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

Submission Title: macFrameCounter problems
Date Submitted: 12 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: macFrameCounter problems

Abstract: This document describes the problems with current global macFrameCounter

Purpose: How to fix macFrameCounter issue.

MacFrameCounter problem

Tero Kivinen

Kona, HI

May 14, 2014

The problem

- macFrameCounter is global to device
- FrameCounter is per remote peer

2011 MAC PIB

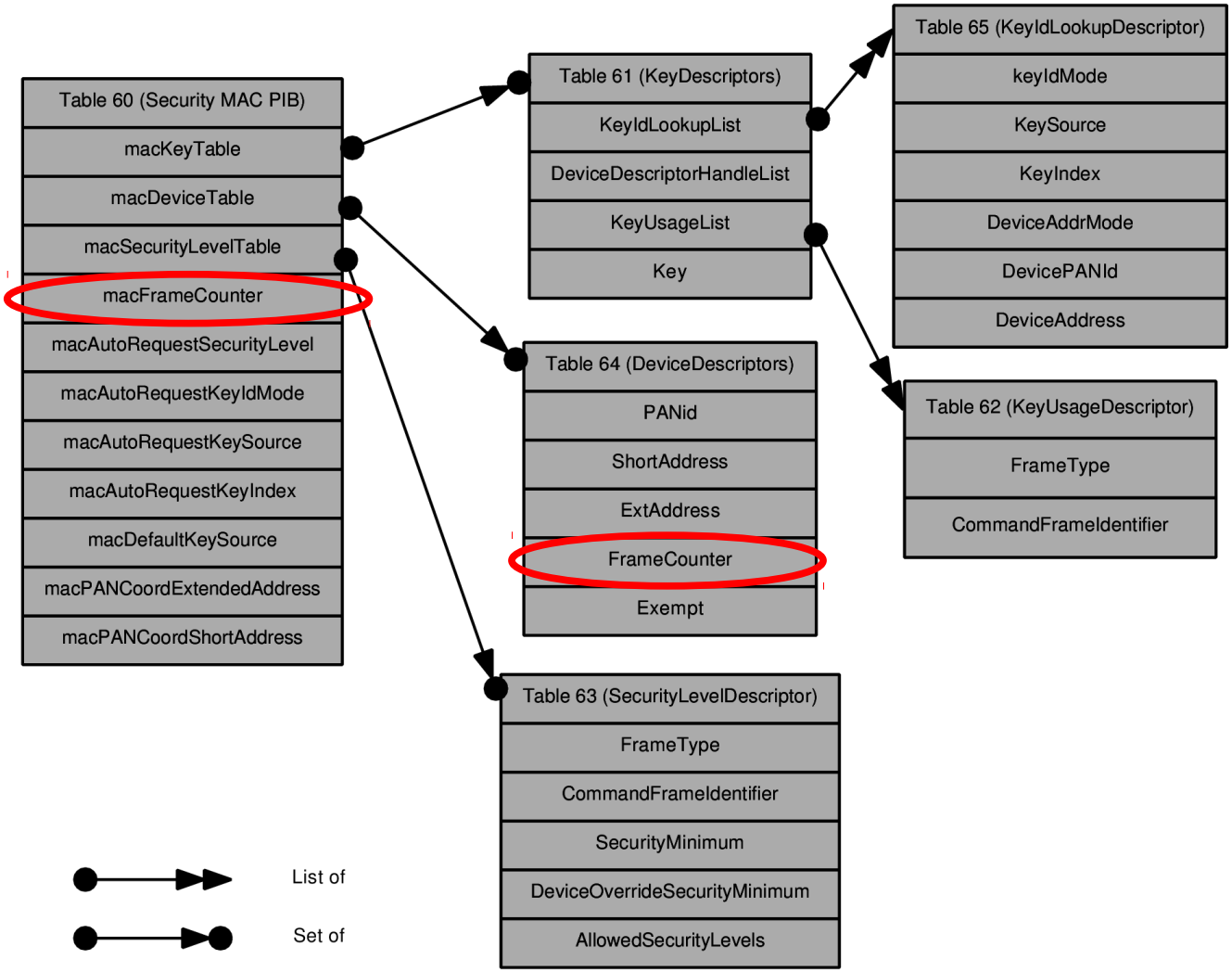
Table 60 (Security MAC PIB)
macKeyTable
macDeviceTable
macSecurityLevelTable
macFrameCounter
macAutoRequestSecurityLevel
macAutoRequestKeyIdMode
macAutoRequestKeySource
macAutoRequestKeyIndex
macDefaultKeySource
macPANCoordExtendedAddress
macPANCoordShortAddress
Table 61 (KeyDescriptors)
KeyIdLookupList
DeviceDescriptorHandleList
KeyUsageList
Key
Table 65 (KeyIdLookupDescriptor)
keyIdMode
KeySource
KeyIndex
DeviceAddrMode
DevicePANId
DeviceAddress
Table 64 (DeviceDescriptors)
PANid
ShortAddress
ExtAddress
FrameCounter
Exempt
Table 62 (KeyUsageDescriptor)
FrameType
CommandFrameIdentifier
Table 63 (SecurityLevelDescriptor)
FrameType
CommandFrameIdentifier
SecurityMinimum
DeviceOverrideSecurityMinimum
AllowedSecurityLevels
List of
Set of

