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

Submission Title: IG SEC Outbound state machine changes
Date Submitted: 17 May, 2014
Source: Tero Kivinen, **Company:** INSIDE Secure
Address: Eerikinkatu 28, FI-00180 Helsinki, Finland
Voice:+358 20 500 7800, **FAX:** +358 20 500 7801, **E-Mail:** kivinen@iki.fi

Re: IG SEC Outbound state machine changes

Abstract: IG SEC changes required for the outbound state machine for proposed solution for the macFrameCounter issue

Purpose:

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.

IG SEC Outbound State Machine

Tero Kivinen

Teleconference meeting 2014-05-27

May 27, 2014

Outbound State Machine Changes

- Based on FrameCounter presentation 15-14-0299-00
- Based on the IEEE 802.15.4 Security Selection Excerpt 15-14-0320-00
- Changes to Section 8.2.1

Proposed Solution

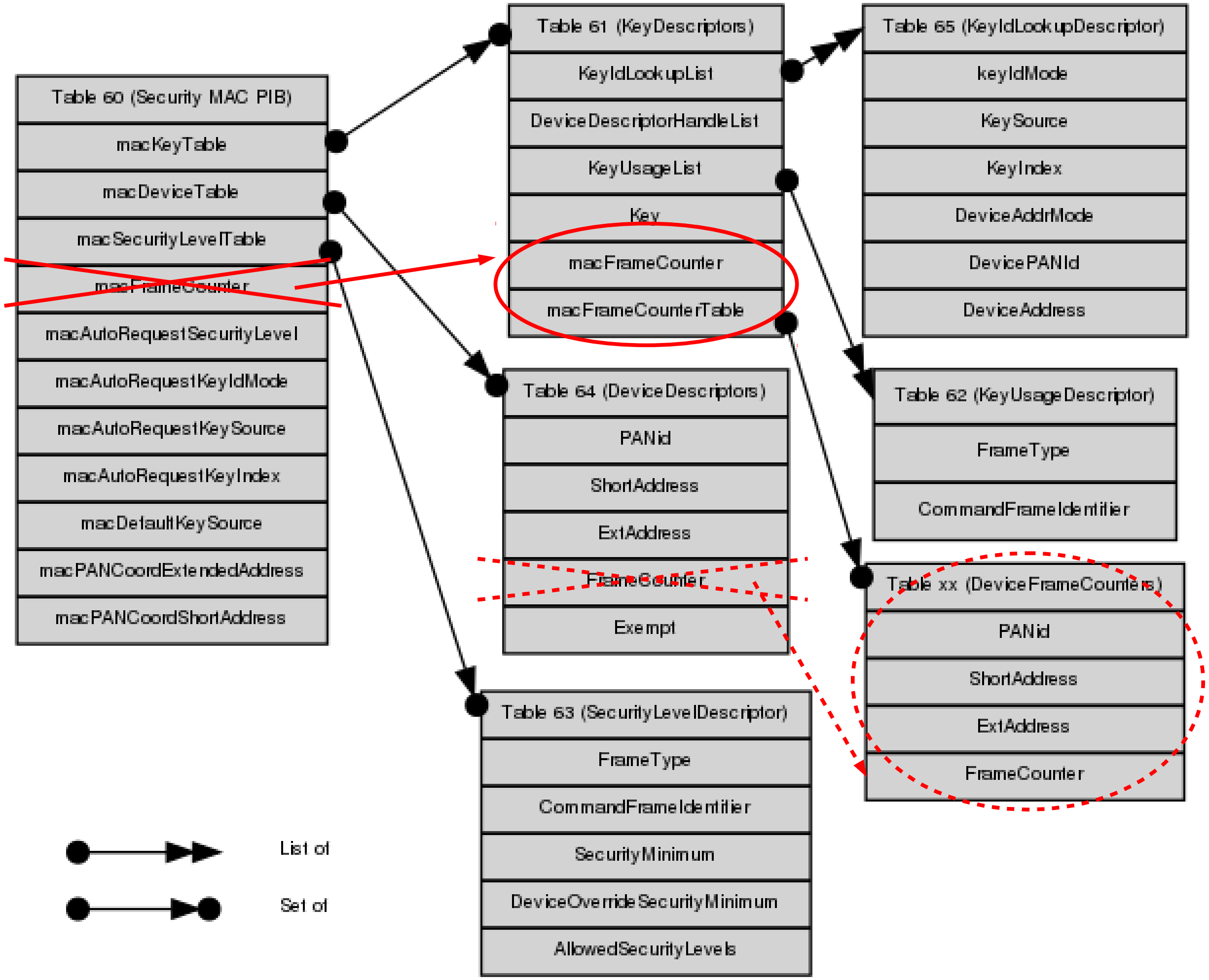

Table 60 (Security MAC PIB)
macKeyTable
macDeviceTable
macSecurityLevelTable
~~macFrameCounter~~
macAutoRequestSecurityLevel
macAutoRequestKeyIdMode
macAutoRequestKeySource
macAutoRequestKeyIndex
macDefaultKeySource
macPANCoordExtendedAddress
macPANCoordShortAddress

Table 61 (KeyDescriptors)
KeyIdLookupList
DeviceDescriptorHandleList
KeyUsageList
Key
macFrameCounter
macFrameCounterTable

Table 65 (KeyIdLookupDescriptor)
keyIdMode
KeySource
KeyIndex
DeviceAddrMode
DevicePANId
DeviceAddress

Table 64 (DeviceDescriptors)
PANid
ShortAddress
ExtAddress
~~FrameCounter~~
Exempt

Table 62 (KeyUsageDescriptor)
FrameType
CommandFrameIdentifier

Table xx (DeviceFrameCounters)
PANid
ShortAddress
ExtAddress
FrameCounter

Table 63 (SecurityLevelDescriptor)
FrameType
CommandFrameIdentifier
SecurityMinimum
DeviceOverrideSecurityMinimum
AllowedSecurityLevels

List of

Set of

Actual Changes

- The steps m) and n) needs to be swapped:
  - Step m) uses macFrameCounter and checks it does not overflow and sets it to FrameCounter
  - Step n) fetches the KeyDescriptor using procedure described in 8.2.2

8.2.1 m) and n)

- m) The procedure shall set the frame counter to the *macFrameCounter* attribute. If the frame counter has the value 0xffffffff, the procedure shall return with a status of COUNTER_ERROR.
- n) The procedure shall obtain the KeyDescriptor using the KeyDescriptor lookup procedure as described in 8.2.2 with the device addressing mode set to DstAddrMode, the device PAN ID set to DstPANID, and the device address set to DstAddr. If that procedure fails, the procedure shall return with a status of UNAVAILABLE_KEY.

Actual Changes, cont

- Change it so that we will first fetch the KeyDescriptor (old step n)
- And then next step will use the macFrameCounter fetched from the KeyDescriptor located in previous step (old step m)

Other things

- In step m) it does not take in to account the 5-byte frame counter, it always compares the frame counter to 0xffffffff.
- On the other hand is the 5-byte frame counter only used with TSCH, and if so then frame counter is not incremented, but ASN is used instead.