capable of being processed. In the base standard it is not clearly defined how the subheaders should be treated

***1.D.1: Need to clearly state that the GMH as well as any non Packing (including Packing/Fragmentation subheader when set to Fragmentation, BR, Extendended, and GMH) subheaders are not considered to be payload, and are therefore not encrypted. Packing/Fragmentation Subheader when set to Packing is considered payload***

Given the capabilities of AES-GCM that is used in the security sublayer, we can use the AES-GCM mechanism to protect subheader information without having to encrypt the actual subheaders. This can be done by using subheader data in the Fixed Field part of the nonce construction as defined in section 8.4.2.2.

Even when considered the adjustment to the MAC and security sublayer (1.D.1) and 1.D.3, an end-to-end security sublayer is preferable when employing distributed R-CPEs to extened coverage to S-CPEs. By end-to-end, it is meant that encryption and decryption is done at the S-CPE and MR-BS. This method is preferable because we do not want to have to distribute keying to R-CPEs for each S-CPE, so that R-CPEs can encrypt/decrypt traffic it exchanges with attached S-CPEs on the AZ. Doing so would introduce a point of vulnerability in the network, and add to the complexity of the R-CPE.

***1.D.2: clearly define and end-to-end security model for distributed R-CPE networks. Only the MR-BS and S-CPE will manage application of cryptopgraphic suites to protect MAC management messages and user data sent between the S-CPE and the MR-BS.***

How subheaders are aligned in MAC PDU construction is defined in the base standard. This aspect shall not change. Concerning the two new Extended subheader types, their use shall be considered first. The Extended Type/Extended BR is only used/transmitted by centralized R-CPEs, and not applicable to S-CPEs communicating through distributed R-CPEs. The Extended Type/Channel Aggregation subheader, Packing/Fragmentation, BR, GMSH, and ARQ feedback can be used by S-CPEs that communicate with the MR-BS through an R-CPE.

***1.D.3: Clearly define what Subheaders are applicable to S-CPEs that talk through a distributed R-CPE. This list should be as follows: BR, Packing/Fragmentation, GMSH, and ARQ feedback. Existing rules in section 7.6.1.2 of 802.22-2011 should be followed when determining the order. The order should be as follows: BR 1st if no GMSH, GMSH then BR if GMSH present, then Extended Type/Channel Aggregation, then ARQ feedback and finally the Fragmentation subheader. Packing subheader is added before each packed SDU.***

As currently defined in LB2 Draft, there is no clear procedure for how centralized and distributed R-CPEs forward traffic between the MR-BS and S-CPEs. A good example of this is section 6.3.3.8 of 802.16-2012. Without this defining how subheaders/PDUs are processed within the context of the security sublayer is difficult to achieve.

***1.D.4: We need to define how a burst is forwarded between access zone and relay zone in the US and DS for distributed R-CPEs. Examples of said procedures are rules for using them are listed in sections 6.3.3.8 & 6.3.3.8.1-6.3.3.8.2 of IEEE Std 802.16-2012.***

As for defining how MAC PDU construction and transmission through distributed R-CPEs should contain the following:

