**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **IEEE 802.15.4-2006 Corrigenda Items** |
| Date | March 18, 2010 |
| Source | René StruikCerticom Corp.5520 Explorer Drive, 4th FloorMississauga, ON L4W 5L1 | E-mail: rstruik@certicom.comPhone: +1 (905) 501-6083Fax: +1 (905) 507-4230 |
| Re: | 08/849r0  |
| Abstract | This document outlines changes to be incorporated with 802.15.4-2006 and is a companion document to 08/849r0, which specifies a streamlined version of Clauses 7.5.8 and 7.6 of IEEE 802.15.4-2006. |
| Purpose | Correct ambiguities and small errors and omissions with IEEE 802.15.4-2006 |
| 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. |

**§5.1 Introduction**

1. While most RFDs are expected to talk only to an FFD, technically, RFD devices can certainly talk to other RFD devices. This has been a source of lots of confusion with users of the standard. **Suggested remedy:** Remove the unenforceable policy statement “An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD.” (p. 13).

**§7.4.2 MAC PIB Attributes**

1. The MAC PIB attribute *macSecurityEnabled* is set to FALSE by default (§7.4.2, cf. Table 86, p. 185). It seems more appropriate to set this to TRUE, since security capability should be switched on, rather than off, by default. Moreover, virtually all 802.15.4 chipsets in existence today have cryptographic support for security implemented. **Suggested remedy:** set to TRUE by default.
2. Access to MAC PIB attributes can be either Read/Write or Read by the higher layer using the MLME-GET.request and MLME-SET.request primitives (cf. §7.4.2, Table 86; §7.6.1, Tables 88-94). From a security perspective, access to keys themselves by higher layers should not be possible (one should be able to write these, but not read these). Similarly, other (non-secret) security parameters that influence the semantics of outgoing and incoming frame security processing (such as security level parameters, etc.) should be written to only if explicitly authorized. **Suggested remedy:** Add language to the effect that the higher layer may impose additional constraints on Read/Write operations without making those devices non-compliant.

**§7.5.6.1 Transmission**

1. If the outgoing frame security procedure is not successful, the frame should not be further processed or sent. **Suggested remedy:** Clarify text accordingly (similar to conditional language on how to deal with incoming frame security processing that is not successful – cf. §7.5.6.2, p. 187).

**§7.5.6.2 Reception and rejection**

1. The current filtering procedure may accept frames originating from the receiving device itself (thus, providing looped behavior). **Suggested remedy:** With third level filtering, silently drop frames purportedly sent from the recipient device itself (this is a primitive level of “source address filtering”).

**§7.5.6.3 Extracting pending data from a coordinator**

1. On p. 188, the sentence “If the requesting device does not receive a data frame from the coordinator within *macMaxFrameTotalWaitTime* CAP symbols in a beacon-enabled PAN, or symbols in a nonbeacon-enabled PAN,…” seems to be missing a MAC PIB parameter. **Suggested remedy:**  Correct accordingly (Note RS: not sure which parameter this should be).

**§7.5.8.2.1 Outgoing frame security procedure**

1. The current outgoing frame security procedure does not check whether so-called “frame counter role-over” may have occurred. **Suggested remedy:** implement this check via a corresponding Blacklisted element. Note RS: unfortunately, this results in some reorganization of MAC PIB attributes and procedures. For details, please cf. 08/849r0, Steps g), h), and l), and Table 91 – Blacklisted element.

**§7.5.8.2.3 Incoming frame security procedure**

1. The current incoming frame security procedure does not properly treat devices with so-called diplomatic immunity status (Exempt status), since one never gets into checking this status of the security level is set to zero (cf. Step f), resp. i)). This prevents the main use case for this Exempt status flag, viz. temporarily allowing unsecured frames for devices in the process of joining a network (and, thereby, prior to obtaining keying material). **Suggested remedy:** Implement this properly, as specified in 08/848r0. Note RS: unfortunately, this seemingly results in massive changes, due to need to untie some of the procedures. In summary, one needs to replace the entire clause by the one stipulated with 08/849r0.
2. The current security level checking procedure accepts incoming frames with a security level that is greater than or equal to a particular minimum security level (as defined in Table 92 – SecurityLevelDescriptor, p. 209). In particular, if this minimum security level is set to zero, this allows receipt of frames that are protected with confidentiality only and without authenticity (security level 0x04). Unfortunately, this may have as side effect that one can manipulate the frame counter entry of the sending device as stored on the recipient device and set this to any value (including 0xffffffff, thereby disabling further communication from that device). This can be prevented by always only allowing secured traffic, but this would hamper flexibility (since now joining devices always have to use Exempt flags and, e.g., unsecured association commands open this up to vulnerabilities). This clearly was not intended. **Suggested remedy:** replace the minimum security level by a set of security levels allowed. Note RS: for details, please see 08/849r0, Step f), §7.5.8.2.11, Table 95 – SecurityModeDescriptor).

**§7.5.6.4 Use of acknowledgements and retransmissions**

1. The mechanism for handling acknowledgements is very poorly described. Lots of information seems to be missing and left as an exercise to the implementer. As an example, §7.5.6.2 does not describe at all how to handle incoming acknowledgement frames: although after rereading the first, second, third level filtering paragraphs multiple times, it seems that acknowledgement frames indeed are processed further, but no reference is made at all to how this is done. In fact, it is suggested that also for acknowledgement frames, the incoming frame security procedure is invoked, but this would fail, since for acknowledgement frames the security enabled subfield of the frame control field is ignored (thus failing §7.5.8.2.3, Step a) – something currently not captured in that procedure); moreover, the security level test (Step e) may fail, since most implementers may not have implemented entries for acknowledgment frames (cf. Table 92, p. 209). The matching procedure of sent frame and corresponding acknowledgement via DSN entry, nor time-outs for keeping this info on the sending device are very poorly, if at all, described. **Suggested remedy:** not sure what to do, since a mystery to me.