macFrameCounter

- This is global to device
  - This is used when sending packets out
    - I.e regardless who the device sends packet to or what key is used the counter is incremented.
- When this reaches 0xffffffff it is not clear what should happen, and how to recover from that.
  - To recover from this, the peer needs to notify all peers it has ever talked to that his macFrameCounter will be reset.
  - If this is not done, then others will drop all his frames as they have too low FrameCounter in the packet.
  - There is no specification telling how to recover.
  - With 1Mbit/s speed, device sending data at full speed that is about 50 days

macFrameCounter continued

- Normally when you rekey the security association you also reset the replay counters so you will not run out of them.
  - Currently there is no text saying what rekey will do to macFrameCounter.
  - This is left to the upper layer, and there is no protocol that I know of to take care of it.
  - When device sending at full speed needs to rekey its unicast key, the whole network will also need to rekey its broadcast key.

macFrameCounter and multiple keys

- One of the reasons for multiple keys between peers is to have different replay counters
  - What are the reasons in 802.154 for having multiple keys between the peers if not that?
- With global counter:
  - You cannot for example create multiple keys at once and start using next one when first one needs to be rekeyed because it is running out of sequence number space.
  - You cannot create separate key for device where you are sending lots of data.
  - Cannot create low volume broadcast key for broadcasts and high volume unicast key for the peer sending lots of data

FrameCounter

- This is per remote peer
  - Identified by PANId, ShortAddress, ExtAddress
  - This is used to check the replay attacks, i.e. if incoming FrameCounter from the device is smaller than this it is dropped.
  - This makes it useless to have multiple keys between same peers

What should be done

- macFrameCounter needs to be per key:
  - should be moved to the KeyDescriptors table.
  - It should be incremented every time key is used.
- FrameCounter needs to be per key and per remote peer.
  - DeviceDescriptors table should have keyIdLookupList having list of keyIdLookupDescriptor, i.e. having KeyIndex and other information too.