1. When EC bit 1 in GMH received from S-CPE & R-CPE will not further fragment/pack PDUs:
	1. When distributed R-CPE receives MAC PDU from a S-CPE with a BR, GMSH, Extended Type/Channel Aggregation, and/or ARQ feedback IE while the EC (Encryption Control) bit in the GMH is set, the subheader(s) are processed as necessary.
	2. The R-CPE forwards the MAC PDU as is. When the MR-BS receives a MAC PDU that was relayed by R-CPE for an attached S-CPE with EC bit set to 1 in the GMH and the Type field field indicating the presence of the BR and/or GMSH, the BR/GMSH subheader will be ignore, because those subheaders will have been processed by the R-CPE.
	3. MR-BS will only process Extended Type/Channel Aggreggation & ARQ feedback IEs.
	4. MR-BS will then process the fragmentation subheader before decrypty/authenticating the MAC PDU, or proceed to decrypt/authenticate the PDU prior to processing each packed SDU.
2. When EC bit 1 in GMH received from S-CPE & R-CPE will further fragment/pack PDUs:
	1. When distributed R-CPE receives MAC PDU from a S-CPE with a BR, GMSH, Extended Type/Channel Aggregation, and/or ARQ feedback IE while the EC (Encryption Control) bit in the GMH is set, the subheader(s) are processed as necessary.
	2. If the R-CPE has to pack multiple PDUs from a S-CPE, if will form a new MAC PDU with a GMH that has EC bit set to 0, indicating packing subheader for each packed PDU from an S-CPE, finally attaching a CRC. The R-CPE forwards the new MAC PDU as currently defined.
		1. When the MR-BS receives the packed PDU it will unpack each of the S-CPE’s MAC PDUs. For each unpacked MAC PDU that was relayed by R-CPE for an attached S-CPE with EC bit set to 1 in the GMH and the Type field field indicating the presence of the BR and/or GMSH, the BR/GMSH subheader will be ignored, because those subheaders will have been processed by the R-CPE.
		2. Each unpacked S-CPE PDU will be processed as indicated in Step 1
	3. If the R-CPE has to fragment a MAC PDU, if will form a new MAC PDU with a GMH that has EC bit set to 0, indicating fragmentation subheader for each PDU fragment from an S-CPE, finally attaching a CRC. The R-CPE forwards each fragment as a new MAC PDU as currently defined.
		1. When the MR-BS receives the new PDU it will unpack the PDU fragment MAC PDU.
		2. It will continue to do this until it receives all fragments from the R-CPE
		3. Once it receives all the fragments of the S-CPEs PDU, MR-BS will only process Extended Type/Channel Aggreggation & ARQ feedback IEs before handing assemble PDU to higher layer
3. When EC bit 0 in GMH received from S-CPE & R-CPE will not further fragment/pack PDUs:
	1. When distributed R-CPE receives MAC PDU from a S-CPE with a BR, GMSH, Extended Type/Channel Aggregation, and/or ARQ feedback IE while the EC (Encryption Control) bit in the GMH is set to 0, the subheader(s) are processed as necessary.
	2. After processing the subheaders the R-CPE will generate a new MAC PDU by:
		1. Strip out the BR and/or GMSH subheader if present, also strip out CRC
		2. Create a new MAC PDU that has GMH with the BR/GMSH indicators in Type field set to 0, preserve settings for Extended Type/Channel Aggregation, ARQ Feedback and packing/fragmentation subheader, recalculate the HCS of the GMH
		3. Add exsiting Extended Type/Channel Aggregatio, ARQ Feedback, and packing/fragmentation subheaders, the existing payload and appended new CRC
	3. The R-CPE forwards the new MAC PDU as currently defined.
	4. MR-BS will process Extended Type/Channel Aggreggation & ARQ feedback IEs, as currently defined
	5. MR-BS will then process the fragmentation subheader, or proceed to processes each packed SDU.
4. When EC bit 0 in GMH received from S-CPE & R-CPE will further fragment/pack PDUs:
	1. When distributed R-CPE receives MAC PDU from a S-CPE with a BR, GMSH, Extended Type/Channel Aggregation, and/or ARQ feedback IE while the EC (Encryption Control) bit in the GMH is set to 0, the subheader(s) are processed as necessary. This is done for each S-CPE that the R-CPE receives a PDU from
	2. For each S-CPE PDU that is received and packing is to be used, each PDU is first transformed by the procedure defined in 3.a and 3.b
		1. If the R-CPE has to pack multiple PDUs from a S-CPE, if will form a new MAC PDU with a GMH that has EC bit set to 0, indicating packing subheader for each packed PDU from an S-CPE, finally attaching a CRC. The R-CPE forwards the new MAC PDU as currently defined.
		2. When the MR-BS receives the packed PDU it will unpack each MAC PDU for the S-CPE.
		3. Each unpacked S-CPE PDU will be processed as indicated in Step 3
	3. For each S-CPE PDU that is received and it has to be fragmented is to be used, each PDU is first transformed by the procedure defined in 3.a and 3.b prior to being fragmented.
		1. If the R-CPE has to fragment a MAC PDU, if will form a new MAC PDU with a GMH that has EC bit set to 0, indicating fragmentation subheader for each PDU fragment from an S-CPE, finally attaching a CRC. The R-CPE forwards each fragment as a new MAC PDU as currently defined.
		2. When the MR-BS receives the new PDU it will unpack the PDU fragment MAC PDU.
		3. It will continue to do this until it receives all fragments from the R-CPE
		4. Once it receives all the fragments of the S-CPEs PDU, MR-BS will only process Extended Type/Channel Aggreggation & ARQ feedback IEs before handing assembled SDU to higher layer

***1.D.5: We need to define a clear procedure for how PDUs are formatted & transmitted when using both & distributed R-CPE. The procedure defiend above should be a good start. It handles what to do when CPEs are configured to use encryption/authentication or not.***

Given the new distributed R-CPE operational mode, we also must first consider how R-CPE and S-CPE network entry and registration should be handled. For distributed R-CPEs themselves, their network entry procedure should follow the established procedure for CPEs.

