**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **PHY Security Primitives** | |
| Date Submitted | May, 2016 | |
| Source | [Byung-Jae Kwak 1, Sangseok Yun 2, Jeongseok Ha 2, Nah-Oak Song 2,] [ETRI 1, KAIST 2] [address] | Voice: [ ] Fax: [ ] E-mail: [bjkwak@etri.re.kr]1, [ssyun@kaist.ac.kr, nsong@kaist.ac.kr]2 |
| Re: |  | |
| Abstract | Primitives required to support PHY layer security | |
| Purpose | Discussion and approval. | |
| Notice | This document has been prepared to assist the IEEE P802.15. 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 acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

1. Overview
2. Normative references
3. Definitions
4. General description
5. MAC protocol
   1. MAC functional description
   2. MAC frame formats
   3. Synchronization procedure
   4. Discovery
   5. Peering
   6. Communication period
   7. MAC commands
      1. Discovery request command
      2. Discovery response command
      3. Peering request command

This command shall be sent by a PD that wishes to peer with a PAC network.

The AR field shall be set to one.

The Peering request command Content field shall be formatted as illustrated in Figure 50.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Bit: **0** | **1** | **2** | **3** | **4-5** | **6** | **7** | **Octets:** 0/2 |
| Reserved | Power source | Receiver on when idle | Security enable | Group mode | PHY security suppor | Reserved | Group ID |

Figure —Peering request command Content field format

Table —Group mode

|  |  |
| --- | --- |
| Group mode | Description |
| 00 | One-to-one [no Group ID present] |
| 01 | One-to-many peering |
| 10 | Many-to-many peering |
| 11 | Reserved |

The Power source field shall be set to one if the device is receiving power from the alternating current source. Otherwise, the Power source field shall be set to zero.

The Receiver on when idle field shall be set to one if the device does not disable its receiver to conserve power during idle periods.

The Security enable field shall be set to one if the device is capable of sending and receiving cryptographically protected MAC frames.

Group ID shall be present if Group enable field is set to one.

PHY security support field shall be set to one if the PD supports PHY layer security, and zero otherwise.

* + 1. Peering response command

The peering response command allows a PD to communicate the results of a peering attempt back to the PD requesting peering.

The Peering response command Content field shall be formatted as illustrated in Figure 51.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bits: 0-1** | **Bits:2-3** | **Bit: 4** | **Bits: 5 - 7** | Octets: **1/2** |
| Group mode | Peering status | PHY security support | Reserved | Multicast group address |

Figure —Peering response command Content field format

GroupMode is indicated in Table 20.

The multicast group address field shall contain the multicast group address (2 octets) of the PAC group.

The values of the Peering status field are defined in Table 21.

Table —Peering status field values

|  |  |
| --- | --- |
| Peering status value | Description |
| 0 | Success |
| 1 | PAC Group at capacity |
| 2 | Access denied |
| 3 | Channel access failure |

If a PD receives a Peering request command with PHY security support field set to one and the PD supports PHY layer security, the PD shall respond with Peering response command with PHY security support set to one. Otherwise, the PHY security support shall be set to zero.

* + 1. De-peering notification command

1. MAC services
   1. MLME-SAP primitives

The MLME-SAP allows to access management commands between the MAC sublayer and MAC user. Table 24 summarizes the primitives supported by the MLME-SAP interface.

Table —MLME-SAP primitives

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Request** | **Confirm** | **Indication** | **Response** |
| MLME-GET | 6.1.1.1 | 6.1.1.2 | − | − |
| MLME-SET | 6.1.1.3 | 6.1.1.4 | − | − |
| MLME-DISCOVERY | 6.1.2.1 | 6.1.2.3 | − | − |
| MLME-PEERING | 6.1.3.1 | 6.1.3.2 | 6.1.3.3 | 6.1.3.4 |
| MLME-DE-PEERING | 6.1.4.1 | 6.1.4.2 | 6.1.4.3 | − |
| MLME-FRAME-ERROR-NOTIFICATION | − | − | 6.1.5.1 | − |
| MLME-RESET | 6.1.6.1 | 6.1.6.2 | − | − |
| MLME-RECEIVER-ENABLE | 6.1.7.1 | 6.1.7.2 | − | − |
| MLME-SCAN | 6.1.8.1 | 6.1.8.2 | − | − |
| MLME-GROUP-START | 6.1.9.1 | 6.1.9.2 | 6.1.9.3 | 6.1.9.4 |
| MLME-SYNCHRONIZATION | 6.1.10.1 | 6.1.10.2 | − | − |
| MLME-SYNCHRONIZATION-LOSS | − | − | 6.1.10.3 | − |
| MLME-CHANNEL-SOUNDING | 6.1.11.1 | 6.1.11.2 | − | − |
| MLME-DPS | 6.1.12.1 | 6.1.12.2 | 6.1.12.3 | − |
| MLME-CALIBRATE | 6.1.13.1 | 6.1.13.2 | − | − |
| MLME-GETCHVALUE | 6.1.14.1 | − | − | 6.1.14.4 |
| MLME-POSTPROCESSING | 6.1.15.1 | 6.1.15.4 | 6.1.15.3 | 6.1.15.2 |

* + 1. PIB access
    2. Discovery primitives
    3. Peering primitives

These primitives are used when a PD becomes peered with another PD.