New MAC PIB

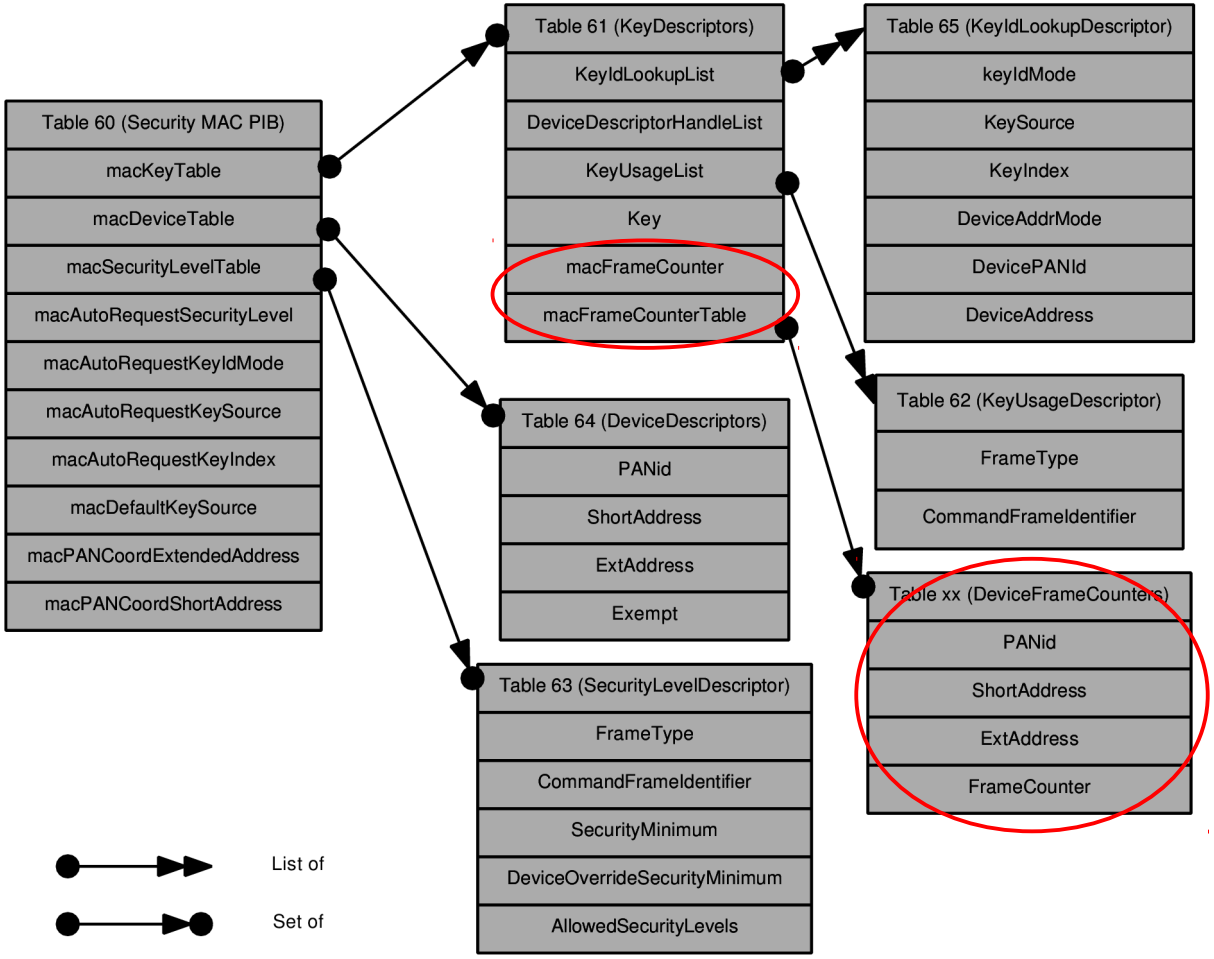
Table 60 (Security MAC PIB)
macKeyTable
macDeviceTable
macSecurityLevelTable
macAutoRequestSecurityLevel
macAutoRequestKeyIdMode
macAutoRequestKeySource
macAutoRequestKeyIndex
macDefaultKeySource
macPANCoordExtendedAddress
macPANCoordShortAddress
Table 61 (KeyDescriptors)
KeyIdLookupList
DeviceDescriptorHandleList
KeyUsageList
Key
macFrameCounter
macFrameCounterTable
Table 65 (KeyIdLookupDescriptor)
keyIdMode
KeySource
KeyIndex
DeviceAddrMode
DevicePANId
DeviceAddress
Table 62 (KeyUsageDescriptor)
FrameType
CommandFrameIdentifier
Table 64 (DeviceDescriptors)
PANid
ShortAddress
ExtAddress
Exempt
Table xx (DeviceFrameCounters)
PANid
ShortAddress
ExtAddress
FrameCounter
Table 63 (SecurityLevelDescriptor)
FrameType
CommandFrameIdentifier
SecurityMinimum
DeviceOverrideSecurityMinimum
AllowedSecurityLevels
List of
Set of

Why this was not problem earlier

- Only problem if you are using multiple keys between peers, i.e. have KeyIdMode that is not 0x00, and you have multiple KeyIndex values between peers.
- Only really problem if you are doing rekey.
- Might be bigger problem when bigger networks want to use multiple keys and do not want to rekey all of them at the same time