***1.D.6: Network entry procedure, through registration, for the distributed R-CPEs themselves should be no different than procedures as currently defined.***

S-CPEs entering the network through distributed R-CPEs, require a different consideration than S-CPEs/legacy CPEs that attach directly to the MR-BS. As currently defined in 7.14.3.11.2, we have text that indicates that the distributed R-CPE can be the arbiter of various MAC management message (e.g. RNG-CMD/RSP, REG-REQ/RSP, DREG-CMD). This is extending the capability of the distributed R-CPE far beyond what is necessary, and replactes some of the functionality of the MR-BS. For example, the SM is a component of the MR-BS/BS, and not the R-CPE, therefore location tracking for the purpose of regulatory domain requirements and incumbent protection, should not be a function of the R-CPE.

***1.D.7: In alignment with recommendations 1.C.3 and 1.D.2, we should update 7.14.3.11.2 to make sure that the MR-BS is the final arbiter of certain MAC management messages. The only MAC management messages that the distributed R-CPE should handle itself (i.e. send to receive from the S-CPE directly) are the CBC-REQ/RSP and DREG-CMD (if sent on the basic FID). Much of 7.14.3.11.2 and 7.14.3.11.3 are redundant, suggestion is to collapse some of these sections***

Further considerations related to the distributed R-CPE and use of the Local Cell Update/Container message is provided in section 1.H of this document.

## 1.E Security Considerations specific to centralized R-CPEs

Centralized R-CPEs can be deployed solely to increase capacity of the network. Centralized R-CPEs differ from distributed R-CPEs in that they are “transparent” to the S-CPE. This because they do not transmit their own preambles and MAPs. All major functions regarding communications are made by the MR-BS and negotiated between the S-CPE and MR-BS.

Despite the differences in operation between distributed and centralized R-CPEs, there are two issues that come up when discussing either type of relay. The first issue is how the centralized CPE forwards bursts between the AZ and RZ in the US and DS. The second issue deals with how MAC PDU is formatted and transmitted when concerning transmission with a centralized R-CPE.

***1.E.1: We need to define how a burst is forwarded between access zone and relay zone in the US and DS. Examples of said procedures are rules for using them are listed in sections 6.3.3.8 & 6.3.3.8.1-6.3.3.8.2 of IEEE Std 802.16-2012.***

Concerning these second issue, we don’t need to lay out a procedure that is complicated as the one recommended for distributed R-CPEs (i.e. 1.D.5) in this document. This is because the S-CPE thinks it’s talking directly to the MR-BS, therefore any packing/fragmentation of PDUs, processing of subheaders, how PDUs with the EC bit set in the GMH (and therefore encrypted/authenticated); are handled at the MR-BS or S-CPE. So, existing procedures as defined in the base standard for how MAC PDUs are handled by the S-CPE and MR-BS are sufficient.

***1.E.2: No new procedures needed for describing how MAC PDUs are formatted and handled in the centralized R-CPE network. This presumes that the R-CPE will be allocated resources for the AZ/RZ in both directions, in such a manner that it will not have to fragment/pack or otherwise manipulate MAC PDUs in transit. A statement to this affect should be made in the text***

Given the new centralized R-CPE operational mode, we also must first consider how R-CPE and S-CPE network entry and registration should be handled. For centralized R-CPEs themselves, their network entry procedure should follow the established procedure for CPEs.

***1.E.3: Network entry procedure, through registration, for the centralized R-CPEs themselves should be no different than procedures as currently defined.***

S-CPEs entering the network through centralized R-CPEs, does not require different consideration than S-CPEs/legacy CPEs that attach directly to the MR-BS. Since centralized R-CPEs are “transparent” to the S-CPE, their operation doesn’t impact an end-to-end operation between the MR-BS and S-CPE.

***1.E.4: Given recommendations 1.C.3, 1.D.2 and 1.D.7, we should consider updating or merging 7.14.3.11.2 7.14.3.11.3 to remove any redundancy.***

Further considerations related to the centralized R-CPE and use of the Local Cell Update/Container message is provided in section 1.H of this document.

## 1.F Allocation of resources based on shared common characteristics

In TGb we introduce the GRA-\*\*\* messages to setup a Group Resource Allocation (GRA) construct. The basic purpose of the GRA construct is to reduce overhead for scheduling bandwidth for S-CPEs that may be located in very close proximity to each other and/or have similar data transmission requirements. This functionality is desireable because it doesn’t require each individual subscriber CPE to make bandwidth requests, thereby reducing overhead.