* + - 1. MLME-PEERING.request

This primitive requests peering with given PD. The properties of this primitive are:

MLME-PEERING.request{

ChannelNumber;

ChannelPage;

GroupMode

MulticastGroup\_ID;

DestinationAddress;

CyclicSuperframeStructure;

PhySecuritySupport;

}

The primitive parameters are defined in Table 35.

Table —MLME-PEERING.request parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Valid range** | **Description** |
| ChannelNumber | Integer | Any valid channel number as defined in Table 67 | The channel number on which to attempt peering. |
| ChannelPage | Integer | Any valid channel page as defined in Table 67 | The channel page on which to attempt peering. |
| GroupMode | Integer | As defined in Table 20 | Group mode determines the type of peering procedure |
| MulticastGroup\_ID | Integer | 0 to 216 −1 | Group ID provided by the application layer. |
| DestinationAddress | MAC address | IEEE 48 bit address | Address of the PD with which to peer for one-to-one peering. |
| CyclicSuperframeStructure | Cyclic-superframe structure descriptor | As defined in Table 31 | Indicates the structure of cyclic-superframe |
| PhySecuritySupport | Enumeration | TRUE, FALSE | Indicates whether the PD is using PHY layer security mode |

When receiving the MLME-PEERING.request primitive with the CyclicSuperfreamStructure parameter, the MAC sublayer sets the PIB with the value of the cyclic-superframe structure descriptor and selects the start time of a cyclic-superframe. After starting a cyclic-superframe, the MAC sublayer inserts the Cyclic-superframe descriptor IE to the MAC header of the Peering Request command frame. The MAC sublayer schedules to access a period of a superframe of a cyclic-superframe.

* + - 1. MLME-PEERING.indication

The primitive is used to indicate the reception of a Peering request command. The properties of this primitive are:

MLME-PEERING.indication{

SourceID;

GroupMode

MulticastGroupID

PHYcapability;

CyclicSuperfameStructure;

PhySecuritySupport;

}

The primitive parameters are defined in Table 37.

Table —MLME-PEERING.indication parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Valid range** | **Description** |
| SourceID | MAC address | PD specific | Address of the PD requesting peering. |
| GroupMode | Integer | As defined in Table 20 | Group mode determines the type of peering procedure |
| MulticastGroup\_ID | Integer | 0 to 216 −1 | Group ID of the requested group. |
| PHYcapability | Enumeration | LOW\_MOBILITY, HIGH\_MOBILITY, GFSK, UWB\_BPM\_BPSK, UWB\_OOK | Operational capability of the PD requesting peering. |
| CyclicSuperframeStructure | Cyclic-superframe structure descriptor | As defined in Table 31 | Indicates the structure of cyclic-superframe |
| PhySecuritySupport | Enumeration | TRUE, FALSE | Indicates whether the PD is using PHY layer security mode |

When receiving the Peering Request command frame with the Cyclic-superframe descriptor IE, the MAC sublayer sets the PIB with the value of Cyclic-superframe Duration field, Primary superframe Number field, Primary superframe Type field, and Secondary superframe Type field. The MAC sublayer notifies the receiving the cyclic-superframe structure to the higher layer with MLME-PEERING.indication primitive. The MAC sublayer calculates the next start of a cyclic-superframe structure with the value of Sequence Number field and of Cyclic-superframe Duration field, and starts to schedule to access a period of a superframe of a cyclic-superframe.

* + - 1. MLME-PEERING.response

The primitive is used to initiate a response to an MLME-PEERING.indication primitive. The properties of this primitive are:

MLME-PEERING.response{

SourceID;

GroupMode;

MulticastGroup\_ID;

Status;

PhySecuritySupport

}

The primitive parameters are defined in Table 38.

Table —MLME-PEERING.response parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Valid range** | **Description** |
| SourceID | MAC address | PD specific | Address of the PD requesting peering. |
| GroupMode | Integer | As defined in Table 20 | Group mode determines the type of peering procedure |
| MulticastGroup ID | Integer | 0 to 216 −1 | ID of the MulticastGroup |
| Status | Enumeration | SUCCESFUL, OUT\_OF\_CAPACITY, ACCESS\_DENIED, | Status of the peering attempt. |
| PhySecuritySupport | Enumeration | TRUE, FALSE | Indicates whether the PD is using PHY layer security mode |

* + - 1. MLME-PEERING.confirm

The primitive reports the result requested by MLME-PEERING.request of the initiating PD. The properties of this primitive are:

MLME-PEERING.confirm{

DestinationAddress;

GroupMode;

MulticastGroup\_ID;

Status;

PhySecuritySupport

}

The primitive parameters are defined in Table 36.

