IEEE P802.15

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **Corrigendum Worksheet** |
| Date Submitted | 18 November, 2009 |
| Source | [Pat Kinney][Kinney Consulting LLC][Lake Zurich, IL] | Voice: [+1 847 960 3715]E-mail: [pat.kinney@ieee.org] |
| Re: | [A committee has been formed, headed by Pat Kinney, vice chair of 802.15, to address the need to correct existing standards as per IEEE rules.] |
| Abstract | [The following submission is a call for participation, applications and proposals from the IEEE, Industry, and Academia.] |
| Purpose | [Request for corrigendum of the IEEE 802.15.4-2006 standard and 802.15.4a-2007] |
| 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. |

**Corrigenda committee members:**

* Patrick Kinney (Kinney Consulting LLC)
* Phil Beecher (PB Consulting)
* James Gilb (SiBeam)
* Jay Bain (Fearn Consulting)

**Request for Corrigenda:**

1. Submitted by Phil Beecher, Integration UK Ltd; 12 November 2007

Section 7.5.8.2.3 Incoming security processing. Sections c) and f) appear to be contradictory. How should the receiver behave when a frame is received with Security Enabled field set to 1 but when the security level in the frame is set to 0? Is this covered in c)? If so, what does f) refer to?

1. Submitted by Phil Beecher, Integration UK Ltd; 12 November 2007

We have been looking at the PHY section of 15.4-2006. Section 6.1.2.2 Channel pages references phyPagesSupported in the PHY PIB, but I cannot find it in the PIB. Was this an omission? Did it ever get given an attribute ID value?

1. Submitted by Phil Beecher, Integration UK Ltd; 8 January 2008

I think there is another problem with 15.4-2006, this time concerning association. The spec describes the behaviour when a device disassociates, also when the coordinator refuses the association request, but it does not describe what should happen if a communication error occurs during the association process, causing the process to fail. I believe this was an oversight in the spec and that the behaviour should be described.

1. Submitted by Phil Beecher, Integration UK Ltd; 9 April 2008

Please could you clarify the behaviour of the MAC in the following situation?

A device is participating in a beacon-enabled network, tracking the beacon of its parent and generating its own beacon.  It receives a beacon from its parent in which the Superframe structure is changed in such a way as to cause the device’s outgoing beacon characteristics to knowingly violate the parent Superframe.

1) Should the device stop sending its own beacon?

2) Inform the next higher layer (NHL) that it has stopped, and if so how?

I think the answers to both these questions should be "yes", and that the device should inform the NHL by generating an MLME-SYNC-LOSS.indication with status of SUPERFRAME\_OVERLAP.  This status enumeration was added in 15.4-2006 as a status for the MLME-START.confirm message to cover the condition described when it occurs during the MLME-START.request.

1. IEEE Std 802.15.4a-2007, 6.8a.12.1, submittedbyDusan Radovic, TES Electronic Solutions, 9 February 2007

Could you clarify the pulse duration given in 6.8a.11.1?

Is it defined on the half of pulse amplitude or as width of the main lobe (from zero to zero)?

In the same part, in the mathematical description (formula), right medium bracket is misplaced should be before the plus sign in the nominator.

1. Submitted by Rene Struik, Certicom, Clause 7.5.8.2.3

Incoming security frame processing does not treat devices with diplomatic immunity (“Exempt status”) properly.

1. The 802.15.4-2006 phrase "**one of the optional PHYs"** is ambiguous since it would seem that optional PHYs from TG4a, TG4c, TG4d, and so on would be required to include the 15.4-2003 868/915 MHz PHYs.
2. IEEE Std 802.15.4a-2007: According to equation 9b (page 76) the systematic output of the encoder g\_0^(k) is encoded into the position of the pulse of the k-th BPPM-BPSK symbol.  According to figure 27j (page 79) input bit b\_0 of the convolutional encoder is mapped to output systematic bit g\_0^(0). The same for subsequent bits, e.g. b\_1 is mapped to g\_0^(1).  However, according to the specification of the convolutional encoder in section 6.8a.10.2 and figure 27k (page 80) there is a one bit delay which would result in e.g. bit b\_0 being mapped to g\_0^(1). Also, g\_0^(0) is always 0 (assuming required initialization of the encoder to the 00 state) so the corresponding transmitted bit doesn't carry any information.
3. IEEE Std 802.15.4a-2007: The published standard is wrong. The equation for C5 should be: C5 = XOR(R0, R1, L1, L3, L4, L6, EXT, P0, P1).