Currently, as defined in Table 19, the GRA-\*\*\* messages are only mapped to the Primary Management FID. When setting the GRA, the GRA-CFG/UPD messages will have to be unicast to each S-CPE being added to the group. This can be inefficient if the group is large enough. Additonal considerations for setting up and manipulating the configuration of GRA groups are provided below (note these are only suggestions:

***1.F.1: To make GRA setup/manipulation more efficient: Add the GRA-CFG as an IE to the DCD/UCD. This way it can be broadcast to the cell and reach all potential group members at once. This method does not have any implications on the security sublayer.***

***1.F.2: To make GRA setup/manipulation more efficient: First setup a multicast group (see 7.17 of 802.22-2011) and add all the S-CPEs to that group. Then multicast the GRA-\*\*\* messages to all of the CPEs within the group. If one member of GRA is a centralized R-CPE, the MR-BS only has to make one multicast transmission. If any member of the group is a distributed R-CPE must first unicast it to the distrubted R-CPE, which then multicasts it to the remaining S-CPEs or could add it to its own DCD/UCD.***

***1.F.3: To make GRA setup/manipulation more efficient and secure: First setup a multicast group (see 7.17 of 802.22-2011) and add all the S-CPEs to that group. Then setup a Group SA (see 8.2.1.1) for that multicast group. Once this is done we can multicast the DS GRA-\*\*\* messages to all of the CPEs w/in the group. If one member of GRA is a centralized R-CPE, the MR-BS only has to make one multicast transmission tthat will be secured on the Primary Multicast Managemet FID. If any member of the group is a distributed R-CPE must first unicast it to the distrubted R-CPE, which then multicasts it to the remaining S-CPEs or could add it to its own DCD/UCD.***

## 1.G A two-link ARQ mechanism

ARQ provides transmission of MAC PDUs that were not received properly to improve robustness of transmission in the US and DS. Currently ARQ maintence is done by the BS and the CPE. This concept is being extended to the R-CPE construct. So regardless of R-CPE type, ARQ can be done on an end-to-end basis between the MR-BS and subscriber CPE.

An additional ARQ mode, two-link, is being considered for R-CPEs in TGb. This mode is applicable to only distributed scheduling R-CPEs. In this mode a separate/distinct ARQ process is mainained on the Relay zone between the MR-BS and R-CPE from a process that would be maintained between the R-CPE and S-CPE on the Access Zone.

The basic operation of the ARQ on either the Access Zone distinct from the Relay Zone is fine. The issue comes with how ARQ feedback is exchanged. ARQ feedback is sent via an IE that is sent as a subheader to the GMH. If the ARQ feedback is sent it’s treated as a per-SDU subheader (see 7.6.1.2), and part of the payload. If S-CPE was setup to provide protection of user data using a cryptographic quite other than 0x00 or 0x01 (as defined), the distributed scheduling R-CPE won’t be able to decrypt the PDU to read the ARQ feedback IE.

***1.G.1: Limit two-link ARQ to operate with S-CPEs connected through distributed R-CPEs.***

***1.G.2: In order to best support and execute two-link ARQ with distributed R-CPEs, the S-CPEs attached to them, have to authenticated and setup with only either cryptographic suite 0x00 (Table 193 802.22-2011). Two link ARQ could possibly be supported for S-CPEs configured for other cryptographic suites if the procedure highlighted by recommendation 1.D.5 is implemented.***

## 1.H Container/Local Cell Update Message operational usage clarification

When considering deployment of either centralized or distributed R-CPEs, we must consider that one or more S-CPEs will be served by a particular R-CPE. This section of the network is considered a “local cell”. In non-relay operation or when using a centralized R-CPE, the BS/MR-BS would have a direct picture of which CPEs (identified by SID) are attached to it.

In a distributed R-CPE relay network, the MR-BS may not have a complete or up-to-date listing of which S-CPEs (by S-CPE SID) are attached through a particular distributed R-CPE. Therefore, to give the MR-BS an up-to-date picture the distributed R-CPE can send a list of currently attached S-CPEs. Toward this end the task group has defined a “Local Cell Update” in section 7.7.25 of the LB2 draft.