Table —MLME-PEERING.confirm parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Valid range** | **Description** |
| DestinationAddress | MAC address | PD specific | Address of the peered PD. |
| GroupMode | Integer | As defined in Table 20 | Group mode determines the type of peering procedure |
| MulticastGroup\_ID | Integer | 0 to 216 −1 | Group ID of the established group. |
| Status | Enumeration | SUCCESS, CHANNEL\_ACCESS\_FAILURE, NO\_ACK, ACCESS\_DENIED, | The status of the peering attempt. |
| PhySecuritySupport | Enumeration | TRUE, FALSE | Indicates whether the PD is using PHY layer security mode |

If the peering request was successful, then the Status parameter will be set to SUCCESS. Otherwise, the Status parameter will be set to indicate the type of failure.

* + 1. De-peering primitives
    2. Frame error notification primitives
    3. Reset MAC sublayer
    4. Receiver enable
    5. Channel scanning
    6. Group configuration
    7. Synchronization
    8. Channel sounding
    9. Dynamic preamble selection
    10. Ranging calibration
    11. Randomness sharing primitives

These primitives are used to request and report quantized channel information,

* + - 1. MLME-GETCHVALUE.request

This primitive requests MAC to quantize and report channel information. The properties of this primitive are:

MLME-GETCHVALUES.request{

}

* + - 1. MLME-GETCHVALUES.response

This primitive reports the result requested by MLME-GETCHVALUES.request. The properties of this primitive are:

MCPS-GETCHVALUES.confirm{

QuantizedCHInfo;

}

The primitive parameters are defined in Table 59.

Table 59—MLME-GETCHVALUES.response parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Valid range** | **Description** |
| QuantizedCHInfo | Integer | 0 to (252 −1) | 1bit quantized channel information |

* + 1. Post processing primitives

These primitives are used to initiate post processing procedure which includes information reconciliation and privacy amplification.

* + - 1. MLME-POSTPROCESSING.request

This primitive requests post processing procedure with given PD. The properties of this primitive are:

MLME-POSTPROCESSING.request{

DestinationAddress;

InfoReconciliation;

PrivacyAmp;

}

The primitive parameters are defined in Table 60.

Table 60—MLME-POSTPROCESSING.request parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Valid range** | **Description** |
| DestinationAddress | MAC address | IEEE 48 bit addressing | Address of the PD with which to peer for one-to-one peering. |
| InfoReconciliation | Bit stream | TBD | A parity part of codeword generated by initiating PD for information reconciliation |
| PrivacyAmp | Integer | TBD | The number of bits which should be eliminated in privacy amplification |

* + - 1. MLME-POSTPROCESSING.indication

This primitive is used to indicate the reception of a post processing request command. The properties of this primitive are:

MLME-POSTPROCESSING.indication{

DestinationAddress;

InfoReconciliation;

PrivacyAmp;

}

The primitive parameters are defined in Table 61.

Table 61—MLME-POSTPROCESSING.indication parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Valid range** | **Description** |
| DestinationAddress | MAC address | IEEE 48 bit addressing | Address of the PD with which to peer for one-to-one peering. |
| InfoReconciliation | Bit stream | TBD | A parity part of codeword generated by initiating PD for information reconciliation |
| PrivacyAmp | Integer | TBD | The number of bits which should be eliminated in privacy amplification |

* + - 1. MLME-POSTPROCESSING.response

This primitive is used to initiate a response to an MLME-POSTPROCESSING.indication primitive. The properties of this primitive are:

MLME- POSTPROCESSING.response{

Status;

}

The primitive parameters are defined in Table 62.

Table 62—MLME-POSTPROCESSING.response parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Valid range** | **Description** |
| Status | Enuermation | SUCCESS, FAIL | The status of CRC check after post processing |

* + - 1. MLME-POSTPROCESSING.confirm

This primitive reports the result requested by MLME-POSTPROCESSING.request of the initiating PD. The properties of this primitive are:

MLME-POSTPROCESSING.confirm{

DestinationAddress;

Status;

}

The primitive parameters are defined in Table 63.

Table 63—MLME-POSTPROCESSING.confirm parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Property** | **Type** | **Valid range** | **Description** |
| DestinationAddress | MAC address | IEEE 48 bit addressing | Address of the PD with which to peer for one-to-one peering. |
| Status | Logical | SUCCESS, FAIL | The status of the request for post processing |

* 1. MAC data service

1. General PHY requirements
2. PHY services
   1. Overview
   2. PHY description
   3. PHY procedures
   4. PHY measurements
   5. PHY services
      1. PLME-SAP primitives
         1. PHY characteristics
         2. Channel information primitives

These primitives are used to provide the channel information.

* + - * 1. PLME-GETCHVALUE.request

This primitive requests a PHY to quantize and report channel information.

PLME-GETCHVALUES.request{

}

* + - * 1. PLME-GETCHVALUE.response

This primitive reports the result requested by PLME-GETCHVALUES.request. The properties of this primitive are:

PLME-GETCHVALUES.response{

QuantizedCHInfo,

}

The primitive parameters are defined in Table 77.

The values assigned to the parameters are specified for the PHYs in clause 9. Not all parameters are used by all PHYs defined within this standard.

Table 77—PLME-GETCHVALUES.response parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Type** | **Value** | **Description** |
| QuantizedCHInfo | Integer | 0 to (252 −1) | 1bit quantized channel information |

* + 1. PHY-SAP primitives