1. IEEE Std 802.15.4a-2007: The rate change ambiguity is not quite as easy, in that we don’t have a unanimous agreement even among ourselves about the correct fix.  Michael says that hardware should be built to most closely adhere to the spec that we all agree is self-contradictory.  This has the practical effect of making the switch to the faster symbol rate happen a little sooner.  I say, “The spec is just wrong, so forget about salvaging wrong stuff, and fix it in the way that does the best thing for system performance.”  That has the practical effect of making the switch to the faster symbol rate happen a little later.   I now work for a telephone equipment company, and Michael is building UWB radio hardware, so Michael’s vote trumps mine.  But…. are we the only two guys who get to vote?  On the first two more obvious issues, I don’t think anyone would feel that a vote is necessary.
2. IEEE Std 802.15.4a-2007: Figure 27j is wrong
3. IEEE Std 802.15.4a-2007, Page 73, line 53, SubmittedbyDusan Radovic, TES Electronic Solutions, 9 February 2007

Instead of “Figure 39c” should be “Table 39c”.

1. IEEE Std 802.15.4a-2007, Page 75, Figure 27d, SubmittedbyDusan Radovic, TES Electronic Solutions, 9 February 2007

SFD for nominal low rate of 150 Kb/s is not according to SFD definition at the page 78. The last two symbols in the Figure 27d have wrong sign, should be –Si and Si.

1. IEEE Std 802.15.4a-2007, Page 89, SubmittedbyDusan Radovic, TES Electronic Solutions, 9 February 2007

Pulse definition formula and duration. One bracket is misplaced in the formula for the referent pulse. Cosine function should contain only of the first part, not of whole nominator. With Tp=2ns the pulse r(t), from the formula, has duration of 2ns. The pulse duration is defined at the half of its maximum amplitude. From Figure 27m referent pulse r(t) duration, defined at the half of the maximal amplitude, is around 1ns. When zero to zero duration is measured it is around 2ns.

1. IEEE Std 802.15.4a-2007, 6.8a.12.: the reference pulse does not comply directly with the PSD requirement
2. IEEE Std 802.15.4a-2007, ***Regarding 6.8a.12.1***

Could you consider the following missing definition of the pulse position?For pulses that have duration Tp shorter than the chip duration, Tc, it is not defined position in a chip. It might be from the beginning of a chip Tp, or centralized position, or Tp before the end, or…

This clarification might be added in 6.8a.12.1 part Baseband impulse response part.

1. Table 39c is erroneous
2. Sections 6.8a.8 (Data Field), 6.8a.9 (UWB PHY Modulation) and 6.8a.10 (UWB PHY FEC) all assume that the convolutional code is used.

The mapping of the bits in case of the convolutional code is not used (which one goes to polarity, which one to position) is not specified.

1. Clause 7.5.6.1 clarify ambiguity in transmission of secure frame

**Resolutions:**

**Item 1)** IEEE Std 802.15.4-2006

No change required:

Step a) in the procedure identifies the case where the Security Enabled subfield is set to zero and the security level thus becomes zero. It is this security level which applies throughout the rest of 7.5.8.2.3 except in the case of c), i.e. the case where the Security Enabled subfield is set to one. In this case, the procedure ensures that the Security Level subfield of the Security Control field is not zero - if it is, it rejects the frame at that point. So the apparently contradictory case in f) only applies when the Security Enabled subfield is set to zero.

This text could perhaps be clearer but this is the result of trying to write a logical procedure in something resembling English whereas a language with proper control flow constructs would have been more appropriate

**Item 2)**IEEE Std 802.15.4-2006

Change required:

The PHY PIB name used on page 29 in the second line of Clause 6.1.2.2 should be corrected to read as "*phyChannelsSupported*". Both the pages and channels supported within that page can be obtained via this attribute and provides the information that a *"phyPagesSupported"* PHY PIB Attribute would.

**Item 3)** IEEE Std 802.15.4-2006

Change required:

15.4-2006 Page 181 section 7.5.3.1 Replace: “If the Association Status field of the command indicates that the association was unsuccessful, the device shall set *macPANId* to the default value (0xffff).”

 with

“If the Association Status field of the command indicates that the association was unsuccessful, or, if there is a communication failure during the association process due to a missed acknowledgement or the association response command frame is not received, the device shall set *macPANId* to the default value (0xffff).”

**Item 4)** IEEE Std 802.15.4-2006

Change required:

The device should stop sending its own beacon and inform the next higher layer by generating an MLME-SYNC-LOSS.indication with status of SUPERFRAME\_OVERLAP.

Note:

This status enumeration was added in 15.4-2006 as a status for the MLME-START.confirm message to cover the condition described when it occurs during the MLME-START.request.