Upon reviewing the structure of the “Local Cell Update” message in 7.7.25 the section title of 7.7.25.1 is Local Cell Update REQ, but the first line of Table Y1 indicates this is a “Container Message”. This in and of it self may be confusing, and the terms “local cell update” and “container message” seem to be used inter-changibly in other parts of the LB2 draft (e.g. 7.14.3.11.2-3).

We are trying to cram two different functions into one message. Along these lines the recommendation is to split these into two different functions. The first functional split is outlined in recommendations 1.H.1, the second in 1.H.2.

Regarding 1.H.1 & 1.H.2, the local cell update function should only handle updating the MR-BS with the members of the distributed R-CPE cell. The DREG-CMD process is special because it can be sent on the basic FID or the primary management FID to an attached S-CPE. If sent on basic FID it’s vulnerable to manipulation, while when sent on the primary management FID it is not. A special provision should be optional to allow bundling the DREG-CMD in the DS.

***1.H.1: Update 7.7.25.1 to define it as a “Local Cell Update Indication (LCU-IND)” message sent from distributed R-CPE to MR-BS to give the MR-BS only a list of SIDs of CPEs currently attached through the distributed R-CPE. Update 7.7.25.2 to define it as a “Local Cell Update Acknowledgement (LCU-ACK)” message sent from MR-BS to R-CPE or to acknowledge reception fo the LCU-IND or from R-CPE to MR-BS to acknowledge reception fo the “Local Cell Update Command (LCU-CMD)” (See 1.H.2).***

The distributed R-CPE can handle ranging and basic capability messages being exchanged with the S-CPE. However, other messages must be exchanged between the S-CPE and MR-BS. This includes channel management, multicast setup, SCM authentication/keying, measurements management. To facilitate this we should define, separate from the Local Cell Update process, a “Container Message”. If the container message contains REG-RSP or DREG-CMD, that can be used to key transmission of Local Cell Update information by R-CPE to MR-BS.

***1.H.2: Update 7.7.26.1 to define it as a “Container Message (CON-MSG)” message sent from either MR-BS or R-CPE to the other. Inside of this message will be a list of messages. For each message, the SID of the recipient, the purpose (or message type), size of message, and message conents (full MAC PDU) shall be provided. Update 7.7.26.2 to define it as “Container Acknowledgement (CON-ACK)”. CON-ACK will be used to acknowledge reception of CON-MSG by recipient.***

Given the clarification between Local Cell Update and Container Message processes, some additional rules regarding the forwarding of messages and cell membership updating need to be considered:

* ***1.H.3: The LCU-IND message would be sent from distributed R-CPE to MR-BS whenever an S-CPE has done one of the following: completed the full network entry process (ranging, basic capability negotiation, authentication, registration), or it has been de-registered.***
* ***1.H.4: If R-CPE receives a container message from MR-BS and sees a REG-RSP or DREG-CMD intended for an S-CPE, it will unpack the message from CON-MSG, forward it to S-CPE, and then send LCU-IND to MR-BS.***
* ***1.H.5: When considering defining message types that can be sent from MR-BS and forwarded through a distributed R-CPE, specifc types should be outline for DREG-CMD with action code 0x05/0x04 or 0x03/0x01. We do this because when the action code in DREG-CMD is 0x05/0x0x4 that should be a trigger for distributed R-CPE to send LCU-IND message. Action code of 0x01/0x03 is not fully derigstering the device, therefore it should trigger local cell update.***
* ***1.H.6: If a message being orginiated at MR-BS and bundled in container message to be forwarded by R-CPE, is a message that is being sent on the Primary Management FID, and is being sent to a S-CPE that has completed initial network entry (including authencation); it is recommended that the message shall be encrypted/authenticated. The same goes for messages originated by S-CPE and bundled by R-CPE for transmission to MR-BS.***
* ***1.H.7: Due to security consideration it is recommended that we forbid distributed R-CPE from originating a DREG-CMD itself, this will only be allowed for ranging and basic capabilities.***
* ***1.H.8: If distributed R-CPE receives container message that includes a RNG-CMD intended for a S-CPE in it’s cell, it will forward that RNG-CMD to the S-CPE.***

# 2. Extensions of Existing Cryptographic Methods

Configuration options for and the application of cryptographic methods that ensure privacy and integrity of MAC PDUs are described in Section 8.4 of the IEEE Std. 802.22-2011. The biggest impact that the application of a cryptographic method has is the overehead it adds to MAC PDU generation and transmission (see 8.4.2.1 of 802.22-2011). The overhead added to the MAC PDU is made up of a “PN” value added before the PDU payload and the “Ciphertext ICV” added at the end.

