Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)

Submission Title: security related CIDs in draft D1
Date Submitted: June 2010
Source: Erman Ayday and Sridhar Rajagopal [Samsung Electronics]
Address:
Contact Information: [sridhar.r@samsung.com]

Re:

Abstract: proposes comment resolutions for a set of CIDs

Purpose:

Comments for CIDs

644,720, 727, 769, 771, 773, 658, 776, 777, 778, 779

CID 644

Comment:

- (TR) §7.2, p. 131ff: It seems that all security provisions of 802.15vlc borrow heavily from 802.15.4-2006. Unfortunately, some of those have small inaccuracies and errors, which are supposed to be tackled with the Corrigendum effort 802.15.4h. Since 802.15vlc does not seem to end up as an amendment of 802.15.4-2006, it seems prudent to incorporate all corrigenda items considered with 802.15.4h and relevant to the Visible Light Communications TG with the 802.15vlc as well. This includes the material in 10/213r1.

Suggested remedy

- make according edits.

Instruction to editor

- Reject. There are already specific comments received for security that have been addressed. There is no need to make the security section dependent on another standard. VLC, due to visibility, has some inherent security characteristics. VLC also does not support a distributed multihop topology such as those used in 802.15.4-2006, reducing its security support requirements.

CID 720

Comment:

- (TR) §7.4.2, p. 163, l. 23-29: Table 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 85; §7.7.1, Tables 95-100). 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.

Instruction to editor

- Section 7.4.2 Line 30, Page 163. Add "**Higher layer may impose additional constraints on read/write operations, without making devices non-compliant**"

CID 727

Comment:

- (TR) §7.4.2, p. 167, Table 85: The MAC PIB attribute *macSecurityEnabled* is set to FALSE by default. 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.

Instruction to editor

- Accept. **Set TRUE by default in Table 85.**

CID 769

Comment:

- ((TR) §7.6.6.1, p. 190, l. 45ff: 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. §7.6.6.2, p. 192).

Instruction to editor

- accept. Section 7.6.8.2.1. page 203, Line 23. Add **"If outgoing frame security procedure is not successful, frame is discarded"**

CID 771

Comment:

- (TR) §7.6.6.2, p. 191, l. 33-43: 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”).

Instruction to editor

- accept. Section 7.6.8.2.3, page 205, line 25. Add **"Incoming frames originating from the receiving device should be directly filtered and the incoming frame security procedure is not applicable.”**

CID 773, 658

Comment:

- (TR) §7.6.6.4, p. 193ff: 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, §7.6.6.4.2 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 §7.6.8.2.3, 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 99, p. 243). 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.
- (TR) §7.2.2, p. 140: It seems imprudent to use acknowledgement frames with a payload field that do not allow for protection of the authenticity of the frame itself, esp. if this serves as more than a simple communication acknowledgement and has piggy-backed information in the payload field.

Suggested remedy

- not sure what to do, since a mystery to me.
- Define a secure acknowledgement frame or adopt the secured acknowledgment frame as also specified with 802.15.4e.

Instruction to editor

- Accept. Section 7.2.2.2.1, Page 141. Line 8. Add **"All other subfields except the security enabled subfield shall be set to zero"**

CID 776

Comment:

- Is the frame counter incremented for retries (of the same frame) as well? How is replay detection and filtering done?

Suggested remedy

- Make them clear.

Instruction to editor

- For all packets, frame counter is increased by 1. The receiver accepts equal or greater than frame counter element of device descriptor. See Page 206. Section 7.6.8.2.3, line 32. Note to editor : No change needed.

CID 777

Comment:

- (TR) §7.6.8.2.1, pp. 203-204: 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.

Instruction to editor

- Accept comment. Different remedy. Section 7.6.8.2.1, Page 203, line 49. Add “After the frame counter has value of 0xffffffff, the procedure returns with status of COUNTER_ERROR **and all keys associated with the device are reinitialized and updated as discussed in Section 7.6.8.1.4”** (page 202, line 36.)

CID 778

Comment:

- (TR) §7.6.8.2.3, p. 205-207: 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 if 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 08/849r0. 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.

Instruction to editor

- Reject. We do not need to support such devices since we do not support a distributed architecture like 802.15.4

CID 779

Comment:

- TR) §7.6.8.2.8, p. 209: 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 802.15.4e document 08/849r0, Step f), §7.5.8.2.11, Table 95 – SecurityModeDescriptor).

Instruction to editor

- Accept in part. Section 7.6.8.2.8 Line 28, page 209. Add "**It is recommended to use MIC for all secure messages as defined in Table 102."**