**Item 5)** IEEE Std 802.15.4a-2007

The above raise two issues firstly there is an error in equation for the reference pulse ,*r*(*t*), in section 6.8a.12.1(draft 7) it should be :



Secondly the requestor asks for a clarification of the pulse width parameter, *Tp*. According to the corrected equation for *r*(*t*) above the parameter *Tp* is the half pulse amplitude point.  So for example if *Tp* = 2 *ns* then r(-1) = r(1) = r(0)/2.

**Item 6)** IEEE Std 802.15.4-2006

Proposed resolution is to replace clause 7.5.8.2.3 with:

**7.5.8.2.3 Incoming frame security procedure**

The input to this procedure is the frame to be unsecured. The outputs from this procedure are the unsecured frame, the security level, the key identifier mode, the key source, the key index and the status of the procedure.

All outputs of this procedure are assumed to be invalid unless and until explicitly set in this procedure.

It is assumed that the PIB attributes associating KeyDescriptors in *macKeyTable* with a single, unique device or a number of devices will have been established by the next higher layer.

The incoming frame security procedure involves the following steps:

1. If the security enabled subfield of the frame control field of the frame to be unsecured is set to zero, the procedure shall set the security level to zero.
2. If the security enabled subfield of the frame control field of the frame to be unsecured is set to one and the frame version number of the frame control field of the frame to be unsecured is set to zero, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of UNSUPPORTED\_LEGACY.
3. If the security enabled subfield of the frame control field of the frame to be unsecured is set to one, the procedure shall set the security level and the key identifier mode to the corresponding subfields of the security control field of the auxiliary security header of the frame to be unsecured, and the key source and key index to the corresponding subfields of the key identifier field of the auxiliary security header of the frame to be unsecured, if present. If the resulting security level is zero, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of UNSUPPORTED\_SECURITY.
4. If the *macSecurityEnabled* attribute is set to FALSE, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of SUCCESS if the security level is equal to zero and with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of UNSUPPORTED\_SECURITY otherwise.
5. The procedure shall obtain the SecurityLevelDescriptor by passing the frame type and depending on whether the frame is a MAC command frame, the first octet of the MAC payload (i.e., command frame identifier for a MAC command frame) to the SecurityLevelDescriptor lookup procedure described in 7.5.8.2.10. If that procedure fails, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of UNAVAILABLE\_SECURITY\_LEVEL.
6. The procedure shall determine whether the frame to be unsecured conforms to the security level policy by passing the SecurityLevelDescriptor and the security level to the incoming security level checking procedure as described in 7.5.8.2.11. If that procedure returns with a failed status, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of IMPROPER\_SECURITY\_LEVEL; otherwise, if that procedure returns with a passed status and the security level is equal to zero, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of SUCCESS.
7. The procedure shall obtain the DeviceDescriptor using the incoming frame device retrieval procedure described in 7.5.8.2.5. If that procedure fails, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of UNAVAILABLE\_DEVICE.
8. If the incoming security level checking procedure of Step f above had as output the ‘conditionally passed’ status, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of SUCCESS if the Exempt element of the DeviceDescriptor is set to TRUE and with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of IMPROPER\_SECURITY\_LEVEL otherwise.
9. The procedure shall set the frame counter to the frame counter field of the auxiliary security header of the frame to be unsecured. If the frame counter has the value 0xffffffff, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of COUNTER\_ERROR.
10. The procedure shall determine whether the frame counter is greater than or equal to the Frame-Counter element of the DeviceDescriptor. If this check fails, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of COUNTER\_ERROR.
11. The procedure shall obtain the KeyDescriptor using the incoming frame key retrieval procedure described in 7.5.8.2.4. If that procedure fails, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of UNAVAILABLE\_KEY.
12. The procedure shall obtain the KeyDeviceDescriptor using the KeyDeviceDescriptor lookup procedure described in 7.5.8.2.7. If that procedure fails or if the Blacklisted element of the KeyDeviceDecriptor is set to TRUE, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of KEY\_ERROR.
13. The procedure shall determine whether the frame to be unsecured conforms to the key usage policy by passing the KeyDescriptor, the frame type and depending on whether the frame is a MAC command frame, the first octet of the MAC payload (i.e., command frame identifier for a MAC command frame) to the incoming key usage policy checking procedure as described in 7.5.8.2.12. If that procedure fails, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of IMPROPER\_KEY\_TYPE.
14. The procedure shall then use the ExtAddress element of the DeviceDescriptor, the frame counter, the security level and the Key element of the KeyDescriptor to produce the unsecured frame according to the CCM\* inverse transformation process described in the security operations (see 7.6.3.5).
	1. If the security level specifies the use of encryption (see Table 96), the decryption operation shall be applied only to the actual payload field within the MAC payload, i.e., the beacon payload field (see 7.2.2.1.8), command payload field (see 7.2.2.4.3), or data payload field (see 7.2.2.2.2), depending on the frame type. The corresponding payload field shall be passed to the CCM\* inverse transformation process described in 7.6.3.5 as the secure payload.
	2. The remaining fields in the MAC payload part of the frame shall be passed to the CCM\* inverse transformation process described in 7.6.3.5 as the non-payload fields (see Table 100).
	3. The ordering and exact manner of performing the decryption and integrity checking operations and the placement of the resulting decrypted data within the MAC payload field shall be as defined in 7.6.3.5.
15. If the CCM\* inverse transformation process fails, the procedure shall set the unsecured frame to be the frame to be unsecured and return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of SECURITY\_ERROR.
16. The procedure shall increment the frame counter by one and set the FrameCounter element of the DeviceDescriptor to the resulting value.
17. If the FrameCounter element is equal to 0xffffffff, the procedure shall set the Blacklisted element of the KeyDeviceDescriptor to TRUE.
18. The procedure shall return with the unsecured frame, the security level, the key identifier mode, the key source, the key index and a status of SUCCESS.