The “PN” value is a counter that keeps track of the # of PDUs encrypted/integrity protected with using the current key that a CPE is setup with. Only one PDU can be encrypted by that key for a particular PDU. By keeping track of the current “PN” value, the CPE and BS can prevent a malicious user from attempting a replay attack (i.e. essentially trying re-transmit a PDU). Currently the “PN” value was allocated to be 3bytes/24bits, where half of that space is allocated to track “PN” values associated with DS PDUs and the other half associated with US PDUs. This means that “PN” will be exhausted after approximately 8e6+ PDUs either DS/US, thus causing the CPE to request a re-keying. If we employ newer modulation/coding modes as well as channel aggregation (Seciont 3 of this document), we could run through the “PN” space much faster than originally intended. This would cause the CPE to need to be re-keyed more often, potentially interrupting service.

***2.1: To avoid premature exhaustion of PN-space we SHALL increase the PN-space to be represented by 4bytes/32bits. This should provide us with more “room” with regard to PN usage, and avoid excessive re-keying of CPEs.***

The other component of cryptographic overhead is the “Ciphertext ICV” that is appended to the end of the PDU. The “Ciphertext ICV” is an integrity check value whose purpose is to allow the person receiving the PDU to verify the integrity of the received PDU. The difference between this method, and say a CRC, is that the “Ciphertext ICV” is generated using more information (e.g. an encryption key) and the ICV itself is very robust to errors and can’t be brute-forced. Currently the “Ciphertext ICV” is generated as part of the AES-GCM (Advanced Encryption Standard-Galois Counter Mode) process, and the size of the ICV defined is 8bytes/64bits. This singular setting is inflexible when considering the extensive modifications to MCS and the increase in throughput. Adding newer modes with a larger ICV with allow for better protection when transmitting PDUs at a larger rate or of a larger size through the channel. The current setting could be considered excessive when considering the datarate/transmission modes currently available in the base standard. Adding newer modes with a smaller ICV size will allow for more efficient operation if the user/network operator desires.

***2.2: Additonal cryptographic methods SHALL be added that make use of a 4byte as a minimum, while the existing 8byte ICV size, will be kept. Additional text given recommendations for which methods to configure for a CPE given the MCS selected for the CPE will be provided as well.***

Currently in the base standard, use of the EC bit in the GMH is used to indicate what type of cryptographic suite is applied to transmission and reception of MAC PDUs. The value of how ECbit is set affects the formatting of MAC PDUs (see section 1.D and 1.E of this document. Unfortunately the conditions on how this bit is set and manipulated can be confusing (see definition of EC field in GMH, negotiation of security parameters in 8.2.2.7 of 802.22-2011).

***2.3: The EC==0 setting should only be applicable when the 0x00 cryptographic suite is selected for the CPEs security association, otherwise it should be 1. This modification will also require updating text (at a minimum) in 8.2.2.7 and description portion of the EC field definition in the GMH.***

# 3. Multi-channel Operation Considerations

Multi-channel operation (see section 7.24 in LB2), aka channel aggregation, is a new capability being considered for addition to the 802.22 standard. This functionality allows the MR-BS and CPEs to make use of multiple channels (simultaneously) to increase the available system bandwidth. There are several points of clarification regarding this new functionality that need to be settled when considering security procedures.

Will the Multi-channel operation and Relay/R-CPE be used simultaneously? The text and example modes (Figure AN1, AO1) in section 7.24 make no mention of R-CPEs. The operation of BS/CPE CAM and CHU, as currently dfined, doesn’t seem like it would be affected. However, if R-CPEs can be used with channel aggregation, the use of the Extended Type/Channel Aggregation subheader, would have to be handled according to the procedures in 1.D and 1.E. These procedures outline how to forward and process MAC PDUs and attached subheaders for situations when MAC PDUs are encrypted/authenticated or not. Also, the text that exists in section 7.24 doesn’t seem to clearly address how the Extended Type/Channel Aggregation subheader is used.

***3.1: If Channel Aggregation is to be used with R-CPEs: Clarification of this operation must be made known in 7.24. This clarification should mention any differenes in channel aggregation use given the type of R-CPE, how the Extended Type/Channel Aggregation subheader is to be used/configured, as well as indication mention of the text that will be added regarding MAC PDU and subheader handling as outline in 1.D and 1.E of this contribution.***

***3.2: If Channel Aggregation and R-CPE operation are mutually exclusive: Clarification regarding this separation (or mutual exclusiveness) of these operational modes must be made in section 7.24. The procedure for how the Exteneded Type/Channel Aggregation subheader is to be used/configured needs to be outlined as well. The processing of MAC PDUs that included the Extended Type/Channel Aggreation subheader will follow existing procedures.***

Now we move to the structure of the Extended Type/Channel Aggregation subheader itself. Implementation of either recommendation 3.1 or 3.2, will require text explaining the procedure for how this subheader is handled. First of all, there is an “Aggregation Type” field that can apparently be set between subsequent transmissions. This could possibly wreak havoc on the security sublayer. If encryption/authentication for a S-CPE is enabled, each MAC PDU that is processed has a PN counter (see 8.4.2 of 802.22-2011), appended to it to provide a measure of protection against replay attacks. The S-CPE/MR-BS uses the PN value received in MAC PDU and checks it against the value it expects it to be +/- a window the received PN could fall in.

If the “Aggregation Type” is set to 0x01/”Transmit Diversity”, one would assume that multiple copies of the exact same PDU are copied to transmissions from each CHU. The receiving node (either MR-BS/S-CPE) would be receiving multiple copies of that PDU.

If the “Aggregation Type is set to 0x02/”Bulk Transmission Mode”, one would assume unique PDUs each with it’s own PN value would be sent through each CHU. The receiving node, would have to have it’s PN window adjust to make sure that the expected PN falls within the window PN\_WINDOW\_SIZE = PN - # of active CHUs : current\_window : PN + # of active CHUs.

Logic could be added regarding monitoring of PN window for each Aggregation Type, but the requirement to support both dynamically will manipulating/verifying encrypted/authenticated MAC PDUs very difficult.

***3.3: Define process by which aggregation type is setup is fixed, or statically managed for a period of time. This implies that only one aggregation type can be engaged in the MR-BS cell at a given time.***

***3.4: Updated text in 8.4.2.1.1 in 802.22-2011 regarding how PN # is to be treated.***

Another consideration is enlarging the PN counter space to addressed transmission of PDUs at an increase rate. Fortunately, recommendation 2.1 in this contribution already addresses this.

Finally, we must also consider the channel aggregation setup/configuration processes outlined in section 7.24.1 of LB2. The first point of contention comes with either of the procedures for adding a new operating channel (7.24.1.1 and 7.24.1.2). How is each CHU (at either the BS or CPE) uniquely identified? At the BS-CHU, using a unique BSID for each BS-CHU is not a problem. From the perspective of the S-CPE, each BS-CHU appears to be a different BS.

However, from the perspective of the CPE-CHU, each requiring its own ID presents a unique problem. Currently any credentials used to allow the CPE to authenticate to the network require a unique ID bound to that CPE. This “unique ID” comes from the FCC ID, Serial #, MAC Address of the device. So, if each CPE-CHU has to have its own “unique ID” that includes a unique MAC Address, then each CHU has to authenticate with at minimum before registration can proceed. Once registration starts, the BS-CHU would have to check its location and see if the CPE-CHU can be allowed service in the network. This might not be a problem if part of the “unique ID” of a CPE CHU doesn’t include a unique MAC Address for that CPE CHU. If it did, each CPE-CHU would also be required to be registered with the database.

Unique identifying BS/CPE-CHU by MAC address will pose problems, and will lead to additional complexity, e.g. the instantiation of multiple MACs at each CPE and require multiple authentications for each CPE-CHU or require re-design of authencation credentials for those CPEs that wish to engage in channel aggregation operations. Security sublayer procedures work best when considering there is one ID for each device. Other optimizatons of Channel Aggregation processes, with or without regard to security practices are TBD (at least until we’ve had discussions on issues/recommendations 3.5 and 3.6.

***3.5: Need clarification on what constitutes a “ID” for a BS/CPE-CHU. If each CHU needs to be uniquely identified, and that the required identity includes MAC Address/FCC ID/Serial #, then any CPEs engaged in channel aggregation will require to only be authenticated and no protection for user data will be afforded. This is still problematic, because each CPE-CHU would required its own credential, given the design of credentials in the existing base standard. A new authentication credential could be design, specific to channel aggregation operations. This isn’t desirable because other systems like Wave2 WiMAX or LTE-Advanced accommodate channel aggregation without these requirements.***

***3.6: Clarification on the ID type for each CHU with regard to the following procedures as defined int the base-standard: registration (REG-REQ/RSP), TVWS databse device registration, and TVWS channel querying have to also be taken into consideration.***

# 4. CBP Protection Considerations

In the base standard method for providing authentication over CBP MAC PDUs transmitted in the SCW were provided. The CBP authentication method is decribed in Section 8.6.2 of 802.22-2011, and is based on a design using ECC-based implicit certificates. These certificates and the authentication signature generation and verification schemes are based on the methods developed for the wireless microphone beacon that is defined in the 802.22.1-2010 standard. The purpose of the CBP protection mechanisms provided in 8.6.2 of 802.22-2011 is to prevent malicious users from formatting and transmitting their own CBP MAC PDUs and transmitting them, thus causing recipients to have to act on them and possibly vacate/share channels with entities that are not legitimate 802.22 (or other TVBDs that can process CBP) networks.