Item 7)

Change the 15.4-2006 phrase "**one of the optional PHYs"** to "**one of the optional PHYs described in 6.7 and 6.8**" This change clarifies that the requirement is limited to the PHYs introduced with the 2006 standard and not the TG4g amendment.

Item 8) IEEE Std 802.15.4a-2007

The stated interpretation is wrong because it results in the first data bit having less redundancy than the other bits. Annex I clearly shows that this first symbol IS transmitted. Nonetheless, to avoid misinterpretation, the main body of the text shall be changed to explicitly state that this symbol is transmitted.

Item 9) IEEE Std 802.15.4a-2007

IEEE Std 802.15.4a-2007 Annex M of D6 page 194 in Table M1: The equation for C5 should be: C5 = XOR(R1, R0, L6, L5, L4, L3, L2, L1, L0, RNG, EXT, P1, P0, C4, C3, C2, C1, C0)

Item 10) IEEE Std 802.15.4a-2007

Fig 27b needs to be corrected to show 21 symbols in the header and 0-1208 symbols in the data.

Add following table after 27b:



Item 11) IEEE Std 802.15.4a-2007 - No change, Figure 27j is not wrong

Item 12) IEEE Std 802.15.4a-2007 - No change, document is correct

Item 13) IEEE Std 802.15.4a-2007

From the text on page 77 describing the optional long SFD we are "spreading" the sequence (Si) with the long SFD sequence. So each 1 or -1 in the long SFD sequence corresponds to the transmission of the sequence 1\*(Si) or -1\*(Si). The last number in the SFD sequence is +1 which would give a positive sign and the 22nd number is -1 which would give a negative sign. The corrected Figure 27d is shown below:



Item 14) IEEE Std 802.15.4a-2007 - Change Figure 27m, pg 83 to that resolution as shown in Item 15

Item 15) IEEE Std 802.15.4a-2007

the reference pulse , *r*(*t*), does not meet the PSD requirements. On this second concern the commenter is correct. The PSD of the reference pulse is slightly higher then -10dBr at the frequency of 0.65/*Tp*. It is the view of the editors that it would make sense for the reference pulse itself to be a valid UWB pulse. A simple modification of the Beta (β) value achieves this. We recommend that a value of β = 0.5 be used in the reference pulse formula given in section 6.8a.12.1. More specifically, on page 88, line 18 the phrase “roll-off factor β = 0.6” should be changed to “roll-off factor β = 0.5” This change would also effect Figure 27m also in section 6.8a.12.1 since the shape of the reference pulse is modified by adjusting the roll-off factor. Figure 27m should therefore, be replaced with the following:



Item 16) IEEE Std 802.15.4a-2007 - No change is needed since this issue does not affect the necessary behavior

Item 17) IEEE Std 802.15.4a-2007 - Table 39c: delete rows Nhdr, Thdr, N data, Tdata

Item 18) IEEE Std 802.15.4a-2007 –

Change text for clauses 6.8a.8 (Data Field), 6.8a.9 (UWB PHY Modulation) and 6.8a.10 (UWB PHY FEC) to state that the even bits are for position and the odd bits are for polarity

Item 19) IEEE Std 802.15.4-2006

Change 7.5.6.1 last paragraph: add to the beginning of the first sentence “ If the status is success…”