In the base standard, the CBP generation/transmission process can be summarized as follows:

1. The SM/BS schedules the active SCW opportunity
2. SM/BS formats a CBP MAC PDU for each CPE it wishes to transmit a CBP
3. BS delivers the CBP MAC PDU to each CPE via the “CBP Relay Message”
4. Each CPE unpacks CBP MAC PDU from the “CBP Relay Message” and transmits it in the scheduled SCW

In the base standard, the CBP reception process can be summarized as follows:

1. The SM/BS schedules the passive SCW opportunity
2. CPE listens during the scheduled passive SCW and captures any received CBP transmission
3. CPE delivers the CBP MAC PDU contents in a bulk measurement report
4. BS unpacks the CBP MAC PDU from bulk measurement report and process it accordingly.

Alternatively, the BS can transmit/receive CBP MAC PDUs in active/passive SCWs that it schedules itself.

The CBP generation/transmission and reception processes were designed as such to put the burden on generation and processing of CBP MAC PDUs into solely the Spectrum Manager/BS and not the CPEs. Since CBP MAC PDUs are not generated on as frequent a basis as other items such as control headers/DCD/UCD, locating CBP MAC PDU processing solely in the Spectrum Manager/BS should not add too much of a burden, regardless of whether or not the CBP Protection mechanism is employed.

The current modifications to section 7.20.1, 7.20.2, and 7.20.3 outlined in LB2 do not conflict with this premise. In 7.20.4.2, we consider reception of a DRZ-FCH as a means of network discovery. The only useful information the DRZ-FCH carries is the CPE ID (MAC address) of the distributed R-CPE. This in and of itself is not very useful information with regards to coexistence. Other items such as coexistence capabilities, quiet period scheduling, SCW scheduling, frame allocations w/in superframe, etc; are also necessary when considering using CBPs for network discovery and coexistence. Also given the design and location of CBP authentication processing located at the SM/BS, then if the DRZ-FCH is a contender for inclusion in a CBP MAC PDU, then CBP Protection mechanisms can’t be employed. Also CBP MAC PDU design laid out 7.20.1.1a, there is no mention of DRZ-FCH.

***4.1: update section 7.20.4 to reference “FCH” as “FCH PHY mode 2” and/or “FCH Phy Mode 2 + Ext FCH”***

***4.2: Remove reference to DRZ-FCH in 7.20.4. Unless there is a compelling reason, DRZ-FCH should not be used as means of identifying a neighboring R-CPE/MR-BS network and that network’s capabilities.***

Give the extensive changes to structure/format of the control header for PHY Mode 2, then the existing text in 8.6.2 needs to be updated to include the elements of the new FCH PHY Mode 2 or FCH PHY Mode 2 + Ext FCH that could possible be transmitted. In the base standard element of the SCH data (namely the BS ID) are used in the certificate generation, certificate verification, signature generation, and signature verification processes.

***4.3: Make changes to text in 8.6.2 to properly accommodate any references to contents of CBP MAC PDU header (FCH PHY Mode 2 or FCH PHY Mode 2 + ext FCH) in certificate generation, certificate validation, signature generation, and signature validation processes associated with CBP MAC PDU generation.***

**References:**

[1] IEEE P802.22b™/D2.0 Draft Standard for Wireless Regional Area Networks Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands - Amendment: Enhancement for broadband services and monitoring applications, April 2014.

[2] IEEE Standard for Information Technology—Telecommunications and information exchange between systems Wireless Regional Area Networks (WRAN)— Specific requirements, Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands, IEEE Std. 802.22-2011, ISBN 978-0-7381-6724-4

[3] Pyo, Chang-woo, “802.22b Letter Ballot 2 Comment database”, DCN 22-14/74r3, https://mentor.ieee.org/802.22/dcn/14/22-14-0074-03-000b-802-22b-letter-ballot-2-comment-database.xlsx